Semi-Annual Progress Report

TIDC Transportation Infrastructure Durability Center
AT THE UNIVERSITY OF MAINE

Project Number and Title: *4.3. Towards Quantitative Cybersecurity Risk Assessment in Transportation Infrastructure*
Research Area: *Thrust 4 Connectivity for enhanced asset and performance management*
PI: *Dr. Song Han, Assistant Professor, Department of Computer Science and Engineering, University of Connecticut*
Reporting Period: *Oct. 1st, 2018 – March 31st, 2019*
Date: *March 31st, 2019*

Overview:

Activities: During the reporting period, the research team at UConn led by PI Han has been exploring the connectivity and security issues in two representative transportation infrastructures: low-power wireless network infrastructure mainly for long-term structural monitoring, and vehicle-to-everything (V2X) communication infrastructure for vehicle-to-vehicle and vehicle-to-infrastructure message passing. The research activities in both directions are summarized as follows:

For the low-power wireless network infrastructure, the research team has been conducting a thorough survey on representative low-power wireless technologies (such as 802.15.4(e)-based technologies, ultra-wideband (UWB), and Bluetooth/BLE), especially on their capabilities to provide real-time and secure data communication. Figure 1 shows the timeline of the development and standardization effort of the 802.15.4(e)-based technologies. The research team gives a thorough comparison among these technologies and summarizes the specific security requirements in low-power real-time wireless network technologies, including attack impact, secure channel, authentication, authorization, accountability and detection, and trust management. Security challenges at individual layers of the wireless protocols (from the physical layer to the application layer in a bottom up fashion) have been identified; the state-of-the-art countermeasures to combat these challenges and their drawbacks are also described and compared in details. Potential solutions are also proposed to address these drawbacks. A survey paper [1] (78 pages with 500 reference papers) is under preparation.

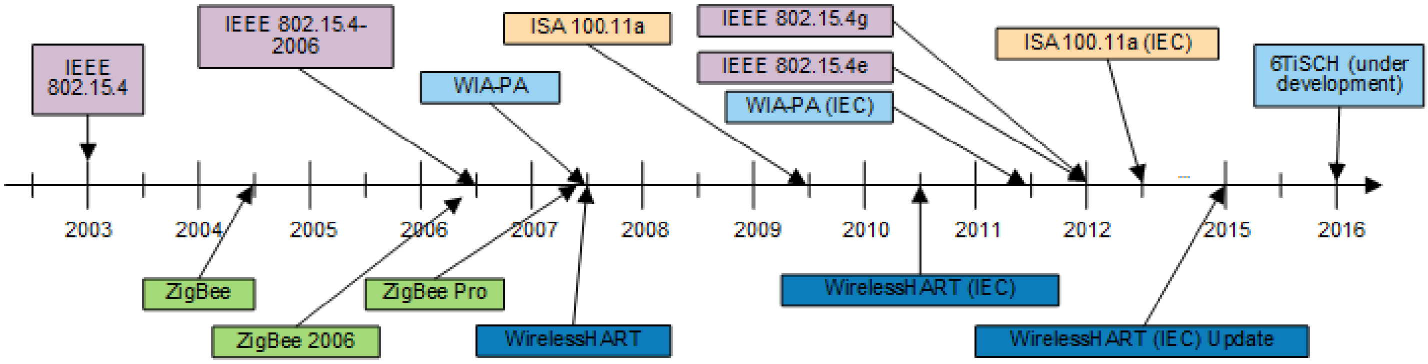

Figure 1: The timeline of the development and standardization of low-power wireless technologies

Among these studied low-power wireless technologies, the research team is particularly interested in the 6TiSCH technology which will become the first industrial IoT standard, and provides the seamless integration of OT (operational technologies) and IT (information technologies). RPL, the IPv6 Routing Protocol for Low-Power and Lossy Networks (LLNs), is used in 6TiSCH for resource-constrained wireless network routing. RPL however is vulnerable to internal routing attacks where compromised nodes may seek to exploit the vulnerability of the Rank value that represents the node's position relative to the root in the RPL graph. The impact of such attacks can be devastating, especially for real-time wireless networks where network-wide time synchronization needs to be maintained during system operation. To address this problem, during the reporting period of this project, one student member of the research team designed two complementary specification-based Intrusion Detection Systems (IDSs), ARM-Pro and FORCE, to protect the RPL topology from Rank-related attacks. ARM-Pro is a hybrid IDS, where the distributed and centralized modules are installed on all RPL nodes and the root, respectively, to identify Rank-related attacks. Unlike ARM-Pro, FORCE is a fully distributed IDS against Rank-related threats, where each node locally analyzes the received control messages from its neighbors and generates alerts upon the discovery of an intrusion. We are evaluating the performance of both IDSs using extensive simulations. The current findings demonstrate that they can effectively detect Rank-related attacks with a high detection rate, yet incurring only moderate computation and communication overheads. Fig.2 gives an example of the 6TiSCH network topology and Figure 3 describes different scenarios of Rank-related attacks.

