Array 11 (2021) 100084

Contents lists available at ScienceDirect

Array

journal homepage: www.sciencedirect.com/journal/array

5G-based V2V broadcast communications: A security perspective

Mujahid Muhammad [a], Ghazanfar Ali Safdar [b,*]

[a] Birmingham City University, Birmingham, B4 7XG, United Kingdom
[b] University of Bedfordshire, Luton, LU1 3JU, United Kingdom

ARTICLE INFO

Keywords:
Authentication
Message integrity
V2X services
5G security
V2V communications

ABSTRACT

The V2V services have been specified by the 3GPP standards body to support road safety and non-safety applications in the 5G cellular networks. It is expected to use the direct link (known as the PC5 interface), as well as the new radio interface in 5G, to provide a connectivity platform among vehicles. Particularly, vehicles will use the PC5 interface to broadcast safety messages to inform each other about potential hazards on the road. In order to function safely, robust security mechanisms are needed to ensure the authenticity of received messages and trustworthiness of message senders. These mechanisms must neither add significantly to message latency nor affect the performance of safety applications. The existing 5G-V2V standard allow protection of V2V messages to be handled by higher layer security solutions defined by other standards in the ITS domain. However having a security solution at the 5G access layer is conceivably preferable in order to ensure system compatibility and reduce deployment cost. Accordingly, the main aim of this paper is to review options for 3GPP access layer security in future 5G-V2V releases. Initially, a summary of 5G-V2V communications and corresponding service requirements is presented. An overview of the application level security standards is also given, followed by a review of the impending options to secure V2V broadcast messages at the 5G access layer. Finally, paper presents the relevant open issues and challenges on providing 3GPP access layer security solution for direct V2V communication.

1. Introduction

Intelligent transportation system (ITS) is a label applied to a range of applications providing advanced services from plat-forms integrating network-connected (usually, road) vehicles and infrastructure. In this context, the communications between vehicles and between vehicles and other ITS nodes are usually categorized in terms of four modes; vehicle-to-vehicle (V2V), vehicle-to-network (V2N), vehicle-to-infrastructure (V2I) and vehicle-to-pedestrian (V2P). Here, 'infrastructure' refers to road-side infrastructure and V2I supports communications between vehicles and a variety of services and functions of the ITS platforms and applications built upon it. Collectively, the modes are known as Vehicle-to-Everything (V2X). V2X communications can be used to improve road safety, enhance traffic efficiency and support advanced in-vehicle user infotainment services. Information received by a vehicle about other nearby vehicles, road conditions, traffic signals, etc., can be merged with the data from the vehicle's on-board sensors to improve the driver's situation awareness and automated/assisted decision making. In this context, V2X can be seen as a means of extending the range, volume and variety of sensor data avail-able to the driver. The organization of connectivity between ITS nodes (vehicles, road-side infrastructure and pedestrian) is based on the well-known OSI (Open System Interconnection) layered reference model, which is extended to form the ITS reference architecture [1], as illustrated in Fig. 1. The architecture consists of four horizontal layers (communication stack) and two vertical functions spanning all layers. The application and facilities layer generate and format different kinds of safety and non-safety messages, and then hand them over to the net-work and transport layers for transportation from the source of a message to its destination. The access layer determines the radio-level communication technology to be used for over-the- air transmission. There are two main technical approaches to this:

- Dedicated Short-Range Communication (DSRC) in the US, and ITS-G5 in the European Cooperative Intelligent Transport Systems (C-ITS) initiative utilize a variant of WiFi technology based on the IEEE 802.11p standard running in the 5.9 GHz frequency band;

* Corresponding author.
E-mail address: ghazanfar.safdar@beds.ac.uk (G.A. Safdar).

https://doi.org/10.1016/j.array.2021.100084
Received 19 April 2021; Received in revised form 6 July 2021; Accepted 6 August 2021
Available online 17 August 2021
2590-0056/© 2021 The Authors. Published by Elsevier Inc. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

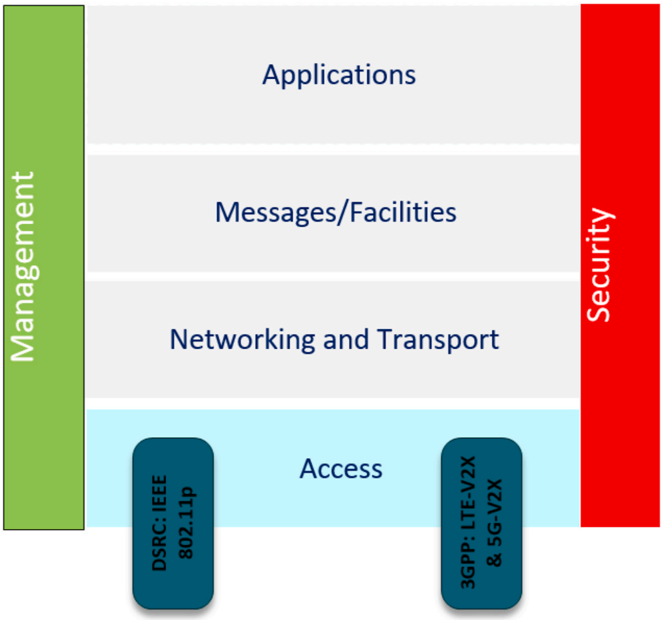

Fig. 1. V2X communication stack.

- Cellular-V2X (C–V2X), which is defined by the 3GPP as part of its LTE and ongoing 5G families of standards. C– V2X includes two modes: longer-range, higher latency. communication via the cellular network known as C–V2N, and low latency, direct communication referred to as C– V2V/I/P.

Referring to Fig. 1, the vertical functions, i.e. security and management services are provided on a layer-by-layer basis to man-age the ITS (safety and non-safety) application requirements and secure the communication between the communicating nodes. Notably, this paper mainly focuses on the security aspect of C– V2V using 5G new radio (5G-NR) as the underlying radio technology.

The 3GPP has, in Release 14 [2] and above, studied the requirements that derive from the wide range of V2X services.

and then approved the support of V2X communication in the current LTE and upcoming 5G-NR technologies. Specifically, the 5G-NR will utilize the existing uplink and downlink to pro-vide V2N communication via the cellular network, and also provides for a direct device-to-device (D2D) link over an interface known as PC5 to enable direct V2V, V2I and V2P communications [3,4], as illustrated in Fig. 2. The 5G system's sup-port for ultra-high data rate, low latency, comprehensive quality of service and extended coverage, provides natural benefits to vehicular communication. As such, 5G-NR along with proper enhancements can be considered as a unified and scalable solution for all V2X communications, which can be managed and controlled by means of widely deployed cellular network infrastructure.

The direct PC5-based communication has lower latency than the uplink/downlink communication via cellular network infrastructure and was originally proposed to support device-to- device proximity services [5]. It is envisioned for the majority of V2V applications, particularly safety use-cases, which have challenging latency requirements. In contrast, the Uu-based communication is expected to support safety applications that require long-range communication, non-safety V2N services like traffic efficiency, and user infotainment applications. These applications have no strict requirements on delay (up to 500 ms) and reliability, although quality degrades with increasing packet loss and longer communication range [6,7].

For short-range direct V2V communication, broadcast *trans*-mission is adopted as primary mode of communication between sending and receiving vehicles. This is because safety information from a given sending vehicle is expected to be known by all vehicles within the vicinity of the sender, in order for them to be aware of the current road condition and take necessary action. For instance, a vehicle reports information about bad traffic conditions to its neighbors, so that they can take necessary action. Also, majority of the safety applications require to process mobility information (e.g. position, speed, direction) of vehicles within the vicinity of the target vehicle. Hence, the PC5 interface is utilised to support the direct exchange of broadcast messages between vehicles that are in close proximity to each other. Each vehicle (henceforth referred to as V-UE) broadcasts messages in a periodic or event-triggered manner, to support various V2V safety applications. The V2V safety applications have the most stringent performance requirements for the communication layer, with some use-cases requiring ultra-reliable communication links and a maximum end-to-end latency of 100 ms or less [8,9].

V2V broadcast messages need to be protected against security threats, which include message forgery, replay, etc. Particularly the spread of malicious information in vehicular network environments could have disastrous consequences, including loss of life and property. Thus, the fundamental security requirements in V2V broadcast systems are firstly to authenticate the source of a received broadcast message, secondly to verify that the message has not been tampered with while it was in transit, and thirdly, to guarantee that the source of a broadcast message can be held accountable for its actions in the event of an investigation. Although these are quite standard requirements for message security in wireless networks, for which well-known solutions exist,

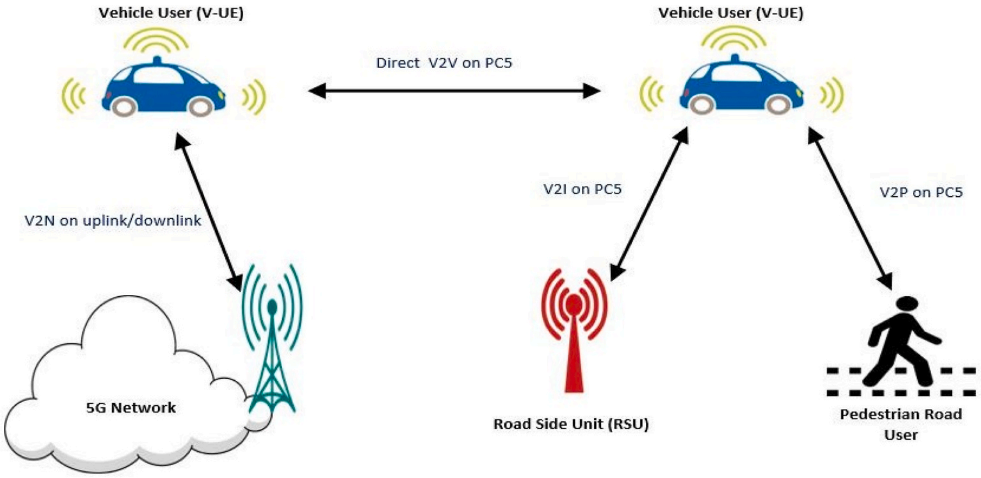

Fig. 2. 5G-V2X communication modes.

