



10-2020


Secure Authentication and Privacy-Preserving Techniques in Vehicular Ad-hoc NETWORKS (VANETs)

Dakshnamoorthy Manivannan
University of Kentucky, dmani2@uky.edu

Shafika Showkat Moni
University of Kentucky, shafika.moni@uky.edu

Sherali Zeadally
University of Kentucky, szeadally@uky.edu

Follow this and additional works at: https://uknowledge.uky.edu/cs_facpub

 Part of the [Computer Sciences Commons](#), and the [Library and Information Science Commons](#)

[Right click to open a feedback form in a new tab to let us know how this document benefits you.](#)

Repository Citation

Manivannan, Dakshnamoorthy; Moni, Shafika Showkat; and Zeadally, Sherali, "Secure Authentication and Privacy-Preserving Techniques in Vehicular Ad-hoc NETWORKS (VANETs)" (2020). *Computer Science Faculty Publications*. 35.

https://uknowledge.uky.edu/cs_facpub/35

This Review is brought to you for free and open access by the Computer Science at UKnowledge. It has been accepted for inclusion in Computer Science Faculty Publications by an authorized administrator of UKnowledge. For more information, please contact UKnowledge@lsv.uky.edu.

Secure Authentication and Privacy-Preserving Techniques in Vehicular Ad-hoc NETworks (VANETs)

Notes/Citation Information

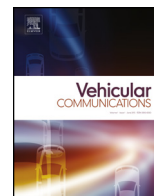
Published in *Vehicular Communications*, v. 25, 100247.

© 2020 The Author(s)

This is an open access article under the CC BY-NC-ND license (<https://creativecommons.org/licenses/by-nc-nd/4.0/>).

Digital Object Identifier (DOI)

<https://doi.org/10.1016/j.vehcom.2020.100247>



Secure authentication and privacy-preserving techniques in Vehicular Ad-hoc NETWORKS (VANETs)

D. Manivannan^{a,*}, Shafika Showkat Moni^a, Sherali Zeadally^b

^a Department of Computer Science, University of Kentucky, Lexington, KY 40508, USA

^b College of Communication and Information, University of Kentucky, Lexington, KY 40506, USA

ARTICLE INFO

Article history:

Received 23 October 2019

Received in revised form 16 January 2020

Accepted 8 February 2020

Available online 21 February 2020

Keywords:

VANETs

Vehicular networks

Securing VANETs

ABSTRACT

In the last decade, there has been growing interest in Vehicular Ad Hoc NETWORKS (VANETs). Today car manufacturers have already started to equip vehicles with sophisticated sensors that can provide many assistive features such as front collision avoidance, automatic lane tracking, partial autonomous driving, suggestive lane changing, and so on. Such technological advancements are enabling the adoption of VANETs not only to provide safer and more comfortable driving experience but also provide many other useful services to the driver as well as passengers of a vehicle. However, privacy, authentication and secure message dissemination are some of the main issues that need to be thoroughly addressed and solved for the widespread adoption/deployment of VANETs. Given the importance of these issues, researchers have spent a lot of effort in these areas over the last decade. We present an overview of the following issues that arise in VANETs: privacy, authentication, and secure message dissemination. Then we present a comprehensive review of various solutions proposed in the last 10 years which address these issues. Our survey sheds light on some open issues that need to be addressed in the future.

© 2020 The Author(s). 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/>).

1. Introduction

Several applications such as early warning systems which can warn about road construction, collisions, weather-related hazards, merging lanes, speed limits for curves, and pedestrian crossing warnings, are ready for the widespread deployment in Vehicular Ad-hoc NETWORKS (VANETs). Apart from assisting drivers to drive safely, VANETs can also provide infotainment to drivers/passengers for a more enjoyable driving as well as riding experience. Furthermore, VANETs can also assist in paying for parking and tolls, finding parking places, updating inbuilt vehicle navigation systems with real-time traffic situation, and downloading music, video and software updates [1–3]. VANETs can also assist law enforcement agencies in reconstructing accidents as well as reaching the location of the accidents faster.

The general model of VANETs proposed in the literature consists of two major components: On Board Units (OBUs), installed on vehicles, and Road Side Units (RSUs) installed on roadside to support the infrastructure needed for the deployment of VANETs.

Each vehicle is assumed to be equipped with a set of sensors to collect phenomena surrounding the vehicle; the OBU processes the information collected by the sensors and sends/receives them to/from other relevant vehicles directly or through nearby RSUs [4]. The RSUs may also connect to the Internet to provide the necessary services to vehicles. A broad range of applications can be enabled by two main types of communication: (i) infrastructure-based communication (Vehicle to Infrastructure (V2I) communication) and (ii) direct communication between vehicles (Vehicle to Vehicle (V2V) communication) [5] as shown in Fig. 1. Major efforts for standardizing VANETs communication protocols have been carried out by the IEEE 802.11 Task Group by defining enhancements to IEEE 802.11 required to support Intelligent Transportation Systems (ITS) applications. This amendment is currently known as IEEE 802.11p. The wireless communication capability between moving vehicles is achieved by using Dedicated Short Range Communication (DSRC). It is anticipated that DSRC will be used for both V2V communication and V2I communication. The spectrum is seen as particularly useful because it can support low-latency, secure transmissions, fast network acquisition and has the ability to handle rapid and frequent hand-overs that are inherent in VANETs; it is also robust in adverse weather conditions [6].

Although the excitement surrounding the potential benefits of VANETs is growing, the dynamic nature of VANETs (vehicles can

* Corresponding author.

E-mail addresses: mani@cs.uky.edu (D. Manivannan), shafika.moni@uky.edu (S.S. Moni), szeadally@uky.edu (S. Zeadally).

URL: <http://www.cs.uky.edu/~manivann> (D. Manivannan).

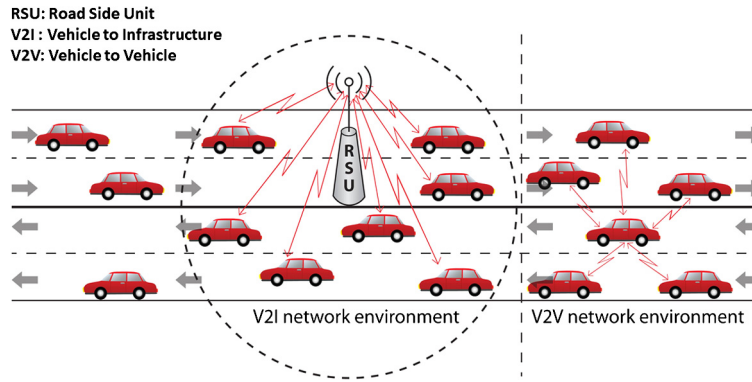


Fig. 1. VANET communication - infrastructure-based and infrastructure-less.

