Title: Advanced Artificial Intelligence for detecting V2X Slicing Attacks

Context:

The Ph.D. position is proposed by the DRIVE lab of the University of Bourgogne Franche Comté, located in Nevers Magny-Cours in France. Staffed by ca. 60 community members of which ca. 30 researchers and ca. 20 PhD. students, the DRIVE laboratory develops high-level applied and fundamental research with cutting-edge equipment. The research work encompasses 2 areas of specialism: intelligent systems with energy optimization as well as mechanics of materials and structures. This work will be done in the context of 5G-INSIGHT (Intelligent orchestrated security and privacy-aware slicing for 5G and beyond vehicular networks), an international ANR research project between France and Luxembourg. This project will deal with different use cases and attack scenarios in the context of 5G vehicular Slicing. The student will actively contribute to the project and will be co-supervised by both DRIVE lab (France) and SECAN-LAB (Luxembourg).

Scientific context:

5G vehicular networks offer interesting applications ranging from safety-related applications to comfort applications. However, 5G Vehicular networks are not only vulnerable to traditional attacks but also to more sophisticated attacks brought by enabling network slicing feature to 5G vehicular networks. Network slicing creates multiple logical instances of the physical network, the so-called network slices, ensuring strict traffic isolation among them, and tailoring the network resources of each slice to a specific (class of) application by leveraging the concepts of software-defined networking (SDN) and network functions virtualization (NFV). It has the potential to enable the coexistence of a wide range of mobile services in the same network infrastructure. Thus, enabling V2X slicing has brought new security requirements and challenges, which have been addressed neither by 5G standards nor by automotive standards. Indeed, new slicing attack vectors will be added to traditional attacks on vehicular networks, which might jeopardize their adoption. Vehicular slicing attacks will exploit that weak point of the slicing chain, the vehicles, to violate the slice isolation and deteriorate its performance. This might lead to dangerous road situations both for drivers and passengers. Attacks on vehicular slicing can be more powerful, especially if they will be combined with internal attacks, which are themselves not easy to detect.

Misbehavior Detection Systems (MDSs) have proven their efficiency to detect internal attacks in traditional vehicular networks, which make them suitable to detect the emerging V2X slicing attacks. MDSs generally use two detection mechanisms: (i) node-centric: this mechanism is primarily interested in nodes (vehicles or gNodeB), and (ii) data-centric: this mechanism is primarily interested in data rather than nodes. Most proposed MDSs adopt a combined approach where a node-centric mechanism is used to evaluate nodes according to the correctness of the exchanged data, while the correctness of data is verified using a data-centric mechanism. However, the current proposed MDSs for 5G vehicular networks are still having open issues, especially on how to ensure a high detection ratio and low false positive while providing privacy protection. In addition, novel techniques should be developed not only for thwarting the new vector of V2X slicing attacks but also for predicting zero-day attacks.

Artificial intelligence is witnessing huge development breakthroughs promising an efficient solution for the network security domain. Indeed, advanced machine learning approaches such as deep learning, transfer learning and federated are real opportunities to develop sophisticated MDSs for 5G vehicular networks.

Main activities

The thesis aims at proposing an advanced machine learning-based framework and techniques for detecting and predicting V2X slicing attacks within the context 5G-INSIGHT considering the case of cross-border areas (i.e., the France-Luxembourg border-crossing case).

In this thesis, the PhD student will start studying state-of-the-art misbehavior detection systems to highlight the limitations of the current solutions facing V2X slicing attacks. He/She will also be involved in generating real and simulated attack data sets in the scope of cross-border scenarios using testbeds, and/or trial sites, and/or network simulators. Data sets will be serving as input to develop advanced machine learning models for attack detection. The student will adopt different machine learning approaches according to the V2X slicing attack properties. He/She will train deep learning models to develop detection mechanisms. He/She will also investigate the transfer learning paradigm for the generalization of the developed ML models. Detection mechanisms should consider privacy preservation. In this vein, the PhD student will consider federated learning in the design of the security architecture. The student will validate proposed solutions in the 5G-INSIGHT Proof-of-Concept.

Key words: 5G Vehicular Networks, Network Slicing, Security and Privacy, Edge-Computing, Software Defined Networking (SDN), Virtual Network Function (VNF) Advanced machine learning, Game theory.

PhD contract: 3 years CDD-FR.

PhD location: This PhD will take place in the premises of DRIVE Lab in Nevers (Bourgogne Franche Comté, France), in cooperation with the University of Luxembourg.

Expected starting date: September/October 2021.

Contacts:

Sidi Mohammed Senouci, University of Burgundy, Nevers, France.

Abdelwahab Boualouache, University of Luxembourg, Luxembourg

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 as well as practical skills with programming languages and software tools (e.g., Python, Matlab, SUMO, OMNET++) and fluent English (written and spoken) are required. Above all, the applicant must be motivated to learn quickly and work effectively on challenging research problems.

How to Apply:

Application process (deadline **june 2021**).
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 5G INSIGHT", which must be addressed to Sidi Mohammed Senouci (sidi-mohammed.senouci@u-bourgogne.fr) and Abdelwahab Boualouache (abdelwahab.boualouache@uni.lu).

Web links of research articles authored by the applicant or the internship report are welcome to be included, too.

References

[1] Lu, Rongxing, et al. "5G vehicle-to-everything services: Gearing up for security and privacy." *Proceedings of the IEEE* 108.2 (2019): 373-389.

[2] Cunha, V. A., da Silva, E., de Carvalho, M. B., Corujo, D., Barraca, J. P., Gomes, D., ... & Aguiar, R. L. (2019). Network slicing security: Challenges and directions. *Internet Technology Letters*, *2*(5), e125.

[3] R. W. van der Heijden, S. Dietzel, T. Leinmuller, and F. Kargl, “Survey on misbehavior detection in cooperative intelligent transportation systems,” IEEE Communications Surveys & Tutorials, vol. 21, no. 1, pp. 779–811,2018.

[4] Tang, Fengxiao, et al. "Future intelligent and secure vehicular network toward 6G: Machine-learning approaches." *Proceedings of the IEEE* 108.2 (2019): 292-307.

[5] Samarakoon, S., Bennis, M., Saad, W., & Debbah, M. (2019). Distributed federated learning for ultra-reliable low-latency vehicular communications. *IEEE Transactions on Communications*.

[6] Boualouache, Abdelwahab, Ridha Soua, and Thomas Engel. "SDN-based Misbehavior Detection System for Vehicular Networks "The 2020 IEEE 91st Vehicular Technology Conference: VTC2020-Spring, IEEE, 2020.