J. A. Onieva, R. Rios, R. Roman, and J. Lopez, "Edge-Assisted Vehicular Networks Security", *IEEE Internet of Things Journal*, vol. 6, pp. 8038-8045, 2019.
http://doi.org/10.1109/JIOT.2019.2904323
NICS Lab. Publications: https://www.nics.uma.es/publications

Edge-Assisted Vehicular Networks Security

Jose A. Onieva, Ruben Rios, Rodrigo Roman, *Member, IEEE* and Javier Lopez, *Senior Member, IEEE*

***Abstract*— Edge Computing paradigms are expected to solve some major problems affecting current application scenarios that rely on Cloud computing resources to operate. These novel paradigms will bring computational resources closer to the users and by doing so they will not only reduce network latency and bandwidth utilization but will also introduce some attractive context-awareness features to these systems. In this paper we show how the enticing features introduced by Edge Computing paradigms can be exploited to improve security and privacy in the critical scenario of vehicular networks (VN), especially existing authentication and revocation issues. In particular, we analyze the security challenges in VN and describe three deployment models for vehicular edge computing, which refrain from using vehicular-to-vehicular communications. The result is that the burden imposed to vehicles is considerably reduced without sacrificing the security or functional features expected in vehicular scenarios.**

***Index Terms*—Internet of Things, Vehicular Networks, Critical Infrastructures, Security, Privacy**

I. Introduction

Critical infrastructures are those assets, services and facilities whose functioning are essential for the operation and wellness of society. These include, among others, the power and water supply systems, the telecommunications and financial systems, and also transportation systems [1].

Transportation systems have a tremendous impact on the daily transport of cargo and people. Problems affecting the transportation system can affect not only the supply and distribution of nourishment but may also imply the loss of human lives. In fact, many people get injured and die every day in road accidents [2]. For that reason, road safety is one of the most promising and eagerly awaited applications of intelligent transportation systems and the Internet of Vehicles [3].

At the core of such transportation systems, we can find a communication infrastructure known as vehicular networks (VN). Vehicular networks can help minimize the risk of accidents, thanks to services like the broadcasting of safety and alert messages. These messages can contain relevant information about the vehicle and the context surrounding it (e.g., the presence of an obstacle or an accident) thus allowing other vehicles to anticipate and prevent dangerous situations.

Given the broadcast nature of this type of messages (i.e., they must be available to any nearby vehicle) and the real-time requirements of road safety application, these messages are usually sent unencrypted. However, it is paramount to authenticate the sender of these messages in order to prevent malicious entities from injecting false data or replaying old messages, as this may result in disastrous consequences, such as traffic congestion and most notably car accidents.

The challenge of authenticating data senders is core to the successful deployment of vehicular networks. Therefore, authentication has been approached by different security standards, such as IEEE 1609.2 and ETSI TS 102 941, mainly by means of a public key infrastructure (PKI) as in traditional networks. Other ITS security-related standards are currently under development, such as ISO/CD TR 17427-5, ISO/AWI TS 21177 and ISO/AWI TS 21185, but no final details are officially confirmed about the means by which authentication will be provided.

Therefore, in current standards, besides issuing digital certificates, which vehicles attach to signed messages for authentication, the PKI has to deal with the creation and distribution of certificate revocation lists (CRL). Prior to accepting a message as valid, it is necessary to check that the certificate is not in the CRL as this would be an indicative of a malicious behavior. Indeed, the retrieval and checking of bulky CRLs is one of the main limiting factors of using PKIs for authentication in vehicular networks and thus some alternative mechanisms have been suggested [4], but none of them can completely solve the aforementioned problems.

As we will show later (see Section III) the communication model is of paramount importance to the challenges VN face. Furthermore, not only authentication is a key property in VN. Location and Identity Privacy are features that necessarily come along with the authentication scheme. Vehicle owners will be reluctant to disclose their routes and identity when communicating and interacting in VN environments.

It is precisely a paradigm shift and a greater support from industry and Consortiums (e.g. Cisco, Nokia, IBM, etc.) to MEC (Multi-access Edge Computing) which brings the opportunity to overcome some of the difficulties encountered so far. After all, vehicle-to-vehicle communications may not be the best solution to achieve the desired authentication and privacy, and current deployments [5] seem to discredit the prior belief that applications with real-time requirements need to be based on inter-vehicle communications.

Therefore, in this paper, we summarize the state of the art on Vehicular Networks security and some pending challenges. Then, we identify how these challenges (such as

This work has been partially supported by the Spanish Ministry of Economy and Competitiveness through the SMOG (TIN2016-79095-C2-1-R) project. The second author is funded by the 'Captación de Talento para la Investigación' fellowship from the University of Malaga.

J. A. Onieva, R. Ríos, R. Román, and J. López are with the University of Málaga, Campus de Teatinos s/n, 29071, Málaga, Spain (email: {onieva, ruben, roman, jlm}@lcc.uma.es).

