REPORT DOCUMENTATION PAGE

Form Approved OMB NO. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (From - To)
19-01-2023	Final Report	25-Dec-2018 - 30-Sep-2022

4. TITLE AND SUBTITLE
Final Report: In-band Wireless Trust Establishment Resistant to Advanced Signal Manipulations

5a. CONTRACT NUMBER
W911NF-19-1-0050

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER
611102
611104

6. AUTHORS

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES AND ADDRESSES
University of Arizona
PO Box 210158, Rm 510

Tucson, AZ 85721 -0158

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)
72603-NC-H.14

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			Ming Li
UU	UU	UU	UU		19b. TELEPHONE NUMBER 520-621-6191

RPPR Final Report
as of 27-Jan-2023

Agency Code: 21XD

Proposal Number: 72603NCH **Agreement Number: W911NF-19-1-0050**
INVESTIGATOR(S):

Name: Ming Li
Email: ming.li@arizona.edu
Phone Number: 5206216191
Principal: Y

Organization: **University of Arizona**
Address: PO Box 210158, Rm 510, Tucson, AZ 857210158
Country: USA

DUNS Number: 806345617 EIN: 866004791
Report Date: 31-Dec-2022 Date Received: 19-Jan-2023
Final Report for Period Beginning 25-Dec-2018 and Ending 30-Sep-2022
Title: In-band Wireless Trust Establishment Resistant to Advanced Signal Manipulations
Begin Performance Period: 25-Dec-2018 **End Performance Period:** 30-Sep-2022
Report Term: 0-Other

Submitted By: Ming Li Email: ming.li@arizona.edu
Phone: (520) 621-6191

Distribution Statement: 1-Approved for public release; distribution is unlimited.

STEM Degrees: 2 **STEM Participants:** 6

Major Goals: This project studies novel trust establishment mechanisms among wireless devices without any prior secrets that are resistant against advanced signal manipulations, merely using wireless in-band transmissions. The main goals are three-fold:

(1) Message integrity verification and authentication under active signal manipulation. We propose to verify message integrity via detecting the presence of signal cancellation attacks, by exploiting helper's co-presence with the device. We also propose novel channel randomization methods that prevent an attacker from accurately predicting the channel and exploit the real-time nature of the attack to thwart signal cancellation attacks.

(2) Modulation-agnostic secure trust establishment. We further propose a set of message integrity and authentication primitives, without any modification to the device's signal format or firmware. Our approach exploits RSS ratio fluctuation patterns and leverages its correlation with random helper motions to prevent signal cancellation.

(3) Group device pairing resistant against signal manipulation. We propose novel primitives to verify the integrity of messages transmitted among a group of devices, that harden signal cancellation via exploiting simultaneous verification from multiple devices including the helper.

Tasks and schedule:

Task 1: Infeasibility of Online Device Differentiation. Target date: end of Q4, Year 1; Actual completion dates: 100% completed; end of Q4.

Task 2: Achieving Mutual Integrity Protection. Target date: end of Q4, Year 1; Actual completion dates: 100% completed; end of Q4.

Task 3: Optimal Antenna Mode Subset Selection. Target date: end of Q2, Year 2; Actual completion dates: 100% completed; end of Q4.

Task 4: Ensuring Compatibility with COTS Devices. Target date: end of Q2, Year 3; Percentage of completion: 100% completed; end of Q4;

Task 5: Exploiting Artificial Random Motions. Target date: end of Q4, Year 3; Percentage of completion: 100%

completed; end of Q4;

Task 6: (In)feasibility of Active Signal Manipulations. Target date: end of Q4, Year 1; Actual completion dates: 100% completed; end of Q4.

Task 7: Exploiting Helper's Motions. Target date: end of Q2, Year 2; Percentage of completion: 100% completed; end of Q4.

Task 8: Reliable Authentication Under Varying Channel Conditions. Target date: end of Q2, Year 3; Percentage of completion: 100% completed; end of Q4.

Task 9: Simultaneous Integrity Verification of All Messages in a Group. Target date: end of Q4, Year 2; Actual completion dates: 100% completed; end of Q4.

Task 10: Exploiting Multiple Verifiers for Enhanced Integrity Verification. Target date: end of Q4, Year 3; Percentage of completion: 100% completed; end of Q4.

Task 11: Detecting Signal Manipulation in a Group Setting. Target date: end of Q4, Year 3; Percentage of completion: 100% completed; end of Q4.

