REPORT DOCUMENTATION PAGE

Form Approved OMB NO. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (From - To)
21-10-2017	Final Report	1-Aug-2014 - 31-Jul-2017

4. TITLE AND SUBTITLE
Final Report: Broadband and High-power Reactive Jamming Resilient Wireless Communication

5a. CONTRACT NUMBER
W911NF-14-1-0324

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER
611102

6. AUTHORS

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES AND ADDRESSES
University of South Florida
3650 Spectrum Blvd
Suite 160
Tampa, FL 33612 -9446

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)
64965-CS.6

12. DISTRIBUTION AVAILIBILITY STATEMENT
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			Yao Liu
UU	UU	UU	UU		19b. TELEPHONE NUMBER 813-974-1079

RPPR Final Report
as of 17-Nov-2017

Agency Code:

Proposal Number: 64965CS **Agreement Number: W911NF-14-1-0324**
INVESTIGATOR(S):

Name: Yao Liu
Email: yliu@cse.usf.edu
Phone Number: 8139741079
Principal: Y

Organization: **University of South Florida**
Address: 3650 Spectrum Blvd, Tampa, FL 336129446
Country: USA
DUNS Number: 069687242 EIN: 593102112
Report Date: 31-Oct-2017 Date Received: 21-Oct-2017
Final Report for Period Beginning 01-Aug-2014 and Ending 31-Jul-2017
Title: Broadband and High-power Reactive Jamming Resilient Wireless Communication
Begin Performance Period: 01-Aug-2014 **End Performance Period:** 31-Jul-2017
Report Term: 0-Other
Submitted By: Yao Liu Email: yliu@cse.usf.edu
Phone: (813) 974-1079
Distribution Statement: 1-Approved for public release; distribution is unlimited.

STEM Degrees: **STEM Participants:**

Major Goals: Jamming attacks are well-known threats to wireless communications. Frequency Hopping Spread Spectrum (FHSS) and Direct Sequence Spread Spectrum (DSSS) are dominantly used for anti-jamming purposes. Although both techniques were developed more than 30 years ago, until now they and their variants have been limited by a common assumption that the jammer can jam only part of the communication channels or has a limited transmit power. Unfortunately, if the jammer is broadband or has a high transmit power, they fail to provide anti-jamming communication.

However, when the broadband and high-power jammer adopts a reactive jamming strategy, a closer examination on the reactive behavior reveals the “Achilles Heel” of such attackers. Reactive jamming is among the most effective jamming attacks. Compared to constant jamming, reactive jamming is more difficult to track and is much more energy-efficient. To be reactive, a reactive jammer stays quiet when the channel is idle, but starts transmitting a radio signal as soon as it senses activity on the channel. Therefore, before the jamming signal arrives, the sender may have already sent several bits. This observation provides insights on designing countermeasures to deal with broadband and high-power reactive jammers. It is easy for people to conceive that a receiver may collect information bits from unjammed parts of received packets and try to assemble these bits together to obtain a message. However, significant technical challenges exist to prevent this intuition from being transformed into a real-world realization.

To use the unjammed bits survived in the jammer’s reaction time to establish jamming-resilient communications, a receiver should have the following essential capabilities. First, the receiver should be able to extract unjammed bits from a received bit stream. Second, the receiver should be able to identify the correct positions of received unjammed bits in an original message. Finally, the receiver should be able to deal with potential fake bits injected by an intelligent reactive jammer. This project aims to create comprehensive techniques that solve the major challenges in
designing these essential capabilities.

Accomplishments: 1) major activities;

The PI has conducted the following research activities: (1) create universal jamming detection techniques that can distinguish between jammed and unjammed bits; (2) create bit synchronization techniques that allow a receiver to identify the correct positions of received unjammed bits and to recover from synchronization errors; and (3) design defense techniques that can address pollution attacks in a secure way.

2) specific objectives;

The objective of this project is to create comprehensive techniques that solve the major challenges in using the unjammed bits survived in the reaction time of a reactive jammer to establish the anti-jamming communication.

3) significant results, including major findings, developments, or conclusions (both positive and negative)

The major discoveries include:

a. It is possible to raise wireless communication from non-existence to being available in extremely hostile environments, where FHSS and DSSS are completely defeated by a broadband and high-power reactive jammer.

b. Wireless physical layer features can be explored to generate a shared key or securely deliver a key to a desired receiver to facilitate the anti-jamming techniques.

c. New anti-jamming techniques can be created to remove the requirement of a shared secret key.