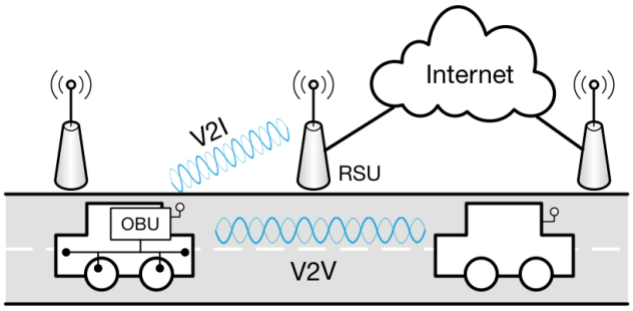

Fig. 1. Simplified vision of a Vehicular Network.

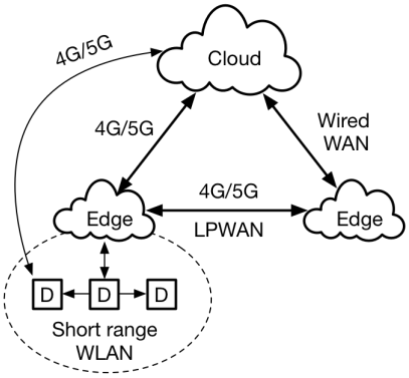

Fig. 2. Simplified vision of Edge Computing.

authentication, anonymity and digital evidence) can be tackled by edge technologies, and analyze how some of these security services can be integrated on Vehicular Edge Computing (VEC) scenarios without relying on inter-vehicle communications. This analysis goes a step beyond the existing state of the art on this area, which focuses on studying the security challenges of edge-enabled Vehicular Networks and providing specific solutions to particular problems.

The rest of the paper is organized as follows. First, we provide some background information on vehicular networks and edge computing highlighting their similarities and differences. Next, in Section III, we review the literature to identify the most relevant security challenges in vehicular networks. Section IV presents our vision of a vehicular edge computing paradigm together with possible deployment models. Finally, Section V analyses how VEC can solve some of the security problems identified in Section III. The conclusions of this paper are presented in Section VI.

II. Background

A. Vehicular Networks

Vehicular networks can be seen as one of the core elements of Intelligent Transportation Systems (ITS) and the Internet of Vehicles (IoV). While resembling traditional sensor and ad-hoc networks in some respects, vehicular networks pose a number of unique challenges. In the scientific literature, several definitions of vehicular networks coexist. In this study, we define a vehicular network trying to convey all the aspects gathered by previous studies while highlighting the unique features of it.

A vehicular network is composed of moving vehicles, which communicate between them vehicle-to-vehicle (V2V), and with the roadside infrastructure vehicle-to-infrastructure (V2I) in order to enable road safety and infotainment applications. This communication can be achieved using cellular technologies (e.g. LTE) or other approaches. A salient feature of these networks is that vehicles are considered to be highly dynamic and fast moving while the infrastructure consists of static nodes. See Fig. 1 for a simplified representation of this scenario.

Vehicle nodes are considered to have limited but sufficient computing and storage capabilities thanks to cutting-edge on-board units (OBU), which internally communicate with the various sensor units the vehicle is equipped with (e.g., front and rear video cameras, LIDAR systems, radars, airbags, tyre pressure, wheel speed sensors, etc.). The static nodes of the network are road-site units (RSU) located at a short distance/range of the vehicles. The communication model of these static nodes with the rest of the infrastructure (and its security profile) is often out of the scope of the vehicular network itself. Note that these elements can appear with different names and deployments options in some ITS standards (e.g. ISO 21217:2014 name them CALM-complaint ITS stations).

At the application level, both cellular-based V2V networks such as C-V2X and other technologies such as 802.11p make use of dedicated vehicular protocols to provide various services, such as broadcasting safety messages. Among these dedicated protocols is DSRC/WAVE (Dedicated Short Range Communications/Wireless Access for Vehicular Environment). All messages sent in the vehicular network are usually broadcast periodically in so-called (authenticated) beacon messages. This might endanger the privacy of drivers, reason for which private authentication schemes are needed.

Traditional vehicular networks consider a communication model in the V2V plane. This model contemplates the case that vehicles cooperate to form a vehicular ad-hoc network without the intervention of RSUs. This involves not only communications between neighboring vehicles but also multihop communications taking advantage of other vehicles as relays. This type of V2V communication is said to be important in case RSUs become unavailable. However, it complicates authentication and privacy issues extensively.

B. Edge Computing

Edge computing encompasses various paradigms (e.g., Multi-Access Edge Computing, Mobile Edge Computing, Fog Computing) that aim to decentralize the Cloud and bring the computational and storage power closer to end-users. By doing so, edge computing paradigms will not only improve user experience due to a reduction of network latency and the overall response time of the system, but will also diminish the bandwidth utilization between the edge and the core of the network, where computing resources are traditionally located in a Cloud environment.