Task 12: Helper Motions in a Group Setting. Target date: end of Q4, Year 3; Percentage of completion: 100% completed; end of Q4.

Accomplishments: Significant results from this project are summarized as follows:

Thrust 1: Message integrity assurance under active signal manipulations

1) Man-in-the-Middle (MitM) resistant secret key agreement using reconfigurable antennas.
Physical-layer key agreement schemes exploit channel randomness and reciprocity for secret key extraction and can achieve information-theoretic secrecy. However, they are also vulnerable to the MitM attack, where an active adversary identifies packet injection opportunities that allow it to successfully influence and extract part of the secret key. To prevent such attacks, we propose to utilize a reconfigurable antenna at the transmitter side to proactively randomize the channel state for different received signal strength (RSS) probing rounds. As a result, the temporal channel correlation observed by the adversary over one round cannot be exploited by the adversary in subsequent rounds. We formally analyze the security of our proposed scheme, and conduct simulations and USRP experiments to validate its security, and evaluate its performance. Results show that our method can reduce the active adversary's success probability to nearly a random guess.

2) Helper-aided channel randomization using reconfigurable antennas.
The above protocol requires additional hardware which may not be standard equipment. Thus, we have developed a new method that employs a helper device equipped with an RA and randomizes the channel. The main idea is that COTS devices can exchange messages and protect the message integrity with the assistance of the helper who is used to relay message digests between the transmitter and receiver. The transmissions from Tx to the helper relay and to the Rx use normal modulation modes, while the helper-to-RX channel uses ON-OFF keying to prevent advanced signal manipulation attacks. The received message from the main channel is compared with the relayed message digest to detect any modification. We theoretically analyzed the probability of symbol flipping attacks for the Tx-to-helper channel and found it to be close to uniform when the helper randomly chooses its receiving antenna modes. Simulations have been conducted and we will experimentally validate the scheme's security on our USRP platform.

Thrust 2: Modulation-agnostic secure trust establishment

1) Secret-free in-band trust establishment for COTS wireless devices
We have developed SFIRE, a novel pairing method for COTS devices that do not require the pre-sharing of any secrets. The method uses PHY-layer attributes to verify the integrity of the communications between two parties and detect active signal manipulation attacks. We introduced the helper paradigm where security is aided by a special device called "the helper", which is responsible for proving the integrity of over-the-air transmissions for devices. Its security relies on a novel "RSS authenticator" that exploits physical signal propagation laws and helper motion to thwart attackers. We used SFIRE to construct a secure in-band pairing protocol based on the Diffie-

Hellman key agreement. Our pairing method does not rely on the so-called “channel advantage” to guarantee the secrecy of the communication and does not require any hardware/firmware modifications or special transmission modes for the device. We enhanced one of the authentication tests to defend against advanced MitM attacks and carried out theoretical analysis and experiments.

2) PHY-layer-based vehicle authentication and motion-claim verification

The security and resilience of cyber-physical systems hinge on creating an authentic virtual representation of the physical world. However, cryptographic primitives cannot bind the sender with his physical attributes such as location/proximity, velocity, time, trajectory, etc. We addressed this problem in the context of connected autonomous vehicles, under the vehicle platooning application. Our work aims to verify whether a new vehicle is truly part of the platoon as it claims. The high-level idea is to verify that vehicles in the same vicinity ``see'' (sense) the same physical environment. We exploited the large-scale fading effect of ambient LTE signals to verify that V2V messages originate from a valid platooning vehicle. Using the RF correlation property, we developed a Proof-of-Following protocol where the prover provides ambient RF samples to the verifier to prove it is following within a certain reference distance (e.g., less than 50m). We performed extensive experiments on a highway and a city environment to validate the security of our method.

The RF correlation-based method cannot verify more fine-grained physical attributes such as relative positioning between vehicles, traveling in the same lane, etc. To address these limitations, we developed a novel physical challenge-response position verification protocol called Wiggle where the verifier vehicle challenges a prover to prove its physical position. After authenticating the prover using cryptographic methods, the verifier challenges the prover to perform a series of random perturbations of its position. The verifier measures those perturbations (using another sensing modality) to bind the prover's digital identity with its physical trajectory.

Finally, we also developed a general motion-claim verification method for connected vehicles with a single verifier, using opportunistic multi-path reflections in the environment to create multiple virtual verifiers. It can verify the location and velocity of a vehicle, by checking the consistency of angle-of-arrival and frequency-of-arrival on each path. We performed experiments using a two-vehicle testbed on a campus street, and results show that reasonable localization accuracy can be achieved.