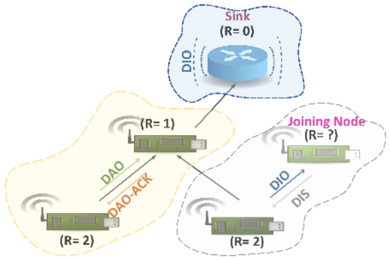

Figure 2: An Example of an RPL DODAG graph

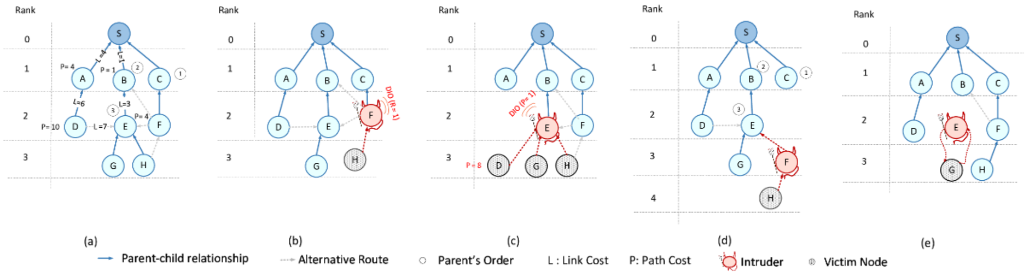

Figure 3: Different scenarios of Rank-related attacks: (a) Healthy RPL topology; (b) DR attack; (c) RAOF attack; (d) WPS attack; and (e) IR attack.

For the V2X communication infrastructure, the research team has been studying various wireless vehicular networking technologies. These technologies inlcude Long Term Evolution (LTE)-based V2X solutions and a variety of dedicated short-range communication (DSRC) standards for use in vehicle-to-vehicle and vehicle-to-roadside communication, such as IEEE 802.11p amendment for wireless access in vehicular environments (WAVE), the IEEE 1609.2, 1609.3, and 1609.4 standards for Security, Network Services and Multi-Channel Operation, the SAE J2735 Message Set Dictionary, and the emerging SAE J2945.1 Communication Minimum Performance Requirements standard. The possible integration of LTE-based technogloies and DSRC technologies are also being studied. Special attention is paid to the security aspects of these communication solutions, especially on the new threats that can emerge during the integration of different technologies. PI Han and Prof. Jonathan Rubin and Kathryn Ballingall from University of Maine have started the intial conversation on the possibility to collaborate on the cybersecurity study in the context of smart and connected bridge. PI Han also have reached out to the Ford Motor Company to study the safety issues and concerns in autonomous vehicles design and analysis. Two NSF proposals have been prepared on this direction during the reporting period. For example, PI Han has worked with Dr. Eric Jackson, the director of the Connecticut Transportation Safety Research Center (CTSRC) at UConn, on an NSF MRI proposal [3] to procure two autonomous vehicles (AVs) along with necessary software and support to conduct sensing and control, public perception, human behavioral, and human-machine interaction research that is needed to facilitate the integration of AVs into our existing transportation system. V2X communication modules will be depoloyed on the acquired AVs to study their connectivity and security issues in real-life scenarios. PI Han is also working with Prof. Mike Lemmon and Prof. Sharon Hu from University of Notre Dame on an NSF CPS proposal [4] to study fast and distributed mechanism design for routing and congestion management in smart highway systems.

Accomplishments: the accomplishments of this project during the report period include two paper drafts, one under preparation and one under submission. Two NSF proposals have also been prepared and are currently under submission.

[1] Gang Wang, Song Han, "Security Issues in Low-Power Wireless Networks: A Stack View", under preparation.