But rather than being a replacement for the Cloud, Edge Computing can be seen as an extension of it (see Fig. 2). Edge devices are expected to coexist with the Cloud conforming a three-tier architecture composed of:

1. *End-user devices*: are the final clients of the system. They are heterogeneous devices (D) that use the Edge to support their operation. Examples of these devices include smartphones, sensor nodes, and mostly any device constrained in some computing sense.
2. *Edge devices*: can be regarded as mini-cloud servers which are geographically distributed and offer services like computational and memory offloading, network and hardware virtualization, etc. They might be deployed in cellular towers, dedicated in-house computers, gateways, routers, and so on.
3. *Cloud servers*: are extremely powerful computers located in a remote location, which basically offer the same services as edge devices but at a larger scale.

Note that the inner tier of the architecture may consist of several layers of devices. In general, the further away from the end-user the more powerful the devices are. Typically, higher-level devices are mostly used for orchestration and management purposes as well as a mechanism for backing up historical and aggregated information. However, the edge is expected to be self-sufficient and not strongly dependent on the existence of higher-level devices.

Based on the above description, we observe that edge computing paradigms and vehicular networks share many similarities. Notwithstanding, edge computing also introduces some disruptive technologies (SDN, NFV, 5G, etc.) not readily available in traditional vehicular networks, which are capable of improving the efficiency, bandwidth utilization, network latency and thereby the overall response time of vehicular systems. Therefore, edge computing is a suitable candidate technology for satisfying the particular requirements of vehicular networks. In particular, timeliness, scalability and reliability are key features provided by Edge Computing, which are crucial to vehicular networks. As we will show later, the novel features and technologies introduced by edge computing will also have a positive impact on the security of vehicular networks.

Moreover, this new paradigm reduces the need for direct communication among end-user devices since edge components can serve as relays of the messages of the network and (pre)process them if needed.

III. Security Challenges in Vehicular Networks

Security services are critical to the deployment of VNs mostly due to the importance of avoiding fake and malicious messages in road-safety applications. Existing solutions and standards typically rely on PKI to solve authentication problems. However, this complicates the task of protecting driver's privacy (and location tracking). As we will show shortly, this issue has been the target of intensive research.

Any authentication scheme in VN involve different phases:

- *ITS initialization*. All participating entities are assumed to register with the ITS Certification Authority for the purpose of obtaining valid credentials. This includes general purpose edge nodes at all levels, RSUs and OBUs. These credentials can have different formats depending on the underlying cryptography.
- *Communication*. V2I and V2V messages are sent using the credentials obtained previously. Depending on the type of credentials, different cryptographic primitives can be used like message authentication codes (MAC) or digital signatures. The latter is the preferred choice.
- *Verification*. Once a message is received, the vehicles need to verify its authenticity; that is, whether the message comes from a legitimate node in the network. To that end, it is required the source's credentials and to check those credentials' status.
- *Revocation*. This mechanism allows the infrastructure to cancel credentials that are deemed to be invalid.

As stated before, achieving authentication and privacy poses unique challenges. Nonetheless, some schemes (including the standard for instance) have managed to fulfil both properties at the same time. Among them, the most studied approach is the use of pseudonyms (see [6] for an extensive survey). This is similar to public key solutions, but certificates are not directly linked to a real identity. Furthermore, in order to provide untraceability, pseudonyms need to change over time, location or context. This is achieved by either storing a pool of pseudonyms or changing them on-demand.

There must also exist a process to allow a trusted authority to revoke the anonymity of a user (i.e., disclose the vehicle's identification number (VID) or electronic license plate) in case the user misbehaves. To that end, during ITS initialization, this privileged entity retains escrow information that enables mapping the issued pseudonyms to the identity of the pseudonym holder.

Two major approaches can be distinguished for pseudonym issuance during ITS initialization: third-party issuance and self-issuance. The majority of approaches rely on third-party issuance (including 1609.2 standard). This party receives different names (CA, Pseudonym Provider, Trusted Authority, etc.). Even more, there are different authorities fulfilling different roles (e.g. enrolment, authorization, issuance, etc.).

These pseudonym schemes can be categorized based on the cryptographic mechanisms they employ into [6]: asymmetric cryptography, identity-based cryptography, group signatures and symmetric cryptography. All of them present their pros and cons. For instance, group signatures authentication schemes (and group management in general) make highly dynamic and fast moving nodes a drawback being the pure P2P communication model the main responsible. Amongst them, asymmetric and identity-based schemes (both with similar characteristics) seem to be the most viable approaches for realizing pseudonymity in vehicular networks. For more details, refer to the aforementioned survey.