the V2V/P/I use cases have particular characteristics that constrain solutions: (1) high mobility of vehicles with short connection time (2) vehicles need to verify and process received broadcast messages rapidly (3) heterogeneous environment with varying density of vehicles and (4) one-way transmission mode with no prior security association. Presently, there are two approaches for application layer security in ITS, namely: the IEEE 1609.2 standard [10] and the European Telecommunication Standard Institute (ETSI) standard [11]. Both solutions rely on the same principles of asymmetric cryptosystems and vehicular public key infrastructure (VPKI). In both approaches, each vehicle owns a private key, and the corresponding public key is made widely available. Together they are used to secure V2V communication by digitally signing and verifying every safety message. The link be-tween the key pair and the identity of its owner is provided by a certificate signed by a certificate authority (CA). However, the benefits of this approach are accompanied by some challenging problems. Research studies have confirmed through simulations [12–14], as well as practical tests on real equipment [15] and modelling [16] that the signature verification overhead of VPKI-based schemes leads to excessive latency or packet loss when road traffic is dense. This therefore raises concern about the performance and scalability of these security solutions particularly in high traffic density regions, where vehicles need to verify large number of received messages within a very short period of time [17]. Currently, there are limited research findings on the experimental deployment and performance evaluation of these security solutions under realistic traffic conditions for safety-critical applications. Moreover, a VPKI-based solution requires the deployment of trusted services for certificate management, which increases system complexity. Despite the shortcomings of these standard solutions, these solutions are applied at the application layer level of the ITS reference architecture. Although 3GPP currently allow V2V security to be handled at the upper layers of the ITS communication stack, while focusing on improving the radio access layer for V2V communication, having a security solution at the 3GPP access layer may be preferable in order to ensure system compatibility and reduce deployment cost.

This paper focuses on the analysis of ways to provide fast and efficient security solutions at the 3GPP radio access layer of 5G-NR systems. In contrast to previous works, such as [18–21] and [22], this article specifically addresses security issues within the context of 5G-based V2V services. The works of [23] investigates the security aspects of 3GPP networks for V2X communications, but focuses on privacy issues of vehicle owners, as well as analyses the security concern when virtualization and software defined networking are used for V2V. Table 1 provides list of abbreviations employed in this paper.

The rest of the paper is organized as follows: Section 2 presents a range of V2V safety applications and their corresponding requirements targeted at the communications network. In Section 3, a background on security aspects as well as security requirements of V2V broadcast communication is presented. The application layer security standards for V2V communication are described in Section 4. Section 5 focuses towards the main aim of this review paper and presents access layer security solutions that employed different cryptographic methods to secure 5G-V2V communication, followed by a comparative and critical analysis of the applied security methods. Further challenges and open research issues are described in Section 6. Finally, Section 7 draws a concluding remarks.

2. V2V applications and use-cases

The 3GPP has identified a number of basic safety and non-safety V2V use-cases relevant to ITS. The communication requirements for these use-cases are shown in Table 2. Also in Release 15 [24], emerging 5G-NR (New Radio) access technology is introduced to support advanced V2X applications that will provide semi-automated and fully automated driving functionalities in addition to the basic safety services. For this, the 3GPP has proposed new enhanced V2V (eV2V) applications and the organization have started work on enhancement of 3GPP support for these new 5G eV2V services in Release 16 [25]. The 5G eV2V applications and use-cases require extremely high data rates, very rigorous reliability, extended communication range and extremely low latency transmissions as included in Table 2.

Table 1
List of abbreviations.

Abbreviation	Extended form
3GPP	3rd Generation Partnership Project
5G-NR	5G New Radio
AA	Authorisation authority
AC	Authentication Centre
CA	Certification Authority
CAMs	Cooperative Awareness Messages
C-ITS	Cooperative ITS
CRL	Certificate Revocation List
C–V2X	Cellular V2X
D2D	Device-to-Device
DENMs	Decentralized Environmental Notification Messages
DoS	Denial of Service
DSRC	Dedicated Short Range Communication
EA	Enrolment Authority
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
ETSI	European Telecommunication Standard In-stitute
eV2V	Enhanced V2V
DoS	Denial of Service
FastAuth	Fast Authentication
HMAC	Hash Message Authentication Code
ITS	Intelligent Transportation Systems
OSI	Open System Interconnection
MAC	Message Authentication Code
MHT	Merkle Hash Tree
RCA	Root Certification Authority
RSU	Road Side Unit Fast Authentication
SelAuth	Selective Authentication
TA	Trusted Authority
TESLA	Time Efficient Stream loss-tolerant Au-thentication
TEAM	Trust Extended Authentication Mechanism
URLLC	Ultra Reliable Low Latency Communications
V-UE	Vehicle User
VCX	V2X Control Function
V2V	Vehicle-to-Vehicle
V2N	Vehicle-to-Network
V2I	Vehicle-to-Infrastructure
V2P	Vehicle-to-Pedestrian
VANETs	Vehicular Ad Hoc Networks
VPKI	Vehicular Public Key Infrastructure

Despite the wide variety of V2V applications and use-cases, there are only two message types defined to convey the applica-tion's information; cooperative awareness messages (CAMs) [26] and decentralized environmental notification messages (DENM) [27]. CAMs are periodic messages exchanged between vehicles to inform each other about the current mobility information for safety purposes. Typical information contained in a CAM mes-sage includes time stamp, vehicle's position, speed, location, heading and other trajectory features provided by measuring in-struments (e.g. speed sensor, GPS, etc.). In contrast, DENMs are safety messages generated upon detecting an event or road hazard and transmitted to warn road users in advance about. this event in a defined geographic area. The data contained in DENM messages are event management information, generation time, validity period, etc., and of course information about the event itself. The most important difference between CAM and DENM is that DENMs are broadcast to vehicles within the event area, and can be extended further by re-broadcasting the message in a multi-hop transmission, while, a CAM is broadcast to all vehicles within the broadcast range, in a single-hop transmission.

As incorrect messages can have safety consequences, security is imperative for V2V services. The main V2V security features are source authentication, message integrity and non-repudiation [28–30].

- Message Modification: A malicious V-UE could alter the messages being broadcast, especially when it is acting as a relay. For instance in multi-hop transmission, a malicious V-UE acting as a relay node may receive messages from one party, change their content, and rebroadcast them to other V-UEs.
- Denial of Service (DoS) attack: The main objective of this attack is to prevent legitimate users from using the network services by tying up finite resources. An example of a DoS attack in the context of V2V, is the situation whereby a V-UE receives a large number of fake or genuine signed messages and is unable to verify them all in time to react. Similarly, the receiver's input message buffer could overflow causing messages to be dropped. Such so-called computation-based DoS can easily occur among vehicles in high traffic density regions even with-out any malicious intention.
- Repudiation: A malicious V-UE may deny that it sent (or did not send) a given message, or may claim falsely that another V-UE sent (or did not send) a given message in order to mislead an investigation. For example, a malicious V-UE sends an emergency vehicle warnings, so it can bypass other V-UEs, but, deny the action later.

Table 2
5G V2X applications, use-cases and corresponding communication requirements. Source [31].

Use-case	V2X Service Type	Message Type	Communication Requirements
Forward Collision Warning	V2V	CAM	• Message payload 50-300 Bytes • Maximum latency 100 ms • Transmission rate 10 messages/s
Control Loss Warning	V2V	DENM	• Message payload 50-300 Bytes • Maximum latency 100 ms • Transmission rate 10 messages/s
Emergency Vehicle Warning	V2V	CAM	• Message payload 400 Bytes • Maximum latency 100 ms • Transmission rate 10 messages/s
Pre-crash Sensing Warning	V2V	DENM	• Message payload 50-300 Bytes • Maximum latency 20 ms • Transmission rate 50 messages/s
Queue Warning	V2V/V2I	DENM	• Message payload 400 Bytes • Maximum latency 100 ms • Transmission rate 10 messages/s
Curve Speed Warning	V2I	Unclear	• Message payload 50-400 Bytes • Maximum latency 1s • Transmission rate 1 message/s
Warning to Pedestrian	V2P	CAM	• Message payload 50-300 Bytes • Maximum latency 100 ms • Transmission rate 10 messages/s
Vehicles Platooning	V2V/V2I	CAM	• Message payload 50-6500 Bytes • Communication range up to 350 m • Maximum latency 25 ms • Transmission rate 40 messages/s
Advanced Driving	V2V/V2I	CAM	• Message payload 300-6500 Bytes • Communication range up to 700 m • Maximum latency 100 ms • Transmission rate 10 messages/s
Extended Sensors	V2V	CAM	• Message payload 1600 Bytes • Communication range up to 1 km • Maximum latency 100 ms • Transmission rate 10 messages/s
Remote Driving	V2V/V2I	CAM	• Maximum latency 5 ms • Transmission rate 200 messages/s
Autonomous Driving	V2V/V2I	CAM	• As low as 1 ms delay • Transmission rate 1000 messages/s

Depending on the event type, confi-dentiality may also be required for DENM messages and there-fore the message will additionally need to be encrypted over the air interface. However, the security mechanisms must not pre-vent CAM and DENM safety messages being exchanged and processed by legitimate V-UEs within the performance require-ments of the underlying safety applications. The next sections discusses in detail the security aspect of V2V communication.

3. Broadcast security for V2V communications

The broadcast nature of the radio medium means that wire-less communications are prone to several forms of attack. In the case of V2V, information from the outside world or un-known vehicles sent over potentially insecure channels directly influences the behaviour of one's vehicle. Consequently, security is considered as an essential part for the wide acceptability of V2V communications. The unique characteristics, constraints and configurations of V2V communication mean that the deployment of a robust security solution is practically hard. This section presents potential security threats that can disrupt a V2V system, and the main security requirements needed to protect V2V communications.