3) Zero-effort two-factor authentication systems.

We studied the problem of two-factor authentication, with the goal of minimizing user effort and enhancing security against device compromise. We developed a zero-effort two-factor authentication protocol, which does not require input from the user. Our methods exploit the continuous co-presence of the user's primary device (a login device such as a laptop or a desktop) and a secondary device (e.g., a smartphone) to automatically generate ``proximity traces.'' Such traces verify the proximity of the login device with a second user device for prolonged periods of time. Due to the continuous nature of the verification, our method does not suffer from known attacks of one-time passwords such as shoulder surfing. Moreover, our protocol is able to automatically recover trust after total secret exposure (e.g., due to the compromise of a password database) without manual re-initialization.

Thrust 3: Group device pairing resistant to active signal manipulations

We address the fundamental problem of securely bootstrapping a group of wireless devices to a hub when none of them share prior secrets with the hub. This scenario aligns with the secure deployment of body area networks, IoT, medical devices, industrial automation sensors, autonomous vehicles, and others. We developed VERSE, a physical-layer group message integrity verification primitive that effectively detects advanced wireless signal manipulations (e.g., MitM attacks). VERSE exploits the existence of multiple devices to verify the integrity of the messages exchanged within the group. We then use VERSE to build a bootstrapping protocol, which securely introduces new devices to the network. Compared to the state-of-the-art, VERSE achieves in-band message integrity verification during secure pairing using only the RF modality without relying on out-of-band channels or extensive human involvement. We study the limits of such advanced wireless attacks and prove that the introduction of multiple legitimate devices can be leveraged to increase the security of the pairing process. We validate our claims via theoretical analysis and extensive experimentation on the USRP platform.

RPPR Final Report
as of 27-Jan-2023

Training Opportunities:
Resources from this project have been used to train and support part four Ph.D. students. The Ph.D. students have been mentored by the PIs in conducting research and have also attended conferences where they have made paper presentations. This exposure has led to significant growth and networking opportunities. Two of the Ph.D. students supported under this award have joined academia as tenure-track assistant professors (in R1 schools) after graduation.

Moreover, results from this project have been integrated into the undergraduate/graduate curriculum at UA in the courses taught by the PIs. For example, PI Li taught the grad-level course “Advanced Topics in Information and Network Security” in Fall of 2020, which is a seminar-type course focusing on advanced cryptographic concepts and wireless/mobile security (8 graduate students registered). Several course projects on wireless security related to this award were assigned and completed by three different teams. This has provided training opportunities for graduate students attending the courses.

In addition, in the Summer of 2021, PI Li and PI Lazos hosted five apprenticeship students for the Army Educational Outreach Program (AEOP)’s Undergraduate Research Apprentice Program/High School Apprentice Program (two undergrads and three high school students), supervising them in two hands-on research projects related to this award. The first project related to secure platooning whereas the second project was on secret-free trust establishment in wireless IoT devices. The students attended a week of short courses (joint with two other ongoing REU projects) on wireless communications, information and network security, machine learning, methods of literature review and research, Latex, and Matlab. The students were also trained to conduct testbed experiments with hardware/software tools like USRP, Matlab, and Labview. The training was supported by three Ph.D. students working on this project who served as day-to-day mentors for the AEOP students. Weekly meetings were held for the whole group to discuss progress and for problem-solving. As part of the daily routine, the AEOP students thought about the design of the approach, discussed ideas with mentors, carried out implementation and experiments on real-world testbeds such as vehicles, routers, and USRPs, and analyzed the data collected, based on which they refined the design and summarized the results. As a result, the AEOP students gained hands-on experience and learned how to do research in an authentic lab environment, and the mentors gained experience in mentoring other students.

RPPR Final Report
as of 27-Jan-2023

Results Dissemination:
The outcomes of this research have been disseminated to communities in the following ways.

- Publications in top international conferences and high-impact IEEE journals.
- Presentations at international conferences, research meetings, and university seminars.
- Integration in the curriculum of several courses (Fundamentals of Computer Networks, Fundamentals of Information and Network Security)
- Publishing of the results on the PI and Co-PI websites.

List of Publications:

[1] Ziqi Xu, Jingcheng Li, Yanjun Pan, Loukas Lazos, Ming Li, and Nirnimesh Ghose, “PoF: Proof-of-following for vehicle platoons,” in The 29th Network and Distributed System Security Symposium (NDSS 2022), pp. 1–18, 2022.

