Project Title: Cybersecurity risk assessment in connected intelligent systems for designing resilient systems

Recipient/Grant (Contract) Number: Carnegie Mellon University, Grant #: 69A3552344811

Center Name: Safety21 National University Transportation Center for Promoting Safety

Research Priority: Promoting Safety

Principal Investigator(s): Zulqarnain Khattak Carnegie Mellon University

PI Contact: zkhattak@cmu.edu

Project Partners:

- Virginia Department of Transportation
- Oak Ridge National Laboratory (DOE)

Research Project Funding: $90,020.00

Project Start and End Date: 07-01-2023 to 06-30-2024

Project Description:

Cybersecurity refers to methods and practices designed for protection of networks, computers, programs, and data from attack, damage, or unauthorized access (1). Cybersecurity has emerged as threat in every field that relies on communications. Therefore, Transportation operation and management systems also utilize wired and wireless communications for managing roadways and are at significant risk of such cyberattacks. These systems were closed proprietary systems (isolated systems) in the past and had very limited cyber vulnerabilities. Those proprietary systems have now transformed into more open systems with increased accessibility (2) due to the emergence of network computing and reliance on emerging technologies such as internet of things (IoT), and connectivity. The National Transportation Communication for Intelligent Transportation Systems (ITS) Protocol (NTCIP) utilize center-to-center communications that rely on request-based protocols through XML messages (3). These protocols rely on the assumptions that most attacks are from the inside, and that hackers make up only a small portion of total intrusions, thus have no built in security (4). The U.S. DOT has also taken a huge initiative to develop a security credential management system (SCMS) (5) A message security solution for vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication. However, communication dependency opens up a wide array of access points, which makes these systems vulnerable to cyberattacks and the least understood in terms of cybersecurity. This proposal is based on the premise that perfect protection from cyberattacks is not realistic. Thus, the proposed research would focus on analyzing the vulnerability of cooperative driving relying on infrastructure- based communication from a real-field experimental data collected at the Aberdeen center in Maryland. Multiple cyberattacks including sensor anomalies, fake BSMs, replay and denial of service would be emulated. Furthermore, the driving conditions from the field experiment would be emulated within a realistic simulation environment to test the consequences of different types of cyberattacks on safety effects of transportation systems and analyze crash types and severity. Long short-term memory with Gaussian mixture (LAGMM) model would be utilized to design efficient and effective anomaly detection method for accounting the temporal relations of trajectories, so that anomalous behavior can be detected in real-time and the severe consequences of cyberattack or sensor anomalies can be avoided. Ultimately, the research would develop a real-time threat-monitoring system to continuously check to see if the system is behaving as expected and degrade the system to a safe state under cyberattacks.

- Description
- Research Approach

Task 1. Cyberattack emulation using real world data from cooperative driving The cyberattack anomalies would be emulated due to lack of publicly available anomalous CAV sensor data. The sensors to be considered have been shown to have vulnerability to cyberattacks and sensor failures by past research (10-12). A reasonable subset of likely attacks would be subjected to a detailed investigation through a series of case studies using the available sensor data. The cyberattacks would be selected based on a higher probability for an attacker to launch these attacks, the ability to compromise CAV operation and safety, and a requirement that the attack needs a reasonable level of expertise and cost. Some examples of the types of attacks to be considered include.

1. Senior anomalies.

2.Infrastructure elements compromised by attacks at the V2I communication.

3. Communication at the vehicle level compromised by attacks at the network level (V2V). With regards to sensor anomalies, three types of attacks would be considered. For instance, a fake data injection attack through CAN bus or on-board diagnostic (OBD) can compromise the in- vehicle speed and acceleration sensors and result in several sensors anomalies. Likewise, an adversary with valid credentials can spoof the GPS through jamming or GPS spoofing attack and compromise the sensor values, thus generating anomalies. Further, an acoustic injection attack can compromise the acceleration sensor and generate anomalies. Furthermore, three types of attacks requiring communication access would be selected for the case studies: fake BSM initiated by spoofing, sybil to access beacons and generate fake messages/BSMs to other surrounding vehicles, replay attack initiated when data packets stored at a previous instance of time are repeated maliciously or replayed, and denial of service attacks which ceases the control inputs and are initiated by sending excessive data packets and flooding the communication channel. The denial-of-service attack results in having no communication of advisories and is similar to jamming attacks. These anomalies would be injected into CAV sensors. The initiation of sensor anomalies due to attacks or sensor failure would be assumed as independent. A single anomaly would be assumed in one time epoch due to independent nature of attacks or faults in sensors and reliability of sensors. Multiple rates alpha including 1%, 5% and 10% would be used to generate several anomalous datasets. The anomalies would be randomly simulated with random sensors. The simulated anomalies would then be added to the base or normal sensor values of the compromised sensor (within lead vehicle or follower). The anomaly types and durations would be varied for instance, anomaly to be simulated for 5mins, 20 mins etc.

