REPORT DOCUMENTATION PAGE

Form Approved OMB NO. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (From - To)
31-08-2018	Final Report	1-Oct-2015 - 30-May-2018

4. TITLE AND SUBTITLE

Final Report: InvisibleSensing: Security Through Invisibility for Dynamically Changing Wireless Sensor Networks Section II A 2 ARO, RESEARCH AREA 5: COMPUTING SCIENCE, 5.3 Information and Software Assurance.

5a. CONTRACT NUMBER
W911NF-15-1-0651

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 Tennessee at Knoxville
Office of Sponsored Programs
1534 White Avenue
Knoxville, TN 37996 -1529

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)
66270-CS.8

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			Jinyuan Sun
UU	UU	UU	UU		19b. TELEPHONE NUMBER 865-974-0426

RPPR Final Report
as of 24-Jan-2019

Agency Code:

Proposal Number: 66270CS **Agreement Number: W911NF-15-1-0651**
INVESTIGATOR(S):

Name: Jinyuan Sun
Email: jysun@utk.edu
Phone Number: 8659740426
Principal: Y

Organization: **University of Tennessee at Knoxville**
Address: Office of Sponsored Programs, Knoxville, TN 379961529
Country: USA

DUNS Number: 003387891 EIN: 626001636
Report Date: 30-May-2018 Date Received: 31-Aug-2018
Final Report for Period Beginning 01-Oct-2015 and Ending 30-May-2018
Title: InvisibleSensing: Security Through Invisibility for Dynamically Changing Wireless Sensor Networks Section II A 2 ARO, RESEARCH AREA 5: COMPUTING SCIENCE, 5.3 Information and Software Assurance.
Begin Performance Period: 01-Oct-2015 **End Performance Period:** 30-May-2018
Report Term: 0-Other

Submitted By: Jinyuan Sun Email: jysun@utk.edu
Phone: (865) 974-0426

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

STEM Degrees: **STEM Participants:**

Major Goals: The proposed research focuses on the development of the fundamental mathematics necessary to analyze the behavior of wireless networks in contested environments, and leveraging such behavior to design an adaptable secure sensing system, InvisibleSensing, suitable for deployment in dynamically changing environments. We propose to explore a new design paradigm where security is achieved through invisibility, i.e., making sensitive sensors and their transmissions disappear by letting the sensors masquerade as general-purpose or other unsuspicious devices in their changing environments. It can greatly raise the bar for adversaries since they need to figure out if their targets are present at all. Our proposed secure sensing system, InvisibleSensing, is intended for military applications where special-purpose sensors are used to monitor and report events that may be of adversaries' interests. InvisibleSensing provides security protection by tricking adversaries into believing that normal traffic is taking place in the system so that our sensors do not become the targets in the first place. Success in devising the invisibility paradigm could potentially change the way modern military security systems are designed and enhance the protection of wireless sensor networks and applications that are highly sensitive in nature. In particular, main goals of the proposed research consist of:
1. Formally define the new security concept invisibility and devise metrics to measure invisibility.
2. Design and develop the InvisibleSensing system to achieve invisibility and efficiency in terms of computation and communication, aiming for practical deployment.
3. Evaluate the security and efficiency of InvisibleSensing by extensive simulations, as well as experiments using hardware testbed.

Accomplishments: Major Activities: We mainly focused on the remaining tasks from last year, i.e., testing models and developing schemes/algorithms for packet-level invisibility and signal-level invisibility, and Tasks 1 and 4, i.e., defining invisibility formally and combine Tasks 2 and 3 to develop a unified framework. We published papers in conference proceedings and journals as well as participated in conferences and workshops. Weekly group meetings were held to check the project progress and provide mentoring for graduate students. I used topics and research outcomes in this project as real-world examples and impact to stimulate students' interests in cybersecurity and sensing systems, by channeling project related materials into my undergraduate course ECE 461 Introduction to Computer Security during this project period. Hands-on projects directly created out of this project were given to undergraduate and high school students who were interested in my research.

Specific Objectives:
To formally define invisibility.
To develop packet-level invisibility techniques.

RPPR Final Report
as of 24-Jan-2019

To develop signal-level invisibility techniques.
To integrate packet-level and signal-level invisibility into a framework.
To develop hardware testbed and run experiments in hostile environments.

Significant Results: During this reporting period, we have obtained significant and positive results to support our proposed research in this project.

Specifically, for the MPC scheme we proposed, we showed that it can be generally applied to most of the current IA systems as long as the output (behavior scores) can be converted to probabilistic values. We also demonstrated that MPC increases authentication accuracy by 18.63% and reduces authentication delay by 7.02 minutes on average. The experiments were conducted using the Friends and Family Dataset as opposed to proprietary datasets, and thus the repeatability is guaranteed.

