5G Vehicle-to-Everything at the Cross-Borders: Security Challenges and Opportunities

Abdelwahab Boualouache, Bouziane Brik, Qiang Tang, Abdelaziz Amara Korba, Sylvain Cherrier, Sidi-Mohammed Senouci, Enric Pardo, Yacine Ghamri-Doudane, Rami Langar, Thomas Engel

5G Vehicle-to-Everything at the Cross-Borders: Security Challenges and Opportunities

Abdelwahab Boualouache*, Bouziane Brik**, Qiang Tang+, Abdelaziz Amara Korba++‖, Sylvain Cherrier‡, Sidi-Mohammed Senouci**, Enric Pardo+, Yacine Ghamri-Doudane++, Rami Langar‡§, and Thomas Engel*

* FSTM, University of Luxembourg, Luxembourg. Email: {firstname.lastname}@uni.lu

** DRIVE EA1859, University of Bourgogne Franche Comté, France. Email: {firstname.lastname}@u-bourgogne.fr

+ ITIS, Luxembourg Institute of Science and Technology (LIST), Luxembourg. Email: {firstname.lastname}@list.lu

++ L3I Laboratory, University of La Rochelle, France. Email: {firstname.lastname}@univ-lr.fr

‖ LRS, Badji Mokhtar Annaba University, Algeria.

‡ LIGM - UMR 8049, University Gustave Eiffel, France. Email: {firstname.lastname}@univ-eiffel.fr

§ Software and IT Engineering Department, École de Technologie Supérieure (ÉTS), Montréal, QC H3C1K3, Canada. Email: {firstname.lastname}@etsmtl.ca

***Abstract*—5G Vehicle-to-Everything (5G-V2X) communications will play a vital role in the development of the automotive industry. Indeed and thanks to the Network Slicing (NS) concept of 5G and beyond networks (B5G), unprecedented new vehicular use–cases can be supported on top of the same physical network. NS promises to enable the sharing of common network infrastructure and resources while ensuring strict traffic isolation and providing necessary network resources to each NS. However, enabling NS in vehicular networks brings new security challenges and requirements that automotive or 5G standards have not yet addressed. Attackers can exploit the weakest link in the slicing chain, connected and automated vehicles, to violate the slice isolation and degrade its performance. Furthermore, these attacks can be more powerful, especially if they are produced in cross-border areas of two countries, which require an optimal network transition from one operator to another. Therefore, this article aims to provide an overview of newly enabled 5G-V2X slicing use cases and their security issues while focusing on cross-border slicing attacks. It also presents the open security issues of 5G-V2X slicing and identifies some opportunities.**

***Index Terms*—5G-V2X, B5G, Network slicing, Cybersecurity, Cross-border areas.**

I. Introduction

5G and beyond networks (B5G) are rapidly evolving in our daily life as the key enablers of Vehicle-to-Everything (V2X) communications. 5G-V2X offers various communication types, namely among vehicles (Vehicle-to-Vehicle (V2V)), between vehicles and an infrastructure (Vehicle-to-Infrastructure (V2I)), remote servers (Vehicle-to-Network (V2N)), even Vulnerable Road Users (VRUs) such as pedestrians and bikers (Vehicle-to-Pedestrian (V2P)) respectively. Specifically, B5G New Radio (NR) harnesses Uu and PC5 radio interfaces for V2X communications. While the Uu radio interface is used for V2N communications, the PC5 radio interface (sidelink) can enable direct V2V, V2P, and V2I communications in the infrastructure coverage and out of the coverage for V2V and V2P [1]. 5G-V2X communications are expected to play a vital role in developing the automotive industry by supporting different new use-cases, including safety, non-safety, and infotainment use-cases, such as fully automated driving, cooperative maneuvering, teleoperation, and cooperative perception [2]. These Use Cases (UCs) come with various requirements, such as ultra-low latency, high communication reliability, high bandwidth, support for a massive number of Connected and Automated Vehicles (CAVs), and reliable Connectivity under high-mobility conditions [2]. Deployment of these UCs will only be possible in the long term with the widespread adoption of B5G technologies, including NS, Software-Defined Networking (SDN), and Network Functions Virtualization (NFV) paradigms [3].

NS enables multiple independent, virtualized logical networks to be built on top of a common physical network infrastructure, leveraging SDN and NFV technologies. Each network slice is an isolated end-to-end network

tailored to provide different requirements that a particular vehicular application needs. Hence, the NS concept has the potential to enable the coexistence of a wide range of vehicular applications sharing a common network infrastructure. However, enabling NS in V2X has brought new security challenges and requirements, which have not been addressed yet, either by automotive standards [4] or by 5G standards [5]. NS adds new attacks in addition to traditional attacks on V2X. Attackers may exploit the weakest link in the slicing chain, CAVs, to violate the slice isolation and degrade its performance. This can therefore lead to dangerous situations for passengers and drivers. Moreover, the attacks on vehicular slicing can be more significant, especially if they occur in cross-border areas where vehicles transit from one country to another [6].