3.1. Threat model

Direct V2V communication belongs to the family of wire-less ad hoc networks. Forms of attack that exist in standard wireless networks (e.g. identity impersonation, DoS, and re-play) also affect V2V communication. In addition, V2V communication possess additional vulnerabilities due to its unique characteristics, sensitivity of the messages being exchanged and the nature of V2V applications. Below is a brief description of major classes of threats related to V2V:

- Bogus Messages: Here a V-UE broadcasts false messages to affect the behaviour of other V-UEs. For instance, a malicious V-UE could report false information about bad traffic conditions to its neighbors, forcing them to take alternate path, while the malicious V-UE frees the path for itself. Also, a malicious V-UE may broadcast harmful messages in order to mislead receiving vehicles regarding the current road condition and cause them to take a wrong decision or action.
- Identity Impersonation: Typically, in V2V scenarios, the receiver does not care about the actual identity of sender, but to filter-out bogus messages, will want to know that the sender is trustworthy/ authorised to send such messages. To counter this, a malicious V-UE may assume the identity of one or more legitimate V-UE in order to broad-cast erroneous messages. Similar messages received apparently from multiple senders could make the information contained in the messages more credible. A malicious V-UE may also want to insert a misleading message into a stream emitted by a legitimate V-UE in order to make receivers think e.g. that the apparent sender had changed speed or direction.
- Replay Messages: It may be difficult for a malicious V- UE to construct a convincing message appearing to come from a legitimate sender. In a replay attack, a malicious V-UE records a message that was transmitted by a legitimate V-UE and later re-broadcasts it one

or more times. Although the message content was genuine at the original time of transmission, it could be misleading if received at a later time or multiple times.

3.2. V2V security requirements

In the absence of a solid security scheme, the potential threats described above can compromise V2V communication. Due to the cooperative nature of V2V safety applications, these attacks could cause serious harm to road users and may possibly lead to loss of lives and property. In order to protect V2V safety applications, the 3GPP working group on security [32] has identified V2V security requirements that need to be fulfilled, as follows:

- Authorization: V-UEs shall be authorized to participate in V2V communication
- Source Authentication: V-UEs should be able to authenticate and verify that the sender of the received broadcast messages has a valid identity
- Message Integrity: The integrity of the received broad-cast messages shall be checked to ensure that the content has not been modified by any party while in transit
- Replay Protection: Freshness of V2V broadcast messages shall be ensured so that receiving vehicles accepts only freshly generated messages, thus preventing replay at-tacks
- Non-repudiation: Ensures that once a V-UE broadcasts a message, it cannot deny that action later in the event that some incorrect behaviour is detected. This property allows a receiving vehicle to prove to a third party who is accountable for generating the broadcast message.

Although 3GPP has specified the above security requirements to protect V2V applications across the PC5 interface, there is no normative solution mandated. Rather, it is left as an application issue, to be handled by higher layer security solutions defined by other standards in the ITS domain. This is because the 3GPP focus is currently more on enhancing the functionality of the radio access layer e.g. radio resource al-location and management among vehicles [33,34], improving 5G physical layer structure [35,36], channel synchronization issues [37], among other things. The next section describes application layer-based security solution and its shortcomings when applied in the context of cellular V2V communication.

4. Application layer security standards for V2V communication

The IEEE 1609.2 and ETSI TS 102–940 are the standards defined by IEEE and ETSI respectively describing security services for V2V communication at the application layer of the ITS reference architecture. These solutions have similar working principles and protect messages using the same security procedures, with minor difference in terms of the number of functional entities and structure. They are both based on the concept of public key cryptography and the use of VPKI to provision and manage security credentials of the vehicles. In a public key cryptosystem, each party has a pair of keys, one that must be kept secret, and the other that is made public. If an agent uses its private key to sign a message, a receiver can use the sender's public key to verify the signature. If the sender's private key has not been disclosed, the receiver can be sure that the message was sent by the owner of the key pair and has not been modified in transit. Often, a third party known as Certificate Authority (CA) will issue a credential known as a certificate, which associates a public key with an identity. The CA signs the certificate with its own private key so that its integrity can be verified by anyone in possession of the CA's own certificate. If the CA is trusted directly, or can derive its authority from a directly-trusted higher CA via a chain of certificates, then a receiver in possession of the sender's certificate, will additionally know the identity of the sender. Similarly, the sender can encrypt a message using its intended recipient's public key and be sure that only the intended recipient can decrypt and read it. Aside from issuing certificates, the CA is also responsible for certificate renewal when the validity of a node's certificate expires, and certificate revocation when a node is compromised or exhibits malicious behaviour. In such situations, the CA in-validates the certificate, adding it to a certificate revocation list (CRL) that is made available to all participating nodes. All receivers check the CRL for each received message prior to verification. Messages that are signed using revoked certificates are discarded.

For illustration, Fig. 3 depicts the high level architecture of the ETSI security standard. A root certificate authority (RCA), has the highest level of trust in the PKI hierarchy, and delivers a certificate each to the enrolment authority (EA) and the authorization authority (AA) to authorize them to issue certificates to V-UEs. The EA issues a long-term certificate to a V-UE during registration, which is considered as a proof of identity, and used to identify and authenticate the vehicle within the PKI. In contrast, the AA issues short-term certificates to V-UEs, which are used to protect the V2V communication. Every broadcast packet contains the signed message together with the sender's short term certificate. Then the receiving vehicle first verifies the sender's certificate and then the signature of the received broadcast message. In this way, a receiving vehicle can ensure the trustworthiness of the sender and the integrity of the received message without a prior security relationship with the sending vehicle. The Elliptic Curve Digital Signature Algorithm (ECDSA) is used in both security solutions because it is fast and efficient compared to other digital signature algorithms such as RSA. A typical packet broadcast by $(V - UE)_S$ to n receivers, $(V - UE)_R n$, has the following format:

$$(\mathrm{V} - \mathrm{UE})_{\mathrm{S}} \rightarrow (\mathrm{V} - \mathrm{UE})_{\mathrm{R}}\mathrm{n} = \{\mathrm{M}, \sigma_{\mathrm{S}\ \mathrm{K}_{S}}\ [\mathrm{M}|\mathrm{T}], \mathrm{Cert}_{\mathrm{s}}\}$$

where M is the message, $\sigma_{S\ Ks}$ $[M\ T]$ indicates digital signature of $(V\ UE)_S$ using its private key over the concatenation of message M and a timestamp T for freshness checking to pre-vent a replay attack. In addition, each packet contains the sending vehicle's digital certificate denoted by $Cert_s$, which contain information as shown below:

$$\mathrm{Cert}_{\mathrm{s}} = \mathrm{PuK}_{\mathrm{s}}|\mathrm{ID}_{\mathrm{S}}\ |\sigma_{\mathrm{S}\ \mathrm{K}CA}\ |\mathrm{ID}_{\mathrm{CA}}|\mathrm{VP}_{\mathrm{time}}$$

where PuK_S is the sending vehicle's public key bound to its identity ID_S, $\sigma_{S\ KCA}$ and ID_{CA} are the authorisation authority's signature and unique identifier respectively, and VP_{time} is the validity time of the certificate. Since each packet includes a digital certificate, any vehicle receiving the packet could con-firm its authenticity by checking that the sender's certificate is signed by a trusted authority, and then verifying the sender's digital signature on the received broadcast packet.

This security approach defined at the application layer satisfies all the fundamental V2V security requirements-source authentication, integrity of data and non-repudiation, and can thus be applied to protect V2V communications. However, the performance of these solutions comes with some practical concerns. Firstly, in the IEEE 1609.2 standard, a CRL is periodically distributed to all connected vehicles in order to check and remove malicious/misbehaving vehicles from the network. This process requires connectivity to disseminate the list and generates high signalling traffic across the network. Moreover, the CRL checking process itself increases the verification time of received broadcast messages. An alternative approach adopted in ETSI TS standard involves issuing of short term certificates in bulk to a given vehicle. However, renewal of short-term certificates on-demand also requires always-on and reliable connection. In addition, the certificate reloading process incurs de-lay of up to 500 ms as investigated in Ref. [38]. Such delay could affect the performance of the underlying V2V safety application.

Secondly, digital signature generation and verification is required for each broadcast message, with verification being performed independently by each recipient. These operations, verification in particular,

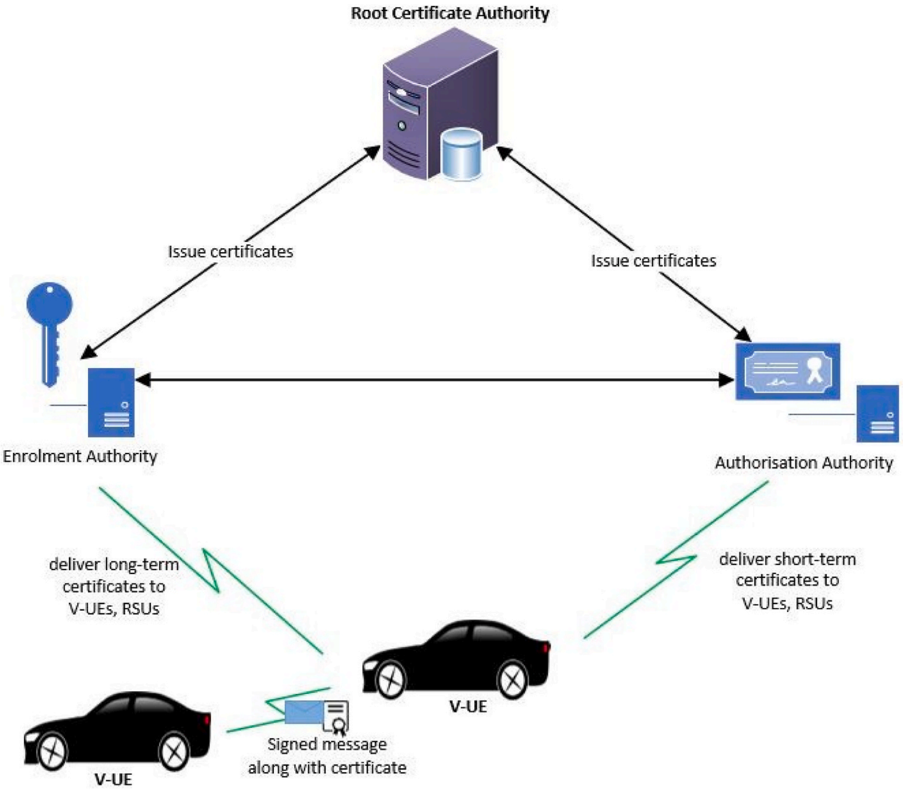
Root Certificate Authority
Issue certificates
Issue certificates
Enrolment Authority
Authorisation Authority
deliver long-term certificates to V-UEs, RSUs
deliver short-term certificates to V-UEs, RSUs
V-UE
V-UE
Signed message along with certificate