4) key outcomes or other achievements

The following techniques have been developed

1. Jamming detection method that uses physical layer modulation properties to identify unjammed bits.

2. Bit synchronization techniques that enable the receiver to find the original positions of received unjammed bits in the original message.

3. Techniques that enable the use of a shared secret key between the sender and the receiver to combat pollution attacks.

4. A fast friendly jamming technique that eliminates the need for demodulation and enables the friendly jammer to verify the received signals directly on the physical layer. This technique can further enhance the accuracy of jamming detection since the friendly jamming signal makes the difference between jammed and unjammed signals more notable.

5. A novel wireless technique named pinpoint waveforming to achieve the location-restricted service access control, i.e., providing wireless services to users at eligible locations only. This technique uses coherent jamming to obtain constructive interference, which can help to send messages in a confidential way. This technique can be used to establish a shared key between a sender and a receiver so as to facilitate the defense against pollution attacks.

6. A novel wireless key establishment technique between a transmitter and receiver pair in the presence of an eavesdropper. This technique enables the transmitter to specify any content as the secret key and removes the reconciliation
process, which is necessary in conventional wireless key establishments.

7. A new anti-jamming scheme named Randomized Positioning DSSS (RP-DSSS) scheme that does not require the sender and receiver to pre-establish a shred key. It randomly relocates the spreading codes information for each message, and thus achieves the enhanced security than the traditional DSSS based schemes.

Training Opportunities: Nothing to Report

Results Dissemination: The PI attended mainstream computer conferences to disseminate the research results. These conferences include IEEE CNS, IEEE INFOCOM, and ACM CCS. The PI also submitted the research results to multiple publication venues, including IEEE Transactions on Dependable and Secure Computing, ACM CCS, IEEE CNS, IEEE ICNC.

RPPR Final Report
as of 17-Nov-2017

Honors and Awards: 1. University of South Florida Outstanding Faculty Achievement Award, 2017.

2. USENIX Security'17 Grant for Women by Google, 2017.

3. University of South Florida Outstanding Faculty Award, 2017.

4. College of Engineering Outstanding Junior Research Achievement Award, 2016.

5. National Science Foundation Faculty Early Career Development (CAREER) award, 2016.

6. Faculty Research Fellow of Air Force Research Lab, 2015.

Protocol Activity Status:

Technology Transfer: Nothing to Report

PARTICIPANTS:

Participant Type: PD/PI
Participant: Yao Liu
Person Months Worked: 3.00 **Funding Support:**
Project Contribution:
International Collaboration:
International Travel:
National Academy Member: N
Other Collaborators:

Participant Type: Graduate Student (research assistant)
Participant: Song Fang
Person Months Worked: 3.00 **Funding Support:**
Project Contribution:
International Collaboration:
International Travel:
National Academy Member: N
Other Collaborators:

Participant Type: Graduate Student (research assistant)
Participant: Tao Wang
Person Months Worked: 3.00 **Funding Support:**
Project Contribution:
International Collaboration:
International Travel:
National Academy Member: N
Other Collaborators:

Participant Type: Graduate Student (research assistant)
Participant: Ian Markwood
Person Months Worked: 3.00 **Funding Support:**
Project Contribution:
International Collaboration:
International Travel:
National Academy Member: N
Other Collaborators:

Participant Type: Graduate Student (research assistant)

RPPR Final Report
as of 17-Nov-2017

Participant: Ian Markwood
Person Months Worked: 3.00 **Funding Support:**
Project Contribution:
International Collaboration:
International Travel:
National Academy Member: N
Other Collaborators:

Participant Type: Graduate Student (research assistant)
Participant: Ahmad Alagil
Person Months Worked: 3.00 **Funding Support:**
Project Contribution:
International Collaboration:
International Travel:
National Academy Member: N
Other Collaborators:

ARTICLES:

