Reference [1]. <https://www.mdpi.com/2079-9292/11/7/1072>

## Challenges

The continuous developments in automotive electronics technologies bring along important challenges that span across several levels, including latency, intelligence, security, and mobility support. This section concentrates on key open issues that need to be worked on or resolved in current and future VIDS (Vehicular IDS).

#### *6.1. External Interfaces and Attack Surface*

The increasing vehicle connectivity will be boosted with the advent of connected and autonomous vehicles (CAVs), which will require communication with other vehicles and objects (such as traffic lights) in the surrounding environment to provide efficient and safe autonomous driving. However, the integration of these communication interfaces with the IVN could also increase the impact and likelihood of security threats. As separating potential attacking network interfaces from IVN, that is, minimizing the attack surface, makes much harder for adversaries to connect to the IVN and mount assaults. This, however, is not practical for certain interfaces. For instance, the OBD port is used to communicate with the vehicle’s systems to help diagnose problems, and thus isolating it from the in-vehicle network is rather unrealistic. Therefore, current solutions incorporate detectors to OBD port to discern between normal and aberrantly injected frames. Moreover, the communication related to systems such as telematics or GPS goes usually through a central gateway or multiple distributed gateways, which are also used to interconnect different buses. Therefore, the implementation of restrictions or rules in such components could be considered to isolate such external communications from the IVN, so that the attack surface could be reduced.

#### *6.2. Interoperability*

As already mentioned, CAVs require remaining in constant communication with their surroundings for being able to assess the current situation and make decisions in real time, ensuring safe transportation. In this respect, the authenticity and integrity of the sensed or received data is a sine qua non for achieving autonomous interconnected safe driving in a dynamic environment. This, however, is not limited to the vehicles themselves as an ad hoc network, but also to the rest of the components and especially to the road and network infrastructure, including Wi-Fi and cellular base stations and both the access and backhaul network links. While some wireless standards, such as IEEE 802.11p (ETSI ITS-G5), LTE-V2X, and New Radio (NR) V2X, have been developed especially for the vehicular terrain, several interoperability issues related to security aspects could be derived from the coexistence of some of these technologies in a real-life deployment that could have a direct impact on the IVN security.

Naturally, as already pointed out, to support interoperability, diminish the attack surface, and support future applications, the connectivity security issues should focus not only on the vehicle itself but on the whole infrastructure and service value chain as well. In this respect, key questions, e.g., who controls and provides the communication infrastructure in the CAV ecosystem, are still to be defined. Simply stated, it is important to correctly and clearly stipulate roles and responsibilities for the involved parties and attain a wise balance between private and public control. Furthermore, the use of private protocols (or the use of own tailored implementations of standard protocols) used by different OEMs may be an impediment for VIDS. That is, the implementation of ECU systems and transport protocols responsible to convey, say, CAN messages may be quite dissimilar across various OEMs. This may result in lowering the detection accuracy of an IDS if it is used in a dissimilar setting. Moreover, the accuracy of detection can be affected by inherent properties of the bus protocol. For instance, CAN messages transmission may occur abruptly due to, say, re-transmissions, bit errors, etc. Therefore, if the IDS is designed based on the normal message transmission profile, it may be prone to a high rate of false positives.

#### *6.3. Heterogeneity of Network Technologies*

Heterogeneous wireless networks, and especially VANETs, are considered to be susceptible to an assortment of threats in comparison to their wired counterparts. This stems from the complex network topology (in-vehicle, road-side, cloud infrastructure, etc.) and the high mobility conditions in the VANET realm. The opponent is presented with a large attack surface, that is, multiple points of entry. These range from accompanying, to vehicle mobile apps, to a plethora of wireless or other type of interfaces, including Wi-Fi, Bluetooth, cellular, FM, keyless entry systems, and even voice commands. All these access points can offer an initial foothold that can possibly lead to compromising the in-vehicle security. Upon compromise, the vehicle and the VANET itself may become prone to a range of perilous attacks, including botnets, and, continuing from the previous point, most of the proposed IVN IDS systems have high accuracy. However, each system monitors a single network layer, and, consequently, they do not provide comprehensive approaches considering the potential impact of diverse attacks at several vehicle network layers.