Whatever the case, an inherent characteristic to all of these schemes is the management of credentials revocation. Vehicles need to verify the authenticity of the messages they receive and thus, credentials used at the time of verification

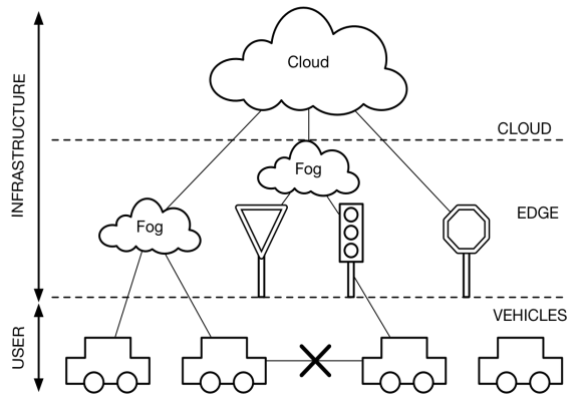

Fig. 3. VEC deployment models.

cannot be revoked or expired. As a consequence, the workload of managing revocation information falls on the vehicles, which affects considerably the latency and network bandwidth. Avoiding this overhead is difficult unless it is handled in a less distributed way. That is, by nodes others than the vehicles themselves but sufficiently close to not increase latency.

There has been little research on VN digital evidence generation and custody. Kopylova et al [7] presented an accident reconstruction scheme for VANETs, with special focus on evidence generation and treatment. How this evidence is securely stored is out of the scope of their work. In [8] authors make the collection of evidence and witnesses the focus of their work, but only from the vehicle point of view (requester) and functionally oriented to demonstrate vehicle's facts, like for instance when in need for challenging a driving fine.

Inter-vehicle communications seem to be a promising antidote to improve the efficiency of road traffic. However, it often encounters disruptions due to high mobility of vehicles causing frequent failures of communication links. This requires additional solutions in order to provide protection against availability failures.

Furthermore, threats to availability are very difficult to protect against. The most common threat to availability is Denial of Service (DoS) attacks in which a high volume of false messages are put into the network with the aim of exhausting ITS stations. Since real-time message distribution is key for vehicular networks functionality, providing techniques to enhance availability is of key importance. Some solutions have been suggested as a countermeasure to DoS attacks in VANETs [9], mainly based on changing technologies, channels or routing features when an attack is detected. This, however, requires prompt reaction.

As already discussed, in VN, anonymous certificates or pseudonyms (named authorization certificates in the standard 1609.2) are used in order to detach the right to access network services from drivers' identities. And these (as well as addresses in lower levels of the protocol stack) need to change periodically in order to avoid vehicle tracking. This provides an acceptable level of anonymity, but in some situations (e.g. safety beaconing) the pseudonym update frequency demand becomes very high as a consequence of the constant need of packets from the vehicles. And the pseudonym change requirement comes at no negligible cost [10].

IV. Vehicular Edge Computing

Vehicular Edge Computing (VEC) can be easily understood as the application of edge computing to vehicular networks. This is not to be confused with the definition contributed by other authors (e.g., [11]), who consider vehicles as edge devices themselves. Although this is an interesting deployment model, we consider vehicles as mere end-users of the infrastructure. Indeed, several studies have started to drive in that direction, as for instance [12], in which predictive vehicle computation offloading to edge devices is tested. Note that this possibility goes beyond outsourcing computation tasks, since virtualization allows transparent and on-the-move tasks completion.

In our definition of VEC we envision three deployment models which can seamlessly coexist. These models, though more simplistic than the models envisioned by other authors, satisfy the most usable and practical scenarios and they can be realized with current technologies and standardization efforts.

A. Deployment models

We distinguish between the user and the infrastructure planes in our definition of VEC. These planes are clearly separated, as shown in Fig. 3. The devices in the infrastructure plane are organized in several layers, but as in traditional edge computing, there is typically a cloud and an edge layer. Based on the way the edge layer is set up, we foresee three possible deployment models:

1. *Fog-based deployment*: This model is based on the utilization of general-purpose fog/edge devices to assist vehicular networks. These general purpose devices have large storage and strong computation capabilities and they can manage communication and computation with multiple vehicles simultaneously, assisting them not only in safety-related applications but also in augmented reality scenarios, data analytics services, infotainment applications, etc.
   This might be possible in several locations like cities or highways, with these devices deployed in cellular towers, shopping malls, etc. However, we consider this deployment model is more likely to occur in sparsely populated regions to avoid the cost of deploying dedicated devices. For instance, some highways span over several kilometers with limited traffic volume. In these situations, short-range communications are uneconomical and the service can still be provided by a lesser number of cellular devices. In fact, we expect the first real-world VEC deployments to use this model, since general-purpose hardware for edge nodes is already in place.
2. *RSU-based deployment*: This deployment model considers the use of roadside devices to support the realization of vehicular networks. These devices are similar to the concept of RSU in traditional vehicular

networks and they are typically attached to road signs, traffic lights, bus stops, etc. These RSUs-like devices typically have less storage and computational capabilities than general-purpose edge devices, but still sufficient for the provision of security services. We consider this type of deployment is more likely in areas where cellular coverage is limited, unstable or jammed. These devices are sufficiently autonomous to operate and support vehicular networks without a continuous link to higher-level devices, such as the Cloud.
As in the previous case, this can be deployed in any scenario, but seems to be more efficient in terms of cost for use cases where the number of vehicles is high.

