Computer Networks 182 (2020) 107523

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

Evaluation of a zone encryption scheme for vehicular networks

Jorge Gallego-Madrid [a], Ramon Sanchez-Iborra [a,*], Jose Santa [b], Antonio Skarmeta [a]

[a] Department of Information and Communication Engineering, University of Murcia, 30100 Murcia, Spain
[b] Department of Electronics, Computer Technology and Projects, Technical University of Cartagena, 30202 Cartagena, Spain

ARTICLE INFO

Keywords:
Zone encryption
Vehicular networks
C-ITS
V2V
Security

ABSTRACT

Vehicular communications are bringing a new wave of applications under the umbrella of the Cooperative Intelligent Transportation Systems (C-ITS). To this end, on-board units are expected to send messages periodically or upon the appearance of a relevant event, to feed an awareness ecosystem that enables safety or traffic efficiency services. This is the case of Cooperative Awareness Messages (CAMs) in Europe, which contain basic vehicle information such as its position or speed, among other parameters. From a network security perspective, CAMs are broadcasted unencrypted over an unprotected radio channel, hence enabling their potential interception and the disclosure of sensitive data. Although public key infrastructures (PKI)-like solutions have been proposed, high computational cost of asymmetric cryptography to cipher application data remains a challenge and a confidentiality alternative is needed. In this work, we present the implementation and evaluation of a symmetric encryption scheme based on disjoint security domains distributed in geographical areas. In the solution, vehicles are able to coordinate and agree on common keys to be used in different security zones. Simulation results show the validity of the zone encryption scheme in diverse vehicular scenarios with different traffic densities. A potential issue in the zone key redistribution consisting in the propagation of wrongly-generated duplicated keys is also detected, which is discussed in detail and a reliable solution based on the support of third-party data-forwarders is proposed and tested. Evaluations reveal good performance of the zone encryption mechanism in terms of robustness and latency, guaranteeing the efficient access to a secured channel while maintaining low computing load.

1. Introduction

Vehicular networks have evolved lastly, fueling the expansion of a rich ecosystem supported by Cooperative Intelligent Transportation Systems (C-ITS) [1]. The principal aim is the development of novel services to improve driving safety and traffic efficiency. To this end, Vehicle to Infrastructure (V2I), Vehicle to Vehicle (V2V) and, in general, Vehicle to Everything (V2X) communications are being studied for enabling information exchange among all the involved elements in vehicular scenarios. In fact, 5G technology has strengthen the idea of V2X [2], with advances in both V2V and V2I connectivity. However, until the wide spread of 5G new radios, the IEEE 802.11p standard[1] is the principal domain-specific communication technology for vehicular applications. Over this transmission layer, the American Administration defines the Wireless Access in Vehicular Environments (WAVE), detailed by the IEEE 1609.x family of standards [3]. In turn, the European Telecommunications Standards Institute (ETSI) has also proposed G5 [4], which is an adaptation of IEEE 802.11p to European regulations. Besides, there are transnational strategies for the deployment of C-ITS solutions that assure the adoption of these technologies in the coming years. A clear example is the C-Roads platform for the deployment of harmonized and interoperable C-ITS services across Europe [5].

A common approach of both the American and European regulations in C-ITS is the usage of a series of periodic messages, namely, Basic Safety Messages (BSMs) in WAVE [3] and Cooperative Awareness Messages (CAMs) in the European architecture [6], which are exchanged among vehicles to inform each other about their position, speed and other state data. Due to the open nature of C-ITS and the cost of asymmetric cryptography, these packets are usually broadcasted unencrypted over an unprotected radio channel. For the European case, for instance, broadcasted messages require authorization, authentication, integrity and privacy, but not confidentiality [7]. These security services are provided through a Public Key Infrastructure (PKI)

* Corresponding author.
E-mail addresses: jorgegm@um.es (J. Gallego-Madrid), ramonsanchez@um.es (R. Sanchez-Iborra), jose.santa@upct.es (J. Santa), skarmeta@um.es (A. Skarmeta).

[1] Recently, the IEEE 802.11p standard has been renamed to IEEE 802.11 networks running outside the context of a basic service set (OCB).

https://doi.org/10.1016/j.comnet.2020.107523
Received 29 June 2020; Received in revised form 12 August 2020; Accepted 28 August 2020
Available online 1 September 2020

architecture based on asymmetric cryptography [8,9]. Thus, vehicles can share sensitive data in clear, without the security level required by critical services. As a consequence, this information can be intercepted, causing information leakage about the status of the ego-vehicle, which is the source of traffic efficiency and critical safety services. Depending on the privacy capabilities included, with these data an attacker may build vehicle profiles by observing which services are used regularly, for instance, and trace vehicles by analyzing messages exchanged during trips.

The proposal in [10] demonstrates the usefulness of providing confidentiality and privacy capabilities to such V2V networks by using security domains distributed in geographical areas. This paper was focused on the cryptographic foundations of the algorithm, but the implications of implementing the proposal in a realistic vehicular scenario were not considered. Therefore, as a complement to this essential contribution, framed within the European project USE-IT,[2] in this work we explore the development, analysis and improvement of this novel zone encryption scheme that enables authenticated and encrypted communication among vehicles in a V2V fashion. It permits to address the problem of authenticity and confidentiality in V2V communications with lightweight message overhead and processing load. The algorithm is based on the use of asymmetric cryptography for exchanging symmetric encryption keys for the different areas in which a certain region is divided. With this strategy, periodic exchanges of safety messages among vehicles is secured, preventing disclosure of sensitive data, traceability of vehicles and manipulation of the messages. The main contributions of this work are the following: (i) a deep characterization of the zone encryption algorithm under actual vehicular settings; (ii) a comprehensive implementation of this security scheme; (iii) an exhaustive performance evaluation considering urban and highway scenarios, for evaluating its feasibility under realistic driving conditions; and (iv) a thorough discussion and a potential solution for the detected problem of redistributing undesired duplicated zone keys.

The remaining of the paper is organized as follows. Section 2 presents the advances beyond the state of the art, by placing the work in the literature. Section 3 dissects the zone encryption algorithm. Section 4 details the implementation and test-bench employed for conducting the evaluation tests. Section 5 presents and discusses the attained results. An issue identified in the encryption algorithm and its solution is discussed and evaluated in Section 6. Finally, Section 7 concludes the paper and introduces future research lines.

2. Related work

Different proposals can be found in the related literature addressing the protection of the wireless segment in V2I architectures. In [11], authors proposed to encrypt the establishment of connections from ambulances to a management center using a PKI, hence, adopting an asymmetric cryptography approach. The solution in [12] also uses asymmetric cryptography in communications between on-board units (OBUs) and road-side units (RSUs), hence creating one-to-one security channels. Authors of [13] presented an equivalent approach but based on symmetric cryptography to protect OBU–RSU links. However, these solutions are not broad enough to consider general C-ITS systems with V2X requirements. In [14] it is presented a fog computing solution for the vehicular domain, aimed at offering contextual route guidance to drivers. Communications are secured using symmetric and asymmetric cryptography, although fog nodes are considered to be set at the infrastructure edge, i.e., RSUs, and the approach mainly considers V2I messaging only. The same drawback is found in the work presented in [15]. However, in this proposal intermediate nodes are employed in the form of proxies to help reducing the computation load of asymmetric cryptography. As a difference to the previous works, the current paper describes a solution in which a first negotiation is carried out to create a session key to be maintained for the next exchanges using symmetric cryptography. This strategy can be considered as a particular case covered by the security solution proposed for vehicular IPv6 communications in [16].

In general, securing V2X communications providing confidentiality is a crucial issue without a straightforward solution up to now. The deployment of symmetric key encryption schemes in C-ITS is not feasible in an immediate way, due to the fact that nearby vehicles should share a common key to be able to communicate. Installing a shared common key inside every vehicle could be considered, but this presents the problem of not being able to revoke the key if it is compromised in a single vehicle. Work in [17] studied the problem of broadcast encryption, in which a central authority distributes the encryption keys to a subset of vehicles to enable the exchange of confidential information among them. This scheme presents notable issues related to key management and necessary bandwidth upon high number of nodes.