For iKey, our real-world experiments with multiple users demonstrate that iKey achieves more than 94% identification accuracy with low false negative rate. We also provided details of designing and implementing such a system. Specifically, we designed a motion segmentation algorithm to detect the transition between two motions from the noisy sensing data. We then leveraged the distinct feature contained in each sub- segment of the unlocking motion, instead of the entire motion, to estimate the probability that the unlocking motion is performed by authorized users of the smartphone.

For the middle layer we built, we conducted experiments on both synthetic (Friends and Family Dataset) and real datasets. The average accuracy of identifying legitimate users is 96.73% using the synthetic dataset and 96.70% using the real dataset. We also tested the power consumption on a low-end Nexus S smartphone to obtain a more pessimistic result. We found that our method consumed 14.5% of the device's total battery usage. The power consumption performance is expected to improve significantly on high-end mobile devices.

We conducted penetration testing and discovered that all IEEE C37.118 frames used by PMU-PDC communications are transferred in clear. Hence, not only can attackers intercept and eavesdrop configuration frames but they can also eavesdrop for command and data frames. We used packet sniffing to confirm that a PMU network is vulnerable to eavesdropping. We then developed a practical exploit to demonstrate what the attacker could do to the power grid when such vulnerabilities are exploited. We considered a scenario where a PMU network is employed to obtain early warning and maintain situational awareness of the potential inter- area oscillations, using the WECC 179-bus sytem. All PMUs send their real-time measurement data to a central PDC. Based on the concentrated measurements at the PDC, the real-time angle of an individual zone is obtained by averaging the measurements of angles reported by the three PMUs in that zone. We applied faults include six three-phase faults at 0s, 40s, 80s, 120s, 160s and 200s near bus 83 to simulate a cascading failure. We then launched the data stream hijacking attack at the 35th second, just prior to the application of the first fault. The attacker hijacks the data stream transmission and keeps replaying to the PDC the rotor angle measurements of all the 12 PMUs between the 30th to 35th second it obtained through eavesdropping. The result was that this false situational awareness was presented to the operator who was blinded from the fact that a cascading failure is happening in the system.

We proposed a simple and practical SSE scheme that aims to protect the privacy of data generated in smart gird. We also implemented a prototype over the statistical data of advanced meter infrastructure (AMI) to show the effectiveness of our approach. Specifically, we reviewed and analyzed the typical state-of-the-art SSE schemes and showed why they are inappropriate for smart grid data. Based on the characteristics of smart grid data, we designed a practical SSE scheme that provides higher space efficiency with tolerable information leakage in real smart grid applications. We implemented a prototype based on the statistic data of AMI provided by the U.S. Energy Information Administration (EIA) to show the effectiveness of our scheme. Our scheme can also be applied to other types of data in the smart grid, such as metering data and PMU/PDC data.

In addition, we proposed a transmission opportunity auction scheme, called TOA, which can support multi-hop data traffic, ensure economic-robustness, and generate high revenue for the auctioneer. Specifically, in TOA, instead of spectrum bands as in traditional spectrum auction schemes, users bid for transmission opportunities (TOs). A TO is defined as the permit of data transmission on a specific link using a certain band, i.e., a link-band pair. The TOA scheme is composed of three procedures: TO allocation, TO scheduling, and pricing, which are performed sequentially and iteratively until the aforementioned goals are reached. We proved that TOA is economic-robust, and conducted extensive simulations to show its effectiveness and efficiency.

RPPR Final Report
as of 24-Jan-2019

Key outcomes or Other achievements:
During this reporting period, we have produced 4 journal papers (to appear, under review or to be submitted) and 3 conference papers (published or under review). A new PhD student and a domestic Master's student were recruited with the support of the grant.

Training Opportunities: In the past year, this project provided partial support for five Ph.D. students. Two of the Ph.D. students are female. Hands-on projects derived from the PersonaIA system and smart grid security based on this project were developed for undergraduate students Andrew Webb, Julian Ball, and Matthew Butera. The progress and contributions made by these students were invaluable to the improvement of the system.

Results Dissemination: The results are mainly disseminated through conference papers and journal publications, as well as presentations at conferences such as IEEE INFOCOM. PI Sun gave a seminar to the faculty and students at Northwest University, Xi'an, China. The research themes in this project were included in talk. Several faculty members and students including females expressed interest in the research. One of the aforementioned papers, iKey, is a collaborative work with Northwest.

