ICMS Chair
Axis 2: Intrusion and abnormal behavior detection

PhD Proposal :
"On board analysis of detection events based on Embedded ML/AI for SDV"

G. Duc[1], L. Rinn[2], and V. T. Nguyen[1]
[1] Telecom Paris / IP Paris,
[2] Ampre / Renault

Keywords: AI for IDS, Cybersecurity, Software-Defined Vehicle, Connected Car

Context :

Vehicles are increasingly connected in a complex, multi-player and diversified connectivity ecosystem (cellular, WiFi, BT, V2X). They are equipped with increasingly advanced driver assistance systems (ADAS), which will eventually take the driver's hands off the wheel and his or her eyes off the road (L3), giving the car autonomy in defined mission conditions (type of road, speed, etc.).

It will therefore become increasingly important to equip the car with attack detection and reaction capabilities to increase its resilience and keep the vehicle and its systems in an acceptable functional mode until the systems return to their nominal mode.

The vehicle's reaction must be proportionate to the type of attack, and in the case of certain attacks associated with assisted driving situations, the reaction must be close to real time. The aim is to ensure that the alert sent back by the car's sensors is a true positive and not a false positive, at the risk of applying an inappropriate remedy.

Connected vehicles present significant cybersecurity risks. Indeed, a connected vehicle has numerous communication channels (internal Ethernet or CAN bus linking the various on-board ECUs, wireless link with certain sensors such as those measuring tire pressure, WiFi or BT link with the driver's and/or passenger's peripherals, 3G/4G/5G link with the Internet, wireless link with other vehicles and the infrastructure...). These communication channels are all points of entry for a potential adversary.

In addition, these vehicles offer more and more services (driving assistance, multimedia, etc.), making their hardware and software architecture increasingly complex. This increased complexity also introduces an additional risk of security flaws.

The combination of this increased complexity and the numerous communication channels that can be exploited by an adversary has a strong impact on the overall cybersecurity risk of these vehicles.

Numerous cybersecurity solutions are developed and integrated into these vehicles, right from the design phase, to reduce the overall risk. However, not all attacks can be taken into account during vehicle design (for example, an attack may have been considered too difficult or too costly at the outset, but has become more accessible with the evolution of attack techniques, or a new class of attack, totally unknown at the time of vehicle design, may emerge) and it is necessary to be able to dynamically detect, during vehicle operation, abnormal vehicle behavior, which may be a symptom of an attack in progress.

New vehicle architectures are of the SDV (Software Defined Vehicle) type. Functions previously performed by several ECUs are now grouped together on a smaller number of more powerful ECUs, hosting several functions in software form running on virtual machines.

State-of-the-art :

Cyber-attacks on vehicle ECUs are detected either by monitoring processes and exchanges on the ECU's internal bus, or in most cases by monitoring exchanges on the intra-vehicle network (CAN, LIN, Ethernet) and detecting intrusion (IDS: intrusion detection system) on this network [1]. The intra-vehicular network includes a large proportion of CAN, which is inherently insecure (no authentication, no encryption, broadcast transmission, prioritization by frame ID, etc.) for reasons of real-time efficiency, and is therefore highly vulnerable [2], except for safety messages between ECUs under the gateway which benefit from MAC authentication (message authentication code). This network is therefore very important to monitor for intrusion detection.

Intrusion detection strategies on a network can be divided into four families [3] : Signature detection [4] ; Parameter tracking [5] ; Information theory [6] ; and Machine Learning [7]. As far as machine learning is concerned, there are several types of approach, depending on the data used for detection (frequencies, time sequences, message content, or mixed) and the AI techniques (supervised, unsupervised, self-supervised learning [8]). Some approaches use AI techniques originally developed for natural language processing, such as LSTM, as messages follow certain sequences [9]. As message sequences are similar to word sequences, GPT (generative pretrained transformer) approaches have been used to learn benign message patterns [10].

Unsupervised machine learning approaches for detecting anomalies on the CAN bus generally learn from a benign, attack-free dataset, which constitutes the nominal operating envelope. The model is then able to detect the majority of events outside this learned envelope [11] by setting thresholds. Supervised approaches, on the other hand, require datasets containing attacks [9].

Many challenges remain unresolved, and the research field is active. Many studies use a very limited number of frame IDs [12], and therefore cannot be applied to a real vehicle. False-positive rates (of the order of several %) and false-negative rates, as well as the time and resources required for detection, are also major issues. Many of the approaches being explored are not embeddable, such as resource-hungry message autoencoders [13]. Embeddability, but also the updating of detection models over the lifetime of vehicles and when architectures evolve for new vehicles, are unresolved issues.

