TIDC Transportation Infrastructure Durability Center
AT THE UNIVERSITY OF MAINE

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: *April 1st, 2021 – June 30th, 2021*
Submission Date: *July 26th, 2021*

Overview:

During this reporting period, we continue to work on the design of the novel authentication method for low-power wireless networks deployed in smart transportation infrastructures by utilizing the background noise information in the field. As presented in the last report, there are three main challenges towards accomplishing this methodology design. 1) The link quality in low-power wireless networks may change significantly due to the environmental noise, and thus the developed machine learning models for authenticating individual links may need to be kept training in the run time. 2) 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. 3) Huge amount of traffic will be generated in such networks and since the authentication accuracy may not reach 100%, many false alarms may present in the system.

The research team focuses on addressing the first challenge in this reporting period. We propose to construct fine-grained performance map on the SNR (signal noise ratio) of individual links by letting the wireless nodes collect SNR measures in the run time in a continuous fashion. Based on these samples, effective machine learning method, such as kernel-based learning, are being employed to approximate the SNR performance map over the entire deployment environment. Online algorithm is also under development to incorporate incremental data inputs instead of requiring all observations in batch.

During the reporting period, the research team also starts to investigate the vulnerability of wireless device binaries which may create security blind spots to have cybercriminals launch zero-day attack to comprise devices and data. Compared to software, device firmware is more notoriously insecure. This is because different from software which can be frequently updated with security patches, it is difficult and costly to add security patches to firmware once it is embedded in a device. The research team is now studying the literature of this topic and will continue this effort in the next reporting period.

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	70% (some parts of Task 2 are concurrent with Task 3)
Overall Project	Oct. 1st, 2018	Sept. 30th, 2021	Around 90%

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, works with the PI on the design of the authentication method for low-power wireless networks and on the literature survey for explorating wireless device firmware vulnerability. Peng Wu has also started to collect the SNR measures from the testbed to facilitate the machine learning algorithm design and performance evaluation.

Dissemination of research results: During the reporting period, the research team mainly focuses on the methodology design and literature survey 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

<u>Participants and Collaborators:</u>

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

<u>Changes:</u> No significant changes on the scope and methodology design in the project.

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

- We will continue to design the authentication method for low-power wireless networks based on the fine-grained SNR performance map.

- We will continue to work on the literature review on vulnerability of wireless device binaries.

- 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.