#### *6.4. Data Privacy*

Another major issue is who regulates access to the data collected by the vehicle, the associated applications, and the backend. In fact, such privacy concerns have been already touched upon by current standards such as the ISO 20077, but, in general, the relevant issues are not well-tackled or defined even in the newest standards and regulations, including the UN R155 and R156. In particular, ISO 20077 defines the concept of *extended vehicle* to represent the increased functionality of vehicles based on the development of services by using their data. Even if a general process is defined for the access to such data by considering the vehicle’s manufacturer, it is still not clear which responsibilities are associated with manufacturers and service providers, which will use such data to develop new services. Furthermore, a 2017 survey performed by the German consumer organization “Stiftung Warentest” revealed that the great majority of connectivity schemes offered by automotive OEMs are prone to certain privacy leaks. Threats against privacy have also been recently exposed for the official (OEM’s) mobile applications that accompany modern vehicles. Namely, among others, personal information may be communicated unencrypted, and certain pieces of private information, including those collected by a VIDS, may be gathered and transmitted without prior user consent. Indeed, in the case of ML-enabled VIDS, the use of modern techniques could lead to increasing privacy risks because of the access to all the data derived from the IVN traffic, as well as the possibility of inferring new sensitive information as a result of applying such techniques. Such solutions could negatively impact data protection, therefore calling for compliance to, say, the General Data Protection Regulation (GDPR).

#### *6.5. Safety Engineering and Quantification of Risk*

As the automotive industry relies heavily on ICT technology, cyberattacks can have direct and adverse effects on transport safety. However, as described by recent works, there is a gap between a vehicle’s functional security and the security aspects of IVNs that requires an adaptation of the existing functional safety methods and processes. The functional safety requirements of the complete lifecycle of every safety-related automotive electronic/electrical system is defined in the ISO 26262 standard. In particular, it addresses possible hazards caused by malfunctioning behavior of safety-related electrical and electronic (E/E) systems, including interaction of these systems. Furthermore, IEC 61,508 covers those aspects to be considered when electrical/electronic/programmable electronic (E/E/PE) systems are used to carry out safety functions. However, such standards cover neither the cybersecurity aspects throughout the vehicle’s lifecycle nor the relationship between safety and cybersecurity concerns. In this context, traditional security engineering falls short and should be combined with safety engineering. Indeed, apart from detecting purely ICT-related threats, IVN IDS should also take into account the safety dimension identifying the risk associated with each attack and implementing the appropriate countermeasures accordingly.

In this respect, cyber risk standardization and regulation is deemed as a decisive factor towards decreasing cyberattacks against automotive. Indeed, cyber risk in this sector may span across diverse levels and be cumbersome to assess and quantify. Moreover, the residual cyber risk, that is, the remaining risk after every cybersecurity recommendation has been taken into account, can be quite high. A prominent example of this situation is the risk associated with the supply chain threat as discussed further. Under this prism, the standardization of cyber risks and risk assessment, also through the lens of recent regulations UN 155 and UN 156, can serve as a lodestar for better understanding and quantifying cyber risk posture of IVN and automotive in general. The interested reader is also referred to the interesting work by Radanliev for analyzing uncontrollable states in complex systems. Additionally, a potential starting point could be based on the consideration of the SAE J3061 guidebook, which provides a cybersecurity process framework and guidance to help organizations identify and assess cybersecurity threats in vehicle systems. More specifically for IVN IDS approaches, the recent ITU-T X.1375 Recommendation establishes a set of guidelines for IVN IDS and identifies threats to existing IVNs, such as CAN, that could potentially imply safety concerns.