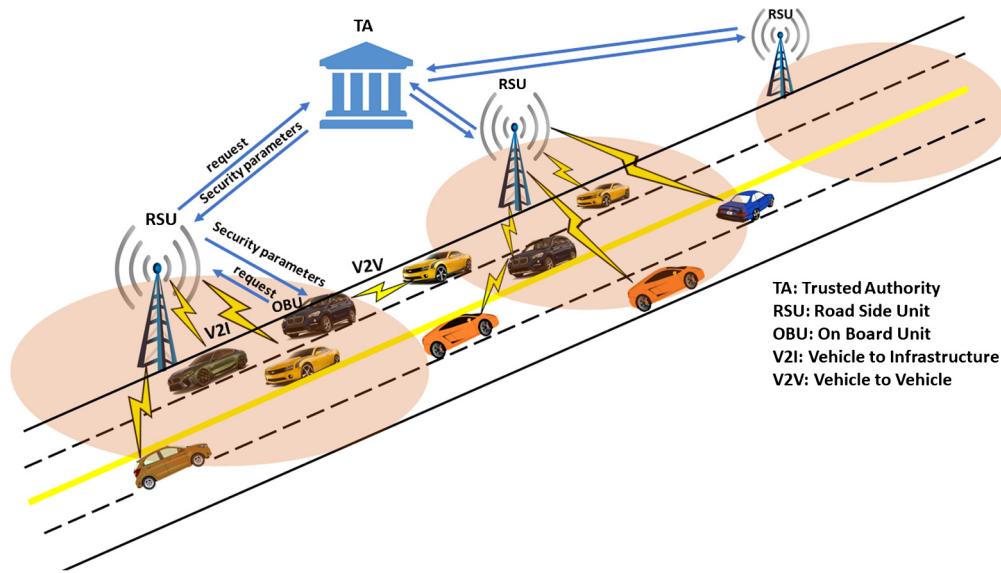


Fig. 2. Securing VANETs using a central Trusted Authority (TA).

join and leave at will) along with a multitude of system and application related requirements make it very challenging to design efficient methods for ensuring privacy of vehicles. Privacy refers to the privacy of the vehicles (drivers) and the location of the vehicles. When a vehicle sends a message, no one (except relevant authorities) should be able to determine the identity or location of the vehicle from the messages a vehicle sent. At the same time, all messages sent by a vehicle should be authenticated before being processed. Until these problems are solved to the best satisfaction of the users, widespread deployment of VANETs cannot take place. Authentication needs to be achieved at two levels – first at node level, referred as node authentication and second at the message level, referred as message authentication [7]. The basic principle of message authentication can be simplified as signing a message by the sender and then verifying the authenticity and integrity of the message at the receiver's end. Certain authentication requirements such as low computational overhead, strong and scalable authentication, efficient and scalable certificate revocation must be addressed and solved to ensure secure communication in VANETs.

Ensuring privacy of vehicles (drivers) is one of the many challenging issues for which an efficient solution needs to be found because an adversary could otherwise trace a vehicle's traveling routes by capturing and analyzing its messages [8] and identify the vehicle (driver) which may have drastic consequences for the drivers. To address this issue, many researchers have proposed protocols wherein vehicles use pseudonyms instead of their real ids in communication while at the same time enabling authori-

ties to extract the real ids from pseudonyms to trace and punish misbehaving vehicles. Such protocols are called conditional privacy-preserving protocols. Assigning pseudonyms to vehicles and changing them frequently is one of the strategies used to ensure privacy of vehicles. To maximize privacy, vehicles must change pseudonyms more frequently although the frequency of such change remains debatable. Factors such as availability and storage size play an important role in determining the rate at which pseudonym should be changed. A vast majority of the papers in the literature addressing security, authentication, and privacy use a TA for obtaining and loading OBUs and RSUs with security parameters such as keys, certificates, and pseudonyms (Fig. 2).

Securing VANETs from attacks from malicious vehicles is also a challenging issue due to the dynamic nature of network formation [9]. Some of these attacks may be carried out by nodes inside the network (i.e., nodes that have been already authorized to be a member of the VANET); other attacks may be carried out by vehicles that do not belong to the VANET. Among the existing types of attacks, message spoofing, message replay attack, message integrity attack, impersonation attack, Denial of Service (DoS) attack and movement tracking attack are the most common.

Traditional approaches for secure and authenticated message dissemination, largely based on message encryption and key management, can only guarantee secure message exchange between known source and destination pairs. These approaches cannot be directly applied in the context of VANETs due to the dynamic nature of VANETs. Message dissemination in VANETs can also be vul-

nerable to insider attacks (i.e., attacks from authenticated VANET members), who may tamper the content of the disseminated messages or send malicious messages. Thus, ensuring the integrity and authenticity of the messages transmitted in VANETs is an important issue. In this paper, we present a survey of some of the research works done in the last ten years addressing privacy, authentication and secure message dissemination in VANETs.

For convenience, we summarize below some of the frequently used acronyms in this paper:

CCN: Content-Centric Networks
 CRL: Certificate Revocation List
 D2D: Device to Device
 DSRC: Dedicated Short Range Communication
 DTNs: Delay Tolerant Networks
 ECC: Elliptic Curve Cryptography
 ECDSA: Elliptic Curve Digital Signature Algorithm
 GUID: Global Unique Identifier
 IBC: Identity Based Cryptography
 ITS: Intelligent Transportation System
 IVC: Inter-Vehicle Communication (same as V2V)
 KDC: Key Distribution Center (same as TA)
 LBS: Location-Based Service
 MLGS: Message-Linkable Group Signature
 OBU: On Board Unit
 PKI: Public Key Infrastructure
 QoS: Quality of Service
 RSU: Road Side Unit
 SDN: Software Defined Network
 TA: Trusted Authority
 TCP: Transmission Control Protocol
 TMKM: Topology Matching Key Management
 USDOT: United States Department of Transportation
 V2I: Vehicle to Infrastructure
 V2V: Vehicle to Vehicle
 VANET: Vehicular Ad-hoc Network
 VHN: Vehicular Heterogeneous Networks
 VPKI: Vehicular Public Key Infrastructure

1.1. Contributions of this work

The main objective of this work is to provide a comprehensive review of the papers published in the last ten years which have proposed privacy and authentication solutions in VANETs. Existing survey papers focus mostly on specific issues or are general surveys about VANETs. We do not have a comprehensive survey of the papers published in the last ten years addressing privacy, authentication and secure message dissemination in VANETs. This work tries to fill this gap. In this survey, we classified the protocols into different categories based on the problems addressed as well as tools and techniques used to solve these problems; we also do a comparative study of the protocols in each category. Our classification of the protocols is not strict because a protocol may belong to two or more categories. For example, a protocol that belongs to "Protocols based on Smart Cards and Tamper-proof Devices" category may also belong to "Protocols Using Bilinear Pairing based Cryptography" also but not conversely. This work would also serve as a suitable reference for researchers working on privacy, authentication and secure message dissemination in VANETs.