This paper provides an overview of emerging slicing-enabled UCs and their potential security challenges while focusing more on cross-border areas, e.g., France and Luxembourg. In particular, this study focuses on three main UCs: automated lane merging/splitting and overtaking real-time traffic flow regulation and network-assisted VRU protection. Note that some literature works (e.g., [7, 8]) have investigated various issues (e.g., interoperability and quality of service, some aspects of security) in the cross-border setting, but our work differs in the fact that we aim at an in-depth analysis of cyber-security issues from different levels including 5G infrastructure, use-case specific issues and other security concerns which become significant in cross-border settings. Finally, we discuss the key technical challenges, open issues, and future research directions to mitigate such vulnerabilities. The remainder of this article is structured into six sections. Section III describes some background regarding 5G and V2X security. Section II presents relevant V2X NS UCs in cross-border areas. Section IV identifies the most relevant slicing-related attacks in this context. Section V discusses security challenges and open issues while pointing out some potential solutions. Section VI concludes the article.

II. 5G-V2X Use Cases

To date, many UCs have been proposed by exploiting different features of the 5G ecosystem [9]. Figure 1 shows three 5G-V2X UCs that leverage NS in cross-border scenarios. It is worth mentioning that these UCs are the focus of our current research project 5G-INSIGHT[1]. The upper part of this Figure is shared between the UCs, showing the 5G-Core and MEC layer of the interconnecting MNOs (home and visited). The cross-border scenario differed from the general multi-MNO scenario since home and visited MNOs are under different policies and regulations, which can directly impact security. For example, policies and regulations regarding certain tools and technologies (e.g., Blockchain) and data processing procedures can limit MNOs from designing efficient security solutions. Therefore, in the cross-border scenario, the MNOs should harmonize their different-level security solutions to meet the policies and regulations of the hosting countries. Moreover, as shown in the Figure, the isolation between UC V2X-NSs is done in the data plane only, i.e., each UC has a dedicated User Plane Function (UPF) hosted in the MEC layer. After crossing the border, the visited MNO allocates a V2X-NS with the same functionality as in V2X-NS as the home MNO. N9 and N32 are reference points given by 5G standards. Specifically, N9 is between two UPFs, and N32 is between the visited 5G core network and the home one. In each UC, the gNodeB (the base station's name in 5G) is attached to the assigned UPF for the data plane and with the 5G Core for the control plane. In the following, we describe the three UCs.

A. Use Case 1: Automated Lane Merging/Splitting and Overtaking

This UC is tailored to highways to enable CAVs to determine the best and safest merging/splitting or overtaking maneuvers according to the current situation. Figure 1 (a) illustrates a scenario from this UC. CAVs gather and analyze their surroundings to derive information about neighbors, including lane position, acceleration, speed, size, etc. Indeed, CAVs may collect data through their onboard sensing equipment (sensors, cameras, radars, etc.) as well as from external roadside sensors and neighboring CAVs. Then, CAVs process data locally and/or at the edge level to help make suitable decisions regarding lane merging/splitting and overtaking maneuvers. The V2X-NS dedicated to this UC should provide low-latency, and reliable communication between CAVs and 5G infrastructures, especially in cross-border areas, where routine procedures such as handovers and roaming occur to migrate from one (home) MNO to another (visited). Attacks on this critical zone for this UC could be fatal, particularly with high-speed CAVs.

B. Use Case 2: Real-time traffic flow regulation

This UC enables traffic regulation in the urban environment, as shown in Figure 1 (b). Multi-access Edge Computing (MEC) nodes continually collect data about

