9-14-2017

Biologically Inspired Network (BiONet) Authentication using Logical and Pathological RF-DNA Credential Pairs

Tyrone A.L. Lewis Sr.

BIOLOGICALLY INSPIRED NETWORK (BIONET) AUTHENTICATION USING LOGICAL AND PATHOLOGICAL RF-DNA CREDENTIAL PAIRS

DISSERTATION

Tyrone A. L. Lewis Sr, Major, USA

AFIT-ENG-DS-17-S-012

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY
AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

AFIT-ENG-DS-17-S-012

BIOLOGICALLY INSPIRED NETWORK (BIONET) AUTHENTICATION USING LOGICAL AND PATHOLOGICAL RF-DNA CREDENTIAL PAIRS

DISSERTATION

Presented to the Faculty

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Doctor of Philosophy

Tyrone A. L. Lewis Sr, MS

Major, USA

September 2017

AFIT-ENG-DS-17-S-012

BIOLOGICALLY INSPIRED NETWORK (BIONET) AUTHENTICATION USING LOGICAL AND PATHOLOGICAL RF-DNA CREDENTIAL PAIRS

Tyrone A. L. Lewis Sr, MS

Major, USA

Committee Membership:

Kenneth M. Hopkinson, PhD
Chairman

Bryan J. Steward, PhD
Member

Maj Joan A. Betances
Member

ADEDJI B. BADIRU, PhD
Dean, Graduate School of Engineering and Management

Abstract

The command and control (C2) of shared space resources are vulnerable to logical credential forgery and impersonation attacks among standardized and interoperable wireless radio frequency (RF) networks. Threats could come from trusted operators (insiders) or from external sources (outsiders). An attacker may gain unauthorized network access and illegally cross into C2 boundaries when conventional network authentication fails. This research proposes an integrated trust management system that uses both application-layer and physical-layer trust markers to authenticate users and their communication sources. In essence, the results from physical-layer RF-DNA fingerprinting techniques are used to improve application-level trust schemes based on command patterns, message structure, and other discernible markers through the use of Bayesian reasoning using an approach adapted from the medical disease diagnostic testing community. In this adapted approach, trust markers of behavior can be used to detect deviations from what is expected, sometimes called byzantine behavior. Suspect communication or traffic patterns are labeled as eNDs (electronic network-diseases). Trust management enabled devices consider the diagnostics of logical and pathological RF-DNA credential pairs and application-layer trust markers to predict and mitigate such eNDs. The method introduced in this dissertation demonstrates an end-to-end physical RF network prototype; introduces a tracking capability for multi-organizational access, and improves upon the accuracy of credential pair identification using either physical-layer or application-layer techniques in isolation.

In the experiments run, the discrimination of insider vs. outsider threats improved by 22%, uplink availability was extended by 51.2% for non-offenders, and the proposed trust system achieved 100% posterior predictions using moderate tolerance settings. The trust system also reduced logical credential forgery acceptance by 84% among tested samples. The system shows promise for more general application in domains including Cyber, Space and eHealth ecosystems.

Acknowledgments

I dedicate this dissertation to my battle buddy and big brother, whom I lost on January 1, 2017 at the hands of untrained police officers that failed to consider the early warning signs and indicators of living with mental illness. I pray that education and training efforts improve among our police force so that the goal of service and protection of life is more equally applied towards those living with mental illness. Through such understanding, improved policy based responses may be modified when indicators of mental illness are suspected and false positive use of lethal force, as corrective treatment, may be avoided or significantly reduced.

Thanks mom and dad for giving me life, love, encouragement and support. Thanks to Dr. Wilhoit for paving the way. Thanks to my sisters for always being there for me. To my children, I love you all. A special thanks to my advisor Dr. Hopkinson, Mr. Sines and Dr. Davis for believing in me and giving me this awesome opportunity. To my Uncle for teaching me to never give up. To my cousin for challenging me to 're-think' my way through life's challenges. A special thanks to my peers, fraternity brothers and friends that supported me throughout this journey. Finally, thank you to my *beautiful* for being my strength in times of weakness, for lending an ear when I needed an audience, for showing me love when I felt alone.

Be brave, be imaginative, be correct… but most of all be unafraid to think outside the box.

Tyrone A. L. Lewis Sr.

Table of Contents

Page

List of Figures

Page

List of Tables

Page

List of Acronyms

AAR	Authorized Acceptance Rate
AFIT	Air Force Institute of Technology
AFSK	Audio Frequency Shift Key
BiONet™	Biologically Inspired Network (Trademark Pending)
dB	Decibel
dT	Decision Threshold
CDH	Command Data Handler
CTMS	Consolidated Trust Management System
DOI	Device of Interest
DRA	Dimension Reduction Analysis
DNA	Deoxyribonucleic Acid
e-CFR	Electronic Code of Federal Regulations
eND	Electronic Network-Disease
FCC	Federal Communications Commission
FP	False Positive
FPR	False Positive Rate
FOR	False Omission Rate
FDR	False Discovery Rate
FVR	False Verification Rate
FPrint	Fingerprint
FM	Frequency Modulation
GMSK	Gaussian Minimum Shift Key

GPS	Global Positioning System
GS	Ground Station
GRLVQI	Generalized Relevance Learning Vector Quantization-Improved Relevance Ranking
iMkr	Indexed Marker Key
ITV	Interaction Trust Value
I-Q	In Phase & Quadrature Phase
LOS	Line of Sight
MAC	Media Access Control (Layer 2 of the OSI Model)
MDA	Multiple Discriminate Analysis
MDA/ML	Multiple Discriminate Analysis/Maximum Likelihood
ML	Maximum Likelihood
ND	Network-Disease
NPV	Negative Predictive Value
NWK	Network (Layer 3 of the OSI Model)
OSI Model	Open Systems Interconnections Model
P2P	Point to Point Network Connection
PPV	Positive Predictive Value
PHY	Physical (Layer 1 of the OSI Model)
RAR	Imposter Acceptance Rate
RF	Radio Frequency
RF-Biomarker	RF-Biological Marker of eND
RF-DNA	Radio Frequency Distinct Native Attribute

RF-measurementB	RF-measurement Bridge
ROC	Receiver Operating Curve
ROI	Region of Interest
RRR	Rogue Rejection Rate
Rx	Receiver
SATCOM	Satellite Communications
SHR	Synchronization Header Response
SOI	Signal of Interest
SN	Sequence Number
SNR	Signal to Noise Ratio
TP	True Positive
TPR	True Positive Rate
TN	True Negative
TNR	True Negative Rate
TVR	True Verification Rate
Tx	Transmitter
UHF	Ultra High Frequency

BIOLOGICALLY INSPIRED NETWORK (BIONET) SECURITY BOUNDARY PROTECTION

Look deep into nature… and then you will understand… (Albert Einstein)

I. Introduction

1.1 Background

The overarching goal of this research aims to discover, characterize and propose a multi-factor credential pairing framework that enhances the mitigation of fraudulent (*infectious*) credential acceptance and unauthorized access into electronic network security boundaries. Early symptoms of network abnormalities, resulting from the acceptance of *infectious* credentials, may originate from *insider* (trusted) or *outsider* (untrusted) electronic sources and, if not properly treated, may lead to a total loss of resource availability (e.g. a distributed denial of service (DDoS) attack) for critical ground resources that support multi-organizational missions in *non-benign* environments. A policy-based categorization of abnormal behavior is informally termed electronic *network-disease (eND).* An investigative study is conducted to quantify the inherent physical RF origin attributes that best predict *eND* using Bayes Theorem in uncertainty to enhance the situational awareness (SA) of Operators and key players whom defend otherwise healthy RF networks. More specifically, a representative miniaturized ultra-high frequency (UHF) CubeSat uplink access boundary, protected using a conventional distributed consolidated trust management system (CTMS) [1] [2], integrates pathological RF-Biomarkers of *eND* to validate the origin integrity of logical credential claims [3] [4] [5] [6].

The hypothesis herein is that logical (digital bit pattern matching) and pathological (trusted RF-Measurements of logical credential transmissions) network access credential pairing may improve conventional authentication schemes in non-benign electronic RF environments.

1.2 Motivation.

Deoxyribose nucleic acid (DNA) was originally invented by Sir Alec Jeffery in 1984, whose initial application of genetic fingerprinting using *DNA* was purposed to control immigration border crossings between established physical geographic boundaries [7] [8]. During this process, the original blood samples from individuals of interest are collected and stored in a central storage location. These raw samples were then processed using Jeffrey's techniques to extract the individual's naturally occurring *DNA* markers using a process involving electrophoresis. The extracted *DNA markers* are then stored as a truth reference template (benchmark) in a database for safekeeping and credential dispute resolution.

During an immigration or geographical border crossing dispute, a previously stored template of the *DNA* marker levels is compared to a new sample collected from some person of interest and used as a *fingerprint* (marker). To authenticate the origin of the individual as a native resident of a country or not, a fresh *DNA* sample is extracted from the person of interest and a comparison is made to the database (benchmark template) of known *DNA* profiles. If the new DNA sample levels match specified levels of the known template, a decision-support response(s) was made to augment the authentication of the targeted person of interest's geographical residency origins. If there is no *fingerprint* match, the person of interest generally was labeled as illegal until further mechanisms (additional evidence testing) proved otherwise.

In a similar fashion of applying *DNA concepts* to identify faces with fingerprints [9], electronic RF fingerprinting concepts are applied towards the identification of electronic devices and their RF transmission origins for the purpose of verification of logical credential claims in an uncertain threat prevalent (e.g. imposter) Cyberspace ecosystem.

Just as physical land boundaries are vulnerable to illegal immigrant crossings, SATCOM (i.e. CubeSat) network communication links are also vulnerable to unauthorized passage of specified RF *link* boundaries to gain access by imposter entities. Such unauthorized link access (infection) can result in undesirable receiver or network behavior to include a total loss of SATCOM resources (spacecraft).

In some wireless networks, the use of technology is employed to communicate between a source and destination device pair, generally referred to as a point-to-point (P2P) network. In a satellite receiver's CDH a remote control device (i.e. ground station) generates an RF waveform onto the uplink using a transmitter to logically encoded telecommand messages. An exemplary example is the P2P network link that exists in a typical garage door opener system or car alarm. In this example, a transmitter is contained in a remote control unit (handheld or mounted) and a receiver (i.e. the opening component) is connected to a garage door motor [10].

Whenever an encoded *command* is received by the garage door motor processing center from the remote control unit, the contents of the waveform received is inspected to detect a matching remote-control identification code before a response to open, close or do nothing is made. In the case of CubeSat, a representational miniaturized satellite network, the transmitter component of a ground station's transceiver is wirelessly connected to an onboard CDH receiving component. Both transceivers are typically comprised of different integrated circuits and other system components. A terminal node code controller (TNC) is used as an intermediate push-to-talk (PTT) device that transforms a signal's digital content to modulated analog waveforms between a PC and an FM front-end transceiver using the AX.25 protocol [11].

When a TNC component of the ground station is activated, the circuit's front-end transmission device (e.g. ICOM-9100 amateur radio) modulates the logical (bits) onto the analog baseband (e.g. 450 MHz FM) signal using some arbitrary standardized protocol (e.g. GMSK). The naturally generated waveform includes the device's logical (bit-level) identification code (i.e. serial number, MAC Address, vehicle ID, FCC ID etc.). This natural state of the RF transmission (RF-Event), prior to demodulation, is of considerable interest in this research to avoid physical RF attribute information loss.

Repeatable transmissions of invariant RF-Event occurrences may be useful in providing a basis for physical attribute interpretation of correlated logical bit decoding. In some cases, where frequency division or time division modulation schemes are employed, information can be transmitted remotely for a single device using separated channels of a baseband waveform like the Air Force's Tactical Targeting Network Technology (TTNT) or the Army's Blue Force Tracking System (BFT) or the Naval Automatic Identification System (AIS) are examples of self-organized TDMA systems [12]. In these cases where identification authentication is required, additional information such as telemetry, geospatial location or other aggregation of information (correlated) can be transmitted in the same baseband waveform carrier using techniques such as signal watermarking or steganography designed as visible or invisible mechanisms that increase the confidence of origin integrity [13].

Currently, these unauthorized activities may originate from an authorized or unauthorized transceiver device, making the tracking of those transactions more difficult for attribution as an *insider* vs. *outsider* threat in a conventional reputation-based trust management scheme. To mitigate the occurrence of unauthorized device link access, a fixed transmitted code pattern is changed whenever the ground station's transmitter is activated.

Conventionally, rolling code algorithms are used such that codes are changed or rolled according to some previously determined fixed sequence, known only to the transmitter and the receiver. This research adapts this behavior and employs a similar scheme in exchanging RF-DNA markers between trusted P2P linked pairs. Any potential eavesdropper or *conman* would now have to guess the start and stop locations of the next credential marker (***iMkr*)** (e.g. rolling) code value in addition to decoding the binary code. A simple replay attempt would always fail since the algorithm does not allow the same rolling code to be executed consecutively. Yet still, when a rolling code is not utilized and instead a fixed code equivalent is used, the above possibilities still hold for vulnerabilities. In these cases, the potential to extract the digital content of $'\boldsymbol{w}'$ through eavesdropping is possible.

Moreover, there is no physical evaluation of the detected physical nature of neither the waveform nor modulation scheme, since these considerations are already necessary and sufficient for standardized and interoperable communication. This research exploits such standardization of analog waveform generation and its repeatability which is favorable to discriminate the physical waveform characteristics generated during each transmission. RF-DNA fingerprinting is a robust collections process that focuses on the physical characteristics of a generated waveform with respect to its instantaneous values in time and space during generation. These key principles of RF-DNA fingerprinting of an RF transmission characteristics of frequency, phase and amplitude [14] are adapted in this research.

1.3 Research Challenges.

The inherent complexity of a non-standard ground station's transmission circuit can produce significant effects on the final RF fingerprint extracted by a receiving device. Even standardized circuit transmissions contain subtle variations due to multiple physical components.

Issues such as device maintenance, user (personnel) changes and command sequence modifications can affect the final RF fingerprint emission from a transmission circuit.

The distance of SATCOM networks far exceeds the length of recent research using RF-DNA fingerprints. At greater distances, RF communications experience degraded signals due to multiple path loss effects from **EMI** sources. At the time of this writing, RF-DNA has been used for line-of-sight (LOS) RF communication links such as microwave links, but has not yet been employed in a UHF SATCOM ecosystems, where multiple path loss is not that significant [15] [16] [17] [18]. As an unintended consequence of interoperability of RF networks, any receiver employing standardized and interoperable RF transmissions may initiate shutdown responses as a result of misfires, natural and man-made EMI sources or other multiple path loss effects on valid RF transmissions. Finally, the capability to support multiple space mission needs requires more expressive policy responses to enable a correct discrimination of behaviors from offensive organizational (*insider*) devices from non-offenders (*benign* transmission events) while providing appropriate decision-support recommendations for true *outsider* threats.

1.4 Research Overview

This dissertation presents a framework to augment network diagnostic utilities in classifying the origin integrity of new RF credential claims as *benign* (high RF origin similarity and low risk of forgery) or *infectious* (low RF origin similarity and high risk of forgery) for causing eND. Here, eND is a specified occurrence of abnormal network behavior (e.g. denial of service) that is likely to result from untreated infectious credential acceptance. A Multi-factor authentication augmentation scheme pairs conventional logical authentication credentials with new physical RF attributes of invariant message transmissions.

Using the paired credential set, a designated authentication device compares new credential extractions from incoming network access requests to a known credential benchmark template for the purpose of validating or disputing the origin integrity of claimed access credentials in an uncertain *non-benign* threat prevalent environment.

In uncertainty, Bayes Theorem is employed to improve the posterior accuracy of 1-1 credential verification. Additionally, extensions are made to an existing interactive trust algorithm to more accurately express *insider* vs. *outsider* threats using aggregated credential diagnostics. For illustrative purposes, the research applies findings to a representative CubeSat (miniaturized satellite) network where a trusted source (fixed ground-station) transmits authentic RF credential claims to an uplink receiver functioning as the authenticating device, which provides an Euclidean distance metric for RF origin similarity comparisons to a trusted RF fingerprint template. This research examines the following overarching research questions;

RQ1: Can we enhance logical (digital) credential authentication schemes using pathological RF-DNA credential diagnostics of RF transmissions? Can useful RF fingerprint extractions from SATCOM networks improve uplink access authentication schemes? If so, can insights gained from these techniques be effectively imparted to cybersecurity key players? Can we enhance logical authentication mechanisms using statistical RF fingerprints pairings? Can RF fingerprinting methods improve uplink access availability for non-offenders in a shared resource operational ecosystem? If the number of RF fingerprint features remains constant for any ROI, then the diagnostic performance is identical for large or small ROIs. However, when an identical classifier is presented with a relatively small ROI, the diagnostic performance is more dependent on sample size rather than the classifier.

Chapter I examines these key research questions over four specific and distinct research components that comprise Chapters II-V of this dissertation. Summaries of these components follow. Chapter II explores the device heterogeneity problem inherent in RF fingerprinting of wireless transmissions which contain invariant regions despite having some portions of the message as fixed. It poses the following research question:

RQ2: Can non-standard regions of interest (ROIs) be used to develop statistically distinct RF fingerprint credentials from electronic device transmissions?

Specifically, Chapter II seeks to; target non-standard ROI fields for RF fingerprint extraction and benchmarking; assess the effects in classification performance of a reduction in sample size for a given RF fingerprint. Non-standard ROIs of logical (bit-level) encoded message fields include USERIDs, device IDs or command sequence IDs. A baseline experiment employs six randomly selected ICOM-9100 radios to transmit identical pulsed telecommands which contain logical authentication credential fields which are paired with non-standard RF transmission ROI fields for unique device identification. The experiment aims to extract an invariant ROI near the standard preamble field as the baseline RF fingerprint (R1). The ROI is further divided into six distinct portions to produce six classification models for comparison. The results of non-standard ROI selection is applied to new telecommand fields that have been transmitted. Results show that using a 66% reduction of the standardized ROI baseline, acceptable levels of accuracy are achieved for SNR > 25dB. Non-standard customization is found to be promising for expressive policy specification of RF fingerprinting targets to support various organizational objectives. The effectiveness of the approach is validated using three software-defined radios (SDRs) configured in a simple network configuration discussed in Chapters III and IV.

Chapter III seeks to position the key insights gained from non-standard ROI selection in Chapter II. It does this by systematically developing RF credential benchmarks to improve posterior diagnostic classification. Specified RF measurements of the transmission's main characteristics are extracted as RF fingerprint features. The top indicators for device verification are called RF-Biomarkers. An *RF-Biomarker* is a physical or intrinsic characteristic of an electronic communication device's RF emissions that indicates abnormal process or response when the origin integrity of RF transmissions are suspect for causing *network-disease*. An arbitrary policy is used to specify the development of device specific credential pairings of logical authentication fields and physical RF fingerprint benchmarks which. The benchmark credential template is validated using a gold standard truth reference which consists of new unseen (logically equivalent to benchmark training transmissions) RF transmissions. More specifically, three diagnostic classifiers are developed for RF fingerprint classification comparisons using binary, ordinal and continuous valued data decision rules. Decision rules are employed using thresholding to assess the overall Euclidean distance of new transmissions using Gauss-Kronrod exact tolerance regions for simple binary classifications. Chapter III examines the research question(s):

RQ3: How does the diagnostic accuracy of ordinal, continuous, binary and Bayesian decision rules compare against conventional methods? Subsequent questions include; How should threshold boundaries be determined? Can the concept of extracting RF Fingerprints from Non-standard ROIs be extended to entire fixed message fields to support a subset of critical commands used for small infrastructure networks? Based on the performance of diagnostic classifiers from Chapter III, Chapter IV hones in on the challenge of indicating the true nature of *insider* vs. *outsider* threat in threat prevalent ecosystems. It examines the following two questions:

RQ4: Can RF fingerprint evidence augment *insider* vs. *outsider* attribution without degrading conventional 2-State performance in uncertainty?

Chapter IV provides a discussion about a well-known interactive trust algorithm employed to mitigate known con-man attack patterns. In such an attack, an interactive trust value (ITV) mechanism is employed to assess the level of trust that an authentication receiver has for some uplink transmission device. A series of 200 transactions are considered during the ITV assessment and at the end of each transaction, a binary classification of Cooperative or defection is made to indicate a trustworthy or untrusted transaction occurrence. When a classification for Cooperation occurs, the ITV value is slightly incremented to indicate a more trusted perspective of the transmitting device's claimed logical credential field. However, a defective transaction results in the loss of trust and a penalty is applied to reduce the ITV. If the ITV falls below a specified threshold of distrust, a Level-3 network treatment response is automatically initiated and uplink access for all ground-stations is denied. The conventional method of transactional classification is extended to include four total possible states. With the introduction of two new states, the research seeks to demonstrate the expressiveness of insider and outsider threat using the proposed method.

Finally, in Chapter V, attention is focused on assessing the diagnostic usefulness of combined classifier performance against a con-man attack. A decision to treat a network for *network-disease* is explored using the benchmark, gold standard and diagnostic performance. Arbitrary decision-rule thresholds are studied to gain insight into potential cost and benefit trade-offs using paired credential diagnostic tests. When diagnostic accuracy fails to meet threshold requirements, Bayes Theorem may be applied to improve the posterior estimates. It examines the primary question:

RQ5: Are simple random log file screenings of claimed RF-DNA credentials useful in indicating earlier warning and preventative treatment options? What is the minimum screening sizes for RF-DNA credentials? When should treatment be given?

In summary, this dissertation examines important research questions involving the mitigation of unauthorized uplink access attempts and focuses on two primary areas. One is applying its insights from RF fingerprinting into device-specific benchmarking to enable 1-to-1 verification, which may help to reduce the acceptance of infectious credentials when logical only-mechanisms fail. The other research focus seeks to identify useful RF-Biomarkers (RF measurements selected as useful discrimination features) that best indicate *network-disease* when the origin integrity of claimed logical and physical credential pairings are inconsistent with benchmark credential signatures.

II. Collection of Non-Standard RF-DNA Fingerprint Credentials

Out of clutter, find simplicity. From discord, find harmony. In the middle of difficulty lies opportunity.

(Albert Einstein)

2.1 Introduction

The aim of this article is to characterize the integration of RF-measurement collections, as RF fingerprints, into a consolidated trust management system (CTMS) architecture for enhanced satellite communication (SATCOM) network security [1] [2] [19] [20]. Uplinks are communication mediums that ground station devices transmit telecommand messages to satellites in space for command and control (C2) of the satellite. A CubeSat is used as to represent a miniaturized SATCOM network and the ICOM-9100 amateur radio represents the ground station transceiver [21] [22].

SATCOM networks in general, can be secured using mechanisms such as encryption, ground station authentication IDs and MAC addresses employing logical network layer security mechanisms. Such mechanisms are inherently based on digital representation of some transmitted payload or *content* for C2 interpretation, administration, and Cyber security defense. As more access is gained to SATCOM, cyber security vulnerabilities such as interception, replay and forgery attacks by imposter devices are expected to increase. Imposter devices can mimic logical (bit-level) content of communications transmitted between SATCOM devices and create undesirable network behavior [23]. Imposter devices can include previously trusted or authorized devices that may abuse or exceed usage privileges or may be complete anonymous devices that have never been seen in the network. The possession of forged or actual abuse of bit-level credentials by persistent imposter entities enables a bypassing of network layer authentication mechanisms.

The detection of such persistent behavior is made more difficult in a multiple path loss ecosystem such as SATCOM links. A priority of maintaining positive C2 of launched spacecraft in spite of noisy EMI ecosystems drives policy to accept a higher risk of misinterpreted bit-level credentials to include the acceptance of anonymous devices. As a result, Cyber Hackers, exploit this vulnerability and seek to gain C2 of the spacecraft for their own purposes. Multiple path loss for Ultra High Frequencies (UHF) instead may be ideal for RF fingerprint.

For UHF, it has been shown that such multiple path loss is not significant and provides a reasonable opportunity to assess effects of multiple path loss discrimination of fingerprinted devices over long UHF SATCOM links [15]. At the time of this writing, RF-measurement has been used for RF communications such as microwave line of sight (LOS) links and is heavily researched for various medium types [17] [16] [18] [15]. In recent work, RF fingerprinting techniques have been used to discriminate SATCOM devices using GPS. Such discrimination suggests authentication of logically transmitted content (e.g. ITV) enhancements is possible using physically (PHY) determined RF fingerprints, which are substantially more difficult to mimic [24]. The implications of having network level discrimination of authorized devices has great appeal to the Cyber-forensics, network security, Cyber-security and SATCOM community in general [25] [26]. However, many of the challenges associated with RF fingerprinting for SATCOM network integration have not been adequately addressed, leaving the physical aspects of SATCOM transmissions potentially vulnerable to Cyber-attacks such as forgeries as described in Duncan's work [1].

Unlike previous research that aims to characterize and extract the RF fingerprint of specific devices, this article discusses some EMI considerations that may adversely impact RF fingerprinting. A study of EMI behavior on various RF fingerprint collection configurations could inform policy that specifies and ultimately selects statistically significant RF-Measurements of the physical attributes associated with logical credential transmissions. After policy specification, the RF-Measurements can be collected as a distribution of distinct values and represent the RF-DNA fingerprint credential used to augment the authentication of a logical credential field. Such pairing of credentials, paired logical and pathological RF-DNA credentials are exchanged from source to destination device for final authentication. Inspiration from medical and biological community provide inspiration for exchanging RF-Measurements between devices for the purpose of authentication enhancement. The proposed framework biologically inspired network (BiONet) framework proposes an integrated multi-factor authentication scheme which provides policy-based RF fingerprints selections for dynamic decision-support systems [27] [28].

The standardized radio frequency (RF) measurements of invariant transmission fields (e.g. *Preamble)* have been effectively used as discriminating features to reliably differentiate FM radios operating in the amateur radio frequency space [18] [11]. This work integrates multi-factor concepts of 'air-monitoring' used in ZigBee networks and consolidated trust management systems (CTMS) architecture. Specifically, the device discrimination capability is extended to enhance the discriminability of specified organization's assigned network layer payload content. Ramsey's 'air-monitor' concept observes physical (analog) wireless network transmissions which augments bit-layer security using RF fingerprints in a Wi-Fi wireless intrusion detection ecosystem [29], while Duncan's CTMS's authentication mechanisms observes logical content of wireless network transmissions to augment upper OSI layers for SATCOM networks [1].

The work here demonstrates reliable differentiation between ICOM-9100 transceivers functioning as ground station devices for SATCOM uplinks. The RF fingerprint techniques used summary statistics of amplitude, phase and frequency as instantaneous transmission waveform components of the transmitted signal of interest. For an arbitrary benchmark of 70% or better ROI classification accuracy, this work shows that reliable PHY-based uplink transceiver discrimination can be achieved at ≥SNR 30dB for reduced sized ROI.

2.2 Trust Management System Enhancements Using RF-measurement

- **2.2.1 SATCOM Overview.**

SATCOM links are generally described as up and *downlink* communications channels to indicate the direction of information flow with respect to earth. The uplink channel's transmission signal source originates from a device located on earth and is propagated upward toward a satellite away from earth. This device may exist as a stand-alone RF emitting device or as a collective member of several devices operating as a unified system. The latter is referred to as the ground station (GS). The *downlink*'s transmission signal originates above the earth's surface and may extend far into space. The satellite transmits signals downward towards a GS on earth using the SATCOM network's *downlink*. When satellites or GS devices communicate directly with each other, they form a point to point (P2P) communications network that consists of two transceiver devices (source and destination). The transmitters used in this article utilize a 2.2GHz *downlink* channel to send information to ground stations, while the GS devices transmit on the uplink in the UHF 450 MHz range to send tele commands to the satellite's command data handler (CDH) receiver. The CDH controls the execution of tele commands through the use of an onboard microcontroller.

Upon receipt of a telecommand message the CTMS determines the authenticity of a GS's identity prior to executing the command. This scheme employs a bit-level credential that is digitally encoded within the carrier's modulated message.

- **2.2.2 ICOM-9100 Transceiver Modulation Scheme.**

The ICOM-9100 radio is an independent duel receiver that fully covers HF up to 1200MHz multiband to include a *Satellite* mode of operation. The ICOM-9100 can modulate and demodulate multiple schemes including, Gaussian minimum shift keying, frequency shift keying (GMSK), and FM among others. One transceiver modulation scheme of interest was the GMSK used by the AX.25 amateur radio protocol [11]. More research is needed to determine the actual front end modulation scheme that is transmitted from the ICOM-9100 after intermediate frequencies have been modulated using some unknown modulation scheme between the terminal node controller and the ICOM-9100.

- **2.2.3 CubeSat Message Format.**

CubeSat is the representative experimentation network of satellites under study in this research effort. Command sequences are executed by the command data handler (CDH) scheduler in order of priority. The CubeSat executes immediate commands with one sequence, one command, and corresponding number of parameter blocks according to the scheduler's storage. There are two types of commands supported by the CubeSat. Unacknowledged Commands: Protocol id 0x1 and Acknowledged Commands: Protocol id 0x2. If a protocol id 0x2 is sent from the command station to the device, the device will send an ACK response back, regardless of the operation. The CubeSat message format is shown in Table 1.

Table 1: CubeSat Message Format with Vehicle ID as the ITV

Mnemonic	Frame Version	Protocol ID	Is Parameter Compressed	Message ID	Authentication Count			Vehicle ID	Reserved	Parameter Length	Parameter Data	CRC CCITT	
Default	0x4	1, 2	0x0	Varies	Sat. Auth. Cnt				0x00	Varies	[0-1,328]	16	
Bits	4	3	1	8	(24+8)				8	8	[0-1,328]	16	
Byte Pos.	0			1	2 LSB	3	4	5 MSB	6	7	[8-N]	N+1 LSB	N+2 MSB

- **2.2.4 Consolidated Trust Management System.**

In Duncan's previous work, the vehicle ID and a sequence number (SN) mechanism field are employed to indicate the current trusted state of a device. However, this network-layer mechanism may be intercepted by a foreign device during a suspected forgery attack. Possessing the next expected SN; a malicious user could insert malicious code that may be executed by the receiving station. The CTMS compares the vehicle ID and message SNs to make an authentication decision using a dynamic interactive trust value (ITV). When matched, the telecommand sequence is allowed to execute. However, when an imposter device is successful with returning the vehicle ID and the correct SN, then the forgery attack has a higher rate of success. Using RF fingerprinting results, the aim is to integrate the physical characteristics of authorized SATCOM devices such that forged tele commands fail to execute because it lacks the unique RF-measurement components of authorized devices. As shown, an imposter ground station may gain unauthorized access to satellite S4 during a successful *uplink* replay attack. Likewise, an imposter satellite (S?) can be manipulated by malicious users who provide modified information over the *downlink*. Having a CTMS properly functioning onboard both the GS and the satellite can offer augmented protection against this type of attack in a distributed system configuration.

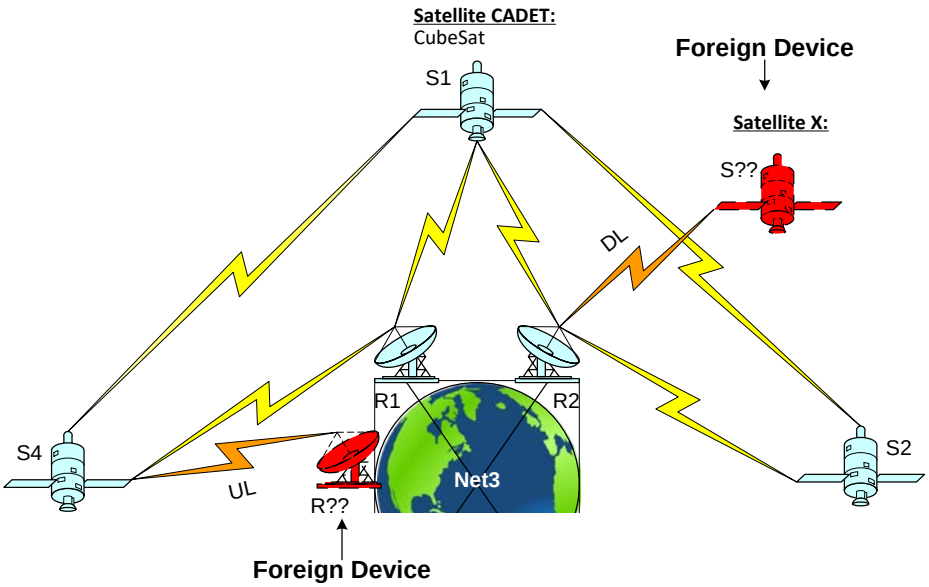


Figure 1. Imposter Threat Model for Unauthorized Link Access

If S4 or R2 have no way of discriminating the physically *inherent* waveform features of imposter devices then the forgery attack may be successful and result in catastrophic consequences such as total loss of spacecraft C2. To mitigate C2 loss, a method to integrate the concepts of RF fingerprinting and CTMS authentication process is introduced in the next section.

- **2.2.5 Physical & Logical Trust Management Integration.**
  A policy-based BiONet concept may be employed as an integrated multi-factor mechanism for network security enhancement by simply adding the concept of 'we' adapted from an 'air-monitoring' scheme which lends itself to added expressiveness of policy-based paired communications that is proposed in this article [14] [24]. Ramsey's three factors becomes modified to be; 1.) "Something *we* have" (ITV – Interaction Trust Value). 2.) "Something *we* are" (PHY – RF fingerprint) simplex. 3.) "Something *we* share" (PHY – RF fingerprint marker pairing) up to full-duplex. An integrated BiONet framework would be most valuable if every received transmission's content is validated by some policy-based physical RF marker.

Since it only takes the acceptance of the content from a single malicious transmission, RF-measurement fractionally validated transmissions may mitigate attacks such as replay and denial of service attacks. The use of the ICOM-9100 transceiver's fixed preamble makes it an early candidate for fractional RF fingerprinting and policy-based RF-measurement exchange mechanism for CTMS security enhancement.

In Figure 2, the imposter threat model is presented with unauthorized link access protection mechanisms. Using the CTMS architecture, RF fingerprints are exchanged between trusted devices to augment the network-layer authentication mechanism for link access. A device that employs the augmented CTMS architecture is indicated in the blue label. On the far left of, S4's response policy is shown to describe actions taken when comparing a received RF fingerprint to a known RF-measurement marker. If S4's extracted RF fingerprint matches its credentials, the identity of the waveform's source is authenticated. Imposter devices (red) attempting to access SATCOM links using forged waveform carriers may be denied access using this physical-layer augmentation scheme. As depicted in Figure 2, if S4 or R2 lacks a defined Bio-Pairing policy $\boldsymbol{p}$ that consists of shared RF-measurement markers of the imposter transmitter, authentication attempts may fail.

2.3 ROI Selection Methodology

An ETTUS USRP X310 software defined radio serves as the RF Signal Intercept Collection System (RFSICS) [30]. Raw collected signals are stored initially as complex in-phase and quadrature (I-Q) components for subsequent post-processing. Secondly, each set of (I-Q) data is decimated by a factor of four and down converted to near-baseband using a 12-bit analog-digital conversion. Collection parameters include sample rate of frequency f_s = 5 MS/s and baseband filter bandwidth W_{BB} = 20 KHz using a 4th-order Butterworth filter. A total of N_P = 971

transmission bursts produced approximately 1800000 samples per burst from N_D = 4 ICOM-9100 450MHz radio transceiver devices. Transceiver positioning is consistent in a given transmission circuits. In this case, collections were made using a *wired* (shielded cable) circuit between the RFSICS and ground station transceiver (i.e. ICOM-9100) device. Amplitude-based threshold detection with a leading edge value of T_D = -6.0 dB is used to identify and extract individual burst transmissions from the multi-second RF collections. The collection SNR for all bursts was SNR_C > 18 dB. Each burst was approximately 350ms in duration.

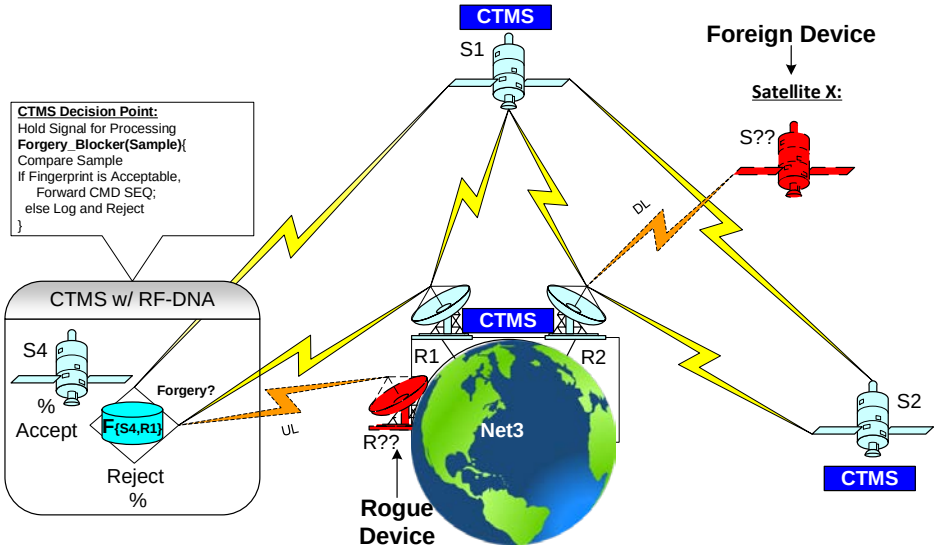


Figure 2. Imposter Access Mitigation using RF fingerprints

- **2.3.1 Statistical Fingerprint Generation**

The statistical fingerprints ***F*** for a signal is derived using Reising's and Ramsey's computations and are summarized here. The components of its instantaneous **amplitude (*a*), phase (ϕ)** and/or **frequency (*f*)** characteristics are used to derive ***F***. More specifically, the sequences **{*a*[*n*]}, {ϕ[*n*]}, and/or {*f*[*n*]}** are generated from (I-Q) samples of the signal ROI, centered (mean removal) and then normalized (division by maximum value). Within specified signal ROI, statistical features are generated as variance **(σ^2),** skewness **(γ),** and/or kurtosis **(*k*).**

The specified signal ROIs are used to generate the RF fingerprint markers in three steps. First, each characteristic sequence is divided into N_R contiguous, equal length sub-sequence regions or sub regions. Secondly, N_S statistical metrics are computed for each sub region, plus the entire fingerprinted region. Finally, the (N_R + 1 total region) are arranged in the vector:

$$FRi = \left[\sigma 2R_i \; \gamma R_i \; kR_i\right] 1 \times 3\,, \tag{1}$$

Where i = 1, 2… N_R + 1. The marker vector from (1) is concatenated to form the composite characteristic vector for each characteristic and is given by

$$\boldsymbol{FC} = \left[FR_1 \vdots FR_2 \vdots FR_3 \; \ldots \; FR_{(NR+1)}\right] 1 \times N_S\,(N_R + 1)\,. \tag{2}$$

If only one signal characteristic (a, ϕ, or f), is used the expression in (2) represents the final fingerprint used for classification. When all N_C = 3 signal characteristics are used, the final *RF fingerprint* is generated by concatenating vectors from (2) according to

$$\boldsymbol{F} = \left[\boldsymbol{F}a \vdots \boldsymbol{F}\phi \vdots \boldsymbol{F}f\right] 1 \times N_S(N_R + 1) \times N_C. \tag{3}$$

No exploratory data analysis was conducted, and the chosen $\boldsymbol{N_R}$ = 10 ROI sub-regions may not be optimal for the selected ROI. More information can be found on optimizing RF-DNA fingerprint generation in [5].

- **2.3.2 Customized ROI Selection**

Adding to the ROI selection process, we further segment the initial waveform into various segments that vary in length, duration and ROI start and stop positions. Using this approach, the initial ROI is segmented into six subsets to formulate distinct RF-measurement models from the original model $\boldsymbol{M}$. In general, there is no need to have a previously existing model $\boldsymbol{M}$, since this can be created for one or multiple models according to some arbitrary criteria. We experimentally chose a known model where classification results exceed an arbitrary 85% classification rate for SNR > 15dB.

Let $\boldsymbol{M}$ = the classification model developed using MDAML per AFIT's RF-DNA fingerprinting process as described in the previous section. Each constituent device is therefore a trusted member of model M where the population size of M $\geq$ 3 in this article is given by $Dev = \{1,2,3, \ldots d\}$. Given an arbitrary ROI segmentation strategy of six conditions, M is segmented into six distinct ROI selections.

The collection of $\mathbf{F}^{C1}$ through $\mathbf{F}^{C6}$ fingerprints produced six variations of the original model as $\boldsymbol{M_1, M_2, M_3, M_4, M_5, M_6}$. These collections of fingerprinted models form the pool of RF-measurement markers for model development and are extracted from each device's decimated (I-Q) data. Each $\boldsymbol{M_i}$ is mapped to a specific $\boldsymbol{ROI_i}$ as ($\boldsymbol{R1, R2, R3, R4, R5}$ and $\boldsymbol{R6}$). The total sample size, start/stop parameters, and the percent of the original $\boldsymbol{M}$ reduction in total sample size are provided in Table 2. $\boldsymbol{R1}$ is the original model $\boldsymbol{M}$, and contains 30,000 samples. $\boldsymbol{R2}$ and $\boldsymbol{R3}$ contain the same start point for ROI model selection as $\boldsymbol{R1}$, whereas $\boldsymbol{R5}$ and $\boldsymbol{R6}$ share the same sampling stop point as $\boldsymbol{R1}$. $\boldsymbol{R4}$ contains 10,000 samples and represents the middle third of $\boldsymbol{R1}$ and represents a 66% decrease in overall $\boldsymbol{ROI}$ sample size that does not share the same start nor stop points.

- **2.3.3 MDA/ML Device Classification Methodology**

Statistical RF fingerprints are generated using (3) for collected transmissions from $\boldsymbol{N_d} = 4$ ICOM-9100 UHF radio transceivers. The fingerprint results are classified using Multiple Discriminant Analysis/Maximum Likelihood (MDA/ML) [31], an extension of Fisher's Linear Discriminant. For the $\boldsymbol{N_c} = 4$ class problems considered here, MDA/ML projects the multidimensional RF fingerprints into a 3-dimentional space for a total of $\boldsymbol{N_c}$ classes and assigned for each fingerprint marker. K-fold cross-validation with $\boldsymbol{K = 5}$ is used to improve classification reliability. The best-performing model generated is then used to classify a set of half of the total bursts or 485 custom fingerprint markers previously unseen.

- **2.3.4 Pre-Classification Feature Dimensionality Reduction**

The MDA/ML classification process does not provide feature relevance statistics for $\boldsymbol{M}$ however, RF fingerprint components that exhibit maximal inter-device dissimilarity and minimal intra-device dissimilarity are generally advantageous for MDA/ML classification. In this case, the ICOM-9100 devices exhibit such dissimilarity. The process for assessing feature relevance is called Dimensional Reduction Analysis (DRA) and aims to reduce RF fingerprint size (minimize $\boldsymbol{N_F}$) and minimal or tolerable impact on classification accuracy. For the $N_D = 4$ device case considered here, the full dimensional fingerprints were calculated to contain $\boldsymbol{N_F} = (\boldsymbol{N_R + 1 = 11}) * (\boldsymbol{N_S = 3}) * (\boldsymbol{N_C = 3}) = \boldsymbol{99}$ features.

Where amplitude features are considered in the first 33 features, phase occupies the second 33 features and frequency is used to assess the frequency features of the fingerprint. Amplitude appears to dominate in this article and was normalized to further differentiate feature relevance. Phase features have been previously noted [14] to be robust despite noisy conditions and are shown to remain virtually unchanged as SNR degrades in general.

2.4 ROI Classification Results

The results are presented here using previous work presentations as a template for results comparison. Specific values and parameter settings have been adjusted to reflect these experimental findings. Analysis revealed that features based on power-spectral-density underperformed relative to features based on the instantaneous a, ϕ, and f time-domain responses.

MDA/ML inter-device classification results were generated for all *4*-class problems using $\boldsymbol{N_d} = 4$ ICOM-9100 devices. Classification experiments used $\boldsymbol{N_P} = \boldsymbol{971}$ valid independent *preamble* pulses (485 each for training and 486 for model classification) and $N_z = 1$ Monte Carlo noise realizations per pulse response at each SNR ranging from 0 to 35 in 5dB steps.

$\boldsymbol{N_{Tst} = (486\ CustomROI)\ x\ (N_z = 1) = 486}$ independent classification decisions are made for each device $\boldsymbol{N_d}$ trial.

Table 2. Custom ROI Start and Stop (I-Q) Waveform Sampling

ROI ID	*Size Reduction (%)*	*Region of Interest Index Marker [Start : Stop]*	*Samples*
*R1	0	25K : 55K	30000
R2	-66.7	25K : 35K	10000
R3	-33.3	25K : 45K	20000
R4	-66.7	35K : 45K	10000
R5	-33.3	35K : 55K	20000
R6	-66.7	45K : 55K	10000

*R1 represents the baseline ROI of an experimentally determined GMSK waveform.

- **2.4.1 Full Dimensional RF fingerprinting Accuracy.**

Full dimensional RF fingerprints include features based on $\boldsymbol{N_c = 3}$ signal characteristics (a, ϕ, and f), $\boldsymbol{N_s = 3}$ statistical fingerprint features (σ^2, γ, and k), and $\boldsymbol{N_r + 1 = 11}$ regions, for a total fingerprint $\boldsymbol{F}$ comprised of $\boldsymbol{N_F = 99}$ RF-measurement features as given by (3). Figure 3 presents the aggregate full dimensional classification accuracies for *all* device permutations at $SNR \in [0\ 35]$ dB levels. The cross-permutation average is shown as the filled asterisk marker connected with black dashed lines of Figure 3. As indicated, the mean classification accuracy exceeds an arbitrary benchmark of 70% for $SNR \geq 30$ dB. This suggests that that the varied ROI selections display similar classification performance and increases as the SNR increases in general for full 99 feature consideration. Implication of less processing of a waveform can achieve similar RF-measurement detection accuracy and lower the overall cost.

- **2.4.2 Reduced Dimensional RF fingerprinting Accuracy.**

While full dimensional RF fingerprinting is effective, the DRA process in Section III.D revealed significant differences (range of p-values) among RF fingerprint components derived from the instantaneous $\{a[n]\}$, $\{\phi[n]\}$, and $\{f[n]\}$ sequences. Classification results are presented here for RF fingerprinting with a 66.7% reduced feature set ($\boldsymbol{N_F = 33}$).

This is done by evaluating classification performance using only amplitude (*Amp-Only*), phase (*PHz-Only*) and frequency (*Frq-Only*) feature subsets of the full dimensional feature set.

Figure 4 presents the aggregate *Amp-Only* classification accuracies for all N_{Prm} = 24 permutations, with the cross-perm average shown with filled asterisk markers. The resulting decline in classification performance is readily apparent by visual comparison with full dimensional RF fingerprint performance using normalization. Relative to the arbitrary benchmark of 70%, *Amp-Only 33 features*, RF fingerprinting requires *SNR* > 25 dB.

Figure 5 presents the aggregate classification accuracies for all $N_{Prm} = 24$ permutations for *Frq-Only* RF fingerprinting, with the cross-perm average shown with filled circle markers. In general, the frequency performance results show no significant change from $\boldsymbol{R1}$ from 0 to 20 dB, but at SNR > 25dB $\boldsymbol{R4}$, $\boldsymbol{R5}$ and $\boldsymbol{R6}$ performs marginally better than random. In all cases, neither frequency-only feature meet the arbitrarily chosen benchmark of 70% at any SNR, which suggests that Frequency may not be the best discriminator for ICOM-9100 devices in this experiment.

Figure 6 presents the aggregate classification accuracies for all N_{Prm} = 24 permutations for *PHz-Only* RF fingerprinting, with the cross-perm average shown with filled asterisk markers. These results show a significant decrease in classification performance when compared to the Amp-Only features depicted in Figure 4. These findings are not consistent with previous RF fingerprinting work using similar devices. The shielded cable configuration may play a factor in this inconsistency; since previous work used free space configurations. *PHz-Only* fingerprinting failed to meet the arbitrary benchmark of 70% for any SNR value used in this simulation. Consistencies are shown that suggest phase remains unchanged despite decreasing SNR. $\boldsymbol{R4}$ has 10,000 samples compared to $\boldsymbol{R5}$'s 20,000 sample size and still achieves a classification accuracy that is 10% lower than $\boldsymbol{R1}$, $\boldsymbol{R2}$, $\boldsymbol{R3}$ and $\boldsymbol{R5}$.

Although the same start point for the ROI selections for $\boldsymbol{R4}$, $\boldsymbol{R5}$ and $\boldsymbol{R6}$ differ, there is no significant difference in RF-measurement classification accuracy, however the sample size of only 10,000 vs. $\boldsymbol{R5}$'s 20,000 samples provides evidence that a savings in processing and ROI location can be achieved using custom ROI selections with minimum effect on detection accuracy. $\boldsymbol{R2}$, which has a sample size equal to $\boldsymbol{R4}$ and $\boldsymbol{R6} = 10{,}000$ samples supports that the sample size is not the only factor, but achieves higher performance since it shares the same start point, which may be closer to the fixed preamble area.

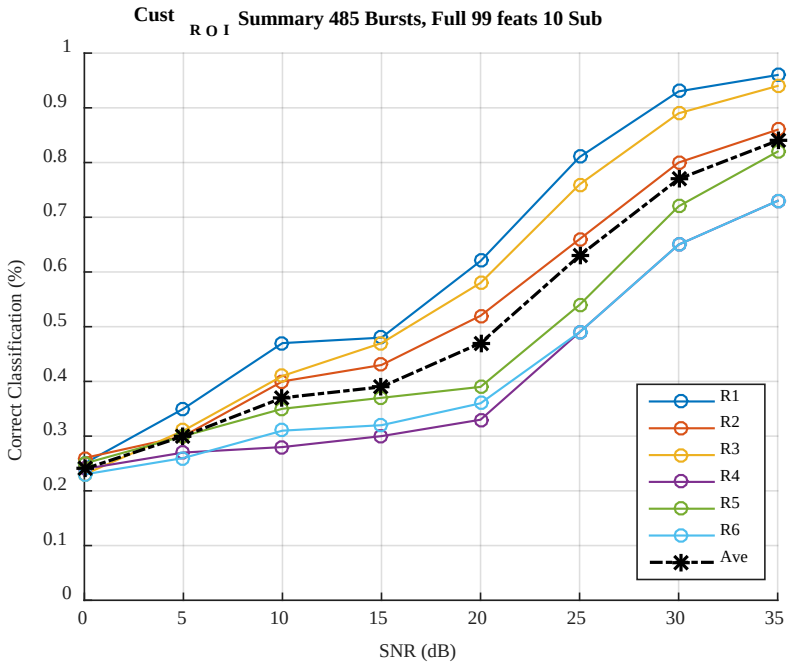


Figure 3. Full Dimensional (NF = 99) Class Accuracy for 24 Permutations

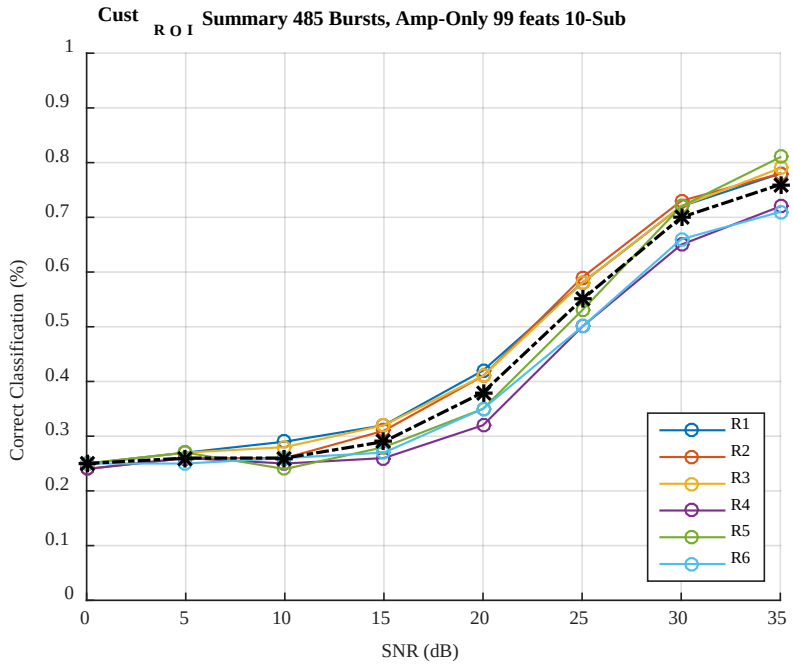


Figure 4. Reduced Dimensional (NF = 33) Class for 24 Permutations (Amp-Only)

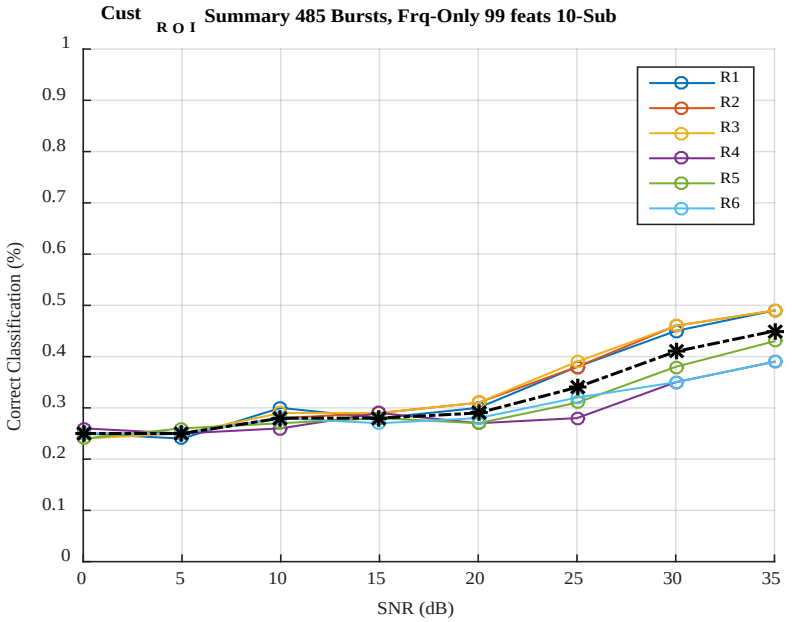


Figure 5. Reduced Dimensional (NF = 33) Class for 24 Permutations (Frq-Only)

Conclusions relative to results in Figure 3 through Figure 6 are visualized using the average performance plots presented in Figure 7 which shows full dimensional and reduced dimensional MDA/ML accuracy averages across all six ROI models for $SNR \in [0\ 35]$ dB. Considering an arbitrary classification accuracy of 70% as a reasonable benchmark for assessing the potential contribution of RF fingerprint features to an overall multi-factor authentication solution, both the full dimensional ($N_F = 99$) and *Amp-Only* ($N_F = 33$) feature sets would perform reliably for $SNR \geq 25$ dB. However, the reduced dimensional *Amp-Only* feature set has the added advantage of only requiring calculation and processing of only one-third the number of features and remains steady in performance for SNR > 10 dB. This steady performance however, meets or exceeds the arbitrary benchmark of 70% classification using the amplitude only features for SNR>20dB.

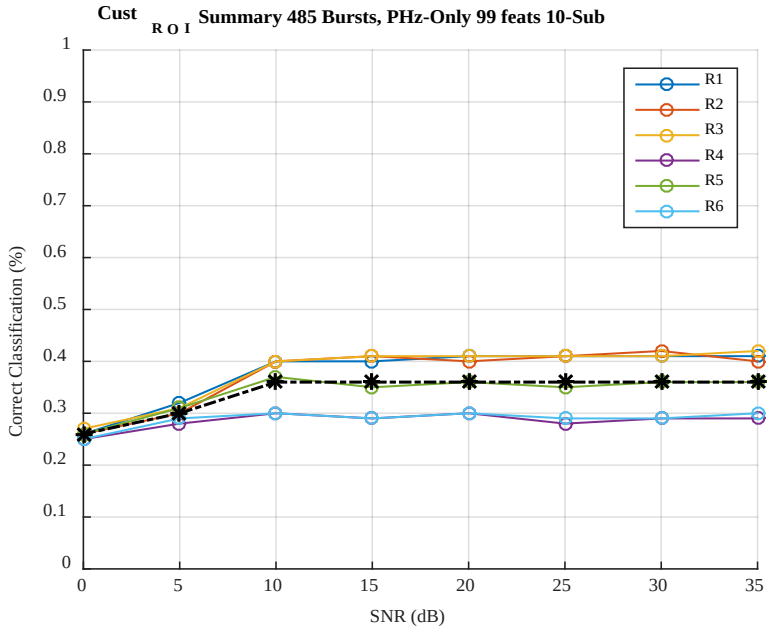


Figure 6. Reduced Dimensional (NF = 33) Class for 24 Permutations (PHz-Only)

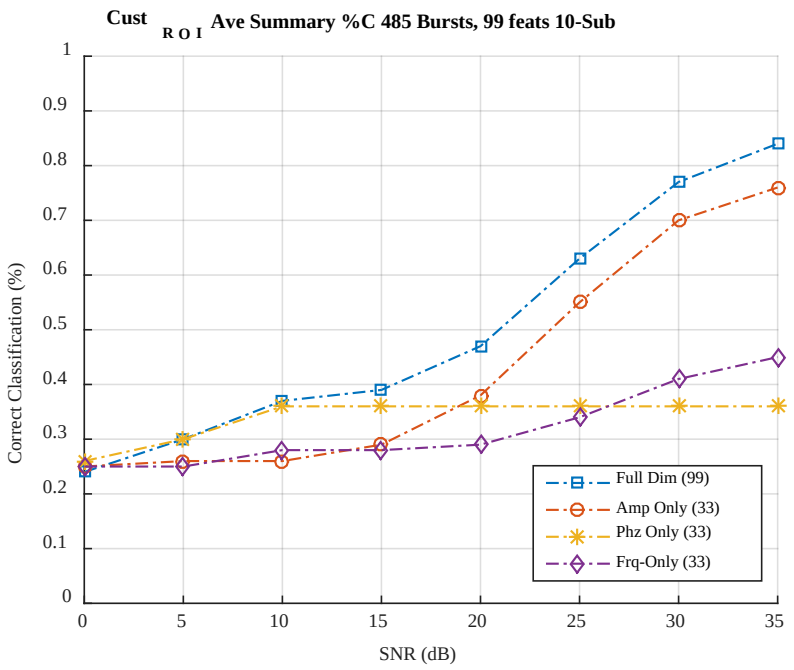


Figure 7. Full Dimensional and Reduced Dimensional MDA/ML Class Averages.

2.5 Conclusion and Future Recommendations

As consumers access demands for SATCOM resource access rise, organizations may become reliant on well- known amateur radio solutions as a first flexible and cost effective option that comes with trust in the operational integrity of their ground stations, satellites and intermediate transceivers. Moving to cost-effective software defined radio options may be less costly for entry; however these devices cannot perform as a stand-alone ground station transmission circuit. This implies that the circuit for RF fingerprinting should have configuration and construction standardization for consistent performance. As the demand for access to SATCOM increase, so does the potential for Cyber-attacks. To mitigate imposter device behavior on specified SATCOM network boundaries, the use of physical or bit-level mechanisms are needed to enhance network or logical level device authentication. Results here demonstrate that customized ROI can be identified given an arbitrary threshold solely by using time-domain RF-measurement statistical features extracted from policy-based customized ROI.

An arbitrary benchmark of 70% classification accuracy was demonstrated for $SNR \geq 35$ dB using like-model ICOM-9100 devices for all reduced fingerprint marker sizes and achieves over 90% classification accuracy using $\boldsymbol{R3}$ as a 33% reduced portion of a standard preamble. The work here builds upon the foundational work that has been previously conducted using RF fingerprints, dimensionality reduction and enhances the cross-layer PHY-MAC-NWK multi-factor authentication framework for air monitoring and trust management systems. The results imply that custom ROIs are achievable and feasible for both cost savings and performance. A bit-level field should be further investigated to see if ROI such fields can be efficiently identified using custom start and stop points such as $\boldsymbol{iMkrs}$. Such a mechanism could be provided in a TDMA or FDMA scheme. A logical field should include a telecommand field for an authorized set of CubeSat satellite command and controls.

Finally, a custom ROI selection scheme should be developed to provide dynamic decision-support capability for telecommand sequence authentication and expressive network security augmentation. As a next step, such a scheme should focus on the CubeSat's Interactive Trust Value (ITV) section of a message's payload. Collections using a *free-space* circuit should be conducted using eight or more radios in a grounded anechoic chamber.

III. Statistical Prediction and Classification of Electronic *Network-Disease*

"The good physician treats the disease; the great physician treats the patient who has the disease." (William Osler)

3.1 Overview

Conventional network diagnostic accuracy studies are difficult to design for maintaining the health of radio frequency (RF) networks due to a lack of a common reference or common operational picture. A common reference, in practice, is used to assess the intrinsic accuracy and posterior usefulness of diagnostic utility tests. Here, a 1-to-1 verification scheme employs Bayes Theorem [32] to compare the specified RF-measurements of new transmission claims against known RF-DNA credential *benchmarks* (signatures) when initial diagnostic results are uncertain. The priori diagnostic test provides the likelihood that the RF origin integrity claims of an uplink access request will be truly *infectious* (unacceptable RF origin similarity) or *benign* (acceptable RF origin similarity) if accepted for further processing by a receiving device. The proposed method selects the highest priori accuracy among binary, ordinal and continuous valued threshold classifiers to improve posterior prediction accuracy of logical-only authentication mechanisms. Processing messages containing *infectious RF* credentials may lead to abnormal network behavior *called electronic network-disease (eND).* The proposed framework for diagnostic testing improves posterior classification accuracy from 32.32% to 100% accuracy among tested samples using a benchmark of 1100 previous RF fingerprint observances. The top distributed denial of service (DDoS) motivation reported among service providers in the enterprise, government and education segment is criminal extortion attacks. Wireless RF networks are often the target of such attacks where the origin integrity (authentication) vulnerabilities exist at the physical and application layer of the OSI model [33].

Conventionally, logical (bit-level) authentication mechanisms are considered in mitigating RF-based attacks by inspecting, classifying and logging suspicious RF communication transactions. However, conventional diagnostic accuracy studies of an RF receiver's log files are difficult to design for RF networks that rely on standard RF modulation schemes and interoperable identification fields. Such schemes and identification fields can be mimicked by software defined radio (SDR) devices. In a threat prevalent ecosystem, RF interception and replay attacks can be employed in efforts to bypass logical authentication schemes and cause a loss of critical network resource availability. Such loss may result from the acceptance of network access credentials originating from unauthorized RF transmission sources that contain bit-level credential forgeries.

Trust is a problem in uncertain threat prevalent monitoring ecosystem with high-authority automation, resulting in an operator who believes the automation is 100% accurate and "re-thinks" their need to rely on other independent decision-support cues that would otherwise indicate abnormal electronic device behavior [34]. Additionally, as more electronic devices are incorporated as integral human support devices, a Cyber Operator's reliance on conventional intrusion detection systems (IDS) during network security monitoring lacks a capability to provide physical RF-DNA origin integrity evidence [35] [36]. A consideration of physical RF attributes, while maintaining network health, may offer early warning against abnormal behavior in electronic networks. Moreover, as the widespread use of implantable medical devices (IMDs) used to treat medical conditions increase, so does the need to ensure privacy of data and prevention of unauthorized modification of the IMDs, causing abnormal behavior in the human subject [37]. Unfortunately, specification-based intrusion detection for wireless IMDs assumes that identification and authentication information cannot be forged [38] which is no longer valid in current threat prevalent cyber ecosystems.

A causation of abnormal electronic device behavior suspected of originating from *infectious* transmissions is called electronic *network-disease (eND).* For electronic patients (node device), RF-measurements of native attributes enable the diagnosis of origin integrity attribution in uncertainty. In this article, a Bayesian-based RF fingerprint filter applies a 1-to-1 credential verification mechanism that compares newly claimed RF signature origins to a known benchmark or gold standard [39]. The individual component features of a composite RF fingerprint are used to verify the origin integrity of RF-Event claims. Our research aims to provide insight into the usefulness of origin integrity verification using RF fingerprints. We explore pre-test (*priori)* and post-test (*posterior)* probability classifications of dichotomous RF-Events A and B, using examples from an arbitrary labeled dataset of *infectious* (B) and *benign* (A) transmission sources. That is, RF-Events originating from A are arbitrarily selected as trusted, while RF transmissions originating from B are electronic forgeries and are untrusted. Bayes' Theorem applies conditional probability to find the posterior estimation that a claimed RF-Event is truly *benign* (a benchmark match) given a *benign* diagnostic test result.

3.2 Background & Related Works

- **3.2.1 Electronic *Network-disease* mitigation**

Biomarkers are defined as [40] [41] "a characteristic that is objectively measured and evaluated as an indicator of normal biological processes, pathogenic processes, or pharmacologic response to therapeutic intervention." Biomarkers assist in the evaluation of distinct physical or natural attributes that are inherent in patients, such as distinct native attributes (DNA). An *RF-Biomarker* is a physical or intrinsic characteristic of an electronic communication device's RF emissions that indicates abnormal process or response when the origin integrity of RF transmissions are suspect for causing *network-disease*.

It is objectively measured and evaluated to differentiate benign (normal) versus infectious (abnormal) electrical RF transmission receipts. RF-biomarker analysis aims to lend further insight into the etiology of a specified network abnormality referred to as *network-disease* (e.g. loss of link access availability) when observed levels are inconsistent. Objective *RF-Biomarker* measurement levels reveal distinct attributes of fixed-circuit emissions of normal transmission processes. As such, a useful RF-Biomarker is distinguishable from other RF-measurement features that do not provide statistically significant decision-support assistance in credential verification.

To reduce uncertainty of a digitally claimed (logical) credential's authenticity, a receiver-specific diagnostic test (*treatment*) considers RF-biomarkers (indicators) to augment the validation of logical credential claims. AN RF-biomarker has a minimum of three major parts; a population of independent RF-measurements as observed by a common RF collection (receiver) device, the statistical distribution of each RF-measurement, a policy specified tolerance region threshold to indicate RF origin similarity acceptance or rejection. All components of RF-Biomarkers should contribute to the aim of indicating early warning detection of *eND*. RF-biomarkers indicate the true origin of w_s given some decision-support tolerance threshold indicated as d_T. RF-biomarker similarity diagnostic results are not a true representation of a received RF-Event's true condition; rather it is a representation of how likely the classified condition is, given a known population and threat prevalence rate [42].

For each RF-biomarker, a statistical RF measurement is taken from the full-wave's real and imaginary parts to include any sub-ROI's real and imaginary parts. This vector of RF-measurements comprises values of independent receiver observations of specified RF-Events. The stored signature of an RF signature contains a distribution of trained observations of w_s.

Using the distribution of each Tx_s device, the probability density function (PDF) can be estimated. The exact equation employed to conduct an RF measurement is represented in this article as $(\star_m)$ where the mth measurement is consistently assessed across a fixed time/space of a received RF-Event. As shown in Table 1, the PDF has been stored for $\vec{x}_i$'s full and sub ROI values for N independent w_s observations by Rx_d. While, all RF-biomarkers of composite RF signatures may not be necessary for accurate comparison, a single indicator alone may not be sufficient for some policy specifications.

This article aims to find the least amount of RF-biomarkers necessary to make appropriate network treatment responses in support of policy while minimizing the acceptance of infectious forgery or impersonation attacks. To support policy p_i, a decision rule is consulted for authentication validation support.

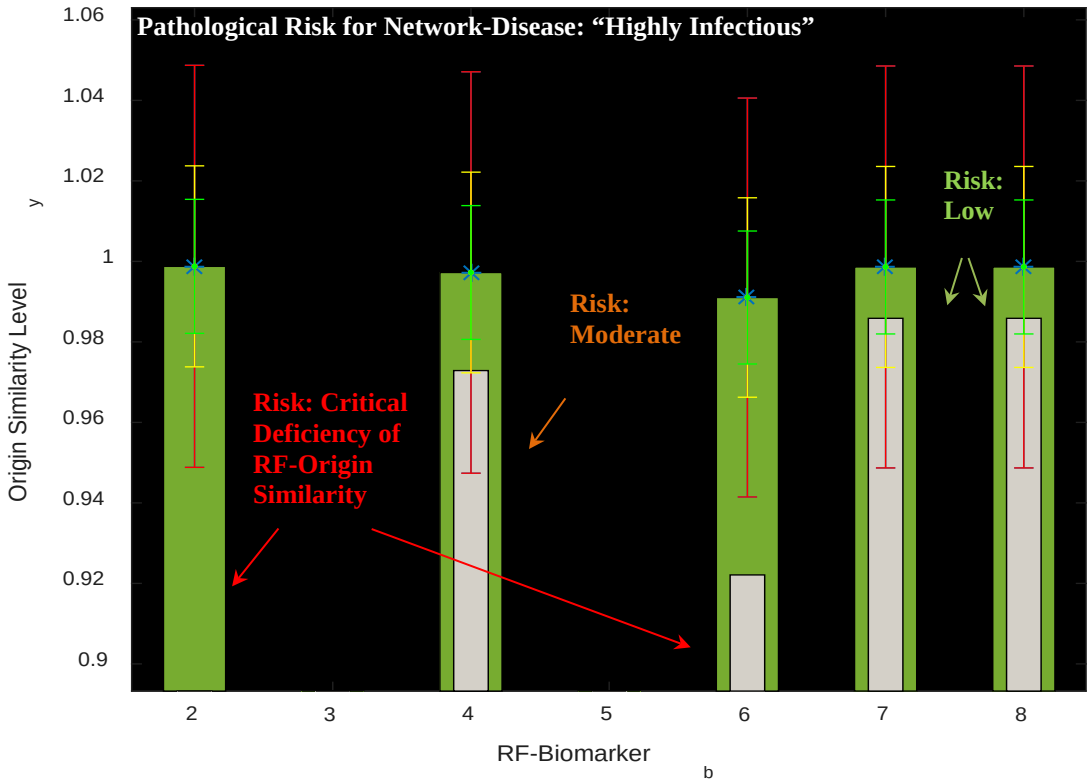


Figure 8. A Diagnostic RF Origin Similarity Test Visualization.

For each c_k^{BIN}, we extract a complex valued RF-Event's signature fingerprint from a specified ROI designated by the **r**th region of a claimed RF-Event w_i. The **m**th $\star$ measurement of *r* is used to compute the RF-measurement statistics. Since we assume that each e_{Tx_s} is physically distinct during the generation of w_s, we obtain trusted physical *credentials* $\left(c_k^{\mathrm{PHY}}\right)$for a given c_k^{BIN}, using RF-measurement $\star_m$ to extract RF-Event signatures from $\boldsymbol{w_s}$ as observable by a designated authenticator Rx_d. Notice, the $\star_m$ measurement occurs prior to demodulation of $\boldsymbol{w_s}$, but may be conducted in parallel to reveal the contents of m after demodulation.

Ahmad (2016) employs an RF-based "biodetection" platform to detect various viruses without using conventional biomarkers. This research suggests an increase in integrating biometrics, biomarker deoxyribonucleic acid (DNA) and RF-DNA fingerprinting terms when identifying humans and machines [43]. At the time of this writing, there was no previous utilization of the term "*RF-Biomarker*". The research contributes a standard naming convention for electronic fingerprinting and treatment recommendations against specific network abnormalities which are suspected to originate from the acceptance of unauthorized RF credentials. For a particular RF-Biomarker (b_k), the pre-test probability that an acceptable tolerance level of similarity for $b_k$appears in an infectious message is estimated by determining the proportion of acceptable b_k appearances in known *benign* RF-Event distributions (0% threat prevalence) versus a distribution of all *infectious* message states (100% threat prevalence).

Bayes Theorem applies conditional probability to estimate the likelihood of occurrence of some RF-Event *B* that has a probability of occurrence greater than 0% [44, p. 20]. Let non-disjoint events *A* and *B* comprise the entire sample space, *S*, and the probability of event *B* is greater than zero.

The conditional probability that event A occurs given that event B occurred is given by

$$P(A|B) = \frac{P(B|A)}{P(B)}. \quad (1)$$

In Biometrics, an estimated 150 standardized indicators [9] called minutia details are used in human fingerprinting techniques. Unfortunately, there is no established number of standardized electronic fingerprint indicators or terminology (i.e. radio frequency fingerprints). Inspired by electronic defense mechanisms against spam and [32] junk email [45] along with authorized wireless uplink access using authentication mechanisms, RF fingerprinting mechanisms are explored to further augment network security. Passive radio frequency (RF) transmitter fingerprinting techniques were used in the mid-90's [18]. Shortly thereafter, unintentional RF emissions were collected from electronic devices, including network interface cards, to discriminate between anomalous behavior [4] [46].

In 1994, Koopman et al., discussed cryptographic methods to authentication transmissions messages using pseudorandom numbers in [47] [48]. DeJean (2007) uses RF-DNA distinct *phase* characteristic-based certificates of authenticity (COA) to augment radio frequency identification (RFID) verification systems by incorporating physical RF attributes into a cryptographic authentication scheme [49]. Currently, RF "distinct native attribute" (RF-DNA) fingerprinting classifies physically distinct RF transmissions based on standardized invariant preamble fields of a message. Invariant fields provide inherent physical characteristic permanence of a composite RF-DNA fingerprint's feature-set. Such a set includes normal distribution of specified RF-measurements of an invariant field for each feature. In RF-DNA fingerprinting, measurements of the main RF characteristics include the instantaneous amplitude, frequency and phase.

The start and stop time of invariant region of interest (ROI) fields indicate the time-series target of RF signature collection. The central moments (skewness, kurtosis, standard deviation and variance) of each main characteristic may also be considered in the composite fingerprint [50] [24] [51] [52]. Reising and Kuciapinski discovered methods to analyze classification parameters, which reduce the composite feature-set's dimensionality [52] [53]. Fingerprint verification of a specified person among all other people in society is conceptually similar to verifying the electronic RF signature of a specific network device from all other devices in its class. In each case, multiple biological details such as age, sex, gender and ethnicity may exist among people to indicate the true fingerprint origin. In electronic devices, digital (electronic) details such an IP address, FCC-ID, and MAC address indicates electronic transmission identification fields.

However, such identification fields are logically encoded, which are vulnerable to forgeries by a capable device such as a software defined radio (SDR) origins. There are various modalities to automate fingerprint authentication and verification of fingerprint details [9]. The minutia detail classification across composite fingerprint features may suffer from poor *detail* (feature) selection when new samples are compared to database templates [54]. Additional methods have been used to automate the discovery of indicators termed "biometrics" in the medical community. Biometrics analyze the quantifiable minutia details to identify people in information systems [55], while regional or localization techniques are employed in electronic networks to capture physical RF features (minutia details) to identify a specific transmission device. During network security monitoring, the visualization of decision-support cues is often employed to assist in enhancing the situation awareness (SA) [56] of Cyber Operators and overall decision-making process to maintain the health of communication networks.

- **3.2.2 Visualization of Decision-Support Cues**

Visualization of benchmark similarity decision-support cues should aim at providing appropriate recommendations to Cyber defenders for accurate response. After detection the physical RF-Event's occurrence, the RF signal's demodulated logical bits are decoded into binary '1s' and '0s' in a specified message format. The ROI associated with the RF signature is examined by aligning the decoded message with the encoding format and compare the invariant credential field's binary values. When the logical (bits) credentials match, the binary fields are logically equivalent. Next, while the demodulation and decoding occurs, the receiving device samples the incoming RF-Event and extracts the specified RF-measurements over the specified time-series ROI. The RF-measurements are then used to represent the physical attributes that are generated by the distinct transmitter while generating RF emissions from a fixed transmission circuit state.

The aim of this step is to identify those RF-measurements, when compared against similar devices, reveal statistical distinctness of fixed RF origins. Network diagnostics are more useful when a significant RF-measurement difference exists between known and new RF-Events.

- **3.2.3 Characteristics of Useful RF-Biomarker Selection**

Following the practice of the medical community, useful criteria assist the decision to treat networks using network-based diagnostic testing. This section discusses criteria to evaluate the potential usefulness of diagnostic features. Key players (e.g. Cyber Operators, network administrators, resource owners and policy makers) may consider the adoption of *RF-biomarker diagnostic testing* capability in two specific areas.

First, *RF-biomarker* candidate screening of log files may determine if *infectious* RF-Events are suspected of unauthorized access attempts given a known threat prevalence and vulnerability. If diagnostic screening is positive for suspicion of infection from a known threat, further tests may be necessary to treat or prevent the occurrence of a specified *network-disease*.