[2] Connor Dickey, Christopher Smith, Quentin Johnson, Jingcheng Li, Ziqi Xu, Loukas Lazos, and Ming Li, "Wiggle: Physical Challenge-Response Verification of Vehicle Platooning," 2023 International Conference on Computing, Networking and Communications (ICNC), Honolulu, HI, Feb. 2023.

[3] Nirnimesh Ghose, Kaustubh Gupta, Loukas Lazos, Ming Li, Ziqi Xu, Jingcheng Li, "ZITA: Zero-Interaction Two-Factor Authentication using Contact Traces and In-band Proximity Verification", under revision, IEEE TMC.

[4] Nirnimesh Ghose, Loukas Lazos, and Ming Li, "In-band Secret-Free Pairing for COTS Wireless Devices", IEEE Transactions on Mobile Computing (TMC, pages 618 – 628, Vol. 21, No. 2, 2020, DOI: 10.1109/TMC. 2020.3015010.

[5] Yanjun Pan, Ziqi Xu, Ming Li and Loukas Lazos, "Man-in-the-Middle Attack Resistant Secret Key Generation via Channel Randomization", The Twenty-Second ACM International Symposium on Theory, Algorithmic Foundations, and Protocol Design for Mobile Networks and Mobile Computing (ACM MobiHoc), Hybrid, July 2021 (20% acceptance rate).

[6] Yanjun Pan, Ming Li, Yantian Hou, Ryan Gerdes, Bedri Cetiner, “Enhance Physical Layer Security via Channel Randomization with Reconfigurable Antennas”, invited chapter in book Proactive and Dynamic Network Defense, Springer, Cliff Wang and Zhuo Lu (Editors), ISBN: 978-3-030-10596-9, to appear, 2019.

[7] Yanjun Pan, Yao Zheng and Ming Li, "ROBin: Known-Plaintext Attack Resistant Orthogonal Blinding via Channel Randomization", IEEE INFOCOM 2020, Apr. 2020, Beijing, China (Acceptance rate: 19.8%)

[8] Mingshun Sun, Yanmao Man, Ming Li, and Ryan Gerdes, "SVM: Secure Vehicle Motion Verification with a Single Wireless Receiver", The 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks (ACM WiSec 2020), Jul. 8-15, 2020 (Acceptance rate: 26%) (Best Paper Award)

Dissertations:

[9] Nirnimesh Ghose, “Authentication and Message Integrity Verification without Secrets, The University of Arizona”, 2019

[10] Yanjun Pan, “Enhance Wireless Network Performance and Security with Reconfigurable Antennas”, The University of Arizona, 2021

Honors and Awards: •Best Paper Award, The 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks (ACM WiSec 2020), for the paper "SVM: Secure Vehicle Motion Verification with a Single Wireless Receiver".
- Distinguished Scholars Award, University of Arizona, 2019
- Craig M. Berge Dean's Faculty Fellowship, College of Engineering, University of Arizona, 2020-2023

Protocol Activity Status:

RPPR Final Report
as of 27-Jan-2023

Technology Transfer: Nothing to Report

PARTICIPANTS:

Participant Type: PD/PI
Participant: Ming Li
Person Months Worked: 1.00 **Funding Support:**
Project Contribution:
National Academy Member: N

Participant Type: Co PD/PI
Participant: Loukas Lazos
Person Months Worked: 1.00 **Funding Support:**
Project Contribution:
National Academy Member: N

Participant Type: Graduate Student (research assistant)
Participant: Yanjun Pan
Person Months Worked: 6.00 **Funding Support:**
Project Contribution:
National Academy Member: N

Participant Type: Graduate Student (research assistant)
Participant: Nirnimesh Ghose
Person Months Worked: 6.00 **Funding Support:**
Project Contribution:
National Academy Member: N

Participant Type: Graduate Student (research assistant)
Participant: Ziqi Xu
Person Months Worked: 6.00 **Funding Support:**
Project Contribution:
National Academy Member: N

Participant Type: Graduate Student (research assistant)
Participant: Jingcheng Li
Person Months Worked: 6.00 **Funding Support:**
Project Contribution:
National Academy Member: N

Participant Type: Undergraduate Student
Participant: Tyler Wong
Person Months Worked: 2.00 **Funding Support:**
Project Contribution:
National Academy Member: N

