Quarterly Progress Report:
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, Associate Professor and Castleman Term Professor in Engineering Innovation, Department of Computer Science and Engineering, University of Connecticut*
Reporting Period: *January 1st, 2021 – March 31st, 2021*
Submission Date: *April 1st, 2021*

Overview:

Our study in the previous reporting periods focuses on the intrusion detection system (IDS) design for insider attack. During this reporting period, we resume our study to look into novel authentication methods for low-power industrial wireless networks deployed in smart transportation infrastructures. In the literature, most authentication methods designed for such networks rely on key-based encryption methods. Those keys are either pre-installed or installed over the air. If the keys are leaked, tampered sensing data or control messages may ruin the entire system. In this work, our security model assumes that: 1) an attacker can intrude into the transportation infrastructure and deploy his evil device somewhere secretly; 2) this powerful attacker knows the key and can eavesdrop, replay and forge any communication; and 3) the attacker can block the communication from legitimate device but cannot remove or replace it with his evil device, otherwise it will be detected by the field operators. Based on this security model, the research team is studying how to utilize the background noise information in the field to authenticate the individual devices based on the fact that noise level and signal strength vary with locations. The key idea of our method is to design and train machine learning models for individual links so that if a packet is from an abnormal/unknown link, then it has a very high possibility to be identified as from the outside attacker. The research team are tackling the following three main challenges towards accomplishing this methodology design. 1) Environmental noise: link quality in low-power wireless networks may change significantly due to the environmental noise. Thus the developed models for individual links may need to be kept training or transfer/reinforcement learning methods need to be employed. 2) Topology change: even for the wireless networks deployed in the environment with limited noise/interference, devices may still change their parents during the operation to seek better connectivity. This will also make the pre-trained models ineffective. 3) Accuracy requirements: huge amount of traffic will be generated in such networks and even a 99.9% accuracy still means that hundreds of false alarms a day. The research team aims to address these above challenges in the following reporting period(s) and implement the solution on the UConn testbed to validate the design and evaluate the performance.

During this reporting period, the research team also continues to work on the development of the 6TiSCH real-time wireless network testbed. A software-defined radio (SDR)-based wireless interferer has been developed and tested. It will be mounted on the mobile robotic platform (Turtlebot 2) to form a mobile interferer in the 6TiSCH network testbed.

Table 1: Task Progress

Task Number	Start Date	End Date	% Complete
Task 1: Context establishment	Oct. 1st, 2018	Sept. 30th, 2019	100%
Task 2: Threat identification	Oct. 1st, 2019	December. 31st, 2020	100%
Task 3: Consequence identification and impact assessment	Oct. 1st, 2020	Sept. 30th, 2021	60% (some parts of Task 2 are concurrent with Task 3)
Overall Project	Oct. 1st, 2018	Sept. 30th, 2021	Around 85%

Table 2: Budget Progress

Project Budget	Spend – Project to Date	% Project to Date*
* The information will be provided by the Institutional Lead.		

Training/professional development: During the reporting period, the PhD student, Mr. Peng Wu, joins the research team to work on the authentication method design based on link quality information. He will replace Areej who successfully completed her defense on December 22, 2020. During this reporting period, Peng has been working with the PI on the literature review of existing methods, design the security model, and identify the key challenges towards the methodology design. He will also be advised by the PI to start the data collection from the testbed and design machine learning models for the proposed authentication method.

Dissemination of research results: During the reporting period, the research team mainly focuses on the methodology design and does not have paper or technical report published.

Table 3: Presentations at Conferences, Workshops, Seminars, and Other Events

Title	Event	Type	Location	Date(s)

Table 4: Publications and Submitted Papers and Reports

Type	Title	Citation	Date	Status

Participants and Collaborators:

Table 5: Active Principal Investigators, faculty, administrators, and Management Team Members

Individual Name	Email Address	Department	Role in Research
Song Han	song.han@uconn.edu	CSE@UConn	Principle Investigator

Table 6: Student Participants during the reporting period

Student Name	Email Address	Class	Major	Role in research
Peng Wu	PhD		Computer Science	Student Researcher

Table 7: Student Graduates

Student Name	Role in Research	Degree	Graduation Date

Table 8: Research Project Collaborators during the reporting period

Organization	Location	Contribution to the Project				
		Financial Support	In-Kind Support	Facilities	Collaborative Research	Personnel Exchanges

Table 9: Other Collaborators

Collaborator Name and Title	Contact Information	Organization and Department	Contribution to Research

Who is the Technical Champion for this project?

Name: Peter J. Calcaterra
Title: Transportation Planner
Organization: Connecticut Department of Transportation

Location (City & State): Connecticut
Email Address: Peter.Calcaterra@ct.gov

Changes: No significant changes on the scope and methodology design in the project.

Planned Activities: Based on the study in this reporting period, we are planning the following activities in the project:

- We will continue our work on the device authentication method design based on the channel-level RSSI information. Will also continue to work on the Turtlebot mobile platform. We plan to mount the software-defined radio (SDR)-based physical interferer on the Turtlebot mobile platform and traverse the network testbed to collect data for developing and training the machine learning models.

- We will continue to work on the literature review on security issues in industrial wireless networks.

- PI Han will recruit 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.