Honors and Awards: Nothing to Report

Protocol Activity Status:

Technology Transfer: Nothing to Report

PARTICIPANTS:

Participant Type: PD/PI
Participant: Jinyuan Stella Sun
Person Months Worked: 1.00 **Funding Support:**
Project Contribution:
International Collaboration:
International Travel:
National Academy Member: N
Other Collaborators:

Participant Type: Co PD/PI
Participant: Husheng Li
Person Months Worked: 1.00 **Funding Support:**
Project Contribution:
International Collaboration:
International Travel:
National Academy Member: N
Other Collaborators:

Participant Type: Graduate Student (research assistant)
Participant: Jiangnan Li
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: Zhongbo Li
Person Months Worked: 11.00 **Funding Support:**
Project Contribution:

International Collaboration:
International Travel:
National Academy Member: N
Other Collaborators:

Participant Type: Graduate Student (research assistant)
Participant: Cindy Yao
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:** 3-Accepted
Journal: IEEE Transactions on Dependable and Secure Computing (TDSC)
Publication Identifier Type: Other Publication Identifier:
Volume: Issue: First Page #:
Date Submitted: 8/31/16 12:00AM Date Published: 8/31/16 4:01PM
Publication Location:
Article Title: PersonaIA: A Lightweight Implic Authentication System based on Customized User Behavior Selection
Authors: Yingyuan Yang, Jinyuan Sun, Linke Guo
Keywords: Implicit authentication, Topic model, Use behavior, Mobile security, Energy efficiency
Abstract: Motivated by the great potential of implicit and seamless user authentication, we attempt to build an implicit authentication system with adaptive sampling that automatically selects dynamic sets of activities for user behavior extraction. User behaviors can change unpredictably which renders it more challenging to develop systems that depend on them. In addition to dynamic behavior extraction, the proposed implicit authentication system differs from the existing systems in terms of energy efficiency for mobile devices. Since implicit authentication systems including the proposed one rely on machine learning, the expensive training process needs be outsourced to the remote server. We propose a W-layer, an overlay that provides a practical and energy-efficient solution for implicit authentication on mobile devices. Our system achieved 93.3% precision and 98.6% accuracy in identifying users and consumed 14.5% of the device's total battery usage even on a low-end Nexus S smartphone.
Distribution Statement: 1-Approved for public release; distribution is unlimited.
Acknowledged Federal Support: **Y**

RPPR Final Report
as of 24-Jan-2019

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: 8/24/17 12:00AM Date Published:
Publication Location:
Article Title: Economic-Robust Transmission Opportunity Auction for D2D Communications in Cognitive Mesh Assisted Cellular Networks
Authors: Ming Li, Weixian Liao, Xuhui Chen, Jinyuan Sun, Xiaoxia Huang, Pan Li
Keywords: Device-to-Device communications, cognitive mesh assisted cellular network, transmission opportunity auction
Abstract: In this paper, we propose a new architecture, called cognitive mesh assisted cellular network (CMCN), in which several secondary service providers (SSPs) deploy CR routers to facilitate D2D communications among wireless users. To address the competition among the SSPs, we further construct a secondary spectrum auction market. Although a few works have studied spectrum auction, most of them are designed for single-hop communications, and it is usually not clear whom a winning user communicates with. Uncertain spectrum availability is not considered in previous schemes either. We propose a transmission opportunity auction scheme, called TOA, which can address these problems. Extensive simulations are conducted to validate the efficiency of the CMCN architecture and that of the TOA scheme.
Distribution Statement: 5-Distribution authorized to DoD Components only
Acknowledged Federal Support: **Y**

Publication Type: Journal Article Peer Reviewed: Y **Publication Status:** 4-Under Review
Journal: IEEE Transactions on Parallel and Distributed Systems
Publication Identifier Type: Publication Identifier:
Volume: Issue: First Page #:
Date Submitted: 8/24/17 12:00AM Date Published:
Publication Location:
Article Title: Privacy-preserving Computation for Large-scale Security-Constrained Optimal Power Flow Problem in Smart Grid
Authors: Xiangyu Niu, Hung Khanh Nguyen, Jinyuan Sun, Zhu Han
Keywords: Optimal Power Flow, Security, Privacy-preserving, Cloud Computing, Smart Grid
Abstract: In this paper, we present a privacy-preserving algorithm to solve the Security Constrained Optimal Power Flow (SCOPF) problem in smart grid. The SCOPF problem seeks the optimal dispatch subject to a set of postulated constraints under the normal and contingency conditions. However, due to the large problem size and real-time requirement, a fast and robust technique is required to solve this problem. Moreover, due to privacy concerns, it is important that the data remains confidential and processes on local computers. Therefore, a fully privacy-preserving algorithm is proposed which performs computation directly over encrypted SCOPF problem. The SCOPF is decomposed into small subproblems correspond to each individual pre-contingency and post-contingency cases using Alternating Direction Method of Multipliers (ADMM) and gradient projection algorithms. Both algorithms are presented for solving SCOPF problem in a privacy-preserving and distributed manner.
Distribution Statement: 5-Distribution authorized to DoD Components only
Acknowledged Federal Support: **Y**