RPPR Final Report
as of 27-Jan-2023

Participant Type: Undergraduate Student
Participant: Nick Smith
Person Months Worked: 2.00 **Funding Support:**
Project Contribution:
National Academy Member: N

Participant Type: High School Student
Participant: Ethan Sayre
Person Months Worked: 2.00 **Funding Support:**
Project Contribution:
National Academy Member: N

Participant Type: High School Student
Participant: David Li
Person Months Worked: 2.00 **Funding Support:**
Project Contribution:
National Academy Member: N

Participant Type: High School Student
Participant: Richard Peng
Person Months Worked: 2.00 **Funding Support:**
Project Contribution:
National Academy Member: N

ARTICLES:

RPPR Final Report
as of 27-Jan-2023

Publication Type: Journal Article Peer Reviewed: Y **Publication Status:** 1-Published
Journal: IEEE TRANSACTIONS ON MOBILE COMPUTING
Publication Identifier Type: DOI Publication Identifier: 10.1109/TMC.2020.3015010
Volume: Issue: First Page #:
Date Submitted: 10/1/20 12:00AM Date Published: 8/7/20 7:00AM
Publication Location:
Article Title: In-band Secret-Free Pairing for COTS Wireless Devices
Authors: Nirnimesh Ghose, Loukas Lazos, and Ming Li
Keywords: Bootstrapping, Physical-layer Security, Wireless Signal Manipulation Attacks, Man-in-the-Middle Attacks, Key Establishment, Message Integrity, Internet-of-Things, Secret-free, In-band, Trust establishment, COTS wireless devices
Abstract: Many IoT devices lack the necessary interfaces (keyboards, screens) for entering passwords or changing default ones. For these devices, bootstrapping trust can be challenging. We address the problem of device pairing in the absence of any shared secrets. Pairing is a two-phase process that requires the mutual authentication between the two parties and the agreement to a common key that can be used to further bootstrap essential cryptographic mechanisms. We propose a secret-free and in-band trust establishment protocol that achieves the secure pairing of commercial off-the-shelf (COTS) wireless devices with a hub. As compared to the state-of-the-art, our protocol does not require any hardware/firmware modification to the devices, or any out-of-band channels, but can be applied to any COTS device. Furthermore, our protocol is resistant to active signal manipulations attacks that include recently demonstrated signal nullification at an intended receiver.
Distribution Statement: 1-Approved for public release; distribution is unlimited.
Acknowledged Federal Support: **Y**

Publication Type: Journal Article Peer Reviewed: Y **Publication Status:** 4-Under Review
Journal: IEEE TRANSACTIONS ON MOBILE COMPUTING
Publication Identifier Type: Publication Identifier:
Volume: Issue: First Page #:
Date Submitted: 1/19/23 12:00AM Date Published:
Publication Location:
Article Title: ZITA: Zero-Interaction Two-Factor Authentication using Contact Traces and In-band Proximity Verification
Authors: Nirnimesh Ghose, Kaustubh Gupta, Loukas Lazos, Ming Li, Ziqi Xu, and Jincheng Li
Keywords: Two-Factor Authentication, Physical-layer Security, Wireless Signal Manipulation Attacks, Man-in-the-Middle Attacks, In-band, COTS wireless devices
Abstract: We propose a zero-interaction, two-factor authentication (ZITA) protocol. In ZITA, the first factor is implemented using the conventional username and password methods. The second factor is completed without any human effort provided that the user is not accessing the service from an unregistered public device and a designated secondary device is physically co-present. To automate the second factor, ZITA exploits the long-term contact between the login device and the secondary device such as a smartphone. Moreover, to thwart man-in-the-middle and co-located attacks, ZITA incorporates a proximity verification test that relies on the randomness of ambient RF signals. Compared with other zero-effort TFA protocols, ZITA remains secure against advanced threats and does not require out-of-band sensors such as microphones, speakers, or photoplethysmograph sensors.
Distribution Statement: 2-Distribution Limited to U.S. Government agencies only; report contains proprietary info
Acknowledged Federal Support: **Y**

CONFERENCE PAPERS:

RPPR Final Report
as of 27-Jan-2023

Publication Type: Conference Paper or Presentation **Publication Status:** 1-Published
Conference Name: IEEE INFOCOM 2020
Date Received: 01-Oct-2020 Conference Date: 27-Apr-2020 Date Published:
Conference Location: Online
Paper Title: ROBin: Known-Plaintext Attack Resistant Orthogonal Blinding via Channel Randomization
Authors: Yanjun Pan, Yao Zheng, Ming Li
Acknowledged Federal Support: **Y**