1.2. Organization of the paper

The rest of the paper is organized as follows: In Section 2, we discuss some of the existing survey papers on VANETs in general and also the survey papers related to privacy, security and authentication in VANETs. In Section 3, we present our survey of papers

published in the last ten years, addressing privacy, authentication and secure message dissemination in VANETs. We discuss some open issues and future directions in Section 4. Finally, we make some concluding remarks in Section 5.

2. Related surveys on VANETs architectures, privacy, security and authentication in VANETs

Many survey papers related to VANETs have been published in the literature. In this section we discuss some of these survey papers published over the last 10 years.

Hartenstein and Laberteaux [2] present a comprehensive study on VANET applications, requirements, topology, channel features and models. The study also covers a brief introduction to the architectures, protocols and standards for VANETs. It also discusses the main challenges facing the widespread implementation of VANETs. A survey on the communication and performance requirements of Inter-Vehicle Communication (IVC) protocols is presented by Willke et al. [10]. They discuss the relevance of different protocols for specific types of IVC applications. Based on this relevance, applications are grouped into classes that share a common communication organization and performance requirements. They listed four types of IVC applications – "General Information Services, Vehicle Safety Information Services, Individual motion control and Group Motion Control". Karagiannis et al. [11] describe VANET application requirements, use cases, architectures, protocols, challenges and some solutions to address these challenges. They primarily discuss the scope and objectives of several ITS projects, architectures and standards in the USA, Europe and Japan. Challenges in the area of anonymity and adaptive privacy, data centric trust and verification, geographical addressing, designing reliable message forwarding algorithm are also mentioned. Riley et al. [12] discuss protocols that use group based and non-group based authentication techniques based on both symmetric and asymmetric cryptography.

Zeaddally et al. [5] discuss recent research in the areas of "routing, broadcasting, Quality of Service (QoS) and security in VANETs". They also present a comparative study of the following VANET simulators: SUMO, MOVE, TranNs, VanetMobiSim, and NCTuns. Current research status, challenges and potentials of VANETs are briefly described by Eze et al. [13]. They discuss how kinematic information of vehicles can be used to support security of communicating vehicles. A vehicle's recent location, position, velocity and acceleration are derived from the kinematic information exchange in V2V and V2I communication. Secure, authentic and reliable exchange of kinematic information is a challenging issue for both safety and non-safety related VANET applications. Whaiduzzaman et al. [14] present a survey of vehicular cloud computing along with its application, cloud formation, key management technique, inter-cloud communication and various privacy and security issues related to inter-cloud communication. They argue that vehicular cloud computing is feasible and more cost-effective compared to normal cloud computing. Mokhtar and Azab [9] present an hierarchical structure of various network layers for VANETs and potential attacks in these layers with corresponding counter measures. Petit et al. [15] discuss the life-cycle of pseudonyms based on asymmetric key, identity, group signature and symmetric key. They also present a qualitative comparison of these four types of pseudonym schemes. Lu and Li [16] present a survey of privacy-preserving authentication of nodes and messages. They classify the various privacy-preserving authentication schemes based on the cryptographic protocols used and the privacy preservation mechanisms used in these schemes. Then they discuss the open issues in this area. Gerla et al. [17] survey content distribution protocols for VANETs.

Table 1
Summary of some of the recent survey papers on VANETs.

Paper	Year published	Area(s) Surveyed
Willke et al. [10]	2009	A survey of Inter-Vehicle Communication(IVC) Protocols and their applications.
Karagiannis et al. [11]	2011	A survey of vehicular networking application requirements, use cases, architectures, protocols, challenges and solutions.
Riley et al. [12]	2011	A survey of different authentication schemes for VANETs.
Zeadally et al. [5]	2012	A survey of routing techniques, Quality of Service (QoS) and security in VANETs.
Eze et al. [13]	2014	A survey of current research status, challenges, and potentials of VANETs.
Whaiduzzaman et al. [14]	2014	A survey of vehicular cloud computing.
Mokhtar et al. [9]	2015	A survey of security features, challenges, and attacks on VANETs.
Petit et al. [15]	2015	A survey of pseudonym schemes in VANETs.
Lu and Li [16]	2016	A Survey of privacy-preserving authentication schemes.
Azees et al. [18]	2016	A survey of security services in VANETs.
Sakizet al. [24]	2017	A survey of attacks and detection mechanism in VANETs and IoV.
Manvi et al. [25]	2017	A survey of authentication schemes for VANETs.
Bernardini et al. [19]	2017	A survey of security and privacy issues in VANETs.
Taimur et al. [23]	2017	A survey of certificate revocation techniques and protocols for VANETs.
Hasrouny et al. [26]	2017	A survey of security challenges and solutions for VANETs.
Ferrag et al. [27]	2017	Survey on privacy
Asuquo et al. [28]	2018	A survey of privacy-enhancing schemes and cryptography approaches for LBS in VANETs and mobile communication.
Lu et al. [30]	2019	A survey on authentication and location privacy protection mechanisms based on pseudonyms

Azees et al. [18] provide a detailed overview of security threats, solutions and related works on availability, confidentiality, authentication, data integrity and non-repudiation in VANETs. They also propose a new secure dual authentication and key management technique for efficient communication in VANETs. Bernardini et al. [19] discuss the security and safety requirements for modern cars, architecture and safety features of AUTomotive Open System ARchitecture (AUTOSAR) [20]. They also provide a survey of research work done in intra-vehicle communication and inter-vehicle communication, and also discuss security and privacy issues related to these communications. The Controller Area Network with Flexible Data rate (CAN-FD) [21], proposed by Gmph is considered to be suitable for intra-vehicle networking. Woo and Jo [22] propose a security architecture for CAN-FD.