Examples of treatment, may include a comprehensive distributed system of RF-biomarker sensor networks with updatable signatures. Table 3 lists situations where diagnostic testing may be beneficial. Consider diagnostic testing of RF-biomarkers when the risk of *network-disease* perception is serious in nature. In addition, the risk of an infectious RF source should be prevalent among similar networks to support increased threat prevalent rate. A finding of infectious evidence (significant dissimilarity) should be treatable in a wireless RF networking ecosystem. Tests should be minimally invasive to RF circuits and should not harm the communication functionality of the receiver (observer). Finally, a diagnostic test should be accurate in its classification of *benign* and *infectious* RF-Events. The threshold level of accuracy will depend on the goals and objectives of network key players.

There are six major steps as shown in Figure 9 which outline the general process of treating *network-disease*. The framework considers RF-biomarker augmentation while considering Table 3.

0.) Define the normal (non-diseased) and abnormal network conditions.
1.) Specify a communication node pairing policy [7].
2.) Collect an RF signature of authorized transmission states.
3.) Specify the acceptable thresholds for diagnostic accuracy and predictive usefulness of RF-measurements.
4.) Specify network treatment response thresholds to assist decision-making in uncertainty.
5.) Assess the diagnostic accuracy for future prediction estimates.
Refine the process and integrate recommendations for improvement.

Table 3. Criterion of Useful RF Diagnostic tests [40]

	Network-disease should be serious or potentially so (e.g. Inability to provide uplink access)
1	*Network-disease* should be relatively **prevalent** in the target population (Cyber Threat Rate is Increasing)
2	*Network-disease* should be **treatable** (Recommendations to Minimize risk of loss to Receiver or Tx in some cases)
3	**Availability of effective treatment responses** infectious RF carriers who test positive (e.g. evidence of infection is present in a specified CubeSat's received authentication log files)
4	The diagnostic test is **not harmful** to an authentication receiver nor cause unnecessary modifications of the incoming RF-Event's physical RF characteristics.
5	The diagnostic test should be **accurate** in classification of *benign* vs. *infectious* RF-Events according to some policy-based threshold(s).

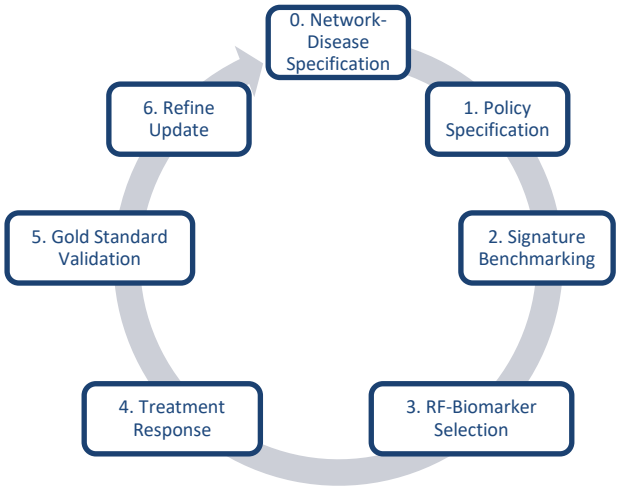


Figure 9. Multi-Factor Authentication Framework

3.2.1 Multi-factor Authentication Framework Overview

- **3.2.1.1 *Network-disease* Specification**

A network abnormality may be attributed to some known or unknown cause. When the cause of a specified abnormality is suspicious of originating from unauthorized or malicious activity such as a cyberattack, its occurrence can be classified as a symptom of realization of *network-disease*. There may be several abnormalities which contribute to observable *network-disease* outcomes.

A specific statement of abnormal network behavior such as the loss of resource availability, caused by a successful DDoS cyberattack provides clarification for strategic targeting, planning, and mitigation of a specific *network-disease* outcome. Moreover, a prevention strategy may specify those electronic transmission states that are authorized and unauthorized to assist in *network-disease* defense and mitigation.

- **3.2.1.2 Policy Specification**

After *network-disease* specification and vulnerability assessment, a user's policy may dictate the flow of information between electronic transmission devices for increased security control. Policy specifies the desired communication paths which originate from trusted electronic devices in authorized transmission states. In addition, naming convention, targeted RF fingerprint ROIs and RF-measurement criteria should be carefully considered. The policy should also indicate the type of electronic receiver that will be employed for demodulation and ultimate authentication of received RF transmission events. Policy should state requirements for interoperability, standardization and invariant field selection. Each of these decisions will guide the RF signature collections process. Finally, levels of acceptance for fingerprint similarity should describe if additional testing is required when a test result is uncertain.

- **3.2.1.3 RF Signature Benchmarking**

RF benchmarking provides trusted RF signatures for diagnostic comparison of new RF-Event claiming to originate from a known fixed transmission source. An authenticating device may possess local or reach-back RF diagnostic capability. When a local device is trained for self-evident authentication of a received RF-Event, the device contains a trusted RF-signature template within its local memory and can conduct the benchmark similarity test while conducting normal communication operations. The memory location of the processor is assumed to be secured for normal operations using RF fingerprints [57].

Such a device trains for self-evident authentication using device-specific observations of an authorized RF-Event transmission from a specified source. As the main characteristics of the RF-Event are collected, additional statistics may be considered if useful.

During a diagnostic test, policy acceptance or rejection thresholds are used by the authentication device to provide a final test estimation of the RF-Events condition as either benign or infectious for causing *network-disease*. RF signature collection provides an initial first step towards developing a useful network diagnostic test benchmark. The aim is to collect a set of RF signatures, usable as templates for integration as a network treatment response in a comprehensive and wellness plan.

- **3.2.1.4 RF-Biomarker Candidate Selection**

Following the collection of RF signature benchmarks, the screening of the most useful RF-measurements is done using statistical and objective analysis. A composite feature-set contains all RF-measurements and statistics of characteristic distributions, however they may not provide useful discrimination information for electronic devices that originate from the same manufacturer and only differ by serial number. Such devices have digital minutia details such as MAC address and FCC-IDs, however they may be mimicked using software defined radios (SDRs) or even worse, may not be considered during network authentication.

The purpose of RF-screening is the discovery of the set of RF-Biomarkers from the candidate feature-set, which provides the most useful electronic device verification accuracy. The goal of candidate screening is to provide the top verification feature-set of a claimed electronic device. The top performing RF-biomarkers are used to compare the logical contents of *m* to the physical attributes of the RF-Event's benchmark to improve posterior classification estimates.

- **3.2.1.5 Gold Standard Validation**

A *diagnostic test* is a formal classification method that partitions a condition into two (e.g. True or False) generalized states [39]. A common diagnostic test, in practice, requires a standard reference for comparisons. A *benchmark* comparison test quantifies a truth reference's measures of performance and is commonly referred to, in the medical community, as a *gold standard (GS)* [42] [58] [39]. A device-specific gold standard (GS) is a source of information, which tells us the true status of received RF transmission event (RF-Event) [42] condition as either *benign* or *infectious*. In this article, the validation test GS file consists of a set of repeatable RF-Events originating from a single trusted device and one or more logically equivalent RF-Event transmissions which originate from physically distinct (distrusted) devices.

Benchmark validation occurs when a GS truth reference is used to assess the diagnostic performance of a classifier and provides insight into the robustness of the benchmark's trained RF signature against new unseen RF signatures. A new validation set of RF-Event collections are collected from the trusted transmission device using identical configurations used for benchmarking to make up the GS file dataset of RF-Events. In addition, RF-measurements are collected from Tx_B by Rx_C.

The goal is to design a truth reference dataset such that the combination of RF-Event conditions (benign vs. infectious) are unknown to a designated authentication device Rx_C. The GS dataset contains the true RF pathology of an RF-Event's condition as *benign* $[D = 1]$ or an *infectious* condition $[D = 0]$. Upon receipt of a new RF-Event, Rx_C employs local diagnostic testing, compares the RF-Biomarker feature-set to its known RF signature benchmark template and reports a diagnostic result. A benign claim test result $[T = 1]$ occurs when the pathological RF origin's similarities of the RF-Event meet acceptable tolerance levels.

An infectious test result $[T = 0]$ occurs when the pathological origin of the RF-Event which fails to meet sufficient origin similarity threshold levels. To conduct a sensitivity or specificity test using a GS, the true condition of all RF-Events samples may consist of entirely all benign or infectious events.

Often times, this practice provides insight into the system's detection capability, but may not provide insight into future observations of RF-Event's received under normal operating conditions. To gain insights into normal operational performance, the GS file should contain an operationally representative proportion of infectious to benign RF-Events. Such a GS file can then be used to assess the estimated system performance under various system modes. The sequence and selection of benign vs. infectious RF-Events should occur randomly to avoid verification bias and to reduce unavoidable experimental errors. After all RF-events contained in the GS file have been presented to the system for classification the raw counts are tabulated for the True Positive, True Negative, False Positive, and False Negative probability rates [39] as described in Section-II (Measuring Diagnostic Accuracy).

A conventional 2x2-count table provides preliminary diagnostic assessment, using a GS file for validation, of N RF-Events. A true positive (TP) GS test result occurs when a received carrier's true signature condition is benign and a diagnostic test reports a benign condition [T=1, D=1]. A true negative (TN) condition occurs when the carrier's true status is infectious and the diagnostic result is infectious [T=0, D=0]. When a diagnostic test reports an infectious carrier condition and the true condition indicated by the GS are benign, a false positive (FP) count is increased [T=1, D=0]. Similarly, when a GS indicates a true benign condition and the test reports an infectious condition, a false negative (FN) result occurs [T=0, D=1].

At the conclusion of the GS validation test, the reported diagnostic results are compared to the truth reference of dataset under various threshold and parameter settings. Depending on the operational ecosystem that a user expects to employ diagnostic testing and their threshold level specifications, a receiver operating curve (ROC) may be useful in deciding the system settings that may provide the best performance to support their policy goals and objectives.

Moreover, a visualization of diagnostic results may also be useful for Cyber defenders during network defense operations as decision-support cues. The GS validation process concludes with a report of the intrinsic accuracy of each diagnostic test. The intrinsic accuracy provides the inherent accuracy (ACC) of a diagnostic test. The posterior classification accuracy provides insight into cost and benefit trade-offs associated with appropriate treatment selection following a diagnostic test.

- **3.2.1.6 Treatment Response**

The purpose of this step provides diagnostic reasoning insight that involves a consideration of *cost* and *benefit* to the network itself, Cyber defender's and key stake holder interests. Some responses are automatic, however in uncertainty; an automatic response may pose high-risk situations. A *benign* RF-Event is highly probable for originating from an authorized source transmission state and is not likely to cause *network-disease* to an authenticating device. However, an *infectious* RF-Event contains suspicious origin integrity evidence which indicates abnormal RF-Event transmissions that may lead to *network-disease* if such events go undetected or untreated. Treatment, in this context, refers to troubleshooting responses taken to mitigate or eliminate early warning signs of *network-disease* resulting from *infectious* credential acceptance.

3.2.1 6.1 Trade-Offs and Risk

There are trade-offs associated with each post-test treatment response of a network's diagnostic result. A benefit occurs when the discovery of infection occurs $[T = 1, D = 1]$ and attempts to gain access are blocked as a treatment response, which ultimately results in the non-occurrence of *network-disease*. However, a cost occurs when *network-disease* occurs despite the use of treatment (e.g. blocking). If the cost of each diagnostic test were identical, then the more tests necessary to make a treatment decision increases with each additional test. Decision-makers aim to make the correct network treatment decision with as few diagnostic tests as necessary.

An arbitrary policy may specify a minimum accuracy of 90% pretest classification accuracy before recommending treatment for a network. Policy determines the goals and objectives and RF-Event similarity thresholds of acceptance for a given operational ecosystem that has known threat prevalence. When a diagnostic result falls below such a treatment threshold, a "do nothing" and continue to monitor treatment recommendation may occur to mitigate *network-disease* symptoms. When intrinsic diagnostic accuracy is undesirable and error are high, additional diagnostics maybe necessary to provide useful decision-support for treatment. In Figure 10 a diagnostic test that falls between $Th_1$and Th_2 indicates inconclusive results and suggests a need for additional diagnostic testing.

Network treatment options are recommendable for results greater than Th_1. Situation (b) may occur when pre-test diagnostic accuracy results contain high errors resulting in less accurate posterior predictive estimates. The use of two thresholds may provide enhanced performance in uncertainty. Unfortunately, prior knowledge of the pre-test classification accuracy is often uncertain and lacks gold standard performance testing.

3.2.1.1.2 Risk

Consider a common network infrastructure, which consists of *n*-nodes. Each node's original configuration through common network administration has inherent trust. That is, the set of nodes, which form the backbone of the network, are the trusted devices. T_x collections of trusted devices form RF-biomarker baseline signatures. Signature development only considers authorized transmission carrier states. Policy specifies trusted device pairings for network communications according to transmission source origination to destination. RF signature comparisons occur as logical credential claims arrive to treatment R_x nodes.

If a physical and logical match is indicated, the bit-level credential is likely authentic and benign; however, when levels are significantly dissimilar, the origin integrity of the carrier is likely infectious and treatment recommendations to prevent *network-disease* may be necessary. When results indicate high *risk*, more information about the RF event may be necessary to validate the origin integrity of fixed transmission sources.

$$risk(y) \equiv P[D = 1 | \, T = t] \tag{2}$$

In general larger values of Y indicate higher levels of risk. In binary marker evaluations, we consider the simple setting where RF-Events either have high or low symptomatic risk values. That is, high $risk(0) \equiv P[D = 0 | \, Y = 0] = NPV$, or the low value where low $risk(1) \equiv P[D = 1 | \, Y = 1] = PPV$.

Pepe recommends that the distribution of risk in the population indicated by the RF-biomarker should be reported (absolute risk and the frequencies of those risks in the population) [59]. The cumulative distribution function of the RF-biomarker under consideration is given by F. The risk level is

$$R(v) = P[D = 1 | \, T = F^{-1}(v)]. \tag{3}$$

Let p = prevalence which indicates how widespread the potential of *network-disease* (threat) is throughout the entire population under consideration.

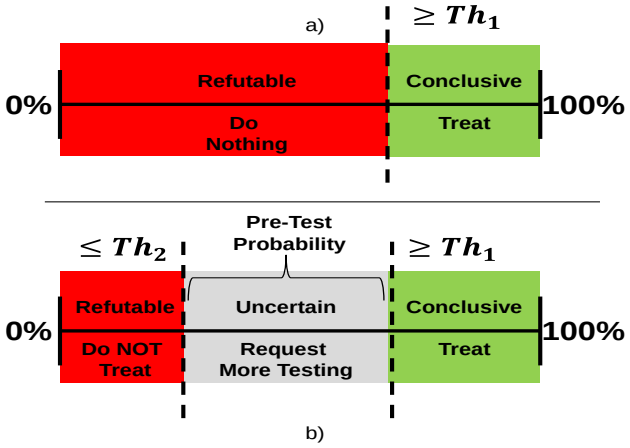


Figure 10. Post-Test Diagnostic Treatment Decision Rules in Uncertainty

- **3.2.1.7 Refine/Update**

After final RF-Biomarker selection, threshold selections, a simulation assesses the posterior accuracy of a diagnostic test using a GS validation file. Updates to the framework proposal can occur at any step without regard to order.

3.2.2 Decision Rules

A decision rule [31] or corresponding likelihood ratio determines the maximum error criterion or maximum a posteriori (MAP). A binary decision rule has two possible outcomes, when a new RF-measurement's RF-Biomarker level falls within the tolerance region, then it is acceptable, rejected otherwise. A tolerance region threshold D_t classifies acceptable Euclidean distance levels of similarity for new RF-Biomarker measurements. A receiver learns to recognize a device specific signature benchmark by observing n independent normal benign RF-Events. After observation of the events, a self-similarity test occurs that consists of all "n-vs.n" observations, measurement and analysis of fingerprints to establish the *true* benchmark similarity levels for each local RF-Biomarker of a composite RF-DNA fingerprint.

The aggregation of three decision-rules (tolerance region, ordinal and continuous) aims to improve posterior probability classifications. Screening, binary, continuous, ordinal and paired diagnostic tests were considered in this article. Each test can be utilized together, independently, or as a single stand-alone test depending on the cost and potential benefit of the test given. A thorough discussion of each threshold decision rule is discussed in [39]. The initial screening of a receiver's log file may be a logical place to conduct *network-disease* screening using a diagnostic test that meets policy thresholds. During the decision to treat a network for symptoms of *network-disease,* an initial screening level criterion $Screen_{LVL}$ specifies the minimum level of RF origin similarity acceptance. This value was experimentally determined by setting $Screen_{LVL} = p$. The screening tolerance is

$$Screen_{TOL} = (n * p) * Screen_{LVL}. \quad (4)$$

3.2.2.1 Tolerance Region

A policy-based tolerance region over a distribution of RF-measurements specifies an acceptable similarity level of at least a proportion p of the population $x - pulses$ (RF-Events) with confidence $(1 - \Psi)$ is contained within its upper $(U(X))$ and lower $L(X)$ limits of acceptance [60]. A regional tolerance region can be computed to support binary classifications of composite RF-DNA fingerprint authenticity using a threshold for acceptance or tolerance rejection, a $(p, 1 - \alpha)$ two-sided binary tolerance interval $(L(X), U(X))$ satisfies the condition

$$P_x\{P_x(L(X) \leq X \leq U(X)|X) \geq \rho\} = 1 - \alpha. \quad (5)$$

Where $'\alpha'$ represents the significance level. Construction of localized RF-Biomarker tolerance regions aim to improve posterior classification of a composite binary tolerance interval. The tolerance region is created using a benchmark Composite RF-DNA fingerprint dataset of size N.

The tolerance factor is computed based on a user's specification for reliability of new comparisons made to a specified benchmark value. The specifications include the *content* of new $'X = b'$ RF-Events (independent random variable) that are to be tested, the overall level of *confidence* that the RF-Biomarker levels should fall within and the *proportion* of X samples that should are acceptable to a known benchmark [60].

Each tolerance region is adjusted using the Gauss-Kronrod factor k_2 [30], which makes the interval slightly different from a conventional confidence interval which is generated about a distribution's mean. Using the training RF benchmark, a tolerance region is computed for each local RF-Biomarker candidate. Each RF-Biomarker candidate component generates a localized benchmark using a $[(\rho = n), (\Psi = \{90,95\})]$ tolerance interval. Threshold Th_1 accepts RF-Events where the combined Euclidean distance of RF-measurements of similarity falls within the bounds of (5). An extension is made to tune this decision rule to reduce errors made from composite averaging of all RF-measurements, instead each localized measurement develops its own local tolerance region specification in parallel. In uncertainty, two or more classifiers used in parallel, as shown in Figure 10b may improve posterior estimates when Bayesian aggregation is employed in uncertainty.

3.2.2.2 Ordinal Valued Threshold

The second decision-rule aims to refine the results obtained in (5) using an ordinal valued threshold. When the total number of characteristic RF-Biomarker features is defined from {1, 2, …, b}, an ordinal threshold setting accounts for the majority vote $'O_{Vote}'$ of local feature diagnostics that meet local policy threshold requirements for acceptable tolerance.

$$O_{dt} = \left(\left(\frac{b}{2}\right) + 1\right). \tag{6}$$

The ordinal valued data decision rule can be reduced to a binary result by comparing 0_{Vote} to the threshold specified in (6) above as;

$$0_{Vote} \geq O_{dt}, \begin{cases} 1, & Similarity\ Majority\ exists; \\ 0, & otherwise. \end{cases} \quad (7)$$

The threshold specification from (6) implies a majority of features, from measurements must meet or exceed local pathology similarity to the RF signature's benchmark. For example, let $b = 8$ local RF-measurements. Let each local RF-measurement that meets acceptable tolerance count as a vote for RF-Event similarity, while each local tolerance failure counts as a vote against RF-Event similarity. When threshold $[O_{dt} = 5]$ and the count of local similarity acceptance meet or exceeds O_{dt}, the RF-Event is counted as a benign RF-Event occurrence.

3.2.2.3 Continuous Valued Threshold

A third decision-rule option employs a continuous data threshold $'Z_{dt}'$ that provides an average risk $'\bar{Z}_{risk}'$ of acceptance based on the benchmark similarity rating, using risk zones. A risk zone divides a binary policy defined tolerance region from (5) into three weighted zones of similarity error (lower is better). Where the upper and lower bounds for $[z = 3]$ zones becomes;

$$\big(L_z(X), U_z(X)\big) = L_3(X) < L_2(X) < L_1(X),\ U_1(X)\ < U_2(X) < U_3(X). \quad (8)$$

Where each local RF-Biomarker candidate receives a risk zone match score that ranges from one to four. In isolation, a risk zone match score value that is close to '1' (i.e. Euclidean distance is near or equal to '0') indicates an RF-Biomarker candidate that has a *high* similarity to the benchmark and presents a low risk of forged credential acceptance.

When a pulse fails to meet the original benchmark's binary tolerance interval, it receives a risk score of four to indicate complete tolerance region boundary failure. When average risk zone scores are less than or equal to Z_{dt}, the pulse is accepted, and rejected otherwise. A comparison of the average risk score ($\bar{Z}_{risk}$) to the threshold Z_{dt} indicates the level of risk associated with allowing network access using the claimed logical credentials of an RF-Event. A summary of the risk zone comparisons is

$$\bar{Z}_{risk} \leq Z_{dt}, \begin{cases} 1, & acceptable\ Risk; \\ 0, & otherwise. \end{cases} \quad (9)$$

3.2.3 Measuring Diagnostic Accuracy

A *classification model* maps each instance of an RF-Event $'W'$ to a predicted class. When conducting analysis of two independent (logical vs physical attributes) variables produced by physical RF transmission events we evaluate the performance of the diagnostic test to correctly classify the condition of the RF-Event's claimed symptoms (decoded bits). The results of the 2x2 count table provide input to computing the probability or predictability of the two conditions.

- **3.2.3.1 Classification Model**

Consider a simple security policy that specifies a set of received *authorized transmission states* by a trusted network communications device as W, where each element of W is mapped to the set of instances $\{s, i\}$ [61]. For example, the RF-Event w_s represents a verified transmission state that is secure. Such a state inherently includes the transmission source of origin while all *other* non-authorized transmission states w_i are specified as insecure regardless of origin [62]. The research goal is to detect *infectious* behavior from unauthorized or insecure transmission origins and prevent electronic *network-disease (eND)* using pathological RF-DNA attributes to enhance logical credential authentication schemes. To that end, we predict secure state classifications to be *benign*, while all insecure transmission state predictions are predicted to be *infectious*.

More formally, let the independent variable D denote the true origin condition of an RF-Event's transmission state as

$$D = \begin{cases} 1 & for\ benign; \\ 0 & for\ non-benign. \end{cases} \quad (10)$$

Let T denote the result of some Diagnostic Test which classifies a received RF-Event W as either benign $'w_s'$ or infectious $'w_i'$. Further, suppose that an RF-DNA fingerprint benchmark has been previously collected and saved for reference by authenticating device Rx_C.

Consider a continuous decision threshold policy that ranges from zero (completely infectious) to one (completely benign). For pure binary decisions, the diagnostic test (T) is represented as

$$T = \begin{cases} 1 & tests\ (+) for\ benign; \\ 0 & tests(-) for\ not\ benign. \end{cases} \quad (11)$$

Given the results of T and the true status D, four basic classification categories can be derived from raw test count classifications of true positive (TP), true negative (TN), false positive (FN) and false negative (FP) using a known *benchmark* truth or GS file truth reference as described previously. The sensitivity (Se) of the diagnostic test provides the probability of a benign test $P(T = 1)$ and is determined by the TP count divided by the total number of RF-Events specified as having benign pathological RF origins. The specificity (Sp) of diagnostic testing is the converse of the Se, measures the capability to exclude infectious carrier conditions, and is expressed by $P(T = 0)$. The prevalence $'p'$ of a specific network threat does not affect the intrinsic diagnostic accuracy indicated by a pre-test Se or Sp accuracy of a diagnostic classifier [42].

A Type-I error measures the FP rate that occurs in proportion to the total number of true benign carriers that exist in the GS. A Type-II error is determined by the FN rate of a carrier's tested result as benign when in fact the RF-Event contains evidence of infection.

Predictive values quantify the usefulness of the paired diagnostic test result for *network-disease* mitigation [39, p. 16]. The probability of a positive test is the positive predictive value (PPV) and the likelihood of a negative test result is the negative predictive (NPV).

- **3.2.3.2 Pre-Test Classification Probabilities (Priori)**

Probability classifications employ various names of the basic count categories. We adopt the medical terminology in this article for the terms, true positive fraction, true negative fraction, false positive fraction and false negative fraction (TPR, TNR, FPR and FNR).

Khanna describes the *pre-test* classification probabilities in terms of rates. For example, when assessing a misdetection or false alarm rate of a system, the TPR may be used to describe the classification system's *reliability* [58]. Fawcet uses the terms *hit rate* and *recall* [61], whereas the medical community employs the term *sensitivity* fractions. Pepe argues that the value is not a rate at all, but a probability [39]. Here we refer to the TPR as the *sensitivity* (Se) to detect a TP classification condition from a population of secure (trusted) instances of W which exists when

$$Se = TPR = P[T = 1 \,|D = 1]. \tag{12}$$

- **3.2.3.3 Post-Test Classification Probabilities(Posterior)**

Predictive values are used to quantify how well (usefulness) a diagnostic test result predicts the true status of an RF-Event's origin. A positive predictive value (PPV) [39], false discovery rate (FDR), negative predictive value (NPV), and false omission rate (FOR) [39]. Bayes' Theorem is adapted from [42] in general form for post-test probabilities as;

$$p(D = d|T = t) = \frac{p(T=t|D=d)p(D=d)}{p(T=t|D=d)p(D=d)+p(T=t|D=1)p(D=1)} \tag{13}$$

The posterior predictive values of a receiver-based diagnostic test are [39]:

$$PPV = P[D = 1 \,|T = 1], \tag{14}$$

$$FDR = (1 - PPV) = P[D = 0 \,|T = 1], \tag{15}$$

$$NPV = P[D = 0|T = 0], \tag{16}$$

and

$$FOR = (1 - NPV) = P[D = 1|T = 0]. \tag{17}$$

Where a perfect test predictor occurs when $PPV = 1$ and $NPV = 1$. When there is no useful information about the true nature of an RF-Event's origin integrity, the classifier is deemed useless. This useless situation occurs when the $PPV = \rho$ and $NPV = (1 - \rho)$.

The roles of D and T are reversed in the *post-test* predictive values relative to their roles in the *pre-test* classification probabilities [Pepe p. 16]. Post-Test classification probabilities are not used to quantify the inherent accuracy of a receiver's diagnostic test [39].

3.2.3.1.1 Measuring Predictive Usefulness

Given ρ and ACC, we can determine the Se probability that an RF-Event will test positive for being benign. A *pre-test probability* is based on the RF-Event's historical profile, modulation schemes, binary encodings, signs, symptoms, and results of any other diagnostic tests performed earlier such as logical credential verification [42] [39] using classification probability parameters (TPR, FPR, ρ). Using Bayes Theorem, multiple prediction estimations aim to improve the predictive accuracy of pre-test diagnostic results. This article adapts two methods from medical diagnostic testing and a general method of aggregation adopted from Rosen et al.

3.2.3.1.2 Relationship between Predictive Values and Classification Probabilities

Predictive values are best used to quantify the usefulness of a diagnostic test [39, p. 16] while *pre-test* classification probabilities are best used to indicate the intrinsic accuracy of a specific diagnostic test. Predictive values are used to assist and provide decision-support to Cyber and Network Operators by providing the likelihood that possible infectious or undesirable behavior is present given the diagnostic test results of Bayesian RF-DNA fingerprint filtering.

When knowledge of ρ from (8) or (9) is available, there is a direct relationship between *posterior* predictive values and *priori* classification probabilities. Prediction values are dependent on three parameters that should be reported in diagnostic test performance results [39].

On one hand, these three parameters can be found using the prior classification probabilities and the disease prevalence as (TPR, FPR, ρ). Using *predictive* values, the parameters used after a diagnostic test is performed are (PPV, NPV, τ) [39, p. 16]. The symbol τ indicates the probability that a specified diagnostic test will result in a positive test $P[T = 1]$.

In the first medical example [39], the diagnostic test's usefulness assessment employs Bayes Theorem to represent the post-test probabilities (PPV, NPV,τ) in terms of the pre-test probabilities (TPR, FPR, ρ) where

$$PPV = \frac{\rho TPR}{\{\rho TPR + (1-\rho)FPR\}}, \tag{18}$$

$$NPV = \frac{(1-\rho)(1-FPR)}{\{(1-\rho)(1-FPR) + \rho(1-TPR)\}}, \tag{19}$$

and

$$\tau = \rho TPR + (1-\rho)FPR \tag{20}$$

Moreover, the pre-test or priori probabilities are written in terms of Posterior probabilities and similarly found as

$$TPR = \frac{\tau PPV}{\{\tau PPV + (1-\tau)(1-NPV)\}}, \tag{21}$$

$$FPR = \frac{\tau(1-PPV)}{\{\tau(1-PPV) + (1-\tau)NPV\}}, \tag{22}$$

and

$$\rho = \tau PPV + (1-\tau)(1-NPV). \tag{23}$$

As a second medical community example of assessing the usefulness of diagnostic accuracy, Zhou's application of Bayes' Theorem computes the posterior probabilities using (4), (7), (15) and (16) as follows [42, pp. 48-49] ;

$$PPV = \frac{Se * P(D = 1)}{Se * P(D = 1) + (1 - Sp) * P(D = 0)} \tag{24}$$

$$NPV = \frac{Sp * P(D = 0)}{Sp * P(D = 0) + (1 - Se) * P(D = 1)} \tag{25}$$

Rosen generally employs Bayes Theorem to mitigate infectious (the occurrence of electronic spam) message acceptance using word occurrence filters. More generally, if B_i is the event where an RF-Event's message contains a set of matching physical RF-Biomarker credential occurrences b_k, then by Bayes' Theorem the prediction probability that a message containing all of the specified RF-Biomarker $b_1, b_2, \ldots, b_k$ as *benign* similarity levels is found by

$$r(b_1, b_2, \ldots, b_k) = \frac{\prod_{i=1}^{k} p(b_k)}{\prod_{i=1}^{k} p(b_k) + \prod_{i=1}^{k} q(b_k)}. \tag{26}$$

For a particular RF-Biomarker (b_k) credential, the pre-test probability that an acceptable tolerance level of similarity for $b_k$appears in an infectious message is estimated by determining the proportion of b_k appearances in known benign RF-Event distributions versus a distribution of all non-benign (infectious) message states exist. Suppose that the probability of some RF-Event B contains a claimed logical message credential c_k greater than '0', which implies that the RF-Event did occur [44, p. 20].

- **3.2.3.4Misclassification Probabilities (Errors)**

  There are two types of errors that may occur during pre-test classification. A Type-I error is referred to as the false positive rate (FPR) and is often indicated by the symbol alpha (α).

When used in computer science applications, it is inappropriate to simply report the misclassification probability, instead report both components of the misclassification probability which is the FNR = (1-TPR) and the FPR [39]. The equation for a Type-I error is

$$FNR = (1 - TPR) = P[T = 0|D = 1]. \quad (27)$$

A Type-II error rate or fraction estimates the probability that a receiver classifies an RF-Event as *infectious* when the true state condition is *benign* as

$$FPR = P[T = 1\,|D = 0]. \quad (28)$$

One method of quantifying diagnostic test accuracy is by considering the frequency of misclassification for each infectious RF-Event states. The paired diagnostic results of (FPR,TPR) probabilities define the likelihood at which (4) occur during a particular diagnostic test [39]. The likelihood of detecting a true negative condition (TNR) is the diagnostic test's specificity (Sp) and is defined as

$$Sp = TNF = (1 - FPR) = P[T = 0 \mid D = 0]. \quad (29)$$

During hypothesis testing, we refer to the null hypothesis (H_0) for the true condition variable ($D = 1$) that an RF-Event likely originates from a trusted source origin versus the alternative hypothesis H_a that ($D = 0$) an RF-Event probably does not originate from a trusted source origin. The overall errors are often referred to as the misclassification probabilities and written using Se and FPR above, provided the *prevalence* of disease is known,

$$\rho = P[D = 0] = \left[\frac{\sum w_i}{\sum w_i + \sum w_s}\right]. \quad (30)$$

When a gold standard *benchmark* is used, (8) is easily determined by taking the occurrences of a state's true condition from a known dataset (gold standard) and divide the total of all samples in the dataset's population. The equation for misclassification probability or prevalence for (8) can be found using (4) and (6) above from [39] as

$$\rho = P[T \neq D] = \rho(1 - TPR) + (1 - \rho)FPR. \quad (31)$$

3.3 Methodology

3.3.1 Experimental Set-Up (Hardware and Software)

The wired circuit depicted in Figure 11 represents the RF-DNA collection and networking experimentation circuit. Each circuit component is labeled with a letter and role for representative icon reference. For example, the device used to generate the initial message for collections is shown as (label | description) PC1| PC1: msg (message) generator. The laptops in Figure 11a and Figure 11f are identically configured with the following; LabVIEW 2014 with RT Modulation Tool Kit, Math Script. Windows 10, (HP Zbook 15) with 32GB RAM, 500GB DDRL 4DM, 5400 RPM, integrated NIC, I Core i7-4800MQ processor. Software includes Microsoft Office 2013, Matlab 2015a, 2016a and Jump Pro 12.1. Each physical circuit had physically distinct hardware, cables and antennae and could transmit or receive. This experiment focused specifically on a simplex uplink transmission scenario.

1) **Transmission Circuit (Ground Station)**

Tx_A, Tx_B and Rx_C are national instrument USRP-2922 software defined radios that differ by serial number only. The blue dashed box on the left of Figure 11 represents the representative ground station circuit or transmission source Tx_A.

In Figure 11a and Figure 11b represent that baseband logical message generator (*msg*), which transmits commands to the front end transmission device Tx_A in Figure 11c (USRP 2922) for final modulation onto the uplink medium. Devices Tx_A and Tx_B (red USRP 2922 in Figure 11c) are the transmitters under test. GS1 is defined as the benchmark validation test for Tx_A emissions as observed by receiver (authenticator) Rx_C. Tx_A*'s* RF emissions are collected for signature profile benchmarking. Tx_B represents an arbitrary opponent transmitter that attempts to forge the credentials of Tx_A.

2) RF-Event and Environmental Considerations

A 2-FSK modulation scheme is used to transmit *msg* over FM using a carrier frequency of 449.9MHz. A 100 kHz offset is set from the center frequency of 450MHz. Each pulse duration is approximately 6.399ms. The receive circuit had a tunable bandwidth selector that was set to 20kHz and detected each pulse using a tunable triggering mechanism based on the magnitude of the amplitude. The FSK deviation was set to 1.

There were eight total RF-measurements that were selected arbitrarily to include the instantaneous amplitude, frequency, and phase. Preliminary results extracted RF-DNA fingerprints near the preamble of ICOM-9100 amateur radios used in an operational ground station circuit, where the amplitude provided the greatest accuracy for correct classification. Therefore, the variance, skewness and kurtosis were set for collection using the USRP SDRs. Finally, the root mean squared error of the amplitude was collected for each pulse.

3) Extraction / Credential Diagnostic (CubeSat)

In Figure 11a, b and c, the purple dashed box encloses the representative CubeSat receiver Rx_C, which authenticates the origin integrity of messages claiming to have originated from Tx_A and is depicted Figure 11f, and Figure 11g.

For each RF-Event pulse (Figure 11d) successfully received by Rx_C (Figure 11g), the RF-DNA is extracted from 10 fixed and equally spaced sub regions plus the full wave regions using complex real and imaginary parts of the analog waveform. This brings the total number of distinct RF-DNA contained within a complete collection to ([8 features] * [22 sub regions]) 176 RF distinct native attributes for possible selection as key discriminating factors.

4) Output Files

There are three output files that are generated by Rx_C following RF-DNA collection. Initially, Rx_C is trained to learn the RF-DNA of each trusted device Tx_i. After that, the benchmark signature is validated for accuracy using new RF-DNA collections from unseen RF-Events from the same device. After benchmarking, Rx_C is placed in testing mode to assess the level of accuracy to diagnose messages which contain potentially infectious credentials.

a) *Data1*: Raw waveform data

Data1 is used to provide validation that a transmitted message is properly received as intended using matched modulation and demodulation schemes for final message decoding.

a) *Data 2*: RF-DNA signature

The RF-DNA benchmark credential consists of the distribution of RF-Measurements previously defined by policy. The benchmark consists of (8 RF-Measurement features * 22 real and imaginary regions of interest) for the full complimentary RF-DNA set. We analyze eight of these 176 using the real values of the full wave characteristics.

b) *Data 3*: Baseline RF-biomarker Levels:

The distribution of measurements obtained from the RF-DNA subset is then assessed using Euclidean distance to assess the level of self-similarity that each feature has with itself. The average result is used as the baseline RF-Biomarker similarity level.

In summary, Tx_A and Tx_B operational modes were set for transmission only. SDR Rx_C functions as the authenticating device which collects RF-measurements transmitted RF-Events (command message). Rx_C was trained using Tx_A's authorized RF-Event transmissions for benchmarking and future 1-to-1 authentication validation. Rx_C's sampling rate was set to 1MS/s to obtain 6.4k sample points per pulse. The transmitted message has a 48-bit preamble, 48-bit payload and a 48-bit postamble. During GS validation, Tx_B is used to provide infectious (unauthorized) transmissions at a prevalence $'p'$ rate up to 20%.

Two commands transmitted from Tx_A and Tx_B are used. All collections and RF-DNA processing was done using the physical circuit Rx_C, which is different from previous research that used a separate non-connected devices for collection and processing. Empirical results suggest same device that collected RF-DNA should be used to validate future claims for consistency.

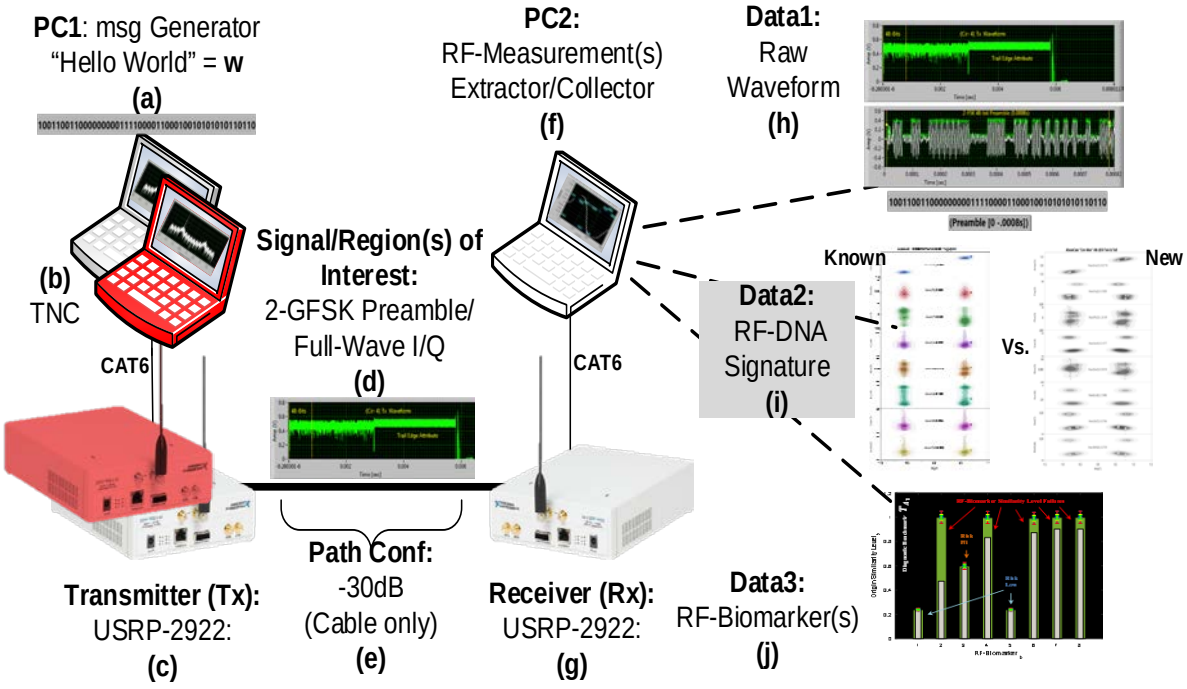


Figure 11. Physical Network Diagram

- **3.3.1.1 Experimental Limitations**

Collections were done in a lab ecosystem where the RF transmission devices were connected to a common ground source shared by Building 646 of the Air Force Institute of Technology (AFIT). Finally, demodulation and decoding verification had 80% levels of success, required multiple attempts to collect sufficient samples during a collection. The successful collection rate was approximately 70%.

The poor performance in transceiver is explained by NI engineers stating that the uncalibrated devices were not "network ready [63] and that synchronization of the underlying FPGA modules were needed to increase decoding accuracy and synchronization [64] [65]. All devices had physically distinct hardware and logically equivalent configurations. The research approach for post-processing and RF-Biomarker selection was conducted on previous RF-DNA fingerprint collections from six ICOM-9100 devices [66], resulting in similar performance.

- **3.3.2 Dataset Selection**

- Benchmark: File 'Cir6DB2922Tx4FullStatsc1' contains 1100*8 RF-measurement samples of RF-Events from A transmitting command-1.
- Benign Claims: File 'Cir6CL2922Tx4FullStatsc1contains 150*8 RF-measurement samples of RF-Events from A transmitting command-1.
- Infectious Claims (B): 'Cir6DB2922Tx5FullStatsc1 contains 1009*8 RF-measurement samples of RF-Events from A transmitting command-1.

Test Population Size: N = 150 for GS and 1100 for benchmark. The tolerance factor for n-150 is $[k_2 = 0.0696]$ and when $[n = 1100]$, $[k_2 = 0.0645]$ when using (5) to compute binary tolerance regions. The coverage is set to 0.05 and the confidence is 90% for the tolerance region calculations.

- **3.3.3 Pre-Processing**

Here, the full wave real valued RF-measurements considered are; absolute value of the peak Amplitude, instantaneous Frequency, instantaneous phase, variance of the amplitude, skewness of the instantaneous amplitude, kurtosis of the instantaneous amplitude, standard

deviation of the instantaneous amplitude, and the root mean squared error of the instantaneous amplitude. Let $B = \{1,2, \dots b\}$ represent the set of RF-measurements used as RF-Biomarker candidates of *network-disease* diagnostics.

- **3.3.4 Benchmarking Process**

The Euclidean distance metric is used to quantify the level of similarity between the benchmark and new RF-Event measurements. An all vs. all approach is used to develop the benchmark's level of self-similarity. After finding such self-similarity, a tolerance $'tol'$ region is determined by varying the acceptable Euclidean similarity distance from [0 to 1] using increments of 0.025. When RF-measurements fall within the tolerance interval, the result is *benign* (Pass), otherwise, a fail results in an *infectious* classification. The local and regional composite benchmark RF-measurement levels are shown in Figure 12. The Composite benchmark and self-similarity levels appear on the right. The local RF-Biomarker candidate similarity levels appear on the let in green. At the top of each measurement level, a tolerance region indicates the acceptable Euclidean distance from the benchmark that a new RF-Event will be accepted or rejected. The tolerance region is divided into three risk zones. When new RF-measurements fall outside of the upper and lower tolerance regions boundaries, the local or composite classification is Infectious.

During the RF signature collections process, RF pulses contained significant variation from pulse to pulse. Some explanation occurs from sampling procedures, while other variations occur due to a lack of device synchronization. The USRP2922 devices are development and testing only devices and not as end network nodes. We improved the synchronization between devices so that a binary string reception and synchronization offset occurs prior to demodulation in order to recover the baseband digital string with confidence.

This step provided verification that the proper message was readable. The reliability of successful receipt was approximately 60%. To mitigate this unfortunate effect, the RF-Event was collected such that the start and end time of each pulse was statistically identical between pulse collections yielding statistically consistent pulse collections of a known RF-Event. To minimize triggered pulse impurities, a filter removes nonconforming pulses in the final benchmark distribution. Using this method, we improved a saved pulse rate to nearly 80% acceptance during raw collections.

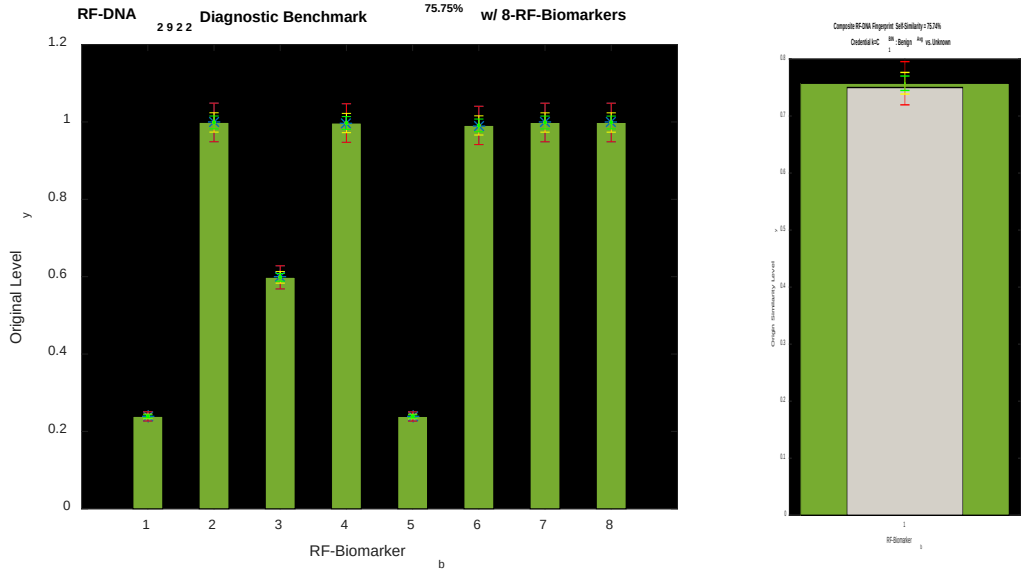


Figure 12. Baseline Benchmark for Transmissions Device $\boldsymbol{Tx_A}$.

- **3.3.4.1 Decision Rules and Treatment Thresholds**

There are three customized classifier decision thresholds rules. 1.) D_t provides a Pass /Fail classification as to whether a new RF-Event's RF-measurements falls within tolerance tol. 2.) An ordinal valued threshold ($O_{dt} = 5$) takes a set of B RF-Biomarker candidates' RF-measurements and computes its all-vs.-all localized independent Euclidian distribution distance using tol as defined above.

In addition, O_{dt} considers a simple majority (b/2 + 1) of all RF-measurements that fall within local tolerance as a regional *benign* result. When a lack of simple *benign* majority exists using O_{dt}, the regional RF-Event is considered *infectious.* 3.) Similar to the ordinal valued threshold, a continuous valued threshold considers a level of risk acceptance for each local RF-Biomarker candidate using $(Z_{dt} = 2.125)$. Each candidate's baseline tolerance region is further divided into three weighted risk zones.

New RF-measurements that fall within risk zone-1 have the lowest weight of $risk = 1$. Moderate risk zone 2's weighting is $[risk = 2]$. RF-measurements that fall within risk zone-3 boundaries meet initial Euclidean distance tolerance levels, yet represents higher $risk = 3$. When an RF-measurement falls outside the upper or lower tolerance regions boundaries of risk zone-3, the risk is critical with $risk = 4$. Each localized RF-Biomarker candidate reports its score and a regional average is considered for the overall level of risk acceptance for RF-Event's further processing. When the average regional risk is less than or equal to Z_{dt}, the RF-Event is classified as benign. The RF-Event is classified as infectious when the regional risk level is greater than Z_{dt}.

- **3.3.4.2 Treatment Response Thresholds.**

Three threshold values are arbitrarily chosen to demonstrate the experiments' proof of concept. The $Screen_{LVL} = 20\%$, GS file size is $n = 150$ and threat $p = 20\%$. The initial log file screening tolerance is $Screen_{TOL} = (150 * 0.2 * 0.2) = 6$. For a specified screening classifier, a decision rule to continue treatment against *network-disease* is assisted using an initial threshold rule as

$$Th_1 = \begin{cases} \text{T}, & SumCount_{TN} \geq Screen_{TOL}; \\ \text{F}, & otherwise. \end{cases} \quad (32)$$

If infection is NOT detected by classifier DT_i, that the sum of TN's did not meet or exceed the screening tolerance level specification of suspected infection levels, consider the classifier's predictive (posterior) usefulness for predicting benign RF-Events with low false omission errors. However, when the TN count meets or exceeds the minimum screening level, the system may be at risk of *network-disease* as a likely outcome. The treatment responses are summarized with the following pseudo code using the threshold settings from Table 4 as follows;

When $[Th_1 = F]$**; //No Infection suspected**
If $[PPV \leq Th_4] \cap [FDR \geq Th_5]$**,**
    // EVIDENCE UNCERTAIN.
    ASK FOR MORE DIAGNOSTIC TESTING
Else
    // REFUTABLE EVIDENCE
    DO NOTHING
End.
When$[Th_1 = T]$ **; Infection of Log Files Suspected**
If $[ACC \leq Th_2] \cup [FPR > Th_3]$
    // EVIDENCE UNCERTAIN.
    ASK FOR MORE DIAGNOSTIC TESTING
Else
If $[NPV \leq Th_6] \cap [FOR > Th_7]$
    // EVIDENCE UNCERTAIN.
    ASK FOR MORE DIAGNOSTIC TESTING
Else
    // CONCLUSIVE EVIDENCE
    TREAT FOR *NETWORK-DISEASE*
End.

Table 4. Treatment Decision-Support Threshold Summary

Threshold / Rule	Parameter	Value	Default
Th_0	Screen?	[Yes/No]	Yes
Th_1	Symptoms?	[T/F]	T
Th_2	ACC	(0:1)	.9
Th_3	FPR	(0:1)	.1
Th_4	PPV	(0:1)	.95
Th_5	FDR	(0:1)	.05
Th_6	NPV	(0:1)	.95
Th_7	FOR	(0:1)	.05
D_t	Global Euclidean Distance	(0:1)	.05
O_{dt}	Local Majority	[0:b]	5
Z_{dt}	Risk Zones	[0:4]	2.125

When a benign test result meets or exceeds threshold limits, the treatment recommendation is “DO NOTHING.” This response implies that a Cyber Operator should continue to monitor the health of the network for signs of infections or abnormal behavior. When an infectious test result’s NPV are less than 90% certain and the PPV, then “Recommend ADDITIONAL TESTING.” In this case, more diagnostic tests should be combined with the initial diagnostic test to improve the negative prediction or rule out as benign.

- **3.3.5 Metrics**

Each classifier’s performance is evaluated for classification accuracy of the truth reference GS file before and after Bayesian aggregation. The intrinsic accuracy and predictive usefulness results will be used to provide decision-support recommendation to treat, do nothing or ask for more diagnostic testing towards mitigation of *network-disease*. Using the raw counts of TN, TP, FN and FP, the priori classification probabilities of TPR, FPR, TNR and FNR will be computed to provide the pre-test classification probabilities and the overall intrinsic accuracy.

Next the usefulness of posterior prediction estimation is assessed by evaluating the probabilities for the PPV, FDR, NPV and FDR classifications. A screening of RF-Biomarker candidates selects the highest pre-test and post-test accuracies with minimal errors while considering the treatment decision rules from Table 4 to establish performance cut-offs. Generally, higher intrinsic accuracy is better and higher posterior predictive accuracy is better.
The top performing classifiers are selected for Bayesian aggregation with the aim of improving the posterior classification estimations. Independent RF-Biomarker candidate classifiers should not be combined with *custom* classifiers to avoid duplicating a same classifier selected bias. The final selection of the top performing classifier’s is reported as the final set of RF-Biomarkers of *network-disease* for device A.

3.4 Results

3.4.1 Visualization and RF Fingerprint Discovery

The waveform displayed in Figure 13 shows a preamble that is 48-bits in length used as the baseline transmitted and received RF-Event. The message "Hello World" is transmitted with a 48-bit preamble followed by a 48-bit postamble and ends at ~0.003-seconds of the RF event. The trail edge of the USRP's RF-Event is lengthy compared to the actual encoded message.

The top graph depicts the averaged received waveform by Circuit-4 while in an authorized state of circuit transmissions by Tx Circuit-6 using 6400 total pulses selected from a pool of four specified commands. During this research, the trail edge could not be modified and as a consequence, consecutive transmission had a minimum wait time of 2 seconds, delaying processing time for real time processing and response actions. In Figure 13, the preamble region shows the real part of the waveform's magnitude. The distinct structure of the amplitude's magnitude enables visual clarity when determining if logical decoding of the message. In this case, the 2-FSK encoding aligns well with the 48-bit preamble bit stream, where a binary encoded 1 represents a low frequency response in amplitude and a 0 represents a higher response. The graph uses Lab VIEW 15 code to support this effort in the summer of 2016.

The purpose of Figure 13 is to provide visual assurance that a transmitted message is successfully received, demodulated and decoded by a designated authentication device. As shown, Rx_C successfully decodes RF-Events at the bit-level for specified ROI recognition. The lower graph of Figure 13 indicates successful decoding of the 48-bit preamble portion of the RF-Event using 2-GFSK demodulations originally transmitted by Tx_A. In this experiment, the entire waveform was considered as the invariant ROI. In practice, this may not be straight forward when portions of fixed messages contain additional synchronization fields that increment automatically.

To enhance intuition, when statistical means testing is available, a visualization which combines the distribution of a GS file's RF-measurements to the distribution of the trusted benchmark may be useful. In Figure 15, a contour plot of the RF-Biomarker's whose mean was significantly different from the trusted benchmark is shown.

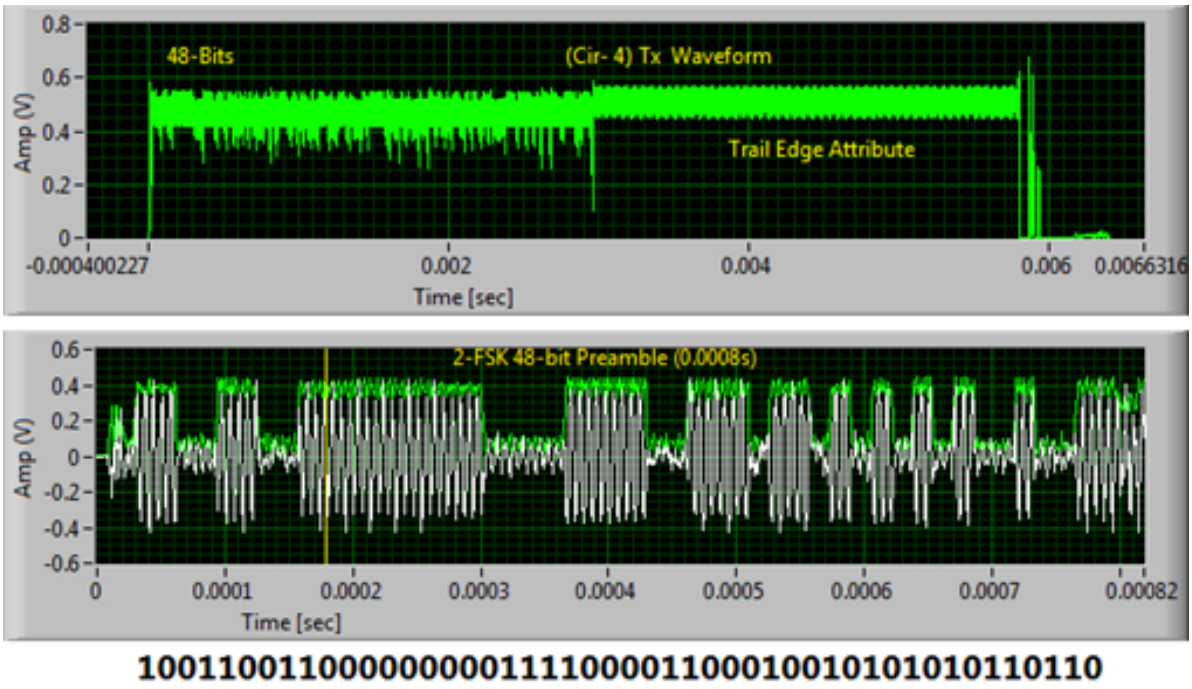


Figure 13. 2-GFSK Waveform

From top to bottom, the amplitude, frequency, phase and standard deviation RF-measurements are plotted against a two-level amplitude. The distribution of RF-measurement values, when the amplitude was low is shown on the left, while the distribution of feature values extracted using specified RF-measurements appear on the right of Figure 15. In addition, each candidate RF-Biomarker is separated by its own scale and stacked on top of each other to visually portray an electronic version of an electrophoresis DNA plot. A comparison of the electronic strands of 'GS file vs. benchmark' for each RF-Biomarker candidate reveals some significant differences in the mean distribution of the underlying RF-Events. Specifically, b_2's benchmark appears to suffer from visible distribution splitting when compared to original benchmark strand.

The greater the statistical difference in electronic similarity, the larger the **split** appears. The prevalence rate is 20% and the noise tolerance level is set at 0.05%. This observation is called *rf-splitting* of a main characteristic's RF-Biomarker strand.

When a candidate is selected as an RF-Biomarker, *rf-splitting* of a main RF characteristic is observed and the difference is statistically significant, the occurrence suggests a good indicator of unauthorized RF transmissions. Such visual observation of *rf-splitting* may provide enhanced decision-support cues for network operators monitoring their real-time networks. A combination of factors which include, visual, statistical and best practice corroboration lends itself to decision-support cue acceptance for network monitoring operations. When reliability of decision-support cues is feasible, a simple visualization such as a bar chart can be used as a quick reference to indicate abnormal network behavior.

In Figure 16 the results of the GS files show the pathological benchmark similarity results (grey) plotted on top of the benchmark (green) levels. There were a total of 120 benign pulses and 30 infectious pulses in the mixture GS file dataset from column two of Table 5. As shown in Figure 16c, the system correctly diagnosed all benign (blue) pulses, and correctly detected the infectious (red) pulses that failed to meet RF-biomarker thresholds. The entire GS file classification (gray) shown in Figure 16c indicates concern for *network-disease*, since the lowest performing classifier's TN count exceeded the minimum threshold of six using (6) above and suggests a need for more diagnostic testing before recommending a treatment response. More specifically, a low level of benchmark similarity is observed by RF-Biomarker candidates b_2, b_4 and b_6. Without having knowledge of what these markers indicate at varying system levels, the certainty of infection is not conclusive. The levels of b_3 indicate a medium risk of infection using Z_{dt}.

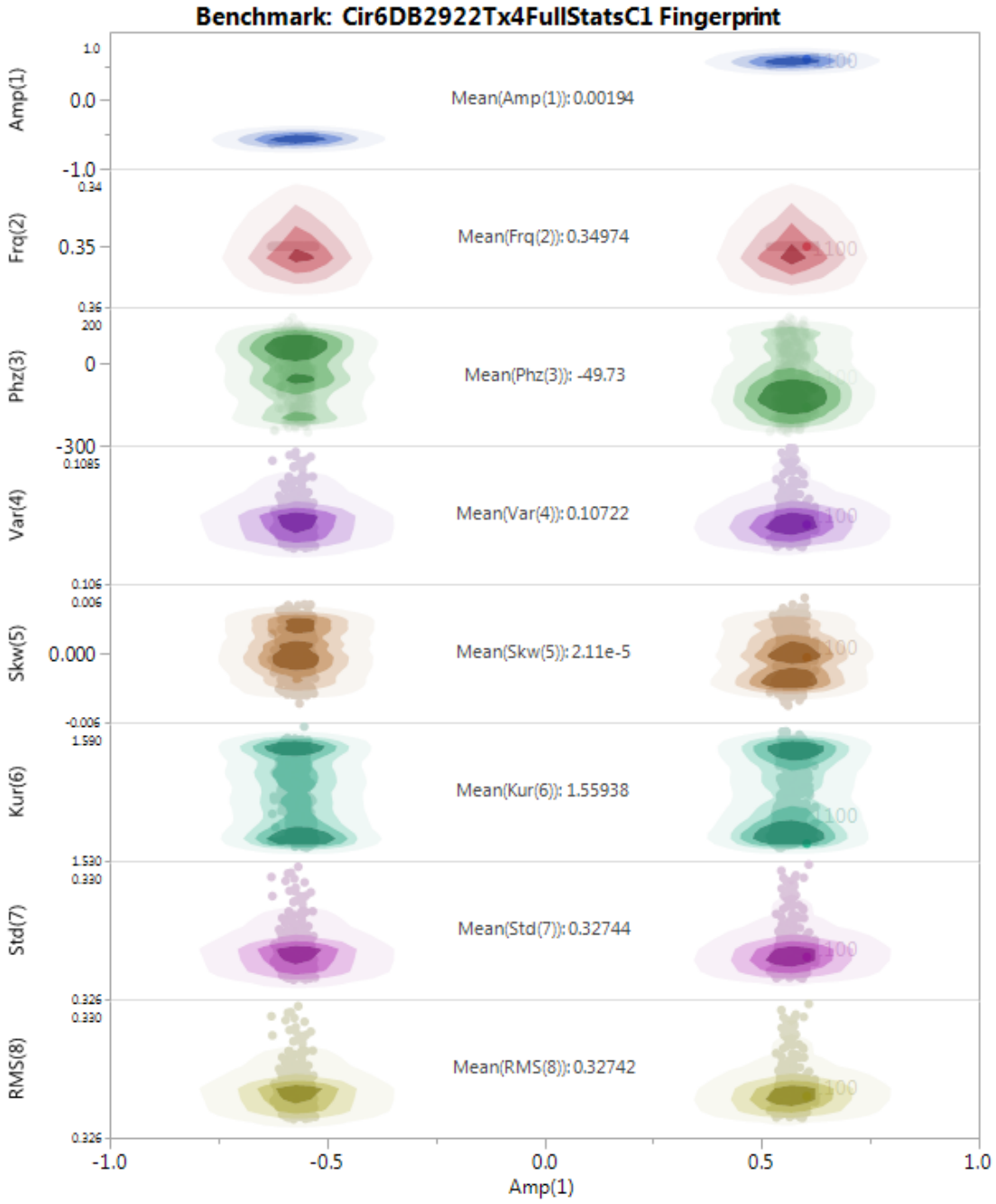


Figure 14. RF-DNA *benchmark* contour plot [n=1100] RF-Events observed by Rx_C

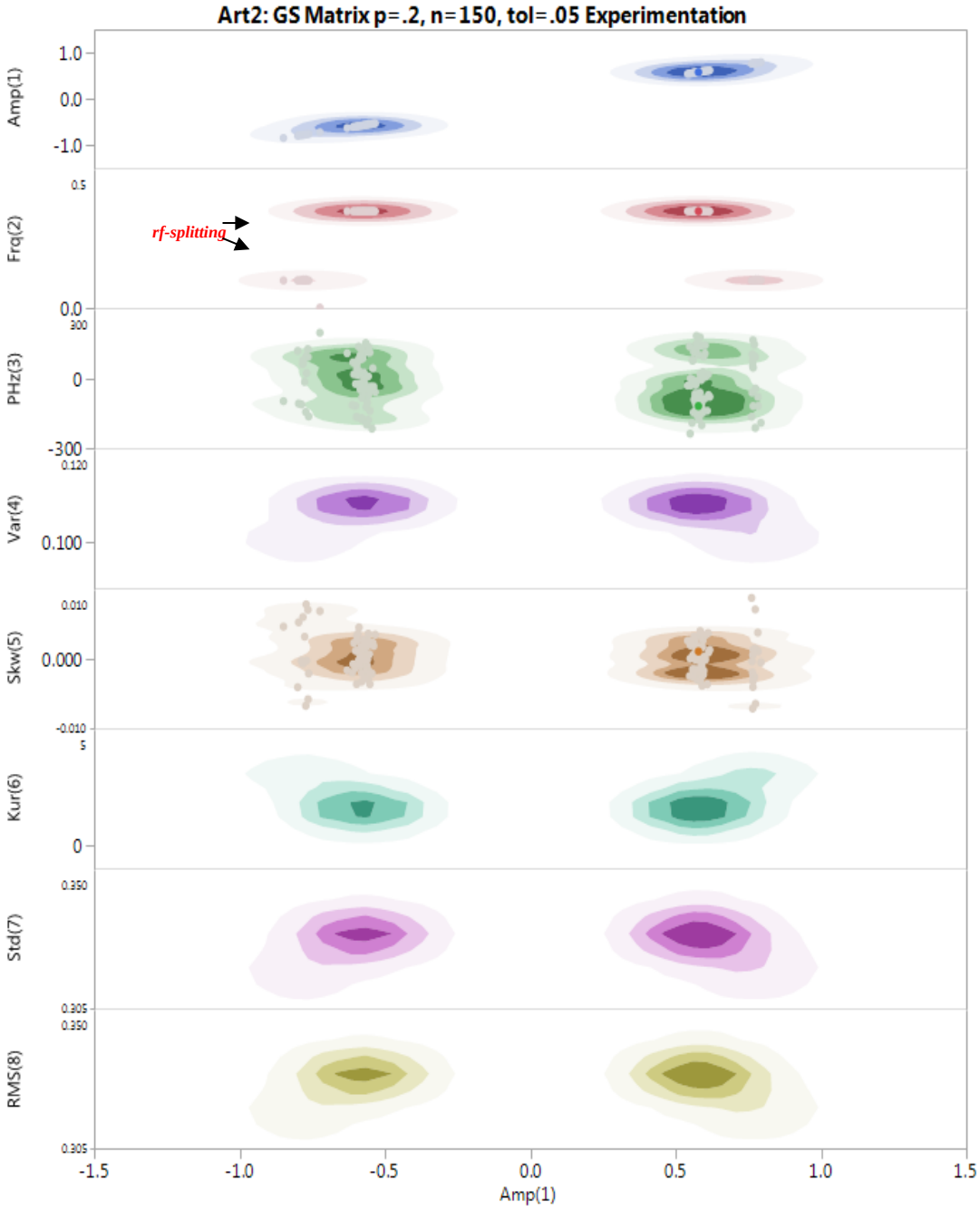


Figure 15. RF-Biomarker b_2 indicates *Rf-splitting* of random log file batch [n=150]

Batch processing might best be used as a forensics augmentation tool for example [8] for electronic authentication device log files. This approach may not be readily useful for real-time information systems that require a pulse by pulse response recommendation.

Infectious GS file RF pulse #5 (red bars) in Figure 16 was is compared to $Rx_C's$ benchmark of $Tx_A's$ authorized transmission of 'command-1'. Similarity results that compare the single pulse to the composite RF-DNA fingerprint are shown on the left of Table 1. RF-Biomarkers 1-6 fail all diagnostic tests, while markers 7-8 falls within a medium risk of truly being infectious. A significant low level of dissimilarity for b_2, b_6 suggest a significant deficiency in benign levels that would be expected to be found in a normal benign pulse received from Tx_4, while the concentration of b_3 and b_5 indicate significant high concentration levels that are outside the observed (Rx_d) boundaries for the composite RF-DNA fingerprint.

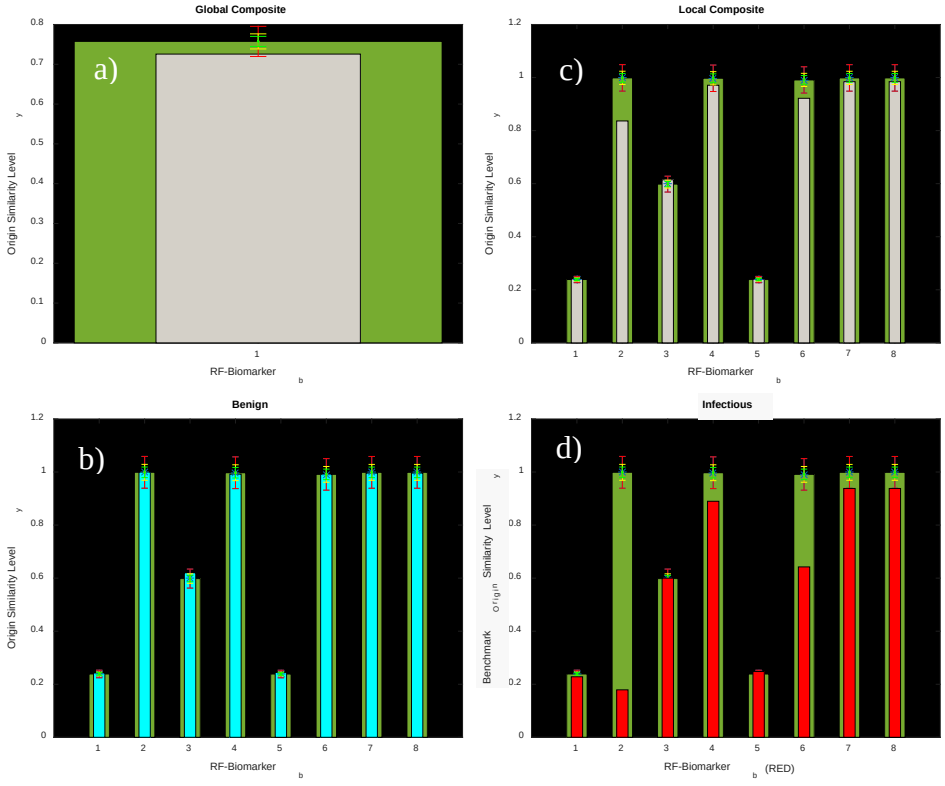


Figure 16. Benchmark vs. single infectious credential originating from $\boldsymbol{Tx_5}$.

3.4.2 Benchmark Results

After decoding confirmation, the benchmarking of Tx_A was conducted to include a self-similarity test to assess the level of consistency that the transmitter had.

The self-similarity level is used as the average expected value for all new RF-Events. The self-similarity results of the benchmark tests are provided in the far right column of Table 5. The benchmark assists classification of new credential authenticity claims in uncertainty. A batch of 150 new validation samples are used in the GS reference dataset where $\rho = 0.2$. Initially, the training set of RF-Events collected from Tx_A resulted in a composite self-similarity score of 75.74%. With the acceptable composite similarity tolerance set to 0.05 average Euclidean distance, the upper and lower bounds for a 95% confidence interval is 79.5358% and 71.9610% respectively.

A classification of any new composite measurement that falls within the bounds is, rightly or wrongly, *benign* using classifier D_t in isolation. As observed in Table 9, the false positive rate using D_t fails to meet the minimum requirements of Th_3. Moreover, its intrinsic accuracy of 84% also fails to meet requirements of Th_2. The use of D_t in isolation implies a high level of uncertainty and requires additional diagnostic testing before a treatment response recommendation occurs. When the localized components of the RF-DNA fingerprint were considered, their independent self-similarity scores were maintained separately for classification and then evaluated using classifier O_{dt} and Z_{dt}. The local self-similarity scores appear in the far right hand column of Table 5. The tolerance region upper and lower boundaries for each risk zone are in Table 6. Using O_{dt} at the same system settings as D_t, achieves an intrinsic accuracy of 99.33%, while classifier Z_{dt}'s ACC is 98%. A treatment recommendation response using combined diagnostic results from O_{dt} and Z_{dt} provides more certainty. However the decision to treat using Z_{dt} alone is still uncertain because the predictive estimate for NPV of 90.9% fails to meet the treatment requirements of Th_6 as specified in Table 4 above. At this point, classifier O_{dt} meets all requirements for usefulness and a conclusive decision to "TREAT" the network can be recommended.

Sometimes, the practice of a single point of classification may be insufficient evidence. In such situations, additional diagnostics may be necessary to corroborate evidence claims. A visualization of the mean's test statistical result appears in Figure 17. RF-Biomarker candidate's b_2, b_3 and b_6 appear as potentially useful classifiers for low tolerance levels. Candidate b_4 had the 4th highest p-Value.

Table 5. Diagnostic Benchmark Similarities for self, GS and Infectious Pulse

RF-Biomarker Candidates	*RF-Event Similarity* Infectious RF-Event (5) n=1, p=1	Gold Standard Batch n= 150, p=0.2	Device A Benchmark n=1100, p =0
b_1	14.20	24.11	23.87
b_2	19.10	83.61	99.87
b_3	97.17	61.11	59.83
b_4	94.99	97.71	99.72
b_5	33.55	24.77	23.86
b_6	65.83	92.31	99.10
b_7	97.46	98.83	99.86
b_8	97.46	98.83	99.86
Composite Strength Score	64.97	72.67	75.74

Table 6. kFactor = 0.0645 and 0.0696 when (n=1100, 150) [60] [67], coverage=.05,confidence= 1-alpha)) (*tol* = .05 and p =.2)

	Upper Risk Tolerance			*Lower Risk Tolerance*		
	Zone-3	*Zone-2*	*Zone-1*	*Zone-1*	*Zone-2*	*Zone-3*
b_1	23.8812	23.5616	23.4551	23.0289	22.9224	22.6027
b_2	98.9549	98.9548	98.9548	98.9546	98.9545	98.9544
b_3	62.1450	61.5796	61.3911	60.6372	60.4487	59.8832
b_4	98.2408	98.2174	98.2096	98.1784	98.1706	98.1472
b_5	24.2642	23.8955	23.7727	23.2812	23.1583	22.7896
b_6	98.1819	98.1663	98.1611	98.1402	98.1350	98.1194
b_7	98.6182	98.6062	98.6023	98.5864	98.5824	98.5705
b_8	98.6182	98.6062	98.6023	98.5864	98.5824	98.5705

The difference between the benchmark (red line) mean is significant for b_2, b_3 and b_6 at a tolerance level of 0.05. The differences between RF-measurement means are not significant for b_1, b_4, b_5, b_6 or b_7 at this setting. Initially, the low p-Values of b_2 < 0.0001, b_3 =0 .0013 and b_6=0.0098, appear as the top candidates for RF-Biomarker selection for Euclidean distance tolerances of +-0.05%. However, b_4's ACC would emerge as a better indicator at higher tolerance levels than b_3.

Table 7. Statistical Analysis: P-Values

Benchmark	***Gold Standard Validation Testing (n=150), Tol = 0.05 dF = 149***			
N=1100 df = 1099	**100% Benign**	**100% Infectious**	**20% Prevalence**	**t-Test (p-value)**
➢ $\bar{b}_1 = 0.00194$	0.0226	-0.0832	0.049	.9266 (0.3556)
$\bar{b}_2 = 0.34974$	0.34995	0.09941	0.2994	-6.0695 (<.0001)*
➢ $\bar{b}_3 = -49.74$	-18.61	-10.641	-20.863	3.2736 (0.0013)*
$\bar{b}_4 = 0.10722$	0.1084	0.09746	0.10588	-1.6586 (0.0993)
$\bar{b}_5 = 0.0000211$	0.00024	0.0006	0.00027	1.0965 (0.2746)
➢ $\bar{b}_6 = 1.55938$	1.56044	3. 64867	2.06577	2.6168 (0.0098)*
$\bar{b}_7 = 0.32744$	0.32923	0.31075	0.3247	-1.5729 (0.1179)
$\bar{b}_8 = 0.32742$	0.32923	0.31073	0.32468	-1.5759 (0.1172)

Each RF-Biomarker's usefulness in similarity discrimination is assessed, where the specified RF-measurement mean from each GS file is compared to the original benchmark trained fil's mean. Using a t-Test, the p-Value for the mixture GS file is provided in the far right column of Table 7. In Table 7, the means comparisons tests for each localized RF-Biomarker candidate is provided for benchmark comparisons against truth references for a 100% benign test, 100% Infectious test and a 20% treat prevalent test.

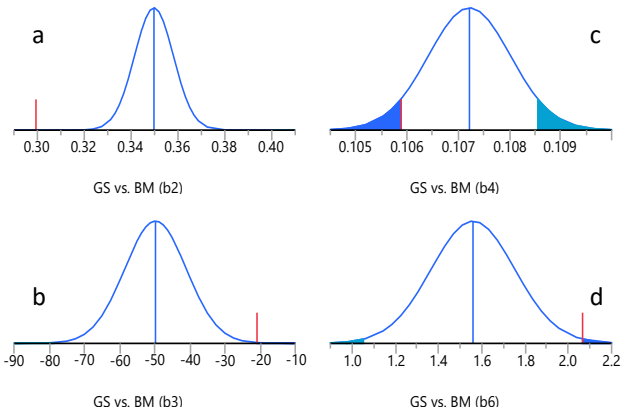


Figure 17. P-Values and Early RF-Biomarker Candidate Selection.