[2] Areej Althubaity, Tao Gong, Mark Nixon, Raymond Kim Kwang Choo, Reda Ammar, Song Han, "Specification-based Detection of Rank-related Attacks in RPL-based Resource-Constrained Real-Time Wireless Networks", submitted to the Special Section on Security, Privacy, and Trust for Industrial IoT in IEEE Trans. on Industrial Informatics, 2019.

[3] NSF MRI: Acquisition of Autonomous Vehicles Project, under submission, $1,120,200, 7/1/2019 – 6/31/2024.

[4] NSF CPS: Medium: Collaborative Research: Fast and Distributed Mechanism Design for Routing and Congestion Management in Smart Highway Systems, under submission, $1,200,000, 9/1/2019 – 8/31/2022.

Training/professional development opportunities: During the reporting period, two PhD students have participated in this research project. One PhD student, Mr. Gang Wang, mainly focuses on the literature survey of low-power wireless network infrastructure for structural monitoring, and pays special attention to the cybersecurity issues in such networks; the other PhD student, Ms. Areej Althubaity, mainly focuses on the IDS design for 6TiSCH wireless networks to identify Rank-related attacks. A new PhD student, Jiachen Wang, is also recruited and will be joining PI Han's research lab in the Fall semester 2019. He will dedicate on studying the cybersecurity issues in V2X infrastructure.

Dissemination of research results: PI Han attended and gave a presentation at the TIDC workshop held at Portsmouth, NH, during Nov. 8-9, 2018 to describe his research work in this project. PI Han also presented this work to CT DOT representative on Feb. 28th to ask for feedback from the domain experts. The PI is planning to visit the Ford Motor Company in the summer of 2019 to present his work to the autonomous vehicle division.

Participants and Collaborators:

PI Song Han, Assistant Professor, Department of Computer Science and Engineering, University of Connecticut

Student Researcher: Gang Wang, PhD student, CSE@UConn, secure low-power wireless network systems design
Student Researcher: Areej Althubaity, PhD student, CSE@UConn, IDS design for 6TiSCH networks
Potential Collaborator: Mr. Bing Ai, Research Engineer, Ford, studies of safety issues in autonomous vehicles

Changes:

No significant changes on the scope and methodology design in the project. Based on extensive literature study, the focused study subjects have been narrowed down from general transportation infrastructure to low-power wireless network infrastructure for structural monitoring and V2X communication infrastructures due to their importance and potential great impact to the US and State DOT and the whole transportation industry. Between these two directions, a higher priority will be given to the V2X communication infrastructure due to its increasing popularity and more challenging research problems whose solutions are still unknown to the research community.

Planned Activities:

Based on the study conducted in this reporting period, we are planning the following R&D activities in the project:

- Extending the literature study on the security issues in low-power wireless networks from 802.15.4(e)-based communication technologies to other technologies as well. This will make the literature study more complete and can cover most well-known wireless technologies designed for long-term structural monitoring. Based on these studies, the survey paper will be finalized and submitted to a prestigious journal in the field, including IEEE Transactions on Vehicular Technology, IEEE Transactions on industrial informatics, and IEEE Communications Surveys & Tutorials.
- A complete survey on existing V2X technologies will be conducted. Special attention will be paid on the potential issues of the existing solutions, their current countermeasures and drawbacks, and potential solutions to addresses these problems. We will study the potential solutions to integrate LTE-based and DSRC-based V2X technologies and the emerging connectivity and security issues during this integration. A complete survey paper is expected to be prepared by the end of the next reporting period and submitted to the prestigious journal as mentioned above.
- Among all the identified security issues during the literature survey on existing V2X technologies, one or two problems will be picked and studied in depth. How to select the research problem(s) will be based on the importance and severity of the problem(s), availability of the dataset and experimental infrastructure, and suggestions from DOT.
- PI Han plans to visit his collaborator, Mr. Bing Ai, at Ford Motor Company to present his previous and ongoing work in the designs of secure and real-time network fabric for cyber-physical systems and to discuss and understand better the safety issues that Ford is experiencing now in the designs of autonomous vehicles.
- PI Han will continue the conversation with Prof. Jonathan Rubin and Kathryn Ballingall from University of Maine to understand better the cybersecurity issues in the context of smart and connected bridge, and work on potential research problems that both UConn and U of Maine have mutual research and development interests.
- PI Han will start recruiting undergraduate students at UConn to join the PI's research lab to work with the PhD student researchers on R&D tasks related to this project. These undergraduate students will work with the PI in the form of either independent studies in the summer of 2019 or senior design project in the Fall semester of 2019.