CONFERENCE PAPERS:

Publication Type: Conference Paper or Presentation **Publication Status:** 1-Published
Conference Name: IEEE ICC
Date Received: 31-Aug-2016 Conference Date: 08-Jun-2015 Date Published: 10-Sep-2015
Conference Location: London, UK
Paper Title: Network Steganography based on Traffic Behavior in Dynamically Changing Wireless Sensor Networks
Authors: Xiangyu Niu, Jinyuan Sun, Husheng Li
Acknowledged Federal Support: **Y**

RPPR Final Report
as of 24-Jan-2019

Publication Type: Conference Paper or Presentation **Publication Status:** 4-Under Review
Conference Name: IEEE INFOCOM
Date Received: 31-Aug-2016 Conference Date: 01-May-2017 Date Published: 01-May-2017
Conference Location: Atlanta, GA
Paper Title: Energy-efficient W-layer for Behavior-based Implicit Authentication on Mobile Devices
Authors: Yingyuan Yang, Jinyuan Sun
Acknowledged Federal Support: **Y**

Publication Type: Conference Paper or Presentation **Publication Status:** 5-Submitted
Conference Name: IEEE INFOCOM
Date Received: 24-Aug-2017 Conference Date: 16-Apr-2018 Date Published:
Conference Location: Honolulu, HI
Paper Title: Dynamic Multi-level Privilege Control in Behavior-based Implicit Authentication Systems Leveraging Mobile Devices
Authors: Yingyuan Yang, Jinyuan Sun
Acknowledged Federal Support: **Y**

DISSERTATIONS:

Publication Type: Thesis or Dissertation
Institution: University of Tennessee
Date Received: 31-Aug-2016 Completion Date: 7/31/16 7:22PM
Title: pDroid: Master Thesis
Authors: Joe Allen
Acknowledged Federal Support: **Y**

ARO Project 66270-CS

InvisibleSensing: Security Through Invisibility for Dynamically Changing Wireless Sensor Networks

(Performance Period: August 1, 2017 – May 30, 2018)

Annual Report

Jinyuan Stella Sun

Department of Electrical Engineering and Computer Science
University of Tennessee
Knoxville, TN 37996
Tel: (865) 974-0426, Fax: (865) 974-4404
Email: jysun@utk.edu
Website: http://web.eecs.utk.edu/~jysun

Husheng Li

Department of Electrical Engineering and Computer Science
University of Tennessee
Knoxville, TN 37996
Tel: (865) 974-3861, Fax: (865) 974-4404
Email: hli31@utk.edu
Website: http://web.eecs.utk.edu/~husheng

1 Introduction

This project is an ARO project. The project started on October 1, 2015 and ended on May 30, 2018. This report summarizes the major research and education activities and findings during the performance period from August 1, 2017 to May 30, 2018.

This project focuses on a new design paradigm to secure dynamically changing wireless sensor networks where security is achieved through invisibility, i.e., making sensitive sensors and their transmissions disappear by letting the sensors masquerade as general-purpose or other unsuspicious devices in their changing environments. It can greatly raise the bar for adversaries since they need to figure out if their targets are present in the first place. The proposed secure sensing system, InvisibleSensing, is intended for military applications where special-purpose sensors are used to monitor and report events that may be of adversaries' interests. InvisibleSensing provides security protection by tricking adversaries into believing that normal traffic is taking place in the system so that our sensors do not become the targets in the first place. Success in devising the invisibility paradigm could potentially change the way modern military security systems are designed and enhance the protection of wireless sensor networks and applications that are highly sensitive in nature.

In what follows, we will present our major research activities and research findings in this reporting year. The whole project team worked together to fulfill the targeted research objectives towards the proposed goals. PI Sun's team worked on developing the packet-level invisibility. PI Li's team worked on developing the signal-level invisibility. Both teams worked together to develop the invisibility definition, unified framework, and testbed. While our research emphasis is on behavior modeling in wireless sensor networks, we have also looked into problems of similar nature in other systems, resulting in solutions to a broader range of engineering problems. In particular, we have focused on modeling and mimicking human behaviors using topic models and applying the results to authentication. We were able to find a public dataset containing comprehensive user behavior data on which we conducted our performance evaluation. Human behaviors are far more complex than sensor behaviors and the insight we have gained will be tremendously helpful to this project. The application we used to evaluate our design, i.e., behavior-based authentication, is similar in nature to making the sensors invisible since both are concerned with learning the behavior of and identifying (mimicking) objects (whether they are sensors or human beings). We will also report findings on security design for other data-driven distributed systems such as smart environments like smart cities and smart grids, and wireless networks.