3.4.3 Gold Standard Validation Results

- **3.4.3.1 Pre-Test Count Totals**

The raw counts results of each classifier when tested against the GS file are shown in Table 8. There were a total of 120 benign RF-Event samples in the dataset, while 30 RF-Events were truly infectious RF-Events originating from Tx_B using logically equivalent software configurations. The table is divided between custom classifier analysis of the local RF-Biomarkers and each independent candidate's performance. Six of eleven classifiers correctly detected all 120 benign RF-Events originating from Tx_A. In addition, six of eleven classifiers detected all infectious RF-Events correctly. However, only b_2 and b_6 achieved perfect classification at the tested system setting. D_t, b_6 and b_7 had the highest false positive counts of 23, while b_1, b_5 and b_7 had false negative counts of 115 or more.

Table 8. Count (p = 0.3 *tol* =0.05 n-150, k2 = 0.0645)

Classifier	*TP*	*FP*	*TN*	*FN*
D_t	120	23	7	0
O_{dt}	119	0	30	1
Z_{dt}	117	0	30	3
b_1	0	0	30	120
b_2	120	0	30	0
b_3	5	1	29	115
b_4	120	3	27	0
b_5	0	0	30	120
b_6	120	0	30	0
b_7	120	23	7	0
b_7	120	23	7	0

- **3.4.3.2 Intrinsic Accuracy Results**

Following the raw classification counts assessed against the GS file, the research turns towards assessing the intrinsic accuracy of each classifier in isolation. The ACC is used to indicate the level of accuracy that a classifier is expected to achieve before a diagnostic test is administered.

A receiver operating curve (ROC) of the diagnostic Se vs. FPR is shown in Figure 18 using four tolerance levels (0.05, 0.2, 0.4 and 0.5) are initially used to provide additional insight into candidate RF-Biomarker performance before final diagnostic test selection. All pre-test classification probabilities are provided in Table 9 for $[tol = 0.05]$ and all other default system settings. In, candidates for RF-Biomarker selection, b_2, b_3 and b_4 have acceptable levels of Sensitivity with low false positive errors. RF-Biomarker candidate b_4 exceeds the FPR threshold when $[tol > 0.025]$. RF-Biomarkers b_1, b_3 are not useful and a performance with a 100% FPR. RF-Biomarker 3's sensitivity of 3% failed to meet the minimum acceptable threshold for ACC.

As the tolerable Euclidean distance for similarity acceptance increases, a general increase in the RPF occurs for all RF-Biomarker candidates, but at various rates. This suggests that a selection of RF-Biomarkers may be more useful at various SNR levels. As shown, RF-Biomarker candidate b_2 meets the TPR and FPR thresholds when $[tol < 0.55]$. Moreover, as the tolerance parameter increases, a different pairing of RF-Biomarkers candidates emerges as possible selections to improve posterior accuracy.

For example, when *tol* = 0.5, the best selection of RF-Biomarkers candidates, that meets all decision rules threshold requirements from Table 4, is candidate $b_2$only. When *tol* = 0.02, b_2 and b_6 provide the best accuracy for detecting benign RF-Event credentials. RF-Biomarker b_6 fails FPR thresholds at *tol* > 0.3, while b_3's limit is *tol* = 0.2. In this experiment, RF-Biomarker candidates b_1, b_5, b_7 and b_8 failed to meet the maximum FPR threshold at any system setting. Although every RF-Biomarker reached acceptable levels for sensitivity when the *tol* reached its limits of *tol* =1, the high FPR indicates a high acceptance of infectious credentials if these markers are used as the sole indicator of for credential verification.

RF-Biomarkers $b_7$and b_8 are sensitive to benign credential acceptance; however, there are considerable false positive errors, which rule them out as useful RF-Biomarkers that can assist in *network-disease* detection and mitigation.

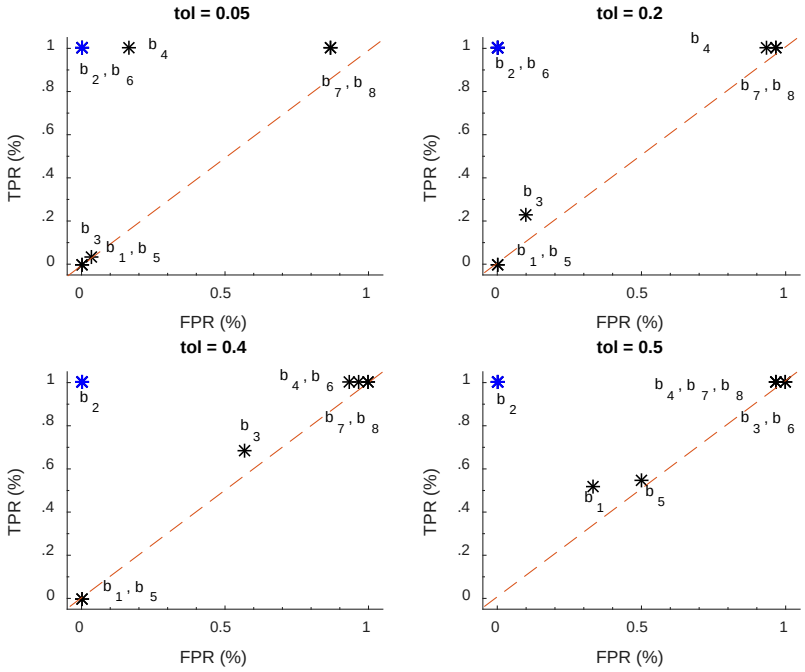


Figure 18. Diagnostic ROC comparisons for tol = 0.05 and p = 20%

Table 9. Pre-Test Classification Probabilities (*tol* = 0.05 and p =0.2)

Threshold	*TPR*	*FPR*	*TNR*	*FNR*	*ACC*
D_t	1	.7667	.2333	0	.8467
O_{dt}	.9917	0	1	.0083	.9933
Z_{dt}	.9750	0	1	.0250	.9800
b_1	0	0	1	1	.2000
b_2	1	0	1	0	1
b_3	.0417	.0333	.9667	.9583	.2267
b_4	1	.1000	.9000	0	.9800
b_5	0	0	1	1	.2000
b_6	1	0	1	0	1
b_7	1	.7667	.2333	0	.8467
b_8	1	.7667	.2333	0	.8467

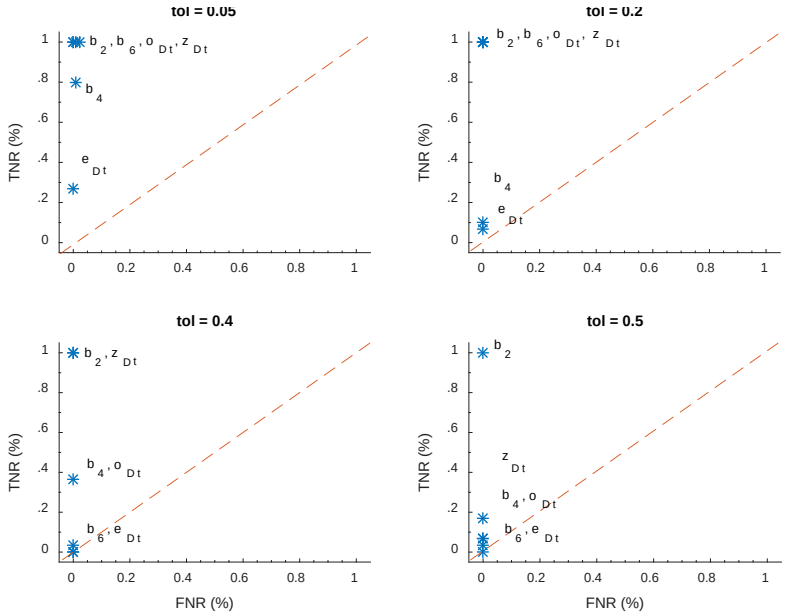


Figure 19. Diagnostic ROC comparisons for tol = [0.5, 0.2, 0.4, 0.5] and p = 20%

- **3.4.3.4 Posterior Classification Probability Results**

The thresholds network treatment when infection of log files is suspected is set to 95% and our 5% errors as shown in Table 4 previously. The findings when the system was set to *tol*=0.05 are found in Table 10. To determine independent classifier usefulness, we consult Table 4's set of threshold values, but may change depending on the user and their objectives. Classifiers D_t, O_{dt}, b_2 and b_6 meet all treatment response threshold requirements. Candidates b_3, b_7 and b_8 suggest random guessing and may indicate a lack of usefulness.

Table 10. Post-Test Probability Estimates (*tol* = 0.05 and p =0.2)

Threshold	*PPV*	*FDR*	*FOR*	*NPV*
D_t	.8392	.1608	0	1
O_{dt}	1	0	.0323	.9677
Z_{dt}	1	0	.0909	.9091
b_1	-	-	-	-
b_2	1	0	0	1
b_3	.5556	.4444	.5556	.4444
b_4	.9091	.0909	.9091	.0909
b_5	-	-	-	-
b_6	1	0	0	1
b_7	.5660	.4340	.5455	.4340
b_8	.5660	.4340	.5455	.4340

- **3.4.3.5 Bayesian Aggregation Results**

Less useful classifiers which may have missed policy acceptance thresholds can be combined using Bayes to improve the predictive estimates and shown in Table 11 using the same four tolerance levels. A Bayesian aggregation of custom classifiers $\{D_t, O_{dt}, Z_{dt}\}$ had perfect classification accuracy up to 0.425 system tolerance levels. In addition, Bayesian aggregation of the independent classifiers $\{b_2, b_4, b_6\}$ achieves perfect posterior estimation. Moreover, candidate b_2 also achieves perfect classification in isolation or when paired with any other qualifying classifier candidate. When Candidates b_4 and b_7 were combined at low tolerances, they achieved an acceptable usefulness rating using thresholds from Table 4 satisfactory 95.1% PPV with 4.9% FDR to meet acceptable treatment threshold requirements. At the same level, the aggregation of b_4 and b_7 saw perfect NPV and FOR posterior accuracy. Unfortunately, as tolerance levels increase, errors increase for b_4 and b_7 aggregation, making this combination of classifier performance useful with the system treatment threshold settings is low. All posterior results, which combine classifiers, are provided in Table 11. As shown, when all custom classifiers are aggregated using Bayes Theorem, the system achieves perfect performance indicating a conclusive result for treatment recommendation consideration. The combination of $[b_3: b_7]$ and $[b_3: b_7: b_8]$ is not useful for the experimental threshold settings of 95%PPV and 5% FDR errors. All combinations of the classifiers shown in Table 11 are useful for indicating infectious log files among.

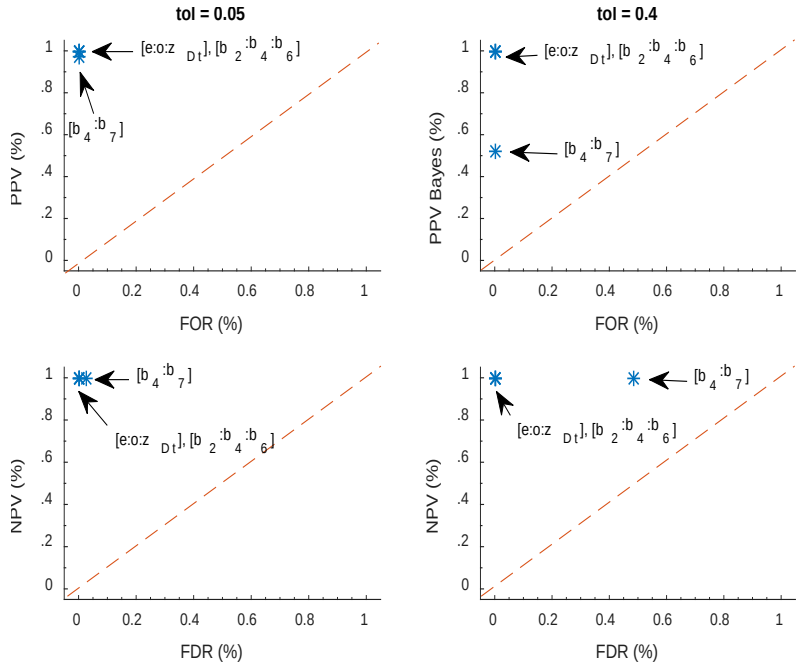


Figure 20. Post Test Diagnostic ROCs for tol = [0.5, 0.5] and p =20%

After gaining more insight into the usefulness of diagnostic aggregation, a more thorough test was conducted to see test the performance of classifier aggregation while varying the threat prevalence rate and tolerance levels from 0 to 1. As shown in Figure 21, the aggregation of RF-Biomarker candidates b_2, b_3 and b_6 achieves the highest intrinsic accuracy and posterior estimation usefulness which meets *network-disease* treatment rules from Table 4. The custom classifier aggregation $[D_t, O_{dt}, Z_{dt}]$, which does not know which independent classifier is statistically best, comes in a close second place, achieving perfect estimation with zero errors until Euclidean distance tolerance levels exceed 42%. Implying that an exhaustive search to identify the single best classifier may not always be necessary for low to moderate tolerance levels. The aggregation of candidates b_4 and b_7 show perfect estimation at low tolerance levels for benign estimations. When tested for NPV performance, the aggregation of b_4: b_7's performance (green dashed) achieves approximately 90% correct estimation at all tested system levels. Such performance indicates a lack of usefulness for b_4: b_7 aggregation combinations.

Table 11. Bayesian Aggregation (*tol* = .05 and p =0.2)

	Posterior Estimates of Multi-factor Diagnostics (%)			
	Benign (1)		***Infectious (0)***	
Diagnostic Combination	***PPV***	***FDR***	***FOR***	***NPV***
$D_t \cap O_{dt}$	1	0	0	1
$D_t \cap Z_{dt}$	1	0	0	1
$O_{dt} \cap Z_{dt}$	1	0	.0004	.9996
$D_t \cap O_{dt} \cap Z_{dt}$	1	0	0	1
b_2, b_4	1	0	0	1
b_2, b_6	1	0	0	1
b_4, b_6	1	0	0	1
b_4, b_7	.9510	.0490	0	1
b_3, b_4	.9490	.0510	.0088	.9912
b_3, b_7	.6198	.3802	0	1
b_3, b_7, b_8	.6802	.3198	0	1
b_2, b_4, b_6	1	0	0	1

- **3.4.3.6 Final RF-Biomarker Selection**

3.4.3.6.1 Top Three Independent Diagnostic Performers

The top three discrimination candidates are selected as RF-Biomarkers of *network-disease*. Their independent or aggregated pre-test classification performances of the top performers are combined using Bayesian methods to improve the posterior classification probabilities. In order, the top performers are b_2, b_4 and b_6.

3.4.3.6.2 Poor Performers

Candidate b_1's performance may be improved by modifying the RF-measurement selection. Here the highest value that appears for the specified ROI time was used. As a consequence, the distribution appears as bimodal distribution.

A consideration of the high and low amplitude values separately, may increase classifier performance and overall similarity scores. Candidates b_6 and b_7's poor performance is attributed again as derivatives of additional statistics that come from the amplitude measurement. These discoveries were not validated during this research.

3.4.3.6.3 Top performers using Bayesian Aggregation

All combinations of the custom $[D_t, O_{dt}, Z_{dt}]$ diagnostic classifiers achieved acceptable performance level for posterior estimation of benign vs. infectious RF-Events. The method of classifier development mitigates the need to conduct exhaustive research which identifies the exact top discriminator and still achieves acceptable performance up to tolerance levels of 42% or more in this experiment. A modification of the default values of Z_{dt} from 2.125 up to 2.5 allows the aggregation to achieve performance levels that match the final RF-Biomarker aggregation combination. Such a modification only increased the overall risk of acceptance by a marginal amount.

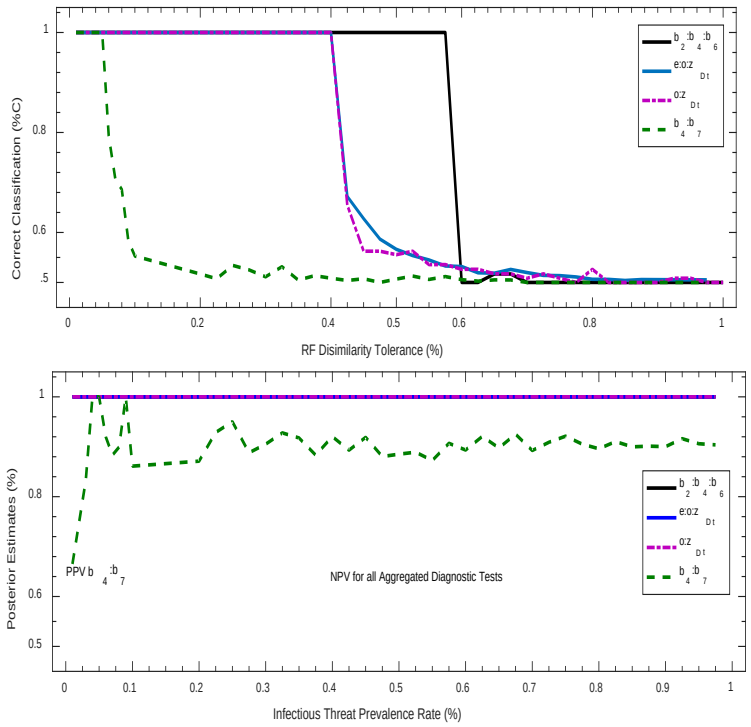


Figure 21. Bayesian Aggregation %C vs. tol = [0:1] p = 0.2, n =150.

The aggregation of b_2: b_4: b_6 was not straight forward. Initially, it appeared that b_2: b_3: b_6 would perform the best however this was only observed at low tolerance acceptance levels. Insight into how the system may behave over a wider tolerance range suggests initial candidate recommendations using statistical evidence for a low system tolerance level result does not hold for higher tolerance levels. This implies that the signal to noise ratio level may significantly affect the diagnostic accuracy at higher noise levels. In addition, the final performance using all three RF-Biomarkers can be reduced to two if policy is acceptable.

3.5 Conclusions

The proposed framework of integrating RF-DNA into electronic RF network authentication schemes to enhance logical credential verification improves posterior prediction usefulness of *benign* vs. *infectious* (imposter) with 100% accuracy in low to medium noise tolerance. Using a majority vote and risk-based diagnostic, an infectious credential detection accuracy of 96.7% and 90.1% improved to 100% when Bayes Theorem is employed. The proposed method does not degrade the performance of existing logical-only authentication schemes and can be used in an "ON/OFF" mode of operation to support multiple missions.

The proof of concept to improve CubeSat uplink authentication was demonstrated using a *first of kind* physical simplex RF communications network using software defined radios (SDRs). Such radios are capable of mimicking standardized and interoperable (logically equivalent bit-level communication) wireless transmissions.

The experimental network was validated to successfully receive, demodulate and decode an intended message transmission originating from a trusted device. After learning a policy specified RF-DNA credential from a trusted origin, the configured authentication device achieved 100% 1-to-1 verification when logical and physical credentials pairs were considered.

An empirical observance of RF-DNA splitting among log file traces was found to indicate a significant difference between a trusted RF-DNA benchmark and a simple random selection from a log file size of 200 received RF-Events. Such significance is described here as *rf-splitting* of an RF-Event's main characteristic (i.e. amplitude, frequency or phase). Diagnostic screening of vulnerable CubeSat receivers would benefit from a log file screening treatment to indicate early warning signs of infectious access attempts originating from unauthorized origins which may lead to electronic network disease. Key players such as Cyber Operators, defenders, administrators, IMDs users and policy makers should seriously consider the cost and benefits of incorporating RF measurements-based diagnostic testing to indicate early warning signs of *eND*.

IV. Interactive Trust Algorithm Extensions of Multi-Factor Authentication Schemes

Forgiveness is relatively easy… its trusting again that is hard. (unknown)

4.1 Overview

A conventional interactive trust algorithm for miniature CubeSat networks employ a binary decision-rule for classifying ground-station uplink transactions as either cooperative or defective states using logical (digital bits) authentication mechanisms. However, in an uncertain environment where digital impersonations are prevalent among standardized and interoperable electronic devices, such an algorithm lacks the capability to express the pathology of received RF transmissions as originating from an *insider* or *outsider* source. In this article, RF-DNA is integrated as a physical attributes based trust mechanism to improve logical-only network authentication schemes. A consideration of physical RF evidence provides expressive insights into the origin integrity of unauthorized RF transmission sources. The proposed enhanced scheme is validated using a con-man abuse case and is shown to significantly reduce Type-I misclassification errors from 84.11% to 0% when RF-DNA benchmarks are considered during system state classifications. The extensions improve upon previously undistinguishable 2-state system by accurately classifying insider vs outsider threats using posterior estimates of RF-DNA credential diagnostics. Moreover, when tracking insider threat behavior, the recommended response more appropriately extends uplink availability by 51.2% for non-offending transmission entities that share uplink resources.

4.2 Introduction

Interoperability and standardization of *electrically identical* [68] network devices continue to play a significant role in maximizing communications across disparate radio frequency (RF) network boundaries. However, collaboration and resource sharing demands (e.g. CubeSat networks) among multiple organizations correlates to increases in unauthorized RF access requests, which threatens the health and security of vulnerable networks [69]. An interoperable software-defined radio (SDR) can mimic a standardized RF device's logical message transmissions, creating physical origin integrity uncertainty for claimed access credentials. Specifically, the physical layer of the Open Systems Interoperability (OSI) model has an inherent vulnerability to *outsider* threats, which eavesdrop, intercept, clone or otherwise conduct logical (binary) attacks using physical RF transmission forgeries to gain or deny access to network resources. Similarly, an *insider* threat vulnerability such as a *con-man* poses a significant risk of going imposter, causing abnormal network behavior. Such vulnerabilities render a specified authentication device as either lacking an intrusion detection and prevention capability or is unintentionally trained (configured) to ignore physical subtleties of statistically distinct RF origin cues [36]. The diagnostic pathology of RF transmission events (RF-Event) may indicate 'early warning' of *infectious* (dissimilar RF-Event) vs. *benign* (similar RF-Event) *RF* credential origins. Failure to consider the pathology of RF-Event transmissions, during authentication, may lead to undesirable network behavior termed *network-disease* (e.g. distributed denial of service (DDoS) or loss of uplink availability). A multi-factor authentication framework (Figure 22) depicts a pairing of logical and physical RF credential information. The steps of the framework include policy specification, feature selection, benchmark template development, gold standard validation and appropriate policy response.

Conventionally, Factor-1 (logical), utilizes traditional network credentials such a User, Device and Command ID fields. Comparisons of new vs. known logical credentials provide a binary result. This approach works well when manufactured device ID fields are distinct among all network devices and access control measures to software modification are in accordance with FCC rules for modifications [68]. Along the bottom of Figure 22, Factor-2 (physical) augments authentication accuracy when logical credentials test positive for a match. Let the set $\{u_1u_2, \ldots u_i, d_1, d_2, \ldots d_i, c_1, c_2, \ldots c_i\}$ respectively represent the authorized bit-level encodings for a claimed USER, DEVICE and COMMAND identification fields as depicted in the truth table of network credential templates using factor-1. The logical credentials indicated on the top (factor-1) of Figure 22 are identified as conventional bit-level identification fields of a transmitted message using some standardized transmission protocol. Along the bottom, physical authentication using factor-2, of authorized message transmissions are indicated using a set of pathological credential templates $\{w_{s1}, w_{s2}, \ldots w_{si}, F_{ws2}, \ldots F_{ws_i}\}$ which represent statistical RF fingerprints of the demodulated bit-level credential fields which resulted from original observances of authorized w_s transmissions. Here, w_s contains the physical RF modulations of bit-level credential region of interest fields $\{u_i, d_i, c_i, \ldots ID_j\}$.

The logical and physical credential templates are locally stored within Rx_C's memory to enable self-evident verification for future multi-factor authentication. As future instances of waveform w_s occur for authentication by Rx_C, two factors are considered for authentication. Using Factor-1, w_s is demodulated for bit-level credential interpretation, but held temporarily until the results of Factor-2 can be determined. Using Factor-2, w_s is sampled according to parameters indicated by the iMkr (start and stop sampling points for RF fingerprinting) for a times-series RF transmission event.

An index parameter determines the sampling start and stop points of a waveform's region of interest (ROI) indicated as the $iMkr$ of w_s. The index dictates the start and stop points of an event, which compares an RF-Event's newly extracted RF fingerprint to a trusted *RF benchmark template*. Each destination device may contain different credentials according to policy p_i. If a statistical fingerprint of an RF-Event matches a claimed benchmark template, the signal is allowed to pass forward to the next checkpoint for higher layer authentication processing if necessary. Table 18 describes multi-factor (factor-1 and factor-2) classification for policy response.

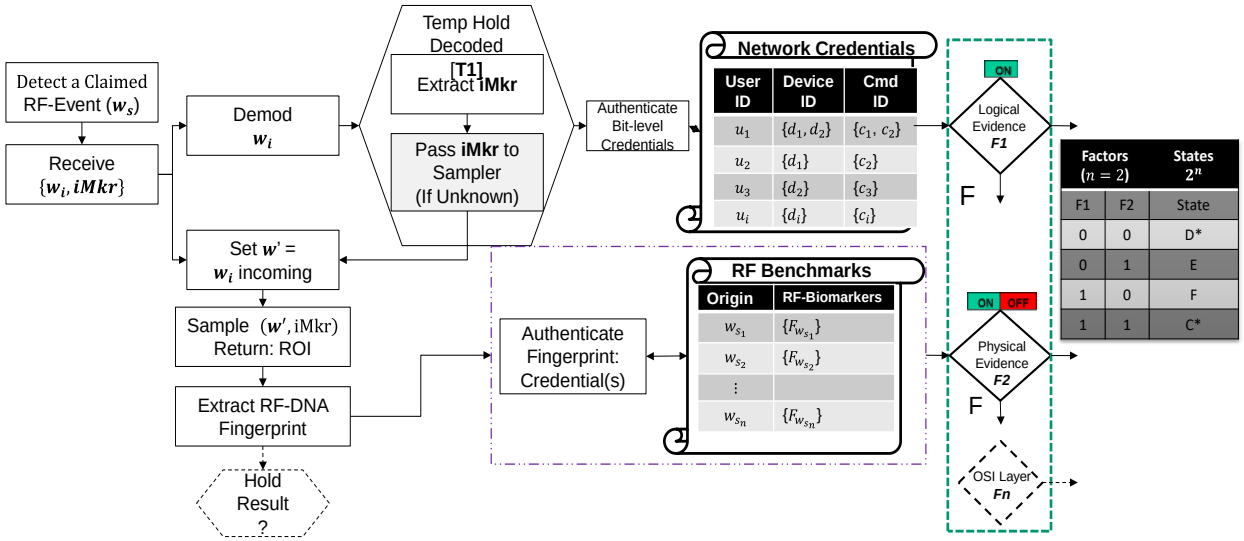


Figure 22. Multi-factor verification using logical and pathological credential pairs

This research aims to assess the impact of a 4-State classification system extension using RF fingerprinting has on the performance of a 2-State system when RF fingerprinting is off. A Bayesian aggregation of pathological RF-Biomarkers and logical evidence pairings aim to improve the posterior classification of credential validation using a distributed consolidated trust managed system (CTMS) [1].

The CTMS manages the trustworthiness of uplink access requests originating from fixed ground stations [21] using logical authentication of a specified RF source identification ID_x credential field (i.e. AuthCount). A representative CubeSat satellite communication (SATCOM) network simulation, considers like-manufacturer and like-model SDRs, employs an interactive trust value (ITV) field mechanism to assess the dynamic reputation trust and authenticity of a claimed credential. Previous work using RF-DNA fingerprints [16] [18] [51] [52] extends RF fingerprinting of invariant protocol message fields (e.g. preamble, postamble, midamble) to include an entire fixed or invariant command message. Such an extension provides a feasible way to consider physical RF-Event information during authentication when logical-only authentication is uncertain. Dimensionality reduction improves the selection of 'useful features' using sensitivity analysis [50] [70].

4.2.1 Background & Related Works

A. Trust

In social or electronic communities, *trust* is a rating assigned by a perceiving (receiver) agent indicated by $'d'$ with respect to a transmitting source agent indicated by $'s'$ for a specified time $'t'$ [71]. An RF pathology authenticator (device d) is defined as having physical RF origin credential templates of statistically trusted RF-Events emplaced in local memory which enables *self-evident* origin verification as suggested in Rasmussen's work [25]. A policy p_i describes the desirable information flow from s to d over a communication link's path. Link l forms a point-to-point (P2P) path from s to d as $(s \rightarrow d)$ if a pairing response exists which specifies the directional communication path's designated receiver for credential verification by authenticator/*observer* d.

The term *con-man* is adapted from [72] to indicate an abuse case profile when s_a takes advantage of d during a series of electronic interactions. Such a case is best described as an *insider-threat* situation when an authorized communication path exists between s and d. During such transactions the *con-man* presents acceptable credentials that are contained within standardized RF modulations of message $'m'$ that lead to a classification of *Cooperation* $'C'$ between s_a and d. Such cooperation may lead to the execution of *infectious* payload data contained within the body of m transmitted by s_a. Then, when it comes to a high –risk interaction, the *con-man* (s_a) will defect. That is, s_a initiates a malicious (e.g. Trojan-horse) transaction that attempts to defraud d. The trust rating about the reputation of s_a updates by d following fraud detection and a transactional state classification of *Defection* $'D'$ occurs. At this point, the *con-man* either attempts to regain lost trust or stop future communication with d. Conventionally, there are 'θ' consecutive C transactions for each D. The con-resistant interaction trust algorithm is provided in Table 12 [73]. To regain trust, s will again initiate several transactions that are C in nature. Here, s hopes to deceive d again by masking its true *infectious* intentions by presenting logically correct message credentials while inserting some unauthorized payload. Several well-known *con-man* attack patterns are recreated in a simulated ecosystem using attack profiles of θ = 5, 10, 15, 20, 25, 30, 35 and 40.

Table 12. Con-Resistant Interaction Trust Algorithm [72]

Cooperation		***Defection***		
$T'_{sd} = T_{sd} + \alpha(1 - T_{sd})$	(1)	$T'_{sd} = \frac{T_{sd} + \beta}{1 - \min(\lvert T_{sd}\rvert, \lvert\beta\rvert)}$	(6)	$T_{sd} > 0$
$T'_{sd} = \frac{T_{sd} + \alpha}{1 - \min(\lvert T_{sd}\rvert, \lvert\alpha\rvert)}$	(2)	$T'_{sd} = T_{sd} + \beta(1 - T_{sd})$	(7)	$T_{sd} < 0$
$T'_{sd} = \alpha$	(3)	$\beta = (\beta - \gamma_d(1 + \beta))$	(8)	$T_{sd} = 0$
$\alpha = \min(\alpha + \gamma_c(\alpha_0 - \alpha), \alpha_0)$	(4)	$\gamma_d = {}^1/_e * \lvert T_{sd}\rvert = \frac{\lvert T_{sd}\rvert}{e}$	(9)	
$\gamma_c = 1 - \lvert\beta\rvert$	(5)	$\alpha = 1 - \lvert\beta\rvert$	(10)	

In such profiles, the con-man will conduct a series of θ transactions that would be classified as C and then immediately initiate a transaction defection classification. A rating of '0' indicates the absence of trust. Initial trust ratings begin at '0' with adjustments occurring throughout directed session interactions from s to d [71]. As link session interactions occur, trust ratings are strengthened or weakened for the next (t +1) transaction period and is based on the perspective of authenticator d. An authenticator (device d) is defined as having physical RF attribute benchmarks of statistically trusted RF-Events that are emplaced in its local memory to enable *self-evident* RF origin integrity as suggested by Rasmussen [25]. Previous research suggests, such a con-man attack may continue indefinitely without detection if θ is sufficiently high [74].

B. A Basis for Collection of Trusted RF-Event Transmission States (w_s)

- **Policy Specification**

A summary of general acceptance policies appears in Table 13. An oracle of acceptance for naturally occurring RF emission similarity development maps the combination of useful logical and physical credentials for RF communication (e.g. e-CFR identification field). Oracle specifications include acceptable RF-measurements, receiver configuration, RF transmission similarity tolerances, fixed vs. mobile stations and acceptable noise. The first property implies an existence of natural RF analog subtleties that exist as distinct electronic device transmissions [3] [4]. The sources of fixed and authorized transmitters influence an RF fingerprint and must remain distinct from all other (e.g. mobile) sources during natural RF generation to satisfy *Property-1*. Secondly, the physical attributes of original (benchmark templates) RF-Events must be inherent among all similar interoperable devices (e.g. emissions made in the ultra-high frequency range) [29] [75].

Thirdly, new RF-Events must be repeatable to enable consistent RF-measurements. *Property-4* suggests statistically significant RF dissimilarity is indicates a risk of infectious credential acceptance. A *self-evident* marker inherently describes the existence of the RF-Event's similarity level without a need for additional interpretation. Receiver *d* owns *self-evident* markers of specified credential of *s* when all properties of Table 13 occur. There is currently no standardized method toward feature selection in an RF networking ecosystem. The aim of policy development is to provide early warning cues of *network-disease*.

- **Feature Selection**

The use of minutia detail classification employs classification across composite features and may suffer from poor detail selection when new samples are compared to database templates [54] [55]. In biometrics, there are an estimated 150 standardized indicators called minutia detail used in human fingerprinting [9] techniques but none in electronic RF fingerprinting. A *Biomarker* is defined as "a characteristic that is objectively measured and evaluated as an indicator of normal biological processes, pathogenic processes, or pharmacologic response to therapeutic intervention" [40] [41]. An *RF-Biomarker* is a physical or intrinsic characteristic of an electronic communication device's RF emissions that indicates abnormal process or response when the origin integrity of RF transmissions are suspect for causing *network-disease*. The introduction of local RF-Biomarker measurement and analysis aims to augment diagnostic utilities employed by network troubleshooters to defend against abnormal behavior [76].

Table 13. Desirable Properties of Unique RF Features

Desired	Description
Property-0:	An Oracle or policy of RF evidence acceptance has been pre-defined as truth. Defining a specific authentication device's measurement of RF fingerprint can be used as a **truth reference**.
Property-1:	An original RF-Event must be **natural** (i.e. analog or continuous) in its immediate existence in time and space rather than existing as a derived logical (e.g. binary or digital) interpretation.
Property-2:	Specified feature attributes of the physical event must be **inherent** among similar RF emission (e.g. Type III frequencygenerating transmitters [77].
Property-3:	The extractable features of RF generating circuits must be repeatable and **evident** from the occurrence of the natural event stimuli**.**
Property-4:	A sample obtained from the RF-Event must provide evidence that its features are **statistically significant** to support known and consistent event measurements.

- **Benchmark Development**

A *benchmark* test applies reference truth dataset for quantitative performance measurement commonly referred, in the medical community, as a *gold standard (GS)* [58] [39]. A gold standard is a source of information, which tells us the statistically true condition status of a received RF-Event transmission using a diagnostic result [42]. The strength of a benchmark is a measure of self-similarity, where high similarity indicates an RF signature that is statistically consistent between samples.

- **Gold Standard Validation (Verification)**

Fingerprint verification for people is very similar in concept for electronic devices and integration of various modalities provides automatic authentication and verification [9]. A Bayesian-based RF-DNA fingerprint filter is inspired from spam filters [32] [45] and applies as a 1-to-1 credential verification scheme, which compares newly claimed RF-Events to a known benchmark or gold standard [39] for verification.

- **Treatment Response**

An optimal system configuration considers the policy and goals of the end-user entity as well as trade-offs. This article demonstrates a proof of concept and leaves optimization for future research. However, some recommendations provide system tuning in Section IV for general operational risk ecosystem consideration.

C. **A Representative SATCOM Network**

Duncan employs a 'One-Factor, Two-state' classification scheme according to d's assessment of a claimed credential's transactional classification and the current ITV level using logical-only authentication mechanisms. An ITV rating about s, from the perspective of d is closed over the interval [-1, 1] where a rating of '-1' indicates a complete distrust of s while a rating of '+1' indicates complete trust in transactions originating from s. An initial rating of '0' indicates the absence of trust [71]. In an abuse case, the *con-man* conducts a series of transaction classifications of *cooperation* $'C'$ or *defection* $'D'$ by authenticator d. Based on the value of the ITV during a session, Duncan employed a three level policy response scheme where he arbitrarily selected a policy-based threshold limit of -0.5 as the lowest acceptable ITV rating that could occur during a series of 200 transactions.

A Level-1 response is referred to as "Trust Management Event Logging Only," where the response actions of the authenticating device includes a comparison check of the command authentication count upon receipt of a new RF-Event and the associated ITV is calculated for the authentication count marker. Once the ITV for authentication count reaches the decision-rule's distrust threshold, an alert is logged indicating excessive invalid attempts. A Level-2 response, termed "Trust Management Event Logging and Prevention," includes the responses of a Level-1. However, once the ITV for authentication count reaches Th command processing halts for anonymous users and an alert is logged indicating excessive invalid command attempts. A Level-3 policy response, "Trust Management Event Logging, Prevention and Recovery," include responses of Level-1 and Level-2. Additionally, A Level-3 response halts command processing for anonymous users and an alert is logged indicating excessive invalid command attempts.

A legitimate ground station must unlock satellite command processing originating from uplink transmissions using the CTMS's onboard logical credential trust mechanism to authenticate the unlock sequence and resume commanding operations.

D. Discovering Evidence of Distrustful RF Transmission Behavior

A strategy for *con-man* attack, denoted as SCA(Θ), remains trustworthy by choosing Θ to be strictly greater than the interactions that precede the attack despite being a *con-man* [72]. The *con-man* repeats the attack pattern after a series of Θ favorable session interactions. Yu and Singh introduced a simple trust algorithm extension to mitigate *con-man* behavior [2], providing a simple binary result per transaction. To assist in mitigating this problem, [72] extends the Con-Resistant Trust Model where known patterns of *con-man* behavior exist. In the scheme, s interacts with d in a favorable number of session iterations before committing a D interaction. Unfortunately, both extension schemes discard critical information (physical RF-measurements), about the physical attributes of fixed transmitters, instead logical-only (demodulated and decoded bits) credential verification is employed.

The proposed scheme enhancements aims to provide more expressive feedback to network tasked with defending against insider and outsider threats that are capable of mimicking logical credentials at the bit-level. In order to meet this objective, the article aims to enhance existing network authentication mechanisms employed by the CTMS using multiple pathological or physical event based mechanisms (i.e. localized components of composite RF-DNA fingerprints) to enhance network defense in Cyberspace [1] [19] [24] [20]. Similar to reputation theory as described by Sabater and Sierra in [74], an agent that has a specified relationship with another agent is more likely to forgive even after being deceived [72]. Forgiveness bounds the limits of a penalty β by some experimentally determined upper and lower bound.

We refer to this term as the fingerprint forgiveness factor indicated by (Φ) and is closed over the interval $[\beta, 1]$. The electromagnetic interference effects that RF-Biomarkers experience during uplink propagation in a SATCOM ecosystem may be negligible for UHF transmissions using FM modulated signals [15].

4.3 Methodology: 2-Factor RF Credential Authentication

- **Experimental Setup (Hardware Software)**

The representative experimental CubeSat uplink configuration is depicted in Figure 23 as the wired and wireless point-to-point (P2P) communications network. Each circuit component is labeled with a letter and role for representative icon reference. For example, the device used to generate the initial message for collections is shown as (label | description) PC1| PC1: msg (message) generator. Each HP Zbook 15 laptop in Figure 23a/b/c $(Tx_A), (Tx_B)$, Figure 23f/g (Rx_C) have 32GB RAM, 500GB DDRL 4DM, 5400 RPM, integrated NIC, I Core i7-4800MQ processor and are identically configured with LabVIEW 2014 with RT Modulation Tool Kit, Math Script, Windows 10, Microsoft Office 2013, Matlab 2015a, 2016a and Jump Pro 12.1. Each physical circuit has physically distinct hardware, cables and antennae and could transmit or receive. The ground station front end transmitters are represented by Tx_A and Tx_B while the CubeSat receiver is represented by Rx_C. The RF radios are randomly selected from National Instrument model USRP-2922 software defined radios (SDRs) that differ by serial number only.

Figure 23a and Figure 23b represent that baseband logical message generator (*msg*), which transmits telecommands to the front end transmitter Tx_A in Figure 23c (USRP 2922) for final modulation onto the uplink medium. Devices Tx_A and Tx_B (red USRP 2922 in Figure 23c) are the transmitters under test. GS1 is defined as the benchmark validation test for Tx_A emissions as observed by receiver (authenticator) Rx_C.

Tx_A's RF emissions are collected for signature profile benchmarking by Rx_C based on predefined policy specifications. Tx_B (red) represents an arbitrary opponent transmitter that attempts to impersonate the credentials of Tx_A. The goal of Rx_C is to provide decision-support for the origin integrity of arriving telecommands that claim to originate from Tx_A. Upon receipt of new RF transmissions, Rx_C, compares the logical and pathological (RF-DNA) credentials to known benchmarks previously known about Tx_A. When both credentials meet arbitrary threshold requirements for acceptability as shown in Figure 23h, the paired RF-Event's credentials are classified as *benign* for causing *eND*. When either credential fails to meet acceptability thresholds, the RF-Event is classified as *infectious* for causing *eND*.

A 2-FSK modulation scheme is used to transmit *msg* over FM using a carrier frequency of 449.9MHz. A 100kHz offset is set from the center frequency of 450MHz. Each pulse duration is approximately 6.399ms. The receive circuit had a tunable bandwidth selector that was set to 20kHz and detected each pulse using a tunable triggering mechanism based on the magnitude of the amplitude. The FSK deviation was set to 1.

- **Experimental Focus**
  Classifier Rx_C trains on 1100 trusted RF-Events from Tx_A while transmitting an authorized command (message-1) to compose a trusted RF-DNA fingerprint *benchmark* template. For each RF-Event pulse (Figure 23d) successfully received by Rx_C (Figure 23g), the RF-DNA is extracted from 10 fixed and equally spaced sub regions plus the full wave regions using complex real and imaginary parts of the analog waveform. This brings the total number of distinct RF-DNA contained within a complete collection to ([8 features] * [22 sub-regions]) 176 RF distinct native attributes for possible selection as RF-Biomarkers of *eND*.

The same RF-DNA fingerprint classifier was then tested using 150 new claimed RF-Events for Tx_A while transmitting from the same authorized state for benchmark verification. The process repeats for three additional commands for Tx_A to provide a total of four benchmarks and four test sets for verification. This procedure repeats for Tx_B. Tx_A is the trusted source, while Tx_B arbitrarily assigned as untrusted. The authorized messages from Tx_A is arbitrarily designated as *Benign*, when USER-1 transmits from Tx_A. We designate all commands from Tx_B and 'command-2' from Tx_A as *Infectious*. Additionally, policy $'p_i'$ specifies Tx_A as having 'command-1' authorization only.

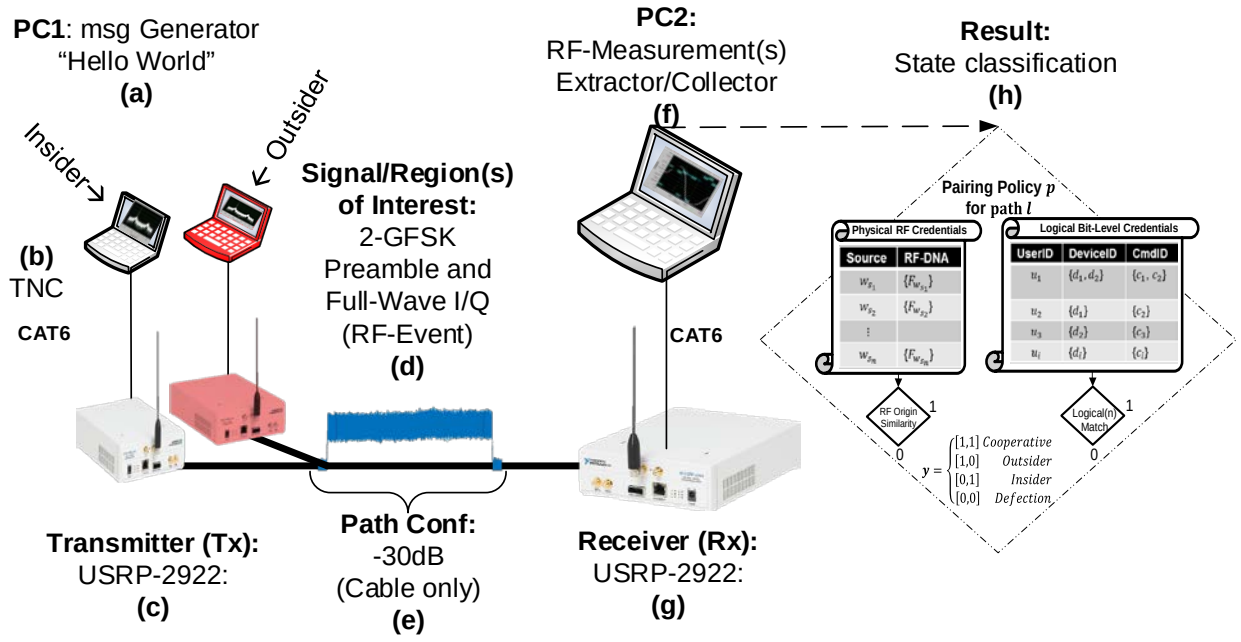


Figure 23. Physical network diagram for Experimentation

- **Abuse Case Description**

In the abuse case experiment, a Bayesian RF-DNA verification filter classifies a new set of 43 benign and 107 infectious (not-benign) RF-Event samples from two physically distinct SDRs. To establish a common reference for test validation, all transmitted RF-Events are logically identical (i.e. the logical/binary decoded bit streams are the same).

A simple random selection of infectious and benign RF-Events replaces defective (*infectious*) transactions '0' using a well-known con-man attack profile $SCA(5)$. A comparison of the final dataset reference and known benchmark levels provides the resulting classification match scores. Initialization settings appear in Table 14. An abuse case adaptation from Duncan sets the first 49 transactions of a truth reference dataset as legitimate command transmissions with 10% bit errors. In the truth, the original "all-benign" dataset receives a simple random sample replacement of the 10% error occurrences as Tx_A 'command-2' transmissions to simulate noise (i.e. bit errors instead of manmade). The indexed replacements were; [5;11;18;22;26;37]. The index replacement's truth column updates to truth condition code = 2. Next, for transactions 50 -150, a simple random sample of RF-Events are selected from Tx_B's pool of 'command-1' and 'command-2' RF-Event samples. Both simple random samples are then arranged to satisfy the abuse case sequence used in Duncan's research, where the first 49 transactions are considered as all *Cooperative* in nature in a 10% BER ecosystem. The count of each command is found in Table 15. The attack occurs at transaction 50 and continues until the end of the sequence of samples. RF-Events for command-1 from Tx_B are as follows;

[52;55;56;59;60;61;66;67;70;72;73;76;78;80;82;83;84;85;87;90;92;94;100;101;102;104;110;115;116;118;119;124;125;126;128;130;131;132;133;134;135;137;139;140;141;142;143;145;147;148;149].

Moreover, Tx_{B_1} replacements are enumerated in the temp truth reference column as number '0'. Tx_{B_2} 'command-2' files are also simple random selections from a population of 500 samples. The gold standard (GS) file index values for these commands are;

[50;51;53;54;57;58;62;63;64;65;68;69;71;74;75;77;79;81;86;88;89;91;93;95;96;97;98;99;103;105;106;107;108;109;111;112;113;114;117;120;121;122;123;127;129;136;138;144;146;150.

Finally, the GS file's truth column was created such that all RF command transmissions originating from Tx_A 'command-1' retained the value of '1' to indicate a true *benign* status, while all other commands were given a value of '0' to indicate the truth status as *infectious*. The con-attack SCA(5) began at transaction 50 and continued until the end of the series of transactions. This sequence represents the final gold standard or truth reference of infectious vs. benign classifications.

Table 14. System Parameter Settings

System Parameter Settings		
	"ON"	**"OFF**
$\boldsymbol{\alpha_{start}}$=	0.1	0.1
$\boldsymbol{\alpha}$ =	α	α
$\boldsymbol{Bonus}$ =	$Bonus = (Bonus + \alpha_{start})$	-
$\boldsymbol{\beta_{start}}$ =	-0.4	-0.4
$\boldsymbol{\beta_{MED}}$ =	$[1.0, 1.25, 1.5, 1, .\mathbf{75}, 2]$	-
$\boldsymbol{\beta_{MAX}}$ =	$[2, \mathbf{2.25}, 2.5, 2.75, 3]$	-
$\boldsymbol{\beta}$ =	β	β
$\boldsymbol{\Phi}$ =	$[1.0, 0.75, \Phi_{HI}, \Phi_{LO}, 25,]$	-
$\boldsymbol{\Phi_{LO}}$ =	0.9451	-
$\boldsymbol{\Phi_{HI}}$ =	0.97	-
$\mathbf{D_t}$ =	0.05	-
$\mathbf{O_{dt}}$ =	5	-
$\mathbf{Z_{dt}}$ =	2.125	-

Table 15. True Status of RF Credentials

RF Origin (Device / Command)	**Logical Credential Similarity [Y/N]**		**Pathological Credential Similarity [Y/N]**	
	[L=1]	**[L=0]**	**[P=1]**	**[P=0]**
A^d, c_1	43	0	43	0
A^d, c_2	0	6	0	6
B^d, c_1	51	0	0	51
B^d, c_2	0	50	0	50
Totals	94	56	43	107

- **Factor-1 Logical (L) Credential Authentication Mechanism**

The monitoring of a simple authentication counter (AuthCount) field is the logical credential benchmark.

- **Factor-2 Physical (P) Credential Authentication Mechanism**
  Using a physical attribute-based mechanism Rx_C compares the physical variations that naturally exist in RF emissions of a telecommand messages. Additionally, the trusted sets of w_s events satisfy all properties of Table 13. We propose a physical enhancement to logical security mechanisms that extends previous work in the SATCOM operational ecosystem [14] [1] for LCP based authentication [76].

- **Policy Response Decision Rules**
  For consistency, Duncan's $Level - 3$ policy response scheme in the CTMS is adopted [72] [1] where the trust threshold is$[Th = -0.5]$. Con-man attack profile SCA(20) analysis provides additional details on the con-resistant algorithm extensions.

- **Verification Metrics**
  In the 2-state interactive classification scheme, RF fingerprinting augmentation is "OFF" and an interactive transaction classification test result of $Class - C$ occurs when a claimed RF-Event's decoded logical credential field matches the benchmark logical bit-pattern when compared. When the decoded credential field fails to match the benchmark identification bit-pattern, a classification of $Class - D$ occurs. In the 4-State system when RF fingerprinting is "ON", the logical and physical credential information is considered in state classification. As uplink transactions occur, a classification $Class - C$ occurs when both diagnostic results test positive. That is, the credential's decided bit-pattern matches the template and the physical RF-measurements extracted from the RF-Event that contained the modulated message also meets origin similarity acceptance levels. Here, a system state classification of $Class - C$ is equivalent to a benign indication of a *network-disease* causing transaction. A system state classification $Class - D$ occurs when a received RF-Event tests negative for both logical and physical RF credential acceptance, which indicates the highest risk of credential forgery.

A system state classification $Class - E$ occurs when a received RF-Event tests positive for logical credential authenticity, but tests negative for possessing acceptable RF origin similarity levels, an indicator of outsider (foreign device) threat attempts. A system state classification $Class - F$ occurs when a received RF-Event tests negative for logical credential authenticity, but tests positive for possessing physical RF credentials, which suggest high RF origin similarity. $Class - F$ indicates an insider threat or perhaps an SDR that mimics the physical and logical characteristics of a trusted transmitter. When neither of the diagnosed credentials match, the interaction state classification is $Class - D$ and is functionally the same as a 2-State classification system [71].

Using the 2-State classification system, we can assess the diagnostic accuracy of credential verification accuracy. The true positive classification occurs when $[L = 1 \,\&\, D = 1]$. A TN occurs when $[L = 0 \,\&\, D = 0]$. That is, when a claimed RF-Event's credentials do not match a diagnostic template and the true condition of the RF-Event is *infectious*. A misclassification error occurs when the logical diagnostic test and true condition status are not the same. A false positive occurs when $[L = 1 \,\&\, D = 0]$. A false negative occurs when $[L = 0 \,\&\, D = 1]$. Lower errors are better. Diagnostic accuracy for the 4-State system is similar. A $TP = benign$ classification occurs when $[L = 1 \,\&\, P = 1]$ and $[D = 1]$. A $TN = infectious$ classification occurs when $[L = 0 \,\&\, P = 0]$ and $[D = 0]$. A FP error occurs when $[L = 1 \,\&P = 1 \,\&D = 0]$. A FN occurs when $[L = 0 \,\&\, P = 0] \,\&\, [D = 1]$. When classifying the system state, a state interaction classification of E occurs when $[L = 1 \,\&\, P = 0]$ despite the true condition of the RF-Event. A state class F occurs when $[L = 0 \,\&\, P = 1]$ regardless of the true RF-Event's credential status.

The state interaction classifications are used in conjunction with the ITV during network monitoring and response activities. For each system state classification, the con-resistant algorithm and the new extensions are applied to update the ITV.

- **Extensions to Con-Resistant Algorithm**

Adapting the characteristics of conventional con-resistant trust models, "trust is hard to earn but easy to lose" [72] [74], we extend the con-resistant algorithm by introducing a state classification-based update schema. The extensions provide state specific considerations to deal with regaining trust or penalty severity for distrust. A *forgiveness* factor Φ extension reduces the penalty (β) for a perceived $Class - F$ interaction classification based on agent $\boldsymbol{d}$'s trust of the received RF-Event's logical and physical credential testing.

A $Class - F$ state, assumes a higher risk of *network-disease* if the RF-Event is accepted as authentic. Similarly, the reward increment size of α can also be modified to support targeted classes that best support operational objectives.

Table 16. Con-resistant interaction trust algorithm State Extensions

Two	***Cooperation (C)***		***Defection (D)***	
Four	C*	E	F	D*
Extensions	$\boldsymbol{a} = \boldsymbol{a} * (\boldsymbol{Bonus})$ $\boldsymbol{\alpha} = \boldsymbol{min}(\boldsymbol{\alpha} + \boldsymbol{\gamma_c}(\boldsymbol{\alpha_0} - \boldsymbol{\alpha}), \boldsymbol{\alpha_0})$ (4) $\boldsymbol{\beta} = \boldsymbol{\beta}$	$\Phi = \beta_{MED}$ $\beta = \beta_{start} * \Phi$ $\alpha = 1 - \lvert\beta\rvert$ (10)	$\Phi = \Phi_{[HI,LO]}$ $\beta = (\beta - \gamma_d(1+\beta))\Phi$ $\alpha = 1 - \lvert\beta\rvert$ (10)	$\Phi = \beta_{MAX}$ $\beta = \beta_{start} * \Phi$ $\alpha = 1 - \lvert\beta\rvert$ (10)

Integrating RF fingerprinting augmentation mechanisms for forgiveness into (8) above from Table 12, the discounted penalty for potential con-man behavior is,

$$\beta = (\beta - \gamma_d(1+\beta))\Phi\,, \tag{11}$$

If d forgives distrustful behavior and maintains an otherwise higher ITV. Similarly, Φ modifications for forgiveness for each penalty state as follows

$$\Phi = \begin{cases} \beta_{MAX} & if\ Class\ D\ [L = 0, P = 0] \\ \beta_{MED} & if\ Class\ E\ [L = 1, P = 0] \\ \Phi_{HI}|_{LO} & if\ Class\ F\ [L = 0, P = 1] \end{cases}, \quad (12)$$

Where β_{MAX} represents the largest penalty for distrustful transactions that classified as D. In case E, a receiver has a valid logical credential, yet the RF fingerprint levels are unacceptable, which leads to a penalty that is higher than the penalty starting value; yet less than the maximum penalty. When logical credential claims fail, yet contain high RF origin similarity acceptance levels, the transaction may be given *forgiveness* because it indicates an insider threat that may be acceptable if the cost of shutting down uplink access is high. In case E, the system logs the transaction as described in a $Level - 3$ responses above. If capable, d provides target blocking recommendations for a specific RF target without creating a denial of service to all non-offending transmission sources. Following a $Class - E$ classification, an update is made such that $\Phi = \beta_{MAX}$ adjusts the penalty step size before calculating the ITV. A new *Bonus* parameter increases the step size of α following an interaction state classification of $Class - C$ as,

$$a = a * (Bonus). \quad (13)$$

The RF-DNA-based authentication mechanism improvements apply when augmentation is "ON" and the forgiveness factor is experimentally determined using an exhaustive search. The original $Class - C$ and $Class - D$ states are retained from previous work, while states E and F are added to improve indications of insider and outsider network threats. A summary of ITV updates following each system state classification is in Table 16 below.

4.4 Results

A. 4-State vs. 2-State System Classifications of Con-Resistant Models

The upper and lower limits of forgiveness (Φ) appear in Table 19 for each *con-man* attack profile were experimentally determined with the aim of enabling tracking of authorized users while increasing uplink availability to non-offenders. Where $\Phi = 1$ and a Case E classification occurs, the upper limit of Φ_{HI} meets or exceeds these objectives in the following ways; first, the overall ITV never drops below an average trust value that is less than the current threshold of -0.5 which prevents the link from shutting down. Secondly, a new threshold can be expressed (e.g. -0.4) as the new threshold to lock out specific users that are participating in seemingly defection transactions.

150 interaction classifications occur for each independent classifier and all results are accounted for when RF-DNA mechanisms are "ON" and "OFF". For classifier D_t there are 13 classifications for $Class - E$ and 16 $Class - F$ classifications of the session interactions. Compared to the 2-State classification scheme, $Class - D$ = $Class - F$ in a 4-State system; however, the response policy of the 2-State system classifier lacks expressiveness to discern context of potential insider vs. outsider threat for enhanced situational awareness. As an unintended consequence the 90 interactions using the uninformed 2-State system allows potential RF source origin integrity forgery vulnerabilities to persist at the physical layer of the network boundary's access point. Classifiers O_{dt} and Z_{dt} improve on the specificity of a perceived insider threat (correctly) but rejects three *benign* (legitimate) credentials as *infectious* (imposter) RF-Events.

When the goal is to stop truly malicious or infectious credential acceptance, the independent RF classifiers was 100% correct. The summary of 2-state vs. 4-State classification mappings appear in Table 18.

Table 17. Tx_{A_1} vs. "All Others" Pre-Test Results $n = 150,\ p = 0.713$.

	Interactive Class				*Raw Counts*			
	True(1)		False(0)		Benign(1)		Infectious(0)	
Diagnostic Test	**C* (11)**	**F (01)**	**E (10)**	**D* (00)**	**TP**	**FN**	**FP**	**TN**
CTMS	133	-	-	17	43	0	90	17
D_t= (0.05)	120	13	16	1	43	0	93	14
O_{dt}= (5)	42	0	91	17	42	1	0	107
Z_{dt}= (2.125)	41	0	92	17	41	2	0	107

B. 4-State Transactional Classification Extensions

The results of experimentally tuning the 4-State parameter extensions from Table 16 appear in Figure 24. The 2-state system transaction classes appear on the left side of the figure, each case shows how the ITV trust plot behaves with parameter settings that range from low to high settings using experimentally determined values. Table 18 below, provides the 2-to-4-State mapping. System classification state C emphasizes the reward of Cooperative behavior, where a perception of authenticity exists. This system state occurs when the logical and physical RF diagnostic results are positive for credential benchmark similarity. However, since both mechanisms test positive for authenticity with a higher posterior estimation of being truly authentic, a user may specify policy to increase trust gains when origin integrity evidence is high and the risk of infectious threats are low [72]. $Class - E$s indicate the potential for *outsider* threats and creates the second highest threat against the system. As the distrusting penalty step size increases, so does the level of reward. Recommended range value increments of 0.25 from 1.5 to 2 for Φ. Moreover, reduce the start value of α by ~10%.

Figure 24 provide parameter tuning results using 485 transactions to yield 244 $Class - C$, 13 $Class - E$, 218 $Class - F$ and 10 $Class - D$ Interactions using Paired Logical and Physical authentication credentials.

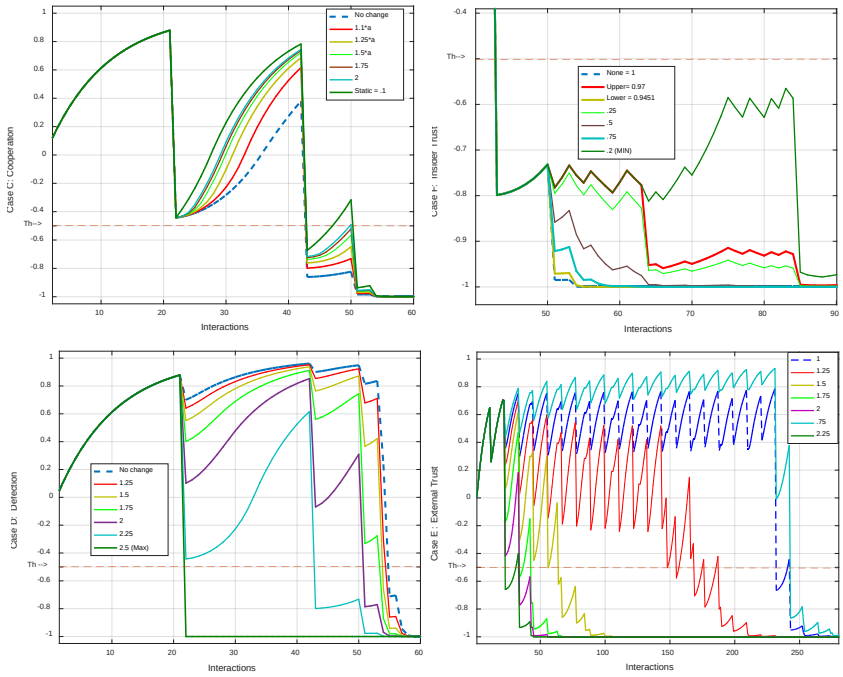


Figure 24. 4-State Extension Results: n=485, p=20% and con-man profile = SCA(20)

For $Class - F$, the emphasis is on *insider* threats that may occur in medium risk ecosystems. The trust curve of Figure 24.f shifts left to right, indicating doubt or uncertainty of trust, which results in delayed responsiveness for initiating a Level-3 response. This becomes apparent when conventional RF fingerprinting of fractional parts of messages (i.e. preamble) occurs based on some specified standardized transmission protocol. Here, an SDR may mimic the preamble's physical transmission characteristics in order to gain access to satellite resources. Such a threat is hard to track, because the authentication credential for the physical evidence is currently not considered by the authentication device. High occurrences of case F behavior may be attributable to more common causes such as new operator error or even noise.

In either case, the system state's recommendation for parameter targeting includes tracking specific transmitter behavior and mitigates the loss of uplink availability for non-offenders. Gaining of trust should be strictly less than $Class - C$ gains. For $Class - D$, the logical and physical classifier tests both report non-matching credentials and the strongest penalty of distrust is recommended for high-risk ecosystems to mitigate the occurrence of *network-disease*. Response policies should target this zone to thwart known prevalent threats. Here, the ITV plot shifts left to right Figure 24.d depending on the penalty step size. Consider the trade-offs associated with losing uplink availability for non-offenders during automatic Level-3 responses by modifying policy to deal with specific physical RF origin abnormalities. A "hands-on" verification step may be necessary (e.g. human-in-the-loop).

Table 18. 2-Factor 4-State Classification Map

	Authentication Mechanism				
	Factor-1 Logical	**Factor-2 Physical**			
State	c_k^{LOG} $[L = l]$	c_k^{PHY} $[P = p]$	**Focus**	**Risk**	**ITV Influence**
$Class - C^*$	L=1	P=1	Authentic	Low	↓↑ Reward
$Class - E$	L=1	P=0	Potential Outsider	Moderate	Delay ↔, ↓↑Reward
$Class - F$	L=0	P=1	Potential Insider	Medium	Forgive ↔, ↓↑Reward
$Class - D^*$	L=0	P=0	Pure Attack	High	↓↑Penalty

C. Trust Forgiveness Extensions for Con-man Attack Mitigation

The forgiveness factor bounds was experimentally determined using ½ step sizes that began with value of 1 to 0.5 to maintain support of the reward and penalty boundaries defined by Duncan. Each attack profile's upper and lower boundaries varied, but a pattern emerges suggesting an upper bound for forgiveness as $\Phi_{upper} \geq 0.9200$. Values that were lower than this rate for $SCA(5)$ violated the bounds placed on β and resulted in an error in processing. See Table 19 for specific experimental boundaries of each attack profile.

The value of θ indicates the attack pattern profile and appears on the left of the table. The 2-state fail/pass classification scores appear in column two of Table 19. The original algorithm's penalty for misbehavior is determined by (8) and extends for forgiveness using (11). When $\Phi = 1$, the value of forgiveness is used as a control factor represented as $\boldsymbol{T_{Control}}$ and (8) = (11). The experimentally determined forgiveness limits for each profile where the goal of enhancing link availability applies an upper limit on forgiveness and the goal of attributing user behavior by providing RF-DNA evidence of potential con-man activity is attainable using a lower limit of forgiveness. As shown in Table 19, the con-man attack pattern as θ increases, and the occurrence of illegal link access attempts decrease. Such a decrease results in a reduced opportunity to detect potential con-man activity. However, since each transaction is considered for trust, the modified forgiveness factor does adversely affect the bounds on α and β.

Figure 25 shows the detailed results of con-man attack profile SCA(20) using 400 interactions. The ITV rating appears along the y-axis while the series interaction number appears along the x-axis. The red dashed horizontal line represents the link shut-down threshold for a $Level - 3$ (uplink access shut-down) policy response for all transmitters. The line (dashed yellow) depicted in shows the original *con-man* attack profile detection that fell below the threshold after 125 session interactions and assumed a final classification of $Class - D$. Again, it is the hope of the *con-man* to gain higher levels of trust using this known attack pattern. The Cyber Defender's decision-support system is capable of logging potential offensive behavior of known users in noisy or up-tempo ecosystems using the values from Table 19. Unauthorized RF transmissions conducted by a con-man insider may be detectable with the implementation of physical layer RF-DNA fingerprint mechanisms.

Insider threat tracking provides a delay or avoidance capability to *untimely* uplink shut-downs when the origin of an offending transmitter that contains valid pathological credentials in one or more fields can be isolated from accessing the network. Adjusting $\boldsymbol{\Phi}$ to its lower bound within four significant digits is ~0.9700 for SCA(20) and the solid (blue) line provides an overall transaction classification of $\boldsymbol{Class - D}$ after 189 session interactions in Figure 25. This system condition has two favorable outcomes. First, the link for non-offenders is available for an extended period before automatically shutting down link access for non-offenders from 125 to 189 interactions. This is a 51.2% increase in resource availability.

Using an upper limit forgiveness value of $\Phi = 0.9451$ will avoid an uplink shut down response, while enabling a capability to track a suspected user's behavior with minimal modifications to existing polices. Figure 25 also shows how the overall trust does not converge to -1 as the lower limits affords. This result may not be suitable for all network administrators. However, notice that a new or complimentary threshold recommendation could possibly halt a suspected entity without halting the entire system if device specific tracking is available. Such a policy response provides minimal system modifications and extends logging capability of RF-DNA evidence. As the rate of attack decreases for the $SCA(\theta)$ profile in Table 19, the rate of Defection reduces from 16.49% using $SCA(5)$ to 3.09% using $SCA(30)$. Therefore, the probability of con-man detection by an isolated classifier becomes more difficult with low defection.

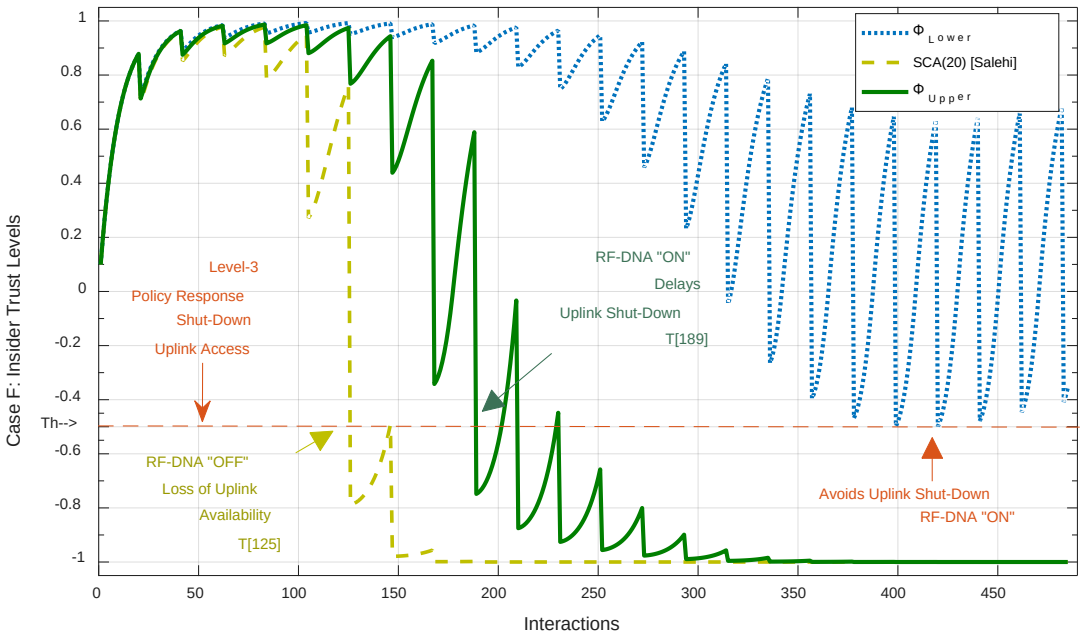


Figure 25. Enhanced *Insider-threat* mitigation w/RF-DNA fingerprints augmentation

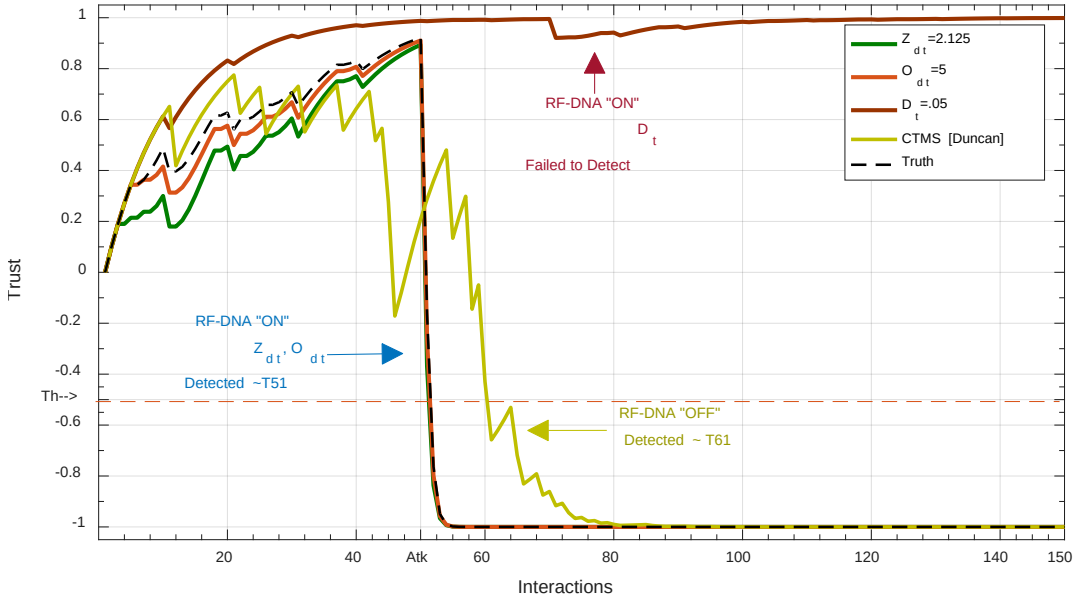
Table 19. Forgiveness Limits (Φ) of trusted rf-DNA fingerprints

Attack Profile	Logical/ Network Only Mechanism			Policy-Based Physical Mechanism Extensions			
	Attempt		$T_{Control}$	Availability (Avoids Shut-Down)		Tracking (Delays Shut-Down)	
SCA Θ	$\frac{Failed}{Total}$	Con-Rate %	$\overline{T}_{sd}$ Φ =1	Φ_{upper}	$\overline{T}_{sd}$	Φ_{lower}	$\overline{T}_{sd}$
SCA5	$\frac{80}{485}$	16.49	-0.9487	0.9200	-0.8645	0.9189	-0.0902
SCA10	$\frac{44}{485}$	9.07	-0.8596	0.9400	-0.7430	0.9245	-0.0003
SCA15	$\frac{\mathbf{30}}{485}$	6.19	-0.7203	0.9600	-0.5745	0.9271	0.3136
SCA20	$\frac{\mathbf{23}}{485}$	4.74	-0.5248	0.9700	-0.2706	0.9451	0.6054
SCA25	$\frac{\mathbf{18}}{485}$	3.71	-0.2813	0.9819	-0.0059	0.9629	0.8348
SCA30	$\frac{\mathbf{15}}{485}$	3.09	0.0007	0.9890	0.2892	0.9776	0.8850
SCA35	$\frac{\mathbf{13}}{485}$	2.68	0.3178	0.9999	0.3472	0.9876	0.9125

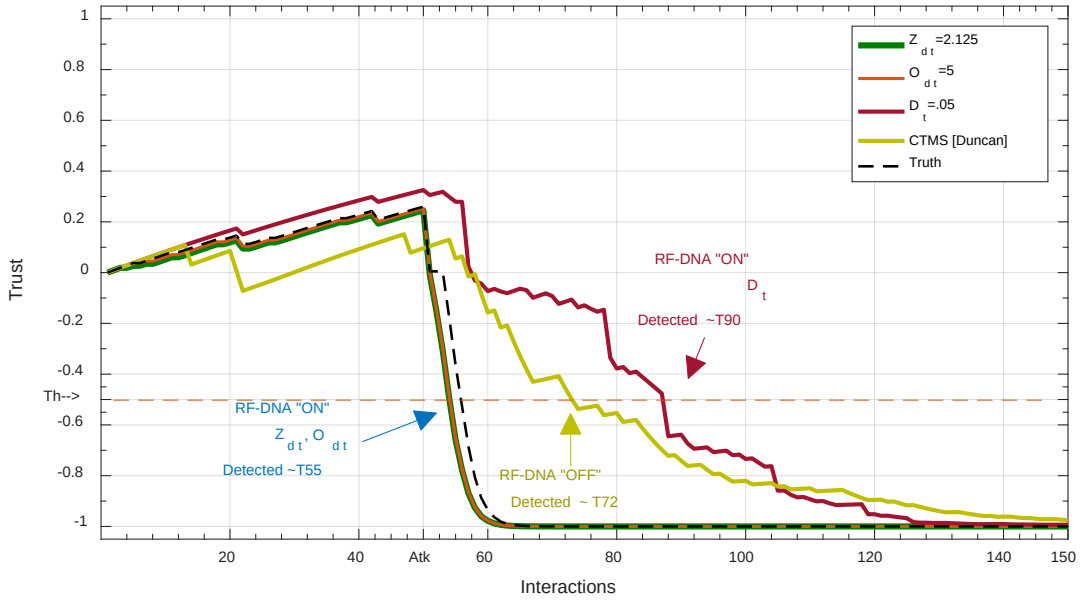
D. Abuse Case Results

In Figure 26, the first 150 results of three new diagnostic tests; D_t(dark red), O_{dt}(orange) and Z_{dt} (green) apply physical RF fingerprinting "ON" to augment a single-factor logical (bit-level) credential authentication scheme. The scheme aims to mitigate a known con-man attack abuse case that begins at transaction 50. A policy response limit of -0.5 initiates an uplink shut-down procedure when trust falls below this policy threshold using the ITV mechanism. AN RF-Event truth reference (dashed black line) indicates the true status of interactive transmission origins in a perfect ecosystem, where the authorized 'command-1' transmissions originating from Tx_A are truly *benign (Cooperative)*, while all other transmissions are truly *infectious (Defection)*.