3. *Hybrid deployment*: This deployment model considers the use of dedicated and general-purpose edge devices typically organized in two tiers. This provides vehicles better communication coverage, more computational and memory resources, and some means for redundancy. Therefore, this model might be more likely in densely constructed areas. We expect this model to be the most predominant one in the future of VEC.

In all models, general-purpose edge nodes and RSUs can be compromised and therefore, security services must not make any assumptions. Nevertheless, it is expected that some general-purpose edge nodes (especially those installed in 5G antennas and intermediate level edge nodes) will be housed in secure facilities and equipped with tamper-resistant hardware modules.

Note that we assume that direct communication between vehicles is suppressed in these deployment scenarios. Even if existing cellular standards like C-V2X provide support for V2V communications, not only we consider that the capabilities of the edge renders V2V communications unnecessary, but at the same time it saves vehicles from P2P, ad-hoc and collision resolution protocols management, since now all these features devolve upon the (edge) infrastructure. We should also note that, even if V2V communications are still available, our analyses will show that security can be greatly be improved thanks to the integration of V2I communications and Vehicular Edge Computing.

It may be argued that suppressing V2V negatively impacts the ability of vehicles to communicate with each other when road-side infrastructure is not available. However, recent advances in cellular communications significantly reduce this risk. In fact, the C-V2X specification defines how vehicles can communicate with each other taking advantage of the cellular infrastructure. Still, there may be regions where the cellular signal is limited or unstable. These situations will not only be rather unusual but also more likely to occur in areas where traffic density is low, such as rural areas. As previously stated, this situation can be overcome with the deployment of RSU-like devices.

Moreover, even though vehicular communication standards, such as DSRC and WAVE, were not designed to cover all deployment models described above, they consider the coexistence with, and even their encapsulation within, other communication protocols. Consequently, the envisioned deployment models can be fulfilled with existing technologies and standards.

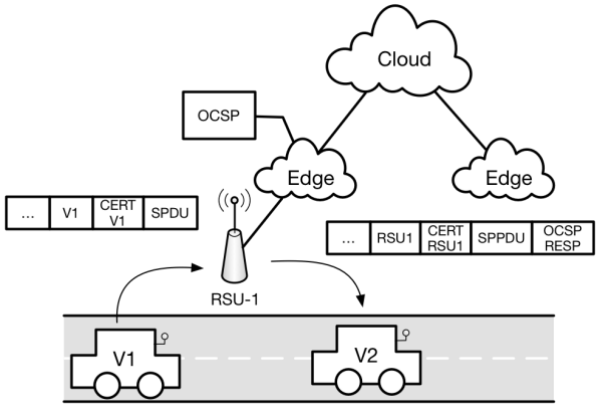

Fig. 4. Packet Transformation.

V. Edge-Assisted Security

Some of the difficulties found so far in VN can be overcome with the application of Edge computing to compliment security services in this paradigm. As previously stated, one of the most important security services and key to vehicular networks is authentication. However, this is not the only service where the application of edge computing can report benefits. Also note that the choice of the deployment model does not have a significant impact on the properties analyzed next.

A. Authentication

In traditional vehicular networks, beacon and safety messages are transmitted using either V2V or V2I communications. Conversely, in our vision of VEC, we eliminate the possibility of using V2V and thereby messages sent by vehicles must be necessarily relayed by edge nodes to reach other vehicles. These messages are authenticated in the same way it is done in VANETs. Therefore, some sort of pseudonym mechanisms must be in place to ensure identity and location privacy. Also, strategies for updating pseudonyms are to be applied in this context.

As seen in Fig 4, messages received by edge nodes (such as authenticated beacon and safety messages, e.g. related to hazardous situations) are modified accordingly in order to reflect the new message packet source and insert the required information (e.g. the GPS location and optionally the source address of the original alert message) into them. This implies more cost on edge devices, but the computational overhead imposed by packet transformation can be regarded as negligible. The most resource-consuming task for edge devices is to verify the revocation status of the vehicle that transmits the message because the edge will only forward the message if the vehicle is considered to be trustworthy.

After the edge device has verified the correct status of the sender and forwarded the message, recipient vehicles only need to verify the revocation status of edge device. This

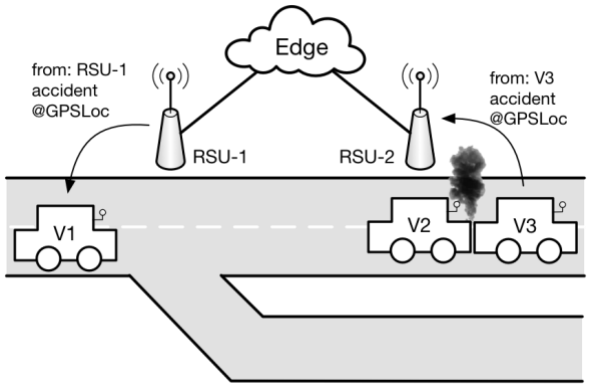

Fig. 5. Packet transformation and anonymity.

reduces significantly the burden of CRLs management, since vehicles do not need to deal with the revocation status information of millions of vehicles any more.