2 New Research Activities and Findings

2.1 Dynamic Multi-level Privilege Control for Behavior-based Implicit Authentication

As with any other practical security system, IA systems need to strike a good balance between security and usability. However, it is highly challenging to achieve such balance due to the dynamically changing behaviors of users. On the one hand, we need the system to cope with a user's

behavior deviation, e.g., a change of routine, and not falsely reject the user (usability). On the other hand, the system needs to differentiate between a legitimate user's changed behavior and other users' behaviors to prevent falsely accepting adversaries (security). Balancing between such false rejects and false accepts improves the authentication accuracy and is the main focus of this work. In addition to false reject rate, another important measure of system usability is authentication delay. Authentication delay mainly consists of training delay to obtain historical behaviors and behavior matching delay, which varies across different authentication schemes and is closely relevant to authentication accuracy. The amount and quality of sensor data collected by the system directly affects the authentication accuracy. Insufficient data collection can result in an inferior historical behavior model that is not representative of a user's behavior. Low quality data can be caused by noisy behavior data (due to either a legitimate user's behavior deviation or adversaries) or noisy sensor readings. Authentication delay is typically increased when the system attempts to improve upon the amount and quality of collected data. Balancing between authentication accuracy and delay is hence another problem this work is trying to solve to further enhance usability.

Existing research on IA systems focuses on the effectiveness of IA schemes, i.e., finding suitable behavioral features such as touch, typing, and other motions that uniquely identify users. Although authentication accuracy and delay were measured as performance indicators, none of the existing works addressed methods to improve them to make the system more user-friendly. We argue that this is a rather important issue to consider since practicality is the key for IA systems to be widely deployed, and provide our solutions in this work. Specifically, we proposed a multi-level privilege control scheme, or MPC, that divides the single privilege level in current systems into multiple fine-grained privilege levels. The privilege levels are used to separate apps based on their level of security so that users can still access the less sensitive apps on their smart devices even if their behaviors change. The levels are dynamically adjusted to reflect the user's dynamically changing behaviors, and therefore enhancing the system's authentication accuracy by balancing between false rejects and false accepts. It is challenging to find such a balance because of the difficulty in distinguishing a user's deviated behaviors from other users' behaviors. In other words, decreased false reject rate may cause increased false accept rate, and vice versa. A fine line needs to be drawn to lower both rates and boost the system's confidence on a user's legitimacy, which requires in-depth analysis of the existing IA schemes and suitable mathematical modeling.

MPC solves the core problem of how to set and adjust the privilege levels such that both false reject rate and false accept rate are decreased, where the problem is modeled by applying physical laws that describe the motion of bodies under the influence of a system of forces. To further correct the privilege level adjustment and improve authentication accuracy, we employed a two-factor authentication mechanism in which the secondary factor provides feedback to identify the user's behavior deviation and filter out noisy sensor readings using Kalman filter. We showed that the proposed MPC can be generally applied to most of the current IA systems as long as the output (behavior scores) can be converted to probabilistic values. We also demonstrated that MPC increases authentication accuracy by 18.63% and reduces authentication delay by 7.02 minutes on average. The experiments were conducted using the Friends and Family Dataset, as opposed to proprietary datasets, and thus the repeatability is guaranteed. This work produced a journal

paper [1] to be submitted.

2.2 iKey: Instantly Knowing Who is Taking on the Smartphone

User identification is of great importance to maintain the security level of a smartphone throughout the login sessions. Currently, there is a lack of research work on user-behavior-based authentication leveraging smartphones that allows multiple users to use the same phone. We proposed iKey, a system which can instantly and inconspicuously identify who is accessing the smartphone and authorize different users with different permissions so that multiple users can have access to a smartphone. iKey achieves this by utilizing only users' short-term (about 2 seconds) interaction with the smartphone, without relying on any predefined motions. The basic idea behind iKey is to distinguish users by identifying the order of the motions from the time they pick up the phone to when they succesfully (or unsuccessfully) log into the phone. For this purpose, we proposed a Markov based model to continuously track the behavior of the smartphone users. Based on this model, iKey is able to instantly and accurately estimate how likely the current behavior is from authorized users. Our real-world experiments with multiple users demonstrate that iKey can achieve high identification accuracy (more than 94%) with low false negative rate. We also provided details of designing and implementing such a system. We solved related challenges to make the scheme practical. Specifically, we designed a motion segmentation algorithm to detect the transition between two motions from the noisy sensing data. We then leveraged the distinct feature contained in each sub-segment of the unlocking motion, instead of the entire motion, to estimate the probability that the unlocking motion is performed by authorized users of the smartphone. This work has produced a journal paper to be submitted [2].