The truth reference indicates that the attack is correctly detected during transactions 51 and 55 for high (Figure 26a) and low (Figure 26b) initial trust settings. The baseline CTMS (yellow line) scheme, employs single-factor authentication of logical (bit-level) mechanisms without augmentation (RF fingerprinting "OFF") and detects the con-man attack at transactions 61 and 72 for high and low trust settings before initiating a $Level - 3$ response. Credential authenticator D_t, underperforms against the baseline and fails to detect the attack at higher trust levels, however D_t successfully detects the attack at transaction 90 using low trust settings. When RF fingerprinting augmentation is "ON", diagnostics using O_{dt} and Z_{dt} show improved performance over the baseline and detects the attack at 51 and 56 before initiating a protective $Level - 3$ posture. That is, the number of forged credential acceptance by the CTMS decreases by 16.39% [(51-61/61)*100] and 16.39% respectively with (O_{dt} & Z_{dt}) RF fingerprinting augmentation, resulting in earlier detection of the attack.



a)



b)

Figure 26. RF-DNA augmentation [ON/OFF], Trust = [HI (a) / Low (b)].

The findings of Figure 26 suggests that when combined with additional information, RF-fingerprinting "ON" augmentation more accurately indicates the true nature of uplink access request origins and provides up to 16.39% earlier indication of RF credential forgeries. Figure 27 provides a comprehensive look at authentication augmentation using RF fingerprints in combination with logical credentials in a multi-factor authentication system. The policy threshold is -0.05, α= 0.009 and β= -0.0789 and $\boldsymbol{\Phi}$= 0.75. The original (dotted black line) con-man attack profile SCA(10) employs a simple trust algorithm where a transaction is classified as trusted or not. After developing an enhanced model in [71] the extensions to the simple trust algorithm in [72] and [1] (dashed Blue), the con-man attack (assumed to occur in a specified sequence over time) is detectable near transaction 145 for a period of 200 transactions. The use of diagnostic RF-DNA augmentation (dashed orange line) against *insider* threats ($Class - E$) detects abnormal behavior (con-man) at transaction 62.

An organization may benefit when network configurations target high risk or imminent threats, where the loss of command and control of satellite resources may be at stake, despite the cost of shutting down uplink access as soon as possible. In orange, we employ forgiveness for a targeted operational ecosystem where an *insider* threat ($Class - F$) user cannot afford to shut down uplink access to all other non-offenders without incurring significant costs. That is to say that a single user of a common ground-station transmission circuit should not be capable of denying uplink availability to all other users of the same front end transmission circuit.

As such, the capability to track trusted transmission origins and target a specific denial of service towards an offending transmitter is more appropriate. Using RF-DNA, a more accurate indication of the threat (insider vs. outsider) is achieved for authentication. A randomly generated sequence (black) shows how simulated noise affects classification accuracy when using RF-DNA.

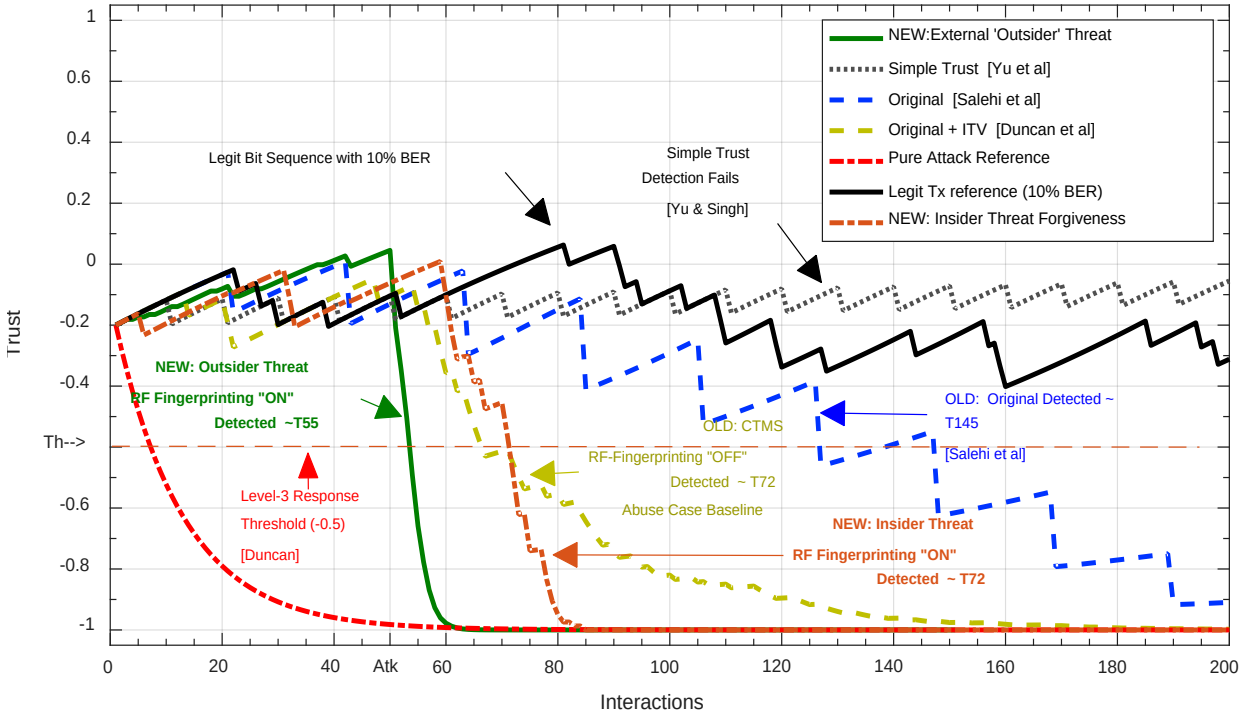


Figure 27. Abuse Case: Mitigation of insider vs. outsider threats.

4.5 Conclusions and Future Work

A need for interoperability of COTS equipment and standardization of wireless network protocols contributes to a growing capability to forge or impersonate digital uplink credentials and gain access to network resources that use logical-only authentication. Such forged access may originate from locally trusted insider or untrusted outsider RF source origins and cause *eND* such as a denial of service to non-offending ground-station sources. A multifactor authentication framework was introduced which pairs logical (bit-level) and pathological (physical) RF-DNA credentials in trust networks using Bayes Theorem. The proposed method provides an expressive 4-State classification scheme that improves posterior estimates of new credential claims over the conventional 2-State system.

Results show that combining additional evidence with the CTMS mechanism improves the expressiveness of insider vs. outsider threats and reduces the risk of *infectious* credential acceptance that may lead to *eND*. With trusted RF-DNA credential mechanisms "ON" the detection of a known cyberattack provides early warning indication of insider vs. outsider threat up to 16.39% earlier. The method provides insider threat behavioral tracking and mitigation response capability which increases uplink availability to shared resources (e.g. CubeSat) by 51.2% for non-offending entities. Extending forgiveness coupled with policy response refinement enables user tracking of suspicious insider threat behavior. In addition, targeting a specific infectious transmitter using $Class - E$ to mitigate outsider therats and $Class - F$ for suspected insider threats, provide more expressive mission support capability. This research demonstrates a policy development approach which leverages the interactive trust value (ITV) mechanism is feasible for batch (e.g. log files), single pulse at a time or fixed time sequenced (e.g. meter readings) transactions.

V. Diagnostic Origin Integrity Screening of Uplink Access Credentials

Listen to your patient, he is telling you the diagnosis. (William Osler)

Conventional authentication of a logical (bit pattern matching) credential is vulnerable to impersonation (forgery) of standardized electronic RF network modulation schemes and may cause abnormal network behavior if accepted as authentic. A con-resistant interactive trust algorithm assists in the mitigation of credential forgery acceptance in conventional benign environments. However, in a threat prevalent environment, conventional authentication mechanisms fail to consider the distinct physical RF attributes originating from fixed ground station circuits. As an unintended consequence, acceptance of forged credentials presented in a con-man attack allows unauthorized access into a network security boundary, which may lead to eND. A diagnostic framework applies Bayes Theorem to combine the RF-DNA pathology of trusted transmissions with its logical (bit-level) credential pair to improve origin integrity verification. A diagnostic screening of authentication log files returns a benign result when paired logical and pathological (physical) credential similarity exist, while a classification of infectious occurs if either credential fails to meet policy acceptance thresholds. A representative CubeSat network demonstrates the feasibility of the proposed method using a trust management system's response policy for distrusted credential detection. The method provides 100% posterior correct classification among tested samples and reduces false positives by 84%. A positive (>10) and negative (~0.1) likelihood ratio implies generalizable utility RF-Biomarker diagnostics.

5.1 Introduction

Confidence in uplink communication often relies on the assumption that an authorized electronic device transmits a fixed identification code matching the intended receiver's stored internal credentials such as authorized username, FCC-ID [68] and password combinations as specified in the link control protocol (LCP) RFC 1661 when authentication is used to conduct a three-way handshake technique like IEEE 802.11 wireless networking protocol [76]. In some cases, the use of frequency-division or time-division modulation schemes can transmit information remotely for a single device using separate channels of a coherent baseband signal [12]. In the cases where identity authentication is required, additional information such as telemetry, geospatial or other correlation of information transmissions in w_s using techniques such as signal watermarking or steganography provides opportunity to detect fraud using visible or invisible mechanisms. Such aggregation of information may increase the confidence of origin integrity [13].

A distributed CTMS manages the trustworthiness of uplink access requests originating from fixed ground stations [21] [1]. Currently, the CTMS encodes and decodes RF modulations of logical (digital bits) credential (AuthCount) fields to support authentication of fixed and standardized layer-2 or layer-3 message identification field ID_x. A satellite receiver employs an interactive trust value (ITV) mechanism to assess the dynamic reputation trust rating of received uplink requests based upon a series of transactional command interactions. The authenticity of such requests depends on the accuracy of digital logic-based authentication mechanism only. A multi-factor authentication air-monitoring framework was introduced using Zig-Bee network devices in [24]. Previous work using RF-DNA fingerprints [16] [18] [51] [52] suggest that the method to obtain preamble fingerprints can be extended to include an entire fixed message.

Such an extension adds an additional authentication factor to provide physical evidence during authentication validation when logical credential authentication alone is uncertain. Dimensionality reduction improves feature selection using sensitivity analysis [50] [70] and is adapted for RF signature analysis.

5.2 Background & Related Works

A Biomarker is defined as [40] [41] "a characteristic that is objectively measured and evaluated as an indicator of normal biological processes, pathogenic processes, or pharmacologic response to therapeutic intervention." Biomarkers assist in the evaluation of distinct physical or natural attributes that are inherent in patients or among social hereditary classification, such as deoxyribonucleic acid (DNA). Similarly, for electronic devices and networks, an *RF-Biomarker* is a physical or intrinsic characteristic of an electronic communication device's RF emissions that indicates abnormal process or response when the origin integrity of RF transmissions are suspect for causing electronic *network-disease.* It is objectively measured and evaluated to differentiate *benign* (normal) versus *infectious* (abnormal) electrical RF transmission receipts. RF-biomarker analysis aims to lend further insight into the etiology of a specified network abnormality referred to as *network-disease* (e.g. loss of link access availability) when observed levels are inconsistent. RF-biomarkers indicate the true origin of a claimed RF-Event given some decision-support tolerance threshold indicated as d_T. Diagnostic results are a representation of how likely the classified condition is, given a known population and threat prevalence rate [42]. Ahmad (2016) employs an RF-based "biodetection" platform to detect various viruses without using conventional biomarkers. This research suggests an increase in integrating biometrics, biomarkers such as DNA and RF distinct native attributes (RF-DNA) fingerprinting [43].

In Biometrics, an estimated 150 standardized indicators called minutia details are used in human fingerprinting techniques [9]. Unfortunately, there is no established number of standardized electronic fingerprint indicators or terminology (i.e. radio frequency fingerprints). Inspired by electronic defense mechanisms against spam and [32] junk email [45] along with authorized wireless uplink access using authentication mechanisms, RF fingerprinting mechanisms are explored to further augment network security. Passive radio frequency (RF) transmitter fingerprinting techniques were used in the mid-90's [18]. Shortly thereafter, unintentional RF emissions were collected from electronic devices, including network interface cards, to discriminate between anomalous behavior [4] [46]. DeJean employs physical characteristic-based certificates of authenticity (COA) to augment radio frequency identification (RFID) verification systems [49].

Currently, RF "distinct native attribute" (RF-DNA) fingerprinting classifies physically distinct RF transmissions based on standardized invariant preamble fields of a message. Invariant fields provide inherent physical characteristic permanence of a composite RF-DNA fingerprint's feature-set. Such a set includes normal distribution of specified RF-measurements of an invariant field for each feature. In RF-DNA fingerprinting, measurements of the main RF characteristics include the instantaneous amplitude, frequency and phase. The start and stop time of invariant region of interest (ROI) fields indicate the time-series target of RF signature collection. The central moments (skewness, kurtosis, standard deviation and variance) of each main characteristic may also be considered in the composite fingerprint [24] [50] [51] [52]. Reising and Kuciapinski discovered methods to analyze classification parameters, which reduce the composite feature-set's dimensionality [52] [53].

There are various modalities to automate fingerprint authentication and verification of electronic fingerprint minutia details (features). However, the minutia detail classification across composite fingerprint features may suffer from poor *detail* (feature) selection when new samples are compared to database templates [54]. Additional methods have been used to automate the discovery of indicators termed "biometrics" in the medical community. These biometrics use minutia details to identify people in information systems [55], while regional or localization techniques are employed in electronic networks to capture physical RF features (minutia details) to identify a specific transmission device. During network security monitoring, the visualization of intrusion detection and prevention system [36] enhances the situation awareness (SA) [56] of Cyber Operators. Responsive network treatment based on the unique physical properties that may exist among physical RF-DNA evidence of infection is currently unavailable.

- **5.2.1 Properties of Unique RF Features**

The first principled (*Property-0*) step of combining the pathology of physical and logical RF evidence is defining policy of acceptance of naturally occurring RF emissions (e.g. e-CFR) measurements. In this article, the RF measurements include amplitude, frequency and phase response from 2-GFSK over single side-band FM carrier transmissions at 449.9MHz. A summary of general acceptance policies of Table 13, considers five properties extended from [3] [4]. $Property-1$ suggests that a specified physical analog transmission circuit is an inherent carrier of distinct RF fingerprints that are contained within specified RF-Events and must be naturally (intrinsic) generated distinct RF origins [3]. The sources of fixed and authorized transmitters influence an RF fingerprint and must remain distinct from all other (e.g. mobile) sources during natural RF generation to satisfy *Property-1*.

To satisfy *Property-2*, the physical attributes of original RF-Events must be inherent among all similar interoperable device emissions (e.g. emissions made in the ultra-high frequency range) [29] [75]. Thirdly, *Property-3* calls for repeatability of fingerprinted RF-Events such that distributions of RF-Event samples are sufficient for RF fingerprint benchmark representation. *Property-4* implies a common RF-Event witness (e.g. authentication receiver) provides consistent measurements of new and recall of benchmark levels during similarity comparisons. Witness (authenticator) *d* has *self-evident* authentication of RF credential claims originating from *s* when all properties of Table 13 are satisfied.

Table 20. Desirable Properties of Unique RF Features

Desired	Description
Property-0:	An Oracle or policy of RF evidence acceptance has been pre-defined as truth. Defining a specific authentication device's measurement of RF fingerprint can be used as a **truth reference**.
Property-1:	An original RF-Event must be **natural** (i.e. analog or continuous) in its immediate existence in time and space rather than existing as a derived logical (e.g. binary or digital) interpretation.
Property-2:	Specified feature attributes of the physical event must be **inherent** among similar RF emission (e.g. Type III frequencygenerating transmitters [77].
Property-3:	The extractable features of RF generating circuits must be repeatable and **evident** from the occurrence of the natural event stimuli**.**
Property-4:	A sample obtained from the RF-Event must provide evidence that its significant features are **statistically unique** to support known and consistent event measurements.

- **5.2.2 Characteristics of Useful Network Diagnostic Tests**

Following the practice of the medical community [39], useful criteria enables network diagnostic test selection to mitigate *network-disease* occurrence. Key players (e.g. Cyber Operators, network administrators, resource owners and policy makers) may consider the adoption of *network diagnostic testing* in two specific areas. First, a screening of d's RF log files aims to identify the presence of *infectious* RF-Events given a known threat prevalence and network vulnerability. If screening reveals abnormal infectious levels, further tests may be necessary to treat or prevent the occurrence of a specified *network-disease*.

Treatment may include a comprehensive distributed system of RF-biomarker sensor networks with updatable signatures. For example, Table 3 lists situations where diagnostic testing may be beneficial when the risk of *network-disease* perception is serious in nature. In addition, the risk of an infectious RF source should be prevalent among similar networks to support increased threat prevalent rate. A finding of infectious evidence (significant dissimilarity) should be treatable in a wireless RF networking ecosystem. Tests should be minimally invasive to RF circuits and should not harm the communication functionality of d. Finally, a diagnostic test should be accurate in its classification of *benign* and *infectious* RF-Events. Figure 28 presents the six general steps of the multi-factor authentication framework using logical and pathological credential benchmarks.

The framework considers RF-biomarker augmentation while considering Table 3. 0.) Define the normal (non-diseased) and abnormal network conditions. 1) Specify communication node pairing policy [7]. 2) Collect RF signatures of authorized transmissions. 3) Specify acceptable thresholds for diagnostic usefulness. 4) Specify network treatment response. 5) Assess the diagnostic accuracy and make recommendations for improvement.

Table 21. Criterion of Useful RF Diagnostic tests [40]

	Network-disease should be serious or potentially so (e.g. Inability to provide uplink access)
1	*Network-disease* should be relatively prevalent in the target population (Cyber Threat Rate is Increasing)
2	*Network-disease* should be treatable (Recommendations to Minimize risk of loss to Receiver or Tx in some cases)
3	Treatment should be available for actual or suspected infectious carriers who test positive (disease is present in log files)
4	The diagnostic test should not harm the authentication receiver nor cause uncessary modifications of the incoming RF-Event's physical RF characteristics.
5	The diagnostic test should accurately classify benign and infectious RF-Events according to some policy-based threshold(s).

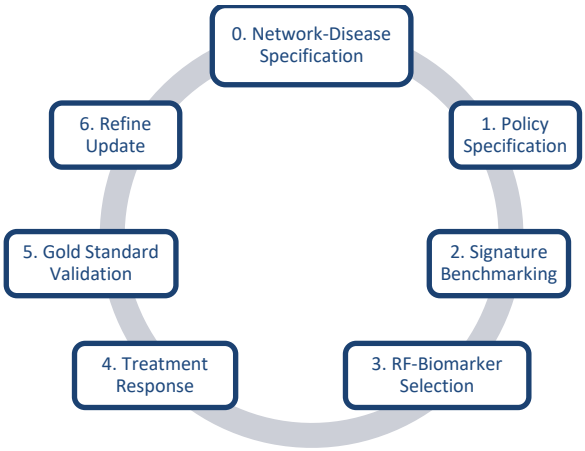


Figure 28. Multi-Factor Authentication Framework

- **5.2.3 Multi-factor Authentication Framework Overview**

5.2.3.1 Network-disease Specification

A network abnormality may be attributed to some known or unknown cause. When the cause of a specified abnormality is suspicious of originating from unauthorized or malicious activity, its occurrence can be classified as a symptom of realization of *network-disease*. There may be several abnormalities which contribute to observable *network-disease* outcomes. Acceptable thresholds, which specify a network abnormality class, depends on the policy of key players.

5.2.3.2 Policy Specification

The ultimate goal of policy development is to provide early warning signs, which can be useful in mitigating or preventing the occurrence of *network-disease*. After *network-disease* specification and vulnerability assessment, a user's policy may dictate the flow of information between electronic transmission devices for increased security control. Policy should therefore, specify desired communication paths which originate from trusted electronic devices in authorized transmission states. In addition, naming convention, targeted RF fingerprint ROIs, and RF-measurement criteria should be carefully considered.

The policy should also indicate the type of electronic receiver that will be employed for demodulation and ultimate authentication of received RF transmission events.

5.2.3.3 RF Signature Benchmarking

RF benchmarking provides trusted RF signatures for diagnostic comparison of new RF-Event claiming to originate from a known fixed transmission source. An authenticating device may possess local or reach-back RF diagnostic capability. When a local device is trained for *self-evident* authentication, a trusted RF-signature template resides within the local memory of the authentication device for benchmark comparisons.

5.2.3.4 RF-Biomarker Candidate Feature Selection

Following the collection of RF signature benchmarks, the screening of the most useful RF-measurements is done using statistical and objective analysis. The purpose of RF-screening is the discovery of the set of RF-Biomarkers from the candidate feature-set, which provides the most useful electronic device verification accuracy. The top performing RF-biomarkers are selected to improve posterior classification estimates.

5.2.3.5 Gold Standard Device Specific Benchmark Validation

A *diagnostic test* is a formal classification method that partitions a condition into two generalized states [39]. A common diagnostic test, in practice, requires a standard reference for comparisons. A *benchmark* comparison test quantifies a truth reference's measures of performance and is commonly referred to, in the medical community, as a *gold standard (GS)* [39] [42] [58]. A device-specific gold standard (GS) is a source of information, which tells us the true status of received RF transmission event (RF-Event) condition as either *benign* or *infectious*. The sequence and selection of benign vs. infectious RF-Events occurs using a simple random process that considers the threat prevalence rate to avoid verification bias and minimizes unavoidable experimental errors.

The GS validation process concludes with a report of the intrinsic, priori, posterior and likelihood ratios for each diagnostic test. The intrinsic accuracy provides the inherent accuracy (ACC) of a diagnostic test. The posterior classification accuracy provides insight into cost and benefit trade-offs associated with appropriate treatment selection following a diagnostic test. A more generalizable diagnostic measure of usefulness is the likelihood ratio (LR) when sufficient representative sampling occurs.

5.2.3.6 Treatment Response Trade-Offs

The purpose of this step provides diagnostic insight that involves a consideration of *cost* and *benefit* to the network itself, Cyber defender's and key stake holder interests. In some uncertain network situations, automatic responses may pose high-risk situations. Treatment, in this context, refers to troubleshooting responses taken to mitigate or eliminate early warning signs of *network-disease.* There are trade-offs associated with each post-test treatment response of a network's diagnostic result. A benefit occurs when the discovery of infection occurs $[T = 1, D = 1]$ and a treatment response is made towards mitigating unauthorized access attempts and a non-occurrence of electronic *network-disease*. However, a cost occurs when electronic *network-disease* occurs despite the use of treatment (e.g. blocking). If the cost of each diagnostic test is identical, then more testing may be necessary to make appropriate treatments. In binary marker evaluations, we consider the simple setting where RF-Events either have high or low symptomatic risk values. That is, high $risk(0) \equiv P[D = 0|\, Y = 0] = NPV$, or the low value where low $risk(1) \equiv P[D = 1|\, Y = 1] = PPV$. The distribution of risk in the population indicated by the RF-biomarker should be reported (absolute risk and the frequencies of those risks in the population) [59]. Let p = prevalence which indicates how widespread the potential of *network-disease* (threat) is throughout the entire population.

5.2.3.7 Refine/Update

After final RF-Biomarker selection, threshold selections, a simulation assesses the posterior accuracy of a diagnostic test using a GS validation file. Updates to the framework proposal can occur at any step without regard to order.

- **5.2.4 Decision Rules**

A decision rule [31] or corresponding likelihood ratio determines the maximum error criterion or maximum a posteriori (MAP). Decision-makers aim to make the correct network treatment decision with as few diagnostic tests as necessary. An arbitrary policy may specify a minimum accuracy of 90% pretest classification accuracy before recommending treatment. During the decision to treat a network for symptoms of *network-disease*, an initial screening level criterion $'Screen_{LVL}'$ specifies the minimum number of infected RF-Event samples that must occur in an arbitrary screening diagnostic test. This value was experimentally determined by setting $Screen_{LVL} = p$. The screening tolerance can be specified using

$$Screen_{TOL} = (n * p) * Screen_{LVL}). \quad (1)$$

A policy-based tolerance region over a distribution of RF-measurements specifies an acceptable similarity level of at least a proportion p of the population $x - pulses$ (RF-Events) with confidence $(1 - \alpha)$ is contained within its upper $(U(X))$ and lower $L(X)$ limits of acceptance [60]. A regional tolerance region specification supports binary classifications of composite RF fingerprint authenticity using a decision-rule or threshold for acceptance vs. rejection. A $(p, 1 - \alpha)$ two-sided binary tolerance interval $(L(X), U(X))$ satisfies the condition

$$P_x\{P_x(L(X) \leq X \leq U(X)|X) \geq \rho\}. \quad (2)$$

Where $'\alpha'$ represents the significance level. Construction of localized RF-Biomarker tolerance regions aim to improve posterior classification of a composite binary tolerance interval. The tolerance factor is computed based on a user's specification for reliability of new comparisons made to a specified benchmark value. The specifications include the *content* of new $'X = b'$ RF-Events (independent random variable) that are to be tested, the overall level of *confidence* that the RF-Biomarker levels should fall within the *proportion* of *X* samples that are acceptable to a known benchmark [60]. Each tolerance region is adjusted using the Gauss-Kronrod factor k_2 [30]. A tolerance region is then computed for each local RF-Biomarker candidate using $[(\rho = n), (\Psi = \{90,95\})]$.

$$Diagnosis = \begin{cases} 1 = benign, & X\ is\ \ within\ Tolerance\ ; \\ 0 = infectious, & X\ is\ Out\ of\ Tolerance\ . \end{cases} \quad (3)$$

In Figure 29(a) after conducting a diagnostic test and getting results. In (b) a diagnostic test that falls between $\boldsymbol{Th_1}$and $\boldsymbol{Th_2}$ indicates inconclusive results and suggests a need for additional diagnostic testing. In both cases, network treatment is recommended for results greater than $\boldsymbol{Th_1}$. In situation (b) may occur when pre-test diagnostic accuracy results contain high errors resulting in less accurate posterior predictive estimates. Threshold Th_i accepts RF-Event samples where the combined Euclidean distance of new RF-measurements falls within tolerance limits (3). In uncertainty, two or more parallel classifiers, as shown in Figure 10b may improve posterior estimates when Bayesian aggregation is employed in uncertainty and more conclusive evidence is necessary. The second decision-rule aims to refine the results obtained in (3) using an ordinal valued threshold. Let *b* represent the total number of independent RF-measurements that are being considered in an RF fingerprint diagnostic test. An ordinal decision-rule or threshold setting accounts for the majority vote $'O_{Vote}'$ status of all b measurements.

Then a $'O'_{Vote}$ decision-rule can be developed using an ordinal valued threshold $'O_{dt}'$ of local feature diagnostics that meet local policy threshold requirements for acceptable tolerance.

$$O_{dt} = \left(\left(\frac{b}{2}\right) + 1\right). \tag{4}$$

The ordinal valued data decision rule reduces to a binary result by comparing the RF-Event's election results of the O_{Vote} to the threshold specified in (6) above as;

$$O_{Vote} \geq O_{dt}, \begin{cases} 1, & Similarity\ Majority\ exists\ (benign); \\ 0, & otherwise\ (infectious). \end{cases} \tag{5}$$

A third decision-rule employs a continuous valued threshold $'Z_{dt}'$ that indicates an RF-Event's average risk $'\bar{Z}_{risk}'$ of acceptance using risk zones. A risk zone divides a binary policy tolerance region from (3) into four weighted risk zones (lower is better). Each risk zone's upper and lower tolerance bounds are;

$$\big(L_z(X), U_z(X)\big) = L_3(X) < L_2(X) < L_1(X),\ U_1(X)\ < U_2(X) < U_3(X). \tag{6}$$

When a pulse fails to meet the original benchmark's binary tolerance interval, a critical risk score of '4' occurs to indicate credential tolerance failure. A comparison of the average risk score ($\bar{Z}_{risk}$) to the threshold Z_{dt} indicates the level of risk as

$$\bar{Z}_{risk} \leq Z_{dt}, \begin{cases} 1, & acceptable\ risk\ (benign); \\ 0, & unacceptable\ risk\ (infectious). \end{cases} \tag{7}$$

In both cases, network treatment is recommended for results greater than or equal to decision-rule Th_1. Using Bayes Theorem, the aggregation of acceptable diagnostic improves posterior probability classifications [39].

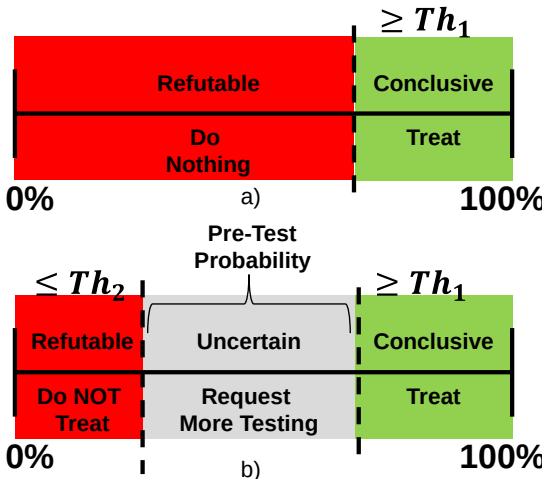


Figure 29. Treatment decision rule using a single (a) and multiple (b) thresholds.

- **5.2.5 Measuring Diagnostic Accuracy**

5.2.5.1 Classification Model

A *classification model* maps each instance of an RF-Event $'W'$ to a predicted class. Consider a simple security policy that specifies a set of received *authorized transmission states* by a trusted network communications device as an element of W, which maps to the set of instances $\{s, i\}$ [61]. For example, the RF-Event w_s represents a verified transmission state that is secure. Such a state inherently includes the transmission source of origin while all *other* non-authorized transmission states w_i are specified as insecure regardless of the source of origin [62]. More formally, let the independent variable D denote the true transmission origin condition of an RF-Event as

$$D = \begin{cases} 1 & for\ benign; \\ 0 & for\ non-benign. \end{cases} \quad (8)$$

Let T denote a diagnostic test's result classifying an instance of W as *benign* $'w_s'$ or *infectious* $'w_i'$. Further, suppose authenticating device $Rx_C's$ previous observances of benign RF-Event transmissions were used for RF benchmark training.

Once trained, Rx_C consider a continuous decision threshold policy that ranges from zero (completely infectious) to one (completely benign). For pure binary decisions, the diagnostic test (T) is represented as

$$T = \begin{cases} 1 & tests\ (+) for\ benign; \\ 0 & tests(-) for\ not\ benign. \end{cases} \quad (9)$$

Given the diagnostic result of T and the true RF-Event's origination status D, four basic classification categories can be derived from raw test count classifications of true positive (TP), true negative (TN), false positive (FN) and false negative (FP) using a known *benchmark* truth or GS file truth reference as described previously. The diagnostic sensitivity (Se) provides the probability of a *benign* diagnostic result $P(T = 1)$ is determined by the TP count divided by the total number of true *benign* RF-Event samples from the GS file. The specificity (Sp) of diagnostic testing is the converse of Se and measures the diagnostic test's capability to exclude *infectious* credential conditions expressed by $P(T = 0)$.

5.2.5.2 Pre-Test Classification Probabilities (Priori)

Probability classifications employ various names of the basic count categories. We adopt the medical terminology in this article for the terms, true positive fraction, true negative fraction, false positive fraction and false negative fraction. Khanna describes the *pre-test* classification probabilities in terms of rates using true positive rate (TPR), false positive rate (FPR), true negative rate (TNR) and false negative rate (FNR). For example, (TPR) is used to describe the classification system's *reliability* [58], Fawcett uses the terms *hit rate* and *recall* [61], whereas the medical community employs the term *sensitivity* fractions. Pepe argues that the value is not a rate at all, but a probability [39].

Here we refer to the TPR as the *sensitivity* (Se) to detect a TP classification condition from a population trusted (secure) instances of W which exists when $Se = TPR = P[T = 1 \mid D = 1]$. A *pre-test probability* is based on the RF-Event's historical profile, modulation schemes, binary encodings, signs, symptoms, and results of any other diagnostic tests performed earlier such as logical credential verification [39] using classification probability parameters (TPR, FPR, ρ). Where ρ indicates the prevalence of infectious samples among the tested population and does not affect the intrinsic accuracy (ACC) of a diagnostic classifier [42].

$$ACC = \frac{TP + TN}{SampleSize}. \tag{10}$$

5.2.5.3 Post-Test Classification Probabilities (Posterior)

Post-Test classification probabilities are not used to quantify the inherent accuracy of a receiver's diagnostic test. The posterior predictive values of a receiver-based diagnostic test are [39] $PPV = P[D = 1 \mid T = 1]$ and the false discovery rate (FDR) error is $FDR = (1 - PPV) = P[D = 0 \mid T = 1]$. The probability that an RF-Event is truly infectious given a negative diagnostic result is called the negative predictive value ($NPV = P[D = 0 | T = 0)$. The probability that an RF-Event is truly benign given an infectious diagnostic result is called the false omission rate ($FOR = (1 - NPV) = P[D = 1 | T = 0)$. Where a perfect test predictor occurs when ($PPV = NPV = 1$). When there is no useful information about the true nature of an RF-Event's origin integrity, the classifier is deemed useless. This useless situation occurs when the $PPV = \rho$ and $NPV = (1 - \rho)$. The roles of D and T are reversed in the *post-test* predictive values relative to their roles in the *pre-test* classification probabilities [39, p. 16]. Posterior predictive values are most useful for a particular study and depends on the level ρ which may not be generalizable beyond the tested samples unless suitable random samples of the general population are considered [78] [79].

5.2.5.3.1 Relationship Between Predictive Values and Classification Probabilities

Predictive values are best used to quantify the usefulness of a diagnostic test while *pre-test* classification probabilities are best used to indicate the intrinsic accuracy (ACC) of a specific diagnostic test. Prediction values are dependent on three parameters that should be reported in diagnostic test performance [39]. When knowledge of ρ from (8) or (9) is available, there is a direct relationship between *posterior* predictive values and *priori* classification probabilities. These three parameters can be found using the priori classification probabilities and the disease prevalence as (TPR, FPR, ρ). The three predictive value parameters that provide post-test statistics are (PPV, NPV, τ) [39, p. 16]. The symbol τ indicates the probability of a positive test $P[T = 1]$.

5.2.5.3.2 Bayesian Aggregation of Multiple Diagnostic Tests

In the first medical example [39], the diagnostic test's usefulness assessment employs Bayes Theorem to represent the post-test probabilities (PPV, NPV,τ) in terms of the pre-test probabilities (TPR, FPR, ρ) where $\left(PPV = \frac{\rho TPR}{\{\rho TPR+(1-\rho)FPR\}}\right)$, $\left(NPV = \frac{(1-\rho)(1-FPR)}{\{(1-\rho)(1-FPR)+\rho(1-TPR)\}}\right)$ and $\tau = (\rho TPR + (1-\rho)FPR)$. Moreover, the pre-test or priori probabilities are written in terms of posterior probabilities and similarly found as

$$\left(TPR = \frac{\tau PPV}{\{\tau PPV+(1-\tau)(1-NPV)\}}\right), \left(FPR = \frac{\tau(1-PPV)}{\{\tau(1-PPV)+(1-\tau)NPV\}}\right)$$

and

$$\left(\rho = \tau PPV + (1-\tau)(1-NPV)\right).$$

As a second medical community example of assessing the usefulness of diagnostic accuracy, Zhou's application of Bayes' Theorem computes the posterior probabilities in [42, pp. 48-49]. Rosen generally employs Bayes Theorem to mitigate the occurrence of electronic spam message acceptance using *word* occurrence filters.

More generally, if B_i is the event where a new RF-Event sample contains a set of matching physical RF-Biomarker credential occurrences b_k, then by Bayes' Theorem the prediction probability that a message containing all specified RF-Biomarker $b_1, b_2, \ldots, b_k$ as *benign* similarity levels is found by

$$r(b_1, b_2, \ldots, b_k) = \frac{\prod_{i=1}^{k} p(b_k)}{\prod_{i=1}^{k} p(b_k) + \prod_{i=1}^{k} q(b_k)}. \quad (11)$$

For a particular RF-Biomarker (b_k) credential, the pre-test probability that an acceptable tolerance level of similarity for $b_k$appears in an infectious message is estimated by determining the proportion of b_k appearances in known *benign* vs. all *infectious* RF-Events.

- **5.2.6 Misclassification Probabilities (Errors)**

One method of quantifying diagnostic test accuracy is by considering the frequency of misclassification for each infectious RF-Event states. There are two types of errors that may occur during pre-test classification. A Type-I error is referred to as the false positive rate (FPR) and is often indicated by the symbol alpha (α). When used in computer science applications, it is inappropriate to simply report the misclassification probability, the FNR = (1-TPR) and the FPR [39]. A Type-II error rate or fraction estimates the probability that a receiver classifies an RF-Event as *infectious* when the true condition is *benign* as the false positive rate ($FPR = P[T = 1 \,|D = 0]$). The paired diagnostic results of (FPR, TPR) probabilities define the likelihood at which (4) occurs during a particular diagnostic test [39].

- **5.2.7 Measuring Predictive Usefulness**

The likelihood ratio (LR) statistic for a given diagnostic test provides the ratio of expected test results in subjects with a certain condition to the subjects without the condition. In this context, a $\left(LR^{+}_{test} = \frac{Se}{FPR}\right)$ ratio indicates a diagnostic test result associated with the presence of RF

signature similarity as a *benign* (positive) condition, whereas the absence of RF transmission similarity indicates an *infectious* (negative) condition using a LR negative $\left(LR^{-}_{test} = \frac{FNR}{Sp}\right)$ [79]. For posterior predictions, we can use a LR for positive $\left(LR^{+}_{Sub} = \frac{PPV}{FOR}\right)$ and negative $\left(LR^{+}_{Sub} = \frac{FDR}{NPV}\right)$ subjects to make the usefulness of a diagnostic test more generalizable. We avoid zero (i.e. replaced with 0.1) and infinite values (i.e. replaced with 10,000) for the LRs adapted from [80].

- **5.2.8 A Representative SATCOM Network**

In social or electronic communities, *trust* is a rating assigned by a perceiving (receiver) agent indicated by $'d'$ with respect to a transmitting source agent indicated by $'s'$ for a specified time t [71] . The term *con-man* is adapted from [72] to indicate requester s who takes advantage of d during a series of access request transactions. During such transactions the *con-man* presents acceptable credentials that are contained within standardized RF modulations of message $'m'$ that lead to a classification of *Cooperation* $'C'$ between s and d. Such cooperation may lead to the execution of *infectious* payload data contained within the body of m transmitted by s. Then, when it comes to a high –risk interaction, the *con-man* will defect. That is, s initiates a Trojan-horse transaction that attempts to defraud d. The trust rating about the reputation of s updates by d following fraud detection and transactional state classification of *Defection* D. At this point, the con-man either attempts to regain lost trust or stop future communication with d. To regain trust, s will again initiate several transactions that are C in nature. Here, s hopes to deceive d again by masking its true *infectious* intentions by presenting logically correct message credentials while inserting some unauthorized payload.

Table 22. Con-Resistant Interaction Trust Algorithm [72]

Cooperation		***Defection***		
$T'_{sd} = T_{sd} + \alpha(1 - T_{sd})$	(1)	$T'_{sd} = \frac{T_{sd} + \beta}{1 - \min(\lvert T_{sd}\rvert, \lvert\beta\rvert)}$	(6)	$T_{sd} > 0$
$T'_{sd} = \frac{T_{sd} + \alpha}{1 - \min(\lvert T_{sd}\rvert, \lvert\alpha\rvert)}$	(2)	$T'_{sd} = T_{sd} + \beta(1 - T_{sd})$	(7)	$T_{sd} < 0$
$T'_{sd} = \alpha$	(3)	$\beta = (\beta - \gamma_d(1 + \beta))$	(8)	$T_{sd} = 0$
$\alpha = \min(\alpha + \gamma_c(\alpha_0 - \alpha), \alpha_0)$	(4)	$\gamma_d = {}^1/_e * \lvert T_{sd}\rvert = \frac{\lvert T_{sd}\rvert}{e}$	(9)	
$\gamma_c = 1 - \lvert\beta\rvert$	(5)	$\alpha = 1 - \lvert\beta\rvert$	(10)	

Several well-known *con-man* attack patterns are recreated in a simulated ecosystem using attack profiles of θ = 5, 10, 15, 20, 25, 30, 35 and 40. In such profiles, the con-man will conduct a series of θ transactions that would be classified as C and then immediately initiate a transaction defection classification. A rating of '0' indicates the absence of trust. Initial trust ratings begin at '0' with adjustments occurring throughout directed session interactions from s to d [71]. As link session interactions occur, trust ratings are strengthened or weakened for the next (t +1) transaction period and is based on the perspective of authenticator d. An authenticator (device d) is defined as having RF-DNA credentials of statistically trusted RF-Events that are emplaced in its local memory to enable *self-evident* origin integrity of trusted sources as suggested in [25].

Duncan employs a two-state system classification scheme according to d's transactional classification and the current level of the ITV assigned by d's logical authentication mechanisms. Based on the value of the ITV during a session, Duncan employed a three level policy response scheme where he arbitrarily selected a policy-based threshold limit of -0.5 as the lowest acceptable ITV rating that could occur during a series of 200 transactions. A Level-1 response is referred to as "Trust Management Event Logging Only" where the response actions of the authenticating device includes a comparison check of the command authentication count upon receipt of a new RF-Event and the associated ITV is calculated for the authentication count marker.

Once the ITV for authentication count reaches the decision-rule's distrust threshold, an alert is logged indicating excessive invalid attempts. A Level-2 response, termed "Trust Management Event Logging and Prevention," includes the responses of a Level-1. However, once the ITV for authentication count reaches Th command processing halts for anonymous users and an alert is logged indicating excessive invalid command attempts. Meanwhile, a Level-3 policy response "Trust Management Event Logging, Prevention and Recovery" include responses of Level-1 and Level-2 and once the ITV for authentication count reaches Th command processing halts for anonymous users and an alert is logged indicating excessive invalid command attempts. A legitimate ground station must unlock satellite commanding and the CTMS via a logical credential trust mechanism to resume commanding operations.

Two transactional state extensions adapt the expressiveness of the con-resistant interaction trust algorithm to provide insight into the nature of a con-man's origination as being an insider vs. outsider threat. In the extension scheme, RF fingerprinting is employed to augment the logical authentication scheme by using physical attributes of fixed RF transmission benchmark origins. An interactive state E occurs when the logical diagnostic test result is positive and the physical RF origin similarity is acceptable. An interactive state F occurs when the logical result is negative for a binary credential match and contains acceptable RF origin similarity levels. The extended multi-factor authentication scheme aims to improve the posterior probability estimates of the isolated authentication mechanism used in uncertainty.

A $Bonus$ and *forgiveness* factor support the extensions. When both authentication mechanisms (i.e. logical and pathological similarity exists) test positive for benign similarity levels, an optional $Bonus$ provides an increase in the reward step-size. The forgiveness factor (Φ) is offers an optional delayed $Level - 3$ response for specific situations.

Table 23. Con-Resistant Interaction Trust Algorithm State Extensions

Two	***Cooperation (C)***		***Defection (D)***	
Four	C*	E	F	D*
Extensions	$\boldsymbol{a = a * (Bonus)}$	$\Phi = \beta_{MED}$	$\Phi = \Phi_{[HI,LO]}$	$\Phi = \beta_{MAX}$
	$\boldsymbol{\alpha = min(\alpha + \gamma_c(\alpha_0 - \alpha), \alpha_0)}$ **(4)**	$\beta = \beta_{start} * \Phi$	$\beta = (\beta - \gamma_d(1+\beta))\Phi$	$\beta = \beta_{start} * \Phi$
	$\boldsymbol{\beta = \beta}$	$\alpha = 1 - \lvert\beta\rvert$ (10)	$\alpha = 1 - \lvert\beta\rvert$ (10)	$\alpha = 1 - \lvert\beta\rvert$ (10)

5.3 Methodology: 2-Factor RF-DNA Credentialing

Figure 30 represents the RF-DNA collection and networking experimentation circuit. Each circuit component is labeled with a letter and role for representative icon reference. For example, the device used to generate the initial message for collections is shown as (label | description)

PC1| PC1: msg (message) generator. The laptops in Figure 30a and Figure 30f are identically configured with the following; LabView 2014 with RT Modulation Tool Kit, Math Script. Windows 10, (HP Zbook 15) with 32GB RAM, 500GB DDRL 4DM, 5400 RPM, integrated NIC, I Core i7-4800MQ processor. Software includes Microsoft Office 2013, Matlab 2015a, 2016a and Jump Pro 12.1. Each physical circuit had physically distinct hardware, cables and antennae and could transmit or receive. This experiment focused specifically on a simplex uplink transmission scenario.

1) Transmission Circuit (Ground Station)

Tx_A, Tx_B and Rx_C are national instrument USRP-2922 software defined radios that differ by serial number only. In Figure 30a and Figure 30b represent that baseband logical message generator (*msg*), which transmits commands to the front end transmission device Tx_A in Figure 30c (USRP 2922) for final modulation onto the uplink medium. Devices Tx_A and Tx_B (red USRP 2922 in Figure 30c) are the transmitters under test. GS1 is defined as the benchmark validation test for Tx_A emissions as observed by receiver (authenticator) Rx_C.

Tx_A's RF emissions are collected for signature profile benchmarking. Tx_B represents an arbitrary opponent transmitter that attempts to forge the credentials of Tx_A.

2) RF-Event and Environmental Considerations

A 2-FSK modulation scheme is used to transmit *msg* over FM using a carrier frequency of 449.9MHz. An 100kHz offset is set from the center frequency of 450MHz. Each pulse duration is approximately 6.399ms. The receive circuit had a tunable bandwidth selector that was set to 20kHz and detected each pulse using a tunable triggering mechanism based on the magnitude of the amplitude. The FSK deviation was set to 1. There were eight total RF-measurements that were selected arbitrarily to include the instantaneous amplitude, frequency, and phase. Preliminary results extracted RF-DNA fingerprints near the preamble of ICOM-9100 amateur radios used in an operational ground station circuit, where the amplitude provided the greatest accuracy for correct classification. Therefore, the variance, skewness and kurtosis were set for collection using the USRP SDRs. Finally, the root mean squared error of the amplitude was collected for each pulse. For each RF-Event pulse (Figure 30d) successfully received by Rx_C (Figure 30g), the RF-DNA is extracted from 10 fixed and equally spaced sub regions plus the full wave regions using complex real and imaginary parts of the analog waveform. This brings the total number of distinct RF-DNA contained within a complete collection to ([8 features] * [22 sub-regions]) 176 RF distinct native attributes for possible selection as key discriminating factors. There are three output files that are generated by Rx_C following RF-DNA collection. Initially, Rx_C is trained to learn the RF-DNA of each trusted device Tx_i. After that, the benchmark signature is validated for accuracy using new RF-DNA collections from unseen RF-Events from the same device. After benchmarking, Rx_C is placed in testing mode to assess the level of accuracy to diagnose messages which contain potentially infectious credentials.

a) Data1: 4-State Transaction Classification of Logical and Pathological Credential Pairs

Data1 (Figure 30h) is used to classify the transactional state of the uplink transmission using a 4-State classification system and two factors. Factor 1 is represented by the logical credential, while factor 2 is the RF-DNA fingerprint of the logical credential as specified by policy.

b) Data 2: RF-DNA signature Comparisons

The RF-DNA benchmark credential (Figure 30i) consists of the distribution of RF-Measurements previously defined by policy. The benchmark consists of (8 RF-Measurement features * 22 real and imaginary regions of interest) for the full complimentary RF-DNA set. We analyze eight of these 176 using the real values of the full wave characteristics.

c) Data 3: Baseline RF-biomarker Levels:

The distribution of measurements obtained from the RF-DNA subset is then assessed using Euclidean distance to assess the level of self-similarity that each feature has with itself as depicted in Figure 30j. The average result is used as the baseline RF-Biomarker similarity level to compare new RF-Events to the benchmark RF-DNA signature previously templated using Data2 above.

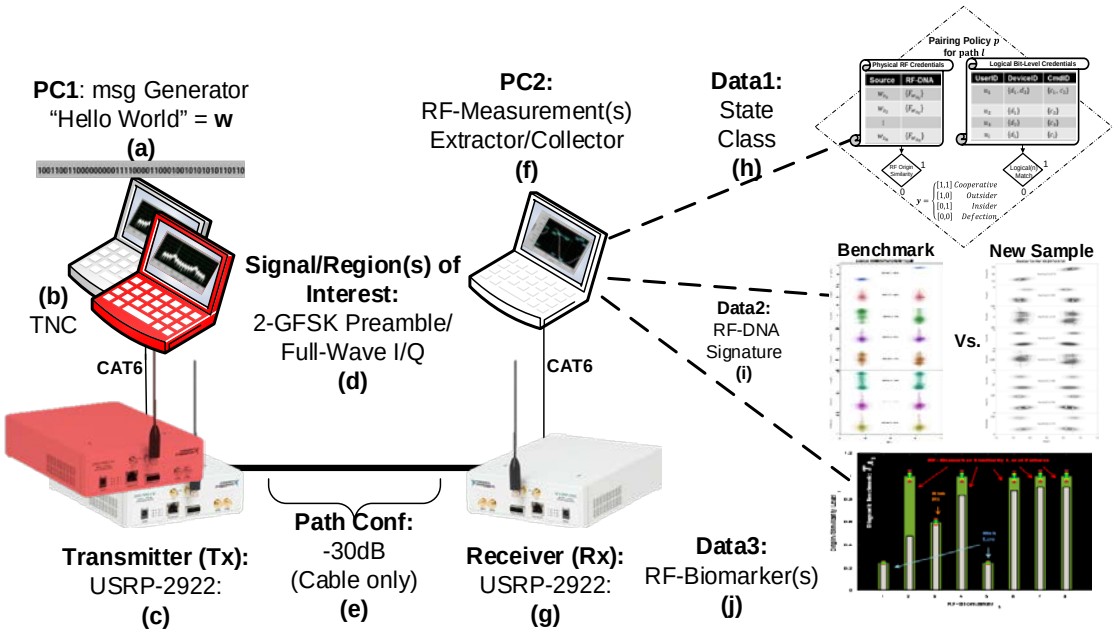


Figure 30. Physical Network Diagram and Data output for Experimentation

Three software defined radios devices $Tx_A = s_i$, $Tx_B = s_a$, and Rx_C are configured transceivers of RF modulated messages in an interoperable network ecosystem. Tx_A and Tx_B were set up as transmitters, while Rx_C was configured as the satellite receiver. Distinct hardware circuits of Tx_A & Tx_B are logically equivalent in configuration for interoperability and standardization of commercial off the shelf equipment. Prior to experimentation, RF-DNA fingerprints of Tx_A and Tx_B are collected using Rx_C for benchmark template development.

Finally, probability classification processing was done using MATLAB version 2015a and LabVIEW's Math Script 2015 module. Rx_C trains on 1100 trusted RF-Events from Tx_A while transmitting an authorized command (message-1) to compose a trusted RF-DNA fingerprint *benchmark* template. The same RF fingerprint classifier was then tested using 150 new claimed RF-Events for Tx_A while transmitting from the same authorized state for benchmark verification.

The process repeats for three additional commands for Tx_A to provide a total of four benchmarks and four test sets for verification. Each device connects to separate laptop PC using LabVIEW 2015 to generate complex RF transmissions that include a 48-bit preamble, 48-bit payload (Credential ID) and 48-bit *postamble*. Authenticator device Rx_C receives, and demodulates transmissions of Tx_A and Tx_B for credential authentication, where Tx_A is randomly selected as the trusted transmission source, while Tx_B is arbitrarily untrusted. We designate the authorized transmissions originating from Tx_A 'command-1' =*Benign*. This research only considers eight arbitrarily selected RF measurements for proof of concept demonstration. We designate all commands from Tx_B and 'command-2' from Tx_A as {All 0thers = *Infectious}*. The system is initialized using a starting low trust reward step-size for ($\boldsymbol{\alpha_{start}} = 0.1$). This is (Bonus = Bonus + $\boldsymbol{\alpha_{start}}$). The distrust penalty, ($\beta_{start} = -0.4$).

To assess the effect on the Level-3 response, during the abuse case, multi-factor authentication using logical and pathological credential mechanisms are used. Forgiveness is used to adjust the penalty step-size when the new sample matches an RF fingerprint benchmark. Low forgiveness $\Phi_{LO} = 0.9451$ is used to **delay** a Level-3 response. High forgiveness, $\Phi_{HI} = 0.97$ is used to **avoid** an uplink shut-down altogether while maintaining the capability for an authentication device to track the distrustful behavior of an offending RF transmitter. The arbitrarily selected thresholds for each diagnostic test is provided in Table 4. In the abuse case experiment, a Bayesian RF fingerprint verification filter classifies a new set of 43 benign and 107 infectious (not-benign) messages from two physically distinct SDRs while logging new RF-measurements of the new RF-Event. To establish a common reference for test validation, all received messages are contained in a modulated transmission RF-Event and are logically identical (i.e. the logical/binary bit streams are the same).

A simple random selection of infectious RF-Events replaces defective transactions '0' using a well-known con-man attack profile model $SCA(5)$ [71]. A comparison of the GS dataset reference and known benchmark levels provides the resulting classification match scores using associated diagnostic thresholds or decision rules in Table 4. The first 49 transactions of the GS truth reference represents legitimate command transmissions with 10% bit errors originating from Tx_A, where 'command-2' from Tx_A is randomly selected as the representative error samples. The random noise replacement index values for this experimental run is; [5;11;18;22;26;37]. The index replacement's truth column updates to truth condition code = 2. Next, for transactions 50 - 150, a simple random selection takes a Tx_B's pool of 'command-1' and 'command-2' RF-Event transmissions and replaces a known benign entry in the reference dataset.

Finally, the gold standard column (14) was created such that all commands that remain for Tx_A 'command-1' retained the value of '1', while all other commands were given a value of '0'.

- **Decision Rules and Treatment Thresholds**

The treatment responses are summarized with the following pseudo code using the threshold settings from Table 4. Each classifier's performance is evaluated for classification accuracy of the truth reference GS file before and after Bayesian aggregation. The intrinsic accuracy and predictive usefulness results will be used to provide decision-support recommendation to treat, do nothing or ask for more diagnostic testing towards mitigation of *network-disease*. Using the raw counts of TN, TP, FN and FP, the priori classification probabilities of TPR, FPR, TNR, and FNR will be computed to provide the pre-test classification probabilities and the overall intrinsic accuracy (ACC). The usefulness of posterior prediction estimation is assessed by evaluating the probabilities for the PPV, FDR, NPV and FDR classifications.

Table 24. Network Treatment Response

When $[Th_1 = F]$*; //No Infection suspected*
    If $[PPV \leq Th_4] \cap [FDR \geq Th_5]$,
        //EVIDENCE UNCERTAIN
        ASK FOR MORE DIAGNOSTIC TESTING
    Else
        //REFUTABLE EVIDENCE
        DO NOTHING
END
When$[Th_1 = T]$ *; Infection of Log Files Suspected*
    If $[ACC \leq Th_2] \cup [FPR > Th_3]$
        //EVIDENCE UNCERTAIN
        ASK FOR MORE DIAGNOSTIC TESTING
    Else
    If $[NPV \leq Th_6] \cap [FOR > Th_7]$
        //EVIDENCE UNCERTAIN
        ASK FOR MORE DIAGNOSTIC TESTING
    Else
        //CONCLUSIVE EVIDENCE
        TREAT FOR *NETWORK-DISEASE* MITIGATION
END

A screening of RF-Biomarker candidates selects the highest pre-test and post-test accuracies with minimal errors while considering the treatment decision rules from Table 4 to establish performance cut-offs. Generally, higher intrinsic accuracy is better and higher posterior predictive accuracy is better. The top performing classifiers are selected for Bayesian aggregation with the aim of improving the posterior classification estimations and reported as the best predictors of *network-disease* for device A.

Table 25. Treatment Decision-Rules

Threshold / Rule	Parameter	Value	Default
Th_0	Screen?	[Yes/No]	Yes
Th_1	Symptoms?	[T/F]	T
Th_2	ACC	(0:1)	.9
Th_3	FPR	(0:1)	.1
Th_4	PPV	(0:1)	.95
Th_5	FDR	(0:1)	.05
Th_6	NPV	(0:1)	.95
Th_7	FOR	(0:1)	.05
D_t	Global Euclidean Distance	(0:1)	.05
O_{dt}	Local Majority	[0:b]	5
Z_{dt}	Risk Zones	[0:4]	2.125

Three diagnostic classifiers are assessed for classification accuracy against the CTMS's baseline logical authentication classifier only. 1.) Diagnostic test D_t provides a binary classification as to whether a new RF-Event's RF-measurements falls within tolerancetol. 2.) An ordinal valued diagnostic test O_{dt} employs an arbitrary decision-rule threshold value of '5'($O_{dt} = 5$). 3.) Finally, a continuous valued diagnostic test employs a decision-rule threshold using risk zones is set such that ($Z_{dt} = 2.125$). Three treatment response threshold values are arbitrarily chosen to demonstrate the experiments' proof of concept. The $Screen_{LVL} = 20\%$, GS file size is $n = 150$ and threat $\rho = 20\%$.

The initial log file screening tolerance is $Screen_{TOL} = (150 * .71 * .71) = 37$. For a specified screening classifier, a decision rule to continue treatment against *network-disease* is assisted using an initial threshold rule as

$$Th_0 = \begin{cases} T, & SumCount_{TN} \geq Screen_{TOL}; \\ F, & otherwise. \end{cases} \quad (12)$$

5.4 Extension Validation and Classification Results

5.4.1 Diagnostic Accuracy Results

5.4.1.1 Raw Diagnostic Counts

The diagnostic test results for each classifier in Table 7. Of the 49 total RF transmissions originating from Tx_A, only 43 are truly *benign* transmissions of command-1, while all other transmissions are *infectious.* The baseline diagnostic classifier ($CTMS$), using the logical decision-rule ITV and transaction state classification had 43 TPs, and 17 TN test results. However the $CTMS$ diagnostic test has 90 FP errors. The composite RF fingerprint classifier decreased in performance compared to the CTMS baseline had 93 FPs and only identified 14 of 107 infectious samples. The ordinal valued classifier O_{dt} had 107 infectious tests, 42 benign tests and a single FN test. Moreover, O_{dt}'s $ACC = 99.33\%$ is a significant improvement over baseline's ACC=40% and meets screening all requirements for conclusive treatment response. Similarly, classifier Z_{dt} out performs the baseline diagnostic test with $ACC = 98.67\%$ and two counts of FN errors. Table 26 provides a summary of the diagnostic ACC performance.

5.4.1.2 Pre-Test (Priori) Diagnostic Classification Probabilities

The priori classification probabilities are provided in Table 27. The Diagnostic classifier D_t underperforms the baseline $CTMS$ by three additional FPs and classifies true negative (infectious) RF samples at a reduced rate of $Sp = 13.08\%$. Fortunately, D_t does not have any FN

classification errors. O_{dt}'s, results indicate significant improvement in reducing the FPR to zero, while increasing Sp to 100%. The $Se = 97.67\%$ of O_{dt} shows a drop in performance over the $CTMS$, however high FPR rates of 90% and 93% were significantly high and indicates significant acceptance of RF credentials of dissimilar RF benchmark origins. Finally, the risk zones classifier saw similar performance improvements as O_{dt} over $CTMS$ and D_t. The risk zone classifier has a higher false negative rate of 4.65% above the ordinal classifier's 2.23%, which increases the rate of rejection for *benign* credentials. The $CTMS$ and D_t diagnostic performance fails arbitrary threshold requirements and requires more diagnostic. Classifiers O_{dt} and Z_{dt} meet arbitrary performance requirements for $ACC \geq 90\%$ and $FPR \leq 10\%$.

Table 26. Abuse Case Interactive State and diagnostic count results

	2*/ 4-System State				***Counts***				
	True(1)		**False (0)**		**Benign(1)**		**Infectious(0)**		**Intrinsic Accuracy**
Diagnostic Test (Threshold)	**C* (11)**	**F (01)**	**E (10)**	**D* (00)**	**TP**	**FN**	**FP**	**TN**	**ACC**
CTMS(P)	133	-	-	17	43	0	90	17	0.4000
D_t= (0.05)	120	13	16	1	43	0	93	14	0.3800
O_{dt}= (5)	42	0	91	17	42	1	0	107	0.9933
Z_{dt}= (2.125)	41	0	92	17	41	2	0	107	0.9867

5.4.1.3 Post-Test (Posterior) Diagnostic Classification Probabilities

When an RF-Event tested positive using the $CTMS$ baseline diagnostic classifier, tests of originated from Tx_A using 'command-1' tested as having authentic credentials 32.33% of the time. Unfortunately, the low $Sp = 15.89\%$ coupled with a high $FPR = 84.11\%$, the usability of the $CTMS$ for isolated authentication in a contested ecosystem does not meet arbitrary thresholds from Table 4. As such, the baseline $CTMS$ and the classifier D_t, did not meet initial screening requirements when at least 37 *infectious* samples are discovered.

Table 27. Con-Man Abuse Case Probability Classification Results

	Classification Probabilities (%)											
	Priori Accuracy				**Likelihood Ratios (Tests)**		**Posterior Accuracy**				**Likelihood Ratios (Subjects)**	
Diagnostic Test (Threshold)	**Se TPR**	**FNR**	**FPR**	**Sp TNR**	**LR+**	**LR-**	**PPV**	**FDR**	**FOR**	**NPV**	**LR+**	**LR-**
CTMS	1	0	0.8411	0.1589	1.19	0.629	0.3233	0.6767	0	1	3.23	0.6767
D_t	1	0	0.8692	0.1308	1.15	0.765	0.3162	0.6838	0	1	3.162	0.6838
O_{dt}	0.9767	0.0233	0	1	9.767	0.023	1	0	0.0093	0.9907	107.53	0.1009
Z_{dt}	0.9535	0.0465	0	1	9.535	0.047	1	0	0.0183	0.9817	54.65	0.1019

When aggregating classifiers D_t and $CTMS$ we improved the PPV to 57.8%, which is marginally better than random guessing. The PPV significantly improves to 100% when combined with any of the three augmentation classifiers. Before aggregation, the NPV for $CTMS$ performance was 100%, meaning that the chance of being correct when tested positive for infectious credentials, the credentials were truly infectious (forgeries). The NPV improved to 100%, which relates to zero false negative errors. Results also show that a significant improvement for O_{dt} and Z_{dt} achieves 100% NPV after Bayesian aggregation with CTMS priori classification. The aggregation of all classifiers further improves posterior classification accuracy results to 100% NPV and 100% PPV with 0% FDR and FOR errors. In this case, we can predict the probability of having received authentic credentials contained within a modulated RF-Event among known RF-Events whose credentials tested positive with 100% likelihood. Prior to aggregation, the CTMS's 67.67% FDR significantly reduces to 0% forged credential acceptance when combined with RF-Biomarker diagnostics. The posterior probabilities are in Table 28.

5.4.1.4 Benchmark Visualization Results

After selection of the most useful diagnostic network classifiers O_{dt}, Z_{dt} or a Bayesian aggregation of the baseline classifier with either O_{dt}, Z_{dt} or all is considered in developing a diagnostic visualization.

Using the LR ratios, we can see that the best indicator before aggregations are classifiers O_{dt} and Z_{dt} for both benign and infectious tests and subjects. Such visualization aims to show a Cyber Operator an intuitive image that describes the RF origin similarity levels of a known RF fingerprint benchmark compared to a new RF fingerprint extraction from a claimed trusted RF origin.

Table 28. Bayesian Aggregation of Pre-test Classifiers

Priori Aggregation of Diagnostic Evidence	**Posterior Origin Integrity Classification** Probability (%) **of Claimed Credential**					
	Benign (1)		**Infectious (0)**		**Likelihood Ratios (Subjects)**	
	PPV	**FDR**	**FOR**	**NPV**	**LR+**	**LR-**
$C_{TMS} \cap D_{dt}$	0.577	0.4213	0	1	5.77	0.4213
$C_{TMS} \cap Z_{dt}$	1	0	0	1	10	0.1000
$D_t \cap O_{dt}$	1	0	0	1	10	0.1000
$O_{dt} \cap Z_{dt}$	1	0	0.0004	0.9996	10	0.1000
$C_{TMS} \cap O_{dt} \cap Z_{dt}$	1	0	0	1	10	0.1000
$C_{TMS} \cap D_t \cap O_{dt} \cap Z_{dt}$	1	0	0	1	10	0.1000

The trusted benchmark's self-similarity score for Tx_A benchmark versus itself is 75.74% appears as green bars in Figure 31. The 'red bars' represents a truly infectious RF-Event samples originating from Tx_B, while the 'blue bars' indicates truly benign RF-Event samples transmitted by originating from Tx_A As shown in (grey bars), RF-Biomarker candidates 1, 3, and 5 meet tolerance acceptance, while all others fail (i.e. candidates 2, 4, 6, 7 and 8). The diagnostic visualization and the statistical tests indicate conclusive evidence for the presence of infectious credentials within the electronic device's local log files. Without treatment, acceptance of such credentials may lead to *network-disease* such as an untimely $Level - 3$ response, preventing access to critical uplink resources for non-offenders. The benchmark contains n=1100 RF-Event samples of Tx_A transmitting 'command-1' as a policy specified authorized transmission state.

In normal operation, RXC extracts new RF fingerprints from incoming RF-Events and conducts a benchmark similarity test using a set of useful RF-Biomarkers. As shown, the diagnostic result indicates conclusive evidence of infectious credentials. There are $[b = 8]$ candidate RF-Biomarkers of *network-disease*. The Euclidean distance of dissimilarity is represented by non-overlapping green and gray bars. Candidate b_2 indicates a likelihood for *rf-splitting* (when a known benchmark similarity mean significantly differs from a tested batch of logically claimed identical samples) and has the most significant dissimilarity.

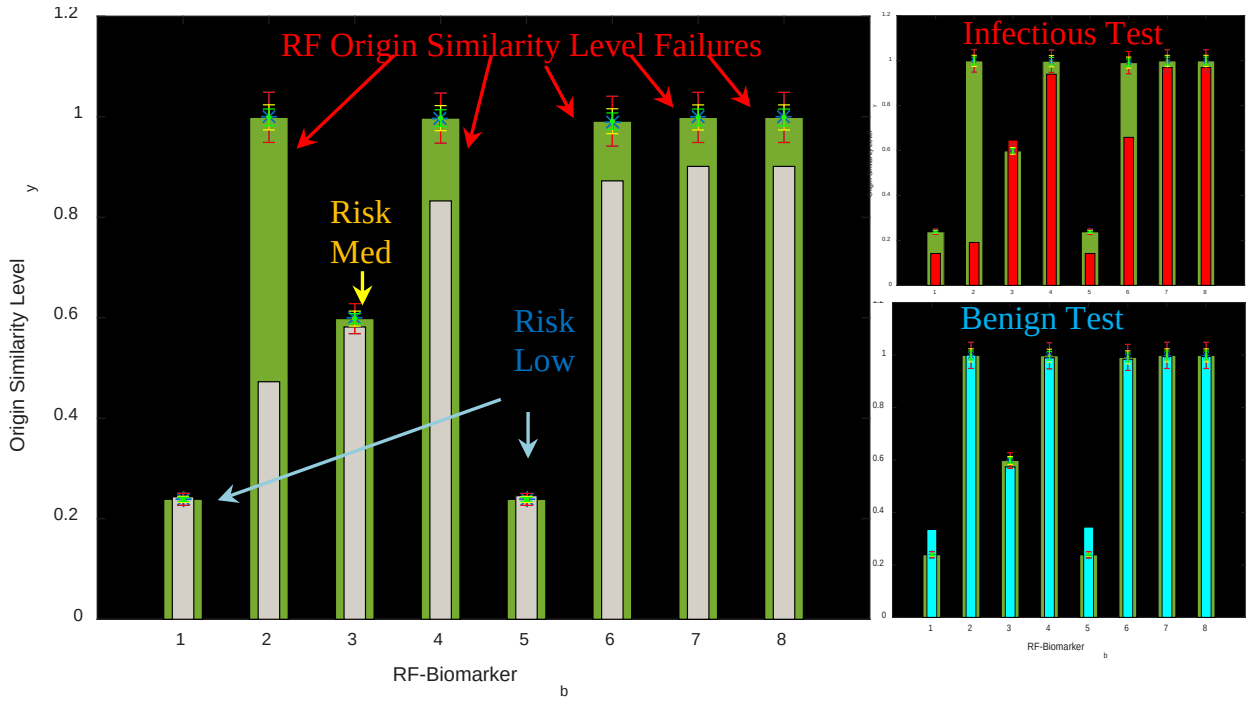


Figure 31. Diagnostic similarity of benchmark (green bars) vs. new (gray bars).

5.5 Chapter Conclusions and Future Work

This research finds diagnostic likelihood ratio statistics of (107.53 and 54.65 for positive ratios and 0.1009 and 0.1019 for negative tests) respectively for O_{dt} and Z_{dt}, which also had the best intrinsic accuracy and predictive accuracy before aggregation.

Result shows useful diagnostic capability in discriminating between the pathology of benign and infectious RF transmissions among the tested samples using statistical RF-Biomarker analysis. Before aggregation, conventional authentication specified fake credentials with 15.89% certainty. Moreover, the positive posterior estimates of 32.33% using conventional tests suffers from intrinsically high 84.11% false positive rates when logical-only (bit-level) authentication schemes are employed in RF threat prevalent environments. With the proposed method, the posterior predictive estimates for correct credential verification increase to 100%. Moreover, using the conventional authentication approach, the false discovery rate of *benign* credentials reduces from 67.67% to 0% using the proposed method. Given the results for diagnostic accuracy, we conclude that the log file of the RF authentication receiver is infected and an automated Level-3 policy response is imminent. Such a response manifests itself as a specific *network-disease* (e.g. denial of service) to all non-offending transmitters or concurrent ground-station users, which may be costly.

Given the prevalence of RF credential infection (forgeries) discovered among log files, we suggest a network-disease treatment plan be immediately implemented to mitigate the loss of critical resource availability. In the future, a more appropriate response may target the blocking of a specific RF origin. Specifically, a consideration of smaller log-file batch sizes or even a pulse by pulse diagnostic approach is feasible using the proposed diagnostic methods. The research proposal is recommended for infrastructure network applications that employ shared resource access from fixed wireless stations (e.g. fixed ground stations or power distribution nodes) to better understand and assess the pathological origin integrity of RF transmission origins in uncertainty. A consideration RF fingerprinting in multi-factor authentication schemes is very promising for network security augmentation.

VI. Research Conclusions

6.1 Research Summary

This dissertation advances network diagnostic utility methods to improve uplink access request authentication from fixed ground-stations through the application of multi-factor pairings of logical and physical RF credentials for origin integrity verification. An end-to-end physical RF network was demonstrated to verify the successful modulation and demodulation of four telecommands using software defined radios as a representative CubeSat network in a lab environment. The proposal was validated using Bayesian aggregation to combine the performance of uncertain diagnostic tests (i.e. failed to meet arbitrary policy threshold accuracy), to improve posterior RF origin integrity classification accuracy to satisfy arbitrary policy specifications. Finally, the discovery of *rf-splitting* of a main RF characteristic in electronic transmission log files, was introduced as a specific *RF-Biomarker* of *network-disease* (e.g. uplink shut-down or DOS) caused by the repeated acceptance of infectious (forgery) credentials. The overarching research questions this dissertation answers is:

RQ1: Can we enhance logical (digital) credential authentication schemes using pathological RF-DNA credential diagnostics of RF transmissions? Can useful RF fingerprint extractions from SATCOM networks improve uplink access authentication schemes? If so, can insights gained from these techniques be effectively imparted to cybersecurity key players? Can we enhance logical authentication mechanisms using statistical RF fingerprints pairings? Can RF fingerprinting methods improve uplink access availability for non-offenders in a shared resource operational ecosystem? Chapter I answers these questions by examining four more specific and distinct research questions that comprise Chapters II-V of this dissertation.

A summary of each chapter's research contributions follows. Chapter II argues that RF fingerprinting methods such as AFIT's RF-DNA fingerprinting of standardized fields (i.e. *preamble*), can be extended for any invariant and repeatable RF transmission unit size, so long as sufficient resources are available for useful processing. Chapter II answers the research question:

RQ2: Can non-standard regions of interest (ROIs) be used to develop statistically distinct RF fingerprint credentials from electronic device transmissions?

To accomplish this, the method applies modifications of AFIT's RF-DNA fingerprinting process to an entire invariant RF transmission region of interest for seven ICOM-9100 radios using a GMSK over FM pulse modulation scheme. Empirical results were collected using an X-310 SDR from AFIT's fixed ground-station transmission circuit during the summer of 2015. The same X-310 SDR receiver was used as the collections device for all ICOM RF fingerprint processing and classification. Authentication accuracy results show that using a 66% reduction of the standardized ROI, that acceptable levels of accuracy (greater than 90%) are achieved for an estimated SNR > 25dB (collected SNR was ~18dB). Non-standard customization is found to be promising for expressive policy specification of RF fingerprinting targets to support various organizational objectives. The effectiveness of the non-standard ROI selection approach is validated using three software-defined radios (SDRs) configured in a simple directed network configuration. It details an experiment performed with I-COM 9100 amateur radios where each radio is placed into a fixed transmission circuit and transmits an identical commands $n = 1000$ times. A specified RF-DNA collections device captures the entire pulse duration of the power spectral density emission and RF fingerprints were generated over the entire waveform as the ROI. Results provide validation that the RF fingerprinting of an entire RF pulse ROI is capable of producing statistically useful benchmark distributions of the RF features.

Given the length of the transmission pulse, the integration of RF fingerprinting in similar SATCOM networks is feasible for authentication augmentation.

Chapter III seeks to position the key insights gained from non-standard ROI selection using specified RF features in Chapter II and highlights the need for a proper definition of the phrase *RF-Biomarker* of *network-disease*—without obvious medical implications. Because the definition of common abnormal network outcomes as a result of successful network attacks (e.g. DDoS, loss of command and control (C2) of a critical resource asset). Because of multiple descriptive terms for RF-measurements as features, minutia detail, localization etc.… there is no standard set of terms which identifies any particular abnormal network behavior result. Because a robust definition does not exist, it is not clear whether the number of available features used in comparison or priori effectiveness of a diagnostic test can be assessed for cost of implementation unless exhaustive effort clearly defines the statistical significance of each RF-measurement. This chapter answers the research question:

RQ3: How does the diagnostic accuracy of ordinal, continuous, binary and Bayesian decision rules compare against conventional methods? How should threshold boundaries be determined? Can the concept of extracting RF fingerprints from non-standard ROIs be extended to entire fixed message fields to support a subset of critical commands used for small infrastructure networks? It does this by systematically developing RF signature benchmarks which improve posterior diagnostic classification using the top performing feature set (RF-Biomarkers) of an RF fingerprint feature that best dichotomizes benign vs infectious transmissions. An arbitrary policy is used to specify the levels of tolerance acceptance in noise of device specific benchmarks.

AN RF-DNA credential benchmark pairing contains local templates of trusted logical and physical RF attributes of authorized device transmissions in a specific authentication receiver's memory. The accuracy of a specified authentication device's local benchmark and is validated using representative truth reference (gold standard) which consists of new unseen logically equivalent transmissions that originate from *benign* (authorized transmission device) and *infectious* (unauthorized transmission device) origins. More specifically, three diagnostic classifiers are developed for RF fingerprint classification performance comparisons using binary, ordinal and continuous valued data. Decision rules are then developed to assess the overall Euclidean distance of new transmission origins using Gauss-Kronrod exact tolerance regions for simple binary classifications; to the benchmark templates. An assessment of available RF features are considered that best indicate *network-disease* as the feature-set of RF-Biomarkers. Results of gold standard testing show that a majority-vote diagnostic classifier and continuous risk zone weighting of custom diagnostic classifiers perform well against brute force discovery of the single best discriminator among available features.

It demonstrates how visualization of a diagnostic result can be used as a decision-support cue when its findings are statistically significant. Most beneficially, the LR statistic suggests the diagnostic performance is generalizable to additional RF device transmissions. Further, the ordinal and continuous valued tests outperform the baseline conventional logical-only authentication test which had a high false positive rate of over 84%. Based on the diagnostic performance from Chapter III, Chapter IV hones in on the challenge of indicating the true nature of an *insider* vs. *outsider* threat in threat prevalent ecosystems.

Chapter IV takes up the challenge of developing expressive insights into the pathology of RF transmissions by integrating multi-factor authentication as a way to classify the origin of RF transmission as more attributable to either an *insider* or *outsider* threat in prevalent ecosystems. It answers the research question:

RQ4: Can RF fingerprint evidence augment *insider* vs. *outsider* attribution without degrading conventional 2-State performance in uncertainty?