Using asymmetric encryption in V2X, as described in [18], implies the use of a PKI to enable secure communication by making vehicles credentials available. Based on previous research works focused on pseudonym certificates, such as [19,20], current C-ITS systems under development in Europe [21] and in the US [3] propose the use of short-lived pseudonyms to authenticate exchanged messages among vehicles. These mechanisms imply the use of a small pool of pseudonyms and OBUs rotate them to gain some degree of privacy. Nevertheless, these approaches try to reach a trade-off between efficiency and privacy level, because they bet on constrained pseudonym schemes aimed to reduce management complexity of the security protocol. Furthermore, despite the fact that messages may be authenticated, data sent are still in plain text due to computing load implications of asymmetric cryptography when applied to application data. Since these messages contain static information such as vehicle dimensions as well as dynamic data regarding heading, speed or position, it is possible to link messages to certain vehicles due to their physical characteristics and driving patterns. Additionally, certificate management is another issue that PKI-based solutions have to deal with. Revocation of certificates in vehicular networks is considered for example in [22]. In this work, revocation lists are updated by using artificial intelligence techniques to detect untrustworthy OBUs.

Work in [23] particularly discusses the problem of computing load when using asymmetric cryptography in constrained OBUs. It indicates that these processes can last seconds for single messages in recent mobile devices, even when using ciphertext-policy attribute-based encryption (CP-ABE) schemes, which employ lightweight procedures. The contribution in [15] also addressed this issue by delegating part of the ciphering load to nearby RSUs. However, this is a strong requirement for generic V2X scenarios. An evolution of this idea is presented in [24], in which nearby RSUs are used for initial authentication and derivation of group keys. In this line, other works have exploited the concept of group-based communications as a mean of developing feasible distributed security solutions in V2X scenarios. The solution in [25] includes improves efficiency and security of V2V one-hop broadcasting schemes, integrating the location-based security approach initially presented in [26]. In this solution, messages are encrypted using a symmetric key obtained on the basis of an RSU area, geographical coordinates, time, and OBU/RSU credentials. Similarly, authors of [27] proposed to group vehicles by speed and path in clusters, establishing a cluster leader in charge of managing public keys. However, the join and key exchange procedures can be a limitation under high dynamic conditions. Work in [28] proposed a system that combines the usage of pseudonyms with group-based encryption in handover areas where the pseudonym is changed. This provides an extra level of security to avoid vehicle tracking, but at the expense of relying on a complex RSU infrastructure.

[2] http://www.chistera.eu/projects/useit.

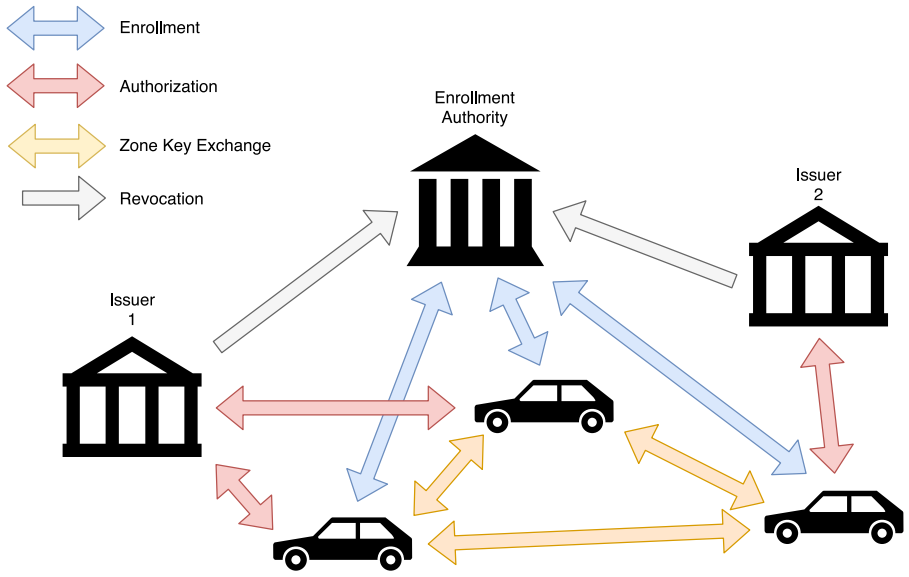


Fig. 1. Zone encryption architecture.

As demonstrated, near works in the literature present flaws and extra complexity for a proper key management and maintenance of communication groups. Besides, they present high computation costs due to asymmetric cryptography and need RSUs to support OBUs in security procedures or computation offloading. For these reasons, the proposal evaluated in this paper presents a distributed solution based on a zone encryption scheme, in which OBUs communicate among them or with RSUs (only if needed) to obtain security material, and symmetric cryptography is used to avoid degrading the performance when providing confidentiality to periodical beating packets.

3. Zone encryption

The zone encryption scheme [10] enables the efficient transmission of authenticated and encrypted CAMs from one vehicle to others that are in its surroundings. Asymmetric cryptography is used by participants to exchange symmetric keys to be used in particular zones (the zone keys). Once the zone keys are distributed, further messages are efficiently secured using symmetric cryptography. As depicted in Fig. 1, the transmitting vehicle has to first anonymously authenticate against the others by using a short-term credential, which is usually obtained from a cryptography issuer. Besides, in order to authenticate and communicate with the issuer, the vehicle is provided with a long-term credential by the Enrollment Authority (EA). Based on these initial steps, the objective of the system is then to preserve confidentiality of V2V communications and privacy of vehicles and drivers.

Given that it is common that vehicles communicate with nearby elements in C-ITS, the zone encryption scheme takes advantage of this spatial locality. It considers a division of the Earth's surface into disjoint zones, in which vehicles inside a particular one have to agree on a shared key to encrypt the transmitted CAMs. Vehicles are also allowed to transmit CAMs to adjacent zones by using previously-retrieved keys, otherwise they cannot do it across the current zone boundaries. Adopting a geographic-based approach brings a series of advantages regarding vehicles security and privacy. Firstly, as all the vehicles within a zone make use of a common encryption key and this key is different in each zone, tracking specific vehicles by an attacker is notably complicated. Besides, the intrinsic distributed nature of the algorithm provides it with higher robustness and independence than centralized solutions, as vehicles coordinate the zone keys generation and exchange themselves. Finally, the encrypted message exchange scheme relies on V2V transmissions; hence, once the vehicles acquire their credentials, the zone encryption mechanism may be implemented in any scenario without a pre-existent fixed vehicular communication infrastructure, e.g., RSUs. The previous aspects support the geographical definition of zones instead of design them according to the coverage of a hypothetical deployed road infrastructure.

Aiming at providing freshness to the different keys and credentials, the scheme states a time division into epochs and periods. The lifetime of the short-term credential is called epoch, which is composed of multiple time periods. These periods determine the validity of the zone keys. Thus, at the beginning of each epoch, a vehicle requests the short-term credential to an issuer by authenticating itself with the long-term credential previously obtained from the EA. With the authentication guaranteed by this short-term credential, a set of vehicles can agree on a key for a zone whose lifetime is the current time period. When an epoch is coming to its end, each vehicle has to request to the issuer for a new credential to operate in the next epoch. In a similar way, whenever a time period is concluding, vehicles have to renew the zone keys of the areas they are currently operating in.

In order to transmit CAMs inside a certain zone, a vehicle must previously obtain the corresponding zone key in a V2V fashion. The required process to complete this operation is depicted in Fig. 2. As can be seen, the zone-key agreement is performed in two steps. Firstly, a car entering a new zone sends a zone key request indicating the zones for which a key is being requested, the time period, and its public key, which is part of its short-term credential. This message can be received by one or more vehicles (A.1) or by none of them (B.1).

In the first situation (A exchange in Fig. 2), when a vehicle enters a zone, it identifies its current and adjacent zones. Then, from this set, it checks the zones for which it does not have the key and broadcasts a key request (A.1). Replies (A.2) are not aggregated, i.e., each node that hears a request can only answer with the key of the zone where it is currently located. As many vehicles may hear this request, an replaying strategy have been developed in order to decide which vehicle is in charge of providing the requested zone key and avoid collisions and channel overload. Those vehicles that can provide the requested key wait during a random back-off time before forwarding it. Meanwhile, they keep sensing the channel for detecting another vehicle's reply. In case of noticing a response from another participant, these vehicles avoid to reply and the requester obtains the zone key from this message.