Fig. 3. ETSI security architecture.

incur high computational overhead, which introduces delay that may breach the latency constraint of some V2V safety applications. According to the results obtained from the implementation of IEEE 1609.2 standard in the works of [39,40], one ECDSA signature generation and verification process can take up to 4 ms and 20 ms per operation, respectively. Consequently, hardware support is required for these cryptographic operations. Furthermore, the size of each signed message is 67 bytes accompanied by certificate of 125 bytes [41]. This means that a message length will be increased by the security overhead associated with signature and certificate sizes. When there are hundreds of vehicles broadcasting safety messages within a communication range, a large number of messages needs to be verified within a very short time inter-val by each receiving vehicle, and this becomes a bottleneck. To demonstrate a typical constraint of VPKI-based solutions in a densely populated environment, consider a scenario where 200 vehicles are broadcasting safety messages between each other. With a beaconing rates of 1–10Hz, each vehicle needs to generate between 1 and 10 signatures per second and needs to verify between 400 and 4000 signatures per second. In such a scenario, many safety messages will get lost or verified out of order, since the time required to verify the signature on the received messages will introduce high delay that may exceed the maximum delay for most V2V safety applications. Hence, the expensive nature of digital signature verification operations could make vehicles vulnerable to computation-based DoS at-tacks without any malicious intent.

Finally, the VPKI-based solution requires a large scale infrastructure for provisioning and revocation of certificates for vehicles and other ITS entities. Such infrastructure is expensive and time-consuming to build, and subject to political and administrative delays. It is not yet clear whether governmental transportation authorities or vehicle manufacturers should be responsible for its establishment and operation. It is evident that PKC-based solutions at the application layer, while satisfying all the required security properties, incur a significant overhead that may impact the critical latency of V2V messages, especially in a dense urban environment. Consequently, there is need to explore other cryptographic methods to build security schemes at the 3GPP access layer.

The following section thoroughly looks into the access layer security solutions which employed different cryptographic methods to secure V2V communication.

5. 3GPP access layer security for V2V broadcast communication

Having reviewed the standard approach to V2V broadcast message security, namely using public key cryptography at the application layer, this section examines candidate approaches to providing robust security features at the 3GPP access layer.

5.1. *Symmetric cryptography-based solution*

3GPP network security is primarily based on symmetric key cryptography, and considerable support for it is already built into the current architecture and standards [42]. Consequently, it makes sense first to consider whether it can also be applied to address the security requirements of direct V2V messages broadcast over the PC5 interface.

Symmetric key cryptography makes used of the same key, known as secret key, for ciphering and deciphering. Compared to public key (asymmetric) cryptography, symmetric cryptography is faster and employs simpler algorithms as basic building blocks (e.g. Message Authentication Code (MAC), hash function) that have linear computational complexity, and so can ensure authenticity of the message source and integrity of the received message with low computational and communication overhead. However, there are also disadvantages. Whereas in asymmetric cryptography, a total of N key pairs is needed to enable secure communication within a community of N nodes, in symmetric cryptography, N*(N-1)/2 secret keys would be required. Furthermore, each pair of nodes needs to agree a key to use without disclosing it others as illustrated in Fig. 4. Thus, key management and

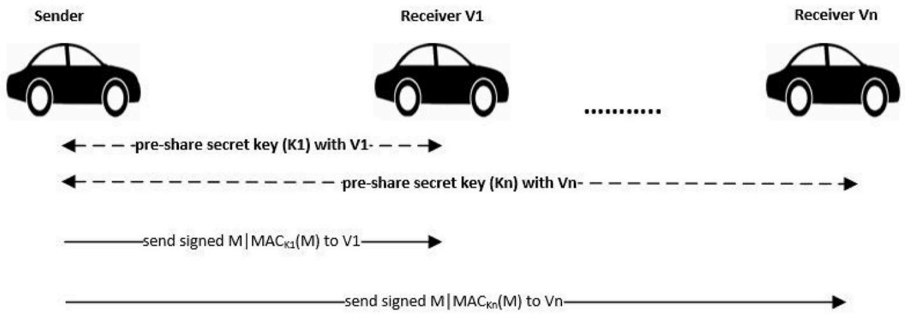
Sender
Receiver V1
Receiver Vn
....
-pre-share secret key (K1) with V1-
pre-share secret key (Kn) with Vn-
send signed M|MAC$_{K1}$(M) to V1
send signed M|MAC$_{Kn}$(M) to Vn

Fig. 4. V2V Secure Message Transmission using Symmetric cryptography-based solution.

distribution is a significant headache.

Using distinct keys for each node pair also makes broad-cast communication impossible. A single symmetric key can be used to support communication within a trusted group of nodes, but the larger the group, the more likely it is for the key to be leaked accidently or for one of the nodes to be unworthy of trust; in either case, all communication within the group is compromised. Non-repudiation also becomes problematic; responsibility for sending a message can only be narrowed down to the membership of the group sharing the key used to create the MAC. Consequently, symmetric-based schemes are often used together with asymmetric ones to overcome above short-comings. A common approach is to use the relatively expensive asymmetric cryptography to establish a secure channel be-tween two mutually-authenticating nodes. A shared secret key is then agreed via this channel, and used with a symmetric scheme to protect the bulk of the communication. In vehicular networks, several research works investigate the use of symmetric cryptographic methods to provide V2V security. For instance, a novel authentication framework for LTE-V2V and V2I communications was proposed in Ref. [43]. It combines sym-metric and public cryptography for mutual authentication be-tween buses and bus stations. Performance evaluation shows.

that their scheme has a reduced authentication time compared to pure asymmetric schemes. In Ref. [44], the authors proposed a broadcast message authentication scheme based on MACs with symmetric encryption. Although this approach attempts to minimize the computational overhead of asymmetric operations, other problems are introduced, such as the need for efficient mechanisms for secret key distribution between the connected vehicles. Also [45], proposed a symmetric-based authentication scheme for vehicular networks. This scheme uses a MAC algorithm with a hash chain element as keys to generate MAC tags. The scheme achieves lower message verification delay when compared to public key based schemes, but does not support the non-repudiation property. Furthermore [46], designed an RSU-aided message authentication scheme. The authors used MAC algorithm and a secret key that is shared between a sending vehicle and the RSU. Whenever a sending vehicle broad-casts a safety message, RSU verifies it first and then notifies all vehicles within its transmission range of the results. In another approach [47], proposed two broadcast authentication schemes based on elliptic curve encryption to overcome the excessive signature verification process. While their FastAuth (fast authentication) scheme secures periodic single-hop beacon messages, the SelAuth (selective authentication) secures multi-hop applications in which a bogus signature may spread out quickly and impact a significant number of vehicles. SelAuth provides fast isolation of malicious senders, even under a dynamic topology at low computational costs.

Similarly, the authors of [48] designed a lightweight and de-centralized authentication scheme called TEAM (trust-extended authentication mechanism). This scheme employs a pre-shared- key, XOR operation and hash function during the authentication process. The scheme was implemented based on the transitive trust relationships between vehicles, and hence provides a de-centralized authentication scheme. In Ref. [49], an authentication scheme that uses one-way hash functions and secret keys be-tween vehicle and RSU was proposed. Also [50], proposed a novel authentication scheme which focuses on sender authenti-cation. The scheme makes use of hash chains and authentica-tion codes signed by an authentication center (AC) to authenti-cate vehicles. Each broadcast packet contains the safety mes-sage along with an authentication code. The receiving vehicle decrypts the code using the pre-loaded public key of an AC, so authenticating the sender and the received message. An RSU- aided message authentication scheme, called RAISE, proposed in Ref. [51] uses a symmetric-based approach. In this scheme, vehicle established a shared secret key with RSU within its vicinity. The RSU are responsible for verifying messages, and then disseminate the verified messages to the vehicles. The scheme also takes the k-anonymity [52] technique to prevent a malicious node from associating a message with a particular vehicle to protect its privacy. However, this scheme is highly dependent on RSUs, which could not be available in all environments. The works of [46] extended the RAISE scheme to include a method for vehicles to cooperatively authenticate messages in locations where RSUs are not available.

5.2. *Asymmetric-based solutions*

Asymmetric cryptosystems can also be used to provide security within the 3GPP access layer. The concept of asymmetric cryptography as applied at the application layer has already been covered in the previous section. The approach would be fundamentally similar here, and would face the same challenges in high traffic density scenarios. It would also require introducing VPKI to 3GPP just to serve the purposes of direct communication via the PC5 interface. The following are research works that uses different approaches to minimize the computational complexity of asymmetric cryptosystems.