#### *6.6. Hardware Limitations*

Hardware limitations of ECU may be a serious hindering factor for the application of some resource-intensive VIDS. Namely, legacy ECUs typically comprise microcontrollers with a maximum clock speed of several hundred MHz and a limited RAM. In this respect, computational complex schemes, such as the one in or others which require extra equipment, may be not be practical for current vehicles. Indeed, storage, computation, battery, and bandwidth limitations can prevent an IDS approach from satisfying the real-time requirements of vehicular environments with the consequent safety implications, which typically involve security risks. These aspects may be exacerbated in the case of sophisticated ML/DL-enabled IDS approaches that could make their deployment in existing IVNs infeasible. To overcome these limitations, a potential approach is the deployment of the IVN IDS in the different gateways, which are typically used to interconnect ECUs. However, it is not clear if existing gateways of commercial vehicles have enough resources to execute complex machine learning algorithms to identity potential security attacks. Another potential approach is the use of intermediate nodes to offload learning tasks for internal vehicle components. However, as already pointed out, this approach could have privacy implications if vehicles need to share their data with external entities. Furthermore, as described by, the deployment of IVN IDS must take into account the instability of vehicle connections due to mobility.

#### *6.7. Use of ML Approaches*

ML algorithms can improve the detection capabilities of IVN IDS. However, the following points should be considered before their deployment. First, a centralized approach sending vehicle data (such as MAC, VIN, and device ID) to a server or the cloud could potentially be associated with privacy concerns. Second, in the same centralized approach, the network and processing delays could hinder the efficacy of the IDS. Third, IVN IDS are based on resource-constrained devices, with limited throughput and intermittent communications, and a centralized machine learning solution could pose high overhead. To this end, federated learning (FL), which refers to a collaborative learning approach based on decentralized data storage, could provide a viable solution respecting privacy and resource limitations. Furthermore, while many ML-enabled IVN IDS approaches have been proposed, the performance evaluation of some of these works have serious limitations, since they only consider performance metrics associated with the accuracy of the ML model being evaluated. An IDS has real-time requirements in the automotive context, so that appropriate countermeasures can be applied immediately after detecting such an attack. Therefore, the development of IDS approaches for in-vehicle networks must consider the complexity to demonstrate its feasibility in a real environment. Furthermore, such evaluations are based on non-exhaustive datasets, which do not cover a variety of attacks spanning across multiple network interfaces and protocol layers. For example, according to, so far only one dataset contains application layer attacks targeting data exfiltration, which nevertheless is quite common to advanced persistent threat (APT) groups. Moreover, no dataset incorporates attacks relevant to FM or voice-commands exploitation. An additional point is that, similar to other contexts, many of the so-far proposed schemes do not provide a detailed overview of the tests performed to assess the accuracy of IDS approaches, or how the datasets were actually used. The main consequence is the difficulty in comparing existing ML-enabled IVN IDS approaches.

#### *6.8. Adversarial ML*

Related to the previous point, adversarial machine learning attacks should be considered as a serious threat to VANET and CAV in general. This is because, among others, this type of assaults may aim at manipulating the results that an IDS can provide. That is, the adversaries may exploit multiple ways of feeding the IDS’s machine learning model with deceptive inputs in an attempt to trick it, and ultimately taint the results. Precisely, as with every other category of attacks, the adversary’s goal can greatly vary because it depends on their position in the network, knowledge, capacity, and motivation. For instance, in a so-called evasion attack, a rogue vehicle may contribute malicious test samples to the network, or the adversary may be able to alter the training data, thus leading the classifier to produce faulty results. In another instance, the aggressor may be able to inject noise to a machine learning model, that is, by manipulating sensor readings or by changing the physical environment in the vehicle’s vicinity.