In turn, if no one is inside the zone when a vehicle requests the zone key (scenario B in Fig. 2), it will not receive any response, so it has to generate a new key for this zone and stores it (B.2). This new key

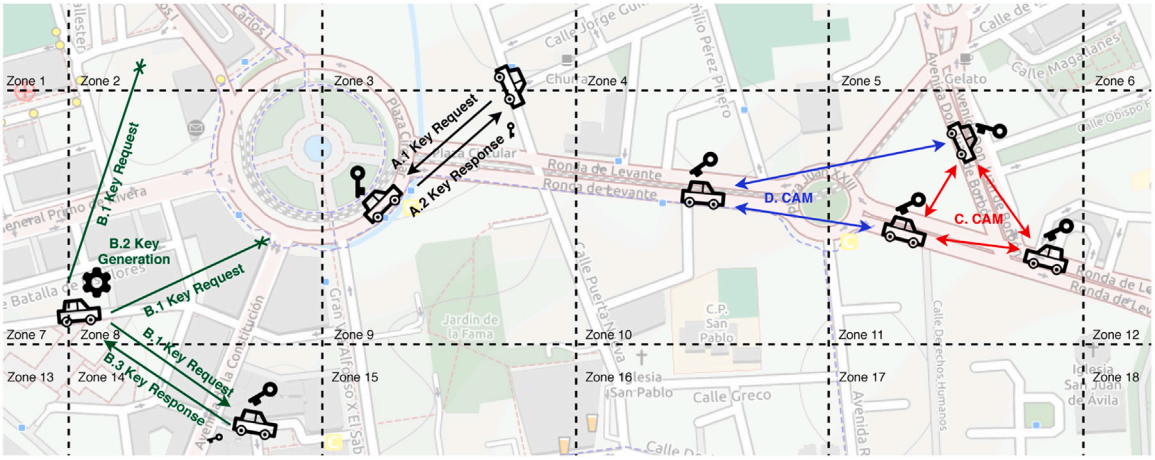


Fig. 2. Zone encryption operation.

n	z_1	t_1	$Kz_1,t_1(Kp)$	...	z_n	t_n	$Kz_n,t_n(Kp)$
$Kp(CAM)$							

Fig. 3. Secured data packet by using zone keys.

will be sent to other cars that subsequently request it. If a requester does not receive the key of an adjacent zone, it is not authorized to generate a new one for that zone. Observe that the vehicle in scenario B has requested the keys for zones 2, 8, and 14. It has received the key from zone 14 (B.3), and it has generated the key for zone 8. As it has not received the key from zone 2, it will ask for it in future requests. To avoid packet collisions when multiple vehicles request a key, it has been developed a key-request strategy based on back-off timers, similar to the response procedure explained above. Upon entering the zone, a vehicle transmits a key request and waits for a reply for a fixed period of time. If no response is obtained, it waits a random back-off time and transmits a second key request. If the node does not receive any answer in this second attempt, it will generate a new zone key.

When a vehicle has to broadcast a CAM, it creates a fresh symmetric key and uses it to encrypt the message data (payload). Then, it ciphers this key with each of the zone keys to which it intends to transmit the message and the results are added to the message in its header, together with the zone and time period of each encryption key. Fig. 3 shows the resulting packet, where n represents the number of zones for which the symmetric key (Kp) has been encrypted. Each ciphertext ($K_{z,t}(Kp)$) includes Kp cyphered by a zone key $K_{z,t}$ and it is preceded by the zone (z) and time period (t) for the employed zone key. Finally, the ciphered CAM ($Kp(CAM)$) is appended as the packet payload. Thereby, when a vehicle receives a CAM, it checks its key store for a match with the zone and time period. If a match is found, the node uses the corresponding zone key to decrypt the symmetric key generated by the sender and, then, deciphers the payload with it. Thus, a node is able to receive messages from the zone in which it is currently located or from the adjacent zones. Scenario C in Fig. 2 shows an intra-zone CAM exchange, while scenario D shows an inter-zone exchange.

4. Implementation and scenario setup

Although a formal complexity and scalability analysis of the zone-encryption scheme can be found in [10], the dynamic nature of C-ITS scenarios suggests that a more realistic evaluation of the security solution should be conducted by using computer simulation. Concretely, we have employed both network and vehicular mobility simulators, which cooperate to recreate realistic vehicular scenarios.

OMNeT++[3] is used as the mentioned network simulator. It is a modular C++ simulation framework that offers a graphical run-time environment, an Eclipse-based IDE, a topology description language, a simulation kernel library, and other helpful utilities. The different components of the network are programmed in C++ and assembled together using a high-level language (NEtwork Description, NED). The Veins[4] library has been integrated within this simulation environment. Veins is an open source framework for designing vehicular network scenarios, which provides a complete suite of network and message models to carry out vehicular network simulations in a realistic way. It implements the de-facto IEEE 802.11 OCB (formerly known as 802.11p) access layer and the rest of the WAVE stack. Hence, Veins defines the 802.11p networking mechanisms and messaging services, e.g., Basic Safety Messages (BSM) and WAVE Service Advertisements (WSA). Given the similarity in their function, BSM messages are used instead of CAM, given that Veins does not includes a CAM implementation.

SUMO[5] has been used to generate realistic vehicular mobility traces. It is an open source traffic simulator that enables the setup of realistic scenarios by simulating the behavior of a set of vehicles defined by the user. It also includes supporting tools such as route finding and visualization. OMNeT++ and SUMO are connected via a TCP socket by using the Traffic Control Interface (TraCI) as communication protocol, which allows bidirectional simulation of road and network traffic.

The implementation of our security proposal has been done using C++, over the WAVE architecture defined in Veins. The basic zone encryption operation module of each node has been integrated within the application level of the stack, while the scheme-specific functionality has been distributed in different developed libraries. To handle the cryptographic procedures included in the zone encryption scheme, the Crypto++ Library[6] has been used. It provides a wide set of cryptographic algorithms as well as a comprehensive documentation about the use of each component. In the initial version of the implementation, RSA has been used as public-key crypto-system, and AES-128 for the symmetric encryption.

To perform the initial evaluation, two scenarios have been considered, using a reference urban setting and a typical highway environment. These scenarios permit to study the performance of the solution

[3] https://omnetpp.org.
[4] https://veins.car2x.org.
[5] https://sumo.dlr.de.
[6] https://cryptopp.com/.

under diverse traffic and mobility conditions. The routes of the vehicles are generated by means of a SUMO script to generate random trips. The minimum distance between the start point and the end of the route has been set to 1000 m. Furthermore, the beginning time of each route is established in the first second of the simulation, making all the vehicles appear at once.

The city model considered to perform the initial evaluation of the scheme is Erlangen, Germany (see Fig. 4(a)). The area involves a square of 2600 m × 2600 m, divided into 169 zones with sides of 200 m (see Fig. 4(b)). This setup allows us the study of a wide variety of situations, such as zones with low density of vehicles or zones suffering from traffic congestion. The city model includes buildings in some parts of the city, which challenges connectivity of vehicles due to signal blockage. The speed limit in the city is 50 km/h (31 mph).

The highway road model has been created from scratch using the SUMO GUI. The highway is 20,2 km long, with three intersections separated by 6 km and two lanes each way. The maximum permissible speed is 120 km/h (74,5 mph). The road is divided longitudinally in areas of 200 m long, which correspond to 101 zones.

In order to study the zone encryption scheme under various traffic conditions, five different traffic-density configurations have been adopted with 100, 250, 500, 750 and 1000 vehicles circulating in both scenarios. The rest of the configuration parameters remain with their default values for comparison purposes. The wireless transmission channel as well as the propagation mechanisms are characterized by the Veins library. As aforementioned, the employed wireless communication technology has been IEEE 802.11 OCB, with a bit-rate of 12 Mbps and a transmission power of 20 mW. Ten runs have been carried out for each configuration to analyze the performance of the zone-encryption algorithm with enough statistical confidence. Hence, the results are averaged and the confidence interval ($\alpha = 0.05$) is provided. As performance metrics, we have considered the following: (i) the number of zone-keys generated when entering a zone without other vehicles, which imply the generation of duplicated keys as explained later; (ii) the number of keys received by all cars within the zone; (iii) the time interval for receiving a key when it has been requested; (iv) the number of sent and received requests; (v) the number of sent and received replies to the requests; and (vi) the CAMs received correctly, incorrectly, and received but not decrypted due to the lack of the proper key.

5. Results

In the following, we present and discuss the results obtained from the conducted simulations in each of the described scenarios. This separation permits to evaluate the performance of the zone encryption algorithm in different situations in terms of vehicle density, driving speed, and transmission obstacles, among others.

5.1. City

Firstly, we focus on the number of key requests sent and delivered to the surrounding vehicles in each of the considered vehicle-density conditions, which are depicted in Fig. 5. The confidence intervals are represented as well, although they are not visible due to their reduced size. Results show the expected behavior, as the overall number of packets increase with the number of vehicles in the scenario. Observe that the delivered requests grow faster because, in denser scenarios, the requests are heard by more vehicles. Both metrics also show that, although the number of vehicles increase up to 1000, the number of requests sent and delivered tend to stabilize as the channel capacity is reached and collisions start to be more frequent.

Table 1 shows the average number of responses sent in total and per request in the scenario. As expected, the total responses increase with the number of the vehicles and the responses per request are higher as the vehicle density is greater. Due to responses per request are registered by correlating the message ID, this parameter represents the average number of key-replies that a node receives when it makes a request (further developed later). In addition, the percentage of requests answered is also shown. In this scenario, between a 60,43% and a 76,05% of the requests sent are received and answered by other vehicles.