More specifically, a multifactor authentication framework was introduced which pairs logical (bit-level) and pathological (physical) credentials in trusted network access authentication schemes using Bayes Theorem. The method provides an expressive 4-state classification scheme that improves the accuracy of posterior estimates of new credential claims. Results show that combining physical RF transmission attributes as additional credential authentication factors (evidence) with logical CTMS authentication mechanisms enable expressive parameter-settings for dynamic threat mitigation. Such a method provides classification risk targets that aim to improve a user's ability to mitigate the risk of *infectious* credential acceptance. An abuse case demonstrated the integration of RF fingerprinting into a logical-only CTMS authentication scheme. With RF fingerprinting "ON" coupled with *insider* forgiveness settings, a con-man threat is still detectable at the same rate or better using the improved method of expressing 4-staes when compared to the conventional abuse case which only considers two states. Such classification state extensions enables user tracking of suspicious insider threat behavior. In addition, targeting a specific infectious transmitter using $Class - E$, provides expressive decision support for *insider* vs *outsider* threat attribution for enhanced mission support.

Finally, in Chapter V, attention is focused on applying the diagnostic usefulness of combined classifier performance against a con-man attack. Chapter V tackles the problem of rigorously characterizing the usefulness of RF fingerprint enhancement of logical mechanisms using a con-man abuse case from previous work. A decision to treat a network for *network-disease* is explored using the benchmark, gold standard and priori diagnostic performance. Arbitrary decision-rules and correlated thresholds are specified to assess the usefulness of aggregated diagnostic performance using a simple cost and benefit analysis for network treatment response recommendation. When classifiers fail to meet threshold requirements, Bayes Theorem is used to improve the posterior estimates. The chapter answers the research question:

RQ5: Are simple random log file screenings of claimed RF-DNA credentials useful in indicating earlier warning and preventative treatment options? What is the minimum screening size? When should treatment be given? What are the costs associated with treatment or non-treatment? Using the LR statistic to indicate diagnostic generalizable usefulness metric, O_{dt} and Z_{dt} diagnostic tests had the best intrinsic accuracy and predictive accuracy before Bayesian aggregation. This result suggests that ordinal and continuous decision-rule thresholding are useful in discriminating between benign and infectious RF transmission origins among tested samples. Before aggregation, logical-only credential authentication could specify a fake credential with 15.89% certainty. Moreover, the posterior estimates for credentials that tested authentic (positive) was correct 32.33% of the time, which is attributable to a high 84.22% FPR for the baseline test. Post Bayesian aggregation, we saw the posterior estimates increase to 100% correct classification, reducing the false positive error to 0%. Moreover, the FDR of *benign* credentials reduces from a 67.67% baseline to 0% using the aggregation method.

In summary, a quantitative study was conducted to help mitigate unintentional acceptance of forged network access credentials in non-benign electronic environments. Continued acceptance of forged credentials using conventional logical-only authentication, may lead to abnormal network behavior termed electronic *network-disease (eND).* The proposed eND treatment framework pairs logical and pathological RF attributes to improve diagnostic authentication schemes of claimed network credentials by;

- Improves discrimination of Insider vs. Outsider Threats
- Reduces conventional false positive rates by more than 84% and
- Recommends treatment responses in uncertainty up to 100% predictive accuracy
- Achieves generalizable likelihood ratios using ordinal and continuous valued decision-rules for diagnostic tests and posterior predictions of a subject's condition.
- Proposes RF-Biomarkers as standardized indicators of eND.

This research findings suggest that logical and pathological network access credential pairing <u>does</u> improve conventional authentication schemes in non-benign electronic RF environments.

There are six main research contributions:

1. Integrated trust management and RF fingerprinting concepts to improve authentication in uncertain RF network environments
2. Extended Interactive Trust algorithm to express insider vs. outsider threats
3. Developed generalizable diagnostic tests using RF-DNA localization
4. Demonstrated AFIT's 1st end-to-end multi-factor logical and pathological authentication network framework
5. Introduced RF-Biomarkers as a standardized indicator of abnormal electronic *network-disease* (eND)
6. Discovered RF-DNA Fingerprints for AFIT's CubeSat uplink signal and presented *rf-splitting* as an RF-Biomarker of eND

6.2 Future Work

There are at multiple natural directions for future research continuation. First, more research should be conducted to validate the current research findings among larger device sets and command combinations of RF-DNA benchmarks. Secondly, an investigative study of RF-DNA ontology development that includes a naming convention for RF-Biomarkers should be studied for to discover broader applications of RF fingerprinting techniques and indicators of electronic abnormalities. Thirdly, gold standard development that emphasizes the performance of the main RF characteristics and the central moments that are generated as RF fingerprint features should be investigated to identify the robustness of central moments vs. main characteristic measurements with respect to discriminability in noise. Those features that provide statistical significance should be targeted for RF-Biomarker standardization and implemented into network treatment response policy. More broadly, future research could examine the following questions:

FRQ: **Can an RF-DNA fingerprint bridge augment conventional authentication schemes to improve the origin integrity of full duplex RF transmissions between disparate network boundaries?**

In an RF fingerprinting bridging scheme, a policy-based RF credential pairing of logical and physical transmission attributes allows devices to artificially inherit the RF-DNA of its specified neighbors for the purpose of *self-evident* identification. The term *inherit* refers to the physical emplacement of localized RF-DNA credentials into the memory of bridge authenticating device. Such *inheritance* is accomplished prior to deployment of an electronic communications network with the aim of supporting policy requirements and objectives. When multiple uplink access attempts originate outside of a satellite's line-of-sight (LOS) receiving footprint and extends beyond P2P communications, a *chain-of-trust* is proposed.

Such a chain ensures that all intermediate devices forming the chain share the intermediate RF-DNA fingerprints of its authorized neighbors [81] as future research using *bridging* techniques. The objective of this future research proposal is to explore control boundaries of electronic network border crossings using paired credential exchanges through an RF-DNA *bridge* relay. In this effort, two or more distinct BiONets have some agreed upon desire to communicate between each other and have a policy that allows for such communication. The policy aims to apply RF-DNA fingerprinting and CTMS concepts in order to enable *self-evident* authentication to occur across network boundaries. In isolation, a disparate network that employs RF-DNA marker exchanges for their administered devices lack inherent self-evident credentials of external logical credentials from specified external devices and cannot effectively communicate. However, if both networks decide on a common device (bridge) in which to conduct controlled communication exchanges, then a bridge between the two networks can be constructed using two way RF-DNA fingerprint authentication paths. This implies that the chosen bridge must be fingerprinted and as such, the RF-DNA credentials of at least one of the adjacent BiONet's nodes must be emplaced in the bridges memory using the RF-DNA exchange algorithm described in Chapter V. Conversely, a subset of the authorized bridge's RF-DNA fingerprints must be emplaced in at least one of the adjacent network's designated bridge's memory for one-way authentication. Such an expressive policy lends itself to support multi-organizational cyberspace mission sharing collaboration in SATCOM ecosystems by enabling a more secure bridging of logically trusted networks.

Secondly, the discovery of statistically significant *rf-splitting* (suggesting RF origin dissimilarity), of an RF-Event's characteristic (e.g. RF-Measurement of its frequency response) suggests that evidence of unauthorized attempts can be easily obtained by log inspections. This future research would answer the question:

FRQ: **Can log file screening of fixed station RF transmissions apply RF fingerprinting to augment Cyberspace forensics?**

Specifically, this research would emphasize how the bridging of wireless authentication schemes between disparate (independent networks) boundaries can be augmented using RF fingerprinting techniques. Moreover, a cost benefit analysis can be conducted to provide insight to suggest best practices for when to conduct initial screening of existing logical-only authentication log files when infection is suspected. An in depth study can determine the likelihood of infection of *rf-splitting* discovery and the associated to a known occurrence of abnormal network behavior (*network-disease*). While current mitigation against network threats employ logical or bit-level authentication mechanisms, RF fingerprinting offer the opportunity to consider the physical attributes of distinct RF transmission sources. In an RF-DNA relaying bridge configuration, an electronic device may provide more secure interconnections between trusted network entities. An ability to track a chain of trust throughout the wide-area transport of an RF transmission's origin to its final destination for authentication would be useful to Cyber professionals and network security experts. Currently, bridging between disparate network boundaries employs conventional logical-only authentication mechanisms, which are vulnerable to SDR attacks. Therefore, researching methods to improve the next generation of infrastructure scale network bridges using RF fingerprinting could make a significant contribution in authentication scheme enhancement for the future of cybersecurity. Additionally, future research could focus on transmission circuit standardization of components. It could examine the question:

FRQ3: **Can fixed-station circuit design and command transmission standardization improve network defense and maintenance procedures?**

This research should focus on the standardization of fixed ground station transmission circuits. This path would further extend the capability accuracy in verification of RF fingerprint extractions from a known ground station circuits. Key areas to study include the generation of a database of transceiver fingerprints under various environmental conditions. A database lends itself to RF-DNA ontology development, transceiver benchmarking and profiling. Database analysis may contribute to better understanding of the effects of environmental factors such as temperature on RF-DNA fingerprints. An immediate impact could be realized from an understanding of changing a major circuit component and determining if a significant change exists in a known fingerprint. Another research effort may discover a process to incorporate concepts of naturalization, death-certificates and similar credentials using RF-DNA mechanisms. The factorial design of experiments focused pathway should include the process of fingerprinting known transceivers using CubeSat in their native operational ecosystems to compare and contrast structural or locality effects that may provide major circuit variations. Finally, a refinement of the circuit's design would be a logical next step towards the advanced study of EMI effects on policy-based RF-DNA marker exchanges. Here an exchange indicates that an authentication receiver has previously collected RF-DNA from the same source that it is authorized to transmit to.

Likewise, the transmission source has previously collected RF-DNA from the transmitting authentication device in the reverse path direction. When policy specifies such an exchange of information, the use of RF-DNA exchanges are implied. This does not mean that RF-DNA results that are collected from a specific receiver is simply transferred to some arbitrary secondary receiver. In preliminary trials, such erroneous misplacement of RF-DNA resulted in a loss ~10% classification accuracy.

ANNEX A: Towards an RF-DNA Marker Exchange Algorithm

A.1 Overview

This annex provides insight towards an RF-DNA Marker Exchange Algorithm for expressive biologically inspired network (BiONet) configuration policy. The algorithm takes in a set of distinct RF-DNA fingerprints previously collected for a multiple discriminate analysis maximum likelihood (MDA/ML) classification model $\boldsymbol{M}$ as its input. A collection of trusted point-to-point (P2P) link *authenticators* are produced as the output. For each *authenticator*, there exists at least one emplaced RF-DNA fingerprint credential of a trusted waveform source's (device) origin. Such emplacement enables *self-evident* authentication of a received waveform's origin to prevent unauthorized link crossings into a bit-level decision-support boundary. A physical-layer authentication mechanism employed by an *authenticator* improves the *confidentiality* of link origin transactions, eliminates anonymous boundary crossings and improves spacecraft *availability* for non-offending entities. Policy expressiveness allows for discrimination of waveform states generated by authorized devices, their users and associated privilege levels by protecting the *integrity* of link access. RF-DNA fingerprinting is employed to detect *self-evident* credentials of inherent physical features that are contained with a modulated waveform carrier.

A.2 Introduction

The basic social unit concept that describes inherent trust among family members are adapted to a BiONet configuration. In such a unit, children learn to understand and discriminate the voices of their parents from other adults even when all adults that speak the same logical message. Children are believed to possess an inherent level of trust of their parents and during transactions of life experiences these children ultimately possess an *inborn* level of trust for their parents and siblings that they would not otherwise have in a reputation-based scheme when dealing with strangers. When exchanges go awry between parent and child, a child is more likely to forgive a parent over a foreign adult. Although the genetics of children may not be the sole contribution towards forgiveness, it is generally known that children nurtured by natural parents tend to trust and forgive those adults more often. Inspired by such occurrences an adapted forgiveness factor $\boldsymbol{\Phi}$ for trust determination in a networking community is introduced.

Extending the biological nature of trust in a close community, this article presents an algorithm that produces a set of authenticators to control access into the network C2 boundary and eliminate anonymous (foreign) or unauthorized access to community resources. Eliminating unauthorized access is an acceptable risk for the purpose of maintaining link *availability* during outsider or more dangerously an insider *conman* attack. The fact that a user or device's interactions may be tracked makes this a feasible mitigation strategy for continued research. This article takes a concepts approach to algorithm development. The definitions are first explored to familiarize the reader with the purpose of a waveform carrier state. After the definitions brief examples are presented followed by informal proofs. The article concludes with a discussion of future research recommendations and physically-determined waveform state network applications.

A depiction of a biologically inspired electronic network (BiONet) using RF-Biomarkers to augment logical credential authentication claims appears in Figure 32. A network of four ground stations (R1, R2, R3 and R4] and four satellites [S1, S2, S3 and S4] are interconnected across Net1 (crosslink) Net2/3 (uplink/downlink) and Net4 (wired) communication links. As a BiONet, each device has been configured according to network policy such that a transmission source's RF-DNA of authorized command transmission fingerprints have been previously collected by a policy specified authentication receiver. During normal operation, the authenticating device extracts new RF fingerprints from incoming transmissions and conducts a diagnostic test on the origin similarity of the new RF-Event to its locally known RF-Event benchmark template. A diagnostic result of *benign* occurs when the new RF fingerprint meets acceptance levels of similarity. However an *infectious* result occurs when the RF origin similarity fails to meet benchmark similarity acceptance levels of the trusted RF origin source.

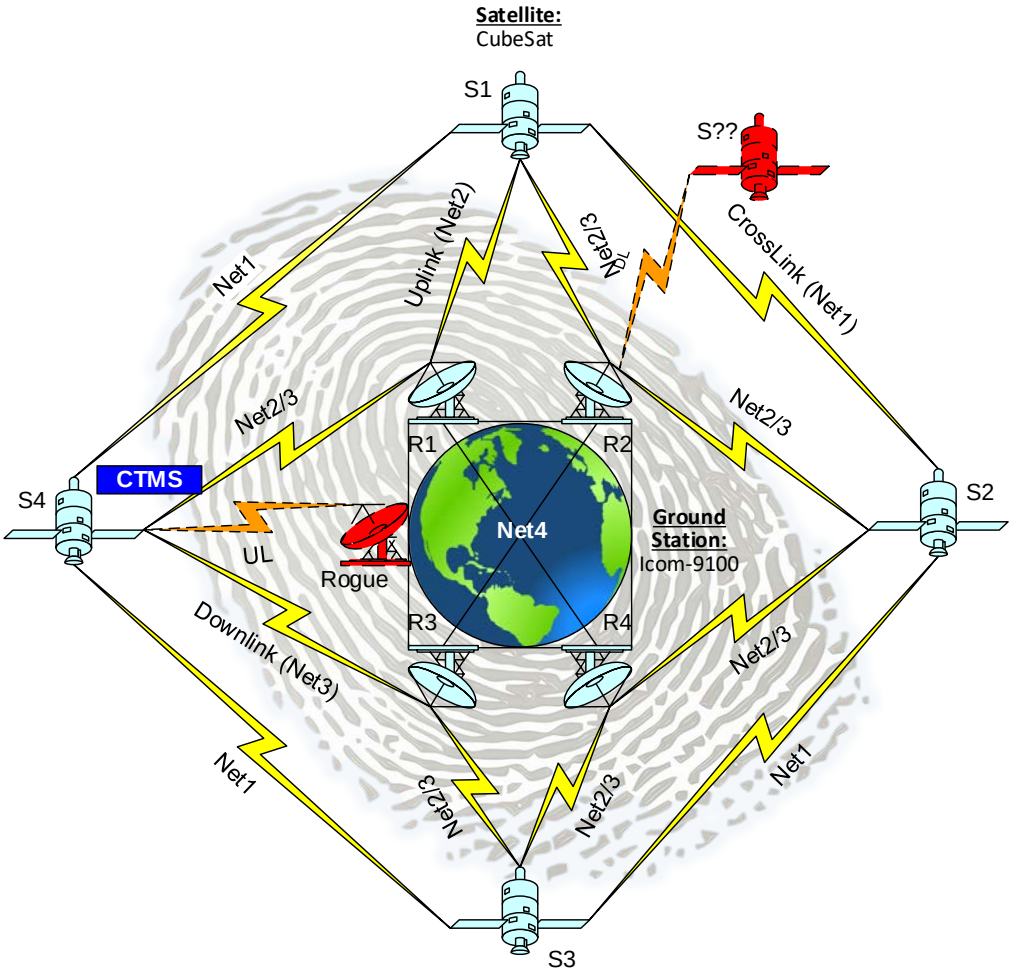


Figure 32. Electronic network access controls using trusted RF-DNA exchanges.

A.3 Methodology

Figure 33 is presented to provide a visualization of RF fingerprinting and policy development for effective emplacement in electronic authentication receivers. Policy p directs the collection of RF fingerprints from trusted devices and is provided as an input to the collections process as depicted in Figure 33a. The desired flow of information from transmission source (s) to authentication destination (d) is specified prior to RF fingerprint collection if necessary. After policy requirements are specified, the set of trusted devices are configured in authorized transmission states and their RF-DNA is extracted using pre-specified RF-Measurements and a designated authentication device which receives the RF transmissions as depicted in (Figure 33b). In order to detect an authorized RF fingerprint and make a comparison, reference fingerprints are simply preloaded or emplaced into every node as described by Rasmussen et. al in [25]. Following benchmark training, subsets of the extracted RF fingerprint samples are emplaced as physical RF attribute credentials (Figure 33c) into the physical local memory of the designated authentication receiver device $\boldsymbol{d}$ as previously defined in the policy specification of the desired flow over the $\boldsymbol{s \rightarrow d}$ communication path. In summary, a policy definition has previously determined the desired exchange of information between s and d for communication. To augment the origin integrity of the s→ d defined by p, the RF-DNA of s is collected by d for 1-to-1 verification in a simplex network configuration. When policy specifies full duplex communication between s and d, the set of RF-DNA collections are said to be *exchanged* between specified communication pairs.

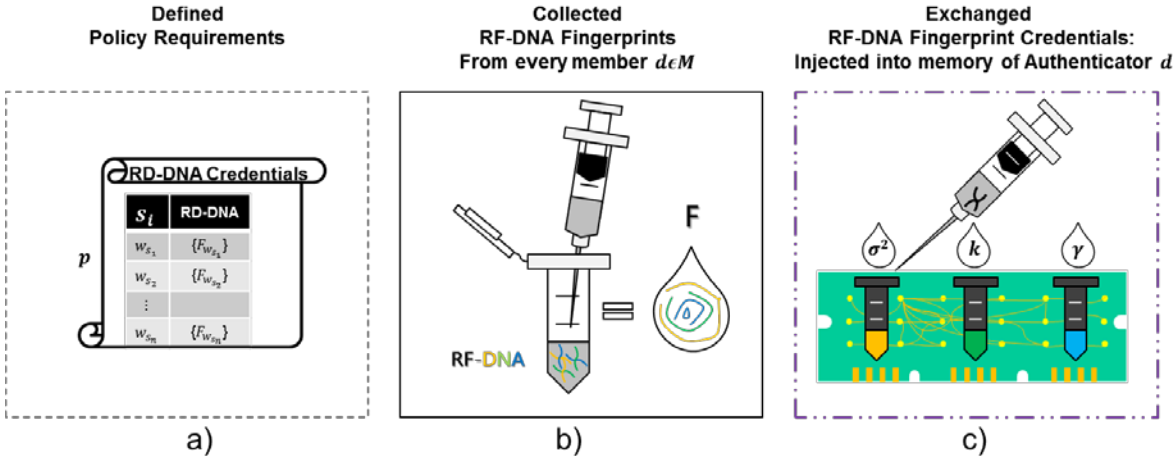


Figure 33. Policy to Extract and Emplace RF-DNA Fingerprints

Figure 34 depicts a graph G that describes bio-pairing paths. In Figure 34a nodes (1,2,3…n) are depicted as possible network transceivers; however there are no specified communication paths although the dashed lines may indicate desirable information flow. In Figure 34b node1 and node4 have two distinct path policy specifications. The first path policy, $\boldsymbol{p_1}\{node4, node1\}$ indicates that some waveform state from $\boldsymbol{s} = node1$ to $\boldsymbol{d} = node4$ exists for authorized communication.

Likewise, the second link $(d_4 \rightarrow s_1)$ specified by policy $\boldsymbol{p_2}$ indicates that some waveform state $\boldsymbol{w_s}$ from $\boldsymbol{s} = node4$ to $\boldsymbol{d} = node1$ exists. Figure 34b indicates that information exchange is one-way and the distinct paths exist between exactly one source and one destination node for the pairing. In Figure 34c, however we notice that each source device has a distinct path indication where the destination node is the same for all sources. In this case, node $\boldsymbol{d}$ functions as a typical hub receiver in a conventional hub-spoke topology network. Here, $\boldsymbol{d}$ is an authorized *authenticator* for each transmission source's generated waveforms. In Figure 34d the credential pairing $\boldsymbol{p}\{\boldsymbol{s}, d_1, d_2, d_3 \ldots d_n\}$ is given where node1 is functioning as the sole transmission source. This type of communication can be described for each distinct link or more traditionally as a broadcast network where each $\boldsymbol{d_n}$ functions as an *authenticator* of the *broadcast* waveforms received from origin $\boldsymbol{s}$. In each policy-based bio-pair each destination device has the additional capability that it can authenticate the received transmission of its sourced partner. In these examples of Figure 34, $\boldsymbol{d_n}$ possesses *self-evident* RF-DNA fingerprint markers of $\boldsymbol{s}$ and can authenticate specified waveforms origins received using such credentials. For all cases, $\boldsymbol{s} \neq \boldsymbol{d}$.

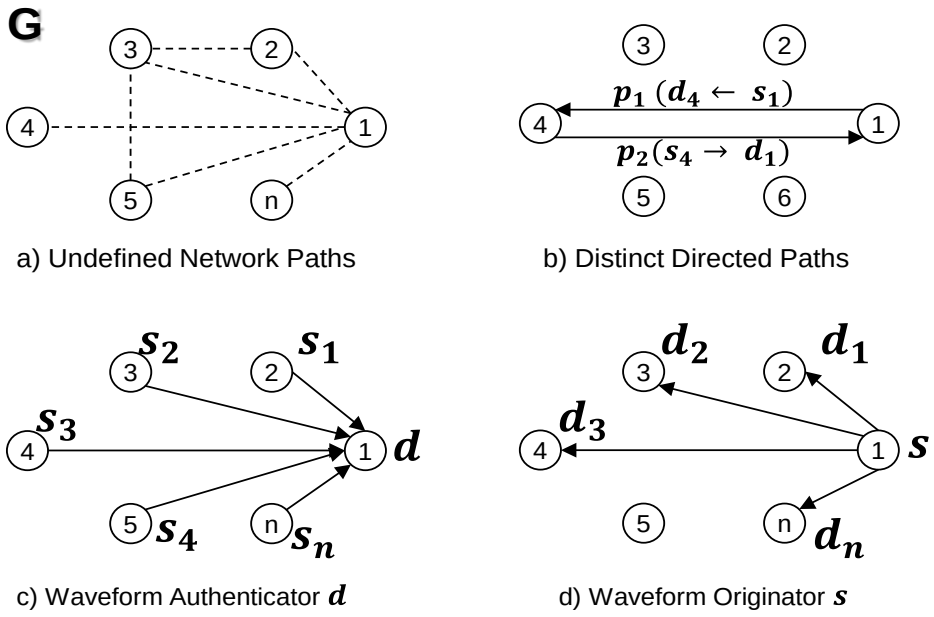


Figure 34. Directed Waveform Origin Bio-Paths

- **A.3.1 Model Definitions.**

By exchanging validated RF-DNA credentials between specified device members, a networked electronic community is capable of recognizing authentic transactions due to an inborn level of trust (*self-evident*) that is contained within an authenticator's local memory. During normal operations, *d listens* for an incoming authorized state of waveform *w* from $\boldsymbol{s}$ that is transmitted over a wireless uplink $\boldsymbol{l}$ using a standardized modulation protocol. Conventionally, after detecting an authorized *w*, the receiving device *d* proceeds to demodulate the carrier and decode a bit-level message *m* for network-layer authentication. The physical origin integrity of *w* is not considered in the conventional approach.

- **A.3.2 Definition-1: Waveform Properties**

Using AFIT's RF-DNA fingerprinting methodology [52] and adapting Dr. Cobb's concept of an *intrinsic* physical layer [4] approach to circuit authentication, four desirable properties of a waveform carrier emerge. The first property suggests that the analog waveform which carries the elusive RF-DNA fingerprint marker must be naturally generated by a distinct origin source. A waveform could originate from a mobile device, stand-alone radio transceiver or a more complex transmission circuit containing multiple subcomponents. The source influences the RF-DNA fingerprint result and must remain distinct from all other sources during natural waveform event generation as the initial *Property-1*. Using a transceiver may also function as a system component in a complex system that employs a TNC, PC, software defined radio (SDR) power amplifiers and the like for ground stations. Previous research has shown that changing out a critical component a circuit's transmitter or receiver may adversely affect the reproduction of and detectability of a statistically significant match for RF-DNA fingerprints. These findings highly imply that circuits remain consistent throughout authorized waveform event generations in order to meet policy objectives.

Table 29: Desirable Properties of Unique Waveform Origin Integrity Features

Desired	***Description***
Property-1:	An original waveform event must be **natural** (i.e. analog or continuous) in its immediate existence in time and space rather than existing as a derived logical (e.g. binary or digital) interpretation.
Property-2:	Specified feature attributes of the event must be **inherent** among similar waveform emission types (e.g. Type III frequency generating transmitters [77].
Property-3:	The extractable features of waveform generating circuits must be repeatable and **evident** from the occurrence of the natural event stimuli**.**
Property-4:	A sample obtained from the waveform event must provide evidence that its features are **statistically significant** to support known and consistent event feature measurements.

As a second desirable property, the physical attributes of the original waveform must be inherent among all similar emissions (e.g. emissions made in the ultra-high frequency range). A third desirable property (*Property-3*) calls for the repeatability of a generated waveform event such that a statistical RF-DNA fingerprint match can be made during waveform marker extractions. *Property-4's* desired waveform properties to contain some agreed up unit of measuring the event such that the manner of measurement is quantifiable and sufficient to describe the event occurrence. An extracted fingerprint sample must be usable as credentialing evidence if a consistent and statistically unique result exists. *Property-4* is desired to provide the evidence of a statistical comparison. A summary of these desirable properties are provided in Table 13 below [4] [3].

- **A.3.3 Definition-2: Waveform State**

The term *state* is used to refer to the circuit configurations of a man-made waveform generator assumes to reproduce such an event. The authorized waveform states that can be generated by trusted circuit origins are provided in Table 4. On the left, the level indicates the generalization for use that a particular waveform could be applied towards device discrimination.

A Level-1 waveform is a circuit that generates a waveform and has as its fingerprinted ROI as a standardized marker such as a *preamble*, *midamble* or *postamble* region of the standardized modulation scheme. Using standardized ROIs provide consistent discriminability since normal communications require the specified modulation scheme for effective communication. Integrating a Level-1 ROI has a low level of complexity for network configurations; however the storage size of a constant region may be too costly for receiver storage and real-time processing limitations. As the level increases for an authorized waveform generation state, the complexity generally increases while the storage requirements generally decrease. At the bottom of Table 30 we see that Level-5 waveform states have a combination of customized ROIs that extract standard regions and non-standard portions of waveform regions as they are generated. These multi-custom ROIs have a high level of complexity, but may yield the smallest storage size requirement for RF-DNA credential verification at the receiving device.

Table 30. Authorized Waveform States for RF-DNA

Level	**Auth States**	*ROI*	*Example*	*Complexity*	*Storage Size*
0	w_0	Baseband SOI	Full Waveform Env Replay	Low	High
1	w_1	Standard	Preamble	Low	High
2	w_2	Custom Standard	Varied Start/Stop of Preamble	Low	Medium
3	w_3	Non-Standard	DeviceID Field	Medium	Medium
4	w_4	Custom Non-Standard	Varied Field Sampling	Medium	Low
⋮	⋮				
s	w_s	Multi-Combination	Custom Preamble & Custom Field	High	Low

- **A.3.4 Definition-3: Waveform Classifications.**

The possible classification determinations adapted from AFIT's RF-DNA fingerprinting process can be made by d upon detection of w as follows; 1.) **Identity Class**: Does message m contain RF-DNA from w_s as claimed by $\boldsymbol{s}$. 2.) **Membership Class**: If w_s's RF-DNA fingerprint matches a member s of M. 3.) **Unknown Class**: If neither identity nor membership of $\boldsymbol{s}$ can be determined. These waveform classification types used for origin authentication are summarized in Table 31. Type I classifications are generally desired.

Table 31. Waveform Classification Types

Classification Type	*Name*
I	Identity
II	Membership
III	Unknown

- **A.3.5 Defintion-3: Region of Interest Index Markers.**

The use of an ROI indexing marker ($\boldsymbol{iMkr}$) is introduced to send either in-band or out-of-band information that may include the ROI's specified start and stop points for fingerprint extraction or a *key* sequence number for synchronization. Prior to network operations, it is assumed that RF-DNA fingerprints have been collected for model $\boldsymbol{M}$.

In $\boldsymbol{M}$, all authorized waveform states have been fingerprinted for each distinct combination of device, user and privilege level combinations. The collected fingerprint results are then considered for RF-DNA exchanges which support the communication path specifications of requirements of policy $\boldsymbol{p}$. After receipt of $\boldsymbol{p}$, a network graph $\boldsymbol{G}$ is configured to support the desired outcome for authenticated information flow using *physically-determined* RF-DNA fingerprint markers as waveform origin credentials. That is to say, for each authenticator device designated as a path receiver $\boldsymbol{d_n}$; the physical memory of $\boldsymbol{d_n}$ is modified such that there exists sufficient RF-DNA fingerprint credentials. Such preplaced credentials, when compared to extracted RF-DNA fingerprint samples received from source $\boldsymbol{s}$, yields a **statistically significant** waveform origin integrity classification result.

Any standardized waveform carrier that contains a baseband equivalent signal $\boldsymbol{m}$ (e.g. 000111) may be emitted along an ultra-high frequency (UHF) communications path as a possible waveform W state generated by some circuit. The acceptance or rejection of $\boldsymbol{m}$ is a function of $\boldsymbol{p}$, such that only authorized states (w_s) are considered for comparison and acceptance by Rx. In this contrivance, artificial RF-DNA *transfusions* are conducted such that $\boldsymbol{d}$ receives the RF-DNA of a trusted donor source (circuit). If such a donation is acceptable (RF-Biomarker levels match) for $\boldsymbol{d}$, then future exposure of the donated samples are recognized by $\boldsymbol{d}$ as if it naturally existed. This novice concept enables the transfusion of said physically-determined RF-DNA fingerprints collected previously from trusted circuits and subsequently emplaced into the physical memory of a designated Rx authenticator device $\boldsymbol{d}$, which is assumed to be secure in as defined by policy according to [57].

- **A.3.6 Definition-4: BiONet.**

A Biologically inspired network (BiONet) is a collection of electronic entities which share one or more *self-evident* origin integrity credentials learned from an authorized transmission source(s). Artificial transfusions of RF-DNA fingerprint credentials are exchanged between members to form a coherent network of communication devices according to $\boldsymbol{p}$. The network's boundaries are controlled by designated Rx authenticators of transmission circuit origins. The term self-evident is defined in section 5.3.11 in more detail.

- **A.3.7 Definition-5: Self-Evident Markers.**

A self-evident marker is defined as an event characteristic that presents a feature that describes the event's occurrence without a need for additional interpretation. A receiver $\boldsymbol{d}$ owns *self-evident* credentials for identity $\boldsymbol{s}$ when all desirable properties of Table 13 are met and a statistical RF-DNA fingerprint credential from a trusted waveform state $\boldsymbol{w_s}$ are found within the memory resources of $\boldsymbol{d}$. This implies that RF-DNA fingerprints are emplaced before authorized communication occurs between devices. A specified policy $\boldsymbol{p}$ between ($\boldsymbol{s \rightarrow d}$) must exist for link $\boldsymbol{l}$ to support a claim of $\boldsymbol{s}$'s apparent waveform classification of Table 31.

- **A.3.8 Message Credential Authentication Schemes**

A.3.8.1 Message Credential Identification

A typical message (m) contains invariant fields used to logically identify network devices in a specified network. Let, ID_k represent a sequence of bits {0110…} represent the bit level identification field used to encode the **k**th credential to authenticate message m as

$$c_k^{BIN} = \{0110 \ldots\} = ID_k \tag{13}$$

Consider Simmons's well-known A-Code authentication scheme involving three electronic circuits (participants) a transmitter (Tx_s), a designated receiver (Rx_d) authenticator and some arbitrary opponent Tx_{oPP} [82]. Circuit Tx_scommunicates information in accordance with some trusted policy-based pairing p, which specifies a set of repeatable binary bit sequences. Such authorization of circuit transmission states enables the generation of repeatable and observable RF-Events for receiver Rx_d's authentication. In order to deceive authenticator Rx_d, Tx_{oPP} tampers with or impersonates either the logical or physical components of the bits, which are included in the RF-Event containing m and emitted by Tx_s. Conventionally, such an impersonation attack of logical attributes, as observed by Rx_d (at the bit-level) may appear as an authentic message $m_j \in M$ at the bit-level for a given decoded RF-Event sequence. Unfortunately, the modifications of the physical attributes may remain undetectable if d filters such information as useless in its determination of a binary '0' or '1' during decoding.

Denote the set of all possible circuit source states authorized in 0 by $\{W\}$. A front-end transmission device Tx_s may modulate a message m toward Rx_d along l. When Tx_s modulates a specified m_{ij} onto its RF circuit carrier the resulting RF-Event generation is visualized as an analog waveform $'\boldsymbol{w_i}'$. Adapting Bishop's definition, a security policy (p_i) is a statement that partitions W into mutually exclusive *authorized (*i.e. *secure)* or *unauthorized (i.e. non-secure)* circuit source states [62]. Where t is the time in which the RF-Event sampling from the **r**th region of interest occurs during message receipt and demodulation of m. A hierarchical pairing of credentials of m_{ij} carried within $\boldsymbol{w_s}$ may provide layered support to the multi-factor authentication model (e.g. OSI or DOD model) shown in Figure 22.

A.3.8.2 Policy Specification

Let network policy p_i specify the **n**th pairing of the **k**th logical and physical credentials of the RF-Event containing m. Such a policy specifies a circuit's front-end device Tx_s as its circuit's encoder where the transmission of m can be decoded by $Rx_d$for validating the authenticity of m. For each logical credential c_k^{BIN} used for message authentication [82] there is an associated **k**th physical c_k^{PHY}credential to support the origin integrity claims of $\boldsymbol{w_s}$ using RF-Biomarkers. More generally, let the set $\{P\}$ of network security policies specify a source to destination ($s \rightarrow d$) pairing of logical and physical credentials of all messages $\{M\}$ for a hierarchical network model from is

$$p_i(m_{ij})_l = \{c_k^{BIN}, c_k^{PHY}\}_l. \tag{14}$$

Where p_i is the **p**th security policy for the $\boldsymbol{l}$th layer of the network model in which the authenticity of the **k**th logical credential for the **c**th commands authentication scheme's utilization. On the left, p defines a trusted waveform state (T1) to authenticate the origin integrity of an RF-Event. On the right, a network-layer authentication scheme employs a bit-level authentication scheme to validate the binary message content. When combined, the physical layer mechanism can enhance the integrity of a message m as well as confidentiality. An assumption that the signal to noise ratio (SNR) is sufficient for RF-DNA mechanism detection and employment for acceptable (True or False) performance. The green bar on the left indicates the *start* point of the sampling ROI, whereas the red bar indicates the sampling ROI *stop* point. When the start and stop points match a standardized modulation scheme, are called termed *preamble*, *midamble* or *postamble* regions.

The combination of the start and stop sampling locations of an ROI are referred to as the $iMkr$. The $iMkr$ key provides the start and stop points for RF-Event sampling.

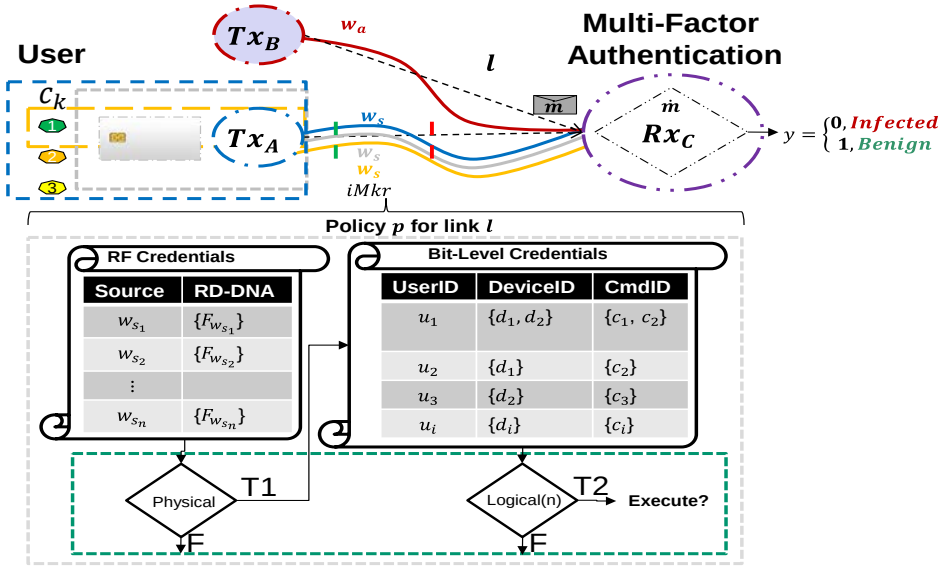


Figure 35. Multifactor Authentication Using Pathological Evidence

The Logical Network Configuration of a trusted source ($s_i = Tx_A$) transmitting a message to d in a wireless RF network environment. Additionally, an untrusted source ($s_a = Tx_B$) is also capable of transmitting a message m to d that is logically equivalent to the modulated bits transmitted by s_1. Upon receipt of an RF-Event (w_s) authenticator $d = Rx_C$ must decide if the origin of the claimed identity associated with m is authentic or not. If d decides based on logical credential authentication alone, the origin integrity is uncertain. If the pathology of RF-Biomarker levels is acceptable for a claimed message and the logical credential is valid, then d authenticates the origin integrity of s_i for uplink access. The pre-authorization, generation and collection of RF fingerprints allows for future pairings of credential authentication schemes. Adapting Bishop's definition, a *security policy* (p_i) is a statement that partitions all possible circuit generating RF transmission states into a set of *authorized (*i.e. *secure)* and *unauthorized (i.e. non-secure)* states [62]. Authorized waveform transmission events inherently carry the trusted RF-DNA fingerprint markers and are generated by s and transmitted to d for origin integrity validation. When p_i specifies a set of authorized circuit transmission states, the resulting secure transmitted waveform events are distinguishable from all other possible events. The set of secure circuit generating RF-Event states are

$$\boldsymbol{w_s}(t) \subseteq w_i\,(t) \;\; where\; i\colon 1,2,\dots s,(s+1),(s+2),\dots(s+i),i. \tag{15}$$

A.3.8.3 RF-Event Generation from Trusted Origins

A simple analogue FM circuit modulates a baseband information signal ($\boldsymbol{s_i}$) onto a fixed sinusoidal carrier wave ($\boldsymbol{c_t}$) and transmits a modulated waveforms w_i as output. A subset of authorized baseband signals are transmitted through a fixed state modulation circuit, producing a trusted complex waveform state as output (w_s). Where $\boldsymbol{w_s}$ is a repeatable modulated waveform state generated by a fixed transmission circuit $c(t)$.

Let $s_s(t)$ represent the trusted subset of input baseband signals into a sinusoidal FM modulator as described by Stewart et al [83]. A single baseband input analog signal with an amplitude A_i and a frequencyf_i is

$$s_i\,(t) = A_i\,cos(2\pi f_i t) = A_i\,cos(\omega_i t) \tag{16}$$

where $\omega_i = 2\pi f_i$. When there is no present input baseband signal, the FM modulated carrier output of a single component with amplitude A_0 and a frequencyf_0 takes the form

$$c\,(t) = A_0\,cos\big(2\pi f_0 t + \hat{\theta}(t)\,\big). \tag{17}$$

Integrating the product of the input baseband signal and a modulation constant k_0 into an FM modulation transmitter, the instantaneous phase (IP) of the generated FM waveform output is determined by:

$$\hat{\theta}(t) = 2\pi K f_m * \sum_{-\infty}^{t} s_i(t) \tag{18}$$

Where K is the gain. As the baseband signal arrives at the circuit for integration, a frequency deviation occurs as sinusoidal terms on either side of the carrier frequency. This deviation is known as the modulation index (H). As a present baseband signal modulates onto $c(t)$ through a fixed FM circuit**,** the phase (effective frequency) of the carrier waveform modifies in response to the amplitude variations of $s_i\,(t)$ according to H. A repeatable FM modulated waveform signal event w_i, using the carrier's amplitude and frequency given by A_c and f_c becomes;

$$w_i\,(t) = A_c\,cos\left(\omega_c t\; +\; H_{fm}\,sin(\omega_i t)\right). \tag{19}$$

Given K and f_c the instantaneous frequency (I_f) is obtained with;

$$I_{f\ w_i} = f_c\; +\; K_{fm} s_i(t)\;Hz. \tag{20}$$

A.3.8.4 Statistical RF-Biomarker Generation

A component RF-biomarker has three major parts, its distribution of RF-measurements collected during profiling, a histogram for graphic visualization and a confidence interval of all acceptable RF measurement values collected (observed) from Tx_s. For each RF-biomarker, a statistical measurement of the full-wave's real and imaginary parts to include any sub-region's real and imaginary parts. This vector of RF-measurements comprises values of independent receiver observations of specified RF-Events.

The stored signature of an RF-biomarker contains a distribution of trained observations of $\boldsymbol{w_s}$. The probability density function pdf estimates occur using the distribution of each Tx_s device. An arbitrary RF measurement $(\star_m)$ indicates the mth measurement occurrence across a fixed time/space of received RF-Events. While, not all RF-biomarkers from an RF-DNA fingerprint may be necessary for accurate comparison, a single indicator alone may not be sufficient for optimal classification of fixed circuit-based encoding rules from [39] [42].

To support the goals of p_i, a decision rule determines the point of partition for acceptance levels for a given RF-biomarker. All RF-Biomarkers that fall short of the decision-rule receive a classification of *infectious*, while all acceptable ones are *benign*. When a credential claim is *benign*, the logical credential (matched bits) claim is recommended as originating from an authentic source, however an *infectious* (deficient levels of benchmark similarity exist in the claimed RF-event) diagnosis indicates a fake credential and recommends a high level of risk for accepting the contents as original.

For every repeatable RF-Event of interest generated from (15), the capture of instantaneous response features retains the waveform's unique I/Q values. The $IMkr$'s specification of sampling for ROI start and stop points assist in receiver identification of w_s. For n-samples, a division of nth ROI sample into N_R equal length contiguous sub-regions plus itself occurs to yield $(N_R + 1)$ total regions for each device's fingerprint generation. Four statistical RF measurements occur for each characteristic of interest. The features include the variance (σ^2), standard deviation (σ), skewness (γ) and kurtosis (κ). The first central moment (arithmetic mean) provides the expected value or mean (μ_1) of a distribution or average center value. The second central moment of a distribution is the variance and gives a measure of how the individual n samples of a population X distributes around the mean μ_1. The standard deviation σ is the positive square root of σ^2. The γ statistic provides a measure of symmetrical similarity of the pdf as the third central moment, while κ (fourth central moment) measures the peak or flatness of a probability distribution function (pdf) [4] [14] [44]. Assuming a Gaussian pdf, let μ_i denote the ith central moment of a random variable X as the vector $\{x(n)\}$, where each central moment's statistic of the pdf can be found by:

$$\mu_2 = \sigma^2 = \frac{1}{N_x}\sum_{n=1}^{N_x}(\bar{x}_c(n) - \mu_1)^2 \,, \tag{21}$$

$$\mu_3 = \gamma = \frac{1}{N_x\sigma^3}\sum_{n=1}^{N_x}(\bar{x}_c(n) - \mu_1)^3 = \frac{\mu_3}{(\mu_2)^{3/2}} \,, \tag{22}$$

and

$$\mu_4 = \kappa = \frac{1}{N_x\sigma^4}\sum_{n=1}^{N_x}(\bar{x}_c(n) - \mu_1)^4 = \frac{\mu_4}{\mu_2^2} \,, \tag{23}$$

where $i = 1,2,3, \ldots N_R + 1$.

The concatenation of central moment statistics form a regional distinct native attribute marker as a vector for each sub-region from the RF-Event's localized ROI as:

$$F_{R_i} = \begin{bmatrix} \sigma R_i \\ \sigma^2 R_i \\ \gamma R_i \\ \kappa R_i \end{bmatrix}. \tag{24}$$

A composite characteristic vector is formed from the Further concatenation of the RF-DNA marker vectors obtained from (24) forms a composite characteristic vector of each selected feature's characteristic response (i.e., A, θ, f) as:

$$F^C = \left[FR_1 \vdots FR_2 \vdots FR_3 \dots FR_{N_R+1}\right]_{1\times 4(N_R+1)}. \quad (25)$$

After selecting the desired number of statistical response features, number of sub-regions and the composite characteristic vectors from (25), a final statistical fingerprint vector construction becomes

$$F^C = [F^{c_1} \vdots F^{c_2} \vdots F^{c_3} \dots \vdots F^{c_b}]_{1\times 4(N_R+1)\times 3}, \quad (26)$$

where b=Total Number of component RF-Biomarker features contained in the composite fingerprint vector.

In (26) above, the composite characteristic vector c_1, c_2 and c_3 represent the selected amplitude, phase and frequency characteristics of the transmitter's full (real and imaginary parts) times series power spectral density that may be used to visualize the RF-Event as a waveform. In conventional waveform analysis of interoperable communication networks, the goal is to ensure that logical interpretations of transmissions receipts occur at the bit-level. This method of analysis typically discards localized physical dissimilarities that may exist in device specific emissions in favor of a more global discrimination approach to distinguish between a binary '1' and '0' to support interoperability and standardization goals.

Where, $c_k^{\text{BIN}} = \text{n} - \text{bits of length L, } s.t.\ n = 0\ or\ 1$ and $c_k^{\text{PHY}}$is a 2-tuple vector of policy-based RF-measurements. Using time series analysis of the RF-Event, Rx_d observes the policy-based message authentication credentials $\left[c_k^{\text{PHY}}\right]$ after receiving a claimed instance of w_s using $\star_m$ across ROI r to support authenticity claims.

$$c_k^{PHY} \xrightarrow{yields} \vec{v}_r. \quad (27)$$

The resulting vector from (27) represents the RF-Biomarkers contained within a received RF-Event w_s as observed by Rx_d. Where $r = \{1,2, \dots j\}$ is the jth sub region of interest from w_s. For each c_k^{BIN}, we extract a complex valued RF-DNA fingerprint from a specified region of interest (ROI) designated by the **r**th region of a claimed RF-Event $\boldsymbol{w_i}$. The **m**th $\star$ measurement of *r* objectively computes the RF-DNA statistics. Since we assume that each e_{Tx_s} is physically distinct during the generation of w_s, we obtain trusted physical *credentials* $\left(c_k^{\text{PHY}}\right)$ for a given c_k^{BIN}, using RF-measurement $\star_m$ to extract RF fingeprrints from $\boldsymbol{w_s}$ as observable by Rx_d.

Where $\star_m$ represents the $\boldsymbol{m}$th "RF-measurement" of a sampled waveform's w_s $\boldsymbol{r}$th region of interest (ROI) over the time (t) interval from a to b. Let a and b represent the start and stop time duration of r as observed by Rx_d. Notice, the $\star_m$ measurement occurs prior to processing of the decoded bit-sequence of $\boldsymbol{w_s}$, but may be conducted in parallel to reveal the contents of m after demodulation using similar techniques. This expression for d's RF-measurement of an incoming RF-event for w_i is

$$Rx_d[\star_m (w_s)_r]_n \xrightarrow{yields} [c_k^{BIN}, c_k^{PHY}]_n. \quad (28)$$

- **A.3.9 Device Specific Encoding Rule Signature Development for Verification**

A.3.9.1 Device-based Encoding Rule

Consider a circuit that is capable of transmitting two of three command messages to Rx_d. Let s_1 = the authorized source circuit state that generates a baseband message to represent command-1 $(c_{k=1})$. Using some fixed bit-sequence ID field, we select Tx_s as the front-end circuit encoder for the authorized carrier source state to Rx_d. In order to protect against attacks from Tx_{oPP}, w_s is encoded using one and only one front end device as the primary circuit state encoding rule. Let $\{E\}$ denote the set of all circuit encoding rules of m where $m \subseteq M$ is much greater than W. A device-based fixed circuit source state encoding rule $e_{Tx_s} \in E$ provides a 1-to-1 mapping from W to M. The range of $e_{Tx_s}(W)$ generated by Tx_s consists of a subset of M that possesses RF-DNA markings of its original source. Prior to transmission, policy p_i specifies the circuit encoding rule e_{Tx_s}, collection of RF measurements and storage of signatures into the memory of Rx_d. Given p_i, w_{s_i}, e_{Tx_s} and Rx_d, we define a circuit source state's RF encoding rule for trusted command messages as;

$$e_{Tx_i}(w_s, m_{is}) \rightarrow (c_k)_{is} \quad (29)$$

Where e_{Tx_s} is the ***s***th transmission device used as the circuit encoding rule, w_s is the device's ***s***th circuit transmission state. The modulated message m_{is} is the ***i***th circuit source state encoding rule of the ***s***th transmission device. The resulting ***k***th command contains the extractable RF fingerprint evidence of the ***m***th message for verification support by the ***d***th authenticator device Rx_d. Repeating (29) to generate RF-Events n-times enables device specific benchmarking of policy-based transmission events. Such encoding using a specified device lends itself to more reliable learning of the physical RF characteristics associated with 'how' Tx_A emits transmissions as observable by Rx_C.

A.3.9.2 Device-Specific Decoding Rule

We now focus on defining a decoding procedure of RF-Events to reveal the logical and physical informational content of $m's$ claimed credentials by a specified authenticator device Rx_d. In general Rx_d observations of RF-DNA fingerprints from a specified transmitter are statistically independent from all other receivers Rx_i. Upon receipt of a new RF-Event w_i, Rx_d tests if m_{ij} appears in the authorized range $e_{Tx_s}(W)$ using some decision-rule or threshold policy. If so, m's chances of acceptance may increase, otherwise m_{ij} rejects additional command processing. Rx_d We assume Tx_{oPP} has perfect knowledge of the communication system, including all devices used to encode the circuit states.

However, Tx_{oPP} does is unaware of any inherent secret RF-DNA characteristics that a source circuit employs as a natural signature encoding rule known by the $s \rightarrow d$ pairing of Tx_s and Rx_d. Tx_{oPP} may succeed in spoofing if and only if the RF-DNA fingerprint indicators of m_{ij} match the fingerprints of previously agreed upon circuit state encodings used prior to communication. The subspace of valid messages as observed by authenticator Rx_d, is unique for each device, however a receiver's ability to sample a continuous RF-Event is imprecise and

therefore there are no perfect matches. A tolerance interval may be effective in mitigating this imperfection. Generally, any logical (digital) command can be decoded using localized RF component features when a policy has specified the communication source to destination path. We state this more formally as;

$$f_{Rx_d}\left((c_k, m_{is}) \rightarrow w_{is}\right) = e_{Tx_i}. \quad (30)$$

Where p_i specifies f_{Rx_d} as an authorized authenticator/observer of RF-Event w_s generated by device encoding rule e_{Tx_s}. By discarding, or failure to consider useful physical RF evidence, it is possible for Rx_d to accept m as authentic using the logical bit-level credentials only. Again, RF-Events having originated from an untrusted source, a classification of 'authentic' occur when logical credentials match. To see this, select any arbitrary receiver of m_{ij} which employs conventional protocols to decode (29) to obtain the **k**th logical bit-level command $m_{ij} \mapsto \left(c_{ij}\right)_k = c_k^{BIN}$ without regard to the associated physical RF-DNA of e_{Tx_s}. Due to high demands for interoperability, there may be multiple instances of RF-events generating sources which generate m that maps to the correct logical interpretations of command c's logical (bits) credentials. As an example, consider of mapping of $e = 3$ interoperable encoding devices that can transmit in only three authorized circuit source states $\boldsymbol{w_s}$ where $s = 3$. We have $e^s = 9$ statistically unique messages are generated using the circuit source encodings to produce three logically equivalent commands that can be decoded by Rx_d. The state of the circuit during transmission of m can originate from a single source or from multiple sources so long as they are physically distinct with respect to the final baseband signal modulation of the circuit's RF carrier. The probability of correctly guessing the AuthCount filed in Duncan's work was 1/1000, which may be detectable in as few as 65 attempts using the CTMS.

Example: When $\boldsymbol{Tx_3 = e_{Tx_3}}$ encoding rule is used to encode circuit state $\boldsymbol{w_3}$, a unique message $\boldsymbol{m_{33}}$ is produced that is logically decodable by $\boldsymbol{Rx_d}$ as a valid command $\boldsymbol{c_3}$ and is be expressed as; $\left\{\boldsymbol{e_{Tx_3}}(\boldsymbol{w_3}) \rightarrow \boldsymbol{m_{33}}\right\} = \boldsymbol{c_3^{BIN}}$. Notice that when devices $\boldsymbol{Tx_1}$ and $\boldsymbol{Tx_2}$ are used in an identical configuration, the logical decoding of $\boldsymbol{m_{33} = m_{13} = m_{23}}$ when the physical characteristics of the RF-Event is discarded during receipt by $\boldsymbol{Rx_d}$.

- **A.3.10 Preparing for Network Integration of Logical and Pathological Authentication Evidence**

The results of F represents a subspace of encoded circuit source states collected as a distribution of N independent samples collected from an authorized RF-Event w_s. For each F of e_{Tx_s}, an encoding rule is used to train Rx_d to know the RF-DNA signature of a given claimed credential c_k^{BIN}.

After training, Rx_d is capable of comparing the similarity of newly received instances of (15) encoded using (29) by conducting RF-measurements and decoding using (30). For each RF-biomarker, measurement taken from a new sample of w_i, a decision threshold d_T provides classification support of logical credential claims using physical attribute augmentation. A discussion of three options for choosing an optimal d_T is next that may yield different classification results. A binary response using a stated similarity for d_T yields a simple '0' or '1' (True or False) result after RF-DNA marker comparisons are made using (31) below and may not be useful in noisy environments.

An ordinal threshold provides the capability to accumulate multiple binary outcomes for a single RF-Event or continuous values. Finally, a continuous d_T yields a compared result value between '0' and '1', where a '0' is not at all similar and a '1' has perfect similarity. A combination of each d_T option may support expressive RF-biomarker vector interpretations of repeatable RF-Event measurements.

A tolerance region threshold $'D_t'$ classifies acceptable Euclidean distance levels of similarity for new RF-Biomarker measurements. An upper and lower bound of algorithm performance, usingD_t's decision rule, determines trust ratings which span a series of interactive trusts transactions [71]. Using an enhancement to the simple interaction trust algorithm, Duncan developed a consolidated trust management system (CTMS) which tracks the level of trust that d has for s using an interactive trust value (ITV) and a specified policy p_i threshold boundary to provide appropriate responses [1]. In this article, enhancements extend a 2-state classification system to 4-states. By adding additional information about prior pathological evidence, a multi-factor device specific (1-to-1) verification system using Bayes Theorem to improve the posterior probability that a claimed RF-Event credential truly originated from a trusted source. Using two factors, the possible classification states of a transaction becomes more expressive to attribute authorized user, device and commands that occur in the network to four possible system states.

The risk response indicates the level of support for authentic claim validations ($c_k^{\mathrm{BIN}} = 1$). In general, a higher level of similarity indicates a low risk (d_{lo}) of command acceptance, while a low level of similarity indicates a higher risk (d_{hi}) of uplink command acceptance. A medium risk recommendation occurs when the similarity of a claimed credential is near tolerance boundaries. The similarity risk responses using 3-levels is summarized as

$$Rx_d^{d_T}(c_k^{PHY}) = y_{\%}^{d_T} \begin{cases} High, & y_{\%} \geq d_{hi} \\ Med, & y_{\%} \lesseqgtr_{dlo}^{dhi} \\ Low, & y_{\%} \leq d_{lo} \end{cases}. \tag{31}$$

In order to augment a Cyber Operator in their task of maintaining the health of a network in accordance with policy, a set of decision rules aim to minimize errors in deciding the true origin integrity of claimed RF-Event. The basic test involves the detection, measurement and analysis of new RF-Event comparisons to a template of trusted RF-Events. Each RF-Event contains identification credentials of a known source. The simple goal is to determine if the received RF-Event originated from a trusted transmitter or not. A first step is defining a truth (oracle) template such that when new RF-Events arrive, the receiver can extract new measurements and make comparisons of its similarity level to a true benchmark signature of the claimed RF-Event. Such previous observation using the same receiver reduces receiver bias.

A receiver learns to recognize a device specific signature benchmark by observing $n = 1100$ independent normal benign RF-Events in accordance with (15) that satisfies all properties of Table 13. After observation of the events, a self-similarity test occurs that consists of all "n-vs.n" observations, measurement and analysis of fingerprints to establish the *true* benchmark similarity levels for each local RF-Biomarker of a composite RF-DNA fingerprint.

- **A.3.11 Region of Interest for Waveform Watermark Selections.**

A specified ROI of a trusted device's waveform is predetermined as candidates for RF-DNA fingerprint credentials. AN ROI can be all or a portion of a transient waveform emission originating from a trusted device $\boldsymbol{s}$. Desirable ROI candidates, for RF-DNA extraction, are standardized regions such as the preamble, midamble and postamble portions of a transmitted waveform [52].

AN ROI marker candidate $\boldsymbol{iMkr^{f_n}}$ is defined as a subset of some chosen $\boldsymbol{f_n}$ for a receiving device $\boldsymbol{d}$ to target for RF-DNA fingerprint validation from $\boldsymbol{s}$. In general any distinct repeatable analog waveform contains distinct features that are extractable for RF-DNA fingerprinting. This implies that RF-DNA fingerprinting can not only be performed on standardized invariant regions, but also on customized invariant regions. For example, let some message $\boldsymbol{m}$ be generated by some device $\boldsymbol{A}$ and is propagated along a transmission circuit and is finally converted from digital to analog using a known modulation scheme. If $\boldsymbol{m}$ contains some invariant field $\boldsymbol{z1}$ and another invariant field $\boldsymbol{z2}$, then a standardized waveform carries some invariant modulation region that is attributable to the waveform itself, and it also carries some region of $\boldsymbol{z1}$ and $\boldsymbol{z2}$, which are also invariant.

Whether or not the fields for $\boldsymbol{z1}$ or $\boldsymbol{z2}$ message state generations, as depicted in Figure 36 are easily located within the waveform carrier immediately from RF-DNA extraction does not imply that these invariant regions do not exist. This is made obvious by the successful decoding of $\boldsymbol{z1}$ and $\boldsymbol{z2}$ by some receiver after successful synchronization and demodulation of the waveform carrier to interpret the bit-level fields.

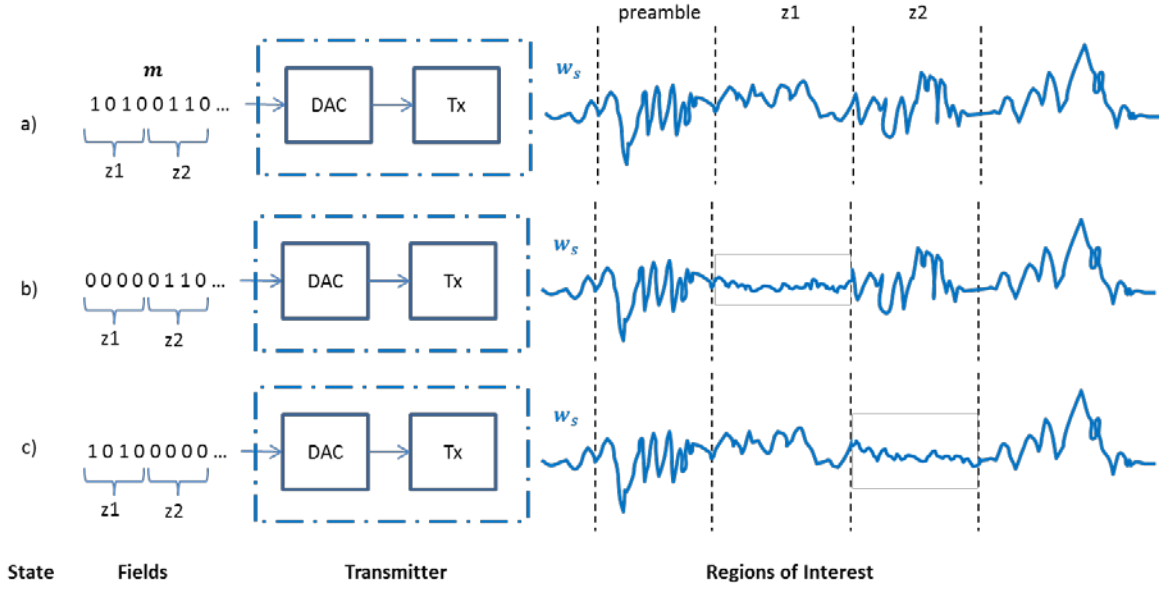


Figure 36. Generalized Modulation of Invariant Message Fields Visualization Only

- **A.3.11.1 Policy-Based Pairing of Constituents.**

Full-Duplex interaction allows RF-DNA marker exchanges with all distinct members in all directions. This policy requires the most receiver processing power and storage requirements, but is the easiest to configure as suggested in Table 30.

For each directed communication path that exists between $(\boldsymbol{s} \rightarrow \boldsymbol{d})$ pairs, select some subset from $\boldsymbol{f}(\boldsymbol{s})$ and transfuse RF-DNA fingerprint credentials into $\boldsymbol{d}$'s profile to meet specified policy objectives. This provides $\boldsymbol{d}$ with knowledgeable credentials of $\boldsymbol{s}$ so when $\boldsymbol{s}$ attempts to communicate with $\boldsymbol{d}$, then $\boldsymbol{d}$ can authenticate the uplink's trusted waveform $\boldsymbol{w_s}$ claiming to originate from $\boldsymbol{s}$. Device $\boldsymbol{d}$'s knowledge of $\boldsymbol{s}$ does not imply that $\boldsymbol{s}$ possesses the same knowledge to authenticate a waveform state originating at $\boldsymbol{d}$.

Unless $\boldsymbol{s}$ is explicitly configured to have knowledge credentials of $\boldsymbol{d}$ as specified by policy $\boldsymbol{p}$, then $\boldsymbol{d}$ cannot be authenticated by $\boldsymbol{s}$, since such credentials may not exist in the full RF-DNA complement $(\boldsymbol{F_{s+}})$ of $\boldsymbol{s}$. A complete paring represents a device's policy-based FULL-RF-DNA complement between $(\boldsymbol{s} \rightarrow \boldsymbol{d})$ such that all necessary RF-DNA fingerprint credentials to authenticate $\boldsymbol{s}$ are stored in $\boldsymbol{d}$'s local storage profile and all vice versa if $\boldsymbol{d}$ is authorized to authenticate transmissions received from **s**. To achieve full duplex communication where each device can authenticate its linked neighbor, all authorized states of $\boldsymbol{w_s}$ events should be fingerprinted to collect RF-DNA. The results are exchanged as credentials between specified devices prior to communication.

For a full complement paring of $\boldsymbol{D} = \mathbf{4}$, we obtain 16 possible full marker exchange pairings for a single ROI fingerprint model. In **Chapter IV**, six ROI models varied by length, duration; sample start and sample stop points of previously collected fingerprints of model $\boldsymbol{M}$. This yields 10626 possible combinations for policy development. Figure 37 depicts a policy pairing scheme $\boldsymbol{p}$ used to define link $\boldsymbol{l}$ communication paths between endpoints $\boldsymbol{s}$ and $\boldsymbol{d}$. The pairing $\boldsymbol{p_i}(\boldsymbol{a}, \boldsymbol{b})$ describes a set of users $\boldsymbol{u}$, ground station devices $\boldsymbol{D}$ and or available satellites for RF-DNA credentials that are used to authenticate link transactions.

On the left of Figure 37, $\boldsymbol{u_1}$ is shown to have a policy that authorizes the use of all command sequences (highlighted in blue). In addition, a $(\boldsymbol{u_1}, \boldsymbol{c})$ pairing is made with $\boldsymbol{D_1}$ given as $\boldsymbol{p_1} = ((\boldsymbol{u_1}, \boldsymbol{c}), \boldsymbol{D_1})$. The RF-DNA fingerprints are collected from appropriate waveform $\boldsymbol{w}$ *states* generated by $\boldsymbol{s}$ such that the extracted RF-DNA fingerprints samples can be authenticated by each $\boldsymbol{d}$ specified by policy $\boldsymbol{p}$. This process is completed for each $((\boldsymbol{u}, \boldsymbol{c}), \boldsymbol{d})$ pairing combination. The resulting RF-DNA fingerprints are stored for policy-based link $\boldsymbol{l}$ pairings as model $\boldsymbol{M}$ as previously described.

The final pairing of a $\boldsymbol{s} \rightarrow \boldsymbol{d}$ path is made to facilitate the transfusion of RF-DNA credentials into the local memory of specified destination device(s) $\boldsymbol{d}$. As shown in Figure 37, the full complement of $\boldsymbol{D_1}$ contains the RF-DNA credentials from Sat1 and itself indicating that it is capable of authenticating waveform states $\boldsymbol{w_s}$ received over downlink $\boldsymbol{l}$ generated from a trusted source (Sat1). The uplink path $\boldsymbol{l}$ depicted in Figure 37, indicates that destination device $(\boldsymbol{d} \in \boldsymbol{M}) = \boldsymbol{Sat1}$ has a full RF-DNA complement containing RF-DNA credentials of all source (ground station) devices $\boldsymbol{s} \in \boldsymbol{M}\ \boldsymbol{s}.\boldsymbol{t}.\boldsymbol{d} \neq \boldsymbol{s}$, which may be generally desirable. All possible pairings are not shown for image clarity.

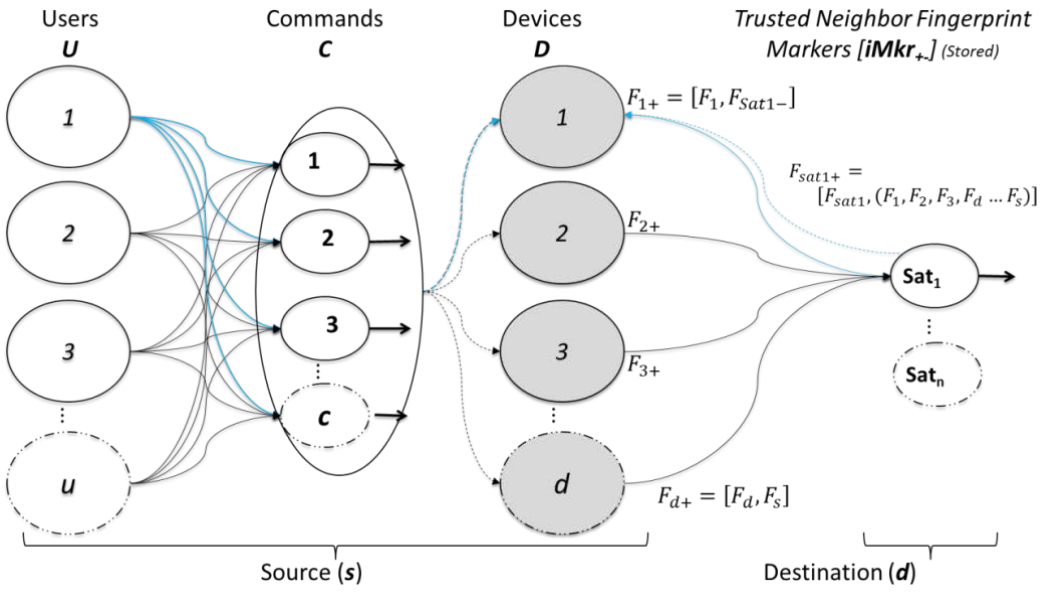


Figure 37. Policy-Based RF-DNA Marker Exchange Pairings

- **A.3.11.2 Covert RF-DNA Watermark Credentials**

This section describes the process of authenticating authorized waveform states using RF-DNA fingerprint credential keys as covert watermarks. The scheme is inspired by the rolling code algorithm discussed in Chapter I. There is no obvious disclosure of a fingerprinted ROI as before, however the end nodes discover the exact location that should be listened to during waveform inspection by utilizing a covert channel to pass credential keys. The purpose of this scheme is to mitigate imposter eavesdropping and sufficient sampling of an intercepted waveform to generate a replay message that mimics a valid RF-DNA credential. A key factor is added to the ***iMkr***, randomized prior to operation and transmitted so that each subsequent key for an ROI is different from the previous key in any transaction sequence. Randomized key exchanges enhance the security of the RF-DNA credentialing scheme. As an example, a repeatable waveform state naturally contains all possible features that can be extracted at any given instance of its existence. Consider the case where a watermarked key is sent to indicate the ROI of a waveform for RF-DNA fingerprint extraction. If the receiver already knows the exact location of the key, then an imposter attacker may exploit this nature. When a watermark is invisible to the attacker, then this is more difficult. By passing pre-determined keys randomly associating those values with valid RF-DNA credentials, it is possible to confuse the attacker and make their guess about which ROI to target and exploit more difficult.

- **A.3.11.3 RF-DNA Concerns with Applications for Mass Destruction.**

There are multiple concerns associated with the employment of RF-DNA credentials to include receiver memory size, circuit development for RF-DNA fingerprint marker extraction from authorized waveform states and network maintenance during circuit modifications and malicious capability of unintended employment of RF-DNA like credentials as covert watermarking. The receiver's memory size of a conventional CubeSat is limited for additional onboard processing of RF-DNA fingerprints.

On one hand, the local memory of a receiver may not be sufficient to store RF-DNA credentials that could provide self-evident waveform authentication. On the other hand, it is not known how fast a comparison could be made if the comparison was temporarily stored on the receiver and a call is made to an off-site location for final verification. Research should continue in determining optimal memory size and processing requirements to support real-time operations or multi-organizational access to shared spacecraft. These implications suggest that a set of authorized waveform state credentials could exist for each participating organization, which must be stored locally for self-evident authentication to occur. This implication may significantly reduce the scale of RF-DNA credential exchanges to backbone infrastructure transactions that provide device-only discrimination. As discussed in Table 30 above, a preamble based ROI provides the most general level of device discrimination of a standardized waveform for fingerprint comparisons. In addition, as the number of distinct links grow so does the path policies and as a consequence the number of authorized waveform states increase. Attempts to extend a general waveform classification to achieve more expressive responses, ROIs should be carefully selected to reduce the size of standardized ROIs. In general, a smaller policy size that specifies authorized waveform states provides the least amount of user attribution. The smaller the subset of exchanged RF-DNA markers, the less storage is required. Normal network maintenance of adding, replacing and upgrading network components must be considered for RF-DNA augmentation.

A.4 Conclusions

A focus and requirement of some physical waveform requirements should be enforced in tomorrow's network security plans. Mass-destruction triggers, if placed in malicious hands could cause significant destruction without leaving a trace for attribution. This suggests a need to develop a massive waveform database that focuses on the physical nature of waveforms instead of their logical interpretations or binary content. In this way, we can take any logical value or message that is carried by a waveform and gain a deeper understanding of its origins using RF-DNA fingerprints. As component changes occur, research should be done to identify the impact and effects on RF-DNA detection for a collected circuit fingerprint and memory emplacement. Perhaps infrastructure network configurations that minimize major component changes should be initially approached. It is obvious that if a circuit fundamentally changes, then any exchanged RF-DNA credential may not work. In light of this situation, an upgrade mechanism should be employed to securely modify the memory of existing authenticators as well as provisioning for added communication paths to an existing or deployed network configuration.

- **A.4.1 Immediate Cause for Concern.**

Unintended consequences may occur with the full realization of distinct standardized waveform recognition. As an immediate example, consider a bad actor who intends to create a mass casualty event by employing an RF-DNA-based remote controlled trigger. Such a trigger can be emplaced inside the memory of a device that contains an explosive payload. A carrier of the device may present the device as harmless to some innocent bystander. As a person comes into range of the explosive device, his or her particular voice characteristics could trigger the explosive device leaving no trace of the true bomber.

This is not out of the realm of feasibility as a similar approach was recently employed to trigger a laptop bomb onboard an airliner [84]. Simply stated, a receiving device that has an emplaced RF-DNA credential may not be detected in a conventional RF probe because the incoming trigger has already been pre-determined and contains statistically unique features. An unsettling situation that is similar to a one-time pad which uses encryption as the triggering response for interpretation.

- **A.4.2 Future Recommendations.**

Research that applies RF-DNA fingerprinting is ongoing and fairly new to the SATCOM community. Network authentication augmentation is an initial first step to enhance network level authentication mechanisms and control access to critical spacecraft command and control boundaries. A logical extension to device discrimination is user discrimination. If we consider a cellular phone that employs some device recognition filter and we have a user that utilizes their voice as a trigger for some control function, then the combination of the device and the user now form evidence for attribution to the user and the device. Research is recommend to explore the limits of discovering traces of RF-DNA evidence in known waveforms based on time and space. Immediate applications for such recognition of RF-DNA markers include home and car security alarms systems, safes and gun cabinet lock controls. Research that augments the C2 of UAV swarms may benefit from RF-DNA fingerprint marker exchanges using multi-factor authentication credentials. Such C2 could be useful for air delivery ventures where customers trust the secure delivery of purchased packages by sampling their voice characteristics ahead of time as the key to sign for deliveries. If no such key exists within the UAV receiving mechanism, then there is no subsequent delivery made. Such a scheme could also be used to conduct business transactions over the Internet for RF-DNA ecommerce credential exchanges. In this effort, waveform authentication can be used by corporations like Amazon to strengthen online purchasing where buyer's voices, fingerprint or PC and natural feature combination as the authorized waveform. This added security mechanism can easily be implemented on existing PC and mobile devices that utilize digital voice mechanisms. RF-DNA has the capability to incorporate any repeatable waveform state of a natural source.

ANNEX B: Ground Station Uplink Fingerprinting for CubeSat Overview

The purpose of this section is to provide a documented record of this research effort. Given the nature of FM radiation and experimentation, the interested reader should seek and follow all safety recommendations with dealing with sustained exposure to RF equipment. The attached ALFE (not listed) is a living document and is presented here as a flashpoint for lab safety considerations. Each annex is written as a stand-alone document and was developed collectively with the goal of assisting a design of experimental approaches to conducting research on SATCOM link analysis using RF-DNA fingerprinting or future Cyber security enhancing mechanisms. The actual code for the RF-DNA fingerprinting process is also a living developmental source code and is not presented as a significant part of this research. Code Snippets that support specific code optimizations that are specific for SATCOM RF-DNA fingerprinting have been presented throughout the document. Finally, the reader should consult the circuit diagram to understand the complexity of a SATCOM's ground station and required background knowledge. These collection procedures were adapted from Reising's (Appendix A pages 68 – 74) work that employed the Agilent E3238S as the radio frequency signal collections (RFSICS) device. The software defined radio models X310 and USRP 2922 are also employed to collect the RF-Event waveforms.

ANNEX C: How to Set Up CGA OS For GS Communications PC1 v3

Research Lead: MAJ Tyrone Lewis
Intern/Research Assistant: Chris Lomanno
Original Date: ~7Aug2015
Editor/s: MAJ Tyrone Lewis and Chelsey Moeller
Description:

The purpose of this document is to provide detailed steps to place the ICOM and CGA software into communications mode. From this mode of communication, the CGA will transmit.

- **C.1 Hardware**
  - ***Model: HP***
  - ***OS: Red Hat Enterprise Linux Workstation Release 6.3***
  - ***Memory: 3.8 GB***
  - ***Disk Space: 328.6 GB***
- **C.2 Software**
  - Neptune Common Ground Architecture

1. To start CGA open a terminal window like the one shown in Figure 38 and type **"csm"** to open a Session 100 Manager: FS7-1 instance.