#### *6.9. Type Approval*

In the automotive ecosystem, the *type approval* is usually referred to as the process to certify a vehicle, or verify that a certain vehicle’s component meets a set of standard requirements. Ideally, such a process should be rooted in a commonly accepted security certification scheme and applied across all the vehicle digital components, either internal, e.g., in-vehicle firewalls, IDSs, and anti-tampering mechanisms, or external, e.g., the associated applications, the backend systems, and the roadside components. In this direction, the standardized common criteria (CC) framework as defined in ISO/IEC 15408 seems a straightforward choice. Indeed, CC represents the most widely deployed and adopted certification scheme; however, it also presents some limitations related to the time and effort required for the execution of the certification process, the analysis of the evaluation-related documentation, and the management of changes in the certified product. Irrespective of whether the CC or a similar methodology will be adopted in the future or not in the automotive realm, certain CC methods can be exploited for evaluations within the framework of ISO/SAE 21434, even without formal certification. By doing so, the security of virtually any vehicle component, including IDS ones, can be systematically scrutinized and assessed at least against any known threat. Moreover, the identification of a certain attack or threat by an IDS could also have an impact on the type approval process of a certain vehicle by requiring a re-certification process. Indeed, vehicles could undergo changes, e.g., due to a software update or a new vulnerability discovered by the IDS, that would require the execution of a new type approval process during their lifecycle.

#### *6.10. Supply Chain*

Supply chain attacks should be considered a serious threat to VANET security in general and to VIDS in particular. In actuality, as described by, the use of components from different manufacturers in a certain vehicle poses significant security challenges for the whole vehicle. For instance, if an official or aftermarket vendor of a certain electronic component is being compromised somewhere along its supply chain, the perpetrator may be able to gain access to the firmware updates of the vendor. Next, the attacker may send malware along a legitimate software update request. Such a compromise may go unnoticed by the VIDS. Therefore, the use of standard approaches and the definition of standard security requirements and guidelines is crucial to ensure that the supply chain of vehicles’ components is based on widely recognized procedures to avoid potential security breaches. In particular, the recent UN 156 Regulation focuses on the requirements of software updates to be considered for the type approval process of the vehicle. Moreover, the use of blockchain approaches could also be considered in the future, so that different manufacturers could share information about their components in a trusted and decentralized way. Indeed, as described by, blockchain technology could also aid in maintaining the security information of each component updated throughout its lifecycle, including information about the certification scheme that was used to certify its security level, as well as the vulnerabilities or threats discovered.

#### *6.11. Components beyond the Vehicle Bus*

Both real-time operating system (RTOS) and middleware security is scarcely addressed in the context of VANET. However, RTOSs such as QNX Neutrino and VxWorks, and middlewares such as Autosar and ZF, may be susceptible to a range of threats and behave differently if being attacked. That is, every RTOS or middleware vendor may implement and assess otherwise the security features of their product, and on top of security by design concerns, in this domain, security through obscurity still remains a thorny issue. This calls for the establishment of minimum security requirements, say, also in the context of and across certification schemes, regulations, and standards. For instance, the UN R155 and UN R156 regulations, adopted in June 2020 by the UNECE World Forum for Harmonization of Vehicle Regulations (UNECE WP.29), are expected to globally shape the future framework around vehicle cybersecurity. Both these regulations applying to passenger cars, vans, trucks, and buses came into force in January 2021. Jointly, they require that cybersecurity measures be implemented in the CAV ecosystem across four distinct axes: (a) managing vehicle cyber risks, (b) securing vehicles in a by-design fashion to mitigate risks along the whole value chain, (c) detecting and responding to security incidents across the vehicle fleet, and (d) providing safe and secure software updates and ensuring vehicle safety is not compromised, thus introducing a legal basis for so-called over-the-air (OTA) updates to onboard vehicle software. Precisely, UN R155 mandates the existence of a certified cybersecurity management system, while UN R156 demands a software update management system as a future condition of type approval.

## Future Trends

Moving one step further from the previous section, the current section identifies trends and forthcoming issues in regard to VIDS technology for the advancement of next-generation automotive electronic systems.