Table 1
Average number of responses sent in total and per request in the city scenario.

Number of vehicles	100	250	500	750	1000
Responses sent in total	1960,30	5090,80	7988,90	9640,20	10 761,90
Responses per request	1,56	1,79	2,15	2,34	2,46
% of requests answered	60,43	67,89	73,74	75,06	76,05

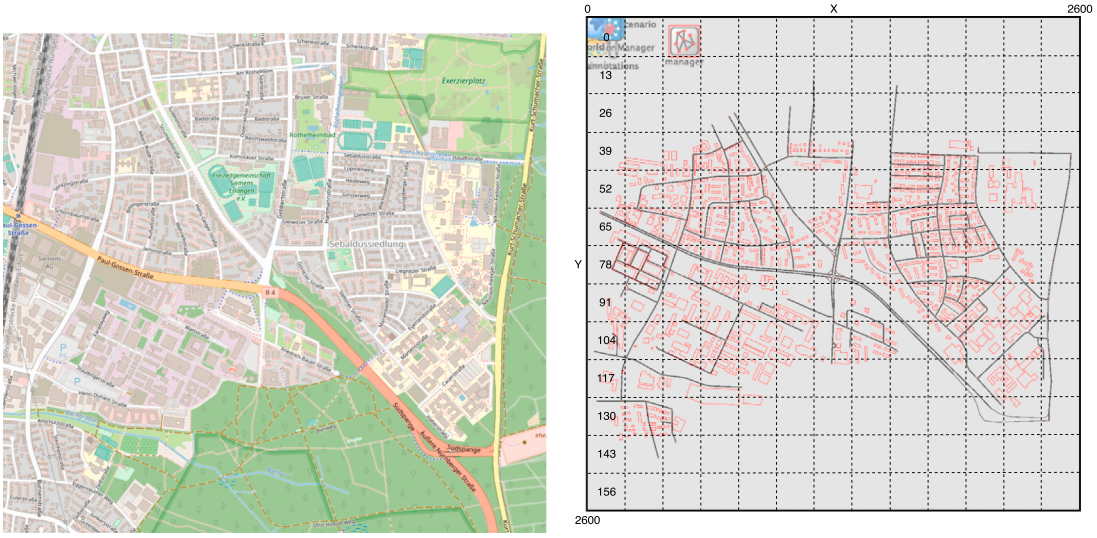
Fig. 6 presents the average number of keys received when they are asked in each zone, together with the average time needed to do so. A clear increment in the number of key received can be seen as the number of vehicles increases, due to when a new car enters a crowded zone and emits a key request it is more likely to find another node able to answer with the zone key. Regarding the average time to receive a key when a vehicle enters a new zone, it stabilizes at around 19 ms, showing that keys are always received within the two reply time windows. However, a slight increment is observed as the number of vehicles increase, due to the saturation of the communication channel. However, a good performance is perceived thanks to the back-off time approximation described above.

The average number of keys generated for each zone is shown in Fig. 7. The key generation is self-triggered when a vehicle requests a zone key and does not receive any reply. The attained results indicates the generation of duplicated keys in the zones, since the average number of keys generated for each zone is greater than one. This is not supposed to happen, as the conducted simulations took place during the same time period, without the need of a renewal process neither for the zone keys nor for the short-term credential. There are two situations detected to cause the generation of duplicated keys: (i) packet losses, due to the presence of obstacles that block the key requests or responses, or packet collisions in overcrowded scenarios; and (ii) vehicles that enter an empty zone, generate a new key and then leave the zone and its adjacent ones propagating this wrongly-generated key. This problem may lead to the situation of two vehicles in the same zone using different encryption keys and being unable to communicate with each other. Besides, if this problem is not detected and corrected, the invalid key may be further propagated to other vehicles. A solution to this issue is presented in Section 6.

Fig. 8 depicts the average number of CAMs correctly received correctly, incorrectly, and without the needed key. Observe that the number of CAMs received incorrectly grows exponentially with the number of vehicles. This is related to the duplication issue discussed above, which aggravates at high vehicle densities. As a consequence, the number of CAMs delivered and decrypted with a wrong key in high density scenarios surpasses the number of CAMs correctly received. Regarding the CAMs received without the required keys, this number is considered negligible considering high network traffic. This issue is provoked by CAMs generated by vehicles in remote zones for which the receiving vehicle does not have the appropriate key. Hence, the key distribution scheme implemented works properly, although its performance can be improved dealing with the key duplication problem.

5.2. Highway

Fig. 9 shows the requests sent and delivered in each simulation configuration. The confidence intervals are also represented, although they are not visible due to their reduced size. As in the previous scenario, results indicate an increment due to higher vehicle density, although the growth is less pronounced than in the urban setup. Sent



(a) Erlangen map view.

(b) SUMO modelling of the map with the defined encryption zones.

Fig. 4. Experiment maps.

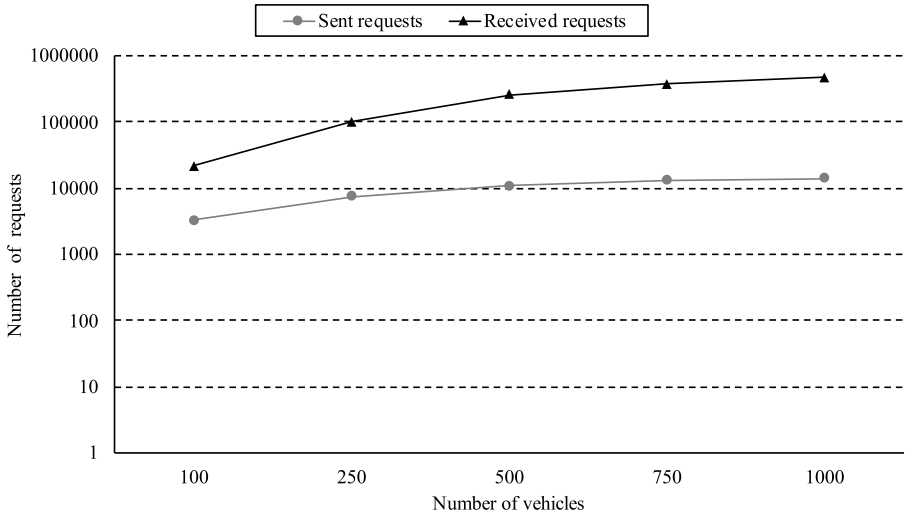


Fig. 5. Average number of requests sent and received in the city scenario (Y axis in logarithmic scale for improving readability).

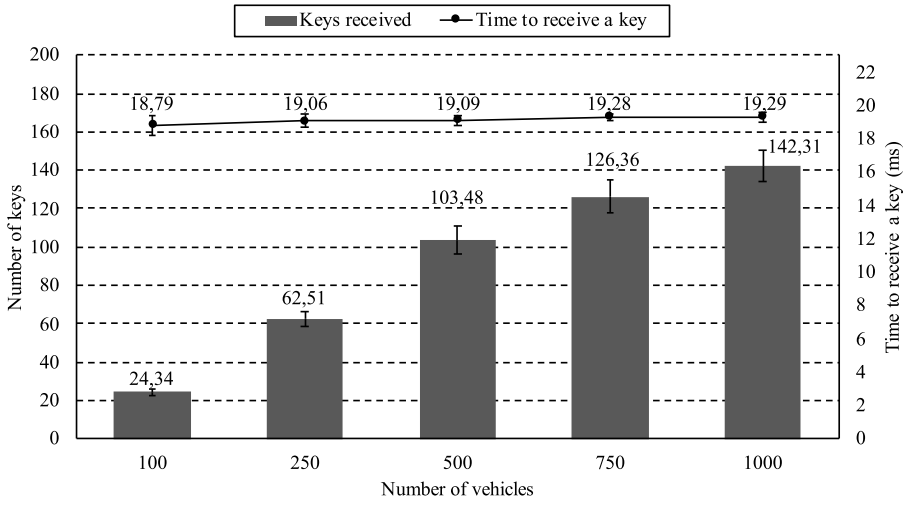


Fig. 6. Average number of requested keys received in each zone and average time to receive them in the city scenario.