[1]http://5g-insight.eu/

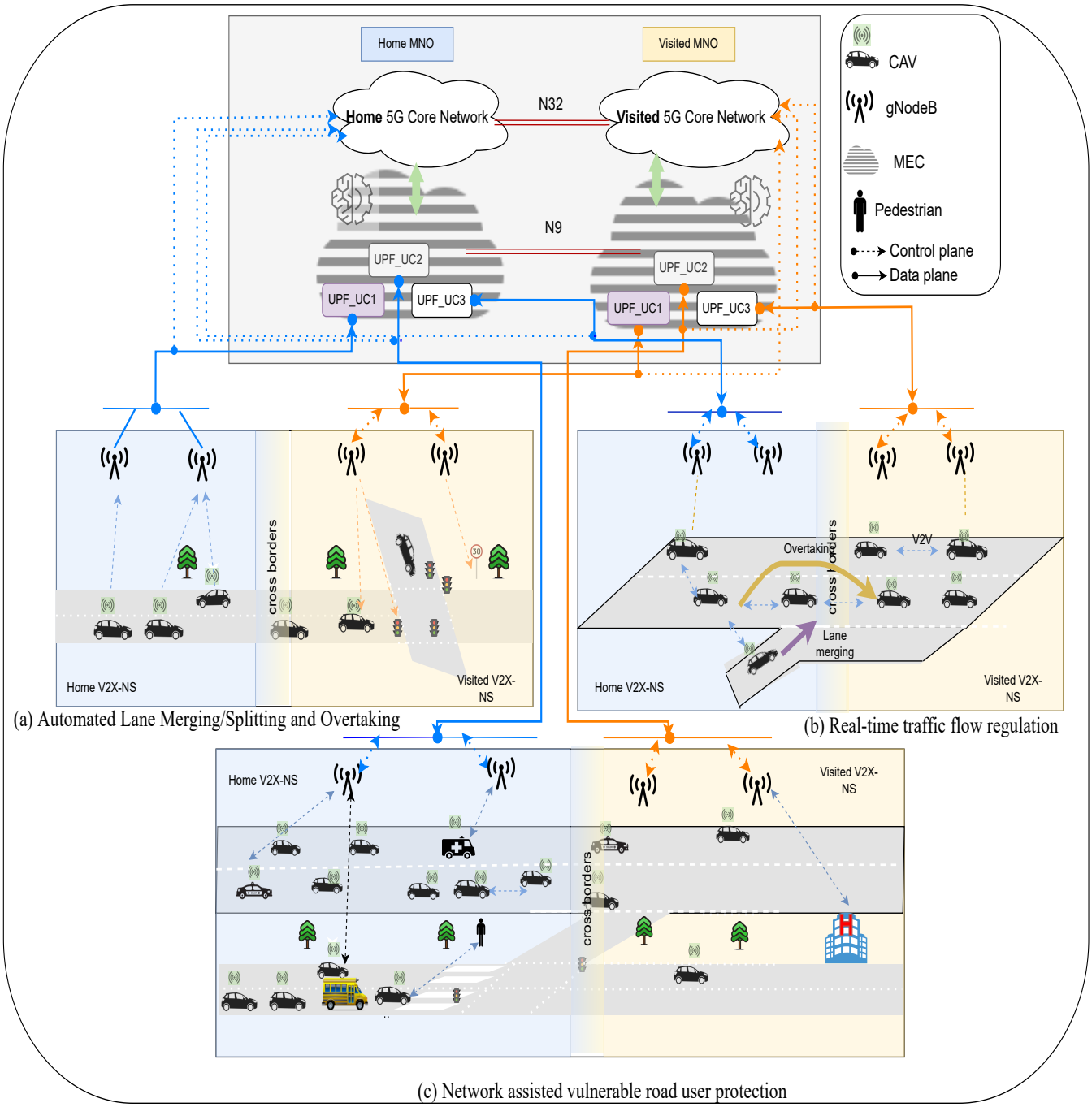

Fig. 1: 5G-V2X UCs at the cross-border area

the current road traffic from CAVs and roadside sensors. Then, they process relevant data using advanced machine-learning algorithms and data mining techniques. After that, MEC nodes make decisions to regularize traffic flow. For example, they synchronize traffic lights and adjust variable traffic signs accordingly. MEC nodes could also send notifications to vehicles/drivers about the traffic flow conditions and recommendations to enhance the traffic flow. The V2X-NS dedicated to this UC should be able to manage massive data received from the V2X node and store it in MEC nodes. These latter nodes play a vital role in this UC, making them suitable targets for attackers to break the V2X-NS. Attacks on MEC nodes can result in road traffic disturbances like traffic jams or even accidents at road intersections, which are very inconvenient for users, especially for workers crossing borders. Attackers can also access sensitive information, which leads to serious privacy issues. Attacks could be

magnified at the cross border since the borders managing areas of MNOs are overlapping.

C. Use Case 3: Network assisted vulnerable road user protection

As shown in Figure 1 (c), this UC encompasses VRUs such as pedestrians and cyclists. It can also provide services to other special CAVs, such as police, ambulances, and school buses. Data about VRUs and special CAVs are continually collected and stored at the MEC level. MEC nodes offer advanced analytical tools to process the collected information. The processed information can serve, for example, to (a) prioritize and facilitate the passage of VRUs; (b) prioritize information sent by special CAVs, like information sent from ambulances to the hospital or police CAVs to the police post. Enabling special CAVs such as police cars and ambulances crossing the border to receive and respond to data from the hosting MEC server could save time and lives. Based on the received data, the crossing vehicle could adapt its path to avoid highly VRUs populated areas, which would reduce the trip times, and prevent accidents. The V2X-NS supports this UC and should provide the necessary network and storage resources to VRUs and special CAVs. MEC also has a vital role in this UC. Thus, V2X-NS is also vulnerable to security and privacy issues described in the second UC. But because this V2X-NS handles highly sensitive information outside the road network, attackers would be more interested in breaching or breaking this V2X-NS.