In [53], the authors used a computationally efficient two-way anonymous authentication scheme based on the anony-mous certificates and signatures to verify the message source and integrity in V2V. Furthermore [54], proposed an enhanced dual authentication and key management scheme for VANETs using the elliptic curve cryptography (ECC) and the Diffie-Hellman key exchange protocol. The works of [55] proposed a two-way authentication scheme in which an anonymous identity was generated by a vehicle and verified by the trust authority to reduce the pressure on key management. Also [56], addresses the delay involved in validating certificate's status. Instead of performing the time consuming CRLs check, the authors use a keyed Hash Message Authentication Code (HMAC), wherein

the key used to calculate the HMAC is shared only between non-revoked vehicles. However, vehicles must still verify the validity of certificate and signature because it still uses a trusted authority (TA) for generating and distributing secret keys and certificates to all vehicles. Certificate revocation is triggered by the TA which involves revoking the current secret key and se curely distributing a new secret key to all non-revoked vehicles. Similarly, the secure privacy-preserving protocol described in Ref. [45] aims to reduce the computational overhead related to dig-ital signature generation and verification of asymmetric-based approach. The authors uses a short message authentication code tag that is appended to each outgoing message in place of a digi tal signature. Furthermore [57], proposes a conditional privacy-preserving authentication protocol based on self-certified public key encryption [58]. The authors aimed to reduce the overhead involved in generation and distribution of pseudonyms and the related certificates. However, the scheme requires the installation of a tamper-proof device in each vehicle.

The anonymous authentication protocol proposed in Ref. [59] uses a trusted authority to assign each vehicle and RSU a long term certificate during registration. Each RSU is responsible for assigning a master key to each vehicle within its region after authenticating the vehicle based on its long term certificate. The vehicles then uses the master key to generate pseudonyms locally and uses them to sign messages to be transmitted. This work has lower signature verification overhead compared to a similar approach described in Ref. [60]. Also, the authors of [61] proposes an efficient method of the distribution of CRLs to vehicles. They use a probabilistic data structure called Bloom fil ters [62] for checking the status of vehicles certificates. Bloom filter is known for low computation complexity since it uses k hash functions to store elements in the filter. This reduces the overhead cost considerably as compared to the conventional CRL checking process, which in turn lowers the message verification time. The use of Bloom filters is also more efficient and cost effective than the RSU-based distribution scheme because it does not require widespread deployment of RSUs.

5.3. Group-based solutions

The cooperative nature of V2V applications can be exploited to provide faster message verification processes for asymmetric-based schemes. Group-based solutions are a subset of asymmetric cryptosystems in which vehicles that are close to each other cooperatively form a group to verify signatures of re ceived messages and share the results with one another. This is possible because vehicles within a given communication range practically receive the same warning message regarding a given event. As a result, group-based solutions reduce the time required for message verification and so help to meet the latency constraints of V2V applications. The works of [63–67] have combined asymmetric cryptography with group signat ture verification techniques in order to reduce the time spent for single message verification at the receiving vehicles. Similarly [46], proposed a cooperative message-authentication scheme. In this scheme, vehicles work together to verify only defined sets of received message signatures according to a selection algo rithm, and then share their results to each other. As vehicles do not verify every single received message, which the computational overhead is reduced as compared to single message verification schemes.

Furthermore, the works of [68,69] designed a scheme which employed cooperative message authentication techniques along with batch group signature verification and hash MAC (HMAC). The works of [70,71] presented a message authentication protocol for vehicular networks that employs a cooperative message authentication scheme and a short group signature technique. In this scheme, some vehicles act as signature verifiers for received messages, whereas other vehicles within the vicinity only receive verified messages from verifier vehicles. A DoS resilient cooperative message verification scheme for V2V communication was proposed in Ref. [72]. In this work, the authors' leverages cooperating vehicles to verify signatures of received messages and then share the verification results with their neighbors. This significantly reduces the computation overhead of verifying each received message by a vehicles, and decreases waiting time of messages in queue before verification. The study in Ref. [73] present a cluster-based algorithm for se-curing emergency messages in V2V. In their scheme, vehicles form clusters and the cluster-heads are responsible for intra-cluster management. The authors also used MAC layer broad-cast protocols for increasing the reliability of emergency message dissemination [74]. proposed an on-the-fly group creation approach in which nearby RSUs create and maintain groups of vehicles. This allows vehicles to join the group maintained by RSU in its range, and also anonymously broadcast authenticated messages to vehicles within its group. However, authenticated message dissemination among vehicles that belongs to different groups is not addressed. They also assumed that RSUs are densely deployed and trustworthy. The study in Ref. [75] uses group signatures and threshold authentication approach. In this scheme, a received message is accepted by a vehicle only after it has been authenticated by a threshold number of other vehicles to reduce the overhead related to downloading and checking CRL. It uses bilinear pairing based cryptography. Since RSUs serve as group managers, if RSUs are compromised, the group keys could be at risk of been compromised.

Group and cooperative-based schemes significantly reduce message verification delay. However, the drawback of group-based signature verification schemes is that it is difficult to form groups of vehicles due to the high relative speed and short connection time between moving vehicles. For instance in high-way scenarios, proximity-based group of vehicles may have an irregular distribution, with members joining and leaving constantly, which makes determining group boundaries a bottleneck. Also, there is a need to establish a trust relationship be-tween those vehicles selected to verify the messages and those receiving the results. All of these contribute to signalling cost, which may lead to excessive delay.

5.4. Hash chain-based solutions

Hash chain techniques leverage lightweight cryptographic primitives (e.g. MACs) to build security solutions appropriate to a wireless environment. One commonly used protocol for broadcast authentication in wireless ad hoc networks is called.

TESLA (time efficient stream loss-tolerant authentication) [70,76]. TESLA uses a symmetric MAC algorithm to protect the integrity of messages, but introduces the element of asymmetry by delaying the disclosure of the secret key used. A given key may only be used by a sender to generate MACs within a well-defined time window, after which it is made public and may be used by receivers to verify the integrity of messages sent within that window. A new key is then used for the next window as illustrated in Fig. 5. A sequence of keys used by a given sender is generated such that the Nth key used is the result of applying a hash function to the N+1th key. Thus the hash function can be used to verify a sequence of keys used by a given sender, and hence the sequence of messages it sent, provided that the first key in the sequence can reliably be attributed to that sender. TESLA requires that communicating nodes synchronize their clocks in advance, and also agree how time is divided into fixed-length windows.

The essential components of TESLA are; one-way key generation, computation of secret key delay disclosure interval, loose time synchronization and a security condition check. Fig. 6 gives the description of the operations of TESLA protocol at both sender and receiver ends. At the sender end, the steps are: secret key pre-computation using hash chain, commitment key distribution and message broadcasting. Storing verified chain commitment key, validation of secret key after every disclosure and message verification are the steps involved at the receiver

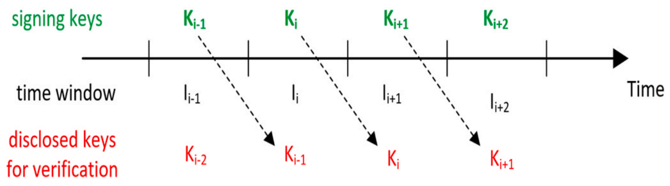

Fig. 5. TESLA's key sequence.

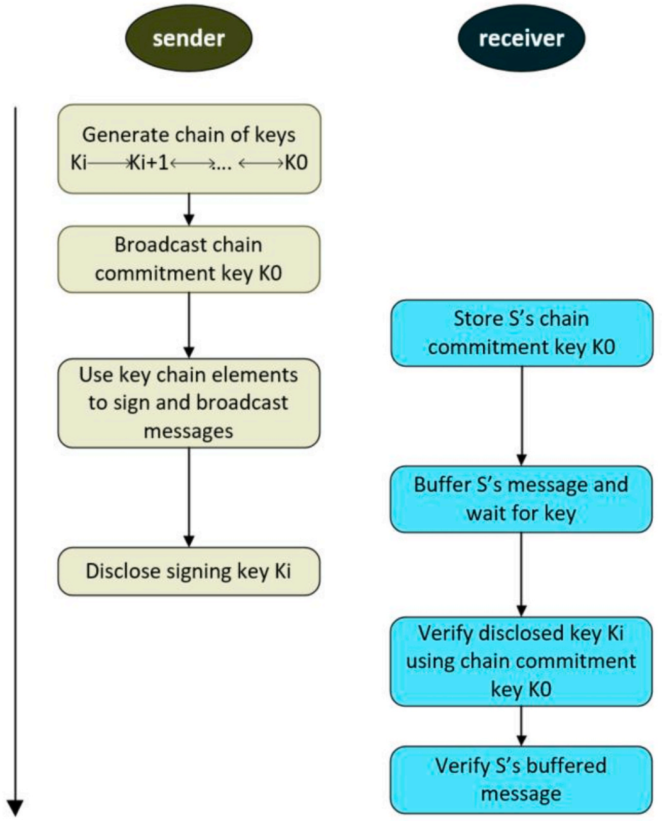
sender
receiver
Generate chain of keys
Ki⟶Ki+1⟵⟶... ⟵⟶K0
Broadcast chain commitment key K0
Use key chain elements to sign and broadcast messages
Disclose signing key Ki
Store S's chain commitment key K0
Buffer S's message and wait for key
Verify disclosed key Ki using chain commitment key K0
Verify S's buffered message

Fig. 6. TESLA's operation.

end.

The main benefits of TESLA are low computation over-head, low communication overhead, and robustness to packet loss. However, TESLA also has some shortcomings: the basic version cannot provide non-repudiation without a trusted time-stamping mechanism; there is a need for something like a conventional PKI to enable the identity of the sender's commitment key chain to be verified; the one-way key chain has a finite length, so new chains need to be created periodically; delayed message verification of at least one time window; and there is a requirement for loose synchronization between sender and receivers. To overcome these shortcomings and to make TESLA adaptable to various environment and network configurations, new versions of TESLA have been proposed, including: immediate authentication TESLA, multiple TESLA, multi-level.