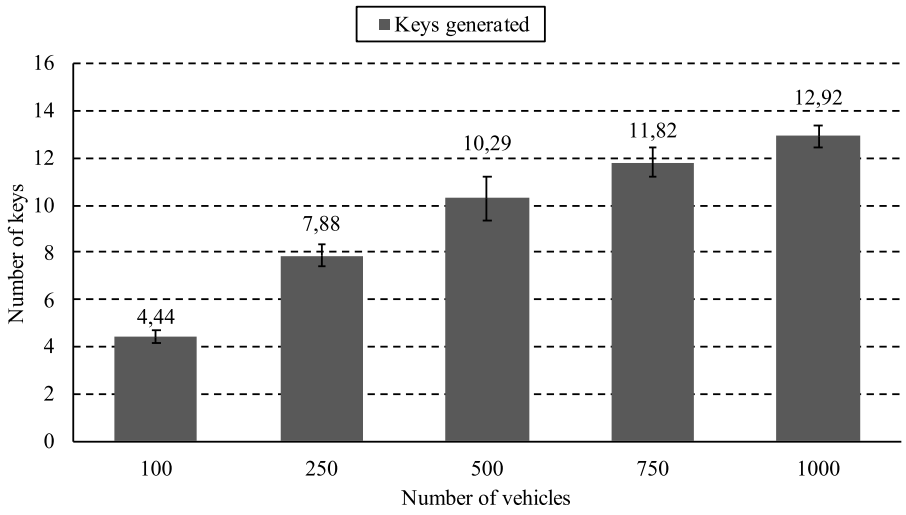


Fig. 7. Average number of keys generated for each zone in the city scenario.

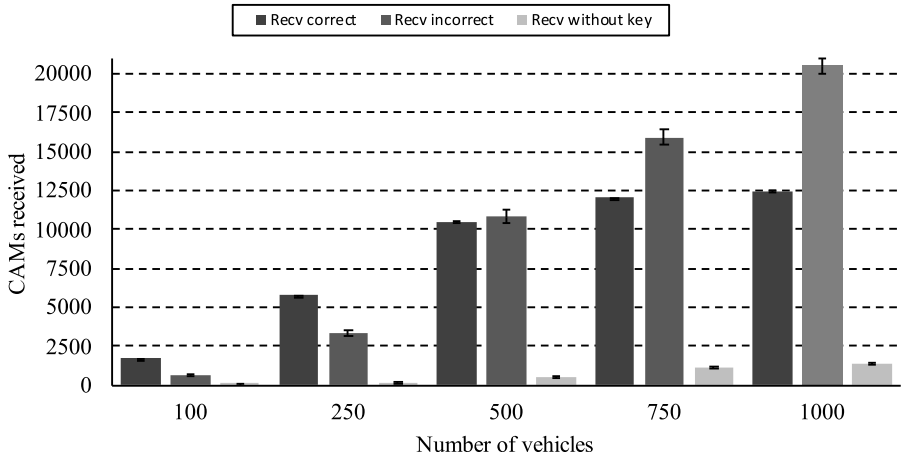


Fig. 8. Average number of CAMs received in the city scenario.

Table 2
Average number of responses sent in total and per request in the highway scenario.

Number of vehicles	100	250	500	750	1000
Responses sent in total	4398,60	11 359,30	22 696,80	28 433,90	32 099,80
Responses per request	1,16	1,29	1,44	1,50	1,53
% of requests answered	55,92	61,62	63,20	63,68	63,76

requests are higher than in the Erlangen one, which is caused by the higher mobility and speed of vehicles in the highway. Delivered requests are lower here, due to traffic jams taking place in the city, which increases the number of close vehicles.

Table 2 shows the average number of responses sent in total and per request. As in the city case, the responses grow with the traffic density; however, here the figures are greater because of the higher number of requests sent in the highway setup. In turn, the responses per requests are lower, because each vehicle asks for the keys of three zones simultaneously instead of nine, like in the city. The percentage of requests answered is also lower and remains stable among different traffic density configurations, except for the one with less vehicles. Given the sparse distribution of vehicles in this scenario, increasing the number of vehicles does not imply the same impact than in the city use case.

In Fig. 10, the average number of keys received due to requests in each zone and the average time to receive them are presented. The number of keys received increases with the traffic density in the highway, and values are greater than those obtained in city simulations, due to the increment of sent responses. As in the city case, the evolution of key reception delay with the traffic density presents a slight increment, due to the gradual saturation of the communication channel when more vehicles are in the scenario, but the time stabilizes below 20 ms.

The average number of keys generated for each zone is depicted in Fig. 11. In this case, the values are less than a half of the ones obtained in the city simulations. The average grows in the first three configurations and then decreases gradually. As explained above, there are two main reasons that provoke the generation of duplicated keys: key request losses due to the presence of obstacles that may block communications or packet collisions in overcrowded scenarios, and vehicles entering an empty zone that generate a new key and then leave the zone and its adjacent ones wrongly propagating it. In this scenario, there are no obstacles, so the first reason is discarded. Therefore, the number of generated keys increases with low densities due to the fact that vehicles in the scenario are dispersed along the road and it is very likely to find situations falling in the second case. However, with high densities, there are fewer empty spaces, so the keys are better distributed.

In Fig. 12, the average number of CAMs received correctly, incorrectly, and without the corresponding key are shown. Observe that the number of CAMs within the last two groups in this scenario is significantly lower than in Erlangen, due to vehicles are more distributed along the road. Furthermore, most of the CAMs are correctly decrypted.

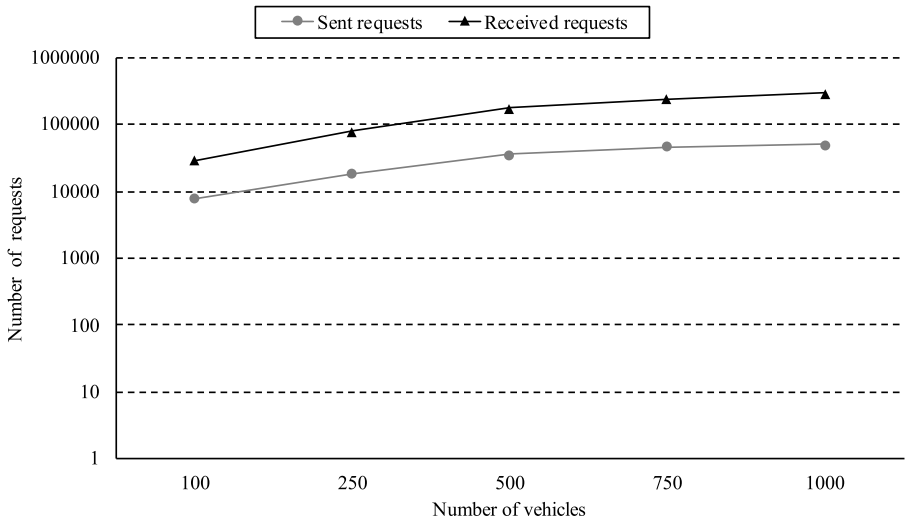


Fig. 9. Average number of requests sent and delivered in the highway scenario (Y axis in logarithmic scale for improving readability).

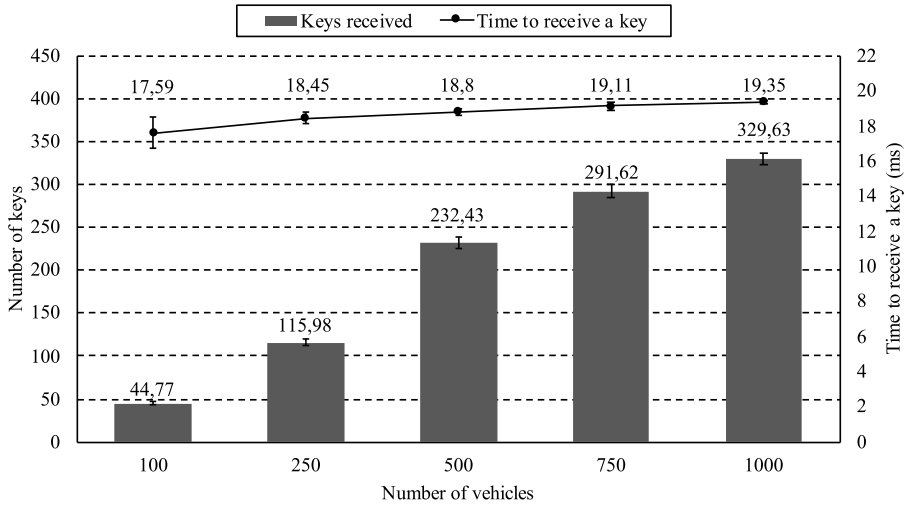


Fig. 10. Average number of keys received in each zone and average time to receive the key in the highway scenario.