Further, mixed anomaly type would also be considered for testing sensitivity, which includes multiple anomalies mixed together.

Task 2. Assessment of Cyberattacks Influence and Anomaly Detection The stability, safety, and privacy of cooperative driving can be severely compromised by all levels of attacks. The conditions from field experiments at Aberdeen Center would be emulated within simulation environment using the available data. The ACC only scenario includes both lead vehicle (LV) and following vehicle (FVs) in ACC mode. The FV speed was set higher than the LV. All vehicles within the group are expected to maintain speed and car following through sensors. The hybrid mode has CACC in LV and ACC mode in FVs. The first LV operates on CACC communication and is a representation of I2V CACC, which receives a reference target speed from the waypoints. Thus, the LV operates using CACC speed and acceleration limits. LV would be controlled automatically to match the set speed, so the LV speed is more stable, which also makes it easier for the FVs to stabilize their speeds.
However, the FVs would operate on ACC control and maintain speed and following distance by only considering the information it receives from its sensors. The CACC mode, where all vehicles follow CACC is a representation of V2V CACC and would govern vehicle following within the platoon in the third scenario. The target speed would control LV while the FVs observe time gap mode via dedicated short-range communication (DSRC) commands.
The scenarios of field experiment within simulated environment would be used to assess the consequences of the aforementioned cyberattacks on system wide performance. Traffic conflicts as defined by (13) “When movement of two or more vehicles remains unchanged as they approach each other, and there is a risk of collision” would be used to assess the safety impact of cyberattacks. The premise behind the use of surrogate safety assessment is that conflicts are more frequent than crashes and can provide a more proactive approach to safety risk assessment since both events have a comparable mechanism. Real crash data from VDOT would be used to validate the observed crash risk. Furthermore, network wide stability would also be assessed from the emulated cyberattacks. Multiple scenarios would be considered including cyberattack on a single vehicle and cyberattack on platoon of vehicles.
The influence of cyberattacks on the lead vehicle as well as cyberattacks on the followers would be assessed.

Task 3: Anomaly Detection and resilience This task would further aim at detecting falsified CAV trajectories from normal CAV trajectories. Considering the aforementioned attack scenarios, falsified trajectories would be generated with four anomalies, the proposed LAGMM consists of two major components: (1) a compression network aiming at generating low-rank approximation for input data by a LSTM autoencoder, which concatenate reduced space features with reconstruction error features, (2) a GMM model to predict likelihood/energy. Given the low rank approximation of the input data, the GMM-based estimation network aims at estimating the density function. The unknown parameters in GMM are mixture component distribution, mixture means Ãµ, and mixture covariance. A multi-layer neural network (MLNN) would be leveraged to predict the mixture membership of each sample data. In the testing process, the sample energy estimated from Gaussian mixture model will be used to predict if the sample data is composed of falsified trajectories or not. Higher energy would indicate a higher probability of anomalies. The LSTMs would be trained to learn normal behaviors. Predictions would be generated at each time step and the prediction errors would indicate the deviations from normal behaviors.
Then a clustering approach would be applied to detect anomaly. Once the anomaly is detected, the system architecture would isolate the anomalous data and operate the system based on redundant historical data termed as normal. This redundancy would allow the system to perform resiliently even under cyberattacks.

Outputs:

-Methodology for emulating different sensor anomalies and cyberattacks based on driving conditions of real-world experiment to assess safety effects of transportation systems; analyze crash types and severity.

-Monitoring system and anomaly detection based on long short-term Gaussian mixture model to detect multiple cyberattacks and revert the cooperative driving to a safe state. -Large-scale cyberattack data for safety assessment with evolving sensor anomalies.

Outcomes/Impacts:

The following outcomes are anticipated:

- Findings would assist state and other agencies with real-world implementation for deployment of the monitoring architectures developed in this research at traffic management centers for detecting anomalies within real-world transportation networks.

- Allow resilient operation of the connected systems under sensor anomalies or cyberattacks.

- Understand the negative impacts of cyberattacks and improve cooperative driving for safer transportation systems.