Khan et al. [23] discussed a classification of different Certificate Revocation List (CRL) distribution techniques using Vehicular Public Key Infrastructure (VPKI) and metrics to evaluate them. Sakiz and Sen [24] discuss existing works on threats and prevention mechanisms; most of the solutions discussed are for OBU-based communications which means that they do not need any dedicated infrastructure such as RSUs. They also point out that Sybil attack is widely addressed by researchers while other types of attacks are not very much addressed. Manvi and Tangade [25] focus on different authentication mechanisms presented in the literature and discuss their pros and cons. Hasrouny et al. [26] present a survey of VANETs security characteristics, architecture, protocols, challenges and solutions. They also present a comparative study of some of the existing security solutions. Ferrag et al. [27] present a critical survey of privacy-preserving protocols presented in the literature for mobile social networks and vehicular social networks. They survey the research works on location privacy, anonymity, and content-oriented privacy. Asuquo et al. [28] outline different security and privacy requirements, attacks and adversary models in Location Based Services (LBS) along with various metrics for evaluating location privacy in VANETs. They also discuss different privacy enhancing approaches presented in recent research works on ensuring location privacy in both VANETs and mobile networks. Boulouache et al. [29] discuss various pseudonym changing strategies presented in the literature and compare the strength and weaknesses of these pseudonym changing strategies. Lu et al. [30] presented a survey focusing on authentication schemes and location privacy protection mechanisms based on pseudonyms. They

also present a survey of various trust management models and also give an update on the latest mobility and network simulators. None of the above surveys has presented a comprehensive survey of articles published in the last ten years addressing privacy, authentication and secure message dissemination in VANETs. In this paper, we try to fill this gap. Table 1 summarizes the areas surveyed by the survey papers that we discussed above.

3. Privacy, conditional privacy, authentication and secure message dissemination in VANETs

In this section, we group the protocols addressing Privacy, Authentication and Secure Message Dissemination in VANETs into different classes and discuss the benefits and drawbacks of the protocols in each class. As we mentioned earlier, it is not possible to provide a strict classification of the protocols because some protocols may fall into two or more different classes. This is only a broad classification.

3.1. Secure content distribution and advertisement dissemination in VANETs

RSUs can offer various services such as Internet access, real time traffic data access, maps, and media files download and software updates download through high speed networks. Vehicle's can make use of these services by connecting to the RSUs through VANET. Many of the research works on this type of service-oriented vehicular communication did not take data security and location privacy of the users into consideration. Recently, advertisements of commercial products to vehicles has been identified as a promising application for VANETs. But dissemination of advertisements can be ineffective and insecure in the presence of non-cooperative selfish vehicles and malicious vehicles. In this subsection, we discuss the protocols designed for secure content distribution/downloading and advertisement dissemination in VANETs.

Huang et al. [31] propose an Anonymous Batch Authentication and Key Agreement (ABAKA) scheme to facilitate the deployment of value-added services in VANETs. To support value-added services provided by Service Providers (SPs), communication between vehicles and SPs should be secure and the message authentication process should be efficient. ABAKA addresses this issue and allows multiple vehicles to be authenticated in batches, rather

Table 2

Summary of the protocols for secure content distribution.

Paper	Year published	Focus area(s) of the paper	Method(s) used	Strengths and Weaknesses
Huang et al. [31]	2011	Authentication and secure content distribution	Generates pseudonyms similar to Lu et al. [32]; ECC.	Pseudonymous batched authentication; ensures secure communication between vehicles and service providers.
Lee et al. [34,35]	2012	Secure incentive-based dissemination of commercial ads	PKI and Signature-Seeking Drive (SSD) framework	Prevents dissemination of false or dummy ads; incentives may result in overspending.
Silva et al. [36]	2016	Secure content distribution in VANETs	Trajectory aware content distribution.	Satisfies more users' interest faster than typical CCNs [37,38].

than one vehicle at a time. It allows the creation of pseudonyms and the respective private keys for each vehicle to ensure conditional privacy. Similar to the approach taken by Lu et al. [32], the Tamper-Proof Device (TPD) can generate private keys based on Elliptic Curve Cryptography (ECC) and the associated pseudonyms and store them. Requiring every vehicle to have a tamper-proof device installed may limit the participation of vehicles in VANET. Moreover, TPDs manufactured may be able to resist known attacks, but not necessarily all future attacks; TPDs could also be susceptible to side-channel attacks mentioned in [33].

Lee et al. [34,35] propose a Signature-Seeking Drive (SSD) which makes the dissemination of advertisements (ads) secure but also suggest providing incentives in the form of virtual cash to motivate non-cooperative vehicles to participate in ad dissemination. Many of the existing incentive schemes rely on tamper-proof hardware, but this scheme leverages on the public key infrastructure to provide incentives securely for cooperating nodes in both single level and multilevel transactions. In this scheme, the Vehicular Authority (VA) is in charge of advertisement authorization and maintenance. The VA also maintains the records of all the transactions. After a vehicle receives an advertisement, it verifies the authenticity of the received ad and sends back its signed receipt to the sender of the ad. Thus, this scheme prevents the dissemination of false or dummy ads. However, when the number of co-operating vehicles increases, this may result in overspending on incentives and hence this approach may not be profitable to advertisers.

The Trajectory-aware Content distribution strategy (TraC), proposed by Silva et al. [36], uses Content-Centric Networks (CCN) [37, 38] to build persistent proactive caches in RSUs. TraC is based on users' trajectory to increase the probability of content delivery, which was not previously taken into account in the CCN based research works in VANET scenarios. In this scheme, RSUs can proactively download the content requested from the Internet even before the arrival of a vehicle within the zone of an RSU. Thus the vehicle does not need to wait for the content to be downloaded when it arrives in the zone of an RSU. Triangular Area Forwarding (TAF) and Distance Minimization Forwarding (DMF) techniques, and a neighborhood discovery protocol are used to forward interest of vehicles to RSUs. The performance of TraC with respect to the content delivery ratio, and how fast content and interests are satisfied is evaluated in the urban, highway and a realistic rush-hour (using Cologne dataset [39]) scenario. Their evaluation shows that TraC satisfies more users' interests and faster compared to typical CCNs in general, and satisfies 50% more interests in the urban scenario.