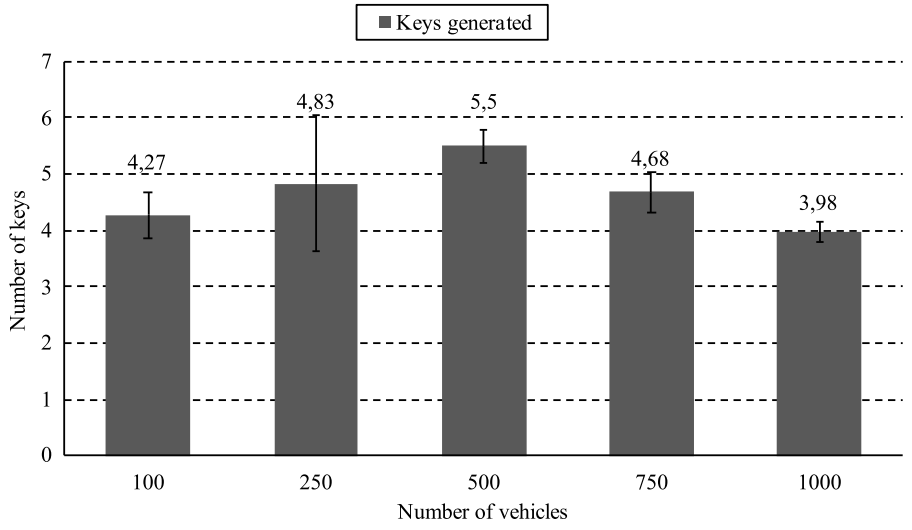


Fig. 11. Average number of keys generated for each zone in the highway scenario.

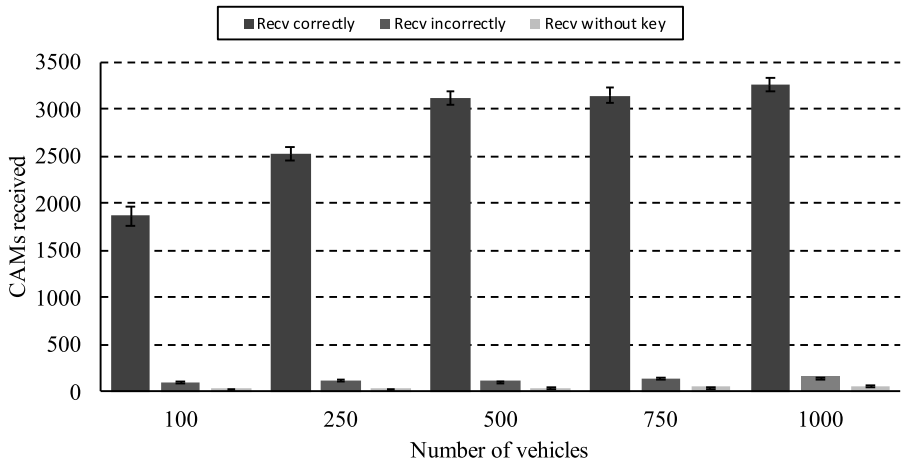


Fig. 12. Average number of CAMs received in the highway scenario.

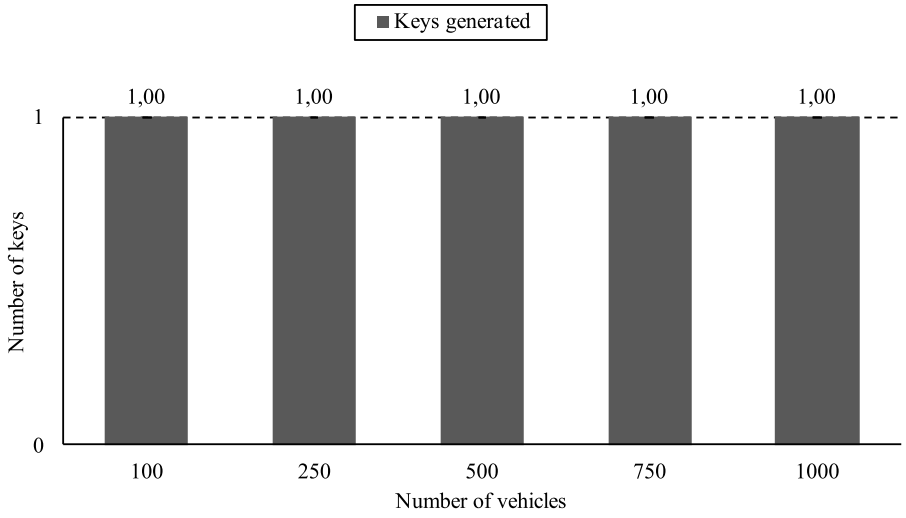


Fig. 13. Average number of keys generated for each zone in the city scenario with the infrastructure solution.

6. Enhanced infrastructure-supported solution

As discussed above, the distributed nature of the zone encryption scheme leads to the key-duplication issue confirmed in the experiments. This undesired situation claims for the presence of a third-party entity with a global view of the scenario to solve the problem. In this line, a solution employing a fixed infrastructure, e.g., cellular network such as 4G/5G [2], has been employed to support the correction of key duplication events. This assumes that vehicles are connected to a central server via this infrastructure, with no packet losses (or a packet-loss recovery mechanism). This entity detects duplicated keys and forwards messages exchanged among vehicles to better propagate correct zone keys. Note that the infrastructure does not take part in solving the duplication issue, since it only acts as a packet forwarder when a duplication is detected. Hence, the zone encryption algorithm maintains its distributed nature.

6.1. Proposed improvement

When a vehicle enters a zone and generates a key (correctly or incorrectly), it has to send a message to the infrastructure containing the zone, the time period, a freshly generated public key, a SHA-256 hash of the generated zone key, a timestamp, and an authentication token. The infrastructure has a database with the messages that contain the hashes of the current active key in each zone, which corresponds to the first received key from the first vehicle entering the zone. When the central server receives this message, it compares the time period and the hash of the received key with the stored ones. If it is the first key received for that zone, the infrastructure keeps the hash, the time period and the timestamp as a reference and it answers the sender vehicle with an acknowledgment allowing the vehicle to use and spread this zone key. On the contrary, if a duplication is detected during a certain time period, i.e., the key has been generated despite the fact that another one already existed, the infrastructure forwards the same received message to the rest of the vehicles in the scenario, searching for a vehicle having the correct key for this specific zone. When a vehicle having the key for the requested zone receives this request, it answers with a new message containing the zone, the time period, an authentication token, and the correct zone key encrypted under the public key of the conflicting node, which was embedded in the forwarded message. The newly created message reaches the conflicting node through the cellular infrastructure, which is in charge of forwarding it. Finally, the conflicting node decrypts the correct zone key with its private key, solving the problem. Furthermore, if the central server receives a zone key not corresponding to the stored one, but generated within a new time period, this means that the infrastructure must renew the stored information corresponding to the current time period.

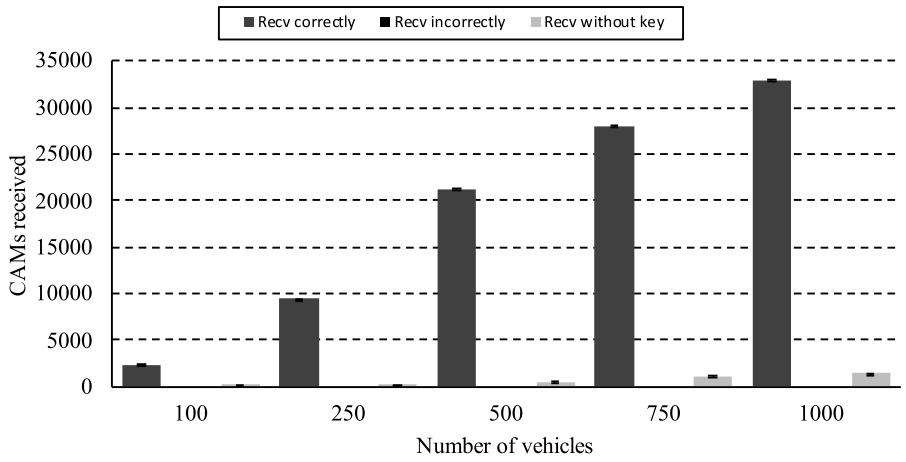


Fig. 14. Average number of CAMs received in the city scenario with the infrastructure solution.