Just as an approximation exercise, it is foreseen that in the year 2020 there will be around 152M of connected cars [13]. Assuming the same probability of misbehavior than in X.509 PKIs, it has been estimated by NIST [14] that the number of certificates to be revoked is about 10%. That means 15,2M of revoked certificates worldwide. Even if we consider 100 different ITS infrastructures, that amounts to 152k revoked certificates by year 2020. DSRC and WAVE standards are known to provide up to 6Mbps [15] communication bandwidth. An X.509 base CRL containing around 152k revoked certificates has a size of approximately 27 Mbits, meaning that an average short range connection (3Mbps) will take around 9 seconds to download the CRL. This is a precious time for safety-related applications.

Notwithstanding, the distributed nature of VEC can help overcome this issue. It is possible to have a base CRL in the Cloud and relevant portions of it closer to the geographical location of vehicles demanding them. These CRLs can be handled by surrogate certification authority services running in trustworthy edge devices. By having these services distributed within the VEC infrastructure it is also possible to reduce the update interval of those geo-located CRLs since any evidence of misbehavior can be analyzed in context in a more timely manner. These changes could be later propagated to higher-level CRLs. This way, time-sensitive operations like authenticated beacon broadcasting can be executed properly. Note that, in fact, these proposals match those provided by the 1609.2 standard in which certificates and CRLs can be geo-located and Misbehavior Authorities are defined.

Actually, other solutions for revocation management exist: delta CRLs (which just makes the download of revocation lists less frequent), the use of balanced hash trees for CRLs distribution, etc. but all of them have one thing in common: they will grow with the number of anonymous certificates revoked. Switching to Vehicular Edge Computing as we envision it, has its advantages: some of the infrastructure edge nodes (e.g. cellular towers) will be less prone to be tampered with and therefore less revocations to be managed by vehicles. Edge nodes need vehicular revocation status, but these devices (general-purpose or RSUs) are always connected to the infrastructure and in most cases their bandwidth can be greatly increased.

Furthermore, OCSP (Online Certificate Status Protocol) stapling techniques nowadays used in PKIs can be exported to these scenarios as a complement, in order to eliminate the need of receiving vehicles for checking infrastructure nodes' certificate validity using CRLs. OCSP servers can be distributed in the higher levels of the infrastructure. In this way, edge nodes and RSUs will repeatedly request OCSP responses for their own certificates within a time window in such a manner that they can attach these signed status responses with the messages they relay to vehicles. It is important to highlight that this type of solution may be inadequate for RSU-based deployments as it is conceived for regions where network connectivity is unstable and we consider it is not secure to deploy OCSP servers in RSU-like devices as they may be tampered with.

B. Anonymity

The use of the edge as intermediary in all communications introduces some privacy benefits. Sending data to another vehicle through an edge device hides the original data sender and thus the sender protects its pseudonym, because, for a time-window, the beacon messages can be relayed and repeated by the RSU/edge node. Suppose there is an accident in the road (see Fig. 5) and some of the cars involved, V3, report this situation to the Edge. By transforming the messages, the edge node hides the identity of the original sender from remote vehicles as they are not in the range of the original data sender. This implies that less pseudonym changes are needed to preserve vehicle's privacy.

An additional advantage is on the data analysis functions provided by the infrastructure. As the data goes up every layer, the data is usually (geo-)aggregated and context-aware services are provided to wider (and less accurate) geo positions. Therefore, if any of the upper levels of the infrastructure is compromised, the data stored will not contain identifying information or its precision will be put individual privacy at risk. In [16], for instance, we observe a fog-assisted traffic control system that leverages the fog nodes in order to come up with local and global decisions for traffic lights. In such system, global decisions are made with aggregated data and thus drivers' raw data is not exposed.

C. Digital Evidence and Misbehavior Detection

An important part is lost due to the proposed message relay mechanism: since both edge devices and vehicles can be compromised, in case of faked sensed data, the receiver cannot confirm which is the actual misbehaving entity. Fake data can come from either the infrastructure or another vehicle.

This situation is easily solved if edge nodes keep evidence, when needed, of received messages. As it occurs in VN, in VEC all messages may be signed and authors cannot therefore deny having sent them (i.e. non-repudiation of origin). For example, a vehicle that is sending misleading information on the state of the roads can be identified by the VEC

architecture, which will then take the appropriate measures such revocating its certificate and informing the authorities.

Thus, when the edge node receives a message from a vehicle, it firstly categorizes it. If the message is safety-related and includes sensed data, it stores it. If not, it relays it and keeps no evidence of it. Edge nodes can periodically send these evidence to the upper levels of the edge computing infrastructure, since the storage size of the cloud is assumed to be unlimited. Therefore, RSUs and close edge nodes only need to store evidence for a limited amount of time. Even under lossy network conditions this is not problematic and thus the deployment model does not have an impact.

When this data reaches a determined intermediate edge node, data analysis can be performed in order to identify misbehaviour communications. This matches and complements the processes defined in the standard 1609.2 of Misbehaviour Authority deployment and misbehaviour reports definition. Since this task does not need to be performed by Cloud servers themselves, not only prompt reaction to vector attacks will be possible, but also geolocated configuration and response actions against them.