#### *7.1. The Transition to Automotive Ethernet*

The increasing use of Ethernet will probably replace existing bus technologies, including FlexRay, MOST, or CAN. Typically, CAN is in charge of controlling the core part of the IVN, while LIN, FlexRay, and MOST serve mainly as auxiliary to the former. It is well known that CAN presents major security issues and other sorts of limitations, including the protocol’s broadcast nature, lack of network segmentation, lack of authentication, and lack of data encryption, and therefore the great majority of VIDS are intended for CAN. In this respect, ECU consolidation, say, through the use of dedicated domain controllers (i.e., gateways) can be seen as a mechanism to lower the complexity of CAVs and diminish the attack surface. In actuality, the heterogeneous automotive networks of proprietary protocols, such as CAN, are anticipated to be quite soon replaced by hierarchical homogeneous Ethernet networks; due to advances in Ethernet time-sensitive networking (TSN) in terms of bandwidth and cost, it is expected that automotive Ethernet will interconnect all the components in the car. Stated simply, while currently CAN has the largest experience and support base from any other bus technology, and despite any extensions such as CAN FD and FlexCAN, Ethernet offers improved network speed, bandwidth, built-in security, and native support for TCP/IP. Namely, the IEEE 802.3ch-2020 amendment to the IEEE 802.3-2018 standard has been developed for serving as the network backbone in the vehicle. This standard defines physical layer specifications and management parameters for a single balanced pair of conductors for links of 2.5 Gb/s, 5 Gb/s, and 10 Gb/s for automotive applications. This transition goes hand-in-hand with diagnostics over IP as standardized in ISO 13400, which, in its latest edition, adds support for transport layer security (TLS). Such diagnostics are not limited to, say, emission-related diagnostics or reading-out of relevant data from the computers in the car, but also apply to vehicle manufacturer-specific applications, such as calibration or electronic component software updates. Using an Ethernet backbone for in-vehicle communications renders external communications, say, between a vehicle and the cloud, transparently compatible. This means that vendors rely on the same networking technology across their whole vehicle infrastructure, thus diminishing complexity and enabling both trouble-free OTA software updates and diagnostics-over-IP. On the downside, the shift to automotive Ethernet instantly makes available to the opponent the whole repertoire of legacy Internet attacks in the automotive ecosystem. However, this also means that legacy IDS methodologies and architectures may be more or less applicable to the automotive sector.

#### *7.2. Use of Blockchain Technology*

The application of distributed ledger technologies (DLTs) in the vehicular ecosystem could serve to establish a decentralized mediator among different stakeholders to promote the development of trusted and innovate services. Indeed, as already mentioned in the previous section, blockchain could help to keep track of the potential attacks performed over IVN components. In particular, several works have been proposed integrating blockchain in the development of IDS approaches for the vehicular ecosystem. For example, based on the fact that V2X brings along dynamic intrusions where the attacks vary by location and time, while the current vehicle IDSs typically deploy preset static rules, the authors in proposed a micro-blockchain-based dynamic IDS. Precisely, micro-blockchains are nested into a macro-blockchain, and jointly provide strategies for detecting intrusions. The scheme has each micro-blockchain deployed in a small geographic region with the purpose of generating, in a tamper-resistant manner, local intrusion detection strategies for vehicles. Moreover, macro-blockchains store all the micro-blockchain models and provide dynamic intrusion detection regional strategies for roaming vehicles. For deploying micro-blockchains in the same region, the scheme relies on network slicing. Proof of work (PoW) is used as the consensus algorithm for the macro-blockchain, while the authors evaluated their scheme through simulations. While this is currently the only work that attempts to harness blockchain technology for V2X IDS, it provides a solid background for the design of advanced IDS schemes in the future. Furthermore, a recent work proposes the integration of blockchain and federated learning, so that RSUs train cooperatively in a certain area for IVN IDS scenarios. In spite of these efforts, it has been widely recognized that the deployment of blockchain poses important challenges that should be considered in such a context. Indeed, it generally presents three main challenges: (a) secure and synchronized software update and validation rules are quite difficult to achieve in blockchain networks, which, for the automotive sector may require the participation of multiple parties/actors; this can be leveraged by an attacker towards exploiting an outdated network or a network that suffers from obsolete validation rules, (b) scalability and high mobility of the blockchain network can possibly affect its overall performance, and (c) blockchain protection against malware is currently not addressed specifically for automotive. Furthermore, most of the works considering blockchain in this context lack a comprehensive evaluation to demonstrate its application in large-scale scenarios.

