REPORT DOCUMENTATION PAGE

Form Approved OMB NO. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (From - To)
28-02-2023	Final Report	15-Apr-2017 - 14-May-2019

4. TITLE AND SUBTITLE
Final Report: Infrastructure for Securing Dynamic Tactical MANETs Research and Education

5a. CONTRACT NUMBER
W911NF-17-1-0178

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER
611103

6. AUTHORS

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES AND ADDRESSES
Stevens Institute of Technology
1 Castle Point on Hudson

Hoboken, NJ 07030 -5991

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS (ES)
U.S. Army Research Office
P.O. Box 12211
Research Triangle Park, NC 27709-2211

10. SPONSOR/MONITOR'S ACRONYM(S)
ARO

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
69996-NC-RIP.1

12. DISTRIBUTION AVAILIBILITY STATEMENT
2 Approved for public release; distribution is unlimited

13. SUPPLEMENTARY NOTES
The views, opinions and/or findings contained in this report are those of the author(s) and should not contrued as an official Department of the Army position, policy or decision, unless so designated by other documentation.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	15. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Yingying Chen
UU	UU	UU	UU		19b. TELEPHONE NUMBER 201-216-8066

RPPR

as of 02-Mar-2023

Agency Code:

Proposal Number: **Agreement Number:**

Organization:
Address: , ,
Country:
DUNS Number: EIN:
Report Date: Date Received:
for Period Beginning and Ending
Title:
Begin Performance Period: **End Performance Period:**
Report Term: -
Submitted By: Email:
Phone:

Distribution Statement: -

STEM Degrees: **STEM Participants:**

Major Goals:

Accomplishments:

Training Opportunities:

Results Dissemination:

Plans Next Period:

Honors and Awards:

Protocol Activity Status:

Technology Transfer:

I certify that the information in the report is complete and accurate:
Signature:
Signature Date:

Final Report

Proposal No. 69996-NC-RIP - Infrastructure for Securing Dynamic Tactical MANETs Research and Education

Agreement Number W911NF-17-1-0178

Major Goals:

This project aims to build an infrastructure that measures, tests, and evaluates various practical parameters when validating existing and new security- oriented research problems in mission-critical tasks under real environments. It targets to bridge the gap between theoretic study and system implementation and further provide valuable performance evaluation feedback to enhance the theoretic study in Army's future wireless systems.

Accomplished:

The project was focused in the following aspects:

With the ubiquitous employment of WiFi technology, almost every electronics in indoor environments (such as access points, laptops, and smart TV) are interconnected wirelessly. The WiFi signals generated by the devices reflected, refracted, and diffracted from objects and human subjects in the room environment, and the channel state information (CSI) of the WiFi signals can capture unique characteristics of the objects and subjects, which can be leveraged for various remote and device-free sensing applications. In this project, we built an 802.11n WiFi infrastructure to comprehensively investigate practical WiFi sensing (i.e., user authentication and in-baggage object identification) and impacting factors in real-world indoor scenarios. The infrastructure includes (1) Dell E6430 laptops equipped with 802.11n 5300 WiFi network interface cards as transmitters and receivers. The laptops run Ubuntu 14.04 operating system with the 4.2.0 kernel for extracting CSI from the Intel 5300 NIC over 30 subcarrier groups (i.e., 1~2 subcarriers per group). (2) TP-link N750 access points as transmitters and receivers. The Qualcomm Atheros WiFi QCA9344 system-on-chip (SoC) allows extracting CS from 56 subcarriers. (3) Aaronia HyperLOG 7060 directional antennas and embedded antennas of laptops/access points to send WiFi signals. The directional antennas can transmit polarized WiFi signals that are more sensitive to materials of different types. (4) We use a Dell desktop as the server connected to all the laptops and access points to collect CSI. The desktop is equipped with a high-end GPU (NVIDIA Quadro) for extracting CSI, conducting signal processing, and performing machine learning. Based on the infrastructure, we investigate two critical WiFi sensing applications: device-free user authentication and in-baggage object identification.