The higher the level in the infrastructure the more powerful this analysis functions become. For instance, if a pseudonym A is used in a particular location and the same pseudonym is used in a remote location, say 100 kms away, in a very short period of time, intermediate edge nodes can directly revoke the credentials, update OCSP servers and push the CRLs to the edge nodes under its hierarchy. Another example of this can be found in [16], in which big data analysis is used in order to detect compromised nodes.

D. Availability

The application of edge computing to vehicular networks also has a positive impact on the availability of trustworthy devices to manage communications. This is made possible due to (i) the tiered architecture in these deployments and (ii) the fact that intermediate edge devices are considered to be physically protected and/or equipped with tamper-resistant hardware modules.

Fog-based deployments will most presumably rely on cellular towers to host VEC applications. Moreover, their operation is expected to be founded upon a root of trust. Therefore, it is very unlikely for them to be manipulated (although not impossible). The main limitation of this deployment model is that a single edge device serves a large area and if it stops working a large number of vehicles will not be able to communicate. Even though this may seem as a big issue, cellular networks tend to cover overlapping areas in order to offer some fault tolerance.

A deployment model consisting of RSU-like units alone presents a different problem. Since these devices are deployed in public areas, they are subject to malfunctioning and to manipulation from attackers. As a result, their certificates might need to be revoked in order to prevent faulty or compromised devices to communicate. Clearly, this is a problem that could be diminished by means of redundant RSU-like devices but as a matter of fact this type of solution has an important economic impact.

A more scalable approach is to rely on a hybrid deployment model such that whenever a RSU-like unit is detected to be compromised, faulty or unresponsive, its certificate is revoked and the edge device supervising that unit takes over. The edge device above RSU-like devices can deal with the communications of revoked units in its area while they are repaired.

Additionally, availability is not a synonym of over deployment. This is another distinctive feature of VEC. Thanks to the use of inherent secure virtualization and SDN (Software Defined Networks) in Edge Computing technologies, the need of computing power and storage requirements can be predicted [17] and distributed as needed. That is, services and functionality provided by the VEC infrastructure will move with the traffic flow in a predictive and timely manner.

As a consequence, fault and congestion tolerance can be achieved. For instance, if a vehicle V1 enters an area in which a faulty or revoked RSU is, thanks to the presence of a second tier with larger coverage (in hybrid deployments), no functionality disruption would occur. Similarly, the presence of numerous vehicles during peak hours should not lessen QoS for vehicle V1, since data analysis allows for service congestion prediction and SDN facilitates managing data congestion (e.g. using Reliable Group Data Delivery trees through OpenFlow or any other proprietary solution). Furthermore, thanks to NFV the edges nodes can replicate network elements on demand. This means V1 will perceive and always-on service in the presence of faults.

VI. Conclusion

Edge technologies will change the way devices interact with each other and the network. And vehicles are part of that universal equation. They are and will become part of the Internet of Vehicles: full digital devices with sensing, computing and communication capacities.

In the (near) future, we will see vehicles as any other device with some distinguishing characteristics: highly mobile, real-time demanding, mainly safety-oriented and secure-critical. Yet, as essential components of the transportation system critical infrastructure, any attack against them will not only affect other essential sectors (e.g. economic and social services), but also human lives.

This is precisely why we have focused this research on the intersection between edge technologies and secure-critical services like authentication, anonymity, digital evidence, and availability. We believe edge technologies will be ready soon to offer enhanced security services to vehicular networks, contributing key features to security: management of local environments with little or no dependence on remote powerful data and computation cloud servers, and provisioning of context information that can be aggregated and analyzed.

References

[1] M. Theoharidou, M. Kandias, and D. Gritzalis, “Securing Transportation-Critical Infrastructures: Trends and Perspectives”. In