#### *7.3. Use of Unsupervised ML Techniques*

The use of ML techniques represents a clear future trend in the development of VIDS. However, it should be noted that, in most of the cases, the proposed approaches are based on supervised learning techniques. This is aligned with a recent work that provides an exhaustive survey of ML approaches to enhance security aspects in vehicular networks. Indeed, the authors analyze 67 papers; while 35 of the analyzed works are based on supervised learning, only 8 use unsupervised techniques. The main limitation of supervised learning techniques is that they require fully labeled datasets, which may be unfeasible in real scenarios where IVNs could generate a large volume of data on a continuous basis. This aspect is also discussed by recent works, which consider the need to foster the use of unsupervised and semisupervised approaches in ML-enabled VIDS. Indeed, the works proposed by lack an exhaustive evaluation of the unsupervised techniques (based on autoencoders and clustering) for detecting attacks in the CAN bus. Furthermore, the papers shows the use of a Kohonen self-organizing map (SOM) network with promising results on a public dataset with several CAN bus attacks. In addition, their research work creates a dataset with several CAN bus attacks that is evaluated by using a long short-term memory (LSTM) and autoencoders. While both approaches present high accuracy scope, still there is the need to evaluate the delay required for the identification of the different attacks, as well as the comparison with other unsupervised techniques. Moreover, in addition to unsupervised approaches, the use of reinforcement learning techniques could also be considered in the vehicular ecosystem, as demonstrated by their recent works for detecting misbehaving vehicles as an alternative to the aforementioned works. However, these techniques still have to meet the performance and accuracy requirements of VIDS to be deployed in the vehicular ecosystem.

#### *7.4. Federated Learning Enabled VIDS*

As an alternative to the use of traditional centralized ML approaches, federated learning (FL) has aroused a significant interest recently from academia and industry. FL provides a key advantage around privacy since the training nodes are able to create a global model without sharing their data. Specifically, the learning process is carried out through a certain number of training rounds, in which each node updates the parameters of a global model by training on its local data. Then, these parameters are aggregated by a central entity to compute an updated version of the global model, which is shared again with the nodes in each training round. In the case of VIDS, the use of FL allows to build an intrusion detection model while the vehicle’s IVN data are not shared. Despite these advantages, the use of FL for VIDS is still in its infancy, and only a few works have been proposed. In particular, a research work proposes a system integrating a federated DL approach with blockchain using the Car-Hacking Dataset. The authors also evaluate the proposed system considering different configurations of malicious nodes. Furthermore, it proposes a VIDS for the CAN bus using random forests in a federated scenario where models are shared through the blockchain. However, the use of FL for intrusion detection still has to face different challenges around communication overhead, delay, and scalability, as well as security and privacy aspects, even if training data are not disclosed. These challenges are exacerbated in the vehicular context where the communication channel and network topology are highly dynamic due to nodes’ mobility, and, consequently, vehicles may join and leave the training process continuously. Therefore, more research efforts are required evaluating the application of FL techniques in vehicular scenarios under real traffic conditions.

#### *7.5. Honeypots and Watchdogs*

Honeypots and watchdogs can cooperate with, or be an integral part of, in-vehicle IDS to improve security, and increase the overall vehicle’s defense capacity against known or unknown attacks. The adversarial ML assaults against an in-vehicle IDS system may be able to fool the IDS and, generally, any ML-driven component. In this mindset, honeypots and watchdogs can be used for minimizing the available opportunities for the attacker. However, so far, both these security components are not explored much in the VANET literature. In particular, their work proposed a cooperative monitoring process in which several watchdogs were intended to obtain and share evidences about vehicles’ behavior. Then, the resulting dataset was used as an input for a classification approach based on SVM to detect malicious vehicles. Authors also reduced the overhead of the proposed approach by restricting the data analysis to specific nodes and migrating a subset of tuples between detection iterations. Furthermore, they introduced an intelligent watchdog to monitor the behavior of vehicles’ ECUs in order to detect potential faults in such components. It is connected to the ECU through a calibration protocol and, in case of detecting abnormal behavior, it can also be used to perform the ECU’s operation. Moreover, a recent work called *HoneyCar* integrates game theory and vulnerabilities from the common vulnerability and exposure (CVE) database to compute optimal honeypot configuration strategies in the vehicular ecosystem. While these works demonstrate the potential of using watchdogs/honeypots in such scenarios, it has not received much attention from the research community so far.