TESLA, TESLA++, and μTESLA. These modify the original. TESLA's operation with respect to reducing message verification delay, varying the key disclosure delay interval, efficient distribution of chain commitment key and applying an appropri ate message verification mechanism. For instance, TESLA++ is designed for vehicular networks [77], and μTESLA was pro-posed for energy-constrained IoT networks [78]. The following paragraph discusses research works that apply the original TESLA and its new variants to create security schemes for broadcast V2V communication.

The works of bib79[47,79,80] addresses the delayed message veri-fication of TESLA using a prediction-based approach in or-der to make it effective in V2V. They exploit the ability of a sending vehicle to predict its own future position by observing its movement pattern between two consecutive positions. The sender constructs a Merkle Hash Tree (MHT) to generate a prediction outcome. This is sent to the receiver in advance to enable instant message verification. Performance evaluation shows that as vehicles future positions are correctly predicted and verified, a considerable number of messages can be verified immediately even in congested environment. How-ever, this depends on the accuracy and computational cost of the chosen prediction algorithms. Similarly [81], designed a broadcast message authentication protocol based on TESLA for V2I networks. This scheme focuses on providing efficient message authentication when vehicles communicate with road-side sensors. In Ref. [82], the authors propose a hybrid authentication mechanism that combines ECDSA with TESLA++. In this scheme, a sender generates both MACs and ECDSA sig-natures for each message to be broadcast. A receiver authenticates each received broadcast message using the TESLA++ verification process and ignores ECDSA signature verification unless either the non-repudiation property is required, or the TESLA++ verification fails due to loss of the MAC packet or message/key packet. Simulation results indicate that packets are mostly authenticated using TESLA++ in less dense traffic conditions. However, in high traffic density situations when the channel contention increases, more packets are dropped before being received and the ECDSA signature verification process is used to authenticate messages.

The works of [83, 84] proposed different approaches to distributing TESLA's chain commitment key in dynamic V2V environment. In [83], the authors proposed a reactive approach; if a vehicle VA receives a message from another vehicle VB, but does not have its commitment key then it sends a key re-quest message to VB. A Bloom filter obtained from a RSU is used in validating VB's response. The authors of [84] adopts a reactive commitment key exchange method. On receiving a message from an unknown vehicle, the receiver broadcasts its own commitment key along with a list of vehicles (including the sender) whose commitment keys it needs. This approach may result in vehicles being overwhelmed with many copies of messages containing commitment keys that they already possess. It.

is computationally expensive to verify the broadcast messages and the scheme is vulnerable to denial of service attacks.

5.5. *Comparison and critical analysis*

In this sub-section, a comparative analysis of the three candidate solutions-symmetric, asymmetric VPKI and hash chain is presented, based on some fundamental security and performance properties that are essential to V2V broadcast communication. Table 3 indicates how each of the candidate solution meet or did not meet the corresponding security and performance properties. The information in there can be used to assess which of these alternatives might be most appropriate to provide robust security solution for which safety application. On one hand, V2V communications should be reliable, secure and provide real-time performance. On the other end, the extra processing and message overheads required for a given security solution should not affect the quality of V2V services. The main idea is therefore to look for an optimal solution that can satisfy the key security properties of V2V broadcast communication with minimal impact to the performance requirements of the underlying safety applications. It should be noted that the figures provided in this table are from a pure software implementation of the crypto algorithms.

Asymmetric PKI-based schemes provides the needed security level, and satisfy majority of the security properties required by V2V broadcast communication. Moreover, these schemes were recommended to secure V2X communications by the security working groups of some standardization bodies e.g. ETSI C2X Communication Consortium (C2X CC). But still there is lack of experimental deployment and performance evaluation of these schemes under realistic traffic conditions for different safety applications. Indeed, the effectiveness of this approach depends on what type of safety messages is protecting and the characteristics of those messages. For safety applications that generate event-driven messages, which do not occur frequently, the asymmetric VPKI-based security solution can be conveniently applied to protect them. On the other hand, for safety applications that generate periodic broadcast messages, the high computation experienced while performing asymmetric operations to verify each received message at the receiving vehicle results in high delay that may exceed the maximum

Table 3
Comparative analysis of security solutions for 5G-V2V broadcast communications.

Security Properties	Asymmetric-based Solu-tions	Symmetric-based Solutions	Hash chain-based Solutions
Cryptographic method	Digital signature algorithms, mostly ECDSA and its variants (NIST and Brainpool curves)	MAC, mostly MD5 and SHA-1	Hash-chain function and MAC
Source Authentication	Yes, by validating identity of message source on certificate	Yes by verifying shared secret key	Yes, by verifying chain commitment key
Message Integrity	Yes, by verifying the signa-ture on received message	Yes, by verifying MAC of received message	Yes, by verifying MAC of received message
Non-repudiation	Yes	No	No
Immediate authentication	Yes, received messages are verified immediately using the certificates attached	Yes	No, have to wait for the secret key to be disclose after a pre-defined time interval
Robustness to packet loss	Not required	–	Yes, Lost keys can be recovered from subsequent received keys
Security Condition checks	Yes, require to check the sta-tus of sender's certificate	No	Yes, require to validate disclosed key is part of sender's key chain
Communication overhead	High - size of certificate and digital signature are 125 bytes and 56–64 bytes, respectively	Low - size of MAC is 8–20 bytes	Low - size of MAC is 8–20 bytes
Computational cost	high - signature verification (up to 20 ms per operation)	low - MAC verifica-tion is 1–10μs	low-low - MAC verification is 1–10μs
Resilience to replay attack	Yes - use of time stamp	Yes - use of time stamp	Yes - use of time stamp
Resilience to signature flooding	No, excessive signature verification can lead to DoS at- tack	Yes	Yes
Buffering overhead	No	No	Yes, messages is temporarily buffered until secret keys is disclosed
Key distribution	Requires PKI to distribute certificates	Pre-loaded/ Key ex-change mechanisms	Use hash chain keys

tolerable latency for these safety-critical applications. Particularly in high vehicle density area, where vehicles exchange periodic safety messages with each other, verifying high number of received messages through signature scheme may lead to DoS attack. This makes asymmetric-based solutions not scalable to traffic density. Therefore, such an environment require faster security solutions that would not affect the performance of V2V safety applications. Moreover, asymmetric VPKI approach were de-signed to provide security services at the application layer level of the communicating vehicles. The implementation of application layer security for.

cellular-based V2V communications might require some system level modification from the mobile operator's side. In addition, interfacing a VPKI system with cellular network elements would raise concerns about signaling cost implication, risk, management and maintenance is-sues, etc., which need to be properly investigated.

With regards to symmetric-based security solutions, these approaches are mainly applicable to vehicle-infrastructure-vehicle mode of communication, not direct V2V. Message verification depends on sending authenticity information from an infrastructure. Although these solutions are extremely fast with low communication and computational overheads, but they do not provide the needed security requirement of proving that a message really originate from a given sender. In addition, they require an efficient key distribution mechanism that will securely guarantee the exchange of shared secret keys between the sender and receiver(s). Distributing secret keys in one-to- many communication environment with dynamically changing end-points like V2V, and no prior knowledge between senders and receivers, is a complex challenge. It is neither efficient nor realistic for vehicles that accidently meet on the road to inter-actively establish a shared secret key between themselves prior to broadcasting messages, for a communication that occur periodically with very short connection time. As such, this security approach is not feasible in V2V broadcast environment.

Security solutions based on hash chain techniques provides fast message verification at low computational cost, which makes them suitable to be applied to secure safety messages in V2V communications. Particularly for safety applications that generate regular and predictable packets, these solutions can be effective with appropriate key disclosure delay interval and time quantization mechanism between senders and receivers. How-ever, the use of hash functions alone with different delayed key techniques in these solutions cannot prove the authenticity of a message sender. Moreover, the delayed key feature require accurate estimation of message propagation times, in order to evaluate a realistic delayed key disclosure time interval. This might be a problem especially with high moving vehicles, where the propagation channel characteristics changes rapidly.

In summary, the cost of cryptographic operations is one of the factors that affect the performance of V2V safety applications. The latency requirements of most V2V safety applications are very strict; there is no stand-alone cryptographic solution that can satisfy all the needed security properties while meeting these latency constraints, particularly in high traffic density areas. Therefore, a hybrid-based approach that combines hash chain technique with digital signature can be applied at the 3GPP access layer to provide fast message verification with non-repudiation property in order to satisfy the security and performance requirements of V2V broadcast communications. Below is a non-exhaustive list of salient features of 5G-based secure broadcast V2V communication as well as some lessons learnt in this study:

- V2X communications can be used to improve road safety, enhance traffic efficiency and provide advanced in-vehicle user infotainment services
- The V2V/P/I use cases have particular characteristics that constrain solutions: (1) high mobility of vehicles with short connection time (2) vehicles need to verify and process received broadcast messages rapidly (3) heterogeneous environment with varying density of vehicles and (4) one-way transmission mode with no prior security association
- The spread of malicious information in vehicular net-work environments could have disastrous consequences, including loss of life and property, thus V2V broadcast messages need to be protected against security threats, which include message forgery, replay, etc.
- Although 3GPP presently concedes security to the upper layers of the ITS stack (i.e. application layer), however application layer techniques incur higher latency, computational intensive and adds considerable overheads. Thus having a security solution at the access layer is conceivably preferable in order to ensure system compatibility and reduce deployment cost.
- The security mechanisms employed in V2V must not pre-vent CAMs and DENMs safety messages being exchanged and processed by

legitimate V-UEs within the performance requirements of the underlying safety applications.

- The cost of cryptographic operations is one of the factors that affect the performance of V2V safety applications. Therefore a hybrid-based approach that combines hash chain technique with digital signature can be applied at the 3GPP access layer to provide fast message verification with non-repudiation property in order to satisfy the security and performance requirements of V2V broadcast communications.

6. Challenges and further work

This section presents the relevant open issues and challenges on providing 3GPP layer security solution for direct 5G-V2V communication over PC5 interface.