Ramakrishnan et al. [40] present a cluster-based algorithm for broadcasting emergency messages in VANETs. They first form clusters and the cluster-heads are responsible for intra-cluster management. They also use MAC layer broadcast protocols for increasing the reliability of emergency message dissemination. Nkenyereye et al. [41] present a vehicular cloud based traffic data dissemination protocol. He et al. [42] present a dropbox based approach for disseminating messages in VANETs. The dropbox based approach can cause delay in message dissemination and hence the receiver may

not be able to get the messages on time. To address this problem, the authors first present a theoretical framework for estimating the delay; then they present a dropbox deployment algorithm. They use dimension enlargement and dynamic programming to design dropbox deployment algorithm.

Table 2 presents a summary of the protocols discussed in this section.

3.2. Protocols that use ID-based signatures and group signatures for authentication of messages

Generally, the Trusted Authority (TA) is responsible for issuing security parameters, such as keys, certificates and pseudonyms to vehicles. When the TA detects (or is informed by an RSU) a malicious vehicle, it revokes the vehicle's certificates (generally, one certificate for each pseudonym) and informs all other vehicles about it. This is a centralized approach which does not scale well. Moreover, as the CRL grows, the message authentication overhead increases. In this subsection, we discuss some solutions proposed for solving these problems using ID-based signatures and ID-based cryptography [43–45].

Jiang et al. [46] design a signature scheme and a signature verification scheme that helps the RSUs in verifying the signatures of the messages including beacon messages sent by vehicles within their transmission range fast and also identify bogus messages. This requires dense deployment of RSUs. Their scheme is based on Hess's signature scheme [47] and ID-based encryption based on Weil pairing [45]. Their scheme requires the signatures of the messages from all vehicles within the transmission range of an RSU to be stored in a binary authentication tree (BAT) structure to facilitate fast verification of signatures. Under this scheme, the RSU can quickly distinguish the bogus messages from the authentic ones. Therefore, this scheme can tolerate, to a large extent, message flooding attacks. The TA is responsible for generating the keys and the associated pseudonyms and distributing them to the respective vehicles and the RSUs. The TA is also responsible for identifying the real id of malicious vehicles (RSU or law enforcement agencies can report pseudonyms vehicles suspected to be malicious to the TA) based on their pseudonym.

Zhang et al. [48] introduced an on-the-fly group creation approach in which the RSUs create and maintain groups. This allows vehicles to join the group maintained by the nearby RSU and also anonymously broadcast authenticated messages to vehicles within its group. However, authenticated message dissemination among vehicles in different groups is not addressed. Their approach is conditional privacy-preserving and it assumes RSUs are densely deployed and trustworthy.

Xie et al. [49] develop a Privacy-Aware Monitoring System (PAMS) that acts as an aggregate query processor to protect the location privacy of vehicles by making the IDs of cars anonymous. The system aggregates vehicle IDs into partial IDs. The key idea is based on k-anonymity [50] in which every record released shares identifying information with at least k-1 other individuals. Zhang et al. [51] propose an ID-based Batch Verification (IBV) scheme.

Batch verification allows verification of signatures received in a time window faster compared to verifying each signature one after the other. Their scheme uses improved Camenisch-Lysyanskaya (CL) signature [52] to verify a batch of signatures $\sigma_1, \sigma_2, \dots, \sigma_n$ of n messages M_1, M_2, \dots, M_n from n different vehicles V_1, V_2, \dots, V_n all at once instead of one at a time. The verification involves checking if one equation involving the parameters in the signatures is satisfied. The cost of computation involved in verifying if the equation is true is comprised of n multiplications n MapToPoint hash, $3n$ additions, and n one-way hash operations. Thus, the verification time for n signatures is a constant times n . This scheme is not resilient to DoS attacks such as Dummy Message Jamming (DMJ) attack. Moreover, Zhang et al.'s [51] scheme can not mitigate replay attack and it does not guarantee signature non-repudiation.

Lee and Lai [53] address the above drawbacks of Zhang et al.'s [51] scheme and extend Zhang et al.'s scheme by adding pseudo identity generation, message signing, and message verification techniques. However, the performance of this approach may degrade when the number of invalid signatures increases. Bayat et al. [54] analyze the authentication scheme for VANETs introduced by Lee et al. [53] and show how that scheme is vulnerable to the impersonation attack so that a malicious user can generate a valid signature on behalf of the other vehicles. Based on this observation, Bayat et al. [54] proposed an improved scheme which addresses this drawback of Lee et al.'s [53] scheme.

In the decentralized group authentication protocol presented by Zhang et al. [55], RSUs are responsible for maintaining and managing the group of vehicles within its transmission range for supporting secure communication between them. The basic idea behind their scheme is as follows: the central TA uses bilinear pairing for generating keys and issuing certificates to vehicles and RSUs. The TA also maintains the CRL. A Tracing Manager (TM) is responsible for tracing malicious vehicles. When a vehicle passes a nearby RSU, it uses signcryption [56] to send an encrypted request to the RSU for a group key. After receiving the group key, it uses the group signature scheme [57] to sign and send messages to members in its group. However, authenticated message dissemination between vehicles in different groups is not addressed.

For linking a message, signed using group key, to the originator of the message in the group, cryptographic technique such as message-linkable group signature (MLGS) [58] is used. Wu et al. [59] also propose a message-linkable group signature approach for thwarting Sybil attacks in VANETs. The priori and posteriori countermeasures used for authenticating messages are based on adaptive threshold authentication (in which a vehicle trusts a message only if the number of anonymous vehicles endorsing the message is greater than or equal to the predetermined threshold) which helps in speeding up verification and validation of a large number of messages in a single batch without compromising security. Xiong et al. [60] propose a scheme for managing communication among a group of vehicles effectively and spontaneously. Their scheme is based on revokable ring signatures proposed by Liu et al. [61]. This scheme allows only valid ring members to generate a ring signature for a message. In addition, trusted authorities are responsible for tracing and revoking the real signer. However, message verification overhead increases when the number of vehicles in the group grows.

Lo et al. [62] use ID-based signature and Elliptic Curve Cryptography in their conditional privacy-preserving authentication scheme for communication between vehicles and RSUs. Their scheme supports batch verification to improve throughput. They show that their scheme has better performance compared to some of the existing pseudonym-based authentication schemes. Biswas et al. [63] present a scheme for authenticating safety messages broadcasted by RSUs. Their scheme is also based on ID-based signatures [43,44] and uses proxy signatures based on Elliptic Curve

Digital Signature Algorithm (ECDSA), the digital signature algorithm specified in IEEE 1609.2 standard [64] for message authentication. They compare the overhead incurred by their algorithm in signing and verification with that of a few other existing algorithms. Among the five algorithms compared, their algorithm is the only one which uses both ID-based and proxy-based signature schemes and yields comparable performance.