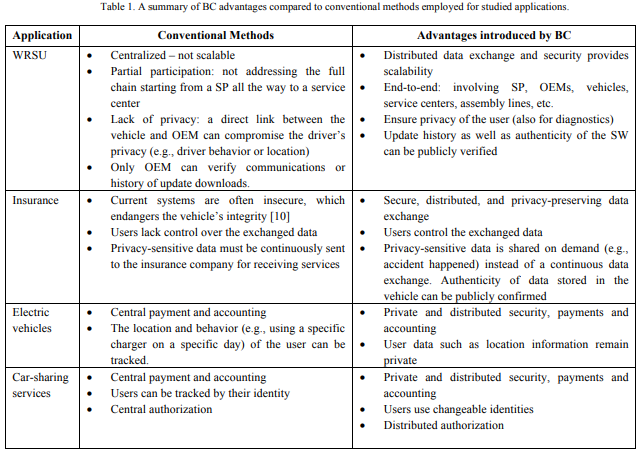
#### *7.6. Mobile Edge Computing for VIDS*

To address the performance and real-time requirements of the vehicular ecosystem, the deployment of edge-computing-based solutions has been widely considered in recent years by using the concept of vehicular edge computing (VEC). The main purpose is to increase storage and computing capabilities at the network to allow end nodes (i.e., vehicles) to offload certain tasks into intermediate devices without the need to use cloud nodes, which can incur an increasing latency. VEC is also intended to facilitate a more efficient approach to manage resource allocation in the vehicular environment, which is considered to be extremely challenging due to frequent network topology changes and communication. In the context of VIDS, the use of edge nodes can facilitate the deployment of more efficient approaches by allowing vehicles to offload the training process to RSUs acting as edge nodes. Indeed, VEC is considered a key component for the deployment of FL-enabled VIDS and FL in general. A potential approach could also be based on vehicles offloading the local training to RSUs, but it could have similar privacy implications to traditional centralized ML approaches. An alternative approach may be based on RSUs acting as the central entity of the FL process by aggregating the model updates calculated by the vehicles themselves using their own local data. In this direction, integrates an edge infrastructure composed of RSUs to build a collaborative intrusion detection model. However, the evaluation does not consider a real vehicle scenario and is based on the obsolete KDDCup99 dataset. Furthermore, the work uses VEC devices acting as blockchain nodes to enable a federated VIDS approach. As already mentioned for the development of FL-enabled VIDS, the deployment of VEC-based solutions still needs additional research considering traffic scenarios with real conditions to demonstrate their feasibility.

#### *7.7. IVN Security for Future CAVs*

As already discussed above, IVNs are currently deployed in environments with limitations in cost, computing capacity, bandwidth, and storage. The evolution of CAVs will eventually lead to new IVN standards. Indeed, such evolution will be realized through an increasing interconnection with vehicles and devices deployed on the roadside composing the so-called Internet of Vehicles (IoV). Therefore, the security concerns of future CAVs will take a broader dimension that needs to address the potential attacks affecting external components, which can be used to launch other attacks over IVNs. As already mentioned, contrary to how CAN was developed, security should be considered in the design phase of these new standards. In fact, standardization activities in the scope of IVNs will be key for the successful deployment of CAVs to come up with a harmonized set of requirements and countermeasures to ensure a more secure vehicular ecosystem. These aspects could also be used to enhance the cybersecurity certification process under a common set of techniques to foster the interoperability of security solutions in such a context.

