
Efficient Intrusion Detection and Privacy Protection Systems to Enhance Cooperative-Intelligent Transportation System (C-ITS) Survivability

---

Host institution: Université de Bourgogne Franche-Comté

Laboratory: DRIVE Laboratory, Nevers

Domain: Computer sciences

Discipline: Networking, Cyber Security

Doctoral school: Sciences physiques pour l'ingénieur et microtechniques - SPIM - ED 37

Context of the PhD thesis:

The great evolution of communication technologies together with the variety and potential availability of network access mediums and service providers have led to the appearance of the Cooperative Intelligent Transportation Systems (C-ITS). C-ITS is based on type of machine-to-machine communication: The basic idea is that vehicles inform their environment about their behavior and in return receive information about their direct environment, through so-called cooperative awareness messages (CAM). If the analysis of the CAM detects an event, a so-called decentralized environmental notification message (DENM) is sent to warn of a risk.

The aim of safety messages is to make vehicles aware about their surrounding environment, which significantly improves road safety. For example, using these messages, vehicles can expect or detect dangerous situations that can cause serious damages on VANETs such as collisions and accidents. As a result, vehicles can then make decisions to prevent such bad consequences. However, although, safety messages are beneficial for road safety, they may also be exploited by adversaries such as passive and active attackers. While the passive attacks seriously impair the confidentiality and privacy of the network, the active attacks can damage the network resources and functioning, by inserting, deleting or modifying the exchanged packets. An active attacker could send authenticated DENM messages that contain false information. However, neighboring nodes could detect this misbehavior by simple observing the physical environment (displacement of the attacker, etc.).

To this end, it is essential to have robust intrusion detection and recovery mechanisms that permit to monitor the system and exclude active attackers and also robust privacy protection mechanisms that permit to preserve the drivers' privacy.

Description of the work:

The introduction of C-ITS exposes the transportation system to new vulnerabilities, such as cyber-attack. In fact, if a physical device is connected to the Internet, it can be targeted with a cyber attack. In order to ensure that C-ITS fulfills its potential, it is imperative that those implementing such systems design and operate them to survive cyber-attacks and other information technology-related threats. Attacking the transportation infrastructure can now be accomplished by attacking these C-ITS information systems in a manner similar to how computer hackers attempt to break into other information systems. These new threats require the set up of new architectures, access control mechanisms and particularly monitoring facilities to detect suspicious behaviors (potentially intrusions) and if necessary to take defensive actions to eliminate or limit the impact of these cyber attacks in the origin of these misbehaviors.

Cryptography and intrusion detection systems (IDS) are two major security mechanisms. On one hand, cryptography is used to ensure message privacy and node authentication, and is used to prevent external intruders to penetrate the network. On the other hand, IDS uses special agents to monitor the behavior of a target node and trigger an alarm when a malicious anomaly is detected.

This thesis proposes to focus on IDS and privacy protection systems to enhance C-ITS Survivability. The main issues are:

- Detection policies (signature based detection, anomaly detection and hybrid detection technique) to prevent the active attacks to occur with objective to reduce the false positive and false negative rates. For anomaly detection, a specific focus on will be done on machine learning (Deep learning, Game theory, reinforcement learning, etc.). Intrusion detection tools already exist in conventional IT installations, but their adaptation to transport systems still poses some theoretical and technological difficulties. In fact, misbehaving active attackers in transport systems are different since we are in a physical-cyber system where any cyber failure can have a direct influence on safety of operation, so potentially can create threats to human life and cause materials damage.
- Recommendation and recovery policies from active attacks in order to enhance the ITS survivability. All responses to attacks must take into account the availability of functionalities considered as critical for a safe operation since a simple revocation/eviction, as proposed in the literature, has no influence on the behavior of a vehicle.
- Privacy protection mechanisms to prevent passive attacks. Indeed, due to the nature of the wireless medium, a passive adversary can easily eavesdrop all the broadcasted safety messages within its region of interest. It can then collect these safety messages and determine the locations visited by vehicles over time. The location tracking of vehicles could violate drivers' privacy since one vehicle is usually associated only with one driver. The privacy in C-ITS must be conditional, where vehicles are anonymous to all ITS participants except the authorities, which must still track them. In order to meet these requirements, many anonymous authentication schemes have been proposed and the most used one is the pseudonymous authentication scheme. However, due to the pseudonyms linking attack, a simple changing of pseudonym have shown to be inefficient to provide the required protection. For this reason, many pseudonym changing strategies have been suggested to provide an effective pseudonym changing. Unfortunately, the development of an effective pseudonym changing strategy for VANETs is still an open issue. Hence, the idea is to propose new mechanisms based on adaptive pseudonym authentication.
- Take into account the requirements of hardware or /and system where these mechanisms are launched (mobility model, data model, resource limitation, communication network specificities, environment deployment, large/small scale, distributed/centralized, real time or not, etc.).

Bibliography:

1. Gerard Le Lann. Protection de la vie privée, innocuité et immunité envers les cybermenaces dans les futurs réseaux de véhicules autonomes connectés. C&ESAR 2017 - Protection des données face à la menace cyber, Nov 2017, Rennes, France. pp.1-21.
2. A. Boualouache, S. M. Senouci and S. Moussaoui, "A Survey on Pseudonym Changing Strategies for Vehicular Ad-Hoc Networks," in IEEE Communications Surveys & Tutorials, vol. 20, no. 1, pp. 770-790, Firstquarter 2018. doi: 10.1109/COMST.2017.2771522
3. E. B. Hamida, H. Noura, and W. Znaidi, "Security of cooperative intelligent transport systems: Standards, threats analysis and cryptographic countermeasures," Electronics, vol. 4, no. 3, pp. 380–423, 2015.
4. H. Sedjelmaci, SM. Senouci, T. Bouali, "Predict and Prevent From Misbehaving Intruders in Heterogeneous Vehicular Networks", Vehicular Communications journal (Elsevier), 21 December 2016.
5. T. Bouali, SM. Senouci, H. Sedjelmaci, "A Distributed Detection and Prevention Scheme from Malicious Nodes in Vehicular Networks", International Journal of Communication Systems (Wiley), January 2016, DOI: 10.1002/dac.3106.

Keywords: IDS, Game theory, Reinforcement learning, Security, Privacy, Confidentiality, Algoritms, Matlab.
PhD contract: Bourse MESR (Ministère de l'enseignement supérieur et de la recherche).
PhD location: This PhD will take place in the premises of the engineering school ISAT and its research laboratory DRIVE located in Nevers, France.
Expected starting date: October/November 2018.
Contacts: Professor, Sidi Mohammed Senouci, Sidi-Mohammed.Senouci@u-bourgogne.fr
Expected Profile: Candidates should own a Master (M.Sc.) or Engineer (B.Sc.) degree in Computer science or Telecoms. Good mathematical background and networking protocols and cyber-security as well as practical skills with programming languages and software tools (e.g., Matlab, NS-3, OMNET++) and fluent English (written and spoken) are required. Above all, the applicants must be motivated to learn quickly and work effectively on challenging research problems.
How to Apply: Application process (Until the position is fulfilled. Deadline June 2018). The following documents are required:
- CV,
- motivation letter,
- statement of research experience and interests,
- transcripts of University transcripts and
- (at least) two reference letters

as attachments of an email, whose subject will be "Application for PhD position University of Bourgogne", which must be addressed to Sidi Mohammed Senouci (sidi-mohammed.senouci@u-bourgogne.fr). Web links of research articles authored by the applicant or the internship report are welcome to be included, too.