Public datasets of exchanges on CAN networks and attacks on these networks exist [OTIDS, SynCAN] and are used in the literature, as are datasets for Ethernet networks [CIC-IDS2017]. They would enable new approaches to be developed and easily compared with published approaches. An important challenge will be to evaluate performance on more realistic datasets, which have yet to be built, in comparison with those on public datasets.

Scientific objectives and challenges:

The final objective of the Ph.D thesis is to develop a system for detecting abnormal behavior inside an SDV vehicle. This detection system will not collect raw data (e.g. messages exchanged between ECUs), but events generated by existing monitoring systems. These events will be processed using AI methods.

The purpose of this treatment is to :

- Mainly, to deliver a constant, controlled flow to offboard to provide the cloud AI with the data it needs to monitor vehicles ;

- Opportunity to provide a detection with zero false positives to trigger a reaction from the autonomous vehicle. The triggering of the reaction can be conditioned by formal rules.

This detection mechanism must take into account the constraints of embedded systems: limited computing and memory resources.
We will also be working on the software parameters to be observed on ECUs, in particular on system calls, in order to go beyond the simple white/black list mechanism.
The challenges are as follows:

- Specification of requirements and construction of datasets
- Relevant AI/ML algorithms with boundary conditions
- Sensitivity and scalability to changes in architecture
- Transposability between Ethernet and CAN networks
- Updating the model over the life of the vehicle
- Strategy for the model when new and undetected attacks are discovered
- Embeddability (model size, computing and memory resources required, response time)

Work plan :

1) State of the art of intrusion and attack detection on SDV based vehicle
2) Construction of datasets and comparison with public datasets
3) Proposition of AI/ML algorithms
4) Performance and limits of the model, benchmark against the state of the art
5) Embeddability conditions and strategy for software and architecture upgrades
6) Thesis Writting and Defense

References :

[1] Rajapaksha, Sampath, et al. "AI-based intrusion detection systems for in-vehicle networks: A survey." *ACM Computing Surveys* 55.11 (2023): 1-40.
[2] Kim, Kyounggon, et al. "Cybersecurity for autonomous vehicles: Review of attacks and defense." *Computers & security* 103 (2021): 102150.
[3] Wu, Wufei, et al. "A survey of intrusion detection for in-vehicle networks." *IEEE Transactions on Intelligent Transportation Systems* 21.3 (2019): 919-933.
[4] Zhao, Yilin, Yijie Xun, and Jiajia Liu. "ClockIDS: A real-time vehicle intrusion detection system based on clock skew." *IEEE Internet of Things Journal* 9.17 (2022): 15593-15606.
[5] Song, Hyun Min, Ha Rang Kim, and Huy Kang Kim. "Intrusion detection system based on the analysis of time intervals of CAN messages for in-vehicle network." *2016 international conference on information networking (ICOIN)*. IEEE, 2016.
[6] Marchetti, Mirco, et al. "Evaluation of anomaly detection for in-vehicle networks through information-theoretic algorithms." *2016 IEEE 2nd International Forum on Research and Technologies for Society and Industry Leveraging a better tomorrow (RTSI)*. IEEE, 2016.
[7] Zhao, Yilin, et al. "GVIDS: A reliable vehicle intrusion detection system based on generative adversarial network." *GLOBECOM 2022-2022 IEEE Global Communications Conference*. IEEE, 2022.

[8] Song, Hyun Min, and Huy Kang Kim. "Self-supervised anomaly detection for in-vehicle network using noised pseudo normal data." *IEEE Transactions on Vehicular Technology*70.2 (2021): 1098-1108.
[9] Hossain, Md Delwar, et al. "LSTM-based intrusion detection system for in-vehicle can bus communications." *Ieee Access* 8 (2020): 185489-185502.
[10] Nam, Minki, Seungyoung Park, and Duk Soo Kim. "Intrusion detection method using bi-directional GPT for in-vehicle controller area networks." *IEEE Access* 9 (2021): 124931-124944.
[11] Seo, Eunbi, Hyun Min Song, and Huy Kang Kim. "GIDS: GAN based intrusion detection system for in-vehicle network." *2018 16th Annual Conference on Privacy, Security and Trust (PST)*. IEEE, 2018.
[12] Hanselmann, Markus, et al. "CANet: An unsupervised intrusion detection system for high dimensional CAN bus data." *Ieee Access* 8 (2020): 58194-58205.
[13] Novikova, Elena, et al. "Autoencoder anomaly detection on large CAN bus data." *Proceedings of DLP-KDD* (2020): 9.