Publication Type: Conference Paper or Presentation **Publication Status:** 1-Published
Conference Name: 2019 Annual Computer Security Applications Conference (ACSAC 2019)
Date Received: 01-Oct-2020 Conference Date: 09-Dec-2019 Date Published:
Conference Location: San Juan
Paper Title: SIMPLE: Single-Frame based Physical Layer Identification for Intrusion Detection and Prevention on In-Vehicle Networks
Authors: Mahsa Foruhandeh, Yanmao Man, Ryan Gerdes, Ming Li, Tam Chantam
Acknowledged Federal Support: **Y**

Publication Type: Conference Paper or Presentation **Publication Status:** 1-Published
Conference Name: The 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks (ACM WiSec 2020)
Date Received: 01-Oct-2020 Conference Date: 08-Jul-2020 Date Published:
Conference Location: Online
Paper Title: SVM: Secure Vehicle Motion Verification with a Single Wireless Receiver
Authors: Mingshun Sun, Yanmao Man, Ming Li, Ryan Gerdes
Acknowledged Federal Support: **Y**

Publication Type: Conference Paper or Presentation **Publication Status:** 1-Published
Conference Name: The Twenty-Second ACM International Symposium on Theory, Algorithmic Foundations, and Protocol Design for Mobile Networks and Mobile Computing (ACM MobiHoc 2021)
Date Received: 23-Aug-2021 Conference Date: 26-Jul-2021 Date Published:
Conference Location: Hybrid
Paper Title: Man-in-the-Middle Attack Resistant Secret Key Generation via Channel Randomization
Authors: Yanjun Pan, Ziqi Xu, Ming Li. Loukas Lazos
Acknowledged Federal Support: **Y**

Publication Type: Conference Paper or Presentation **Publication Status:** 1-Published
Conference Name: NDSS 2022
Date Received: 19-Jan-2023 Conference Date: 25-Apr-2022 Date Published: 25-Apr-2022
Conference Location: San diego
Paper Title: PoF: Proof-of-Following for Vehicle Platoons
Authors: Ziqi Xu, Jingcheng Li, Yanjun Pan, Loukas Lazos, Ming Li, Nirnimesh Ghose
Acknowledged Federal Support: **Y**

Publication Type: Conference Paper or Presentation **Publication Status:** 3-Accepted
Conference Name: 2023 International Conference on Computing, Networking and Communications (ICNC)
Date Received: 19-Jan-2023 Conference Date: 20-Feb-2023 Date Published:
Conference Location: Honolulu, HI
Paper Title: Wiggle: Physical Challenge-Response Verification of Vehicle Platooning
Authors: Connor Dickey, Christopher Smith, Quentin Johnson, Jingcheng Li, Ziqi Xu, Loukas Lazos, Ming Li
Acknowledged Federal Support: **Y**

RPPR Final Report
as of 27-Jan-2023

Publication Type: Conference Paper or Presentation **Publication Status:** 1-Published
Conference Name: The 39th IEEE Symposium on Security & Privacy (Oakland) (IEEE S&P 2018)
Date Received: 19-Jan-2023 Conference Date: 21-May-2018 Date Published:
Conference Location: San Francisco, CA
Paper Title: Secure Device Bootstrapping without Secrets Resistant to Signal Manipulation Attacks
Authors: Nirnimesh Ghose, Loukas Lazos, Ming Li
Acknowledged Federal Support: **Y**

DISSERTATIONS:

Publication Type: Thesis or Dissertation
Institution: The University of Arizona
Date Received: 04-Sep-2019 Completion Date: 5/1/19 9:45PM
Title: AUTHENTICATION AND MESSAGE INTEGRITY VERIFICATION WITHOUT SECRETS
Authors: Nirnimesh Ghose
Acknowledged Federal Support: **Y**

Publication Type: Thesis or Dissertation
Institution: The University of Arizona
Date Received: 23-Aug-2021 Completion Date: 7/31/21 3:41PM
Title: Enhance Wireless Network Performance and Security with Reconfigurable Antennas
Authors: Yanjun Pan
Acknowledged Federal Support: **Y**

Partners

,

I certify that the information in the report is complete and accurate:
Signature: Ming Li
Signature Date: 1/19/23 5:39PM

Nothing to report in the uploaded pdf (see accomplishments)