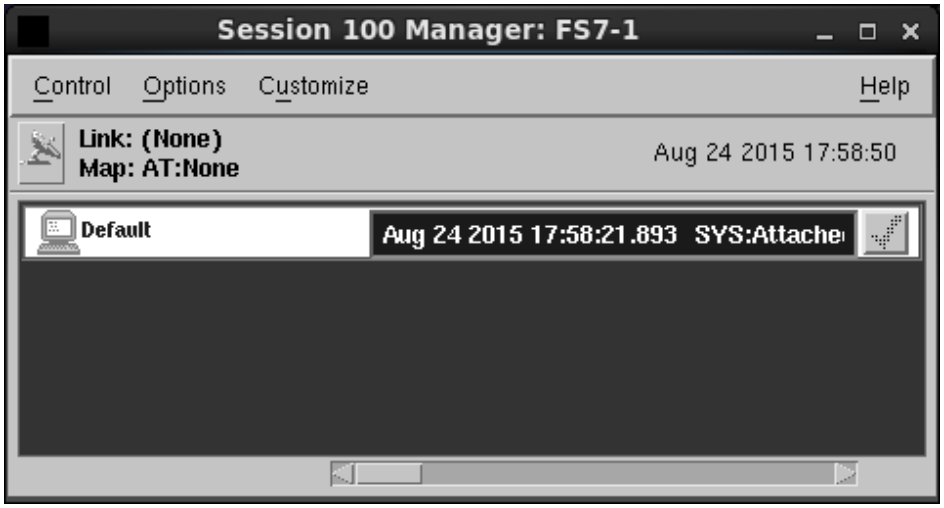


Figure 38. CGA Terminal Session 100 Window

2. From the Session Manager Screen, under the tab "Options"
   a. click "Projects" -> "C2B_Setup_UHF"

3. Continue to click "cont" as the Neptune window depicted in Figure 39, loads scripts and device drivers. If errors occur within the Neptune window click the yellow box labeled

"Cont" // Allows the program to continue

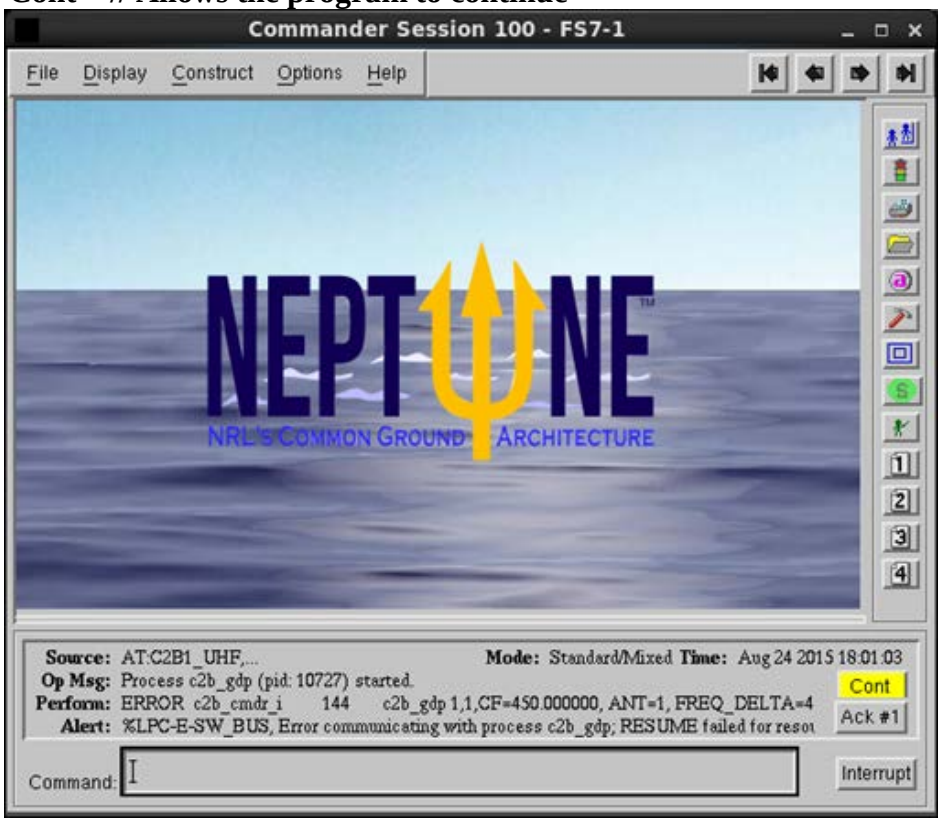


Figure 39. **N**eptune Window In Cent Operating System

4. Once the Neptune was completely loaded all necessary files and set drivers, the Commander Session 100 window will become active and at the command prompt we can enter the file that contains the telecommand messages as shown in `Figure 40`. To run the Automation code written by Mr. Christopher Lomanno, entitled *C2B_RF_fingerprint_1001.per* type into the command line box:

"per C2B_RF_fingerprint.per" //Original file

"per C2B_RF_fingerprint_1001.per" // Modified naming convention

"per C2B_RF_fingerprint_101.per" // Modified file with 101 bursts

The "**C2B_RF_fingerprint.per"** will command the ICOM to send 1001 pulses to the signal collection device (X310). The current version will complete in approximately 17 minutes.

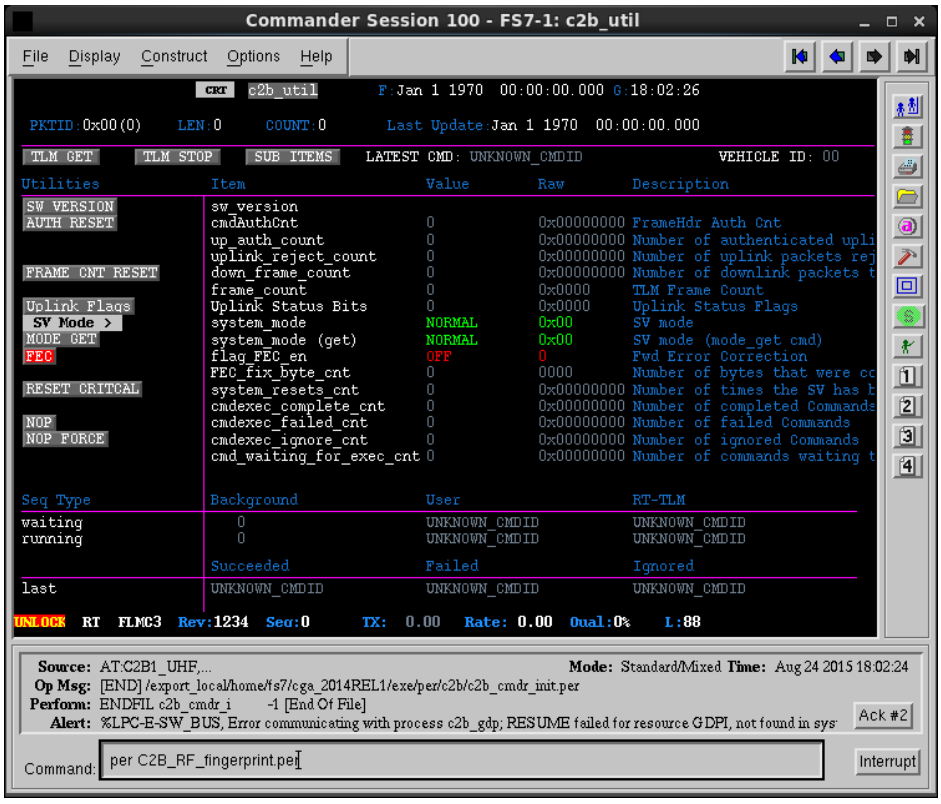


Figure 40. Tele command Message Generation on Cent OS PC

5. We are now ready to transmit the automation code and generate transient pulses from the TNC to the ICOM. The ICOM will then modulate the message using GMSK and the red LED light indicator should flash.
    i. To start the transmission click "**enter**"
    ii. To pause the transmission, click **"pause"** the lower right hand corner of the window.
    iii. To resume click **"Cont"** in the lower right hand corner of the window.
6. To close the Commander Session, **click X** in the top right corner of `Figure 41`.
7. To close the Session Manager,
    i. Click Control -- > "Stop Node" -- > "*SVR1*" -- > OK
    ii. For example 2: Control -- > "Sab-stop" -- > "node-AFMC-3"

(then click 'ok' when prompted)

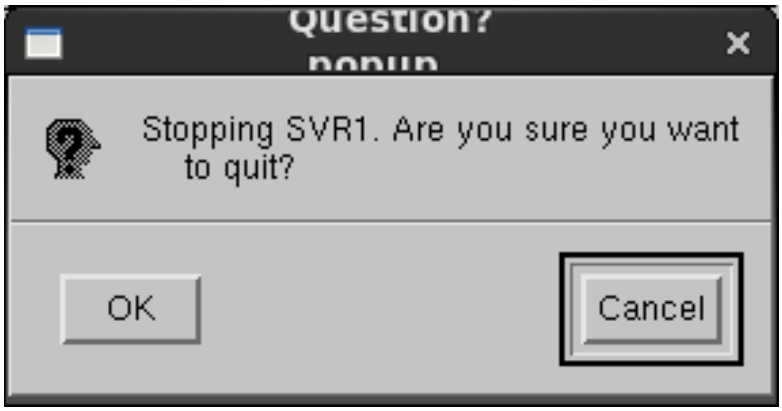


Figure 41. Stop Tele command Generation Server Prompt

8. Return to the original terminal window (Open a new one if closed)
   a. type **"ipcs"**
   b. Verify that all values = 2 under the **"nattach"** column. Wait for five seconds and type "ipcs" again to see if the column has been attached.

      i. If some value is not == 2 after waiting five seconds, type **"ipcrm -m ########"** // where ####### is the shmid of the process where nattach isn't equal to 2. For example, if row 1 column nattach had a value !=2, then record the corresponding shmid value, and then type in the command above with this recorded shmid.

This completes this portion of the guide.

Notes for automation script modifications

1) TO SEND FEWER PULSES: (**Must have root permissions to copy and paste a new file for script execution**) You can edit the script so that it sends fewer pulses through the CGA. This is useful if you want to have (say) 20 pulses for testing purposes instead of sending 1001 pulses. Likewise, you can change it to send 2001 pulses etc…
   a. copy "C2B_RF_fingerprint.per"
   b. paste the original file and rename to some *new_file*C2B_RF_fingerprint_101.per
   c. Restart CMDR
2) Repeat steps above and insert

   ***new_file*C2B_RF_fingerprint_101.per**

   in the command line prompt.

It's located in "/export_local/home/mc3ops/cga_2014REL1/exe". If you edit the file save it then restart CMDR.

2) Commands names and parameters are located in "c2b_cmds.txt" in "/export_local/home/mc3ops/cga_2014REL1/cga_proj/c2b/db/".

ANNEX D: How to Set Up the Recording (Collections) Laptop

Research Lead: MAJ Tyrone Lewis
Intern/Research Assistant: Evan Kain
Original Date: ~08AUG2015
Editors: Chelsey Moeller
Description:

This guide will take you through the process of setting up the recording laptop (PC2) of the circuit diagram. There will be information on what type of software is needed and also how to visually see the data pulse.

- **D.1 Hardware**
  - Make: HP
  - Model: Elite Book 8560w
  - OS: Ubuntu 14.04 LTS (64-bit)
  - Memory: 15.6 GB
  - Disk Space: 231.6 GB
- **D.2 Software**
  - GNU Radio Companion 3.7.7
  - Command Input Interface: Ubuntu Terminal
  - Center Frequency: 449.8MHz
  - Gain: 18dB
  - Sampling Rate: 5MSPS

1. When powering on PC2 select the Ubuntu operation.
   i. To do this use the up and down arrow keys to highlight the Ubuntu.
   ii. Then click "enter" to select Ubuntu.

   Note the password for the PC is: Password!123
2. Plug PC2 into an outlet for power supply.
   i. Note: PC2 cannot record if it is not plugged into a power outlet.
3. Open a terminal window by clicking the "search your computer and online sources" tab found in the upper left hand corner of the screen.
   i. Type "Terminal" into the search bar.
   ii. Once the terminal icon appears, click on it to open a terminal.
4. From the terminal window, type the following command:
   i. uhd_rx_cfile –args -addr=<IP Address> -f <center frequency> -g <RF Gain> --samp-rate=<sampling rate> <filename>
   ii. The IP address is the IP address of the X-310 being used. For our purposes the IP address is 192.168.10.2
   iii. The center frequency is the center frequency of the recording in Hz. The center frequency for our set up is 449.8e6 Hz
   iv. The RF gain is the internal gain in dB that the SDR applies after receiving the signal. We are using the gain of 18 dB.
   v. The sampling rate is the rate at which the SDR will sample the signal in samples/second. The sample rate we want is 5e6 samples/second.
   vi. The filename is the name of the file where the data will be saved.

The format being used for the file name is <make of transmitter>_<model>_<serial number of device>_g_<gain in dB on SDR>_p_<transmission power(preferably in Watts, but visual bars in this case)>_fingerprints

<make >_<model>_<serial number >_g_<gain >_p_<TXPwr>_fingerprints

a. E.G. **ICOM_9100_02001003_g_18_p_4_fingerprints.**

vii. The entire code should be similar to this e.g.

uhd_rx_cfile --args -addr=192.168.10.2-f 449.8e6 -g 18 --samp-rate=5e6 ICOM_9100_02001003_g_18_p_4_fingerprints

viii. Once you have typed the command into the terminal window click "enter" to begin recording data. If you are recording properly the screen should look like this:

5. To stop recording click "ctrl+c" in the terminal window.
6. To see a visual representation of the frequency domain on PC2, type the following command in the terminal you opened in step 2:

uhd_fft --args -addr=<IP Address> -f <center frequency> -g <RF Gain> --samp-rate=<sampling rate>

i. The parameters for this command will be the same as the parameters for the recording command from step 4. Note: You do not need a file name when running fft.
    1. If the transmission is working properly you should expect a peak around the expected transmission frequency.
    2. If there is no peak, try adjusting the gain or turning the "peak hold" option on.The peak hold option will be located near the top right of the window.
7. If the noise level is too high, try lowering the gain.
    i. To do this close the current window and follow step 4 again and adjust the gain accordingly.
8. The default save location for the recordings is the home folder.
    i. To find this click the icon labeled files in the upper left hand corner.
    ii. You should see a file named with the same name you entered during step 4.i.5 that appears.
9. To close the fft window click the "x" in the upper left corner or click "ctrl+c" in the terminal window.
10. To transfer the saved file from PC2 to PC3 for RF-DNA Extraction; plug in your USB hard drive to PC2.
    i. Move the saved file to the USB hard drive for transfer to PC3.
    ii. Plug in the USB Hard Drive to PC3 and see **Annex C**: *How to run MatLab scripts in PC3* for more information.

ANNEX E: How to Process the Collected Data Files with MATLAB

Research Lead: MAJ Tyrone Lewis
Intern/Research Assistant: Chelsey Moeller
Original Date: 26Aug2015
Editor/s:
Description:

The purpose of this guide is to step by step show you how to process the data you previously recorded on your PC2. This guide will tell you which parameters in the MatLab files that you will need to change to get the proper results.

- **E.1 Hardware**
  - Make: HP
  - Model: Z820 Workstation
  - OS: Ubuntu 14.04 LTS (64-bit)
  - Memory: 125.8 GB
  - Disk Space: 1.8TB
- **E.2 Software**
  - ***MATLAB 2015aX-CTU Application Version 5.2.8.6***

1. PC3 runs Ubuntu. Once turned on open MatLab by following these steps:
   a. Click the "search your computer and online sources" icon found in the upper left
   b. Once the window is open type "terminal" in the search bar, then click "enter."
   c. When the "terminal" icon appears below the search bar, double click the icon.
   d. In the "terminal" window type "MatLab," then click "enter."
2. Once MatLab is open you will need to add the MatLab files **model_RF_2.m**, **RFDNA_fPrintGen_V7.m, MDAML_ClassifyMain_V8.m, MDAML_Verification_V8.m,** and your data to the path for MatLab.
   a. Right click the folders containing these files.
   b. Click "add to path."
   c. Click "selected folders and subfolders." You now have all of your file paths
3. Click the open folder in the in the upper left corner of the MatLab window.
   a. Click the "open" folder.
   b. Navigate to the file where your MatLab files **model_RF_2.m**, **RFDNA_fPrintGen_V7.m, MDAML_ClassifyMain_V8.m,** and **MDAML_Verification_V8.m** are all saved to.
   c. Double click each of the above MatLab files to open the MatLab editor window
4. The first MatLab script you are going to run is **model_RF_2.m**.
   a. Navigate to the MatLab editor window, and click on the **model_RF_2.m** tab at the top of the screen.
   b. Navigate to line 41 to load your raw data collection
      i. Depending on the number of devices you line should look like: Devicestrings=['<file-data1>'; '<file-data2>' ; '<file-data3>' ; '<file-data4>'];
      ii. At line 124, you will need to change the first name to a desired name as:

save('<your-choice-of-file-name>', 'InSig', 'FingerPrints', 'DetParams', 'XDelta', '-v7.3');

iii. Take not of this file name. You will need it again.

c. Click the "save" icon in the upper left corner of the window.
d. Click the "run" icon at the top of the window.
e. You should see on the other MatLab window the script running.

5. The next MatLab script you will run is **RFDNA_fPrintGen_V7.m.**
   a. Return to the MatLab editor window, and click the tab **RFDNA_fPrintGen_V7.m**.
   b. At line 85, and 87 insert the file name that you created from step 4.b.
      i. The lines should look like this:
      ii. Line 85: InputFileName= '<your-file-name-from-part-4b>';
      iii. Line 87: SaveFileName='<your-file-name-from-part-4b>';
      iv. You may also wish to change other parameter such as line 110 the DecFact or line 98, the SNRin values. Reference Annex <?>: fPrintGen_V7 for more information.
   c. Click "Save" in the upper left hand corner of the window.
   d. Click "Run" at the top of the window.
   e. Once the MatLab script is finished running take note of the output file name. It should look similar to: **<Input-file-name>_TimeDomfeats_DecFact=<#>**

6. You are now ready to run the script **MDAML_ClassifyMain_V8.m**.
   a. At lines 84 and 85 you will enter the file name (the output name from 5.e.)
   line 84: **InputFileName= ' <Input-file-name>_TimeDomfeats_DecFact=<#>';** line 85: **SaveFileName= '<Input-file-name>_TimeDomfeats_DecFact=<#>';**
   b. You will also need to change the SNR values, number of pulses for training, and the plot control variables to your specifications. See annex <?>: ClassiffyMain_V8 for more information.
   c. Click "Save" in the upper left hand corner of the window.
   d. Click "Run" at the top of the window.
   e. You should notice a series of plots appear.
   f. After the script has ran take note of the name of the output file. It should look similar to: **<Input-file-name>_TimeDomFeats_DecFact=<#>_<#>SNRVals_DraModDev_<#>Feats**

7. Now the script **MDAML_Verification_V8.m** is to run.
   a. In line 52 load the file output from the script RFDNA_FPrintGen_V7. It should look like: Line 52: **load <Input-file-name>_TimeDomFeats_DecFact=<#>.mat**
   b. At line 55 you enter the file output from the script **MDAML_ClassifyMain_V8** that you previously ran. Line 55 should look like:
   load <Input-file-name>_TimeDomFeats_DecFact=<#>_<#>SNRVals_DraModDev_<#>Feats
   c. Choose a name to save the file name under at line 57.
   Line 57: SaveFileName = '<file-name>'
   d. Click "Save" in the upper left hand corner of the window.
   e. Click "Run" at the top of the window.

ANNEX F: How to Set Up the Terminal Node Controller (TNC)

Research Lead: MAJ Tyrone Lewis
Intern/Research Assistant: Evan Kain
Original Date: ~08AUG2015
Editor/s: Chelsey Moeller
Description:

The purpose of this guide is to explain how to properly set up the physical connections for the Terminal Node Controller (TNC). These instructions are based off of using a Kantronics 9612 plus model TNC.

- **F.1 Hardware**
  - Make: Kantronics
  - Model: Packet Communicator 9612 Plus
  - Serial Number: 919194? (number is located on bottom of device)
  - Operating Mode: KISS
  - Outgoing Port: 2
  - Baud Rate: 9600

1. Connect the TNC to power using the power connection provided with the TNC. Use the port on the left rear side of the TNC for the connection.
2. Connect the TNC to the transceiver using a 6-pin-mini-DIN male to DB-15 male connection. The 6-pin-mini-DIN side connects to the transceiver via the connection labeled DATA2.
3. The 6-pin-mini-DIN connection can be found in the middle of the transceiver's rear panel (See Figure 46 of **Annex F**: *How to Setup the ICOM 9100 Device.*
4. The DB-15 male connection for the TNC is in the middle of the rear panel on the TNC.
5. Next connect the TNC to the computer using a set of two cable connections.
   a. The first connection uses a male DB-25 to female DB-9 cable. The male DB-25 connection is connected to the port labeled "computer" on the rear panel of the TNC.
   b. The second cable is a male DB-9 to USB. The male DB-9 end is connected to the female DB-9 connector from part 5.a. The USB is then plugged into PC1.
   c. This connection is labeled "PC1 to TNC"
6. See **Annex E:** *How to Set Up and Use the X-CTU Terminal Software.*
7. J16 is currently set as closed. Default is open.
8. Type "Display" on the terminal window to show a complete list of the TNC settings.

ANNEX G: How to Set Up and Use the X-CTU Software v3

Research Lead: MAJ Tyrone Lewis
Intern/Research Assistant: Evan Kain
Original Date: ~ 13AUG2015
Editors: Chelsey Moeller and MAJ Tyrone Lewis

- **G.1 Description:**

Note, the automation for transient burst generation is only functional in the **intface** kiss mode, which is the current MC3 default mode of operation. When operating in the convers mode as done here for testing purposes in a lab environment, the burst generation must be performed manually. The goal is to generate transient burst automatically. These directions are provided to bring a new TNC into initial operation and then to perform transient burst generation tests in kiss mode. If the TNC has already been set up, move to step eleven of this document.

1. Download drivers if necessary. (Download/open X-CTU or other configuration software to use the packet communicator)
2. Connect PC USB port to TNC's Port 2 with specified cable found in **Annex D**: *Setting Up the Packet Communicator's Terminal Node Controller (TNC).*
3. Power on the TNC
4. Ensure the connecting device (TNC) is recognized by the computer and that the proper drivers are installed.
5. Open the X-CTU program
6. Click on the terminal tab near the top of the screen to open the *terminal* window.
7. You can Type "help" to display available commands, and type "help <command>" to access descriptions and directions for each command.
8. From the command window, check to ensure that *command mode* is enabled. There should be a **.cmd:** directly to the left of the blinking cursor.

   Depending on the window output check one of these options:
   1. If screen has no output as shown in Figure 42 and Figure 43, enter the "C0 FF C0" hex command as follows:
      a. Click Assemble Packet (From the X-CTU Terminal Window)

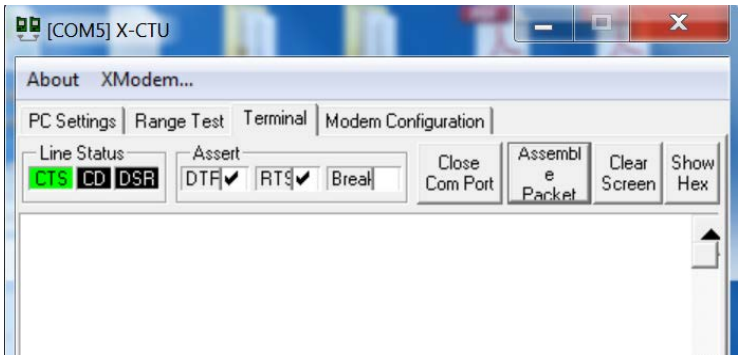


Figure 42. X-CTU Software Output (Blank Screen)

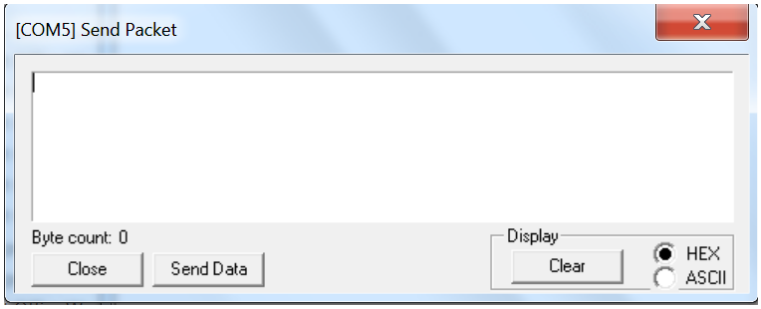


Figure 43. X-CTU Assemble Packet Screen (Hex display)

a. Click the HEX in the Display box shown in Figure 44.
b. Type “C0 FF C0” in the “Assemble Packet” window
c. Then click send data.
d. To check that the command worked properly you should see information on your screen shown in Figure 45.

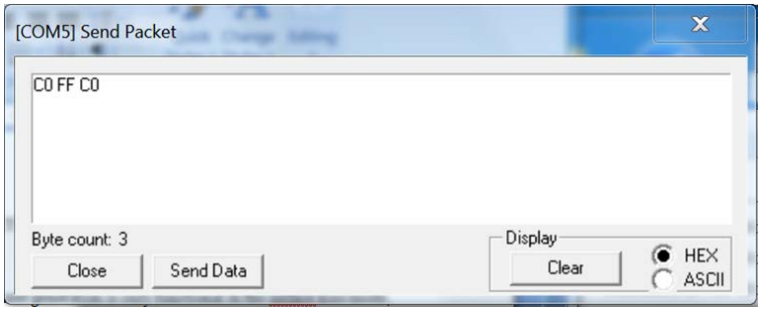


Figure 44. X-CTU TNC Command Terminal

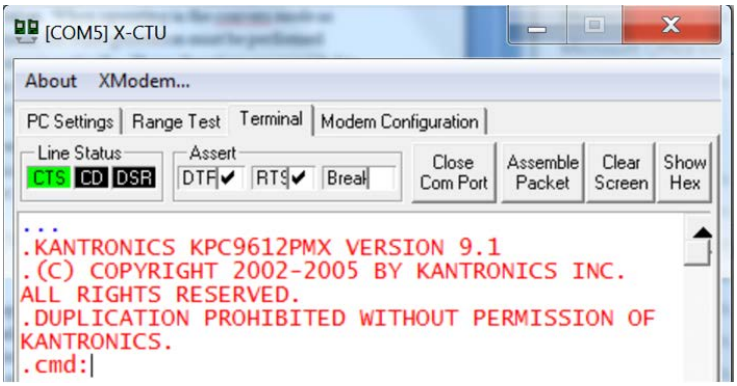


Figure 45. X-CTU Hex Command Executed

2. If screen has unintelligible output, press "*"
    a. At the prompt enter the call sign (Default = Alice1)

9. Enter the following command settings once you are in command mode and display a ".cmd:" on the terminal screen.
    i. Type "MAXUSERS 10" after the **.cmd:**
    ii. Type "XMITLVL 24" after the **.cmd:**
10. To display the port number being recognized by the TNC, or to change the Port follow these steps:
    a. Check port setting by typing the following command
        i. Type "Port" into the terminal window of the X-CTU software after the **.cmd:**
        ii. The terminal will then notify you of the port being used.

    b. If the port is not correct you can change it by following the below steps. Note: for the purposes of this setup the TNC must be set to port 2.
        i. Type "port <number>" after the **.cmd:** in the terminal window. Note- (You cannot change the port in kiss mode. You should be in Terminal mode for making such a change)
        ii. To verify the port changed refer back to step 10.a.

    c. To display the current interface mode:
        i. Type "intface" after the **.cmd:** in the terminal window.
        ii. The terminal will then display the current interface mode. Note: we need the interface to be in KISS mode.
        iii. If this is not the desired mode, refer to step 10.d.
    d. To change the interface to kiss:
        i. Type "intface kiss" after the **.cmd:**
        ii. To verify the change refer back to step 10.c.
    e. Power cycle the TNC for five seconds. The basic configurations for operation are complete.

- **G.2 Verify Manual Conversation Capability Between TNC and ICOM**

11. To verify the physical connection between the TNC and ICOM you must be in "convers" mode. While in the converse interface, commands can be sent to the transceiver directly by typing into the window or by assembling a packet. To set this up follow these steps.

    a. Type "convers" at the .cmd prompt.
    b. Click the "Assemble Packet" button
        i. After the *Send Packet* window opens type a message, then click "enter." In this window you can choose between sending packets using ASCII or hexadecimal encoding using the two buttons on the bottom right corner labeled "ASCII" and "HEX."
        ii. Click "send packet" and see if the red Xmit light for port 1 and the ICOM transmit LED both light up then they are communicating. If they do not light up the packet was not sent.
        iii. If the LEDs did not light up:
            1. Be sure to check the connections again and make sure the software is working properly.
            2. If this does not fix the issue, go back to the terminal window and type "paclen" This should display the maximum packet length as <number>/<number>.
            3. If the packet length is larger than the number of bytes (displayed next to "byte count" in the lower left corner of the "send packet" window) in the message you are trying to send there are at two ways to fix the issue outlined below.
            4. The first method is to type "0D 0A" when sending hexadecimal packets.
            5. Another way is to type "paclen <number>" in the terminal window to change the packet length to match the size of your commands.
            6. If neither of these works consult your TNC manual.
12. If you would like to exit converse mode
    a. Click "ctrl + c" to exit out of converse mode (**3 times in rapid succession**).
    b. To check to see if you exited properly out of converse mode refer back to step 10.c.
    c. If this does not work go back and follow step 10 again.

ANNEX H: How to Set up the ICOM 9100 Front End Transceiver

Research Lead: MAJ Tyrone Lewis
Intern/Research Assistant: Chelsey Moeller
Original Date: ~ 14AUG2015
Editor/s: Chelsey Moeller
Description:

This guide will help you to properly set up your ICOM 9100 transceiver. This guide will walk you through making the correct setting changes.

- **H.1 Hardware**
  - Make: ICOM
  - Model: ICOM-9100
  - Serial Number:02001133,02001255,02001075, 02001003
  - Transmission Frequency: 450MHz
  - Data Mode: On
  - 9600bps: Enabled
  - Transmission Mode: FM
  - Continuous Transmission: Off
  - RF Power: 4 Bars (7.5 Watts?)
  - Modulation Scheme: GMSK Digital Phase Modulation
  - CI-V Address:(depends on device)
  - CI-V Rate: 19200

1. First insure all of the proper physical connections are made. Insure that none of the leads are bent.
   a. The ICOM should be connected from its DATA2 socket to the TNC DB-15 socket through a male 6-pin-mini-DIC to male DB-15 cable.
   b. The ICOM should have a power cable connected to power.
   c. An N-type connection from the ICOM to SMA connection on the X-310.
      i. This cable should have two inline 30dB attenuators connected in series.
      ii. On one end of the attenuators there should be a BNC connector that is then connecting a coaxial cable to the ICOM through an N-type connection.
      iii. The other end of the attenuator should have an SMA male to male cable connecting the attenuators to the X-310.

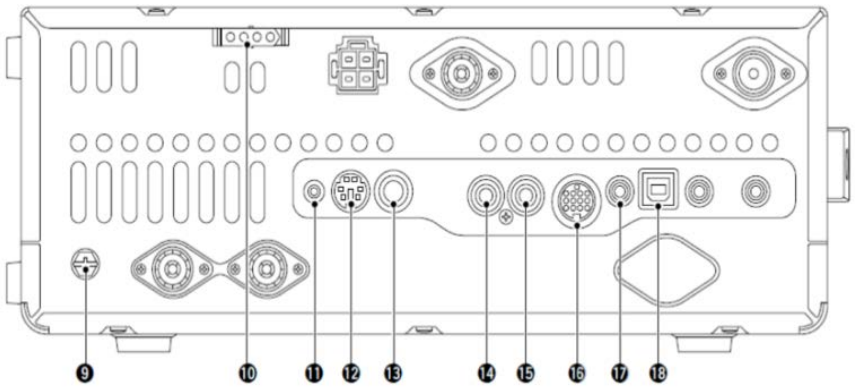


Figure 46. ICOM-9100 PIN Diagram.

2. Turn on the device by holding down the power button. Reference page 1 of the ICOM manual for more information.
3. Hit the AM/FM button until the FM frequency band is selected. Reference page 43 of the ICOM manual for more information.
4. Hold the F-INP button to key in the frequency manually. Our preferred frequency is 450 MHz Reference page 6 of the ICOM manual for more information.
5. Hold down the MENU button to enter a SET submenu. Reference page 3 of manual.
    a. Press F-1/F-2 to navigate to option 57. Turn main dial to set the 9600 baud rate. Reference page 173.
    b. In the same submenu use F-1/F-2 to navigate to option 61 to set the CI-V rate to 19200 using the main dial. References page three.
    c. Navigate to option 60 to set the CI-V address to an address unique from other radios. Reference page 3.
    d. Press menu to save these settings. Reference page 3.
6. Insure that RF Power knob is turned all the way counter clockwise. Then press the TRANSMIT button to turn the continuous transmission on (The MAIN LED should be red, and on). Then rotate the RF Power knob clockwise to increase power to four bars. Reference page 1 and 3 of the ICOM manual.
    a. Turn the transmission off before proceeding. Make sure the red LED is off or green.
7. Hold down the AM/FM button for one second until a ‘D’ appears. Reference page 43 of the ICOM manual.

ANNEX I: Swapping Out ICOM Radios for Transceiver Testing

Research Lead: MAJ Tyrone Lewis
Intern/Research Assistant: Chris Lomanno
Original Date: ~ 7AUG2015
Editors: Chelsey Moeller and MAJ Tyrone Lewis
Description:

The purpose of this guide is to swap out BRAND NEW ICOM transmitter device radios. Where swap out means that we have a configuration file that selectively communicates to an ICOM device using its uncommented scripts.

If the ICOM serial numbers are *KNOWN, then* follow the instructions in the document "MC3 Users Guide" on page 35 to swap out devices.

When using a radio you have not used before (Unknown Serial ID), follow these instructions to **Find the device ID**.

1) Ensure the cable is connected from the ICOM to PC via USB connection. (INSERT PIC HERE)
2) Open a terminal window to obtain the command prompt for example **[fs7@fs7-1].**
   a. Type in **"lshal -m"**. This command will find all new devices that are attempting to communicate on the USB port going into the PC from the ICOM as connected from step 1.

You'll see a lot of activity in the terminal.

You're looking for some lines that look like:

"usb_device_10c4_ea60_IC_9100_02001255_A added"
"usb_device_10c4_ea60_IC_9100_02001255_A_if0 added"

4) Record the device ID as the number that appears near the end of the line statement above e.g. **"02001255"**.
5) Press Control-C to break out of "lshal -m"
6) Safely remove the ICOM device cable connection from the PC port.

B. After finding the *Device ID* as described above, modify the "99-cga.rules" file so that the code script can find the proper device ID.

1) To Modify the file 99-cga.rules obtain the directory of the file location and type:
   a. "sudo gedit /etc/udev/rules.d/99-cga.rules"
   Alternatively
   b. **"sudo gedit"** //The gedit software opens a blank document
   Click File Open
   Navigate to the file location of the KNOWN stored file for 99-cga.rules.
   Open the file for editing, using gedit.

2) There are groups of four lines of code each prefaced with the comment:

```
"######## Radio 02001003 ##########"
KERNEL==”ttyUSB*”, SYSFS{serial}==”ICOM-9100 02001003 A”, SYMLINK+=”UHFICOM”,
GROUP=”uucp”, MODE=”0666”
KERNEL==”ttyUSB*”, SYSFS{serial}==”ICOM-9100 02001003 A”, SYMLINK+=”ICOM1”,
GROUP=”uucp”, MODE=”0666”
```

where **02001003** is the ID number for the radio.

If there is multiple device IDs listed in the file, then find the radio you wish to communicate with. Ensure the lines corresponding to the four lines of code are not commented out for your device of interest. Comment out all other devices that are not of interest for communication. For example, when the code looks like the sample script below:

```
#########RADIO 02001255#############
KERNEL=="ttyUSB*", SYSFS{serial}=="ICOM-9100 02001255 A", SYMLINK+="UHFICOM",
GROUP="uucp", MODE="0666"
KERNEL=="ttyUSB*", SYSFS{serial}=="ICOM-9100 02001255 A", SYMLINK+="ICOM1",
GROUP="uucp", MODE="0666"

#########RADIO 02001133#############
#KERNEL=="ttyUSB*", SYSFS{serial}=="ICOM-9100 02001133 A", SYMLINK+="UHFICOM",
#GROUP="uucp", MODE="0666"
#KERNEL=="ttyUSB*", SYSFS{serial}=="ICOM-9100 02001133 A", SYMLINK+="ICOM1",
#GROUP="uucp", MODE="0666"

#########RADIO  02001075####################
#KERNEL=="ttyUSB*", SYSFS{serial}=="ICOM-9100 02001075 A", SYMLINK+="UHFICOM",
#GROUP="uucp", MODE="0666"
#KERNEL=="ttyUSB*", SYSFS{serial}=="ICOM-9100 02001075 A", SYMLINK+="ICOM1",
#GROUP="uucp", MODE="0666"
```

Then the code will work for Radio 02001255 but neither of the others.

To add another radio to this script follow the instructions above for copy and paste the four lines as a new entry into the script and then modify the *Device ID* number in the code with the ID number from your new radio (if you don’t know this radio number, see part A).

3) Save the file (99-cga.rules) and close it.

This completes the step to set up a new ICOM and prepare the device for communication between the CGA CentOS< -- > PC < -- > TNC < -- > ICOM

C. Prepare the transceiver to transmit

1. There are two cables to change. Cable one is the TNC to PC (USB – DB-25 and cable two is a DB-15 to DATA2 for the ICOM to TNC. Make sure the Packet Communicator (TNC) is connected properly (via an SHF cable) to the ICOM you are using. Also make sure the ICOM you are using is connected to the receiver properly (via an N-type to SMA connection).

2. Adjust the settings on the ICOM radio. For more information, consult **Annex H**: *Setting Up the ICOM 9100.*

3. See power attenuation calculations for important transmission setting to avoid damage to devices and or personnel.

ANNEX J: How to Set Up the USRP X-310 SDR for Fingerprint Collections

Research Lead: MAJ Tyrone Lewis
Intern/Research Assistant: Evan Kain
Original Date: ~08AUG2015
Editor/s: Chelsey Moeller
Description:

The purpose of this guide is to explain the physical connections needed for proper set up of the X-310.

- **Hardware**
  - Make: Ettus
  - Model: USRP X310
  - Serial Number: F4F7CC
  - Firmware Version: 11
  - IP Address: 192.168.10.2
  - Gain: 18dB
  - Recording Center Frequency: 449.8MHz
  - Sampling Rate: 5MSPS
  - Save File Location: Internal Hard Drive of Receiving Laptop

Note: GNU Radio will need to be set up on PC2, for recording with the X-310.

1. Plug the X-310 into a power outlet using the power cord included.
   a. The power cord will connect to the SDR using the port labeled “PWR” on the far left of the rear panel.
2. Connect the SDR to the recording laptop using a 1G Ethernet cable.
   a. The cable will connect to the SDR using the leftmost Ethernet port labeled “1G/10G ETH.” This port will be the first Ethernet port from the left on the rear panel on the X-310.
   b. The Ethernet cable will also connect to the left Ethernet port of PC2. This port is found on the left side near the rear of the laptop.
3. Connect the recording antenna or wired antenna connection using the SMA connection labeled “TX/RX” inside the “RF A” section on the front panel of the SDR.
   a. The SMA connection will be the second connection from the left.
4. Turn the power on using the “PWR” button on the far right of the front panel.
5. Warning: Do not send more than -15 dBm of power for the “TX/RX” connection. You will damage the X-310.

ANNEX K: How to Install GNU Radio v1

Research Lead: MAJ Tyrone Lewis
Intern/Research Assistant: Chelsey Moeller
Original Date: 27Aug2015
Editor/s:
Description:

This guide is to help you install GNU Radio on your recording laptop (PC2). If GNU Radio is already installed you can skip to **Annex A**: *Operation of CGA on PC1* and **Annex H**: *Setting Up the USRP X-310 SDR*. **Annex B**: *Setting Up the Recording Laptop (PC2*) has information on software needs.

1. First you will need to open a terminal in your PC2.
2. You will need to download GNU Radio. If you have already done this skip to step three. To download
    a. Type "**git clone http: //gnuradio.org/git/gnuradio.git**"
    b. Or type "**git clone git: // gnuradio.org/gnuradio.git**"
3. Now you need to configure and build your GNU radio.
    a. Type in the terminal window:
        i. **cd gnuradio**
        ii. **mkdir build**
        iii. **cd build**
        iv. **cmake ../**
        v. **make**
4. After you build the GNU radio you need to do software self-check.
    a. Type into the terminal window "**make test**"
5. You can now install the GNU radio for general use.
    a. Type in the terminal window "**sudo make install**"

ANNEX L: How to Calculate Load Attenuation for Power Transmission

Research Lead: MAJ Tyrone Lewis
Intern/Research Assistant: Daniel Crane
Original Date: 14Aug2015
As of Date: 24SEP15
Editor/s: Chelsey Moeller, Tyrone Lewis

Power Loss between the ICOM and X310.
We connect the ICOM to the X310 through:

1) an N-type to female SMA cable
2) A male SMA to female BNC adapter
3) A 2.5 foot coaxial cable
4) A female BNC to female BNC adapter
5) A second 2.5 foot coaxial cable identical to (3)
6) A female BNC to female SMA adapter
7) A 30 db attenuator
8) A second 30 db attenuate (identical to (7))
9) A SMA cable

Total Loss:

Rough estimates for the loss in each of the nine wires or adapters.

1) A rough estimate I found was 0.78 dBs'
2) A maximum of 0.5 dBs and a minimum of 0.03 dBs'
3) About 0.425 dBs
4) Less than 0.1 dBs
5) 0.425 dBs
6) Max of 0.5 dBs and min of 0.03 dBs'
7) 30 dBs (obviously)
8) 30 dBs
9) 0.2 dBs

Altogether, the total dB drop from the ICOM to the X310 will be:
0.78+0.5+0.425+0.1+0.425+0.5+30+30+0.2 = 62.93 dBs'

Thus, because the maximum dBm the X310 can take is -15 dBm, the maximum power we can send from the ICOM will just be -15+62.93 = 47.93 which is equal to 62.087 Watts. However, because our attenuators are only rated at 20 Watts we certainly don't want to be transmitting at over 20 Watts anyway. We also don't want to be sending almost exactly -15 dBm' s into the X310. But this does show us that we may increase the power coming from the ICOM if we wish. Figure 47 provides a quick reference for estimated power for the X310.

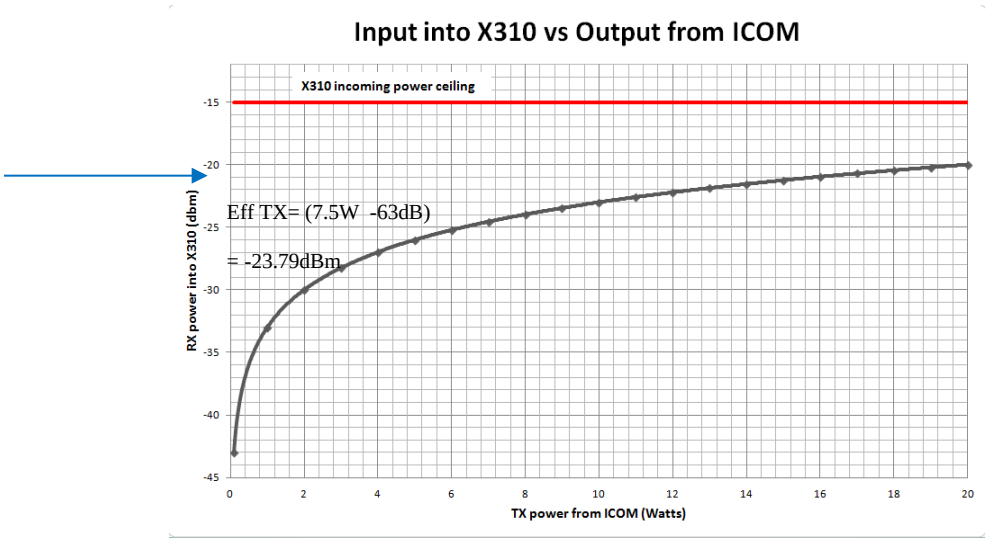


Figure 47. Load Attenuation for TX-RX Transmissions

Table 32. Power Attenuation

Watts	dBM	-Loss ~63dB
0.000032	-15	-77.5475
0.0001	-10	-72.5475
0.000316	-5	-67.5475
0.000794	-1	-63.5475
0.001	0	-62.5475
0.002	3.0103	-59.5372
0.003	4.771213	-57.776287
1	30	-32.5475
2	33.0103	-29.5372
3	34.771213	-27.776287
4	36.0206	-26.5269
5	36.9897	-25.5578
6	37.781513	-24.765987
7	38.45098	-24.09652
7.5	38.750613	-23.796887
8	39.0309	-23.5166
9	39.542425	-23.005075
10	40	-22.5475
11	40.413927	-22.133573
12	40.791812	-21.755688
13	41.139434	-21.408066
14	41.46128	-21.08622
15	41.760913	-20.786587
16	42.0412	-20.5063
17	42.304489	-20.243011
18	42.552725	-19.994775
19	42.787536	-19.759964
20	43.0103	-19.5372
30	44.771213	-17.776287
40	46.0206	-16.5269
50	46.9897	-15.5578
60	47.781513	-14.765987
70	48.45098	-14.09652
80	49.0309	-13.5166
90	49.542425	-13.005075
100	50	-12.5475

ANNEX M: Naming Conventions Data File Storage

Research Lead: MAJ Tyrone Lewis
Intern/Research Assistant: Chelsey Moeller
Original Date: 27Aug2015
Editor/s:
Description:

The purpose of the R data store is for storage directly from the capturing device. It stores raw data as IQ data, and has the following naming convention:

<make>_<model>_<serial number or other unique device identifier>_g_<gain in dB on SDR settings>_p_<transmission power (preferably in Watts, but in visual bars for now)>

The following is an example of this naming convention for an ICOM 9100 with the serial number 02005468 collected using a receiver gain of 24dB and a transceiver power of 3 bars:

ICOM_9100_5468_g_24_p_3

The R data store allows for the data to be transported quickly and easily from PC2 to PC3. In order to store files in the R data store, the SDR recording command's (see annex <number>) filename parameter will have a filename that uses the naming convention given above. After this initial storage, the data is moved from PC2 to a removable hard drive and again to PC3 form the removable hard drive.

The **N** data store provides a .mat file which contains the variables and parameters used for pulse detection as well as statistic generation. In addition, it houses variables which contain these pulses and statistics. The data store has the following format:

Section 1:<make>_<model>_<serial number or other unique device identifier>_
Section 2: g_<gain in dB on SDR settings>_ p_<transmission power (preferably in Watts, but in visual bars for now)>_analysis_bursts

Section 1 is then repeated and concatenated for each device. Section 2 is then appended to the repeated section 1. The following is an example of this naming convention for several ICOM 9100 transceivers with the serial numbers 02001234, 02001255, 02001003, 02001235, and 02009876 collected using a receiver gain of 18dB and a transceiver power of 4 bars:

ICOM_9100_1234_ ICOM_9100_1255_ ICOM_9100_1003_ ICOM_9100_1235_ ICOM_9100_9876_g_18_p_4_analysis_bursts

The purpose of the N data store is to pre-process the raw IQ data into pulses that can be easily read by MATLAB scripts and compute the statistics needed for fingerprint generation. The **A** data store holds the computed fingerprints from the tested devices. It contains statistics, features, and full fingerprints which are used to identify the various devices. Each file in the data store is named according to the following convention:

Section 1:<make>_<model>_<serial number or other unique device identifier>_

Section 2: g_<gain in dB on SDR settings>_ p_<transmission power (preferably in Watts, but in visual bars for now)>_fingerprints

Section 1 is then repeated and concatenated for each device. Section 2 is then appended to the repeated section 1. The following is an example of this naming convention for an ICOM 9100 with the serial number 02004968 collected using a receiver gain of 12dB and a transceiver power of 5 bars:

ICOM_9100_4968_g_12_p_5_fingerprints

The purpose of the A data store is to hold a fingerprint file which can be easily loaded into and used by the classification and verification programs.

Note: The 0200 at the beginning of the ICOM 9100 serial numbers is common to all ICOM 9100 transceivers and is thus omitted.

ANNEX N: How to Capture Waveform Data Instructions

Research Lead: MAJ Tyrone Lewis
Intern/Research Assistant: Daniel Crane
Original Date: 14Aug2015
Editor/s: Chelsey Moeller

1. Turn on transmission computer
2. Turn on Kantronics Packet Communicator
3. Turn on ICOM radio
4. Turn on SDR
5. Turn on receiving computer.
6. Check physical connections from the transmission computer to the packet communicator to the ICOM to the SDR to the receiving computer
7. Open X-CTU software on transmission computer.
    a. If screen has unintelligible output, press * and then enter call sign
    b. If screen has ".cmd," type "intface"
        i. If the output is not "intface kiss," type "intface kiss"
    c. If screen has no output cycle the power by turning it off, waiting five seconds, and then turning it on again.
        i. Keep cycling the power until there is output on the screen.
8. Type |2a to change the port to 2a.
9. Click "assemble packet," type a packet payload, and click "send packet."
10. If red "XMit" light does not light up on packet communicator, there is a problem with the computer to packet communicator connection.
    a. Type "convers" into the X-CTU terminal to enter conversation mode.
    b. Try sending a packet again.
    c. If this does not work, cycle the power.
    d. If this does not work, there may be a problem with the physical connection.
11. Follow Chris Lomanno' s MC3 ground station commander instructions to switch ICOM configurations for the transmission computer as well as the transmitted command and payload.
12. Configure ICOM to transmit at 450MHz from the main band.
    a. Hit AM/FM button until FM frequency band is selected.
    b. Hold the F-INP button to begin keying in the frequency using the numbered buttons on the top left of the front face of the ICOM.
    c. Hold the MENU button for 1 second to enter the SET submenu.
    d. Press F-1 or F-2 to navigate to option 57, the 9600 baud rate.
    e. Rotate the main dial to turn this option on.
    f. Navigate to option 61 to set the CI-V rate to 19200 using the F-1 and F-2 buttons as well as the main dial.
    g. Navigate to option 60 to set the CI-V address to an address unique from the other radios.
    h. Press menu to save these settings.

i. Briefly press TRANSMIT to turn continuous transmission on (the MAIN LED should be red) and rotate the RF POWER knob clockwise to increase or counter-clockwise to decrease RF power to 4 bars.
j. Make sure the MAIN LED is green or off before transmission. If the light is red, press the TRANSMIT button to turn off continuous transmission.
k. Hold AM/FM button until a D appears in the top left corner of the display screen to turn the data mode on.

13. Open the Linux command terminal on the receiving computer.
14. Type the uhd_rx_cfile recording command found in memory.
    a. The following settings should be saved
        i. addr=192.168.10.2
        ii. f: 449.8e6 Hz
        iii. g: 18dB
        iv. samp-rate: 5e6 samples/second
        v. filename follows format laid out earlier in documentation (“debug_dev_<device id>_g_<gain in dB>_p_<bars of power on ICOM>
    b. Note: To access a GUI for an fft, replace ud_rx_cfile with uhd_fft and remove the file name from the recording command.
15. After the receiving computer indicates that it is successfully recording, wait 20 seconds and begin sending packets from the transmission computer.
16. Copy the bit file from the home folder of the receiving computer to an external drive.

Eject the drive, and move the file from the removable drive to the desktop computer to be processed.

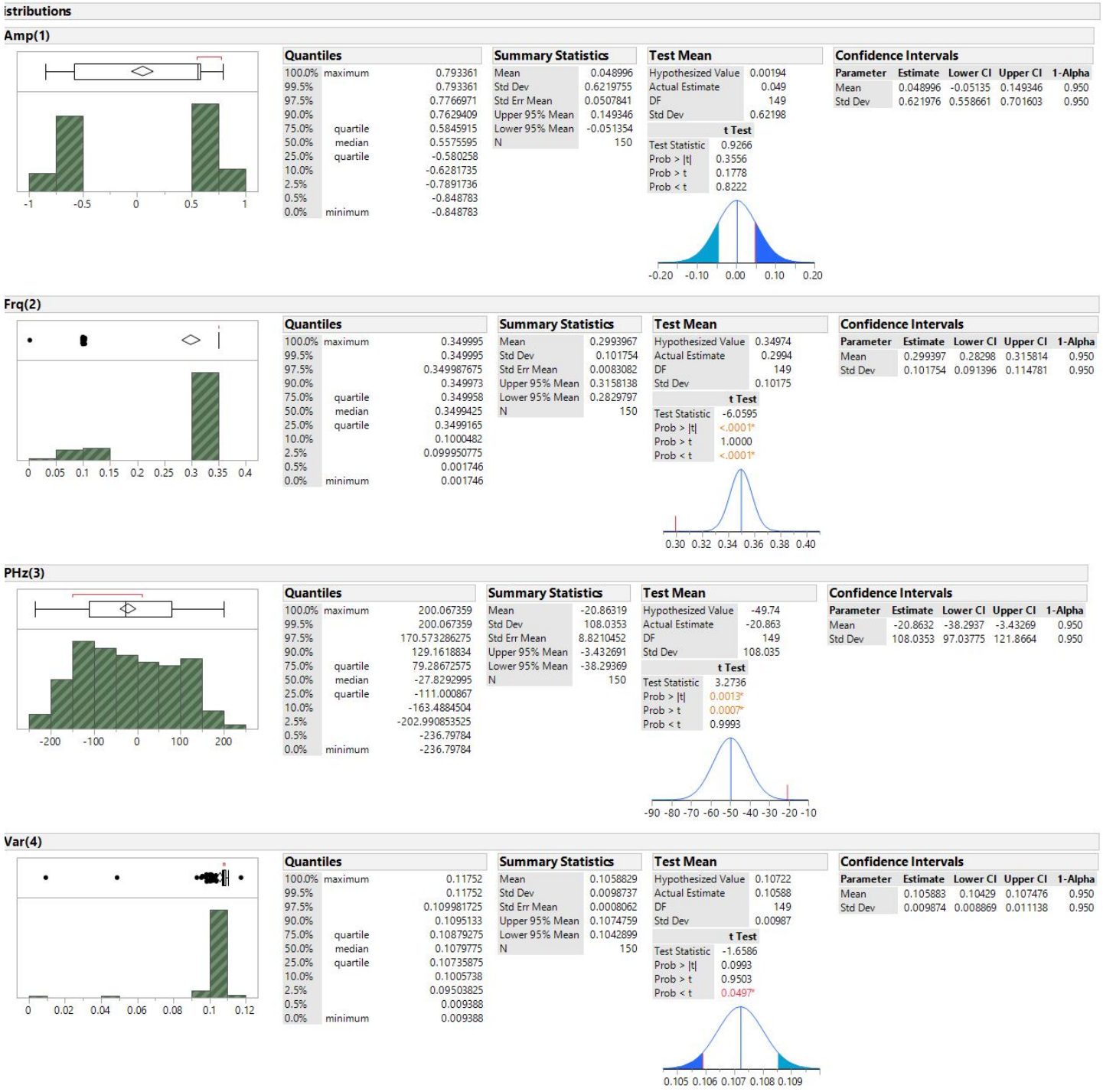


Figure 48. Statistics for RF-Biomarker Candidates b1-b4

ANNEX O: Simple Gold Standard Truth Reference File Set-Up

Table 33. A2 Gold Standard Validation Development

RF-DNA Marker Exchanges: Gold Standard Truth Reference file

Inputs:
D = Infectious // Infectious Pulses that may cause Network Disease
B = Claim // Benign Pulses that are not attributable to Network Disease
p = // threat Prevalence Rate
TRUTH = [1, 1, 1, … 1]; // True Condition of Pulse in Claim file All Ones
GSClaim = [Claim Truth];

Begin

```
InfectedRows = randperm(size(GSClaim,1));
if p > 0
        for v = 1:length(InfectedRows)
            GSClaim(INF(v),:) = D(INF(v),:); % <--- Infectious
Payload
            TRUTH(INF(v),:) = 0;
        end
    end
    B = GSClaim;
```

Return: GSClaim

ANNEX P: Wired RF-DNA Collections Configuration

P1. Preliminary Configuration

The very nature of the generated waveform and its fingerprinted regions is directly related to a statistical RF-DNA result since the waveform is a direct product of the signal transformations that propagate through a physical circuit. The wired circuit depicted in Figure 49 represents the resulting RF lab experimentation circuit for RF-DNA collections and performance testing. Each component of the circuit is labeled with a letter. After each label, the component's role is provided along with a corresponding icon. For example, the device used to generate the initial message for collections is shown as (label | description) PC1| PC1: msg (message) generator in Figure 49a.

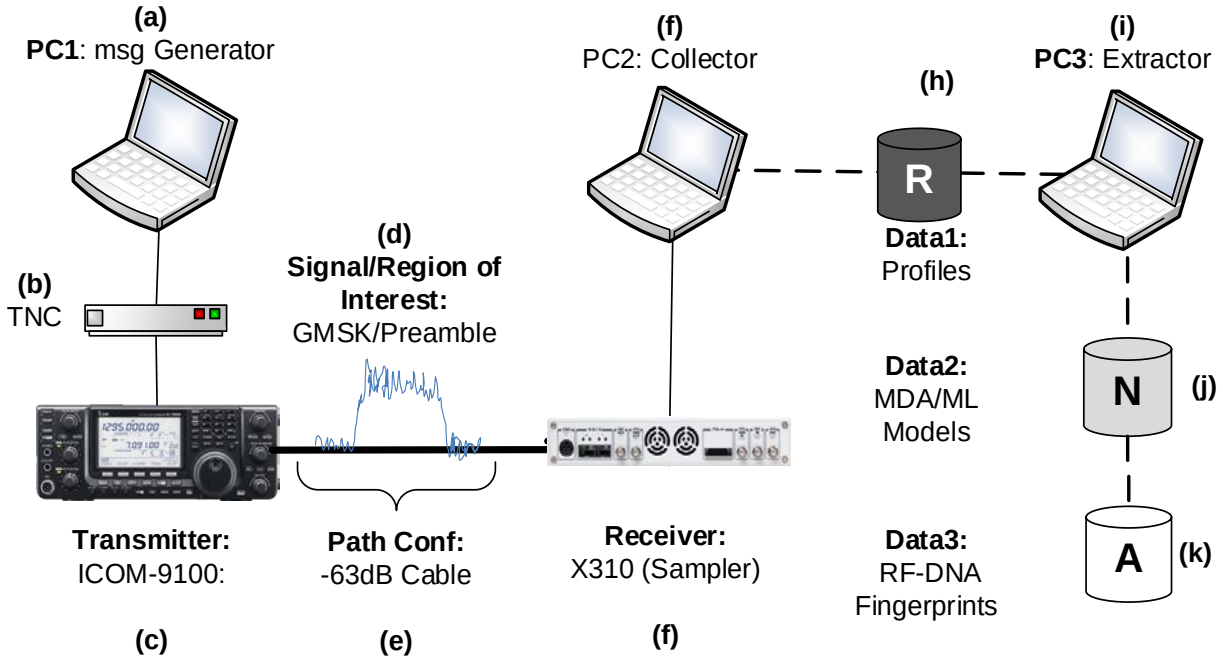


Figure 49. Wired Uplink Circuit for RF-DNA Fingerprint Collections

For each device of interest, PC1 passes a series of *msg* to the terminal node controller TNC (b) using a serial RS232 connection. The TNC converts the *msg* using AX.25 and transmits *msg* to the UHF ICOM-9100 transceiver (c). The transceiver wraps the *msg* using a GMSK modulated waveform to produce the analog SOI (d) with an estimated output power of 7.5W through the wired connection (e). The wired cable induces a 63dB load attenuation of the ICOM's output power. The X310 (g) software defined radio (SDR) receives and collects samples from the SOI at a rate of 5Ms/s with an 18dB SNR gain. As the X310 samples of each incoming waveform's modulated *msg*, the distinct characteristics contained in each burst sample are stored in PC2 (f) in a raw file format in ***R*** (h) as instantaneous amplitude, frequency and phase values. PC3 (i) is then used to extract the statistical RF-DNA fingerprints from (h) using specified ROIs and feature setting parameters.

P2. Improved Configuration Using Point to point SDRs

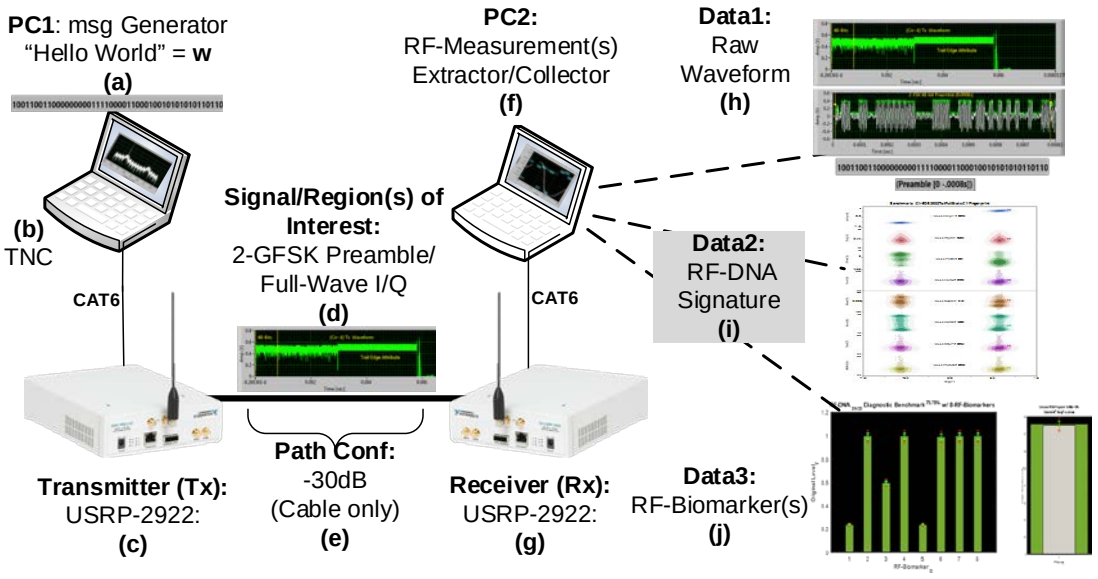


Figure 50. Improved RF-DNA Benchmarking Configuration

P3. Improved Configuration for ICOM-9100 Collections

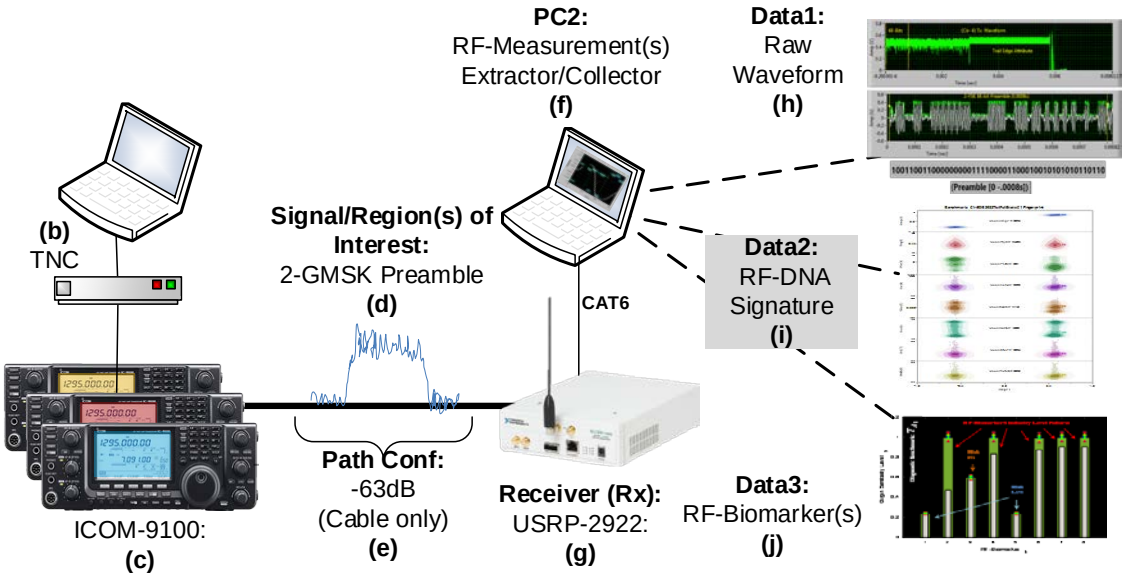


Figure 51. ICOM-9100 Using USRP 2922 as RF-DNA Credential Extractor.

P4. Improved Configuration for Abuse Case and Near Real-Time Analysis

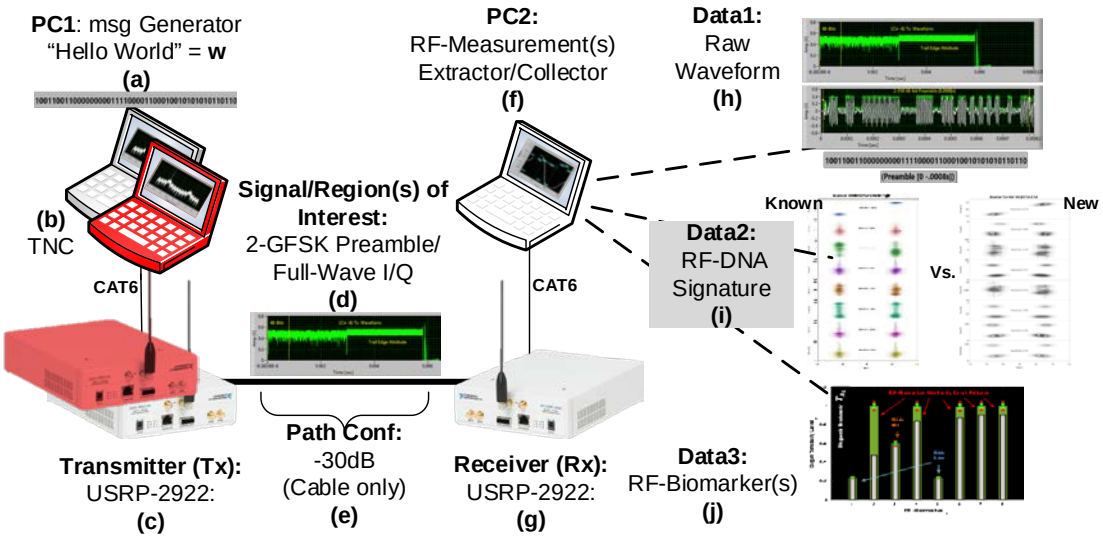


Figure 52. Experimental Configuration for Real-Time Test (Wireless Only!!)