Publication Type: Journal Article Peer Reviewed: Y **Publication Status:** 5-Submitted
Journal: IEEE Transactions on Dependable and Secure Computing
Publication Identifier Type: DOI Publication Identifier: 10.1109/TDSC.2015.2399304
Volume: 0 Issue: 0 First Page #: 0
Date Submitted: Date Published:
Publication Location:
Article Title: Wireless Communications under Broadband Reactive Jamming Attacks
Authors:
Keywords: Wireless Communication, Jamming Attacks, Reactive Jammer, Broadband
Abstract: A reactive jammer jams wireless channels only when target devices are transmitting; Compared to constant jamming, reactive jamming is harder to track and compensate against [2], [41]. Frequency Hopping Spread Spectrum (FHSS) and Direct Sequence Spread Spectrum (DSSS) have been widely used as countermeasures against jamming attacks. However, both will fail if the jammer jams all frequency channels or has high transmit power. In this paper, we propose an anti-jamming communication system that allows communication in the presence of a broadband and high power reactive jammer. The proposed system transmits messages by harnessing the reaction time of a reactive jammer. It does not assume a reactive jammer with limited spectrum coverage and transmit power, and thus can be used in scenarios where traditional approaches fail. We develop a prototype of the proposed system using GNURadio. Our experimental evaluation shows that when a powerful reactive jammer is presence, the prototype still keep

Acknowledged Federal Support:

RPPR Final Report
as of 17-Nov-2017

Publication Type: Journal Article Peer Reviewed: Y **Publication Status:** 1-Published
Journal: IEEE Transactions on Dependable and Secure Computing
Publication Identifier Type: DOI Publication Identifier: 10.1109/TDSC.2015.2399304
Volume: 0 Issue: 99 First Page #: 0
Date Submitted: Date Published:
Publication Location:
Article Title: Wireless Communications under Broadband Reactive Jamming Attacks
Authors:
Keywords: Wireless Communication, Jamming Attacks, Reactive Jammer, Broadband
Abstract: A reactive jammer jams wireless channels only when target devices are transmitting; Compared to constant jamming, reactive jamming is harder to track and compensate against [2], [38]. Frequency Hopping Spread Spectrum (FHSS) and Direct Sequence Spread Spectrum (DSSS) have been widely used as countermeasures against jamming attacks. However, both will fail if the jammer jams all frequency channels or has high transmit power. In this paper, we propose an anti-jamming communication system that allows communication in the presence of a broadband and high power reactive jammer. The proposed system transmits messages by harnessing the reaction time of a reactive jammer. It does not assume a reactive jammer with limited spectrum coverage and transmit power, and thus can be used in scenarios where traditional approaches fail. We develop a prototype of the proposed system using GNURadio. Our experimental evaluation shows that when a powerful reactive jammer is present, the prototype still keeps
Distribution Statement: 1-Approved for public release; distribution is unlimited.
Acknowledged Federal Support:

CONFERENCE PAPERS:

Publication Type: Conference Paper or Presentation **Publication Status:** 1-Published
Conference Name: 2016 International Conference on Computing, Networking and Communications (ICNC)
Date Received: 26-Jul-2016 Conference Date: 15-Feb-2016 Date Published: 16-Feb-2016
Conference Location: Kauai, HI, USA
Paper Title: Randomized positioning DSSS for anti-jamming wireless communications
Authors: Ahmad Alagil, Meshari Alotaibi, Yao Liu
Acknowledged Federal Support: **Y**

Publication Type: Conference Paper or Presentation **Publication Status:** 1-Published
Conference Name: MILCOM 2015 - 2015 IEEE Military Communications Conference
Date Received: 26-Jul-2016 Conference Date: 26-Oct-2015 Date Published: 26-Oct-2015
Conference Location: Tampa, FL, USA
Paper Title: No time to demodulate - fast physical layer verification of friendly jamming
Authors: Shen, Wenbo; Liu, Yao; He, Xiaofan; Dai, Huaiyu Dai; and Ning, Peng
Acknowledged Federal Support: **Y**

Publication Type: Conference Paper or Presentation **Publication Status:** 1-Published
Conference Name: the 22nd ACM SIGSAC Conference
Date Received: 26-Jul-2016 Conference Date: 12-Oct-2015 Date Published: 12-Oct-2015
Conference Location: Denver, Colorado, USA
Paper Title: Location-restricted Services Access Control Leveraging Pinpoint Waveforming
Authors: Wang, Tao; Liu, Yao; Pei, Qingqi; and Hou,Tao
Acknowledged Federal Support: **Y**

RPPR Final Report
as of 17-Nov-2017

Nothing to report in the uploaded pdf (see accomplishments)