Chim et al. [65] propose a software based Secure and Privacy Enhancing Communication Scheme (SPECS) which relies on ID-Based Cryptography (IBC) with bilinear pairing. In this scheme, after an initial handshaking with the nearby RSU, vehicles belonging to the same group can communicate securely without the aid of the RSU. They make use of two Bloom filters [75], namely, positive and negative filters to reduce the message overhead and false positives during message authentication. Positive filter stores the authentic vehicle's hash value of pseudonym and messages, and the negative filter stores the hash value of pseudonym and messages of vehicles that have not been authenticated. It has low communication overhead and it also has an effective batch verification success rate. However, it can be vulnerable to impersonation attack.

Hsiao et al. [66] present two broadcast authentication schemes (FastAuth and SelAuth) to deal with the signature flooding problem (i.e., reduce the computation overhead involved in verifying a large number of signatures in a short amount of time). The FastAuth protocol is based on chained Huffman hash trees (a data structure designed by them) for securing periodic single-hop beacon messages. This scheme supports a one-time signature scheme whose signature verification is claimed to be 50 times faster and signature generation is claimed to be 20 times faster than using Elliptic Curve Digital Signature Algorithm (ECDSA), the Digital Signature Algorithm specified in IEEE 1609.2 standard [64] for authentication. The other protocol, namely, the SelAuth protocol, helps in isolating malicious nodes faster by selecting messages that need to be verified before forwarding. They use a selection algorithm to distinguish benign neighbors from malicious neighbors which helps in restricting the spread of messages with invalid signatures to a small area. They also show that SelAuth incurs 10% - 35% additional computational overhead compared to other closely related schemes while containing 99% of invalid signatures to one hop. They only focus on broadcast authentication and not point-to-point message authentication.

Wasef and Shen [72,73] try to reduce the time involved in checking the CRLs during message authentication; they use the keyed Hash Message Authentication Code (HMAC), wherein the key used to calculate the HMAC is shared only between non-revoked OBUs. However, vehicles must still verify the validity of certificate and signature because it still uses a TA for generating and distributing secret keys and certificates to all OBUs. Certificate revocation is triggered by the TA which involves revoking the current secret key and securely distributing a new secret key to all non-revoked OBUs.

The dual authentication and key management technique presented by Vijayakumar et al. [67] is based on Chinese Remainder Theorem (CRT) where both hash code and fingerprints of each participating vehicle are used for dual authentication. In their approach, the TA divides the users into two groups, namely Primary and Secondary, and then generates two different group keys for these two different groups of users. It provides service to vehicles' users on the basis of a Service Level Agreement (SLA). The shared group keys are refreshed when a new user joins the group or an existing group member leaves the group, thus making this scheme resistant to forward secrecy and backward secrecy attack. It is shown that this scheme is computationally more efficient compared to some of the other existing schemes, such as Chinese Remainder Group Key (CRGK) [76] and Key-tree Chinese Remain-

Table 3

Brief summary of the protocols that use ID-based signatures and/or group signatures for authentication of messages.

Paper	Year published	Focus area(s) of the paper	Method(s) used	Strengths and weaknesses
Jiang et al. [46]	2009	Privacy, security and authentication	Hess's signature scheme [47] and ID-based encryption based on Weil pairing [45]	Bogus message identification; batch verification; constructing Binary tree for storing signatures in dynamic environment; requires dense deployment of RSUs because authentication of messages is done by RSUs.
Xie et al. [49]	2010	Privacy aware traffic monitoring	PKI and Euler Histograms (EHs)	Can process a large number of queries effectively and accurately. Many IDs need to be managed.
Zhang et al. [51]	2011	ID-based batch verification	Improved Camenisch-Lysyanskaya (CL) signature [52]	Reduces message loss ratio and communication overhead; not resistant to DoS attack.
Bayat et al. [54]	2015	Privacy, security and authentication	ECC	Addresses a drawback of the protocol presented in [53] and presents a solution.
Lee and Lai [53]	2013	Efficient verification of messages	Bilinear pairing and batch verification with group testing	Can resist replay attack and non-repudiation attack; may not be able to detect illegal signatures.
Zhang et al. [55]	2010	Authentication, privacy, traceability and confidentiality	Bilinear pairing, group signature [57] and signcryption [56]	RSUs are responsible for maintaining groups, so decentralized in some sense; no scalable mechanism to support broadcast throughout the network; group-signatures generally have high signature verification and revocation costs.
Wu et al. [59]	2010	Security, privacy and trust in V2V communication	Bilinear pairing, Message Linkable Group Signature (MLGS) and batch-verification	Accelerates verification of messages; difficult to manage revocation process.
Xiong et al. [60]	2010	Secure V2V communication	Bilinear pairing and Revocable ring signatures [61]	Does not require ubiquitous deployment of RSUs; message verification cost may increase as the number of vehicles grows.
Lo et al. [62]	2011	Authentication, security and privacy	ID-based signature and ECDSA	Supports batch verification.
Biswas et al. [63]	2011	Authentication	ID and Proxy-based signature scheme	Has lower overhead compared to some compared algorithms; addresses only authentication of RSU messages.
Chim et al. [65]	2011	Authentication, security and privacy	Identity Based Cryptography (IBC) with bilinear pairing	Low overhead and authenticates messages effectively; can be vulnerable to impersonation attack.
Hsiao et al. [66]	2011	Broadcast authentication	Chained Huffman hash trees (based on Merkle hash tree and Huffman tree)	More efficient than ECDSA specified in IEEE 1609.2 standard; the protocol for authenticating beacons will not work correctly if beacons are missed.

der Theorem (KCRT) [77]. However, they do not address the privacy of users in their work.

Zhang et al. [70] present a conditional privacy-preserving authentication protocol based on ID-based aggregate signatures and bilinear pairing based cryptography. Their approach allows hierarchical aggregation of signatures and batch verification. Their hierarchical aggregation technique allows re-aggregation which reduces transmission and storage overhead. Moreover, it has lower waiting time for aggregation compared to some of the other approaches presented in the literature.

Shao et al. [68] use group signatures and threshold authentication (in which a 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 revealed. The location of vehicles can be traced by RSUs in this approach. The privacy-preserving authentication protocol presented by Zhang et al. [69] uses multiple trusted authorities (i.e., a central trusted authority and RSUs which are assumed to be trusted as well) and ID-based aggregate signatures. The same authors also present two other protocols for message authentication based on aggregated signatures [70,78]. However, they do not compare the performance of this protocol [69] with these two other protocols [70,78].