Table I shows a comparative matrix of the presented UCs. As we can see, the proposed UCs generally have different characteristics in terms of goal, environment, and automation level. But they are all relevant to cross-border scenarios. UC 1 aims to provide safety in fully autonomous driving on highways where the primary communication type is V2V. UC 2 aims to ensure traffic efficiency in an urban environment leveraging edge-computing capabilities; thus, frequent communications with infrastructure are employed. UC 3 seeks to protect VRUs in mixed road areas (e.g., highway, urban, etc.) using various communication types, including V2P. On the other hand, from the perspective of 3GPP [10], UC 1 belongs to the advanced driving UC group. In contrast, UCs 2 and 3 can be part of the advanced driving, and the extended sensors UC groups simultaneously since they collect data from local and external sensors and use this information for traffic efficiency and road safety.

III. 5G and V2X Security Background

In this section, we briefly recap some 5G security backgrounds and key features such as NS, then recap the ETSI's V2X security work and link it to 5G. This preliminary background serves as a basis for the discussion in Section IV.

A. 5G and NS Security in a Nutshell

Unlike in the previous generations, special efforts have been dedicated to addressing the security issues in the development of 5G. For example, in the EU, many research projects have been carried out under the 5G Infrastructure Public Private Partnership (5G PPP)[2], a joint initiative between the European Commission and the European ICT industry.

5G security architecture and mechanisms have been comprehensively defined in several 3GPP specifications and reports. For example, the technical specification TS 33.501 specifies the security architecture, and the 3GPP TS 33.122 document specifies the security architecture for the common API framework as per the architecture and procedures defined in 3GPP TS 23.222.

The standardization of 5G security has also benefited from other organizations such as ETSI, GSMA, and ITU-T. For example, GSMA has contributed to improving 5G security, e.g., its Fraud and Security Group has published the FS.36 reference document

for *5G Interconnect Security*[3].

NS is a core technology to exploit the full potential of 5G networks. A dedicated network function called NS Selection Function (NSSF) has been dedicated to managing slice instances in a 5G network. The 3GPP technical reports TR 33.811 and TR 33.813 study the threats, potential security requirements, and solutions for the 5G NS management features.

The low latency and high throughput properties of 5G make it an ideal communication infrastructure for mission-critical applications, such as those we mention in Section II. With the new Service Based Architecture (SBA) for the core network and all the dedicated security mechanisms, 5G further provides a foundation to build trustworthy applications. In comparison to other infrastructures, 5G possesses additional advantages from the perspective of seamless service delivery in cross-border scenarios, due to the uniform standards (including security) and policy enforcement. For the latter, if we take Europe as an example, the European Union Agency for Cybersecurity[4] (ENISA) has done an excellent job in promoting 5G security for the whole European Union (EU).

[2]https://5g-ppp.eu/

[3]https://www.gsma.com/newsroom/wp-content/uploads//NG.113-v2.0-9.pdf

[4]https://www.enisa.europa.eu

TABLE I: A comparative study

5G-V2X Use case	Goal	Environment	Communication types	Automation level	3GPP mapping
Use case 1	Safe autonomous driving	Highway	V2V and V2N	Full Automation	Advanced Driving
Use case 2	Traffic Efficiency	Urban	V2I and V2N	Conditional Automation	Advanced Driving Extended sensors
Use case 3	VRU security Public services	Mix (Highway + Urban)	V2I, V2P, and V2N	Conditional Automation	Advanced Driving Extended sensors

B. 5G and V2X Security

With respect to V2X, ETSI has proposed TS 102 940, which is about V2X communications security architecture and security management. Based on the security services defined in ETSI TS 102 731, this document identifies the functional entities required to support security in a V2X environment and the relationships between the entities themselves and the elements of the V2X reference architecture defined in ETSI TS 302 665. Moreover, ETSI has proposed TS 102 941, which identifies the trust establishment and privacy management required to support security in a V2X environment and the relationships between the entities themselves and the elements of the ITS reference architecture defined in ETSI TS 302 665.

When 5G is employed as the communication infrastructure for V2X, 5G security and privacy issues impact the security and privacy of V2X communication. Specifically, V2X benefits from 5G enabling technologies, particularly NS. As a remark, V2X could become vulnerable to security and privacy issues coming with these technologies. The problem is getting worse for cross-border V2X Network Slices (V2X-NSs). Indeed, in these areas, 5G network security does not only depend on the originating Mobile Network Operator (MNO), but also on the visited one, while considering all roaming scenarios. Therefore, in practice, to address cross-border V2X-NS cases, 5G security must be considered along with V2X UCs. We elaborate further on this matter in Section IV.