6.1. *Ubiquitous security solutions*

3GPP also defines autonomous operation (also referred to as Mode 4) for the PC5-based V2V communication. In here, vehicles in close proximity self-assign radio resources from a pre-defined resource pool, use other source of time synchronization, and independently scheduled communication between themselves without any network assistance. In the near future, this mode of operation will attract much interest in order to realize the full benefits of intelligent transport systems. Moreover, in situations where there is no network availability e.g. high-way or rural roads, vehicles shall solely rely on the direct PC5 link for both data exchange and control signaling. To this end, there is need to extend the security solution to cater for such a distributed and independent setup.

6.2. *Support for multi-hop broadcast network*

Some safety applications require multi-hop transmission of the safety messages in order to extend message reachability to vehicles that are few meters away from the incidence area. In multi-hop broadcast transmission, some vehicles acts as relay nodes by re-broadcasting the safety messages to their neighbors. Each forwarded broadcast packet should be verified at every hop before re-transmission. It is important for any security solution that is envisioned for cellular-V2X system to sup-port multi-hop communication so that only verified messages are forwarded.

6.3. *Implementing vehicular VPKI in 5G cellular network*

How a VPKI architecture is implemented can vary from one system to another. As such, the introduction of VPKI system in existing 3GPP architecture is another research area that need to be investigated. The VPKI system will require to be inter-faced with core network nodes to receive requests, distribute certificates, collect misbehaviour reports, and revoke certificates. This will increase the signaling cost within the mobile network side. Therefore, the complexity and cost of having a VPKI system into a 3GPP architecture need to be properly understood. Also, support for roaming among vehicles

that belongs to different operators is an issue. In roaming situations, vehicles needs to obtain certificates from their respective home network V2X Control Function (VCF) and at the same time, use the certificates to verify messages exchanged between them-selves. How different VCFs for different operators coordinate certificate distribution and management is a challenge. There is need for the security scheme to offer a universal method that can support V2V secure communications, even during roaming and across multiple operators.

7. Conclusion

V2V safety applications aims to improve road safety and traffic efficiency by sending advanced warning messages to drivers to support their decisions, through the cooperative exchange of messages between connected vehicles. Since these safety messages are broadcasted in open access environment, it is there-fore important to ensure that safety messages indeed originate from a legitimate vehicle, and that the received message content can be verified in a timely manner by the receiving vehicles without impacting the critical latency of safety applications. The approach to provide these security goals for V2V safety applications is predominantly based on cryptographic methods. However, the unique characteristics of V2V broadcast communication as well as the performance requirements of the safety applications imposes a great challenge to implement a security solution.

In this paper, after reviewing the benefits of using cellular-based radio technologies to provide communication platform for vehicles to exchange safety messages, different V2V applications, use-cases and their corresponding performance requirements were presented. Moving on to the main aim of this study, which is investigating the security aspect of 5G-based V2V broadcast communication in cellular network, various security issues were identified and a survey of different cryptographic methods used to build defence mechanism and largely satisfy the required security properties in V2V communication was provided from the literature. The access layer cryptographic options are asymmetric VPKI, symmetric and hash chains. Each of these options have their own benefits and weaknesses, particularly when applied to V2V broadcast domain. When compared, a few points can be highlighted: symmetric-based solutions are faster than asymmetric VPKI- based solutions. However, security can be better achieved by digital signatures that provide non-repudiation and immediate authentication benefits. On the other hand, for V2V safety applications that periodically generate broadcast messages, asymmetric VPKI-based security solutions cannot efficiently handle these kind of messages especially in denser traffic environment since they have longer message verification time compared to other methods. Therefore, a hybrid composition of hash chains with intermittent digital signatures is more appropriate for these type of safety applications.

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.

References

[1] ETSI. European standard (telecommunications series) intelligent trans- port systems (its); communications architecture". ETSI 2010;1.

[2] 3GPP-TR22.885. 3rd generation partnership project; study on LTE support for v2x services". 2015. 14.

[3] Seo H, Lee K-D, Yasukawa S, Peng Y, Sartori P. Lte evolution for vehicle-to-everything services. IEEE Commun Mag 2016;54(6):22–8.

[4] Abboud K, Omar HA, Zhuang W. Interworking of dsrc and cellular network technologies for v2x communications: a survey. IEEE Trans Veh Technol 2016;65 (12):9457–70.

[5] Doppler K, Rinne M, Wijting C, Ribeiro CB, Hugl K. Device-to- device communication as an underlay to lte-advanced networks. IEEE Commun Mag 2009; 47(12).

[6] Chen S, Hu J, Shi Y, Zhao L. Lte-v: a td-lte-based v2x solution for future vehicular network. IEEE Internet of Things Journal 2016;3(6):997–1005.

[7] Araniti G, Campolo C, Condoluci M, Iera A, Molinaro A. LTE for vehicular networking: a survey. IEEE Commun Mag 2013;51(5):148–57.

[8] 3GPP-TR22.885. 3rd generation partnership project; study on lte support of vehicle-to-everything (v2x) services. 2015 (release 14).

[9] 3GPP-TR36.885. 3rd generation partnership project; technical specification group radio access network. Study on lte-based v2x services. 2016 (release 14).

[10] Kenney JB. Dedicated short-range communications (dsrc) standards in the United States. Proc IEEE 2011;99(7):1162–82.

[11] ETSI-TS102.940. Intelligent transport systems (its); security; its communications security architecture and security management. 2018.

[12] Fernandes B, Rufino J, Alam M, Ferreira J. Implementation and analysis of ieee and etsi security standards for vehicular communications. Mobile Network Appl 2018; 23(3):469–78.

[13] Lyu C, Gu D, Zhang X, Sun S, Tang Y. Efficient, fast and scalable authentication for VANETS. In: 2013 IEEE wireless communications and networking conference (WCNC). IEEE; 2013. p. 1768–73.

[14] Haas JJ, Hu Y-C, Laberteaux KP. Real-world VANET security protocol performance. GLOBECOM 2009-2009 IEEE global telecommunications conference. IEEE; 2009. p. 1–7.

[15] Dai J, Pu L, Xu K, Meng Z, Liu Z, Zhang L. The implementation and performance evaluation of wave based secured vehicular communication system. In: 2017 IEEE 85th vehicular technology conference (VTC spring). IEEE; 2017. p. 1–5.

[16] Muhammad M, Kearney P, Aneiba A, Kunz A. Analysis of security overhead in broadcast v2v communications. International conference on computer safety, reliability, and security. Springer; 2019. p. 251–63.

[17] Cincilla P, Hicham O, Charles B. Vehicular pki scalability-consistency trade-offs in large scale distributed scenarios. Vehicular networking conference (VNC). 2016. p. 1–8. IEEE, IEEE, 2016.

[18] Mejri MN, Ben-Othman J, Hamdi M. Survey on vanet security challenges and possible cryptographic solutions. Vehicular Communications 2014;1(2):53–66.

[19] Manvi SS, Tangade S. A survey on authentication schemes in vanets for secured communication. Vehicular Communications 2017;9. ISSN: 2214-2096:19–30.

[20] Muhammad M, Safdar GA. Survey on existing authentication issues for cellular-assisted v2x communication. Vehicular Communications 2018;12:50–65.

[21] Yoshizawa T, Preneel B. Survey of security aspect of v2x standards and related issues. In: 2019 IEEE conference on standards for communications and networking (CSCN). IEEE; 2019. p. 1–5.

[22] Arif M, Wang G, Bhuiyan MZA, Wang T, Chen J. A survey on security attacks in VANETs: communication, applications and challenges. Vehicular Communications 2019;19:100179.

[23] Cao J, Ma M, Li H, Ma R, Sun Y, Yu P, Xiong L. A survey on security aspects for 3gpp 5g networks. IEEE communications surveys & tutorials 2019;22(1):170–95.

[24] 3GPP-TS22.186. 3rd generation partnership project; Technical Specification group services and system aspects; enhancement of 3gpp support for v2x scenarios. 2017. 15.

[25] 3GPP-TR22.886. 3rd generation partnership project. Technical Specification group services and system aspects; study on enhancement of 3gpp support for 5g v2x services. 2018 (release 16).

[26] ETSI-EN-302-637-2-v1.3.2. Intelligent transport systems; vehicular communications; basic set of applications; part 2. Specification of co- operative awareness basic service; 2014.

[27] ETSI-EN-302-637-3-v1.3.2. Intelligent transport systems; vehicular communications; basic set of applications; part 3. Specification of de- centralized environmental notification basic service; 2014.

[28] Galaviz-Mosqueda A, Morales-Sandoval M, Villarreal-Reyes S, Galeana-Zapién H, Rivera-Rodŕıguez R, Alonso-Arévalo MA. Multi- hop broadcast message dissemination in vehicular ad hoc networks: a security perspective review. Int J Distributed Sens Netw 2017;13(11):1550147717741263.

[29] Grover K, Lim A. A survey of broadcast authentication schemes for wireless networks. Ad Hoc Netw 2015;24:288–316.

[30] Raya M, Hubaux J-P. Securing vehicular ad hoc networks. J Comput Secur 2007;15 (1):39–68.

[31] Lee K-D. V2x application requirements by NGMN alliance. 2017.

[32] 3GPP-TR33.885. 3rd generation partnership project; Technical specification group services and system aspects; study on security aspects for lte support of vehicle-to-everything (v2x) services (release 14). 2017.

[33] Gonzalez-Mart in M, Sepulcre M, Molina-Masegosa R, Gozalvez J. Analytical models of the performance of c-v2x mode 4 vehicular communications. IEEE Trans Veh Technol 2018;68(2):1155–66.

[34] Abbas F, Fan P, Khan Z. A novel low-latency v2v resource allocation scheme based on cellular v2x communications. IEEE Trans Intell Transport Syst 2018;20(6): 2185–97.