2.3 Energy-efficient W-layer for Behavior-based Implicit Authentication

We built an overlay, called W-layer, that runs independently within the device and can be integrated seamlessly with various machine learning algorithms implicit authentication (IA) is based on. To ensure practical deployment for smart devices, our system was made energy-efficient by leveraging lightweight computation and adaptive sampling. The uniqueness of W-layer is two-fold. First, W-layer provides a client-side lightweight IA solution that can replace or assist in the IA solution that relies on complex machine learning. The majority of existing research work relies heavily on machine learning models such as Support Vector Machine (SVM), k Nearest Neighbor (kNN) and Gaussian Mixture Model (GMM), where the expensive training process needs be outsourced to the remote server. This design not only increases the communication burden between the client and server, but also potentially increases the chance of private data leakage. W-layer is energy-efficient in that only lightweight computation is involved in behavior matching and adaptive sampling is employed to keep the sensing overhead at bay. The resulting solution is therefore practical even on low-end mobile devices. In addition, W-layer is a self-contained IA solution that can replace the machine learning-based solutions. To use W-layer as an assisting technology, machine learning can be run in the server to obtain a reference behavior model for each user. This reference model will be used by W-layer to guide activity data collection and real-time behavior matching. In this case,

machine learning will run much less frequently (assuming behavior change happens less often than authentication) and less real-time communication will take place. Second, W-layer addresses the challenging problem of distinguishing between legitimate users' behavior deviation and illegitimate users' behaviors which affects the accuracy and practicality of the IA system.

To successfully develop W-layer, we need to solve challenges related to system design, which are associated with designing the system architecture of W-layer and developing it into a practical system. Specifically, we need to devise a real-time behavior matching algorithm which is the core component of and suitable for IA. To ensure practical deployment and user acceptance, this algorithm should improve system reliability by reducing the false negative and false positive rates. These challenges were resolved by our novel Wind Vane Module (WVM) in W-layer. To evaluate our method, we conducted several experiments on both synthetic and real datasets. The average accuracy of identifying legitimate users is 96.73% using the synthetic dataset and 96.70% using the real dataset. We also tested the power consumption on a low-end Nexus S smartphone to obtain a more pessimistic result. We found that our method consumed 14.5% of the device's total battery usage. The power consumption performance is expected to improve significantly on high-end mobile devices. This work produced a conference paper [3] that was accepted by and presented at *IEEE INFOCOM'17* in 2017.

3 Security and Privacy in Related Diversified Systems

The developed techniques in this project are crucial to the success of next-generation secure smart/mobile and wireless technologies, and can be used to find novel solutions to supporting more diversified applications, such as smart environments like smart cities and smart grids, and wireless networks. We also explored the security and privacy issues in such systems using the techniques developed in this project.

3.1 Vulnerability Assessment for PMU Communication Networks

The smart grid is introducing many salient features such as wide-area situational awareness, precise demand response, and substation automation. These features are enabled by data communication networks that facilitate the collection, transfer, and processing of a wide variety of data regarding different components of the smart grid. As a result, the smart grid's heavy dependence on data inevitably poses a great challenge to ensuring data integrity and authenticity. Even with defending mechanisms such as firewalls, the internal network can no longer be deemed physically isolated. Additionally, experiences with information security in common computer networks reveal that flawed designs, implementations, and configurations of the communication networks introduce vulnerabilities. These vulnerabilities open opportunities for attackers to launch cyber attacks. In this research paper, we attempted to gain more insights into the security of the PMU communication network by exploring, validating, and demonstrating vulnerabilities.

We conducted penetration testing and discovered in the reconnaissance phase that all IEEE C37.118 frames used by PMU-PDC communications are transferred in clear. Hence, not only can

attackers intercept and eavesdrop configuration frames but they can also eavesdrop for command and data frames. We used packet sniffing to confirm that a PMU network is vulnerable to eavesdropping. As the C37.118 standard does not specify any user authentication mechanism, it is possible for the attackers to impersonate a legitimate publishing or subscribing devices and confuse, mislead, and sabotage other parties in the PMU network. Similarly, C37.118 doesn not have any message authentication mechanism in place. As a result, all frames are subject to frame modifications, and a receiving device is unable to distinguish between legitimate frames and modified frames. We used packet sniffing and packet injection to validate this vulnerability. As a stateful protocol, a device that runs C37.118 protocol manages its transition of states based on its current state and the frames it receives. If the incoming frames are expected under the current state, the device should make the state transitions accordingly. If not, the device should also handle for the case properly. In practice, implementations of PMU or PDC may ignore this situation. They become unresponsive or even crash upon receiving an unexpected frame. We used packet injection and fuzzing to confirm that the PMU and PDC implementations in our PMU network prototype have such a vulnerability.