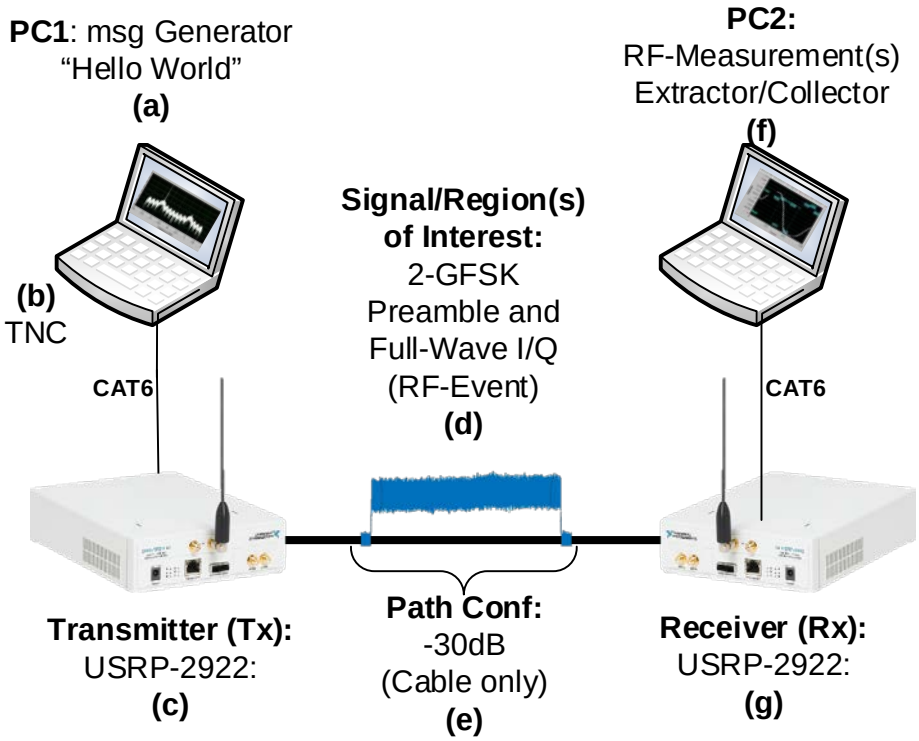


Figure 53. Simple circuit diagram

Table 34. LabVIEW settings for RF-DNA Collection Profiling

Receiver ID	USRP2922 (Cir4) Collector 2
Transmitter ID	USRP2922 Collector 1 (Cir5)
Environmental Conditions	Wireless Chamber
Collected SNR	18
Modulation Scheme	2-FSK
Carrier Frequency	449.900M
Filter Frequency (Offset From Center Frequency)	100.000k
Sampling Rate	1.000M
Pulse Duration	6.399m
Number of Pulses	1.100k
Sampled Points in Each Pulse	6.400k
Pulse Length in Samples	6.390k
Trigger Amplitude Threshold	300.000m
Percentage from Beginning of Pulse	0
Percentage from End of Pulse	18
NZ Samples Before Pulse	10
Demodulation	None
Bandwidth	20.000k
FM Deviation	450.000M
FSK Deviation	1
# Subregions	10
# Subsections	8
Output Bit Stream	

ANNEX Q: Tolerance Region Calculations

```
%% ToleranceFactorGK(n,coverage,confidence,m,nu,d2)
% Call the function called "ToleranceFactor.m" to compute the tolerance
% region.  Provide the following inputs
n= 150; % numberOfIncPulses;
m = 1; % Number of independent samples
nu = m*(n-1);
d2 = 1/n;
alpha = .05; % Confidence Significane level
% proportion = 1-tol; % Use to make Ty's method equivalent to this one
proportion = .95; % Content of Population considered
coverage = 1 - proportion;
confidence = 1 - alpha;
kFactor = ToleranceFactorGK(n,coverage,confidence)

%% Run Loop after Computing Tolerance Region/Interval
for k2=kFactor;
    for l = 1:size(Y,2);
        pdX=fitdist(Y(:,l),'Normal');
        ci = paramci(pdX,'Alpha',alpha);
        % Added the abs function to avoid negative levels
        z3U = abs(mean(ci(:,1)+ (k2*mean(ci(:,2)))/1));
        z3L = abs(mean(ci(:,1)- (k2*mean(ci(:,2)))/1));
        z2U = abs(mean(ci(:,1)+ (k2*mean(ci(:,2)))/2));
        z2L = abs(mean(ci(:,1)- (k2*mean(ci(:,2)))/2));
        z1U = abs(mean(ci(:,1)+ (k2*mean(ci(:,2)))/3));
        z1L = abs(mean(ci(:,1)- (k2*mean(ci(:,2)))/3));
        % 2- Return 8x6 Zone Boundaries for AvgRFDNASig
        zonesTOL = [zonesTOL; z3U z2U z1U z1L z2L z3L];
        ciTOL = [ciTOL; ci];
    end
end
% ---> END Tolerance Interval Zone
References:  [60] [67].
```

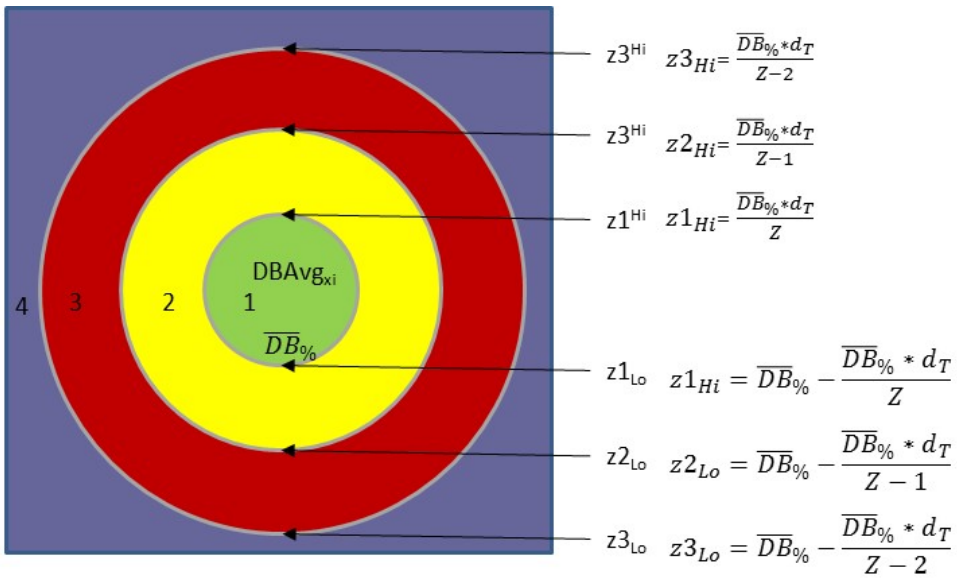


Figure 54. RF Origin Integrity Risk Acceptance

ANNEX R: Interactive Trust Algorithm Extensions

```
% Interactive Trust Algorithm Extensions
Defaults
% Goal = 1;
% PhiUPP = 1;
% PhiLOW = 1;
% CounterE = 0;
% MAXPENALTY = 1; %Between 2 and 2.5
% MEDPENALTY = 1; %Between 1 and 2 FOR CASE E
% Bonus = 1;
% Reward_Offset1 = 1;
for i= 1:min(length(SCA),length(GSMatrix))

    %% Set Up Transaction Settings for System State Classification and I-Trust Marker adjustments
    % Factor 2 is new,  Given Status of F1 = 1 here is CLAIMED.  Implies a logical mechanism has
authenticated the transaction.
    % If F2 = 0, then this credential has failed even though F1 Passed.
    %% ADD PHYSICAL RF-DNA TEST HERE
    if RF_DNASupport == 1  % RF-DNA Augmentation is ON
        % F1 = Factor 1 = Logical (Bits) Classified Result
        F1 = round(SCA(:,i)); % Factor 1 (ITV AuthCount Credential Result)
        %         F2 = round(SCA(:,i));
        %         F2 = Factor 2 = Physical (RF-Measurment) Classified Result
        F2 = round(F2_TRUTH(:,i)); % Factor 2 (FPrint auth credential Status Result)
        %         F2 = round(RFDNA_dT(:,i)); % Factor 2 (FPrint auth credential Status Result)
        %         F2 = round(RF_DNAodT(:,i)); % Binary test Result Using Ordinal dT
        %         F2 = round(RF_DNAzdT(:,i)); % Binary Test using Continuous dT
        %         F2 = ZEROS(:,i);
        %         F2 = F1;

        %% Compute Extension parameters if RF-DNA Augmentation is "ON"
        if F1 == 1 && F2 == 1 && RF_DNASupport ==1
            %             a = a*(2); % Bonus Calculation
            a = a*(Bonus);
            Reward_Offset1 = a;
        elseif F1 == 1 && F2 == 1 && RF_DNASupport ==0
            a=a;
            Reward_Offset1 = 1;
            ForgiveFactor = 1;
        end
        % CASE E GOAL:  Decrease Reward because Fingerprint Failed
        if F1 == 1 && F2 == 0 && RF_DNASupport ==1;
            %             ForgiveFactor = 1;
            PHI = MEDPENALTY;
            B = (B_start)*PHI;
            CounterE = CounterE + 1;
            Reward_Offset1 = 1;
        elseif F1 == 1 && F2 == 0 && RF_DNASupport ==0;
            Reward_Offset1 = 1;
            B = B;
        end
        % CASE F
        if F1 == 0 && F2 == 1 && RF_DNASupport ==1 && Goal == 1
            PHI = PhiUPP;
            PHI = .2
            ForgiveFactor = PHI;
        elseif F1 == 0 && F2 == 1 && RF_DNASupport ==1 && Goal == 0
            PHI = PhiLow;
            ForgiveFactor = PHI;
        end
        % CASE D
        if F1 == 0 && F2 == 0 && RF_DNASupport ==1
            ForgiveFactor = .75;
            PHI=MAXPENALTY;  % Use [2, {MAXPENALTY = 2.25}, 2.5, 2.75, 3]
            B = (B_start)*PHI;
            B = B*PHI;  % Use if testing RF_DNASupport ON|OFF
```

```
        elseif F1 == 0 && F2 == 0 && RF_DNASupport ==0
            %             PHI=1;
            %             B = B*PHI;
            ForgiveFactor = 1;
            Reward_Offset1 = 1;
        end
    else
        %% RF-DNA Augmentation OFF
        % USE Default 2-State system parameters for initialization
        F1 = round(SCA(:,i)); % Factor 1 (ITV AuthCount Credential Result)
        %         F2 = 0;  % RF-DNA Augmentation is OFF
        F2 = F1; % RF-DNA Augmentation is OFF
        %          F2 = round(RFDNA_dT(:,i));
        Reward_Offset1 = 1;
        ForgiveFactor = 1;
    end

    %% CASE C When Open_Session_Tij > 0 && [F1 = 1, F2 = 1]
    % If [L=1,P=1] & Prev_Trust > 0
    if F1 == 1 && F2 == 1 && Open_Session_Tij > 0
        C = 1;  % ValidUser & Valid Device  % Classify Transaction as Cooperation in nature
        %Con-Man Extension Updates for COOPERATION interaction
        B = B;
        Gamma_coop_DISC = 1 - abs(B);
        a = min((a + Gamma_coop_DISC * (a_start - a)),a_start); % a is never > a_start
        % END CON-MAN Extensions
        Current_Tij = (Open_Session_Tij + (a*(1-Open_Session_Tij))); % Yu Ver
        %         Current_Tij = (Open_Session_Tij + (a*(1-Open_Session_Tij)))*Bonus; % Ty Ver
        %         Current_Tij = (Open_Session_Tij + a)/(1-min((abs(Open_Session_Tij)),abs(a)))%
Duncan ver
        Close_Session_Tij = Current_Tij;
        Trust_Vector = [Trust_Vector; Close_Session_Tij];
        Open_Session_Tij = Close_Session_Tij;
        CountCoop = CountCoop + 1;

        %% CASE C when Open_Session_Tij < 0 F1 = 1 F2 = 1  [L=1,P=1] Tij <0
    elseif F1 == 1 && F2 == 1 Open_Session_Tij < 0
        C = 1;  % ValidUser & Valid Device  % Classify Transaction as Cooperation in nature
        B=B;
        Gamma_coop_DISC = 1 - abs(B);
        a = min((a + Gamma_coop_DISC * (a_start - a)),a_start); % a is never > a_start
        Current_Tij = (Open_Session_Tij + a)/(1-min((abs(Open_Session_Tij)),abs(a))); % Yu Ver
        %         TransTrustCals = (Open_Session_Tij + (a*(1-Open_Session_Tij))) %Duncan Version
        %         Current_Tij = (Open_Session_Tij + (a*(1-Open_Session_Tij)))*Bonus; % Ty Ver
        Close_Session_Tij = Current_Tij;
        Trust_Vector = [Trust_Vector; Close_Session_Tij];
        Open_Session_Tij = Close_Session_Tij;
        CountCoop = CountCoop + 1;

        %% CASE C when Open_Session_Tij == 0 F1 = 1 F2 = 1 [L=1,P=1]
    elseif  F1 == 1 && F2 == 1 && Open_Session_Tij == 0;
        C = 1;  % ValidUser & Valid Device  % Classify Transaction as Cooperation in nature
        %Con-Man Extension Updates to a for COOPERATION interaction
        Gamma_coop = eC * abs(Open_Session_Tij);
        a = min((a + Gamma_coop_DISC * (a_start - a)),a_start); % a is never > a_start
        B=B;
        Current_Tij = (a); %Yu Ver
        %             Current_Tij = (Open_Session_Tij + a)*Bonus; % Ty Ver
        Close_Session_Tij = Current_Tij;
        Trust_Vector = [Trust_Vector; Close_Session_Tij];
        Open_Session_Tij = Close_Session_Tij;
        CountCoop = CountCoop + 1;
        %If Interaction == DDEFECTION (D) then compute trust as follows

        %% CASE E When Open_Session_Tij > 0  F1 = 1 F2 = 0  [L=1,P=0]
        % Moderate Forgiveness Here
        % Attack Category:  Outsider Threat (IMPOSTER ACTOR)
        % Logical Mechanism Result is Positive
        % Physical Mechanism Result is negative for Fingerprint match and
```

```
        % is referred to as being potentially INFECTIOUS
        % GOAL:  Reduce REWARD since FINGERPRINT MATCH FAILED!!
    elseif  F1 == 1 && F2 == 0 && Open_Session_Tij > 0
        E = 1;% AuthUserOnly & InvalidDevice Fingerprints Out of Tolerance
        %%Con-Man Extension Updates to a for COOPERATION interaction
        B=B;
        Gamma_coop_DISC = 1 - abs(B);
        %         a = min((a + Gamma_coop_DISC * (a_start - a)),a_start); % a is never > a_start
        %Start Test
        if RF_DNASupport ==0
            a = (min((a + Gamma_coop_DISC * (a_start - a)),a_start)*Reward_Offset1); % Ty Version
        else
            a=0;  % No forgiveness increase Bonus is given in this case
            %             a = (min((a + Gamma_coop_DISC * (a_start -
a)),a_start)*Reward_Offset1); % Ty Version
        end

        Current_Tij = (Open_Session_Tij + (a*(1-Open_Session_Tij))); % Yu Ver
        %         Current_Tij = (Open_Session_Tij + (a*(1-Open_Session_Tij)))*Bonus; % Ty Ver
        %             Current_Tij = (Open_Session_Tij + a)/(1-
min((abs(Open_Session_Tij)),abs(a)))% Duncan ver
        Close_Session_Tij = Current_Tij;
        Trust_Vector = [Trust_Vector; Close_Session_Tij];
        Open_Session_Tij = Close_Session_Tij;
        CountEImposter = CountEImposter + 1;

        %% CASE E and Open_Session_Tij < 0 F1 = 1 F2 = 0
    elseif F1 == 1 && F2 == 0 && Open_Session_Tij < 0
        %Con-Man Extension Updates to a for COOPE
        E = 1;% AuthUserOnly & InvalidDevice Fingerprints FPRINT = INFECTIOUS
        B=B;
        Gamma_coop_DISC = 1 - abs(B);
        if RF_DNASupport ==0
            a = min((a + Gamma_coop_DISC * (a_start - a)),a_start)*Reward_Offset1; % Ty Version
RFDNA AUG
            Current_Tij = (Open_Session_Tij + a)/(1-min((abs(Open_Session_Tij)),abs(a)));
        else
            Gamma_def_DISC = eC * abs(Open_Session_Tij);
            B = (B - Gamma_def_DISC * (1 + B))*ForgiveFactor;% RFDNA Penalty(Ty)
            a = a * (1 - abs(B));
            Current_Tij = (Open_Session_Tij + (B*(1+Open_Session_Tij)));% Yu Version
        end
        Close_Session_Tij = Current_Tij;
        Trust_Vector = [Trust_Vector; Close_Session_Tij];
        Open_Session_Tij = Close_Session_Tij;
        CountEImposter = CountEImposter + 1;
        %% CASE E when Open_Session_Tij == 0 F1 = 1 F2 = 0
    elseif F1 == 1 && F2 == 0 && Open_Session_Tij == 0;
        E = 1;% AuthUserOnly & InvalidDevice
        Gamma_coop_DISC = 1 - abs(B);
        B=B;
        Gamma_coop = eC * abs(Open_Session_Tij);
        %         a = min((a + Gamma_coop_DISC * (a_start - a)),a_start); % a is never > a_start
        a = min((a + Gamma_coop_DISC * (a_start - a)),a_start)*Reward_Offset1; % Ty Version RFDNA
Aug
        % Notice that --> "Open_Session_Tij" == 0
        Current_Tij = (Open_Session_Tij + a); % Yu Ver
        Current_Tij = (a); % Yu Ver
        Close_Session_Tij = Current_Tij;
        Trust_Vector = [Trust_Vector; Close_Session_Tij];
        Open_Session_Tij = Close_Session_Tij;
        CountEImposter = CountEImposter + 1;
    end

    %%  Case F When Open_Session_Tij > 0 F1 = 0 F2 = 1
    % Normally we would Penalize for a Incorrect Bit- Sequence
    % Here, we consider a fingerprint match and we decrease the penalty for
    % such an incorrect logical sequence.  The trust is still decreased, but at a reduced
       Rate.  Beware!!! This could indicate an INSIDER THREAT
```

```
    if F1 == 0 && F2 == 1 && Open_Session_Tij > 0
        F = 1; % InvalidUser & AuthDeviceOnly
        %Con-Man Extension Updates to a for DEFECTION interaction
        Gamma_def_DISC = eC * abs(Open_Session_Tij);
        B = (B - Gamma_def_DISC * (1 + B))*ForgiveFactor;%RF Penalty(Ty ver)
        a = a * (1 - abs(B)); % Reward/ Forgiveness
        %         B = (B - Gamma_def_DISC * (1 + B)) % Duncan Ver
        Current_Tij = (Open_Session_Tij + B)/(1-min(abs(Open_Session_Tij), abs(B)));% Yu Version
        %             TransTrustCals = (Open_Session_Tij + (B*(1-Open_Session_Tij))) %Duncan Vers
        Close_Session_Tij = Current_Tij;
        Trust_Vector = [Trust_Vector; Close_Session_Tij];
        Open_Session_Tij = Close_Session_Tij;
        CountFCon = CountFCon + 1;

        %%  Case F When Open_Session_Tij < 0 F1 = 0 F2 = 1
    elseif F1 == 0 && F2 == 1 && Open_Session_Tij < 0
        F = 1; % InvalidUser & AuthDeviceOnly
        %Con-Man Extension Updates to a for DEFECTION interaction
        Gamma_def_DISC = eC * abs(Open_Session_Tij);
        B = (B - Gamma_def_DISC * (1 + B))*ForgiveFactor;%RF Penalty Reduction(Ty ver)
        a = a * (1 - abs(B));
        %         B = B - Gamma_def * (1 + B);
        Current_Tij = (Open_Session_Tij + (B*(1+Open_Session_Tij)));% Yu Version
        %             Current_Tij = (Open_Session_Tij + B)/(1-min(abs(Open_Session_Tij),
abs(B)))% Duncan Version
        Close_Session_Tij = Current_Tij;
        Trust_Vector = [Trust_Vector; Close_Session_Tij];
        Open_Session_Tij = Close_Session_Tij;
        CountFCon = CountFCon + 1;

        %%  Case F When Open_Session_Tij == 0 F1 = 0 F2 = 1
    elseif F1 == 0 && F2 == 1 && Open_Session_Tij == 0;
        F = 1; % InvalidUser & AuthDeviceOnly
        %Con-Man Extension Updates to a for DEFECTION interaction
        Gamma_def_DISC = eC * abs(Open_Session_Tij);
        %         B = B - Gamma_def * (1 + B);
        B = (B - Gamma_def_DISC * (1 + B))*ForgiveFactor;%RFDNA Penalty(Ty)
        a = a * (1 - abs(B));
        Current_Tij = (Open_Session_Tij + B);
        Close_Session_Tij = Current_Tij;
        Trust_Vector = [Trust_Vector; Close_Session_Tij];
        Open_Session_Tij = Close_Session_Tij;
        CountFCon = CountFCon + 1;

 %%  Case D When Open_Session_Tij > 0 F1 = 0 F2 = 0
    elseif F1 == 0 && F2 == 0 && Open_Session_Tij > 0
        D = 1; % InvalidUser & InvalidDevice
        %Con-Man Extension Updates to a for DEFECTION interaction
        Gamma_def_DISC = eC * abs(Open_Session_Tij);
        %         B = B - Gamma_def_DISC * (1 + B); %Duncan Ver
        B = (B - Gamma_def_DISC * (1 + B))*ForgiveFactor;% RFDNA Penalty(Ty)
        a = a * (1 - abs(B));
        Current_Tij = (Open_Session_Tij + B)/(1-min(abs(Open_Session_Tij), abs(B)));% Yu Version
        % TransTrustCals = (Open_Session_Tij + (B*(1-Open_Session_Tij))) %Duncan Vers
        Close_Session_Tij = Current_Tij;
        Trust_Vector = [Trust_Vector; Close_Session_Tij];
        Open_Session_Tij = Close_Session_Tij;
        CountDefect = CountDefect + 1;

        %%  Case D When Open_Session_Tij < 0 F1 = 0 F2 = 0
    elseif F1 == 0 && F2 == 0 && Open_Session_Tij < 0
        D = 1; % InvalidUser & InvalidDevice
        %Con-Man Extension Updates to a for DEFECTION interaction
        Gamma_def_DISC = eC * abs(Open_Session_Tij);
        %             B = B - Gamma_def_DISC * (1 + B); %Duncan Ver
        B = (B - Gamma_def_DISC * (1 + B))*ForgiveFactor;% RFDNA Penalty(Ty)
        a = a * (1 - abs(B));
        Current_Tij = (Open_Session_Tij + (B*(1+Open_Session_Tij)));% Yu Version
```

```
        %         Current_Tij = (Open_Session_Tij + B)/(1-min(abs(Open_Session_Tij), abs(B)))%
Duncan Version
        Close_Session_Tij = Current_Tij;
        Trust_Vector = [Trust_Vector; Close_Session_Tij];
        Open_Session_Tij = Close_Session_Tij;
        CountDefect = CountDefect + 1;
        %%  Case D When Open_Session_Tij == 0 F1 = 0 F2 = 0
    elseif F1 == 0 && F2 == 0 && Open_Session_Tij == 0;
        D = 1; % InvalidUser & InvalidDevice
        %Con-Man Extension Updates to a for DEFECTION interaction
        Gamma_def_DISC = eC * abs(Open_Session_Tij);
        %             B = B - Gamma_def_DISC * (1 + B); %Duncan Ver
        B = (B - Gamma_def_DISC * (1 + B))*ForgiveFactor;% RFDNA Penalty(Ty)
        a = a * (1 - abs(B));
        Current_Tij = (Open_Session_Tij + B);
        Close_Session_Tij = Current_Tij;
        Trust_Vector = [Trust_Vector; Close_Session_Tij];
        Open_Session_Tij = Close_Session_Tij;
        CountDefect = CountDefect + 1;
    end
    time = time + 1;
    a_Vector = [a_Vector;a];
    B_Vector = [B_Vector;B];
    PairedF1_F2 = [PairedF1_F2; F1 F2];
End
References: [1] [2] [71] [72]
```

ANNEX S: Examples

- **S.1 Example: Receiver Perspective of Self-Evident Credential Classification.**

Assume $\boldsymbol{d}$ is capable of detecting an incoming waveform $\boldsymbol{w}$ from a set of authorized communication members of model $\boldsymbol{M}$. Let $\boldsymbol{d}$ receive some authorized instance $\boldsymbol{w_s}$ from $\boldsymbol{s}$ for bit-level augmentation concerning the contents of $\boldsymbol{m}$. The determination of the identity of $\boldsymbol{s}$ by $\boldsymbol{d}$ is *self-evident* if and only if $\boldsymbol{d}$ *owns* the physical layer evidence (i.e. RF-DNA credentials) which statistically describe the event stimulus of $\boldsymbol{s}$'s generated waveform state $\boldsymbol{w_s}$ prior to processing the logical contents of $\boldsymbol{m}$. In order for this claim to be true, all properties listed in Table 13 must hold. Recall, since $\boldsymbol{d}$ has previously received some incoming waveform emission $\boldsymbol{w}$ over link $\boldsymbol{l}$ we can assume that a standardized modulation scheme was detectable by the receiver that supports the P2P communications path. Link $\boldsymbol{l}$ has an existing policy $\boldsymbol{p}$ that exists between ($\boldsymbol{s} \rightarrow \boldsymbol{d}$).

Using the assumptions above, *Property-1* is satisfied since the waveform had to be detected if it was received. If we assert that $\boldsymbol{d}$ is only able to *listen* to incoming GFSK modulated messages on the 400-512 MHz frequency with a channel spacing of 25 kHz, then we can satisfy *Property-2* since transmitters or receivers of any waveform $\boldsymbol{w_i}$ using a standardized modulation scheme may physically carry the logically encoded contents of $\boldsymbol{m}$ [75] [77]. *Property-3* is satisfied by asserting that a particular device $\boldsymbol{s}$ is authorized to communicate with device $\boldsymbol{d}$ if a policy pairing $\boldsymbol{p}$ exists for such a specified path. As such, it is implied that $\boldsymbol{s}$ has some physically distinct markers which do not have to be explicitly revealed for authentication. That is to say that the distinguishing marker could have been predetermined or transmitted through some covert mechanism or channel (e.g. separate TDMA timeslot) or it can exist as a natural consequence of analog waveform generation using a standardized modulation scheme.

It is not yet obvious that the represented event of $\boldsymbol{w_s}$ was in fact distinctly generated by $\boldsymbol{s}$ without sampling an RF fingerprint using the $\boldsymbol{iMKr}$ to target an ROI and make a comparison to a known result that was distinctly produced by $\boldsymbol{s}$ during the development of $\boldsymbol{M}$. This enables $\boldsymbol{d}$ to *listen* and distinguish between *whom* (i.e. which $\boldsymbol{s}$ most likely generated the event) is talking instead of *what* (event interpretation of some response) is communicated by $\boldsymbol{s}$ in $\boldsymbol{m}$. When an extracted RF fingerprint sample, processed by $\boldsymbol{d}$ yields a statistically unique result of the event's measurable features (i.e. a match) then *Property-4* is satisfied. It was stated in the above claim that $\boldsymbol{d}$ has *self-evident* credentials to identify source $\boldsymbol{s}$.

Authenticator $\boldsymbol{d}$ can authenticate $\boldsymbol{s}$ using trusted preplaced RF credentials for comparison to incoming waveform RF fingerprint sample extractions. If upon comparison, a match exists, then those physically distinguishable waveform feature extractions made using ROI marker(s) of $\boldsymbol{w_i}$ are now assumed to be inherently generated by $\boldsymbol{s}$. This profound assumption is justified by the fact that the physical characteristics of the extracted fingerprints suggest a statistically significant result that cannot dismiss the uniqueness of the compared sample to a known physically-determined credential.

Since all properties of Table 13 have been satisfied and $\boldsymbol{d}$ possesses emplaced RF credential of $\boldsymbol{s}$, it can be concluded that the generated features of event $\boldsymbol{w_i}$ can be statistically attributed as originating from device* $\boldsymbol{s}$ as claimed and its origin integrity is therefore *self-evident* to *authenticator* $\boldsymbol{d}$, namely $\boldsymbol{w_s}$. ■

*Note, a validated *self-evident* credential does not imply that the logical contents of $\boldsymbol{m}$ are authorized. In this case, the waveform state, as received, is statistically significant for attribution to an authorized physical origin *device* (i.e. source $\boldsymbol{s}$). At the time of this writing, there is no known research on RF-DNA exchange mechanisms which attributes a *user* to a specified circuit or device.

- **S.2 Example2: Receiver-focused Self-Evident Classification.**

In a BiONet, each constituent ***d*** inherently understands the nature of its neighbor's physical waveform characteristics. That is, d has an internal sampling of authorized waveform states that contain the frequency, amplitude and phase statistics. We refer to quantifiable statistics of a waveform's characteristics as its *voice* (e.g. a child understand through learning, the voice of its mother in a noisy social gathering). As a natural consequence, each ***d*** can accurately distinguish the *voice* of foreign *or anonymous* device waveforms w_a from those spoken (generated) by trusted neighbor devices within acceptable levels of accuracy. In the inspirational case of a child that has learned their mother's voice, yet mistakes their aunt's voice as their own mother's until some other correlating cue emerges which disqualifies the aunt's voice as being the authentic voice of mom. Genetic inheritance influences the DNA structure of children, however factors such as social conditioning mechanisms and environmental factors are considered to formalize whom a child trusts.

Inspired by genetics and social conditioning concepts, this algorithm adapts these concepts to enable artificially inherited RF-DNA so that devices that share RF-DNA markers are more likely to trust the contents of their voices. A policy-based RF credential pairing allows devices to artificially inherit the RF-DNA of its specified neighbors for the purpose of *self-evident* identification. The term inherit refers to the physical emplacement of localized RF-DNA credentials into the memory of authenticating devices. Such *inheritance* is accomplished prior to deployment of an electronic communications network with the aim of supporting the policy's goals requirements and objectives. Such an expressive policy lends itself to support multi-organizational Cyberspace mission sharing collaboration in SATCOM ecosystems by bridging their trusted networks using RF-DNA *bridges* (RF-DNAB).

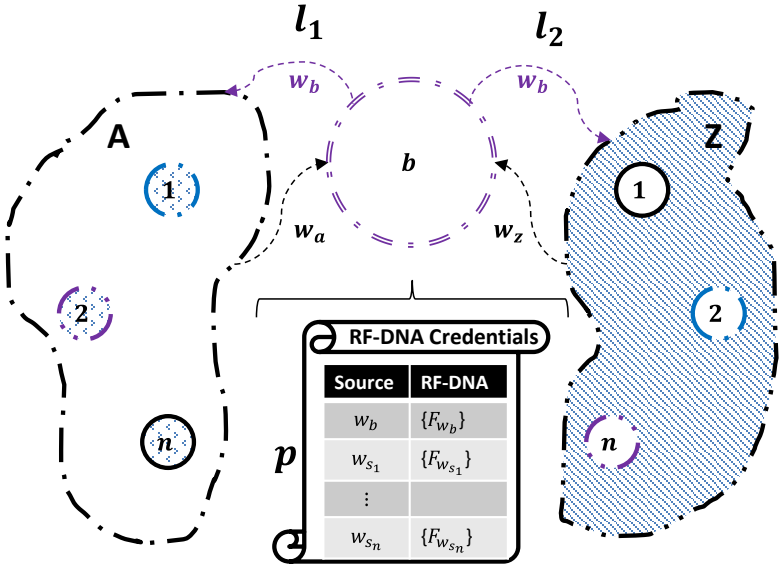


Figure 55. A Pathological Bridged Relay using an RF-DNA Chain-of-Trust

For example, the physical layer of network security boundaries can be augmented by bridging multiple instances of distinct BiONets to support scarce resource sharing. Distinct BiONets ***A*** and ***Z*** are connected through some shared infrastructure bridging device ***b*** depicted in Figure 55. This implies that both networks have authorized device ***b*** as a trusted source.

Since each BiONet has distinct network authentication boundaries defined by its collection of authorized links $\boldsymbol{l}$, there must be a policy for device $\boldsymbol{b}$ that shares the RF-DNA markers of a source device $\boldsymbol{A_s}$ and a source device $\boldsymbol{Z_s}$. Likewise, a subset of $\boldsymbol{b}$'s RF-DNA markers are shared with some *authenticator* in the respective BiONets indicated as $\boldsymbol{A_d}$ and $\boldsymbol{Z_d}$.

Given a set of devices for fingerprinting, let model $\boldsymbol{M}$ be the specified collection of all authorized satellite communication transceiver devices $\boldsymbol{d}$ such that each constituent $\boldsymbol{d}$ forms a network (e.g. CubeSat). The size of $\boldsymbol{M}$ shall be determined by the cardinality of $\boldsymbol{D}$ as modeled during the RF-DNA fingerprinting process and classified using MDA/ML where classification size is greater than two. We define the set of distinct constituent devices as $\boldsymbol{D} = \{1,2,3, \ldots \boldsymbol{n}\}$. Each $\boldsymbol{F_D}$ (the RF fingerprints of device $\boldsymbol{D}$) contains one or more RF-DNA fingerprint collections of $size \geq n$ for each constituent device. The letter $\boldsymbol{n}$ is the number of fingerprint credentials that have been emplaced into the memory of an *authenticator* according to the path specification of policy $\boldsymbol{p}$.

- **S.3 Example3: P2P Link Credential Extraction and Authentication.**

A P2P SATCOM network is depicted in Figure 56 where $\boldsymbol{p}$ exists for the ($\boldsymbol{s} \rightarrow \boldsymbol{d}$) path $\boldsymbol{l}$. Let $\boldsymbol{s} = \boldsymbol{R1}$ and $\boldsymbol{d} = \boldsymbol{S4}$. Upon receipt of an ROI marker $\boldsymbol{iMkr}$ (e.g. indexed value) by $\boldsymbol{d}$, the RF-DNA fingerprint is extracted from $\boldsymbol{w}$ and statistically compared to a known value (previously emplaced) which $\boldsymbol{S4}$ may inherently understand about $\boldsymbol{R1}$. That is, $\boldsymbol{S4}$ compares the claimed covertly carried fingerprint $\boldsymbol{R1}(\boldsymbol{f_n})$ received to $\boldsymbol{R1}(\boldsymbol{f_n})$ using $\boldsymbol{iMkr}^{\boldsymbol{f_n}}$ to extract a specified RF-DNA fingerprint sample from $\boldsymbol{w}$'s ROI. S4 compares the claimed identity to a known credential for a potential match upon receipt of the claimed credentials from R1.

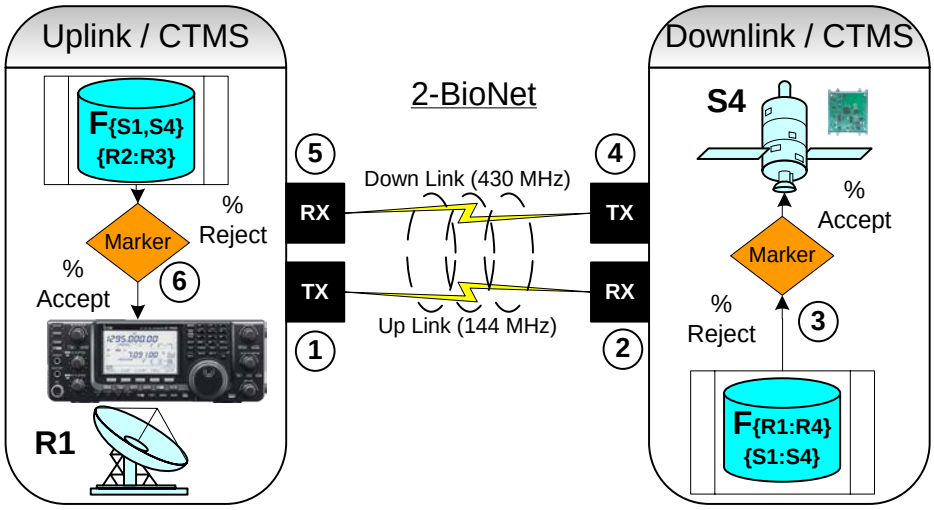


Figure 56. 2-Device Ground Station to CubeSat RF-DNA Exchange

For clarity, the local memory of each authenticator device $\boldsymbol{d_{auth}}$ contains all authorized $\boldsymbol{s}$ RF-DNA fingerprints in accordance with policy-based configurations. This is a necessary requirement for member authentication during communication exchanges. Following the approach described above, more expressive pairings of P2P links are achievable if we enforce three requirements.

First, $\boldsymbol{s}$ must be a member of $\boldsymbol{M}$. Secondly, $\boldsymbol{s}$'s RF-DNA markers must be emplaced by $\boldsymbol{d}$ as the credential authenticator. In other words, the policy must have previously specified that $\boldsymbol{d}$ could receive messages from $\boldsymbol{s}$. Thirdly, a receiver cannot authenticate anonymous sources. The last requirement can be met during processing where either a classification type is unknown and there is no binary ID field, or there is a known classification type and no data is present in the ID field.

- **S.4 Example4: Handling Anonymous Messages.**

Let it be the case that device $\boldsymbol{d}$ receives an incoming waveform $\boldsymbol{w}$ from some anonymous device $\boldsymbol{s_a}$ which contains a properly modulated message $\boldsymbol{m}$ using GMSK in a UHF SATCOM ecosystem. Under the conditions of the BiONet, $\boldsymbol{d}$ cannot authenticate the identity of $\boldsymbol{s}$ using RF-DNA fingerprinting. All of the desirable properties sufficiently exist in $\boldsymbol{w}$ however**;** $\boldsymbol{d}$ lacks the necessary inborn or preplaced memory credentials to make an authentication using RF-DNA fingerprints for $\boldsymbol{s_a}$. We could stop here, but a deeper discussion allows enhanced understanding as to why not.

Consider the pairing between $\boldsymbol{s_a \rightarrow d}$ as being distinct, then $\boldsymbol{s_a}$must be a member of the MDA/ML model $\boldsymbol{M}$ by earlier arguments. It is known that $\boldsymbol{d}$ is a member of $\boldsymbol{M}$, which implies $\boldsymbol{d}$ must possess RF-DNA credentials of at least one other member $\boldsymbol{s} \in \boldsymbol{M}$ because it has been designated as a receiving *authenticator* device. As a result, $\boldsymbol{d}$ inherited knowledge of *physically-determined* credentials of at least one source $\boldsymbol{s}$. However, since $\boldsymbol{d}$ is preconfigured with authorized credentials that are necessary and sufficient for self-evident authentication of specified states of $\boldsymbol{w}$ containing $\boldsymbol{m}$, the specified states of $\boldsymbol{w}$ must originate from distinct members of model $\boldsymbol{M}$. Since $\boldsymbol{s = s_a}$ then $\boldsymbol{s_a}$ must be a member of $\boldsymbol{M}$. Now, each constituent of $\boldsymbol{M}$ is distinct, and the statistical features of the characteristics computed for $\boldsymbol{s_a}$ do not statistically match an emplaced RF-DNA credential. Without consideration for a possible link pairing policy $\boldsymbol{p}$ to define a $\boldsymbol{s_a \rightarrow d}$ path, an authorized link $\boldsymbol{l}$ also does not exist. Any RF-DNA fingerprint extraction from $\boldsymbol{s_a}$ yields a statistically significant binary result; however the fingerprint is not repeatable from an authorized source, and therefore *Property-3* is not satisfied since there is no evidence that a trusted waveform $\boldsymbol{w_s}$ originated from $\boldsymbol{s_a}$. Finally, upon inspection of the full RF-DNA complement memory space of $\boldsymbol{d}$, if there is no evidence or discovery of emplaced RF-DNA credentials in the memory of $\boldsymbol{d}$, then the authenticator lacks any known RF-DNA credential of $\boldsymbol{s_a}$ nor any $\boldsymbol{iMkr}$ to authenticate the waveform origin integrity of source $\boldsymbol{s_a}$. ■

The following informal result emerges from the above argument. A controlled physical circuit which consistently generates repeatable distinct waveform states can be quantified as having statistically unique *self-evident* features. Such uniqueness derived from a physical occurrence, lends itself to expressive logical interpretations. When correlated with other environmental cues, logical interpretations based on physically-determined uniqueness may be useful in security augmentation ventures.

ANNEX T: FSK/FM Transmit Documentation and Guide

Research Lead: MAJ Tyrone Lewis
Intern/Research Assistant: Paul Dunaway
File Location (PC-4):
C:\Users\TLewis1\Desktop\Paul \FSK Tx – V9.5 - Pulse and Replay
C:\Users\TLewis1\Desktop\Paul\DEPENDENCIES\Extract Number of Pulses from Raw Data
C:\Users\TLewis1\Desktop\Paul\Inputs

How to Use

1) Open **FSK Tx – V9.5 – Pulse and Replay.vi** by double-clicking the **FSK Tx** desktop shortcut; this will open the Front Panel of the VI.
2) Under "*USRP Tx & Filter Settings*", ensure the following default values are correct:
   A. **Tx Device**: 192.168.10.2
   B. **Tx Antenna**: TX1 (if the antenna or wire is on TX1 of the USRP device)
   C. **Tx Filter**: None
   D. **Alpha**: 0.50
   E. **Filter Length**: 4
   F. **Symbol phase continuity**: continuous

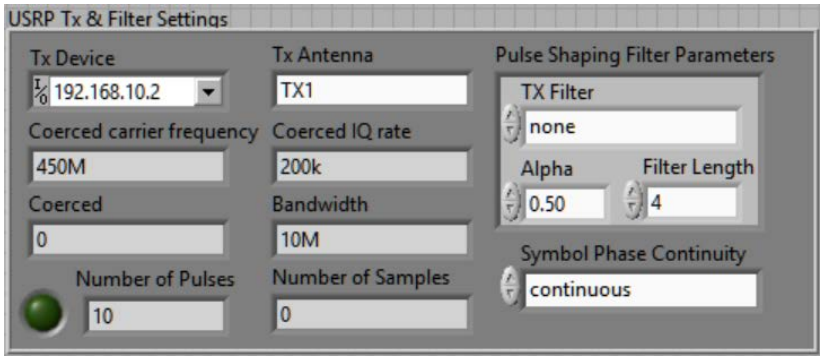


Figure 57. USRP Tx& Filter Settings

3) There are 2 main transmission options:
   A. OPTION 1 (Figure 2.a): Transmit a Message (M)
      i. Under "*Message (M) Settings*", select the desired method of creating message (m) from one of the following options in the radio button menu:
         1. **pRNG** – Randomly generated message
         2. **Manual Input** – Manually entered message
         3. **Input File** – Binary stream from file
            a. Select 3 binary text files (txt file containing only 1's and 0's):
               1) **Preamble** – a text file for the preamble of the message
               2) **Payload** – the actual binary message or command
               3) **Postamble** – a text file for the postamble of the message
      ii. NOTE: The Green LED's only verify which method was selected
   B. OPTION 2 (Figure 2.b): Transmit a previously recorded transmission

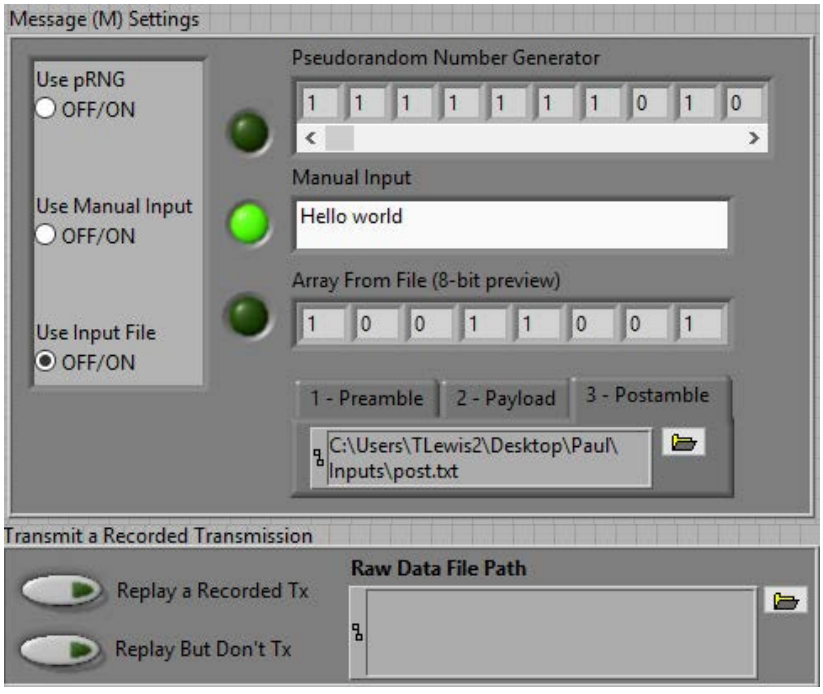
i. Under "*Transmit a Recorded Transmission*", click '**Replay a Recorded Transmission'**
ii. Enter the file path of the raw data file under **Raw Data File Path**

4) In the bottom row of the Dial Block (Figure 2.c):
   A. Set **FSK M-ary** to 2 (Default)
   B. Set **Samples/Symbol** to 16 (Default)
   C. Select a Time **Delay** (≥2s)
   D. Select the **Number of Pulses** to be transmitted (>0)
5) To run the VI: In the menu bar, select "**Operate -> Run**"
6) To cease transmitting and stop the VI: In the menu bar, select "**Operate -> Stop**"

NOTE: *All parameters are dynamic, meaning any parameter can be changed during transmission without needing to restart the program.*

A. In the upper left-hand corner of the front panel is the **USRP Tx & Filter Settings** group, containing:
   a. **Tx Device** (192.168.10.2) – This is the IP of the USRP transmitter
   b. **Tx Antenna** (TX1) – This is the antenna port being used
   c. **TX Filter** ("none") – This allows the operator to choose what transmission filter to use
   d. **Alpha** (0.50) – Used to compute the *calculate deviation*
   e. **Filter Length** (4) – This allows the operator to set the pulse-shaping filter's length, in symbols

   Symbol phase continuity ("continuous"**)** – This specifies the symbols' phase transitions as *continuous* or *discontinuous*



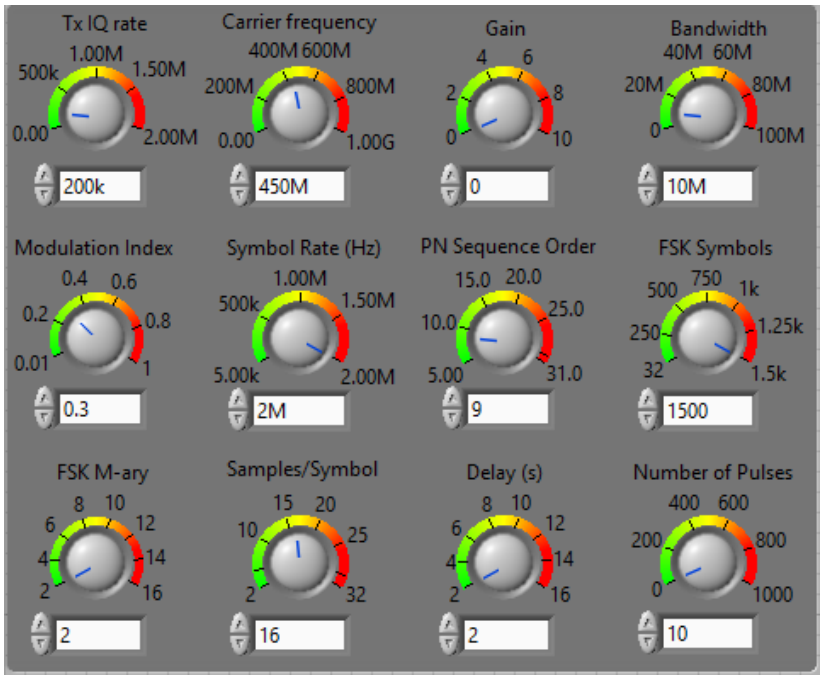


Figure 58a. (TOP): Message (M) Settings

Figure 58b. (MIDDLE): Transmit a Recorder Transmission

Figure 58c. (BOTTOM): Dial Block (default values displayed)

Parameter Defaults and Descriptions

B. To the right of the **USRP Tx & Filter Settings** widget is the **Message (M)** widget, containing:
   a. **A Radio-Button Menu** (*Use pRNG*) – This allows the operator to choose how the message (m) is created:
      - Use pRNG – This option will generate message (m) using a *Pseudorandom Number Generator*
      - Use Input Bitstream – This option will use the 8-bit manual input, *Manual Input*
      - Use Input File – This option will concatenate the bits in 3 binary text files (the preamble, payload, and postamble) to construct message (m)
   b. **Manual Input** – This allows the operator to manually input text (alphanumeric); converts from ASCII to Binary
   c. **File Path** – The operator must select a file

C. Below the **USRP Tx & Filter Settings** widget is the **Transmit a Recorded Transmission** widget, containing:
   a. **Replay a Recorded Transmission** (Off) – Allows the operator to transmit a raw data file
   b. **Replay But Don't Tx** (Off) – Allows the operator to visualize a transmission without actually transmitting anything
   c. **Raw Data File Path –** The file path to the raw data file

D. Dial Block:

a. **Tx IQ Rate** (200k) – Allows the operator to change the IQ rate (samples per second)
b. **Carrier Frequency** (450M) – Specifies the frequency of the transmission
c. **Gain** (0) – Specifies the aggregated gain in dB
d. **Bandwidth** (10M) – Specifies the bandwidth of the transmission
e. **Modulation Index** (0.3) – Utilized to compute the *calculated deviation*
f. **Symbol Rate** (2M) – Utilized to compute the *calculated deviation*
g. **PN Sequence Order** (9) – Utilized to compute the pseudorandom number generated message (m)
h. **FSK Symbols** (1500) – Utilized to compute the pseudorandom number generated message (m)
i. **FSK M-ary** (2) – Specifies the number of frequency deviations
j. **Samples/Symbol** (16) – Specifies the number of samples per symbol
k. **Delay** (2) – Allows the operator to specify a time delay between pulses (>2 sec)
l. **Number of Pulses** (10) – Allows the operator to specify the number of pulses to be transmitted
    - NOTE: a pulse is a single transmission of message (m), from beginning to end, without repeating or adding filler bits to meet a bit-length requirement

E. Deviation Panel:
    a. **FSK Deviation (Hz)** (100) – Specifies the FSK frequency deviation
    b. **Use Calculated Deviation** (Off) – this toggle button allows the operator to choose whether to utilize the *calculated deviation* or to utilize the *FSK deviation (Hz)* input
F. FM Panel:
    a. **FM Deviation** (450) – Specifies the FM frequency deviation
    b. **FM** (Off)- this toggle button allows the operator to choose whether to transmit only FSK (off) or FSK on FM (on)

Visual Aid Descriptions

A. Graphs:
    a. **I/Q Graph** – Portrays the FSK constellation
    b. **Tx Signal** – Depicts the waveform power spectrum
    c. **Tx Pulse** – Depicts the pulse being transmitted
B. Indicators:
    a. **Number of Pulses** (*USRP Tx Filter Settings*) – Indicates the number of pulses already transmitted
    b. **Number of Samples** (*Transmit a Recorded Transmission*) – Indicates how many samples are being transmitted (based on the rows of data in the Raw Data file)
C. Common Errors:
    a. **File I/O**: File Not Found – Check if all File Path Entry boxes have valid file paths
    b. **File Type**:
        i. **Raw Data File Path** must be a tdms file

- i.e.: “C:\Users\TLewis2\Desktop\Evan\Databases\D0\NewRawData.tdms”

ii. **File Path** (under **Message (M) Settings**) must be a text document containing only 1’s and 0’s
- i.e.: “C:\Users\TLewis2\Desktop\Paul\Inputs\m_01.txt”

c. **No Devices Found:** Check USRP-2922 unit is powered on and connected to the PC via an Ethernet cable

D. Bit Streams:
a. **Tx’d bit-stream**: the bit stream being transmitted
b. **Rx’d bit-stream**: what the receiver should/will receive

ANNEX U: FSK/FM Receiver Documentation and Guide

Research Lead: MAJ Tyrone Lewis
Intern/Research Assistant: Evan Kain
Description:

In order to properly use this vi, the following guide is provided to give a high level overview of each section on the front panel. This guide assumes you have had some experience with NI LabVIEW and that you understand the basic principles of signal processing. It will walk through each tab of the vi's front panel and describe the layout as well as the default values and functionality of each control and indicator.

Front Panel Description and Pictures: The front panel consists of four tabs 0 - Setup, 1 – Main, 2 – Stats, and 3 – File Paths. The 0 - Setup tab shown below contains the setup information for different devices and operation mode controls. It is used to determine the high level function of the vi. It is intended to give the user more control over the function of the vi. Use this tab when changing the high level function of the vi such as continuous collection, comparison, stats generation, etc. Pay close attention to which features are enabled as these will drastically change what the program does.

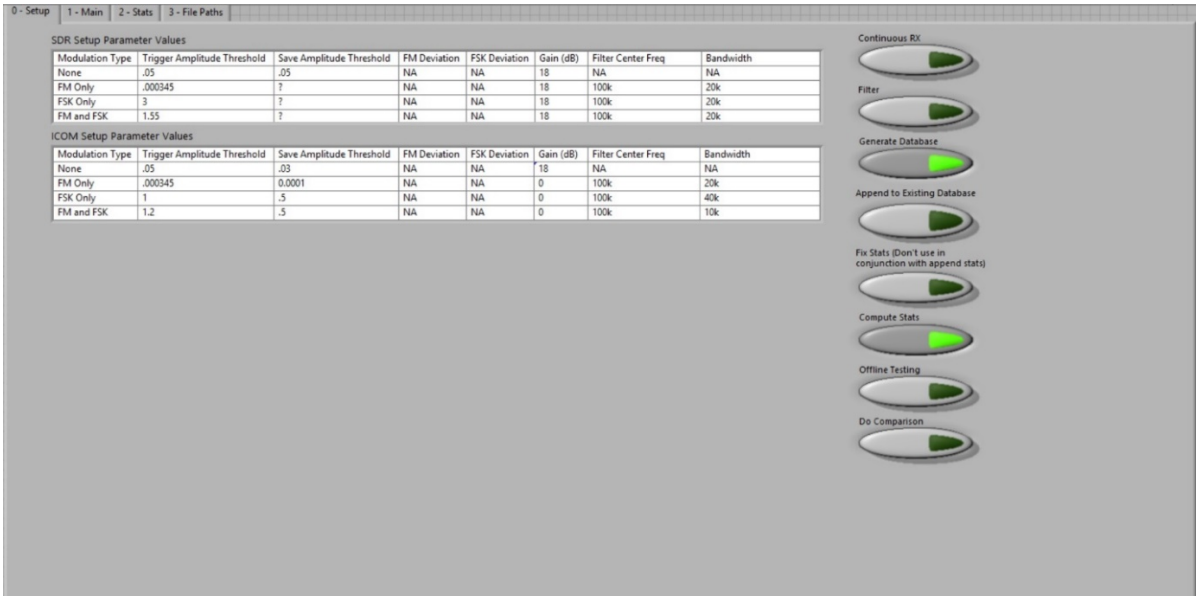


Figure 59. 0 - Setup Tab

The 1 - Main tab shown on the following page contains the controls and indicators for the receiving feature of the VI. The purpose of this tab is to set the receiver parameters. It will also provide indications of the real values of these parameters as well as the data output from the receiver. This tab is intended to provide the user more control of the receiver as well as give a thorough indication of how the receiver is actually functioning. This tab should be used when changing the receiver settings and during an active collection. Please use this to verify that the receiver settings are correct with the graphs on the right side of the panel.

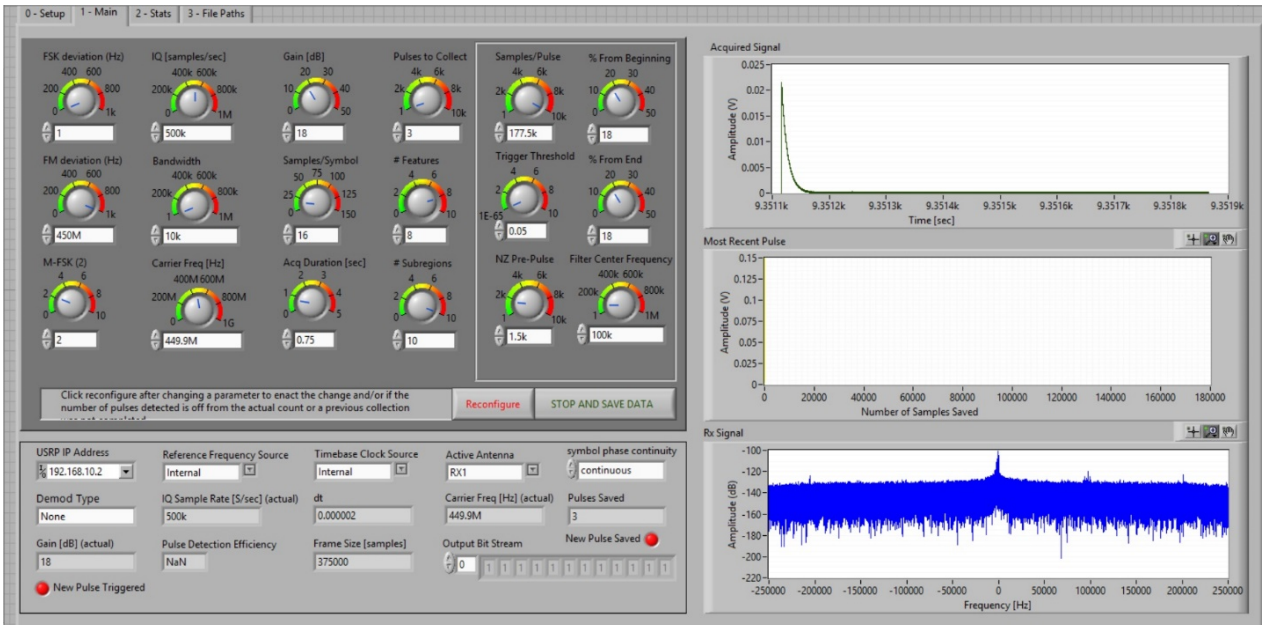


Figure 60. 1 - Main Tab

The Stats Tab shown below contains the controls and indicators for statistical comparisons as well as information for stats generation and database generation. It provides several options for various comparisons and recommendations and is intended to give the operator a thorough examination of whether an incoming pulse set adequately compares to a known set of pulses. Use this tab after a collection is done and you plan on comparing two or more different sets of pulses. Also use this tab at the start of a new collection to verify that the correct database information is entered.

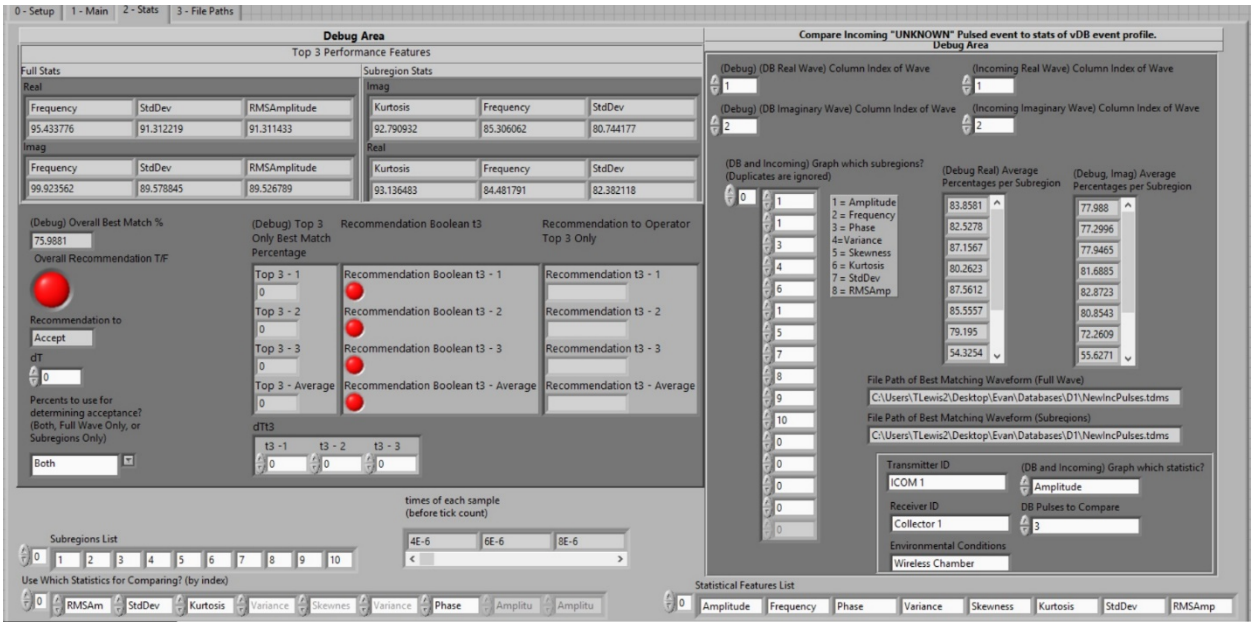


Figure 61. 2-Stats Tab

The 3 - File Paths tab shown below contains the file path inputs for the databases for comparison or generation as well as the file paths to which output data will be immediately saved. This vi provides the ability to direct almost every file generated to a specific path. This functionality is intended to provide more flexibility to the operator and help organize the saved data. Use this tab at the beginning of each collection to set the file paths you would like to change.

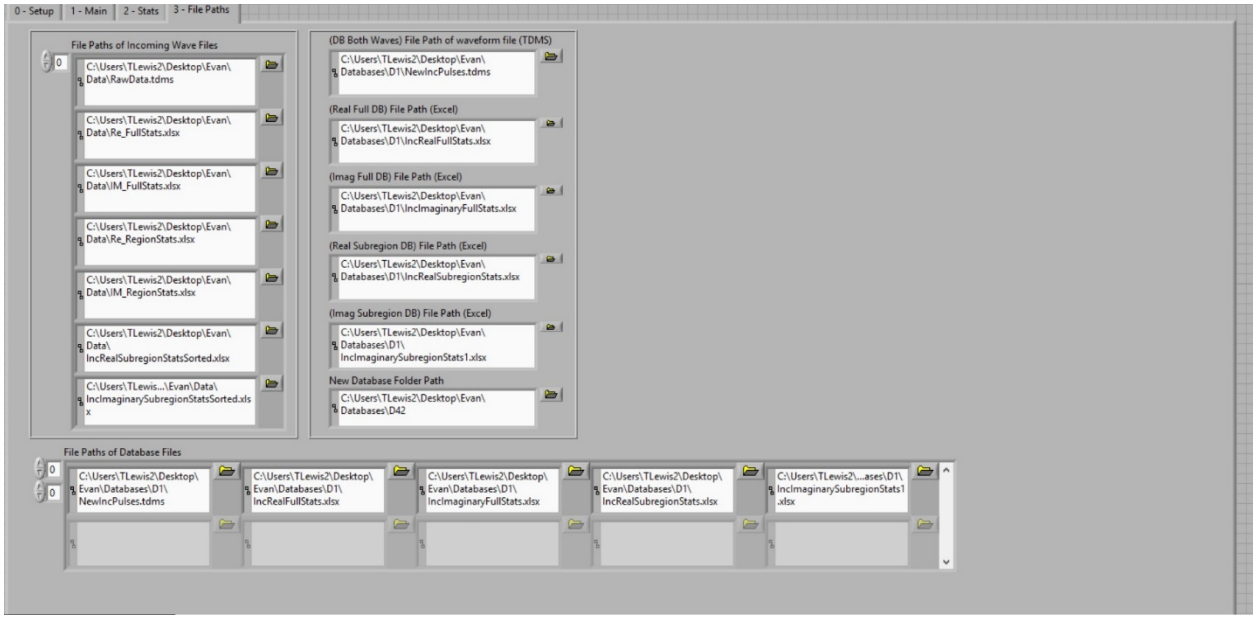


Figure 62. 3 - File Paths Tab

Setup Controls and Parameter Defaults:

The following section reviews the parameter default values and controls. Setup Parameter Value Tables: The setup parameter value tables shown below, offer default settings for the proper triggering and capture of pulses for a given transmission device and demodulation type.

SDR Setup Parameter Values

Modulation Type	Trigger Amplitude Threshold	Save Amplitude Threshold	FM Deviation	FSK Deviation	Gain (dB)	Filter Center Freq	Bandwidth
None	.05	.05	NA	NA	18	NA	NA
FM Only	.000345	?	NA	NA	18	100k	20k
FSK Only	3	?	NA	NA	18	100k	20k
FM and FSK	1.55	?	NA	NA	18	100k	20k

ICOM Setup Parameter Values

Modulation Type	Trigger Amplitude Threshold	Save Amplitude Threshold	FM Deviation	FSK Deviation	Gain (dB)	Filter Center Freq	Bandwidth
None	.05	.03	NA	NA	18	NA	NA
FM Only	.000345	0.0001	NA	NA	0	100k	20k
FSK Only	1	.5	NA	NA	0	100k	40k
FM and FSK	1.2	.5	NA	NA	0	100k	10k

Figure 63. Setup Parameter Value Tables

a. The tables should be filled with “NA” if the parameter does not apply to the particular demodulation type and a question mark if unknown.
b. The values can be changed by hand, and they should be used to modify settings on the 1 - Main tab.

2. Operation Control Buttons: Light green when pressed (i.e. logical high), dark green when not pressed.

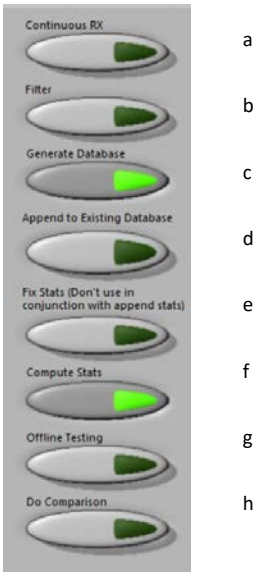


Figure 64. Transceiver's operational control buttons

Settings shown are for a collection that generates a database and computes stats without doing anything else.

a. Continuous RX: When pressed, the continuous RX button allows for the program to receive pulses indefinitely.
b. Filter: When pressed, applies a fourth order band pass, Butterworth filter to the waveform before triggering.
c. Generate Database: When pressed, generates a database folder at the defined folder path which contains a profile description, the raw data files, and the statistics files for a given collection.
d. Append to Existing Database: When pressed, appends any newly collected pulses to the database at the defined folder path.

    i. WARNING: Do not use in conjunction with fix stats as this causes a multitude of errors and could delete data from the existing database.

e. Fix Stats: When pressed, bypasses the receiver and regenerates statistics and database files.
    i. Note: This feature requires an unorganized raw data file to be saved in an existing database folder.
        1. This unorganized raw data format will be defined later in this file and was defined in the project overview documentation.

    ii. WARNING: Do not use in conjunction with append to existing database as this causes a multitude of errors and could delete data from the existing database

f. Compute Stats: When pressed, computes statistics for all captured pulses.
    i. Note: Must be pressed when doing a statistical comparison or generating a database.
g. Offline Testing: When pressed, bypasses all receiving, statistical generation, and database generation functions. Executes a gold standard diagnostic test and gold standard generation.

i. Non-functional as of version 2.7.
ii. The gold standard is discussed in the project overview documentation.

h. Do Comparison: Compares incoming pulses against a set of files from an existing database.
i. Note: The database files are chosen on the 3 - File Paths tab.

i. Note: All buttons on this tab switch when pressed.

3. Default settings for the parameter value tables can be used for collection settings.
4. The default parameters for the setup controls are for a collection in which new data is collected and a new database is generated with statistics. No other features are enabled by default.

Setup Controls and Parameter How To: This section details the controls of tab 1 – Main Tab.

1. Enable desired features.
   a. Click on the operation control buttons to enable or disable them as necessary.
   b. Each collection will have different features enabled depending on what features are desired. See the setup controls and parameter defaults for descriptions.
2. After collecting on an undocumented device type, create a new parameter value table.
3. After collecting with an undocumented demodulation type, put new values in the parameter value table.

RX Controls and Default Values:

The following section reviews the RX controls and their default values. The top label indicates functions, the knob provides dynamic control tuning, and boxes group similar controls.

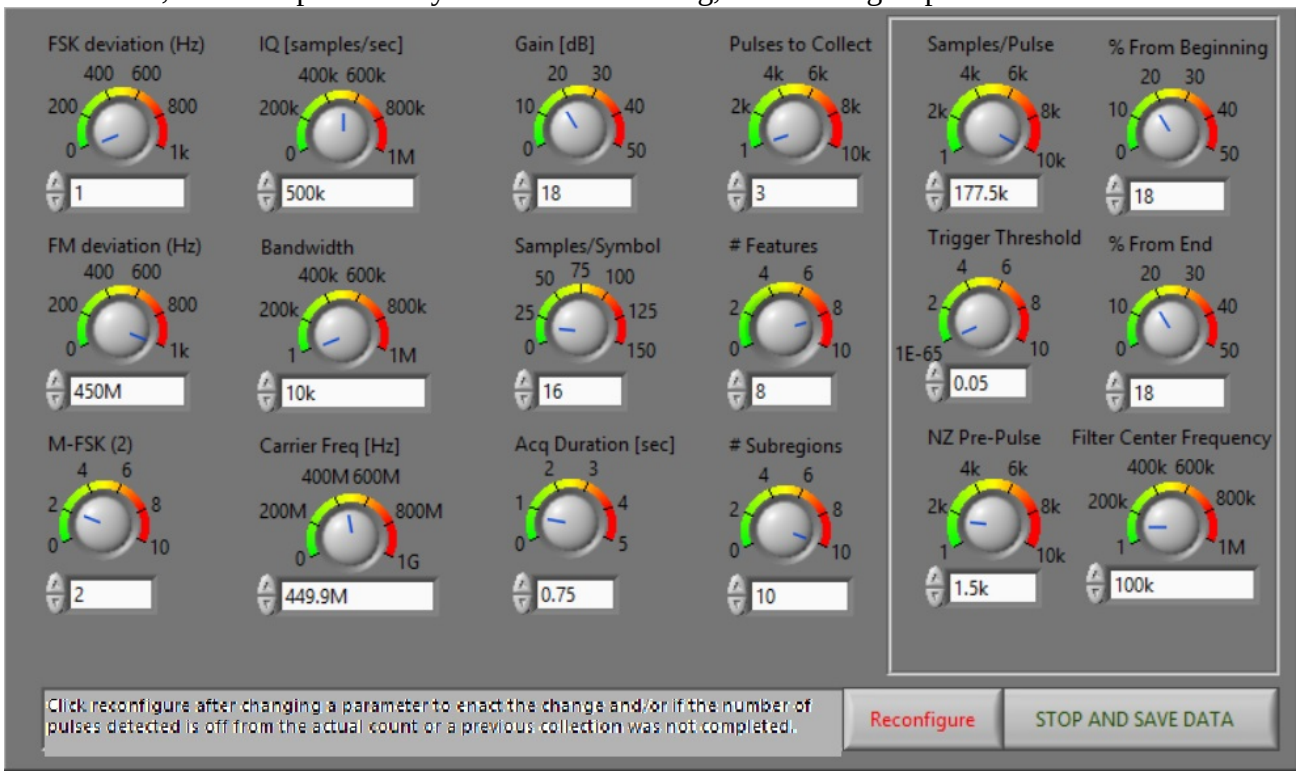


Figure 65. RX Controls

1. FSK Deviation [Hz]: Sets the FSK deviation in Hz.
   a. For use with FSK demodulation.
   b. The default value is 1 for development.

2. FM Deviation [Hz]: Sets the FM deviation in Hz.
    a. For use with FM demodulation.
    b. The default value is 450M for development.
3. M-FSK: Sets the M value for M-ary FSK modulation.
    a. For use with FSK demodulation.
    b. The default value is 2 as this is the default transmission M-ary FSK.
4. IQ [Samples/sec]: Sets the IQ sampling rate in samples per second.
    a. The default value is500kM for development.
5. Bandwidth: Sets the frequency bandwidth for the collection.
    a. The default value is 10k for development.
    b. Note: Also sets the frequency bandwidth for the external filter when applied.
6. Carrier Freq [Hz]: Sets the frequency of the collecting SDR in Hz.
    a. The default value is 449.9M since the default transmission frequency is 450M.
    b. Note: This value is set to the transmission center frequency with a slight offset for better collections.
7. Gain [dB]: Sets the receiver gain in decibels.
    a. The default value is 18 for development.
8. Samples/Symbol: Sets the number of received samples per expected symbol.
    a. The default value is 16 for development.
    b. Note: Used for FSK demodulation.
9. Acq Duration [sec]: Sets the acquire window size.
    a. The default value is 750ms because the longest pulse we have received up to this point is less than 400ms which falls easily in this acquire window.
    b. Note: A longer acquire duration will capture more data per acquire window and help catch a full pulse. However, a longer acquire duration will use more memory and may cause the program to crash at high IQ rates.
    c. Note: A shorter acquire duration will update faster and may alleviate memory issues. However, the shorter duration may not capture a full pulse.
10. Pulses to Collect: Sets the maximum number of pulses the receiver collects before it stops collecting.
    a. The default value is 3 for development.
    b. Note: This parameter is ignored when continuous RX is enabled on the 0 - Setup tab.
11. # Features: Sets the number of features for which statistics are generated.
    a. The default value is 8 since this is the original number of features calculated.
    b. Note: Ignored when generate stats, do comparison, and generate database are all disabled on the 0 - Setup tab.
12. # Sub-regions: Sets the number of sub-regions for which statistics are generated.
    a. The default value is 10 for development.
    b. Note: Ignored when generate stats, do comparison, and generate database are all disabled on the 0 - Setup tab.
13. Samples/Pulse: Sets the number of samples captured in each pulse.
    a. The default value is 177.5k for development.
    b. Note: This conditions the maximum length of the triggered pulse. All samples after this value will be ignored until the next acquire window is processed.
14. Trigger Threshold: Sets the signal magnitude trigger threshold.
    a. The default value is .05 for development.

b. Note: When a signal magnitude's response is detected within the acquire window's threshold, a pulse of length X samples is measured using the pre-specified RF-Measurement(s) for a given ROI.

c. WARNING: If the signal to noise ratio is low, this value may need to be set very carefully to avoid improper triggering.

15. NZ Pre-Pulse: Sets the number of samples before a triggered pulse that will be captured.
    a. The default value is 1.5k for development.

    b. WARNING: A higher number for NZ Pre-Pulse will store more samples in a buffer and could cause crashes at high IQ rates due to memory issues.

16. % From Beginning: Used to condition the pulse save length.
    a. The triggered pulse does not save if it falls below the save threshold within $\frac{100+(\%\ From\ Beginning)}{100} \times (NZ\ Pre\ Pulse)$ samples of the triggered pulse.
    b. The default value is 18 for development.
    c. WARNING: Setting this value too empirically low will allow pulses of insufficient length to be saved.
    d. WARNING: Setting this value too empirically high will cause pulses of sufficient length to be thrown away.
    e. WARNING: If $\%\ From\ Beginning\ +\ \%\ From\ Beginning \geq 100$, no triggered pulses will be saved.
    f. WARNING: If $\%\ From\ Beginning\ +\ \%\ From\ Beginning \geq 100$, all triggered pulses will be saved.

17. % From End: Used to condition the pulse save length.
    a. The triggered pulse does not save if it falls below the save threshold within $\frac{100-(\%\ From\ End)}{100} \times (Samples/Pulse)$ samples of the end of the pulse.
    b. The default value is 18 for development.
    c. WARNING: Setting this value too empirically high will allow pulses of insufficient length to be saved.
    d. WARNING: Setting this value too empirically low will cause pulses of sufficient length to be thrown away.
    e. WARNING: If $\%\ From\ Beginning\ +\ \%\ From\ Beginning \geq 100$, no triggered pulses will be saved.
    f. WARNING: If $\%\ From\ Beginning\ +\ \%\ From\ Beginning \geq 100$, all triggered pulses will be saved.

18. Filter Center Frequency: Sets the center frequency of the external, bandpass, fourth order, Butterworth filter.
    a. The default value is 100k for development.

b. Note: The pass band of the Butterworth filter is from $\frac{Filter\ Center\ Frequency - Bandwidth}{2}$ to $\frac{Filter\ Center\ Frequency + Bandwidth}{2}$ Hz.

19. The "Reconfigure" and "STOP AND SAVE DATA" buttons shown on the right of figure 7 are also very important to correct operation.
    a. The Reconfigure button should be pressed any time a change is made to the controls during an active receiving session. The changes will not take effect until Reconfigure is pressed. In addition, if the number of pulse that are expected to be received is lower than the total number of pulses that were received during the last collection, reconfigure must be pressed to reset the pulse count ceiling. If reconfigure is not pressed in this scenario, the program will not save any data.
20. The stop and save data button resets the pulse count, stops the receive session, and saves the raw data for further collection.

RX Controls How To:

1. FSK Deviation [Hz]: Set the desired FSK deviation in Hz.
    a. Attempt to match this to the transmitter settings.
2. FM Deviation [Hz]: Set the desired FM deviation in Hz.
    a. Attempt to match this to the transmitter settings.
3. M-FSK: Set the desired M to match the transmitter.
4. IQ [Samples/sec]: Sets the IQ sampling rate in samples per second.
    a. Note: Oversample as much as possible as your signal can always be resampled at a lower rate.
5. Bandwidth: Set the frequency bandwidth for the collection in Hz.
6. Carrier Freq [Hz]: Sets the frequency of the collecting SDR in Hz.
    a. Set slightly lower than the transmitted center frequency in order to collect the clearest signal.
7. Gain [dB]: Set the receiver gain in decibels.
    a. Note: Amplifies noise as well as the received signal.
        i. Turn gain up on the transmitter end if the SNR is a problem.
8. Samples/Symbol: Set the number of received samples per expected symbol.
    a. Attempt to match this to the transmitter settings.
9. Acq Duration [sec]: Set this to be at least twice as long as the expected pulse length in seconds.
10. Pulses to Collect: Set to the number of pulses you want to save.
11. # Features: Sets to the number of features you want to generate statistics for.
    a. Note: The calculated features are in a set order and it is currently impossible to generate them out of order.
        i. i.e. You can't generate some higher numbered features without generating the lower numbered ones.
12. # Sub-regions: Set the number of sub-regions for which statistics are generated.
    a. Empirically determined for best results.
13. Go to the 0 - Setup tab and turn on continuous RX.
14. If the number of pulses saved is incorrect, or if the present value of pulses to collect is less than the value of pulses to collect from the previous collection, click the reconfigure button.
15. Press **Run** on the VI.
16. Trigger Threshold: Set the signal magnitude trigger threshold
    a. Set as low as possible without triggering a pulse off of noise.

17. Begin transmitting pulses with the transmitter.
18. Raise the trigger threshold if the receiver is triggering but is capturing data that does not belong to your transmission.
19. If the receiver does not trigger on any pulses, consider turning the gain up on the transmitter.
20. NZ Pre-Pulse: Set to a high number so that you capture the entire front end of the pulse.
    a. Reduce until you capture as few noise samples as possible while still capturing the full front end of the pulse.
21. Samples/Pulse: Set to a high number so that you capture the entire back end of the pulse.
    a. Reduce until you capture as few noise samples as possible while still capturing the full front end of the pulse.
22. % From Beginning: Set to 0 and observe if the pulse saved LED lights up.
    a. Gradually increase until the pulse saved LED no longer lights up for pulses with insufficient front end characteristics.
        i. i.e. If the pulse is too short or has strange downward spikes, increase this value until similar pulses no longer save.
23. % From End: Set to 0 and observe if the pulse saved LED lights up.
    a. Gradually increase until the pulse saved LED no longer lights up for pulses with insufficient front end characteristics but does light up for pulses with desirable characteristics.
        i. i.e. If the pulse is too short or has strange downward spikes, increase this value until similar pulses no longer save.
24. Make sure that the filter button is turned off on the 0 - Setup tab.
25. Filter Center Frequency: Set this to the frequency of the highest spike on the PSD.
26. Turn the filter button on if demodulating or operating in a noisy environment.

Hardware and Processing Controls Description and Defaults: This section will review the physical and processing controls.

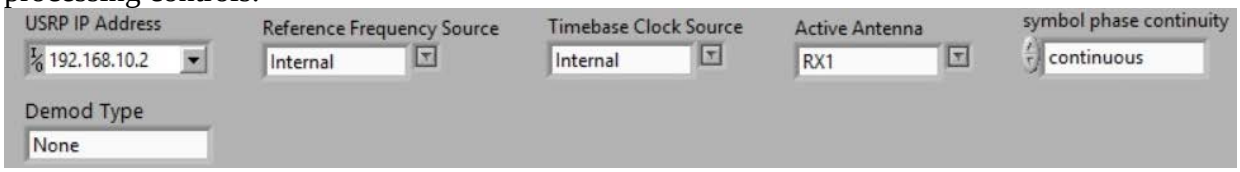


Figure 66. Physical and Processing Controls

1. USRP IP Address: Set to the IP address of the USRP 2922 used for recording.
    a. The default is 192.168.10.2 for each USRP 2922.
2. Reference Frequency Source: Set to the desired frequency reference source.
    a. The default is internal.
3. Timebase Clock Source: Set to the desired clock source.
    a. The default is internal.
4. Active Antenna: Set to the desired antenna for receiving.
    a. The default is RX1.
5. Symbol Phase Continuity: Set to the expected symbol phase continuity.
    a. The default is continuous.
6. Demod Type: Set to the desired demodulation type.
    a. The default is none.

Hardware and Processing Controls How To:

1. Verify that the USRP IP Address is at the default value of 192.168.10.2.

    a. If the default value is unavailable, click refresh from the drop down menu and select the default value.
        i. Alternatively, go to the USRP-utils program found at C:\Program Files (x86)\National Instruments\NI-USRP\utilities
    b. If the default value does not work, you most likely have a connection issue.
        i. Please contact National Instruments if this problem arises.
2. Set the reference frequency source to internal unless you have connected the SDR to an external frequency source in which case you should select the appropriate external connection.
3. Set the reference timebase source to internal unless you have connected the SDR to an external timing source in which case you should select the appropriate external connection.
4. Set the active antenna to the antenna you intend to receive from.

WARNING: Choosing the wrong antenna may still allow you to collect data, but the data will be inconsistent with other collections and will not be usable for comparisons.

5. Symbol Phase Continuity: Match this parameter to that of the transmitter.
6. Demod Type: Set this to the desired demodulation type in order to retrieve the logical bits transmitted.
    a. Note: Does not return correct bit stream as of version 2.7.

RX Indicators and Graphs Descriptions:

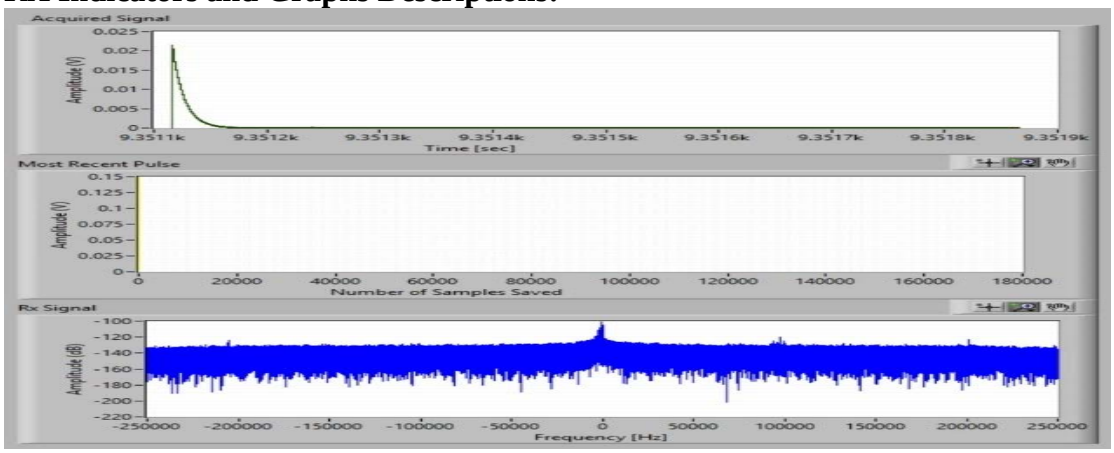


Figure 67. RX Graphs

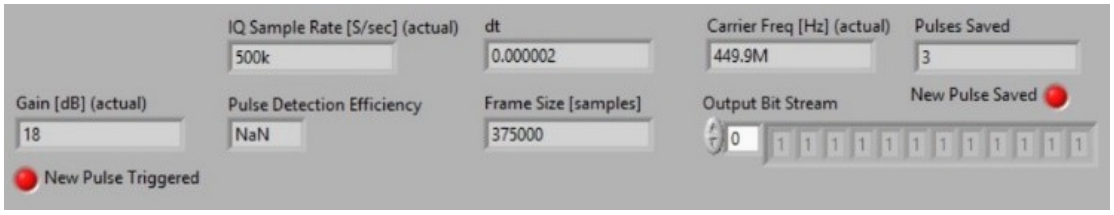


Figure 68. RX Indicators

1. Acquired Signal: Plots the data captured during the acquire window set by the acq duration control.
    a. Displays the magnitude of the data by default.
    b. Can be modified to display just I data or Q data.
        i. To enable other data displays, right click on the acquired signal graph, and select visible items.
            1. Check the plot legend box.
                a. Enable desired displays using this box.
                b. If the box does not display checkboxes next to each plot option, right click the box and go to visible items and enable plot legend checkbox.
2. Most Recent Pulse: Plots the most recently triggered pulse.
    a. Displays the pulse magnitude by default.
        i. To enable other data displays, right click on the most recent pulse graph, and select visible items.
            1. Check the plot legend box.
                a. Enable desired displays using this box.
                b. If the box does not display checkboxes next to each plot option, right click the box and go to visible items and enable plot legend checkbox.
3. RX Signal: Plots the power spectral density of the acquired signal.
    a. Use this graph to verify that the received signal is similar to the transmitted one and that you are not receiving any unauthorized transmissions.
4. IQ Sample Rate [S/sec] (actual): Displays the coerced IQ rate.
    a. Use this indicator to verify that the expected IQ rate does not violate the physical limitations of the recording device.
5. dt: Displays the coerced dt.

    a. Use this indicator to verify that the expected dt does not violate the physical limitations of the recording device.
6. Carrier Frequency [Hz] (actual): Displays the coerced carrier frequency.
    a. Use this indicator to verify that the expected carrier frequency does not violate the physical limitations of the recording device.
7. Pulses Saved: Indicates the number of pulses saved during the collection.
    a. Use this to verify that the expected number of pulses saved is equal to the actual number of pulses saved.
8. Gain [dB] (actual): Displays the coerced gain.
    a. Use this indicator to verify that the expected gain does not violate the physical limitations of the recording device.
9. Pulse Detection Efficiency: Displays the decimal ratio of pulses saved to pulses triggered.
    a. Use this to estimate how long a collection will take or whether or not you should change the constraints on the saved pulse size.
10. Frame Size [samples]: Displays the size of the acquire window in samples.
    a. Use this to verify the total acquire window size in samples and set your pulse length accordingly.
11. Output Bit Stream: Displays the demodulated bit stream from the received signal.
    a. Note: Disabled when demodulation type is set to “None.”
    b. Note: Does not return the correct bit stream as of version 2.7.
12. New Pulse Saved: Boolean indicator that flashes green when a pulse is saved.
    a. Use to verify that pulses are saved properly.
13. New Pulse Triggered: Boolean indicator that flashes green when a pulse is triggered.
    a. Use to verify that pulses are triggered properly.