Reference [2] <https://arxiv.org/ftp/arxiv/papers/1704/1704.00073.pdf>



## *Security and Privacy Analysis:*

In this section, we discuss the privacy and security of the proposed architecture.

**Privacy:** The privacy of the proposed method is derived from the Blockchain (BC) system, where each node employs a unique public key (PK) for communication with other overlay nodes, preventing malicious nodes from tracking an overlay node's activities. Vehicles are equipped with in-vehicle storage to safeguard privacy-sensitive data, and vehicle owners have the option to disclose this data to service providers when necessary, such as in accident claims. To mitigate the risk of a linking attack, where an attacker tries to deanonymize a user by linking different pieces of data associated with the same anonymous user, each user adopts a strategy of using a fresh key for each interaction within the overlay. This proactive measure enhances user privacy by preventing the linkage of public keys and fortifies the overall security of the system.

**Security:** The security of the architecture is predominantly ensured through the use of Blockchain (BC). Each transaction within the Blockchain contains a data hash, ensuring data integrity, and employs asymmetric encryption methods for encryption, providing confidentiality. Access control in the form of a key list maintained by On-Board Modules (OBMs) ensures that only transactions with embedded Public Keys (PKs) matching the OBM's key list can be forwarded to a cluster member. To assess the resilience of the architecture against security attacks targeting smart vehicles, various attack scenarios are evaluated. These scenarios focus on potential threats to the security of smart vehicles and aim to determine the architecture's ability to withstand and mitigate such attacks.

**Changing a software binary in the cloud:** In scenarios where an attacker aims to compromise cloud storage and tamper with the software binary to inject malware into numerous vehicles, the discrepancy between the hash of the infected binary and the hash included in the multisig transaction, jointly signed by the software provider and the original equipment manufacturer (OEM), enables vehicles to promptly identify such attacks before installing the compromised software update. This mechanism ensures that the authenticity of the software remains intact, as any alteration in the binary triggers a hash mismatch, providing a robust defense against potential malware injection attempts by unauthorized entities.

**Distributing a false update by claiming to be the OEM or SW update provider:** The overlay nodes possess knowledge of the public keys (PK) associated with the Original Equipment Manufacturer (OEM) and the Software Provider (SW provider). This knowledge acts as a safeguard, preventing an attacker from falsely asserting to be either the OEM or the SW provider. Such a deceptive claim would necessitate possession of the private key corresponding to the relevant public key associated with the respective entities. This security measure reinforces the authentication process, ensuring that only entities with the proper private key can legitimately represent themselves as the OEM or SW provider within the network.

**Distributed Denial of Service (DDoS) attack:** In orchestrating a DDoS attack, the attacker must compromise a substantial number of vehicles within the overlay network. These compromised vehicles then flood a specific overlay node with numerous transactions, aiming to overwhelm it. Transactions are broadcast to all Overlay Blockchain Modules (OBMs), and an OBM forwards a transaction to a cluster member only if the keys in the transaction match with a key pair in the OBM's key list. Overlay nodes grant authorization to requesters by uploading key pairs to the key list of the OBM. Transactions involved in the DDoS attack, lacking matching key pairs, are consequently dropped, mitigating their impact on the targeted node.

**Future Research Directions In this section, we summarize future research directions:**

• **Key management:** Each vehicle owns multiple keys for communication with SPs or users, which may change during the vehicle lifetime. Managing keys introduces a new research challenge.

• **Caching data:** Each connected vehicle, must download data, e.g. SW update, from a cloud which incurs packet overhead and delay in the overlay. Introducing caching in OBMs can reduce such overhead.

• **Applications:** The proposed architecture suits a broader range of applications, e.g. congestion control that can be explored in more detail.

• **Mobility:** Frequent mobility of the vehicles increases the packet and processing overhead resulting from the handover process. New mobility-friendly methods can be introduced to reduce this overhead.