We then developed a practical exploit to demonstrate what the attacker could do to the power grid when such vulnerabilities are exploited. We considered a scenario where a PMU network is employed to obtain early warning and maintain situational awareness of the potential inter-area oscillations, using the WECC 179-bus sytem. All PMUs send their real-time measurement data to a central PDC. Based on the concentrated measurements at the PDC, the real-time angle of an individual zone is obtained by averaging the measurements of angles reported by the three PMUs in that zone. We applied faults include six three-phase faults at 0s, 40s, 80s, 120s, 160s and 200s near bus 83 to simulate a cascading failure. We then launched the data stream hijacking attack at the 35th second, just prior to the application of the first fault. The attacker hijacks the data stream transmission and keeps replaying to the PDC the rotor angle measurements of all the 12 PMUs between the 30th to 35th second it obtained through eavesdropping. The result was that this false situational awareness was presented to the operator who was blinded from the fact that a cascading failure is happening in the system. This work produced a conference paper that was submitted to *SmartCom 2018* [4].

3.2 Privacy-preserving Computation for Large-scale Security-constrained Optimal Power Flow Problem in Smart Grid

In order to adequately supply the connected load while minimizing the operating costs, system operators need to solve the optimal power flow (OPF) problem subject to physical constraints and control limits of the power system. However, due to the large-scale interconnected topology of transmission and distribution networks, the OPF model can not ensure the demand-supply balance condition when the power system experiences unexpected failure and disconnection of components such as generators, transmission lines, transformers, etc., known as an outage or a contingency. To address this issue, security requirements ensure the power system to continue its reliable operation during contingency scenarios and need to be performed with the OPF problem, which is referred to as the security-constrained optimal power flow (SCOPF) problem. The optimal solution of

the SCOPF problem produces the minimal cost generation dispatch while still assures that the power system remains balanced and no operational constraints is violated in both the normal state and contingencies. The state-of-the-art formulation of SCOPF, the corrective SCOPF, generates additional variables, which sharply increase the problem size when numerous contingencies are taken into account. The large-scale formulated problem may result in excessive memory usage and unacceptable computation time. Recently, cloud computing has demonstrated its huge potential of tremendously speeding up intensive computation while reducing the cost. Hence, outsourcing the SCOPF problem to the cloud has emerged as a promising solution to the aforementioned problem. Nonetheless, the fact that the operation takes place entirely at a third party will inevitably raise privacy concerns about data sensitivity.

We proposed a privacy-preserving algorithm to demonstrate the feasibility of solving the corrective SCOPF problem without losing data privacy. Our basic idea is to let the ISO company encrypt their private data after which a third party performs the SCOPF algorithm over the encrypted data without decrypting it. The third party then sends the encrypted result to the ISO company, which can be decrypted using the pre-distributed secret key. This is accomplished by leveraging additive Homomorphic Encryption (such as the Paillier Cryptosystem). However, according to the additive homomorphism property, we cannot directly solve the SCOPF problem using any available methods. In this work, we leverage both alternating direction method of multipliers (ADMM) and gradient projection algorithm to transform the SCOPF problem into a solvable problem for additive homomorphic cryptosystem. Although the proposed scheme is based on ADMM and gradient projection, it can be easily extended to more sophisticated optimization algorithms. In addition, our proposed method is not limited to solve the SCOPF problem. It can also be applied to any other applications that involve ADMM or gradient projection for optimization problems such as Internet congestion control and power system state estimation. Security analysis showed that our algorithm can preserve both system privacy and data privacy. Performance evaluations validated the effectiveness of the proposed algorithm. This work produced a journal paper [5] that has been submitted to *IEEE Transactions on Dependable and Secure Computing (TDSC)*.

3.3 A Practical Searchable Symmetric Encryption Scheme (SSE) for Smart Grid Data

Outsourcing data storage to remote cloud can be an economical solution to enhance data management in smart grid ecosystem. To protect the privacy of data, the utility company may choose to encrypt the data before uploading them to the cloud. However, while encryption provides confidentiality to data, it also sacrifices the data owners' ability to query special segments in their data. Searchable symmetric encryption is a technology that enables users to store document in ciphertext form while keeping the functionality of searching for keywords in the documents. However, most state-of-the-art SSE algorithms only focus on general document storage, which may become unsuitable when applied to smart grid applications. We proposed a simple, practical SSE scheme that aims to protect the privacy of data generated in smart gird. We also implemented a prototype over the statistical data of advanced meter infrastructure (AMI) to show the effectiveness of our

approach.