Lai et al. [71] discuss the security challenges, requirements and benefits of group communication in Software Defined Network (SDN) based 5G-VANETs. They propose a Secure Group Mobility management Framework (SGMF) for group-oriented vehicular communication based on modified IPsec packet and an addressing

method described in [79]. Their scheme performs better compared to some of the existing mobility management schemes with respect to hand over signaling overhead and latency. However, the hand over signaling cost may increase as the density and mobility of vehicles increase.

Cui et al. [74] propose a Secure Privacy-preserving Authentication scheme using Cuckoo Filter (SPACF). Their goal is to achieve higher success rate than some of the previously proposed schemes in the batch verification phase. Cuckoo filter and binary search are used to accomplish their goal. SPACF is shown to be more efficient than some of the previous schemes because it is pairing free and does not use map-to-point hash functions. However, this ID-based scheme still suffers from inherent key escrow problem despite eliminating much of the limitations of Public Key Infrastructure (PKI) and ID-based Batch Verification (IBV).

Table 3 and 4 summarize the strengths and weaknesses of the protocols discussed in this section.

3.3. Protocols that use RSUs for authentication and/or key distribution

Some protocols presented in the literature, offload some work (such as message authentication, packet forwarding) from vehicles to RSUs and/or some work (such as key management and CRL distribution, detecting and reporting suspicious vehicles) from TA to RSUs. In this subsection we discuss protocols belonging to this category.

The RSU-aided message authentication scheme, called RAISE, proposed by Zhang et al. [80] offloads the overhead involved in message authentication to RSUs. This requires dense deployment of RSUs. Vehicles establish a shared key with the RSU using Diffie-

Table 4

Brief summary of the protocols that use ID-based signatures and/or group signatures for authentication of messages continued.

Vijayakumar et al. [67]	2016	Secure data transmission in VANETs	Vehicular Public Key Infrastructure (VPKI) and dual authentication and key management techniques	Provides resistance against forward secrecy and backward secrecy attacks; takes single broadcast message to get the updated group key; does not address location privacy.
Shao et al. [68]	2016	Privacy, security, and authentication	Bilinear pairing; group signatures; threshold based authentication	Facilitates revocation, unforgeability, anonymity, and traceability; overhead due to the use of bilinear pairing; group-signatures generally have higher signature verification and revocation costs; since RSUs serve as group managers if RSUs are compromised, the group keys could be revealed. The location of the vehicles can be tracked by RSUs in this approach.
Zhang et al. [69]	2017	Privacy, security, and authentication	Bilinear pairing based cryptography; multiple trusted authorities; ID-based aggregate signature technique for authentication	Certificate distribution is not centralized; Bilinear pairing based cryptography generally has high computational overhead.
Zhang et al. [70]	2016	Privacy, security and authentication	ID-based aggregate signatures; hierarchical aggregation of signatures and bilinear pairing based cryptography	Signature aggregation and re-aggregation helps in reducing transmission and storage overhead; waiting time needed for aggregation is also reduced compared to some other protocols; bilinear pairing based cryptography has high computation overhead.
Lai et al. [71]	2017	Secure group communication in SDN based 5G-VANETs	PKI; secure group management and group handover	Provides better group hand over authentication in terms of hand over signaling overhead and latency; cost may increase with increase in density and mobility of vehicles.
Wasef and Shen [72,73]	2009	Fast message authentication	Bilinear pairing	Claims to make the CRL checking process faster; High overheads involved in distributing a secret key to all non-revoked OBUs.
Cui et al. [74]	2017	Privacy, security and Authentication	Cuckoo filter and binary search methods	It is pairing free and does not use map-to-point hash functions; suffers from inherent key escrow problem.

Hellman algorithm. They also take the k-anonymity [50] approach to prevent an adversary from associating a message with a particular vehicle to ensure the privacy of the vehicles.

The message authentication scheme proposed by Zhang et al. [81] is an extension of the scheme presented in [80]; this extension includes a method for vehicles to cooperatively authenticate messages in the absence of an RSU. Hao et al. [82,141] present a distributed key management framework and also a method for cooperative message authentication for speeding up message authentication. Sun et al. [83] also present a group signature and identity-based signature scheme for secure and authenticated message dissemination. Papadimitratos et al. [84] also present a distributed method for distributing CRLs using RSUs to reduce the overhead involved in CRL distribution.

Lu et al. [85] propose a Social-based Privacy-preserving packet forwarding (SPRING) protocol which prevents packet analysis attack, packet tracing attack, black hole attack and grey hole attack in vehicular Delay Tolerant Networks (DTNs). This protocol relies on placing RSUs at high social intersections and using group signatures to prevent the disclosure of identity of senders, target vehicles and relaying vehicles. The RSUs help in forwarding packets between vehicles which helps in reducing packet loss.

Shim's [86] Conditional Privacy-preserving Authentication Scheme (CPAS), is a secure conditional privacy-preserving scheme for V2I communications. It uses bilinear pairing based cryptography to generate and store key parameters and ID-based signatures for authentication. Their scheme requires RSUs to verify messages sent by vehicles in batches to speed up the message authentication process. They do not address V2V communications.

The Logical Key Hierarchy (LKH) based schemes [87–89] and Topology Matching Key Management (TMKM) based schemes [90–92] for Group Key Management (GKM) wherein all the key management functionalities are handled by the Key Distribution Center (KDC) have re-keying overhead. Park et al. [93] address this problem and propose a Group Key Management (GKM) scheme, called RSU-based Decentralized Key Management (RDKM). RDKM is based on versaKey framework [94] for secure vehicular multicast commu-

nication. In this scheme, part of the GKM functions are offloaded to RSUs in a distributed manner. For efficient operation of this protocol, the authors suggest placing RSUs at the intersection of streets. For forming groups, the authors suggest placing vehicles within the region of an RSU in the same group. This helps an RSU manage the group keys efficiently. Their performance evaluation shows that this approach results in approximately 60% to 80% reduction in communication overhead compared to some of the existing GKM-based schemes. They also propose a new performance measure namely, Group Key Management Overhead (GKMO), and observe a rapid increase in GKMO for both LKH and TMKM schemes compared to the RDKM scheme. However, RDKM requires more storage space to store information about keys at each vehicle compared to the LKH and TMKM schemes.