[35] Anwar W, Franchi N, Fettweis G. Physical layer evaluation of v2x communications technologies: 5g nr-v2x, lte-v2x. IEEE 802.11 bd, and IEEE 802.11 p, in: 2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall) 2019:1–7. IEEE.

[36] Boban M, Manolakis K, Ibrahim M, Bazzi S, Xu W. Design aspects for 5g v2x physical layer. In: Standards for communications and networking (CSCN), 2016 IEEE conference on. IEEE; 2016. p. 1–7.

[37] Abbasi M, Shahraki A, Barzegar HR, Pahl C. Synchronization tech- niques in "device to device-and vehicle to vehicle-enabled" cellular net- works: a survey. Comput Electr Eng 2021;90:106955.

[38] Haidar F, Kaiser A, Lonc B. On the performance evaluation of vehicular pki protocol for v2x communications security. In: Vehicular technology conference (VTC-Fall); 2017. p. 1–5. IEEE 86th, IEEE, 2017.

[39] Hamida EB, Noura H, Znaidi W. Security of cooperative intelligent transport systems: standards, threats analysis and cryptographic counter- measures. Electronics 2015;4(3):380–423.

[40] Sch ütze T. Automotive security: cryptography for car2x communication. Embedded world conference, vol. 3; 2011.

[41] Ibrahim S, Hamdy M. A comparison on vanet authentication schemes: public key vs. symmetric key. Computer engineering & systems (IC- CES), 2015 tenth international conference on. IEEE; 2015. p. 341–5.

[42] 3GPP-TS33.102. 3rd generation partnership project; technical specification group services and system aspects; 3G security. security architecture; 2020. 16.

[43] Li G, Ma M, Liu C, Shu Y. An efficient authentication framework over heterogeneous vehicular networks. Communication systems (ICCS), 2016 IEEE international conference on. IEEE; 2016. p. 1–6.

[44] Ying B, Makrakis D, Mouftah HT. Privacy preserving broadcast message authentication protocol for vanets. J Netw Comput Appl 2013;36(5):1352–64.

[45] Lin X, Sun X, Wang X, Zhang C, Ho P-H, Shen X. Tsvc: timed efficient and secure vehicular communications with privacy preserving. IEEE Trans Wireless Commun 2008;7(12):4987–98.

[46] Zhang C, Lin X, Lu R, Ho P-H, Shen X. An efficient message authentication scheme for vehicular communications. IEEE Trans Veh Technol 2008;57(6):3357–68.

[47] Hsiao H-C, Studer A, Chen C, Perrig A, Bai F, Bellur B, Iyer A. Flooding-resilient broadcast authentication for vanets. Proceedings of the 17th annual international conference on Mobile computing and net- working. ACM; 2011. p. 193–204.

[48] Chuang M-C, Lee J-F, Team. Trust-extended authentication mechanism for vehicular ad hoc networks. IEEE systems journal 2014;8(3):749–58.

[49] Chim TW, Yiu S, Hui LC, Li VO. Security and privacy issues for inter-vehicle communications in vanets. In: Sensor, mesh and ad hoc communications and networks workshops, 2009. SECON workshops'09 6th annual IEEE communications society conference on. IEEE; 2009. p. 1–3.

[50] Vighnesh N, Kavita N, Urs SR, Sampalli S. A novel sender authentication scheme based on hash chain for vehicular ad-hoc networks. Wireless technology and applications (ISWTA), 2011 IEEE symposium on. IEEE; 2011. p. 96–101.

[51] Zhang C, Lin X, Lu R, Ho P-H. Raise: an efficient RSU-aided message authentication scheme in vehicular communication networks. 2008 IEEE international conference on communications. IEEE; 2008. p. 1451–7.

[52] Sweeney L, anonymity k-. A model for protecting privacy. Int J Uncertain Fuzziness Knowledge-Based Syst 2002;10(5):557–70.

[53] Vijayakumar P, Chang V, Deborah LJ, Balusamy B, Shynu P. Computationally efficient privacy preserving anonymous mutual and batch authentication schemes for vehicular ad hoc networks. Future Generat Comput Syst 2018;78:943–55.

[54] Balaji NA, Sukumar R, Parvathy M. Enhanced dual authentication and key management scheme for data authentication in vehicular ad hoc net- work. Comput Electr Eng 2019;76:94–110.

[55] Liu Y, Wang Y, Chang G. Efficient privacy-preserving dual authentication and key agreement scheme for secure v2v communications in an IoV paradigm. IEEE Trans Intell Transport Syst 2017;18(10):2740–9.

[56] Wasef A, Shen X. Emap: expedite message authentication protocol for vehicular ad hoc networks. IEEE Trans Mobile Comput 2011;12(1):78–89.

[57] Zhang J, Zhen W, Xu M. An efficient privacy-preserving authentication protocol in vanets. 2013 IEEE 9th international conference on mobile ad-hoc and sensor networks. IEEE; 2013. p. 272–7.

[58] Girault M. Self-certified public keys. In: Workshop on the theory and application of of cryptographic techniques. Springer; 1991. p. 490–7.

[59] Wang S, Yao N. Liap: a local identity-based anonymous message authentication protocol in vanets. Comput Commun 2017;112:154–64.

[60] Jiang S, Zhu X, Wang L. An efficient anonymous batch authentication scheme based on HMAC for vanets. IEEE Trans Intell Transport Syst 2016;17(8):2193–204.

[61] Haas JJ, Hu Y-C, Laberteaux KP. Efficient certificate revocation list organization and distribution. IEEE J Sel Area Commun 2011;29(3):595–604.

[62] Bloom BH. Space/time trade-offs in hash coding with allowable errors. Commun ACM 1970;13(7):422–6.

[63] Vijayakumar P, Azees M, Kannan A, Deborah LJ. Dual authentication and key management techniques for secure data transmission in vehicular ad hoc networks. IEEE Trans Intell Transport Syst 2016;17(4):1015–28.

[64] Lin X, Sun X, Ho P-H, Shen X. Gsis: a secure and privacy-preserving protocol for vehicular communications. IEEE Trans Veh Technol 2007;56(6):3442–56.

[65] Calandriello G, Papadimitratos P, Hubaux J-P, Lioy A. Efficient and robust pseudonymous authentication in vanet. In: Proceedings of the fourth ACM international workshop on Vehicular ad hoc networks. ACM; 2007. p. 19–28.

[66] Wasef A, Shen X. Efficient group signature scheme supporting batch verification for securing vehicular networks. In: Communications (ICC). 2010 IEEE International Conference on, IEEE; 2010. p. 1–5.

[67] Zhang L, Wu Q, Solanas A, Domingo-Ferrer J. A scalable robust authentication protocol for secure vehicular communications. IEEE Trans Veh Technol 2010;59 (4):1606–17.

[68] Zhu X, Jiang S, Wang L, Li H. Efficient privacy-preserving authentication for vehicular ad hoc networks. IEEE Trans Veh Technol 2014;63(2):907–19.

[69] Lin X, Li X. Achieving efficient cooperative message authentication in vehicular ad hoc networks. IEEE Trans Veh Technol 2013;62(7):3339–48.

[70] Shen W, Liu L, Cao X, Hao Y, Cheng Y. Cooperative message au-thentication in vehicular cyber-physical systems. IEEE Transactions on Emerging Topics in Computing 2013;1(1):84–97.

[71] Hao Y, Han T, Cheng Y. A cooperative message authentication protocol in vanets. In: Global communication conference (GLOBECOM); 2012. p. 5562–6. IEEE, IEEE, 2012.

[72] Dietzel S, ürtler JG, Kargl F. A resilient in-network aggregation mechanism for vanets based on dissemination redundancy. Ad Hoc Netw 2016;37:101–9.

[73] Ramakrishnan B, Nishanth RB, Joe MM, Selvi M. Cluster based emergency message broadcasting technique for vehicular ad hoc network. Wireless Network 2017;23 (1):233–48.

[74] Zhang L, Wu Q, Solanas A, Domingo-Ferrer J. A scalable robust authentication protocol for secure vehicular communications. IEEE Trans Veh Technol 2009;59 (4):1606–17.

[75] Shao J, Lin X, Lu R, Zuo C. A threshold anonymous authentication protocol for vanets. IEEE Trans Veh Technol 2015;65(3):1711–20.

[76] Perrig A, Canetti R, Tygar JD, Song D. The tesla broadcast authentication protocol. Rsa Cryptobytes 2005;5.

[77] Studer A, Bai F, Bellur B, Perrig A. Flexible, extensible, and efficient vanet authentication. J Commun Network 2009;11(6):574–88.

[78] Perrig A, Szewczyk R, Tygar JD, Wen V, Culler DE. Spins: security protocols for sensor networks, Wireless networks 8 (5). 2002. p. 521–34.

[79] Lyu C, Gu D, Zeng Y, Mohapatra P. Pba: prediction-based authentic- cation for vehicle-to-vehicle communications. IEEE Trans Dependable Secure Comput 2016; 13(1):71–83.

[80] Lalli M, Graphy GS. Prediction based dual authentication model for vanet. 2017 international conference on computing methodologies and communication (ICCMC). IEEE; 2017. p. 693–9.

[81] Ruan N, Hori Y. Dos attack-tolerant tesla-based broadcast authentication protocol in internet of things. Mobile and wireless networking (iCOST), 2012 international conference on selected topics in. IEEE; 2012. p. 60–5.

[82] Abueh YJ, Liu H. Message authentication in driverless cars. Tech- nologies for homeland security (HST), 2016 IEEE symposium on. IEEE; 2016. p. 1–6.

[83] Bao S, Hathal W, Cruickshank H, Sun Z, Asuquo P, Lei A. A lightweight authentication and privacy-preserving scheme for vanets using tesla and bloom filters. ICT Express 2018;4(4):221–7.

[84] Hu YC, Laberteaux KP. Strong vanet security on a budget, in: proceedings of workshop on embedded security in cars (ESCAR) 2006;6:1–9. Citeseer.