Specifically, we reviewed and analyzed the typical state-of-the-art SSE schemes and showed why they are inappropriate for smart grid data. Based on the characteristics of smart grid data, we designed a practical SSE scheme that provides higher space efficiency with tolerable information leakage in real smart grid applications. We implemented a prototype based on the statistic data of AMI provided by the U.S. Energy Information Administration (EIA) to show the effectiveness of our scheme. Our scheme can also be applied to other types of data in the smart grid, such as metering data and PMU/PDC data. This work has produced a conference paper to be submitted [6].

3.4 Economic-Robust Transmission Opportunity Auction for D2D Communications in Cognitive Mesh Assisted Cellular Networks

The rapid growth of wireless devices and services exacerbates the problem of spectrum scarcity in wireless networks. Recently, spectrum auction has emerged as one of the most promising techniques to enhance spectrum utilization and mitigate this problem. Although there exist some works studying spectrum auction, most of them are designed for single-hop communications, and it is usually not clear whom a winning user communicates with. Moreover, most previous auction schemes only focus on satisfying the incentive compatibility property, also called truthfulness, but ignore another two critical properties: individual rationality, and budget balance. Thus, they may not be economic-robust. In this work, we proposed a transmission opportunity auction scheme, called TOA, which can support multi-hop data traffic, ensure economic-robustness, and generate high revenue for the auctioneer. Specifically, in TOA, instead of spectrum bands as in traditional spectrum auction schemes, users bid for transmission opportunities (TOs). A TO is defined as the permit of data transmission on a specific link using a certain band, i.e., a link-band pair. The TOA scheme is composed of three procedures: TO allocation, TO scheduling, and pricing, which are performed sequentially and iteratively until the aforementioned goals are reached. We proved that TOA is economic-robust, and conducted extensive simulations to show its effectiveness and efficiency. This work produced a journal paper [7] that has been accepted to *IEEE Transactions on Mobile Computing (TMC)*.

4 Graduate Student Mentoring

Graduate students play a significant role in conducting the proposed research work in this project. PI Sun was able to recruit one more PhD student, and a domestic Master's student with the support of this grant. In addition, two other PhD students including a female student, are partially supported by this project. PI Sun focused on fostering their creative and critical thinking, quantitative analysis skills, independent research capability, and collaboration skills. We held weekly meetings where we discussed research tasks and challenges in this project. PI Sun also held one-on-one weekly meetings with these students to understand their individual needs and help with their personal growth.

5 Outreach and Education Activities for Broader Impact

Our major results have been disseminated through presentations and publications in meetings, conferences, and journals. A substantial quantity of the materials of this project have also been made publicly available on PI Sun's website: `http://web.eecs.utk.edu/~jysun`.

In the past year, the research outcome and design methodologies developed in this project have been channeled into the classroom, and have contributed to hands-on projects for undergraduate research and young scholars. The research in this project is one of the main topics in one undergraduate course *ECE 461: Introduction to Computer Security*, one undergraduate/graduate course *ECE 453/553: Computer Communication Networks*, and one graduate seminar course *ECE 692: Advanced Topics in Computer Security Research* at UTK. Hands-on projects derived from the PersonaIA system and smart grid security based on this project were developed for undergraduate students Andrew Webb, Julian Ball, and Matthew Butera. The progress and contributions made by these students were invaluable to the improvement of the system.

References

[1] Y. Yang and J. Sun, "Dynamic multi-level privilege control in behavior-based implicit authentication systems leveraging mobile devices." https://arxiv.org/abs/1808.00638, july 2018.

[2] J. He, X. Chen, and J. Sun, "ikey: Instantly knowing who is taking the smartphone," *To be submitted*, 2018.

[3] Y. Yang and J. Sun, "Energy-efficient w-layer for behavior-based implicit authentication on mobile devices," in *Proceedings of IEEE INFOCOM'17*, 2017.

[4] X. Niu, Y. Tong, and J. Sun, "Vulnerability assessment for pmu communication networks," *Submitted to SmartCom 2018*, july 2018.

[5] X. Niu, H. Nguyen, J. Sun, and Z. Han, "Privacy-preserving computation for large-scale security-constrained optimal power flow problem in smart grid," *submitted to IEEE Transactions on Dependable and Secure Computing (TDSC), Manuscript #TDSC-2018-03-0110*, 2018.

[6] J. Li and J. Sun, "A practical searchable symmetric encryption scheme for smart grid data." https://arxiv.org/abs/1808.00645, july 2018.

[7] M. Li, W. Liao, X. Chen, J. Sun, X. Huang, and P. Li, "Economic-robust transmission opportunity auction for d2d communications in cognitive mesh assisted cellular networks," *To appear in IEEE Transactions on Mobile Computing*, 2018.