IV. Security and Privacy in Cross-Border Settings

In this section, we first discuss some general security concerns in 5G that affect the UCs which use this technology, then identify several selected attacks against V2X-NS systems, and finally point out a few specific security challenges of V2X-NS systems in cross-border areas.

A. 5G Related Concerns

Despite the current security mechanisms, researchers have shown that various threats exist. Køien in [11] provides a detailed analysis of this subject. While there is a major security issue identified, this paper does pinpoint many subtle issues, such as vulnerabilities in integrated software components. Regarding NS, Olimid and Nencioni presented several security issues in 5G covering the life-cycle, intra-slice, and inter-slice aspects. Adaptive Mobile Security company published a report [5], which emphasizes at new approaches are required to mitigate the vulnerabilities, including user data extraction, Denial of Service (DoS) attacks, and illegitimate data access in slices. The ENISA report [6] surveys the security threats against SDN technologies and highlights that an API exploitation threat can result in unauthorized disclosure, compromise of integrity and/or destruction of information, or unauthorized destruction/degradation of service.

It is worth emphasizing that 5G introduces new security mechanisms and procedures but at the same time also preserves some previous ones. In particular, the MNOs have the flexibility to determine which mechanism to use based on their own policies. It will not be a surprise that some MNOs will continue to use legacy security mechanisms even though they are less secure or robust than the new ones. At the EU level, ENISA has developed a 5G toolbox[7] which contains both strategic and technical measures. These measures help the national regulators and the MNOs (and their partners such as cloud providers and service providers) to fulfill a pan-European security objective. Moreover, the toolbox also outlines a set of supporting actions to support the achievement of the security objectives. Despite the efforts, the application of this toolbox varies substantially in EU[8]. This creates potential security issues in cross-

[5]https://info.adaptivemobile.com/ 5g-network-slicing-security

[6]https://www.enisa.europa.eu/publications/sdn-threat-landscape

[7]https://www.enisa.europa.eu/news/enisa-news/5g

[8]https://www.pwc.fi/en/publications/
the-practical-pitfalls-of-the-eus-enisa-5g-security-requirements.html

border scenarios, like ours in this paper.

B. Selected Attacks against V2X-NS System

Regarding the V2X System, there is a plethora of attacks that target different components or mechanisms inside. In our analysis, we select several NS-related attacks which are critical for our UCs mentioned in the previous section.

- **Denial of Slice Service (DoSS) attack**: is a particular class of DoS attacks targeting V2X-NSs. This attack aims to directly or indirectly exhaust the resources of the V2X-NS. For example, an attacker can inject multiple messages using its pseudonyms as Sybils, which will degrade the performance of the underlying V2X-NS and other V2X-NSs that share the same physical infrastructure. In distributed DoSS scenarios, several malicious nodes within one V2X-NS or multiple V2X-NSs can collaborate and synchronize to carry out the attack. This attack can be more challenging to detect if the attackers belong to multiple V2X-NSs.
- **Network Slice Manager Impersonation (NSMI):** the slice manager is the core component in NS, which is in charge of the life cycle management of the network slices. The placement of the V2X slice manager in the proximity of CAVs (e.g., at the MEC) offers a better response time [12]. However, this will increase the risk of impersonation attacks. For example, an attacker can pretend to be a slice manager to monopolize the slice resources for its benefit.
- **Unauthorized Access to Slices (UA2S):** This attack uses two or more malicious CAVs attached to V2X-NSs providing different services. These CAVs can create a tunnel to share the V2X-NS service with each other. In other words, CAVs will have unauthorized access to V2X-NS that are not attached to them.
- **Sealing Between Slices (SBS):** Since a CAV could be attached to several slices simultaneously, malicious CAVs can exploit this feature to violate the isolation of V2X-NSs.
- **Selective jamming attack:** In contrast to traditional jamming attacks, this attack targets the V2X-NS network resources. Several CAVs can collaborate or alternate to perform this attack, making it difficult to detect.
- **Eavesdropping:** the attacker gathers data regarding a particular V2X-NS to extract information that can be leveraged. For example, the attacker exploits unencrypted traffic broadcast by CAVs to track the trajectories of their victims.

DoSS selective jamming attacks can directly disrupt the communication between vehicles and other entities. For UCs 1 and 2, such disruption may cause catastrophic consequences. NSMI attack may allow the attacker to take over the NS management and may cause similar or even more serious consequences than the aforementioned attacks in all three UCs. In comparison, UAS, SBS, and eavesdropping attacks will expose private information to the attacker, which may use to disrupt the normal operations of the system.