Proc. Global Security, Safety and Sustainability & e-Democracy, Thessaloniki, Greece, August 2011, pp. 171–178.
[2] European Commission, "Road Safety: Statistics – accidents data", https://ec.europa.eu/transport/road_safety/specialist/statistics_en Accessed on Jan 2019.
[3] J. Contreras, S. Zeadally, J. A. Guerrero-Ibañez, "Internet of Vehicles: Architecture, Protocols, and Security", IEEE Internet of Things, vol. 5, no. 5, pp. 3701–3709, Oct. 2018, doi:10.1109/JIOT.2017.2690902.
[4] S.S. Manvi, and S. Tangade, "A survey on authentication schemes in VANETs for secured communication", *Vehicular Communications*, vol. 9, pp. 19–30, July 2017, doi:10.1016/J.VEHCOM.2017.02.001.
[5] Nokia, "Safer and efficient highway ready for future mobility" https://networks.nokia.com/use-case/highways/C-V2X-communications. Accessed on Jan 2019.
[6] J. Petit, F. Schaub, M. Feiri, and F. Kargl, "Pseudonym Schemes in Vehicular Networks: A Survey", *IEEE Communications Surveys & Tutorials*, vol. 17, no. 1, pp. 228–255, first quarter 2015, doi:10.1109/COMST.2014.2345420.
[7] Y. Kopylova, C. Farkas, and W. Xu, "Accurate Accident Reconstruction in VANET". In *Proc. Data and Applications Security and Privacy XXV*, Richmond, VA, USA, July 2011, pp. 271–279.
[8] J. de Fuentes, L. Gonzalez-Manzano, A. Gonzalez-Tablas, and J. Blasco, "WEVAN – A mechanism for evidence creation and verification in VANETs," *Journal of Systems Architecture*, vol. 59, no. 10, pp. 985–995, November 2013, doi:10.1016/j.sysarc.2013.07.009.
[9] H. Hasbullah, I. A. Soomro, and J. A. Manan, "Denial of Service (DOS) Attack and Its Possible Solutions in VANET", *International Journal of Electrical, Computer, Energetic, Electronic and Communication Engineering*, vol. 4, no. 5, pp. 813–817, 2010.
[10] E. Fonseca, A. Festag, R. Baldessari, and R. I. Aguiar, "Support of Anonymity in VANETs - Putting Pseudonymity into Practice". In *Proc. IEEE Wireless Communications and Networking Conference (WCNC)*, Hong Kong, March 2007, pp. 3400–3405.
[11] Y. Xiao, and C. Zhu, "Vehicular fog computing: Vision and challenges". In *Proc. IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, Kona, HI, USA, March 2017, pp. 6–9.
[12] K. Zhang, Y. Mao, S. Leng, Y. He, and Y. Zhang, "Mobile-Edge Computing for Vehicular Networks: A Promising Network Paradigm with Predictive Off-Loading", *IEEE Vehicular Technology Magazine*, vol. 12, no. 2, pp. 36–44, April 2017, doi:10.1109/MVT.2017.2668838.
[13] N. McCarthy, "Connected Cars by the Numbers", https://www.forbes.com/sites/niallmccarthy/2015/01/27/connected-cars-by-the-numbers-infographic/#2256d6e71028. Accessed on Jan2019.
[14] S. Berkovits, S. Chokhani, J. A. Furlong, J. A. Geiter, and J. C. Guild, "Public key infrastructure study", Final Report. Produced by MITRE Corporation for NIST, 1994.
[15] J. B. Kenney, "Dedicated Short-Range Communications (DSRC) Standards in the United States", *Proceedings of the IEEE*, vol. 99, no. 7, pp. 1162–1182, June 2011, doi:10.1109/JPROC.2011.2132790.
[16] C. Huang, R. Lu, and K.-K. R Choo, "Vehicular Fog Computing: Architecture, Use Case, and Security and Forensic Challenges", *IEEE Communications Magazine*, vol. 55, no. 11, pp. 105–111, November 2017, doi:10.1109/MCOM.2017.1700322.
[17] A. Ermagun, D. Levinson, "Spatiotemporal traffic forecasting: review and proposed directions, Transport Reviews", *Transport Reviews*, vol. 38, no. 6, pp. 786–814, 2018, doi: 10.1080/01441647.2018.1442887.

Jose A. Onieva received his PhD degree from the University of Malaga (2006). He has been actively involved in ICT European and national funded information security related projects. He has published in several international journal and conferences in the field of Information Security. He is author of the book "Secure Multi-Party Non-Repudiation Protocols and Applications" published by Springer. Since 2011 he has been working as an Associate Professor in the Computer Science Department at the University of Malaga. Currently involved in the research of core security services for edge computing, covert channels and digital evidence.

Ruben Rios is a Postdoctoral Researcher at the University of Malaga, Spain. His main research activities are centered on the design and development of solutions for the protection of digital privacy and anonymity with a focus on scenarios with resource-constrained devices. He is also interested in the security of Edge Computing platforms and services. Dr. Rios was awarded the FPU fellowship from the Spanish Ministry of Education and received the prize to the most outstanding Ph.D. thesis from the University of Malaga.

Rodrigo Roman is an Assistant Professor at the University of Malaga, Spain. His main topic of research is the protection of Internet of Things architectures and its building block technologies in various contexts, such as Industry 4.0 and digital homes. In addition, Dr. Roman is currently researching the security challenges of all Edge infrastructures, such as Fog Computing and Multi-Access Edge Computing. He has participated in several Spanish and European research projects, and published more than 40 articles in various international journals and conference.

Javier Lopez is Full Professor at the University of Malaga and Head of the Network, Information and Computer Security Laboratory (NICS Lab). His research activities focus on network & information security and Critical Information Infrastructures. He is currently Editor-in-Chief of the International Journal of Information Security, and member of the editorial boards of the journals Computers & Security, IET Information Security, IEEE Wireless Communication, Journal of Computer Security, and IEEE Internet of Things Journal, amongst others. Prof. Lopez is the Spanish representative at IFIP Technical Committee 11 Security and Protection in Information Processing Systems.