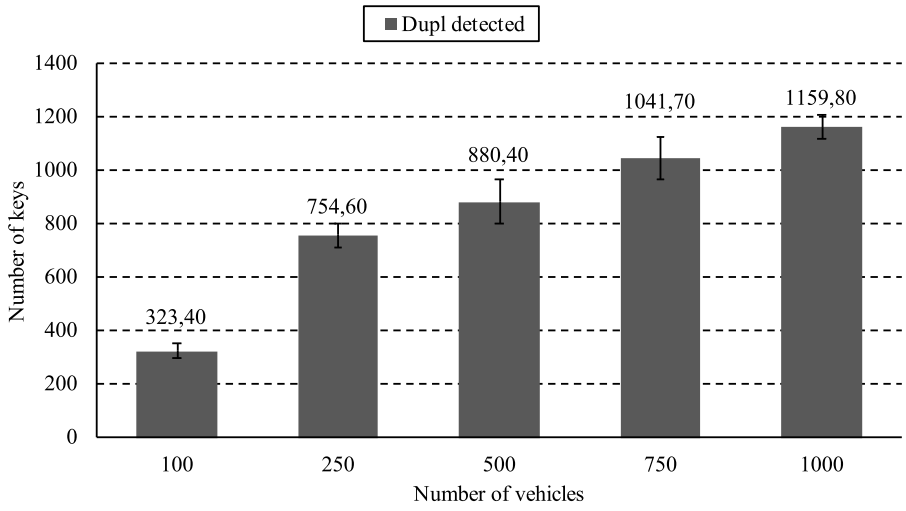


Fig. 15. Number of key duplications detected by the infrastructure in the city scenario with the infrastructure solution.

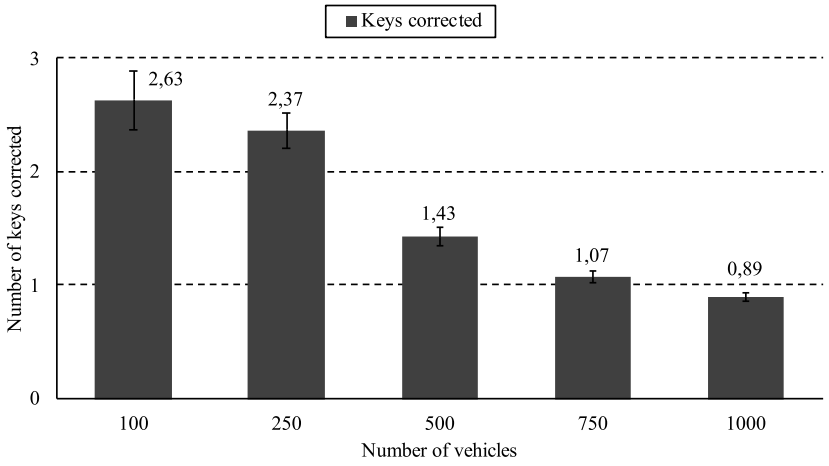


Fig. 16. Average number of keys corrected per vehicle in the city scenario with the infrastructure solution.

6.2. Evaluation

In order to validate and test the performance of this infrastructure-based solution, another set of simulations has been carried out in the most challenging scenario, i.e., the urban one. The same configuration parameters are used, with the difference of including the cellular infrastructure as a support network for solving the key-duplication conflicts.

Fig. 13 shows that the average number of keys generated for each zone is one. This implies that only one key is used in each zone of the scenario during the lifetime of the simulation, which is understood as the proof that the proposed mechanism solves the duplication issue.

The average number of CAMs received correctly, incorrectly, and without the corresponding key is shown in Fig. 14. Unlike the values obtained in the original city simulation (see Fig. 8), where CAMs received incorrectly grew exponentially, in this new scenario they have disappeared, due to the absence of duplicated keys. As a consequence, the number of CAM received correctly significantly increases, while the ones received without the corresponding key remain at similar levels.

The average number of total key duplications detected by the infrastructure is shown in Fig. 15. The value notably increases with the vehicle number, reaching more than one thousand duplications in high-density configurations. The reason behind this increment is the rise of collisions when a vehicle enters a zone and request the key, leading to generate wrong new keys.

Fig. 16 depicts the average number of keys corrected per vehicle during the whole simulation. This corrections are triggered when a key-correction request is received from the infrastructure. The value decreases with the node density, since the key corrections are distributed among a greater number of vehicles in the scenario.

7. Conclusions

In C-ITS, sensitive data can be shared without a proper level of security due computational and management costs implied by PKI-based solutions. Hence, vehicles broadcast periodic messages such as CAMs in clear using a unprotected radio channel. Consequently, a malicious user may obtain information about vehicles or drivers leading to different attacks. V2X scenarios make them difficult to come up with a confidentiality solution that meets the distributed requirements of this kind of networks. In this work, we have implemented and evaluated a novel proposal that divides geographical areas into disjoint security zones in order to provide privacy and confidentiality using efficient symmetric cryptography. The zone-encryption scheme proposes an initial authentication using short-term certificates and, after that, OBUs are able to use self-created symmetric keys to cipher messages in their current area. This is a distributed security mechanism that uses efficient encryption for V2X messages. The solution has been developed and analyzed in terms of operation and performance under realistic settings, as a complement to the original presentation of the algorithm, focused on the cryptographic foundations.

The implementation has been evaluated in a network simulator (OMNeT++) using urban and highway scenarios, generating realistic mobility traces and using an IEEE 802.11 OCB channel model. The results show that the proposal correctly generates zone-keys and their exchange among vehicles circulating in the area. The number of messages sent and received increase with the number of nodes, but tend to stabilize with high figures, maintaining collisions thanks to a back-off timer-based approach. The average time to receive a zone key is low, below 20 ms for all the considered cases, which is understood as a reasonable delay for being able to provide confidentiality to messaging services. Moreover, the analysis has empirically demonstrated an operation and performance issue in the solution, due to its distributed nature, based on the duplication of zone keys within particular zones for the same time period. A solution based on a third-party infrastructure that is employed as a reliable packet-forwarder, has been proposed and evaluated, demonstrating its validity to solve the issue.

Future research lines consider the development of the authentication part of the scheme as well as the evaluation of the solution considering dynamic zones depending on the type of scenario and the current number of vehicles.

CRediT authorship contribution statement

Jorge Gallego-Madrid: Software, Validation, Investigation, Data curation, Writing - original draft, Writing - review & editing, Visualization. **Ramon Sanchez-Iborra:** Conceptualization, Methodology, Formal analysis, Resources, Writing - original draft, Writing - review & editing, Supervision, Project administration. **Jose Santa:** Conceptualization, Methodology, Validation, Investigation, Writing - original draft, Writing - review & editing, Supervision. **Antonio Skarmeta:** Conceptualization, Methodology, Writing - review & editing, Supervision, Project administration, Funding acquisition.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

This work has been supported by the Spanish Ministry of Science, Innovation and Universities, under the Ramon y Cajal Program (Grant No. RYC-2017-23823) and the projects PERSEIDES, Spain (Grant No. TIN2017-86885-R with ERDF funds) and Go2Edge, Spain (RED2018-102585-T); and by the European Commission, under the projects 5G-MOBIX (Grant No. 825496) and INSPIRE-5Gplus (Grant No. 871808).

References

[1] R.I. Meneguette, R.E. De Grande, A.A.F. Loureiro, Intelligent Transport System in Smart Cities: Aspects and Challenges of Vehicular Networks and Cloud, first ed., in: Urban Computing, Springer International Publishing, Cham, 2018, http://dx.doi.org/10.1007/978-3-319-93332-0, URL http://link.springer.com/10.1007/978-3-319-93332-0.

[2] S.A.A. Shah, E. Ahmed, M. Imran, S. Zeadally, 5G for vehicular communications, IEEE Commun. Mag. 56 (1) (2018) 111–117, http://dx.doi.org/10.1109/MCOM.2018.1700467, URL http://ieeexplore.ieee.org/document/8255748/.

[3] National Highway Traffic Safety Administration. U.S. Department of Transportation, Notice of proposed rulemarking for federal motor vehicle safety standards; V2V communications, Fed. Regist. 82 (8) (2017).

[4] ETSI, ETSI ES 202 663 - Intelligent Transport Systems (ITS); European Profile Standard for the Physical and Medium Access Control Layer of Intelligent Transport Systems Operating in the 5 GHz Frequency Band, Tech. rep., ETSI, 2010.

[5] C-ROADS, Harmonised C-ITS Specifications for Europe, Release 1.4, Tech. rep., C-ROADS, 2019.

[6] ETSI, Intelligent Transportation Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service, Technical Report ETSI EN 302 637-2 v1.3.1, Tech. rep., ETSI, 2014.

[7] ETSI, ETSI TS 102 731 - Intelligent Transport Systems (ITS); Security; Security Services and Architecture, Tech. rep., ETSI, 2010.

[8] European Commission, Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS), Tech. rep., European Commission, 2018.

[9] European Commission, Security Policy & Governance Framework for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS), Tech. rep., European Commission, 2017.