In UC 3, a group of malicious nodes could misuse the network-assisted VRU protection system to overload the MEC server, delay communication, and cause significant traffic disruption. Consider a scenario where one or several (compromised) nodes broadcast false awareness messages with multiple spoofed locations and identities to report the presence of many VRUs in the area or alarm about collision risk. The processing related to the dynamic motion prediction of many VRUs will consume the computation resources of the MEC server. In addition, the malicious traffic will be amplified by the MEC server and the other nodes due to the subsequent broadcast of maneuver coordination messages, collective perception messages, and awareness messages to signal hazard situations, which will degrade the performance of the underlying V2X-NS and other V2X-NSs that share the same physical infrastructure. Furthermore, the false alarms may trigger simultaneous collision avoidance actions (emergency braking or slowing down), causing significant traffic disruptions.

C. Special cross-border challenges

For the previously mentioned UCs, when the communication is done with 5G technologies, we expect the communication links to be secured with confidentiality and integrity. Therefore, attacks like eavesdropping can be prevented. Indeed, the CAVs can rely on Transport Layer Security (TLS) or Datagram TLS (DTLS) to secure their communication with the infrastructure. While the communication among CAVs and other entities such as VRUs might not be able to use TLS or DTLS directly since a common Public Key Infrastructure (PKI) might not be available, or a strong privacy/anonymity requirement may exist in this case. In any case, security mechanisms should be implemented; otherwise, the envisioned functionalities will not be properly achieved. We consider this as the first challenge for the UCs.

When 5G and V2X security mechanisms are enabled, there may be some overlaps, e.g., the mutual authentication between different entities. A particular focus will be privacy protection. A combined analysis

based on 5G and V2X mechanisms is needed to ensure privacy protection for honest participants. With proper confidentiality and integrity mechanisms deployed and appropriate confidentiality management, we expect that some of the typical attacks could be mitigated. To facilitate our discussion, we distinguish between insider and outsider attackers:

- For an outsider attacker, the most realistic attacks that can be carried out are jamming and denial of service attacks. The impact can be a delay in message delivery and disruption of services for the target victims. The outsider attacker can also perform an eavesdropping attack to passively collect network traffic. By doing so, it may be able to deduce some private information of benign users.
- For an insider attacker, all attacks may be relevant. However, if we assume that all communications pass through secure channels, mitigating some malicious behaviors from the insiders may be straightforward. However, insider attacks can inject false information without being directly detected. For example, traditional security solutions cannot mitigate false position attacks. Instead, detecting and mitigating such internal attacks need more sophisticated solutions listed in Section V. On the other hand, there might be security and privacy trade-offs in this case, as revealing identity information may cause privacy concerns.

In the cross-border setting, we need to focus on two aspects. First, we need to maintain seamless security channels between the participants, e.g., between a CAV registered at one MNO and a MEC registered with another MNO. Without proper configuration and interoperable credential management, the risk of service disruption is high. The other aspect is to jointly detect attacks (e.g., jamming and DoSS) by all the entities across the borders. We also foresee serious privacy issues when data is required to power machine learning (ML)-based solutions. Moreover, the prevention of attacks like sealing between slices may depend on the security policies of the involved MNOs. If one MNO's security policy somehow allows such attacks, then additional security measures should be deployed to counter the attacks.

V. Open Issues, Challenges and Potential Solutions

This section discusses some of the challenges of securing V2X-NS systems in cross-border areas while highlighting potential security enablers.

A. Advanced Deep Learning for Attack Detection

Protecting V2X-NS attacks, especially in cross-border areas, is tedious due to the advanced techniques used by the attackers to adapt to the defender's security mechanisms. ML/Deep Learning (DL) tools are emerging to address these challenges. However, given the complexity of the system, which involves the V2X NS and cross-border network procedures, ML/DL-enabled detection systems should be designed efficiently to cover various V2X slicing attacks. In particular, centralized ML/DL architecture cannot handle such complex systems due to their rigidity and limitations in updating the security system. Instead, collaborative and distributed ML/DL are more suitable for building collaborative attack detection systems. Another challenge, specific to the cross-border context, is that MNOs on both sides cannot share sensitive security data, such as users' locations, thus putting their consumers' privacy at risk. Federated Learning (FL) could address this challenge [13] by allowing home and visited MNOs to collaborate on building attack detection models without sharing their data. FL also reduces the training workload of the security DL models by distributing the training load to several workers instead of training DL models centrally. Specifically, visited and home MNOs can have their own FL network to build a global model to detect attacks listed in Section IV. Each MNO's FL network consists of an FL coordinator and a set of FL workers that train local models based on the MNO's private data. Building a global model happens in several rounds. In each round, the FL coordinator receives updates from FL workers, aggregate them, and update the global model. The process continues until obtaining a global model with satisfactory accuracy. Once both visited and home MNOs have their models ready, they can mutually update them by sharing their parameters.