User authentication is a critical process in both corporate and home environments due to the ever-growing security and privacy concerns. With the advancement of smart cities and home environments, the concept of user authentication is evolved with a broader implication by not only preventing unauthorized users from accessing confidential information but also providing opportunities for customized services corresponding to a specific user. Traditional approaches to user authentication either require specialized device installation or inconvenient wearable sensor attachment. In this project, we aim to support the extended concept of user authentication by developing a device-free approach based on the designed WiFi infrastructure. We designed a

system that utilizes WiFi signals to capture unique human physiological and behavioral characteristics inherited from their daily activities. Particularly, we extract representative features from both amplitude and relative phase of CSI measurements in WiFi signals, which have the potential to reveal unique characteristics of different users. In addition, a three-layer deep neural network model is developed to learn high-level abstractions of human physiological and behavioral characteristics for both activity recognition and human identification. We conducted extensive experiments involving 11 subjects for testing accessing restricted areas and operating risky appliances. A total of 8 walking activities and 8 stationary activities (30 rounds for each) are performed by 11 and 5 volunteers in these two indoor environments, respectively. In total, we collected 3,336 activity segments performed by 11 subjects in the office environment, and 834 activity segments performed by 5 subjects in the apartment. Our system can achieve over 94% and 91% authentication accuracy through walking and stationary activities, respectively.

Furthermore, the growing needs of public safety urgently require scalable and low-cost techniques on detecting dangerous objects (e.g., lethal weapons, homemade-bombs, explosive chemicals) hidden in baggage. Traditional baggage check involves either high manpower for manual examinations or expensive and specialized instruments, such as X-ray and CT. As such, many public places (i.e., museums and schools) that lack of strict security check are exposed to high risk. In this project, we propose to utilize the CSI of WiFi signals to detect suspicious objects that are suspected to be dangerous (i.e., defined as any metal and liquid object) without penetrating into the user's privacy through physically opening the baggage. Our suspicious object detection system significantly reduces the deployment cost and is easy to set up in public venues. Towards this end, our system is realized by two major components: it first detects the existence of suspicious objects and identifies the dangerous material type based on the reconstructed CSI complex value (including both amplitude and phase information); it then determines the risk level of the object by examining the object's dimension (i.e., liquid volume and metal object's shape) based on the reconstructed CSI complex of the signals reflected by the object. We evaluate our system with the combination of 15 different target objects in three categories (i.e., metal, liquid and non-dangerous) and 6 representative bags/boxes in three categories (i.e., backpack/handbag, cardboard boxes, thick plastic bag). For the material identification, we put each of the 15 objects in 6 bags/boxes respectively and experiment. Each experiment is repeated 5 times while slightly changing the object's position and orientation. For dangerous object risk level estimation, we place the metal objects across multiple positions to estimate the size (i.e. width and height). Moreover, we have three different size containers (i.e., large, medium and small) filled with different volumes of liquid to estimate liquid volume. Overall, over 800 experimental data traces are collected to evaluate our proposed system. The results show that our system can detect over 95% suspicious objects in different types of bags and successfully identify 90% dangerous material types. In addition, our system can achieve the average errors of 16ml and 0.5cm when estimating the volume of liquid and shape (i.e., width and height) of metal objects, respectively.

Training

The WiFi communication and sensing infrastructure developed in this project has been used in the course projects for a cross listed (between graduate and senior undergraduate) course of Principles on Mobile Embedded Systems.

Dissemination

Two papers are published during this reporting period:

Shi, Cong; Liu, Jian; Liu, Hongbo; Chen, Yingying. “Smart User Authentication through Actuation of Daily Activities Leveraging WiFi-enabled IoT”. Proceedings of the 18th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc 2017), Chennai, India, July 2017. DOI: 10.1145/3084041.3084061.

Wang, Chen; Liu, Jian; Chen, Yingying; Liu, Hongbo; Wang, Yan. “Towards In-baggage Suspicious Object Detection Using Commodity WiFi”. Proceedings of IEEE International Communications and Network Security (CNS 2018), Beijing, China, May/June 2018. DOI: 10.1109/CNS.2018.8433142.

Honors

None.

Tech Transfer

Not yet.

Participants

Yingying Chen from Rutgers University is the PI working on this project. Yu-Dong Yao from Stevens Institute of Technology is the Co-PI working on this project. When this project was funded. Yingying Chen was with Stevens Institute of Technology.