Stats and Comparison: The following steps will guide you through the 2 - Stats tab of the front panel.

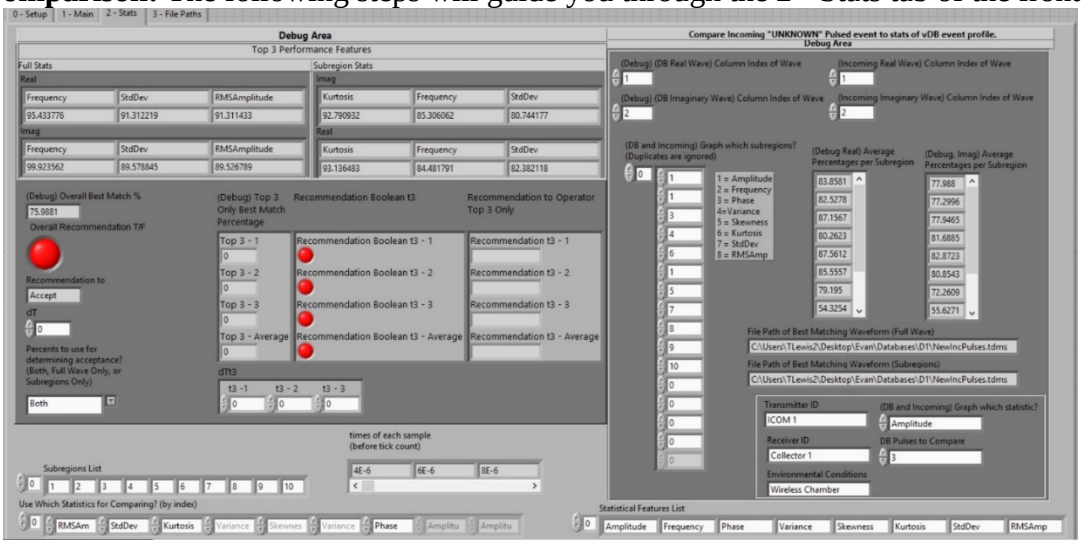


Figure 69. 2 - Stats Tab

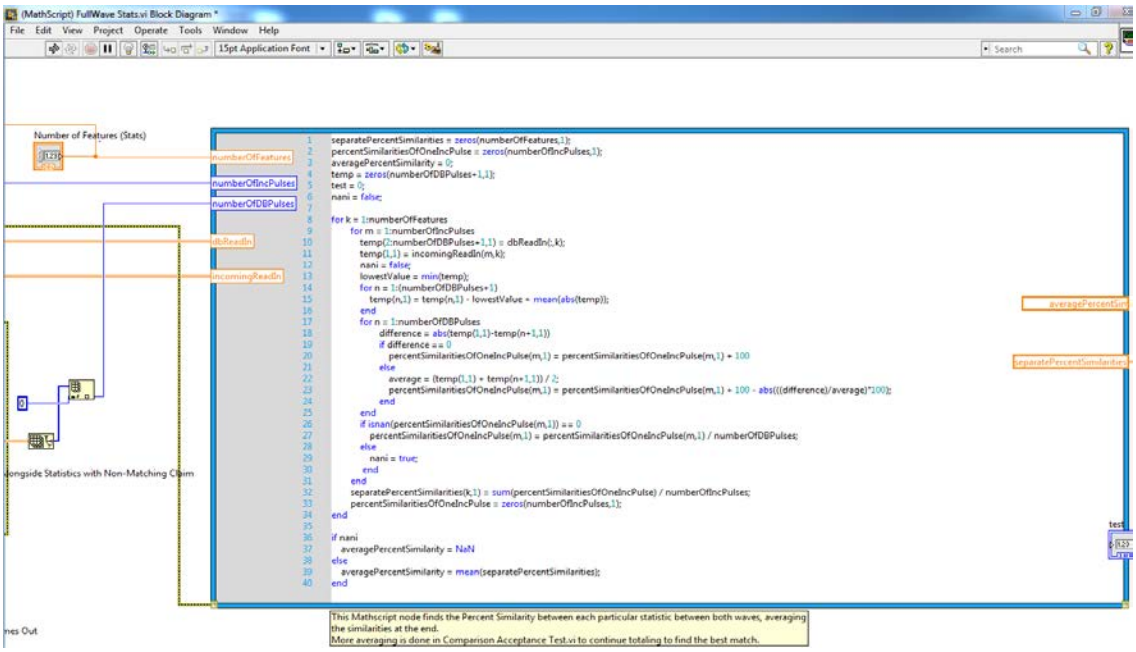


Figure 70. RF-Measurement comparisons using LabVIEW's Math Script

1. Top 3 Performance Features: Display the names and values of the top three performing features for the real and imaginary data for the full wave and across all the sub-regions.
    a. Use to determine which features perform the best classifications.
2. (Debug) Overall Best Match %: Shows the best overall match percentage for a given comparison.
    a. Use this to determine the acceptance threshold for the recommendation to the operator.
3. Overall Recommendation TF: Boolean indicator that displays whether a given pulse meets the acceptance threshold standards for a given comparison.
    a. Use to determine whether a given pulse should be accepted as a valid command.
4. dT: Sets the acceptance threshold for the operator recommendation.
    a. Use to determine the rigor of the comparisons.
5. Percents to use for determining acceptance? (Both, Full Wave Only, or Subregion Only): Use to control which statistics will be used to determine whether a pulse is deemed similar enough during comparison.
    a. Options allow for the use of only full wave statistics, only subregion statistics, or the arithmetic mean of both.
6. (Debug) Top 3 Only Best Match Percentage: Shows the best overall match percentage for each of the top three compared statistics as well as the arithmetic mean of their best match percentages.
    a. Use this to determine the effectiveness of each of the top 3 statistics individually.
7. Recommendation Boolean t3: Displays whether a pulse would be recommended as similar for each of the top 3 statistics as well as for their arithmetic mean.
    a. Use this to determine the effectiveness of each of the top 3 statistics.
8. Recommendation to Operator Top 3 Only: Displays whether a pulse would be recommended as similar for each of the top 3 statistics as well as for their arithmetic mean.
    a. Use this to determine the effectiveness of each of the top 3 statistics.
9. dTt3: Sets an acceptance threshold for each of the top three statistics for comparison.

    a. Use this to determine how a network would accept or reject a pulse as similar based off of each of the top three statistics.
10. Sub-regions List: List of the numerical sub-regions for which statistics are computed.
    a. Note: Saved in the database profile description.
11. Times of Each Sample (before tick count): Displays the times at the start of each subregion for which statistics are calculated.
12. Use which Statistics for Comparing? (by index): Used to select which statistics will be used for comparison by name.
    a. Select which statistics to use by cycling through the options.
13. (Debug) (DB Real Wave) Column Index of Wave: Determines which wave dataset will be plotted in the Read and Graph Waveform Values against Subregion Statistics vi.
    a. The options are the following:
        i. 0=Time
        ii. 1=Real
        iii. 2=Imaginary
14. (Debug) (DB Imaginary Wave) Column Index of Wave: Determines which wave dataset will be plotted in the Read and Graph Waveform Values against Subregion Statistics vi.
    a. The options are the following:
        i. 0=Time
        ii. 1=Real
        iii. 2=Imaginary
15. (Incoming Real Wave) Column Index of Wave: Determines which wave dataset will be plotted in the Read and Graph Waveform Values against Subregion Statistics vi.
    a. The options are the following:
        i. 0=Time
        ii. 1=Real
        iii. 2=Imaginary
16. (Incoming Imaginary Wave) Column Index of Wave: Determines which wave dataset will be plotted in the Read and Graph Waveform Values against Subregion Statistics vi.
    a. The options are the following:
        i. 0=Time
        ii. 1=Real
        iii. 2=Imaginary
17. (DB and Incoming) Graph which sub-regions? (duplicates are ignored): Graphs the sub-regions by index number in the Compare DB and Inc Waveform Using Real and Imag Waveform Values vs. Subregion Stats vi.
    a. The numbers are mapped to statistics names following the table immediately to the right of the array.
18. (Debug Real) Average Percentages per Subregion: Displays the arithmetic mean of each subregion's calculated statistics for the real incoming waveform.
    a. Use to determine which sub-regions are best for classifications.
19. (Debug Imag) Average Percentages per Subregion: Displays the arithmetic mean of each subregion's calculated statistics for the imaginary incoming waveform.
    a. Use to determine which sub-regions are best for classifications.
20. File Path of Best Matching Waveform (Full Wave): Displays the file path for the raw data file of the most similar database waveform for a given incoming waveform based off of full wave comparisons.

    a. Use this to determine which device is most similar to the incoming waveform's transmission device.
21. File Path of Best Matching Waveform (Sub-regions): Displays the file path for the raw data file of the most similar database waveform for a given incoming waveform based off of subregion comparisons.
    a. Use this to determine which device is most similar to the incoming waveform's transmission device.
22. Transmitter ID: Used to store the transmitter ID in the database profile description.
    a. Type in the Transmitter ID.
23. (DB and Incoming) Graph which statistic?: Determines which statistics will be graphed in the Read and Graph Waveform Values against Subregion Statistics vi.
    a. Use to visualize the effectiveness of each statistic.
24. Receiver ID: Used to record the receiver ID in the database profile description.
    a. Type in the receiver ID.
25. DB Pulses to compare: Set the number of pulses from the database that will be used for comparisons.
    a. Note: Should not be larger than the actual number of pulses stored in a database.
26. Environmental Conditions: Used to record the environmental conditions in the database profile description:
    a. Type in the environmental conditions.
27. Statistical Features List: Used to record the names of the statistical features for which stats were generated in the database profile description.
    a. Type in the feature names.

File Paths: This section reviews the file paths tab of the front panel.

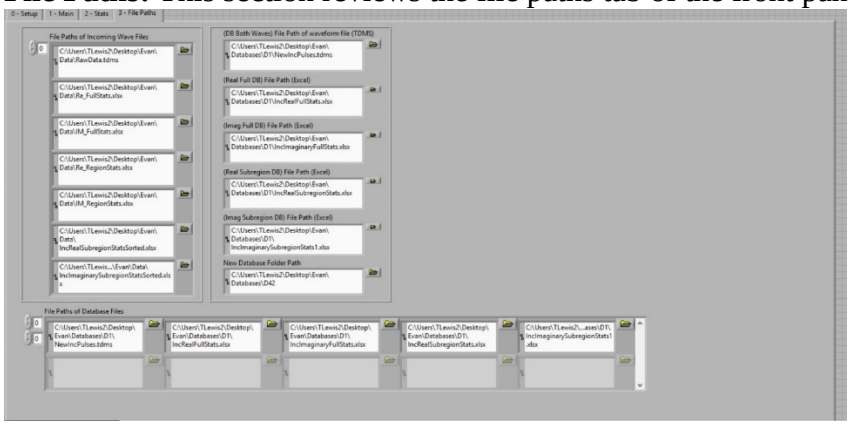


Figure 71. File Paths Tab

1. File Paths of Incoming Files: Array containing the file paths to which each incoming wave file will be saved.
    a. Input in the following order from the top of the array to the bottom of the array:
        i. Unorganized raw data (tdms)
        ii. Real full stats (excel)
        iii. Imaginary full stats (excel)
        iv. Real unsorted subregion stats (excel)
        v. Imaginary unsorted subregion stats (excel)
        vi. Real sorted subregion stats (excel)

vii. Imaginary sorted subregion stats (excel)
   b. To change, click on the small yellow folder button and choose a new file path.
2. (DB Both Waves) File Path of Waveform File (TDMS): File path of organized raw data file from existing database to be used for comparison.
   a. TDMS file format.
   b. To change, click on the small yellow folder button and choose a new file path.
3. (Real Full DB) File Path (Excel): File path of real full stats file from existing database to be used for comparison.
   a. .xlsx file format.
   b. To change, click on the small yellow folder button and choose a new file path.
4. (Imag Full DB) File Path (Excel): File path of imaginary full stats file from existing database to be used for comparison.
   a. .xlsx file format.
   b. To change, click on the small yellow folder button and choose a new file path.
5. (Real Subregion DB) File Path (Excel): File path of real subregion stats file from existing database to be used for comparison.
   a. .xlsx file format.
   b. To change, click on small yellow folder button and choose a new file path.
6. (Imag Subregion DB) File Path (Excel): File path of imaginary subregion stats file from existing database to be used for comparison.
   a. .xlsx file format.
   b. To change, click on the small yellow folder button and choose a new file path.
7. New Database Folder Path: Folder path of new database to be created.
   a. Creates or overwrites database at this location when enabled.
   b. Appends to database at this location when enabled.
   c. Reads unorganized raw data file from this location when fix stats is enabled.
8. File Paths of Database Files: 2D array of file paths for database comparisons.
   a. Each row of the array is used to specify a different device.
   b. Within each row, the database files must be selected in the following order from left to right:
      i. Organized raw data (tdms)
      ii. Real full stats (excel)
      iii. Imaginary full stats (excel)
      iv. Real sorted subregion stats (excel)
      v. Imaginary sorted subregion stats (excel)

ANNEX V: Generating Messages for Invariant Transmissions

Research Lead: Maj. T. Lewis
Intern/Research Assistant: Paul Dunaway

Requirements:

- Python 2.7 Installed
- Windows 7 or later
- To edit the program, Python 2.7 IDLE is recommended

Instructions:

1) In **File Explorer**, navigate to "C:\Users\TLewis2\Desktop\Paul\"
2) Double click "**GenerateMFiles.py**" to run the script
3) Once the script has finished, a new File Explorer window will appear at the location of the saved message files

Files Created:

1) "**m_01.txt**" – 1500 characters, repeated '0101' pattern
2) "**m_0011.txt**" – 1500 characters, repeated '0011' pattern
3) "**m_all_ones.txt**" – 1500 1's (ones)
4) "**m_all_zeros.txt**" – 1500 0's (zeros)
5) "**m_random1.txt**" – 1500 characters, random number of 0's and 1's, scattered
6) "**m_random2.txt**" – 1500 characters, random number of 0's and 1's, scattered, just another RNG algorithm

ANNEX W: Generating Trusted Waveform States w_s

A simple analogue FM circuit modulates a baseband information signal ($\boldsymbol{s_i}$) onto a fixed sinusoidal carrier wave ($\boldsymbol{c_t}$) and transmits a modulated waveforms w_i as output. A subset of authorized baseband signals are transmitted through a fixed state modulation circuit, producing a trusted complex waveform state as output (w_s). Where $\boldsymbol{w_s}$ is a repeatable modulated waveform state generated by a fixed transmission circuit $c(t)$. Let $s_s(t)$ represent the trusted subset of input baseband signals into a sinusoidal FM modulator as described by Stewart et al [85]. A single baseband input analog signal with an amplitude A_i and a frequency f_i can be expressed as;

$$s_i\,(t) = A_i\,cos(2\pi f_i t) = A_i\,cos(\omega_i t) \tag{1}$$

Where $\omega_i = 2\pi f_i$.

When there is no present input baseband signal, the FM modulated carrier output of a single component with amplitude A_0 and a frequency f_0 takes the form;

$$c\,(t) = A_0\,cos\big(2\pi f_0 t + \hat{\theta}(t)\,\big) \tag{2}$$

Summing the product of the input baseband signal and a modulation constant k_0 into an FM modulation transmitter, the instantaneous phase (IP) of the generated FM waveform output is determined by:

$$\hat{\theta}(t) = 2\pi K f_m * \sum_{-\infty}^{t} s_i(t) \tag{3}$$

Where K is the gain. As the baseband signal arrives at the circuit for integration, a frequency deviation occurs as sinusoidal terms on either side of the carrier frequency. This deviation is known as the modulation index and represented by the symbol (H). As a present baseband signal is modulated onto $c(t)$ through a fixed FM circuit, the phase (effective frequency) of the carrier waveform is modified in response to the amplitude variations of $s_i\,(t)$ according to H. A repeatable FM modulated waveform signal event w_i, using the carrier's amplitude and frequency given by A_c and f_c becomes;

$$w_i\,(t) = A_c\,cos\left(\omega_c t\; +\; H_{fm}\,sin(\omega_i t)\right) \tag{4}$$

Given K and f_c the instantaneous frequency (I_f) is obtained with;

$$I_{f\,_{w_i}} = f_c\; +\; K_{fm} s_i(t)\;Hz \tag{5}$$

1) RF-DNA Fingerprint Process Overview

The values of the physical waveform event as provided in Eq. (4) contain only the real valued data and may not produce statistically significant results that describe the repeatable waveform's characteristics uniquely. Physical phenomenon descriptors [86] of a signal such as its instantaneous Amplitude (I_A), Phase (I_θ) and Frequency (I_f) are often used to quantify the waveform and is represented here as $A(n)$, $\theta(n)$ and $f(n)$ respectively. In order to maintain the uniqueness property of instantaneous features of a modulated waveform, the sampled waveform must maintain the real and imaginary (I/Q) features of w_i**.** A Hilbert

transform is used to preserve the extracted I/Q feature values of w_i [4] and is used to up convert Eq.(4) and becomes complex as:

$$w_{iC}(t) = w_I(t) + w_Q(t) \tag{6}$$

These retained I/Q data values are used to compute the I_θ features as;

$$I_\theta = \theta_{w_{iC}}(n) = tan^{-1}\left[\frac{w_{Q(n)}}{w_{I(n)}}\right] \tag{7}$$

Compared to Eq.(15) the I_f features of a unique complex waveform are computed as;

$$I_f = f_{iC}(n) = \frac{1}{2\pi}\left[\frac{d\theta_{w_i}(n)}{dt}\right] Hz \tag{8}$$

Statistical RF-DNA fingerprints (F) are features generated based on the statistical behavior of the instantaneous response(s) over some fixed regions of interest (ROI) contained within the result of Eq.(6) above [4]. An example of an ROI in a standardized modulation scheme such as GFSK signals is the *preamble* region. A preamble is a standardized protocol encoding specification used in a communications signaling scheme.

Using a specified ROI instead of the entire $\boldsymbol{w_i}$, a less computationally expensive I_A can be used to determine the signal's central moments for a population of n samples. The population mean across the entire waveform is used to remove collection bias and to account for uncontrolled power variation that may occur. This transformation is used to center the waveform and can be applied to a specific ROI for optimal feature computation. The centered amplitude ($A_{centered}$) is therefore:

$$A_{centered}(n) = A(n) - \mu_A \tag{9}$$

$$f_{centered}(n) = f(n) - \mu_f \tag{10}$$

Normalization is performed for each sample of the specified ROI by dividing by the maximum magnitude of responses of Eqs. (9) and (10) to yield the first central moments for amplitude and frequency as;

$$\bar{A}_{centered}(n) = \frac{A_{centered}(n)}{max|A|} \tag{11}$$

$$\bar{f}_{centered}(n) = \frac{f_{centered}(n)}{max|f|} \tag{12}$$

The trusted circuits states are used to generate the trusted waveform event, collect ROI samples, and process the RF-DNA fingerprint credentials for future authentication operations. Adapting Bishop's definition, a *security policy* (p_i) is a statement that partitions all possible circuit generating waveform states into a two sets of *authorized (*i.e. *secure)* and *unauthorized (i.e. non-secure)* states [62]. Authorized waveform transmission events inherently carry the trusted RF-DNA fingerprint markers and are generated by s and transmitted to d for origin integrity validation. When p_i specifies a set of authorized circuit transmission states, the resulting secure transmitted waveforms constitute the RF-Events and is distinguishable from all other possible events Eq.(6). The set of trusted waveform states are defined as;

$$\boldsymbol{w_s}(t) \subseteq w_i\,(t) \;\; where\; i{:}\, 1,2,\dots s,(s+1),(s+2),\dots(s+i),i \tag{13}$$

2) Device Specific Encoding Rule Signature Development for Verification

Device-based Encoding Rule

Consider a circuit that is capable of transmitting two of four command messages to Rx_d. Let s_1 = the authorized source circuit state that generates a baseband message to represent command-1 $(c_{k=1})$. Using some fixed bit-sequence ID field, we select Tx_s as the front-end circuit encoder for the authorized carrier source state to Rx_d. In order to protect against attacks from Tx_{oPP}, w_s is encoded using one and only one front end device as the primary circuit state encoding rule. Let $\{E\}$ denote the set of all circuit encoding rules of m where $m \subseteq M$ is much greater than W. A device-based circuit source state encoding rule of a fixed circuit is denoted by $e_{Tx_s} \in E$ and provides a 1-to-1 mapping from W to M. The range of $e_{Tx_s}(W)$ generated by Tx_s consists of a subset of M that possesses the RF-DNA markings of its original source. Prior to transmission, policy p_i is made such that network devices Tx_s and Rx_d agree upon a w_s to employ the circuit encoding rule e_{Tx_s}, collect RF measurements of the device encoded state and stores the RF-DNA fingerprint signature into the memory of Rx_d. Given p_i, w_{s_i}, e_{Tx_s} and Rx_d, we define a circuit source state's RF-DNA fingerprint supportive encoding rule for trusted command messages as;

$$e_{Tx_i}(w_s, m_{is}) \rightarrow (c_k)_{is} \tag{14}$$

Where e_{Tx_s} is the ***s***th transmission device used as the circuit encoding rule, w_s is the device's ***s***th circuit transmission state. The modulated message m_{is} is the ***i***th circuit source state that was encoded using the ***s***th transmission device. The resulting ***k***th command contains the extractable RF-DNA fingerprints of the ***m***th message. Such credentials may be validated by a designated ***d***th authenticator device Rx_d upon receipt of a new claim.

Device-Specific Decoding Rule

We now focus on defining a decoding procedure of RF-Events to reveal the logical and physical informational content of $m's$ claimed credentials by a specified authenticator device Rx_d. In general Rx_d observed RF-DNA fingerprint extractions from a specified transmitter are statistically independent from all other receivers Rx_i. The encoded circuit credential c_k from Eq(3) are transmitted across a communication medium (e.g. wireless). Upon receipt of an RF-Event w_i, Rx_d tests to see if m_{ij} appears in the authorized range $e_{Tx_s}(W)$. If so, m's chances of being accepted as authentic may increase, otherwise m_{ij} is rejected for command processing. Rx_d recovers the source circuit state from m_{ij} by physically determining (i.e. RF measurements) its RF-Biomarker levels under policy-based device encoding rule for a given circuit. We assume Tx_{oPP} has perfect knowledge of the communication system, including all devices used to encode the circuit states. However, Tx_{oPP} does is unaware of any inherent secret RF-DNA characteristics that a source circuit employs as a natural signature encoding rule known by the $s \rightarrow d$ pairing of Tx_s and Rx_d. Tx_{oPP} may succeed in spoofing if and only if the RF-DNA fingerprint indicators of m_{ij} match the fingerprints of previously agreed upon circuit state encodings used prior to communication. The subspace of valid messages as observed by authenticator Rx_d, is unique for each device, however a receiver's ability to sample a continuous RF-Event is imprecise and therefore there are no perfect matches. A tolerance interval may be effective in mitigating this imperfection.

Generally, any logical command can be decoded using localized RF component features when a policy has specified the communication source to destination path. We state this more formally as follows;

$$f_{Rx_d}\left((c_k, m_{is}) \rightarrow w_{is}\right) = e_{Tx_i} \tag{15}$$

Where p_i specifies f_{Rx_d} as an authorized authenticator/observer of RF-Event w_s generated by device encoding rule e_{Tx_s}. When physical evidence is discarded from incoming RF-Events, it may be possible for Rx_d to accept m as authentic based on the decoded bit-level credential match, despite having originated from an untrusted physical circuit source state. To see this, select any arbitrary receiver of m_{ij} which employs conventional protocols to decode (1) to obtain the **k**th logical bit-level command $m_{ij} \mapsto \left(c_{ij}\right)_k = c_k^{BIN}$ without regard to the associated physical RF-DNA of e_{Tx_s}. Due to high demands for interoperability, there may be multiple instances of RF-events generating sources which generate m that maps to the correct logical interpretations of command c's logical (bits) credentials. As an example, consider of mapping of $e = 3$ interoperable encoding devices that can transmit in only three authorized circuit source states $\boldsymbol{w_s}$ where $s = 3$. We have $e^s = 9$ statistically unique messages are generated using the circuit source encodings to produce three logically equivalent commands that can be decoded by Rx_d. The state of the circuit during transmission of m can be from a single source or from multiple sources so long as they are physically distinct with respect to the final baseband signal that is modulated onto the circuit's RF carrier. Example: When $\boldsymbol{Tx_3 = e_{Tx_3}}$ encoding rule is used to encode circuit state $\boldsymbol{w_3}$, a unique message $\boldsymbol{m_{33}}$ is produced that is logically decodable by $\boldsymbol{Rx_d}$ as a valid command $\boldsymbol{c_3}$ and is be expressed as; $\left\{\boldsymbol{e_{Tx_3}(w_3) \rightarrow m_{33}}\right\} = \boldsymbol{c_3^{BIN}}$. Notice that when devices $\boldsymbol{Tx_1}$ and $\boldsymbol{Tx_2}$ are used in an identical configuration, the logical decoding of $\boldsymbol{m_{33} = m_{13} = m_{23}}$ when the physical characteristics of the RF-Event is discarded during receipt by $\boldsymbol{Rx_d}$.

ANNEX X: Composite RF-DNA Strength Augmentation

Multiple decision-support thresholds employed in parallel improves the baseline diagnostic test of RF-DNA fingerprinting. A benchmark RF-DNA signature template utilizes fingerprints from authorized circuit source states to develop authentication support credentials. A physical network configuration transmits and receives modulated messages from trusted sources for authentication using exchanged RF-DNA fingerprints. This article aims to improve the confidence of logical-only claims using a combined physically determined RF-DNA fingerprint to augment authenticity verification in uncertain conditions. Results show an initial baseline intrinsic accuracy of 84% using a composite RF-DNA fingerprint containing eight distinct features improves to near perfect infectious and benign correct classification. The infectious credential acceptance rate improves from 23.3% (baseline) to 100% (augmented). Multiple authentication verification mechanisms generally increase the intrinsic accuracy of a composite RF-DNA fingerprint classifier.

Introduction

A diagnostic radio frequency distinct native attribute (RF-DNA) fingerprint template is developed as an initial classification baseline for mitigating infectious credential acceptance in a network environment. The baseline intrinsic accuracy of the classifier is augmented using multiple classifiers sing three main treatments. The first treatment incorporates ordinal data thresholds that employs a majority + 1 rule for classification. The second treatment incorporates continuous data thresholds by dividing the baseline confidence interval into four weighted risk zones. In all cases, the initial baseline threshold employs a Euclidean distance measure of similarity to classify logical credentials contained within received RF modulation emissions as either benign or infectious. If a RF pulse's underlying physical credential matches the template, then the logically claimed credential classification is a genuine benign credential. However, when an infectious classification occurs, the claimed contents of the RF pulse are untrusted and may cause undesirable network behavior called network *disease* if processed by a network node.

Background

Measuring Diagnostic Accuracy

When conducting analysis of two independent (logical vs physical attributes) variables produced by physical RF transmission events we evaluate the performance of a diagnostic test (binary classifier) to correctly classify the condition of the RF-carrier's symptoms and ultimately to classify the paired diagnostic condition of a logical and physical signature comparison. A gold standard (GS) is developed to conduct a prediction test after signature collection and combined credential classification [39].

Using a conventional 2x2-count table (confusion matrix) [61], the preliminary assessment of the GS is presented which accounts for the total number of carrier samples

(N) in the population. A true positive (TP) GS test result occurs when a received carrier's true signature condition is benign and a diagnostic test reports a benign carrier condition.

A true negative (TN) condition occurs when the carrier's true status is infectious and the diagnostic result is infectious. When a diagnostic test reports an infectious carrier condition and the true condition indicated by the GS are benign, a false positive (FP) count is increased. Similarly, when a GS indicates a true benign condition and the test reports an infectious condition, a false negative (FN) result occurs. The results of the count table indicate the probability or predictability of the two conditions.

The sensitivity (Se) of the diagnostic test provides the probability that a test result will be positive (benign) and is determined by the TP count divided by the total number of carriers specified as signature immunizations. The specificity (Sp) of diagnostic testing is the converse of the Se and measures the capability to exclude infectious carrier conditions. The prevalence of a specific network threat does not affect the intrinsic diagnostic accuracy indicated by a test's Se or Sp [61].

When considering network response or treatment options when infectious (unauthorized or rogue) carriers are indicated, a policy defined decision threshold (dT) is used. For binary data, *dT* is used that best dichotomizes uncertain conditions into one of two classes. Here, dT is determined using signature values of observed RF-biomarker levels, which indicate the most dissimilarity or disease risk(X). A trade off exists when developing a *dT* that best classifies a GS condition. A net *benefit* is realized when an observed abnormal network disease outcome occurs despite diagnostic treatment against infectious carriers. The overall *cost* of disease avoidance is realized when observers (authenticator device node) needlessly (utilize scarce resources) *suffer* because infectious carriers do not exist in the network environment (i.e.$p = 0$), yet treatment is still provided. A Type-I error measures the FP rate that occurs in proportion to the total number of true benign carriers that exist in the GS. A Type-II error is determined by the FN rate of a carrier's tested result as benign when in fact the RF-carrier is infectious. Predictive values quantify the usefulness of the paired diagnostic test result for network disease mitigation [39]. The probability of a positive test is the positive predictive value (PPV) and the likelihood of a negative test result is the negative predictive (NPV).

Methodology

The configuration of three transceiver devices appears as a wireless communications network in Figure 1. Policy determines authorized transmission and receiver device pairs. As shown, trusted transmission circuit source state (Tx_s) is authorized to generate logical messages m_i using some credential (c_k) and transmit its modulated RF-event towards a specified destination authenticator Rx_d for diagnostics of the credentials used to enhance the determination of the true origin integrity of m_i. An opponent transmitter (Tx_{oPP}) aims to impersonate or modify m_i generated by Tx_s in order to bypass bit-level authentication mechanisms and gain unauthorized access to resources controlled by Rx_d. $Rx_d{}'s$ network treatment and wellness plan (RF-DNA

immunization using RF-Biomarkers) against a specific network disease caused by infectious credential acceptance is employed to mitigate the prevailing threat presented by Tx_{oPP}.

Prior to conducting network operations, the memory emplacement of RF-DNA fingerprints of Tx_s occurs inside Rx_d as a trusted benign signature (immunization). During normal communication operations, a comparison of a new claim's fingerprint against the baseline signature occurs. The diagnostic tests provides a match (BENIGN) or infectious (No Match) result. When an *infectious* result occurs, an appropriate treatment response follows to mitigate the occurrence of network disease in the future. A *benign* diagnostic result improves the confidence of logical credential mechanism validations.

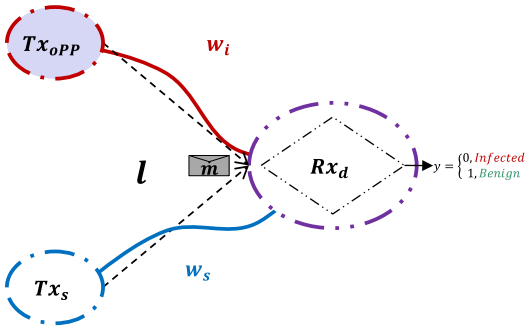


Figure 72. Impersonation Threat Model

There are 1100 training pulses observed by Rx_d and which form the basis of an independently observed or device specific benchmark RF-Event diagnostic test. To determine the strength of the training pulses, a self-similarity test assists in determining if a distribution of pulses appears normal. After validating that the distribution for the composite RF-DNA was normally distributed, the self-similarity test, where each 1100 pulses compares to all other 1099 pulses. The average Euclidean distance between all pulses becomes the benchmark's composite average *strength* score. This score simply provides a measure of well each training pulse looks like its population of peers. In theory, each pulse would look perfectly identical, however we aim to obtain statistical similarity with little population variance.

To evaluate the composite RF-DNA benchmark strength, 150 new credential claims from source Tx_s are generated and diagnosed by Rx_d. Next, an additional set of 150 new credential claims are generated from unknown source Tx_{oPP} using identical modulation schemes and communication protocols as Tx_s. Finally, a device specific Gold Standard (GS) test development begins, where the stored RF-DNA fingerprint results extracted from the new 150 benign claims from Tx_s, are modified by randomly selecting infectious results extracted Tx_{oPP}. The final GS contains a 150-sample dataset, using a p = 20% threat prevalence rate, yielding 120 TRUE benign pulses and 30 TRUE infectious pulses. Each composite contains eight RF measurements taken

over the same region of interest which produces eight distinct RF-biomarker levels for each measurement.

Baseline Decision Threshold Selection

The tolerance of IAC experimentally increases from zero to one in increments of .01 to determine if the area under the curve is significant. An arbitrary tolerance of 0.05 selection results in a 95% confidence interval of ICA.

In this article the benign credential acceptance (BCA) is synonymous to a TP, while a count of infectious credential acceptance (ICA) is synonymous is TN. The probability rates for sensitivity (Se) specificity (Sp), intrinsic accuracy (ACC) BCA and ICA are compared using three parallel decision support threshold treatments.

A baseline intrinsic accuracy score results using a fixed tolerance of $dT = 0.05$ and a normalized Euclidean distance metric. After the baseline results were determined, we considered augmenting the results to improve ACC using ordinal and continuous valued thresholds. The objective of each treatment aims at maximizing the ACC while minimizing the rate of ICA.

Fusion of Multiple Decision-Support Cues (Multimodal/Multi-factor)

An decision-support cue provides useful information that is considered in making decisions after the knowledge of the cue's state is considered (posterior). The states of a cue contains rich information characteristics such that certain states provide more or less information depending on the characteristics or features correlated with the cue's indicated state. An indicator such as a RF fingerprint should satisfy the following requirements of universality, uniqueness, permanence and collectability. In RF-DNA fingerprinting Temple et. al uses the main characteristics of amplitude, frequency, phase. The features of the RF-DNA fingerprints are then collected using a RF measurement device that captures the skewness, kurtosis, variance and standard deviation for each characteristic to meet the requirements above. In order to make a fingerprint useful, the features of a unique subject must be stored and later recalled for comparison to a new fingerprint. During the comparison, the same characteristics are considered and the status of the feature cues are measured. In dynamic network decision making, the state of such cues are often used to enhance a person's situational awareness (SA) [56] about the network's behavior during troubleshooting or normal operation procedures. Each feature may be collected by one or more sensor devices (modality) to form a composite RF-DNA fingerprint which is contain the richest indicator features concerning the cue's original or more natural state.

Keeping an accurate track of a cue's state in a dynamic environment may lead to unacceptable misclassification rates for decision makers. For this reason, a unimodal approach that utilizes a single authentication classifier may not be trusted in uncertain situations such as noise or high threat prevalence. By integrating or fusing multiple decision-support cues, the accuracy of unimodal classifier performance is generally

improved when **Invalid source specified.** multifactor (multimodal) authentication mechanisms are combined [9] **Invalid source specified.**.

Fusion conducted during earlier stages of *match scoring* is preferred in practice because of the ease of access to output scores when classifier modalities are poorly integrated or simply incompatible or when no access is available to a modality's raw feature extraction data-set **Invalid source specified.**. Nonetheless, Ross suggests that multimodal fusion at the *feature* extraction level may provide better recognition results, despite the difficulties in practice.

Bigun employs a Bayesian-based algorithm which aggregates and calibrates expert opinion match scores using independent classifier aggregation assessments and aggregation based on classifiers with some level of dependency for assessments prior to decision calibration **Invalid source specified.**. In practice, multiple techniques should be combined or integrated to improve verification accuracy [55]. Brunelli combines acoustical and visual classifiers to improve authentication verification systems [55]. In some cases, the integration of multiple classifiers may degrade overall performance, and when combined, the classifier's result must be

Here, we follow the technique of Bigun for the second case where a single receiver employs multiple independent RF-measurement classifiers towards the development of a single decision classification score. This technique is different from other RF fingerprinting techniques because it employs multiple decision thresholds to enhance a composite unimodal RF-DNA fingerprint template. In addition, each component feature of the fingerprint has its own tunable classifier at the decision level **Invalid source specified.**. In this article, such decision-level features are *RF-Biomarkers* and represent the physical RF characteristic of a received transmission event. As new RF events arrive for authentication verification, specific RF-Biomarker level extractions compare against benchmark levels. Specified decision thresholds determine the comparison score's classification result that indicates normal or abnormal network behavior.

Ordinal O_{dt} Selection/ Augmentation1

The two additional decision support augmentations include ordinal (odT) and continuous (zdT) decision-support criteria thresholds. The metric for odT match scoring considers the overall count of selected RF-Biomarker levels that passed for a given pulse. Given the variability in self-similarity inherent in a RF-DNA fingerprint benchmark profile, a general rule suggests that a majority of RF-Biomarkers should meet or exceed acceptance limits for a given threshold selection. While this may seem sound for acceptance, the converse may not hold since any single failure to meet a benchmark level by any RF-Biomarker may disqualify the acceptance of the entire pulse.

Continuous Risk Zones Z_{dt} Selection/ Augmentation2

The second threshold considers continuous data to partition the original benchmark baseline confidence interval into multiple (weighted) risk zones. Zone-1 indicates a RF-Biomarker match score that is 98.3% similar or better to a trusted benchmark. A Zone-2 result indicates match score outside of Zone-1 and meets a 96.67% benchmark similarity. A Zone-3 indicates that a RF-Biomarker exceeded the boundaries of Zone-1 and Zone-2, but falls within the original baseline 95% confidence interval {U,L}. All other match scores values are considered Zone-4 critical failures using $\boldsymbol{Z_{dt}}$. Each RF-Biomarker's zones are independent. A total of 1200 RF-Biomarkers (8RF-Biomarkers/Pulses* 150Pulses) are considered during this experiment.

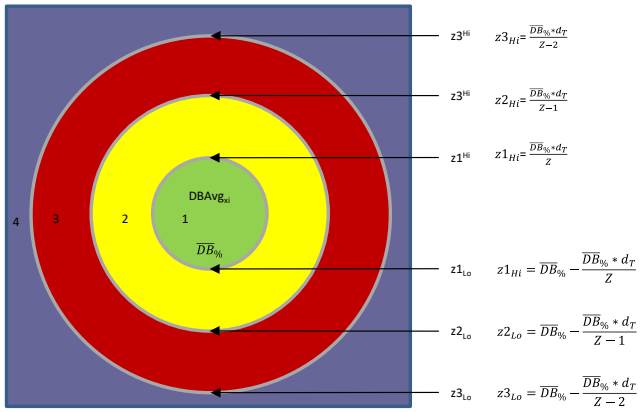


Figure 73. RF-Biomarker Risk Zones of Acceptance

Results & Analysis

As an initial first step towards developing a diagnostic test, the aim was to collect a set of RF-DNA fingerprints, usable as signature template profiles for integration as a network treatment and wellness plan. During the RF-DNA fingerprint collections process, pulses contained significant variation from pulse to pulse. Some explanation occurs from sampling procedures, while other variations occur due to a lack of device synchronization. The USRP2922 devices are development and testing only devices and not as intended as end network nodes. We improved the synchronization between devices so that a binary string reception and synchronization offset occurs prior to demodulation in order to recover and decode the baseband digital string with confidence. This step provided verification that the proper message was readable. The reliability of successful receipt was approximately 60%. To mitigate this unfortunate effect, the RF-event was collected such that the start and end time of each pulse was statistically identical between pulse collections yielding statistically consistent pulse collections of a known RF-event. To minimize triggered pulse impurities, a filter

removes nonconforming pulses in the final benchmark distribution. Using this method, we improved a saved pulse rate to nearly 80% acceptance during raw collections.

Baseline Benchmark Results

A ROC curve of Figure 4. Indicates a trade-off between the rate of benign credential acceptance (BCA) versus the infectious credential acceptance (ICA) rate when varying a tolerance threshold value from 0 to 1. The upper left hand quadrant suggests an optimized system may achieve approximately 85% BAC, while allowing approximately 20% of infectious credentials. The red line indicates a chance line. The ROC indicates a threshold of less than 0.2 would provide a 80% confidence interval for BCA, while risking a 20% ICA rate. The lower bound of the ROC indicates that a dT selected below 0.05 may result in less than 70% BCA yet achieve over 90% infectious credential rejection. This article arbitrarily selected a $dT = 0.05$ with an infectious credential prevalence rate $p = 0.2$. These selections provide a 95% confidence interval for BCA, while allowing about 5% ICA. As the ROC curve shows, baseline accuracy fails to achieve 100% accuracy however, when augmented with additional threshold conditioning, near perfect classification is possible. The summary performance results obtained appear in Tables 2-9.

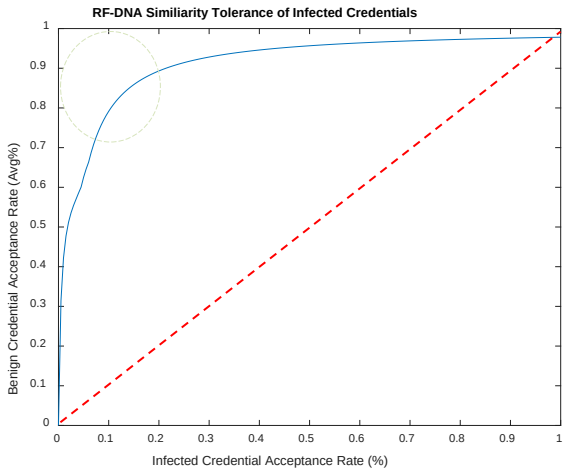


Figure 74. Benign vs. Infectious Credential Acceptance.

Table 35 shows the composite RF-DNA *benchmark* profile of a collection of 1100 pulses for $Tx_s{}'$s normal RF-Biomarker response levels. The diagnostic benchmark (DB) strength consistency across all RF-Biomarker levels for the transmitter was 75.7480%. Using a 95% tolerance interval, valid average RF-Biomarker levels could fall within 72 – 79%. The results of comparing a single infectious credential show a similarity of 64.97%. When using a gold standard, against a population of 150 new credential claims and a 20% threat prevalence, the average similarity of the benchmark dropped to 72.67%. While all new 150 benign claims averaged 76.02% benchmark

similarity. Table 35 indicates that the benchmark similarity does provide some level of discrimination between benign and infectious credentials.

Table 35 Similarities for self, vs. (n=150) batch vs. single infectious RF-Event

RF-Biomarker Classifier	*Infectious Pulse #5*	*Gold Standard Batch N= 150, p=0.2*	*DB=1100 Benchmark*
b_1	14.20	24.11	23.87
b_2	19.10	83.61	99.87
b_3	97.17	61.11	59.83
b_4	94.99	97.71	99.72
b_5	33.55	24.77	23.86
b_6	65.83	92.31	99.10
b_7	97.46	98.83	99.86
b_8	97.46	98.83	99.86
Composite Strength Score	64.97	72.67	75.74

Baseline Benchmark

The baseline RF-DNA diagnostic *benchmark* is composed of eight independent RF-biomarker components and is visualized in as the green bar plot in Figure 5 to represent the average response of true benign fingerprint similarity levels that are observed by Rx_d from the transmission source Tx_s. At the top of each RFB, a three-tier 95% tolerance interval indicates how well a claimed credential's claimed level matches its benchmark.

As depicted in Figure 6, a set of $N = 150$ pulses are received and diagnosed for network disease to enhance the confidence of logical authentication validation in uncertainty. The batched processed GS file's results are compared to the benchmark, where the claimed values are indicated in gray and the benchmark level is in green. An examination of Figure 6 indicates that $\boldsymbol{RF_{b1}}$ $\boldsymbol{RF_{b5}}$, $\boldsymbol{RF_{b7}}$, and $\boldsymbol{RF_{b8}}$ show a strong zone1(low risk) level of similarity zone acceptance, while $\boldsymbol{RF_{b2}}$ and $\boldsymbol{RF_{b6}}$ indicates a significant RF-Biomarker level deficiency and fails to meet any target zone of risk acceptance. $\boldsymbol{RF_{b6}}$ also fails to meet zone tolerance requirements. $\boldsymbol{RF_{b4}}$ indicates a Zone-2 (medium risk) acceptance.

The benchmark RF-Biomarker levels of a composite RF-DNA fingerprint profile is displayed as green bars that range in concentration from zero to one. The benchmark is used to assist new credential authentication claims in uncertainty. A set of 150 new pulses are compared as a batch process to detect the possibility of infectious credential acceptance. The diagnostic results are indicated in grey and are plotted on top of the benchmark levels. There were a total of 120 benign pulses and 30 infectious pulses in this batch dataset. As shown, the system correctly diagnosed all benign pulses, and correctly specified the infectious pulses that failed to meet RF-biomarker thresholds. Overall, the batch indicates concern for infection that may lead to network disease specifically with a low level of $\boldsymbol{RF_{b1}}$ and $\boldsymbol{RF_{b6}}$. The levels of $\boldsymbol{RF_{b3}}$ indicate a medium risk of infection. Batch processing might best be used as a forensics

augmentation tool for example, but may not be readily useful for real-time information systems that require a pulse by pulse response.

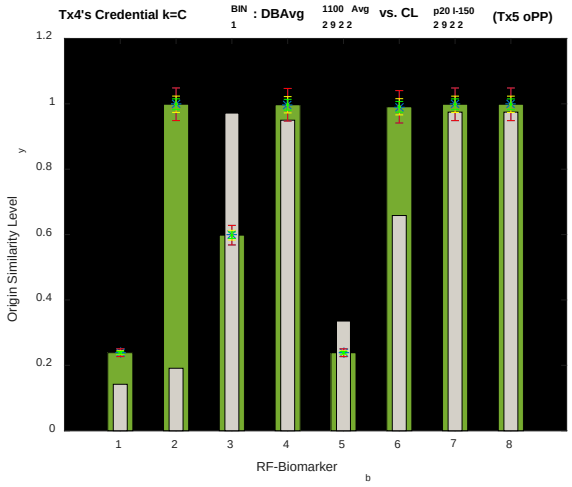


Figure 75. Benchmark vs. single *infectious* credential from Tx_5.

Infectious Pulse #5 was selected from a Gold Standard benchmark test developed specifically for trusted device Tx_4. Similarity results that compare the single pulse to the composite RF-DNA fingerprint is shown on the left of Table 36. RF-Biomarkers 1-6 fail all diagnostic tests, while markers 7-8 fall within a medium risk of truly being infectious. A significant low level of dissimilarity for $\boldsymbol{RF_{b2}}, \boldsymbol{RF_{b6}}$ suggest a significant deficiency in benign levels that wold be expected to be found in a normal benign pulse received from Tx_4, while the concentration of $\boldsymbol{RF_{b3}}$ and $\boldsymbol{RF_{b5}}$ indicate significant high concentration levels that are outside the observed (Rx_d) boundries for the composite RF-DNA fingerprint. The entire 95% confidence interval spans the width of red error bars for the benchmark levels. Yellow error bars indicate a medium risk of ICA. The green error zone indicates that a RF-Biomarker has a similarity level that matches a benchmark profile, which suggests a low level of risk.

The Gold Standard developed for USRP2922 Tx4 represents the base benign credential file with 150 pulses. Tx5 is the opponent device that provides infectious pulses at a rate of $p = 0.2$ or 20% of the N benign pulses. The truth of each pulse is withheld from the observer Rx_d until during testing. After testing, a count table of BCA (TP), ICA (TN), FP, FN presents the receiver diagnostic performance findings.

Table 2 provides a summary of the counts that occurred from the GS diagnostic test of 150 new pulse claims. The system diagnoses results in 143 benign and seven infectious classifications. In truth, there are 120 benign and 30 infectious pulses in the GS population.

Table 36 Baseline (2x2) Count Table using Euclidean Distance

True Condition Status	*Positive (Test =1)*		*Negative (Test =0)*		*Totals*
Benign = 1	BCAs	120	FN	0	120
Infectious = 0	FPs	23	ICA	7	30
Totals		143		32	150

A probability table provides a measure of how likely a system will perform in normal operations when placed in a representative operational environment. The probability can be determined using the GS total population size to determine the rate of acceptance for BCA and ICA. The Se was found to be 100%, while the false positive rate was high at 76.67%. Although the false negative rate was low at 0%, the Sp was 23.33%. The overall intrinsic accuracy is used as a single estimate of how well the receiver will perform and considers the Se and Sp rates. The baseline benchmark ACC without improvements was computed to be 84.0% recalling the value indicated in the ROC from Figure 4. Above, this empirical result is close to the estimate maximum of 85% occurring at the elbow of the curve.

Table 37. Baseline Diagnostics Probability Results

True Condition Status	*Positive (Test =1)*		*Negative (Test =0)*		*Totals*
Benign = 1	Se	100%	FNR	0%	1
Infectious = 0	FPR	76.67%	Sp	23.33%	1

Baseline Benchmark + O_{dt} Results

After the benchmark intrinsic accuracy was experimentally determined, we introduced the additional threshold treatments to see if we could improve upon the rate of specificity. First, we employed the RF-biomarkers as described above but we included a minimum count of five that must meet passing requirements before the entire pulse if accepted as benign. This improvement produced an immediate decrease in the baseline FPR down to 0%. At the same time, the ICA rate increased from seven infectious pulses detections to 30 (100%) detection rate. The support of an ordinal valued threshold increases the ACC percentage by 328.63%.

Similar results were observed when the baseline benchmark performance was enhanced using risk zones and continuous date values. The risk zones ranged from 1 to 4. The BCA count declined by 2 pulses compared to the baseline benchmark, however the diagnosis of infectious pulses increased to 100% detection of the 30 pulses that were contained within the GS file. The two misses BCA pulses were counted as false negative pulses. The zone based ACC also improved to 100%.

Table 38. Count table of baseline Benchmark with treatments

Threshold	*BCA (TP)*	*FP*	*ICA (TN)*	*FN*
dT = 0.05	120	23	7	0
O_{dt} ***= 5/8***	120	0	30	0
Z_{dt} ***= 2.125***	118	0	30	2

Table 39. Results of baseline, ordinal and continuous zone diagnostic

Threshold	*Se%*	*FPR %*	*Sp%*	*FNR %*	*NPV %*	*PPV %*	*ACC %*
dT = 0.05	100	76.67	23.33	0	100	82.76	84.0
O_{dt} ***= 5/8***	100	0	100	0	100	96.77	96.77
Z_{dt} ***= 2.125***	98.3	0	100	1.67	100	100	98.67

The risk zones performance is further compared against the benchmark's results to understand the expressive nature of risk labels. 1200 RF-Biomarkers were assessed using the GS file dataset. The benchmark diagnosed 653/1200 RF-Biomarkers as being benign, in actuality there were 960 truly benign RF-Biomarkers contained within the dataset. Using the risk zones, we see that 605/960 benign pulses (63%) were within the low risk zone of acceptance. Approximately 4.6% of benign RF-Biomarkers were diagnosed as medium risk zones for infection.

Table 40. Baseline vs. Z_{dt} comparison for a 95% TI, n=1200 RF-Events

	Zone	*Baseline*	
Zone1	605	653	***Pass***
Zone2	10	-	-
Zone3	45	-	-
Zone4	540	547	***Fail***
%Pass	55.0	54.42	
Benign	960	960	
Infectious	240	240	
Totals	1200	1200	

Table 41. Ordinal and Continuous data threshold performance (Averaged 10 Trials)

edT	*eACC%*	*ePRt*	O_{dt}	*oACC%*	*oPRat*	Z_{dt}	*zACC%*	*zPRt*
BM	84.0	94.67	0	80.0	100	0	20.00	55.08
			1	85.3	94.67	.5	20.00	54.75
			2	86.67	96.00	1	20.00	55.5
			3	96.67	82.00	1.5	20.00	54.42
			4	100	80.00	2	25.33	55.25
			5	99.5	79.33	2.125	98.67	55.17
			6	23.3	3.33	2.25	99.33	54.58
			7	20.0	0	2.375	99.33	54.92
			8	20.0	0	2.5	99.33	54.50
						3	100.0	55.25
						3.5	96.67	54.50
						4	80.0	55.33

Conclusions and Future Recommendations

Using RF-DNA *benchmarks* as the basis for diagnosing infectious credentials, the research found significant improvement in the intrinsic accuracy by using multiple parallel decision-support thresholds. Such a scheme shows tremendous potential for larger datasets and devices synchronized for network communication. The benchmark's ACC improved to over 99.99% using $odT = \frac{sum\ of\ Passed}{total\ RF-Biomarkers} = \frac{5}{8}$ decision-support threshold for acceptance for each pulse received. In addition, the benchmark's ACC using zdT improves to 98.67%, providing more classification expressiveness. These findings suggest a multiple decision-support threshold criteria for benchmark level comparisons, coupled with component RF-Biomarker level augmentation provides improved network health for the prevention of network disease. An integrated multimodal verification technique allows dynamic selection of critical indicators that best discriminate between two classes using fusion at the feature and decision levels for verification.

Future Research Recommendations

Conduct a 'Forensics Analysis' augmentation application Study for *batch* post-processing of log files to determine if a receiver/network has or is likely to develop a specified network disease outcome. A comparison of benchmark values can be made using the RF-DNA and component RF-Biomarkers contained within the log files to determine if RF-DNA treatment is recommended to prevent or cure known or potential network disease (e.g. impersonation attacks). Test the device specific Gold Standards using more than one opponent to see how it does against like and dissimilar devices. Provide appropriate recommender system for infectious diagnosis using continuous data and risk zone classifications.

VII. References

[1] M. C. Duncan, K. M. Hopkinson, E. D. Trias and J. W. Humphries, "Trust Management Approach to Satellite System Telecommanding Security," *Journal of Aerospace Information Systems,* pp. 19-33, 2014.

[2] G. M. Coates, K. M. Hopkinson, S. R. Graham and S. H. Kurkowski, "A Trust System Architecture for SCADA Network Security," *IEEE Transactions on Power Delivery ,* pp. 158-169, 2009.

[3] W. E. Cobb, M. A. Temple, R. O. Baldwin, E. W. Garcia and E. D. Laspe, "Intrinsic Physical Layer Authentication Of Integrated Circuits". United States of America Patent US9036891 B2, 19 May 2015.

[4] W. E. Cobb, E. W. Garcia, M. A. Temple, R. O. Baldwin and Y. C. Kim, "Physical Layer Identification of Embedded Devices Using RF-DNA Fingerprinting," in *Waveforms and Signal Processing Track Military Communications Conference*, San Jose, CA, 2010.

[5] R. D. Deppensmith and S. J. Stone, "Optimized Fingerprint Generation Using Unintentional Emission Radio-Frequency Distinct Native Attributes (RF-DNA)," in *IEEE National Aerospace and Electronics Conference (NAECON)*, Dayton, 2014.

[6] T. Kohno, B. Andre and C. K. C, "Remote Physical Device Fingerprinting," *IEEE Transactions on Dependable and Secure Computing,* vol. 2, no. 2, pp. 93-108, 2005.

[7] A. J. Jeffreys and J. S. R. Brookfield, "Positive Identification of an Immigration Test-Case Using Human DNA Fingerprints," *Nature,* Oct 31 - Nov 6 1985.

[8] P. Gill, A. J. Jeffreys and D. J. Werret, "Forensic Application of DNA ‘Fingerprints’," *Nature,* vol. 318, no. 6046, pp. 577-579, August - September 1985.

[9] L. Hong and A. Jain, "Integrating Faces and Fingerprints for Personal Identification," *IEEE Transactions on Pattern Analysis and Machine Intelligence,* vol. 20, no. 12, pp. 1295-1307, 1998.

[10] E. G. Soenen, G. B. Davis and A. Dycus, "Rolling Code Identification Scheme For Remote Control Applications". United States Patent 5598475, 28 January 1997.

[11] T. L. Fox, "AX.25 Amateur Packet-Radio Link-Layer Protocol," American Radio Relay League INC, Newington, CT, 1984.

[12] H. Lans, "Position Indicating System". US Patent 5506587 A, 9 Apr 1996.

[13] T. G. Anderson and W. A. Boothroyd, "Transaction Execution System With Secure Data Storage and Communications". Patent 3956615, 11 May 1976.

[14] M. D. Williams, M. A. Temple and D. R. Reising, "Augmenting Bit-Level Network Security Using Physical Layer RF-DNA Fingerprinting," in *IEEE Global Telecommunications Conference (GLOBECOM)*, Miami, FL, 2010.

[15] V. L. Piscane and M. M. Feen, "Propagation Effects at Radio Frequencies on Satellite Navigation Systems," *5th Communications Satellite Systems Conference,* 1974.

[16] K. J. Ellis and N. Seriken, "Characteristics of Radio Transmitter Fingerprints," *Radio Science,* vol. 36, no. 4, pp. 585-597, July 2001.

[17] S. Stone and M. Temple, "Radio-Frequency-Based Anomaly Detection for Programmable Logic Controllers in the Critical Infrastructure," *International Journal of Critical Infrastructure Protections,* pp. 66-73, 2012.

[18] J. Toonstra and K. W, "A Radio Transmitter Fingerprinting System ODO-1," *Canadian Conference on Electrical and Computer Engineering,* vol. 1, pp. 60-63, 26-29 May 1996.

[19] B. W. Ramsey, T. D. Stubbs, B. E. Mullins, M. A. Temple and M. A. Buckner, "Wireless Infrastructure Protection Using Low-Cost Radio Frequency

Fingerprinting Receivers," *International Journal of Critical Infrastructure Protection*, pp. 27-39, 2015.

[20] C. Dubendorfer, B. Ramsey and M. Temple, "Zigbee Device Verification For Securing Industrial Control And Building Automation Systems," in *Critical Infrastructure Protection VII*, J. Butts and S. Shenoi, Eds., Washington, DC: Springer, 2013, pp. 47-62.

[21] G. C. Morrison, "Mobile Cubesat Command and Control Assemble and Lessons Learned," NPS, Monterey, CA, 2011.

[22] Icom Of America, "ICOM Instruction Manual IC-9100 HF/VHF/UHF Transceiver," Icom-Inc, Osaka, 2011.

[23] L. Zhang, C. An, Q. Zhang and C. Tang, "Misbehavior Detection Algorithm in CCSDS Space Telecommand System," *IEEE Communications Letters*, vol. 14, no. 8, pp. 746 - 748, 2010.

[24] B. W. Ramsey, M. A. Temple and B. E. Mullins, "PHY Foundation for Multi-Factor ZigBee Node Authentication," Air Fource Institute of Technology, Wright Patterson Air Force Base, 2015.

[25] K. B. Rasmussen and S. Capkun, "Implications of Radio Fingerprinting on The Security of Sensor Networks," in *Third International Conference on Security and Privacy in Communications Networks and Workshops (SecureComm)*, Nice, France, 2007.

[26] B. R. Kasper and C. Srdjan, "Implications of Radio Fingerprints on the Security of Sensor Networks," in *Third International Conference on Security and Privacy in Communications Networks and the Workshops (SecureComm)*, Nice, France, 2007.

[27] T. Lewis and K. M. Hopkinson, "Technical Report: Link Analysis & Threat Mitigation for Satellite Systems," 2015.

[28] T. Lewis, "Technical Report: Summer 2015 Summarized Preliminary Results and Future Research Proposal," 2015.

[29] B. W. Ramsey, B. E. Mullins, M. A. Temple and M. R. Grimaila, "Wireless Intrusion Detection and Device Fingerprinting Through Preamble Manipulation," *IEEE Transactions on Dependable and Secure Computing,* vol. 12, no. 5, pp. 585-596, 2015.

[30] E. Research, "USRP X300 and X310 X Series Product Manual," Ettus, Santa Clara, 2015.

[31] B. Sklar, "Fundamentals of Statistical Decision Theory," in *Digital Communications; Fundamentals and Applications*, 2nd ed., Upper Saddle River, Prentice Hall, 2001, pp. 1035-1050.

[32] K. H. Rosen, "Bayes Theorem," in *Discrete Mathematics and Its Applications,* 7th ed., New York, New York: McGraw-Hill, 2012, pp. 468-475.

[33] Cyber Security Division of NETSCOUT, "Worldwide Infrastructure Security Report: Attack Rates DDOS," Arbor Networks, 2016.

[34] R. Parasurman, "Humans and Automation: Use, Misuse, Disuse, Abuse," *Human Factors,* vol. 39, no. 2, pp. 230-253, 1997.

[35] K. A. Scarfone and P. M. Mell, "Guide to Intrusion Detection and Prevention Systems (IDPS): Special Publication 800-94," National Institute of Standards and Technology, 2007.

[36] T. A. S. Lewis, "An Artificial Neural Network-Based Decision-Support System for Integrated Network Security," Master's Thesis, Air Force Institute of Technology, Graduate School of Engineering and Management, Wright-Patterson AFB OH, 2014.

[37] C. Camara, P. Peris-Lopez and J. E. Tapiador, "Security and Privacy Issues in Implantable Medical Devices: A Comprehensive Survey," *Journal of Biomedical Informatics*, vol. 55, pp. 272-289, 2015.

[38] M. Darji and B. Trivedi, "IMD-IDS a Specification based Intrusion Detection System for Wireless IMDs," *International Journal of Applied Information Systems (IJAIS),* vol. 5, no. 6, pp. 19-23, April 2012.

[39] M. S. Pepe, The Statistical Evaluation of Medical Tests for Classification and Prediction, Oxford, New York: Oxford University Press, 2003.

[40] V. S. Vaidya and J. V. Bonventre, "Biomarkers: An Evolutionary Perspective," in *Biomarkers In Medicine, Drug Discovery, and Environmental Health*, Hoboken, New Jersey: Wiley, 2010, p. 1.

[41] C. L. Edelstein, Biomarkers of Kidney Disease, 1st ed., London, UK: Academic Press, 2011.

[42] X.-H. Zhou, N. A. Obuchowski and D. K. McClish, Statistical Methods in Diagnostic Medicine, Hoboken: Wiley, 2011.

[43] A. Ahmad, Mahmoud and T. A. Rizvi, "Virus Detection by Monitoring its Radio Frequency Response Versus Temperature," in *IEEE Progress in Electromagnetic Research Symposium (PIERS)*, 2016.

[44] G. Casella and R. L. Berger, "Conditional Probability and Independence," in *Statistical Inference*, 2nd ed., Belmont, California: Brooks/Cole, Cengage Learning, 2002, pp. 20-27.

[45] M. Sahami, S. Dumas, D. Heckerman and E. Horvitz, "A Bayesian Approach to Filtering Junk EMail," in *Learning for Text Categorization: Papers from the Workshop*, 1998.

[46] V. Brik and a. et, "Wireless Device Identification with Radiometric Signatures," in *Proceedings of the 14th ACM Iinternational Conference on Mobile Computing and Networking*, 2008.

[47] P. J. J. Koopman and A. M. Hebron, "Cryptographic Authentication of Transmitted Messages Using Pseudorandom Numbers". United States Patent 5377270, 27 Dec 1994.

[48] P. J. Koopman and A. Hebron, "Pseudorandom Number Generation And Cryptographic Authentication". United States Patent 5363448, 8 Nov 1994.

[49] G. DeJean and D. Kirovski, "RF-DNA: Radio-Frequency Certificates of Authenticity," in *Cryptographic Hardware and Embedded Systems*, p. Paillier and I. Verbauwhede, Eds., Vienna, 2007, pp. 346-363.

[50] R. W. Klein, M. A. Temple and D. R. Reising, "Sensitivity Analysis of Burst Detection and RF Fingerprinting Classification Performance," *IEEE International Communications Conference (ICC)*, pp. 1-5, 2009.

[51] W. C. Suski, M. A. Temple, M. J. Mendenhall and R. F. Mills, "Using Spectral Fingerprints to Improve Wireless Network Security," in *IEEE Global Telecommunications Conference (GLOBECOM)*, New Orleans, 2008.

[52] D. R. Reising, M. A. Temple and J. A. Jackson, "Authorized and Rogue Device Discrimination Using Dimensionally Reduced RF-DNA Fingerprints," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 6, pp. 1180 - 1192, 5 February 2015.

[53] K. S. Kuciapinski, M. A. Temple and R. W. Klein, "ANOVA-BASED RF DNA Analysis: Identifying Significant Parameters for Device Classification," in *IEEE Proceedings of the International Conference on Wireless Information Networks and Systems (WINSYS)*, 2010.

[54] M. Azizyan, I. Constandache and R. R. Choudhury, "SurroundSense: Mobile Phone Localization via Ambience Fingerprinting," in *Proceedings of the 15th Annual International Conference on Mobile Computing and Networking*, 2009.

[55] R. Clarke, "Human Identification in Information Systems: Management Challenges and Public Policy Issues," *Information Technology & People*, vol. 7, no. 4, pp. 6-37, 1994.

[56] M. R. Endsley and D. J. Garland, Situation Awareness Analysis and Measurement, M. R. Endsley, Ed., Boca Raton, Florida: CRC Press, 2000.

[57] J. D. Tygar, "Dyad: A System Using Physically Secure Co-Processors," Research Showcase, 1991.

[58] R. Khanna, "Systems Engineering for Large-Scale Fingerprint Systems," in *Automatic Fingerprint Recognition Systems*, N. Ratha and R. Bolle, Eds., New York, Springer-Verlag, 2004, pp. 283-304.

[59] Y. Huang, M. S. Pepe and Z. Feng, "Evaluating the Predictiveness of a Continuous Marker," *Biometrics,* vol. 63, pp. 1181-1188, 2007.

[60] M. K. Krishnamoorthy, Statistical Tolerance Regions: Theory, Applications and Computation, Hoboken: John Wiley & Sons, 2009.

[61] T. Fawcett, "ROC Graphs: Notes and Practical Considerations for Researchers," *Machine Learning,* vol. 31, no. 1, pp. 1-38, 2004.

[62] M. Bishop, "Security Policies," in *Computer Security: Art and Science (2 Volume Set) 1st Edition*, 1 ed., vol. 2, Boston, Addison-Wesley, 2003, pp. 95-122.

[63] J. Riggles, *Rotating Constellations of Rx FSK Graph,* Wright Patterson Air Force Base: National Instruments, 2016.

[64] "http://www.ni.com/labview/," [Online].

[65] "http://www.ni.com/pdf/manuals/375868a.pdf," National Instruments, [Online]. Available: http://www.ni.com/pdf/manuals/375868a.pdf. [Accessed 2016].

[66] "http://www.icomamerica.com/en/products/amateur/hf/9100/specifications.aspx," Icom of America. [Online]. [Accessed 2016].

[67] V. Witkovsky, "ToleranceFactor - A MATLAB Algorithm for Computing the Exact Tolerance Factors of the Tolerance Limits For Normal Distributions," MATLAB Central File Exchange, 2009.

[68] U.S. Government Publishing Office, "Electronic Code of Federal Regulations: Title 47 Frequency Allocations and Radio Treaty Matters; General Rules and Regulations," 2017.

[69] R. Santamarta, "A Wake-Up Call for SATCOM Security," IOActive Comphrensive information Security, Seattle, 2014.

[70] D. R. Reising, "Exploitation of RF-DNA For Device Classification and Verification Using GRLVQI Processing," Air University, Wright-Patterson AFB, 2012.

[71] B. Yu and M. P. Singh, "A Social Mechanism of Reputation Management in Electronic Communities," in *Cooperative Information Agents IV - The Future of Information Agents in Cyberspace*, vol. 1860, M. Klusch and L. Kerschberg, Eds., Boston, MA: Springer, 2000, pp. 154-165.

[72] A. Salehi-Abari and T. White, "Towards Con-Resistant Trust Models for Distributed Agent Systems," *Proceedings of the 21st International Joint Conference on Artificial Intelligence (IJCAI)*, pp. 272-277, 2009.

[73] C. M. Shipman, K. M. Hopkinson and J. J. Lopez, "Con-Resistant Trust for Improved Reliability in a Smart-Grid Special Protection System," *IEEE Transactions on Power Delivery*, vol. 30, no. 1, pp. 455-462, 21 January 2015.

[74] J. Sabater, M. Paolucci and R. Conte, "Reputation and Image Among Autonomous Partners," *Journal of Artificial Societies and Social Simulation*, vol. 9, no. 2, 31 Mar 2006.

[75] NIOJ, "Fixed and Base Station FM Receivers," National Institite of Justice, 1988.

[76] C. M. Kozierok, "PPP Core Protocols: Link Control, Network Control, and Authentication," in *The TCP/IP Guide: A Comprehensive, Illustrated Internet Protocols Reference*, San Franscisco, No Starch Press, 2005, pp. 155-165.

[77] Law Enforcement Standards Laboratory of the National Bureau of Standards, "Fixed and Base Station FM Transmitters: NIJ Standard-0201.01," US Department of Justice, 1987.

[78] D. G. Altman, "Statistics Notes: Diagnostic Tests 2: Predictive Values," *BMJ*, vol. 309, no. 102, p. 102, July 1994.

[79] J. Deeks and D. G. Altman, "Diagnostic Tests 4: Likelihood Ratios," *BMJ*, vol. 329, no. 7458, pp. 168-169, 17 July 2004.

[80] H. J. V. D. Helm and E. A. H. Hische, "Application of Bayes's Theorem to Results of Quantitative Clinical Chemical Determinations," *Clinical Chemistry,* vol. 25, no. 6, pp. 985-988, June 1979.

[81] D. G. Abraham and G. P. Double, "Secure Component Authentication System". Patent 4799061, 18 November 1985.

[82] G. J. Simmons, "A Survey of Information Authentication," *Prooceedings of the IEEE*, vol. 76, no. 5, pp. 603-620, May 1988.

[83] "Frequency Modulation (FM) Theory and Simulation," in *Software Defined Radio using MATLAB & Simulink and the RTL-SDR*, 1st ed., Glasgow, Scotland: Strathclyde Academic Media, 2015, pp. 329-366.

[84] H. Vogt, "Airline Passenger Hid Bomb in Laptop, Somali Authorities Say," 8 JFebruary 2016. [Online]. Available: http://www.wsj.com/articles/airline-passenger-hid-bomb-in-laptop-somali-authorities-say-1454954126. [Accessed 8 February 2016].

[85] B. Stewart, K. Barlee, D. Atkinson and L. Crockett, "Frequency Modulation (FM) Theory and Simulation," in *Software Defined Radio using MATLAB & Simulink and the RTL-SDR*, 1st ed., Glasgow, Scotland: Strathclyde Academic Media, 2015, pp. 329-366.

[86] B. Boashash, "Estimating and Interpreting the Instantaneous Frequency of a Signal Part 1: Fundamentals," *Proceedings of the IEEE,* vol. 80, no. 4, pp. 520-538, April 1992.

Index

P2P
Point to Point Network, xx
PHY
Physical Layer 1of OSI, xx
RF
Radio Frequency, xx, 26, 27, 304
RF-DNA
Radio Frequency Distinct Native Attribute, xx, 26, 27, 304
ROC
Receiver Operating Curve, xxi
ROI
Region of Interest, xxi
RRR
Rogue Rejection Rate, xxi
Rx
Receiver, xxi
SATCOM
Satellite Communication, xxi, 24, 27, 304
SHR
Synchronization Header Response, xxi
SN
sequence number, xxi
SNR
Signal to Noise Ratio, xxi
TVR
True Verification Rate, xxi
Tx
Transmitter, xxi
UHF
Ultra High Frequency, xxi

Vita

Major Tyrone A. L. Lewis graduated from Central high school in Springfield Missouri. He joined the Army in 1996 as a Private and was quickly promoted through the ranks to Staff Sergeant in 2001. After being selected for Officer Candidate School, he was commissioned at Fort Benning Georgia in 2002 and recognized as a Distinguished Honor Graduate. He graduated Magna Cum Laude from the University Of Maryland University College in College Park, Maryland with a Bachelor of Science degree in Management Studies in 2004.

In his first assignment as an Ordnance Officer in 2004, Ty led a platoon of 135 Soldiers in the direct support maintenance of M1A1 and M1A2 tanks for 3 Corps Field Artillery, and was recognized for integrating disparate logistical systems which corrected a two year inventory deficiency and reduced maintenance back log by over 30% as the Maintenance Control Officer. He graduated from the Army's Telecommunications Systems Engineer Course in 2006, and deployed to Iraq as the junior network engineer for 3rd Infantry Division during the *surge*. His highest award, The Bronze Star, was received for his engineering contributions to include a fiber-based communications infrastructure design for enduring forward operating base Delta. He received the Rowan Award for his design and demonstration of Fort Gordon Georgia's Installation-wide Signal Training Network in 2010. He was promoted below the zone to Major in 2011. In August 2015, received his master's degree in Computer Science at the Air Force Institute of Technology (AFIT). Upon graduation, he plans to continue discovering, understanding and making contributions.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From – To)*
14-09-2017	DISSERTATION	September 2014 – September 2017

TITLE AND SUBTITLE
Biologically Inspired Network (BiONet) Authentication using Logical and Pathological RF-DNA Credential Pairs

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Lewis, Tyrone A.L. Sr., Major, USA

5d. PROJECT NUMBER
17G213

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S)
Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
2950 Hobson Way
WPAFB OH 45433-8865

8. PERFORMING ORGANIZATION REPORT NUMBER
AFIT-ENG-DS-17-S-012

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
AIR FORCE RESEARCH LABORATORY
ATTN: Michael Gudaitis
525 BROOKS RD
Rome Lab AFB, NY 13441
Phone: (315)-330-44, Email: michael.gudaitis@us.af.mil

10. SPONSOR/MONITOR'S ACRONYM(S)
AFRL/RITE

11. SPONSOR/MONITOR'S REPORT NUMBER(S):

12. DISTRIBUTION/AVAILABILITY STATEMENT
DISTRUBTION STATEMENT A. APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

13. SUPPLEMENTARY NOTES
This material is declared a work of the U.S. Government and is not subject to copyright protection in the United States.

14. ABSTRACT

The command and control (C2) of shared space resources are vulnerable to logical credential forgery and impersonation attacks among standardized and interoperable wireless radio frequency (RF) networks. Threats could come from trusted operators (insiders) or from external sources (outsiders). An attacker may gain unauthorized network access and illegally cross into C2 boundaries when conventional network authentication fails. This research proposes an integrated trust management system that uses both application-layer and physical-layer trust markers to authenticate users and their communication sources. In essence, the results from physical-layer RF-DNA fingerprinting techniques are used to improve application-level trust schemes based on command patterns, message structure, and other discernible markers through the use of Bayesian reasoning using an approach adapted from the medical disease diagnostic testing community. In this adapted approach, trust markers of behavior can be used to detect deviations from what is expected, sometimes called byzantine behavior. Suspect communication or traffic patterns are labeled as $eNDs$ (electronic network-diseases). Trust management enabled devices consider the diagnostics of logical and pathological RF-DNA credential pairs and application-layer trust markers to predict and mitigate such $eNDs$. The method introduced in this dissertation demonstrates an end-to-end physical RF network prototype; introduces a tracking capability for multi-organizational access, and improves upon the accuracy of credential pair identification using either physical-layer or application-layer techniques in isolation. In the experiments run, the discrimination of insider vs. outsider threats improved by 22%, uplink availability was extended by 51.2% for non-offenders, and the proposed trust system achieved 100% posterior predictions using moderate tolerance settings. The trust system also reduced logical credential forgery acceptance by 84% among tested samples. The system shows promise for more general application in domains including Cyber, Space and eHealth ecosystems.

15. SUBJECT TERMS
(cyberattack, diagnostics, authentication, electronic network-disease, RF-DNA, RF fingerprint, RF-biomarker)

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Dr. Kenneth M. Hopkinson, AFIT/ENG
U	U	U	UU	299	19b. TELEPHONE NUMBER *(Include area code)* (937) 255-6565, ext. 6195 (Kenneth.m.hopkinson@afit.edu)

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39-18