B. Blockchain and deception security for attack mitigation

Considering CAVs or VRUs crossing country borders, the visited MNO should allocate a V2X-NS to them with the same characteristics as the home MNO. Thus, interconnecting MNOs requires building trust between them to ensure continuous delivery of V2X-NS services and prevent attackers from exploiting this interconnection point to break or disrupt V2X-NS. To this end, blockchain and smart contracts could be the best candidates to build trust here and protect ML/DL-based attack detection systems [14]. However, blockchain-based solutions should deal with context-related obstacles such as scalability issues that come with the increased number of

users and the V2X-NSs policy, legislation, and regulation issues since home and visited MNOs belong to separate administrative domains. Consortium blockchains could be an enabler, allowing selected parties on each MNO to create and validate blocks and insert them into the blockchain using lightweight consensus protocols such as Delegated Byzantine Fault Tolerance (dBFT). dBFT provides high throughput and fast consensus time while being high fault tolerance. However, visited and home MNO should agree on which data to put into the blockchain to comply with privacy regulations in each country. In addition, smart contracts should be carefully designed to respect the V2X-NS's Service Level Agreement (SLA) and regulation policies for each country home and visited, such as security policies listed at the end of the subsection IV.C.

Another approach to mitigating attacks is deception security, which aims to slow down, trap, deflect and prevent an intruder from gaining access to an entity's information system. Honeypots are one of the powerful tools to implement a deception security strategy [15]. For example, we can deploy a distributed honeypot composed of a fake MEC node that mimics the behavior of the actual node, with fake gNodeB and CAVs to distract attackers from the actual target and redirect malicious traffic. It is also possible to set up a fake V2X-NS or create a sinkhole-type slice with a small portion of physical resources to isolate and mitigate the attackers' action and then study how the attackers proceed to get unauthorized access. The main challenge to address here is what is optimal to place honeypots for enhancing higher utility while reducing false positives of redirecting legitimate traffic toward honeypots.

C. Federated learning for privacy protection

Privacy protection is another challenge faced by V2X NS at the cross-borders. As described in the UC section, CAVs and VRUs share their sensitive information with MEC nodes for analysis and decision-making using ML/DL approaches. Information exchange between MEC nodes of the home and visited MNOs is vital to provide CAVs and VRUs with smooth service continuity while crossing the borders of the two countries. Thus, attack detection and mitigation at the MEC level are paramount, especially in cross-border areas. On the other hand, MEC nodes in each MNO (home/visited) store sensitive data (e.g., past trajectories) regarding CAVs and VRUs, while they are under administrative control. Sharing these data with MEC nodes of another MNO can violate users' privacy protection. The challenge then is how to ensure the V2X-NS services while crossing the border without sharing data between MNOs. FL could also be a promising solution to address this challenge [13]. Indeed, MEC nodes can train their local models leveraging the local data and then share only ML/DL models' parameters to build global models tailored to V2X-NS-enabled UCs. Therefore, different learning models can be generated at the cross-borders without sharing private data related to both sides such as users' mobility information. Moreover, secure Multi-party Computation is one of the interesting cryptographic approaches for MECs to jointly build or test ML models using their private datasets in a distributed way without revealing their private datasets to each other.

VI. Conclusion

Securing V2X NS in the cross-border area is a challenge. While standards development organizations are making progress in 5G NS security, V2X at the cross-borders is yet not addressed. This paper outlines this progress and identifies relevant and challenging V2X UCs in this context. Moreover, it describes V2X NS attacks with particular attention to cross-border areas. Finally, this paper discusses security and privacy challenges while identifying open issues and opportunities for cross-border V2X NS, with a focus on attack detection, attack mitigation, and privacy protection potential solutions.

Acknowledgment

This work was supported by the 5G-INSIGHT bilateral project (ID: 14891397) / (ANR-20-CE25-0015-16) funded by the Luxembourg National Research Fund (FNR), and by the French National Research Agency (ANR).

References

[1] D. Garcia-Roger, E. E. González, D. Martín-Sacristán, and J. F. Monserrat, "V2x support in 3gpp specifications: From 4g to 5g and beyond," *IEEE access*, vol. 8, pp. 190 946–190 963, 2020.

[2] A. Alalewi, I. Dayoub, and S. Cherkaoui, "On 5G-V2X Use Cases and Enabling Technologies: A Comprehensive Survey," *IEEE Access*, vol. 9, pp. 107 710–107 737, 2021.

[3] I. Afolabi, T. Taleb, K. Samdanis, A. Ksentini, and H. Flinck, "Network Slicing and Softwarization: A Survey on Principles, Enabling Technologies, and Solutions," *IEEE Communications Surveys Tutorials*, vol. 20, no. 3, pp. 2429–2453, 2018.

[4] "Intelligent transport systems (its); security; threat, vulnerability and risk analysis (tvra)," ETSI TR 102 893 V1.2.1, Tech. Rep., Mar 2017.

[5] "Study on security aspects of enhanced network slicing," 3GPP TR 33.813, V0.8.0, Tech. Rep., Nov 2019.