[10] J. Camenisch, M. Drijvers, A. Lehmann, G. Neven, P. Towa, Zone encryption with anonymous authentication for V2V communication, in: 5th IEEE European Symposium on Security and Privacy, 2020, pp. 1–7.

[11] C.-L. Chen, I.-C. Chang, C.-H. Chang, Y.-F. Wang, A secure ambulance communication protocol for VANET, Wirel. Pers. Commun. 73 (3) (2013) 1187–1213, http://dx.doi.org/10.1007/s11277-013-1273-y.

[12] A. Malik, B. Pandey, Asymmetric encryption based secure and efficient data gathering technique in VANET, in: 2017 7th International Conference on Cloud Computing, Data Science Engineering - Confluence, 2017, pp. 369–372, http://dx.doi.org/10.1109/CONFLUENCE.2017.7943177.

[13] A. Abdellaoui, O. Azzam, H. Chaoui, H. elachgar, N. Hmina, XxTEA-VCLOUD: A security scheme for the vehicular cloud network using a lightweight encryption algorithm, in: Proceedings of the 2018 International Conference on Cloud Computing and Internet of Things, in: CCIOT 2018, ACM, New York, NY, USA, 2018, pp. 67–72, http://dx.doi.org/10.1145/3291064.3291076, URL http://doi.acm.org/10.1145/3291064.3291076.

[14] L. Wang, G. Liu, L. Sun, A secure and privacy-preserving navigation scheme using spatial crowdsourcing in fog-based VANETs, Sensors 17 (4) (2017) http://dx.doi.org/10.3390/s17040668, URL https://www.mdpi.com/1424-8220/17/4/668.

[15] S. Kanchan, N.S. Chaudhari, SRCPR: Signrecrypting proxy re-signature in secure VANET groups, IEEE Access 6 (2018) 59282–59295, http://dx.doi.org/10.1109/ACCESS.2018.2870477.

[16] P.J. Fernandez, J. Santa, F. Bernal, A.F. Skarmeta, Securing vehicular IPv6 communications, IEEE Trans. Dependable Secure Comput. 13 (1) (2016) 46–58, http://dx.doi.org/10.1109/TDSC.2015.2399300.

[17] C. Freitag, J. Katz, N. Klein, Symmetric-key broadcast encryption: The multi-sender case, Lecture Notes in Comput. Sci. (2017) 200–214, http://dx.doi.org/10.1007/978-3-319-60080-2_16.

[18] T. Limbasiya, D. Das, Secure message transmission algorithm for vehicle to vehicle (v2v) communication, in: 2016 IEEE Region 10 Conference (TENCON), 2016, pp. 2507–2512, http://dx.doi.org/10.1109/TENCON.2016.7848485.

[19] C. Wang, D. Shi, X. Xu, Pseudonym-based cryptography and its application in vehicular ad hoc networks, in: 2014 Ninth International Conference on Broadband and Wireless Computing, Communication and Applications, 2014, pp. 253–260, http://dx.doi.org/10.1109/BWCCA.2014.72.

[20] C. Wang, D. Shi, X. Xu, J. Fang, An anonymous data access scheme for VANET using pseudonym-based cryptography, J. Ambient Intell. Humaniz. Comput. 7 (1) (2016) 63–71, http://dx.doi.org/10.1007/s12652-015-0301-z.

[21] ETSI, Intelligent Transport Systems (ITS); Trust and Privacy Management, European standard, ETSI, 2018.

[22] N. Kumar, R. Iqbal, S. Misra, J.J. Rodrigues, An intelligent approach for building a secure decentralized public key infrastructure in VANET, J. Comput. System Sci. 81 (6) (2015) 1042–1058, http://dx.doi.org/10.1016/j.jcss.2014.12.016, Special Issue on Optimisation, Security, Privacy and Trust in E-business Systems. URL http://www.sciencedirect.com/science/article/pii/S0022000014001809.

[23] X. Liu, Y. Xia, W. Chen, Y. Xiang, M.M. Hassan, A. Alelaiwi, SEMD: Secure and efficient message dissemination with policy enforcement in VANET, J. Comput. System Sci. 82 (8) (2016) 1316–1328, http://dx.doi.org/10.1016/j.jcss.2016.05.006, URL http://www.sciencedirect.com/science/article/pii/S0022000016300320.

[24] L. Liu, Y. Wang, J. Zhang, Q. Yang, A secure and efficient group key agreement scheme for VANET, Sensors 19 (3) (2019) http://dx.doi.org/10.3390/s19030482, URL https://www.mdpi.com/1424-8220/19/3/482.

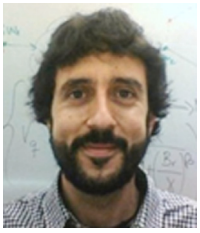
[25] R. Hussain, Z. Rezaeifar, Y.-H. Lee, H. Oh, Secure and privacy-aware traffic information as a service in VANET-based clouds, Pervasive Mob. Comput. 24 (2015) 194–209, http://dx.doi.org/10.1016/j.pmcj.2015.07.007, Special Issue on Secure Ubiquitous Computing. URL http://www.sciencedirect.com/science/article/pii/S1574119215001455.

[26] R. Hussain, F. Abbas, J. Son, H. Oh, TIaaS: Secure cloud-assisted traffic information dissemination in vehicular ad hoc networks, in: 2013 13th IEEE/ACM International Symposium on Cluster, Cloud, and Grid Computing, 2013, pp. 178–179, http://dx.doi.org/10.1109/CCGrid.2013.38.

[27] H. Toulni, M. Boudhane, B. Nsiri, M. Miyara, An adaptive key exchange procedure for VANET, Int. J. Adv. Comput. Sci. Appl. 7 (4) (2016) http://dx.doi.org/10.14569/ijacsa.2016.070441.

[28] X. Deng, X. Xin, T. Gao, A location privacy protection scheme based on random encryption period for VSNs, J. Ambient Intell. Humaniz. Comput. (2019) http://dx.doi.org/10.1007/s12652-019-01227-z.

Jorge Gallego-Madrid received the B.Sc. degree in Computer Engineering and the M.Sc. on New Technologies in Computer Science from University of Murcia in 2018 and 2019, respectively. Currently, he is a predoctoral researcher at Department of Information and Communication Engineering at the same university. His research interests include Internet of Things, intelligent transportation systems, 5G and network slicing techniques.



Ramon Sanchez-Iborra is an Assistant Professor and Researcher at the Information and Communications Engineering Department in the University of Murcia, Spain. From the Technical University of Cartagena (Spain), he received the B.Sc. degree in telecommunication engineering in 2007 and the M.Sc. and Ph.D. degrees in information and communication technologies in 2013 and 2015, respectively. He has been an invited professor at the Faculty of Computer Science of the AMIKOM Yogyakarta University, Indonesia (2019) and at the Engineering Faculty of the University of Quindío, Colombia (2017). He has been a post-doctoral visiting researcher at the ARTS research-group of the Mediterranean University of Reggio Calabria, Italy (2018), the Quality and Usability Lab of the Technical University of Berlin, Germany (2018), and the Fraunhofer FOKUS Institute, Berlin Germany (2019. His main research interests are QoE in multimedia services, management of wireless mobile networks, 5G slicing, and IoT/M2M architectures. He has published more than 50 papers in national and international conferences and journals. He has collaborated as a TPC member and reviewer for international journals and conferences such as *IEEE ICC*, *EAI ADHOCNETS* or *IEEE Communications Magazine*.

Jose Santa received the M.S. degree (5 years) in computer engineering from the University of Murcia, Spain, in 2004, the M.S. degree in advanced information and telematics technologies and the Ph.D. degree in computer engineering with European Mention at the University of Murcia, in 2008 and 2009, respectively. A great part of his research work, both before and after his Ph.D., is about intelligent transportation systems, mobile communications, next-generation networks, cyber–physical systems, and Internet of Things (IoT), with special emphasis on real prototypes and evaluation. He is currently a Senior Research Fellow (Ramon y Cajal) with the Department of Electronics, Computer Technology and Projects, Technical University of Cartagena. He has been part of international and national projects, such as the EU GIROADS, ITSSv6, FOTsis, 5G-MOBIX, 5GINFIRE, and the Spanish OASIS, TIMI, m:Via and S-CICLO, among others. He has been granted by the BBVA Foundation with a Leonardo Project.

Antonio Skarmeta received the B.S. degree (Hons.) from the University of Murcia, Spain, the M.S. degree from the University of Granada, and the Ph.D. degree from the University of Murcia, all in computer science. He has been a Full Professor with the University of Murcia, since 2009. He has been part of many EU FP projects and even coordinated some of them. He has published more than 200 international articles. His main interests include the integration of security services, identity, the IoT, 5G, and smart cities.