[6] A. Kousaridas, M. Fallgren, E. Fischer, F. Moscatelli, R. Vilalta, M. Mühleisen, S. Barmpounakis, X. Vilajosana, S. Euler, B. Tossou, and J. Alonso-Zarate, "5G Vehicle-to-Everything Services in Cross-Border Environments: Standardization and Challenges," *IEEE Communications Standards Magazine*, vol. 5, no. 1, pp. 22–30, 2021.

[7] D. Hetzer, M. Mühleisen, A. Kousaridas, S. Barmpounakis, S. Wendt, K. Eckert, A. Schimpe, J. Löfhede, and J. Alonso-Zarate, "5g connected and automated driving: use cases, technologies and trials in cross-border environments," *EURASIP J. Wirel. Commun. Netw.*, vol. 2021, no. 1, p. 97, 2021.

[8] A. Kousaridas, M. Fallgren, E. Fischer, F. Moscatelli, R. Vilalta, M. Mühleisen, S. Barmpounakis, X. Vilajosana, S. Euler, B. Tossou, and J. Alonso-Zarate, "5g vehicle-to-everything services in cross-border environments: Standardization and challenges," *IEEE Communications Standards Magazine*, vol. 5, no. 1, pp. 22–30, 2021.

[9] J. Navarro-Ortiz, P. Romero-Diaz, S. Sendra, P. Ameigeiras, J. J. Ramos-Munoz, and J. M. Lopez-Soler, "A survey on 5g usage scenarios and traffic models," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 905–929, 2020.

[10] 3GPP TR 22.886, "Study on enhancement of 3GPP Support for 5G V2X Services," Dec 2018.

[11] G. M. Køien, "On Threats to the 5G Service Based Architecture," *Wireless Personal Communications*, vol. 119, no. 1, pp. 97–116, 2021.

[12] H. Khan, P. Luoto, S. Samarakoon, M. Bennis, and M. Latva-Aho, "Network slicing for vehicular communication," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 1, p. e3652, 2021.

[13] J. Posner, L. Tseng, M. Aloqaily, and Y. Jararweh, "Federated learning in vehicular networks: opportunities and solutions," *IEEE Network*, vol. 35, no. 2, pp. 152–159, 2021.

[14] M. A. Togou, T. Bi, K. Dev, K. McDonnell, A. Milenovic, H. Tewari, and G.-M. Muntean, "DBNS: A distributed blockchain-enabled network slicing framework for 5G networks," *IEEE Communications Magazine*, vol. 58, no. 11, pp. 90–96, 2020.

[15] S. Panda, S. Rass, S. Moschoyiannis, K. Liang, G. Loukas, and E. Panaousis, "HoneyCar: A Framework to Configure Honeypot Vulnerabilities on the Internet of Vehicles," *arXiv preprint arXiv:2111.02364*, 2021.

BIOGRAPHY

Abdelwahab Boualouache is a research associate at the University of Luxembourg. His current research covers security and privacy in the area of mobile and wireless networks, mainly focusing on topics related to 5G and beyond 5G cellular networks and CAVs.

Bouziane Brik is an associate professor at the University of Burgundy and DRIVE laboratory, France. His research interests include IoT in industrial systems, smart grids, and vehicular networks.

Qiang Tang is a Research Group Leader at the Luxembourg Institute of Science and Technology (LIST). His research interests include applied cryptography, privacy enhancing technologies (PETs), and the security and privacy issues in DLT/blockchain.

Abdelaziz Amara Korba has been working as an associate professor since 2016. His areas of interest include network security, and intrusion and anomaly detection, and applied DL/ML techniques.

Sylvain Cherrier is an associate professor at University Gustave Eiffel, France. He is interested in the IoT, mainly in software architecture designed for the domain, using Service approaches.

Sidi Mohammed Senouci is a full professor at the University of Burgundy, France. His current research interests include Intelligent Transportation Systems, Smart Grids, Security and Intrusion Detection Systems.

Enric Pardo is a Research and Technology Associate at the Luxembourg Institute of Science and Technology (LIST). His research interests include the mathematical modeling for resource allocation in 5G-and-beyond and V2X.

Yacine Ghamri-Doudane is Full Professor at La Rochelle University in France. His current research interests lay in the area of wireless networking and mobile computing with a current emphasis on topics related to the IoT, CAV, and 5G and Beyond

Rami Langar is a Full Professor in Computer Networks affiliated with University Gustave Eiffel (France) since 2016, and École de Technologie Supérieure, Montréal (Canada) since 2021. His research interests include resource management in future wireless systems, NS in 5G/6G, SDN, and green networking.

Thomas Engel is a Professor of Computer Networks at the University of Luxembourg. His SECAN-Lab team deals with performance, privacy, and identity handling in Next Generation Networks.