In a Sybil attack, a malicious node can use multiple identities and inject false messages into the network. Zhou et al. [98] propose a protocol, called Privacy Preserving Detection of Abuses of Pseudonyms (P^2 DAP), to detect Sybil attacks. In their scheme, the Department of Motor Vehicles is used as the TA to provide a pool of pseudonyms to each vehicle and releases part of its workload to RSUs as follows. Two-level hashing of every pseudonym is generated where the key of the first-level hash is known to the RSUs to identify whether the pseudonyms belong to the same group of vehicles. The second-level hash key is known only to the TA to map each pseudonym to an individual vehicle. Each time an RSU finds suspicious pseudonyms, it reports this incident to the TA for verification. But the generation and management of a large number of pseudonyms can be costly.

The authentication and key establishment scheme for V2V and V2I communications, presented by Li et al. [95], is also based on ID-based public-key cryptography, blind signatures [100,101], and one-way hash chain. The blind signature scheme used in their scheme allows vehicles to communicate with the RSUs to access the services provided by them without revealing their real identities, location, and so on. They use TA for populating the OBUs with the necessary secret key, group key and pseudo id offline or

Table 5

Summary of the protocols that use RSUs for authentication and/or key distribution.

Paper	Year published	Focus area(s) of the paper	Method(s) used	Strengths and weaknesses
Li et al. [95]	2008	Location privacy and authentication	ID-based public-key cryptography, blind signature, and one-way hash chain	Solves location privacy, anonymity problem; uses a central trusted third party, which is not scalable.
Zhang et al. [80,81]	2008	Privacy, security and authentication	RSU-aided message authentication, cooperative message authentication, Diffie-Hellman algorithm and k-anonymity	Offloads the overhead involved in message authentication to RSUs; low communication overhead. Diffie-Hellman protocol is prone to man-in-the middle attack; vehicles still need to be pre-loaded with public keys; widespread deployment of RSUs is necessary.
Lin et al. [96]	2008	Privacy, security and authentication	Uses TA to get (public, private) keys; TESLA [97] hash chains for message authentication	Aims to reduce the overhead involved in certificate generation and distribution.
Lu et al. [85]	2010	Secure packet forwarding in vehicular DTNs and privacy	RSU assisted packet forwarding; Bilinear pairing	Provides high packet delivery ratio, preserves conditional privacy and resists packet tracing attack, packet analysis attack, and black (grey) hole attacks; ignores mobility of vehicles and fluctuations in traffic.
Park et al. [93]	2011	Distributed key management	PKI and RSU-based key management	Reduces re-keying overhead; can have high storage overhead to store a large number of keys.
Zhou et al. [98]	2011	Privacy and security; Sybil Attack Detection	Distributed passive overhearing by RSUs; PKI based pseudonym assignment	Detects Sybil attacks with low overhead and delay.
Shim's [86]	2012	Privacy and authenticated V2I communication	ID-based cryptography; bilinear pairing based cryptography for key generation	Fast batch verification of messages at the RSUs; vehicles need to be equipped with Tamper-Proof Devices (TPDs); TPDs could be susceptible to side-channel attacks.
Bao et al. [99]	2017	Privacy, security and authentication	TESLA protocol [97]; Bloom Filters [75]	Uses a new certificate revocation mechanism.

through a secure secret channel. The methods used are not simple and moreover using a centralized TA is not scalable.

The secure privacy-preserving protocol presented by Lin et al. [96] aims to reduce the overhead related to signing and verifying packets based on public key cryptography. They propose attaching a short message authentication code tag with each packet instead of a signature. As in the TESLA protocol [97], each vehicle generates a hash chain h_1, h_2, \dots, h_n from a random seed S ; here, $h_n = S$, and $h_i = H^{j-i}(h_j)$ for $i < j$, where H is a hash function. Each element in the hash chain is used as key to generate MAC codes for several packets and the keys are released after a short delay δ (as in [97]) for the receiver to authenticate the packet.

The privacy-preserving authentication scheme presented by Bao et al. [99] uses TESLA protocol [97] and Bloom Filters [75]. This protocol complements the work of Lyu et al. [102] in the following aspects: (i) To preserve privacy, the RSUs assign timestamp based pseudonyms to vehicles within each group which is determined based on speed, direction and other factors; (ii) In contrast to TESLA, public key rebroadcasting for new vehicles is done using Bloom Filters; (iii) The certificate revocation mechanism used to detect malicious vehicles differs from the one used in [102]. Table 5 summarizes the strengths and weaknesses of the protocols discussed in this section.

3.4. Protocols using bilinear pairing based cryptography

Lin et al. [103] present a conditional privacy-preserving PKI-based authentication protocol that uses ID-based signatures and bilinear pairing based cryptography. They use the short group signature scheme, introduced by Boneh et al. [108], for signing messages. It requires each vehicle store the certificates of all neighboring vehicles. In this approach, the signature verification involves $3 \times n$ bilinear pairing operations where n is the number of entries in the CRL. Moreover, if the group leader is malicious and reveals the key, the entire group will be compromised.

The conditional privacy-preserving protocol using bilinear pairing based cryptography, presented by Lu et al. [32], aims to address

the overhead related to preloading the OBUs with large number of pseudonyms to preserve anonymity and the overhead due to certificate distribution/verification and revocation. To achieve this, each OBU issues a request for a short-time anonymous key certificate from the nearby RSU and also checks with the RSU for the latest CRL. Using the certificate, the OBU generates pseudonyms and uses it for communicating anonymously. This would require RSUs to be deployed densely. Also, creating pseudonyms can cause delay and the certificate revocation scheme is not clear.

The Aggregate Privacy Preserving Authentication (APPA) protocol presented by Zhang et al. [78] also uses a TA to issue the initial bilinear pairing based security parameters and keys to vehicles. This scheme facilitates aggregating and authenticating messages in groups. Zhang et al. [105] propose a conditional privacy-preserving authentication protocol based on self-certified public key encryption [106], and bilinear pairing. Their aim is to reduce the overhead involved in generation and distribution of pseudonyms and the related certificates. Their approach requires the installation of a tamper-proof device in each vehicle. Every vehicle that participates in VANET needs to have a tamper-proof device installed, which may limit the participation of vehicles in VANETs.

Huang et al.'s [104] scheme, like many others, uses a TA (usually the Department of Motor Vehicles (DMV)) to issue the initial security parameters and keys to vehicles, based on bilinear pairing. The TA also issues a token that uniquely and anonymously identifies the vehicle. Then, the vehicle uses this token to authenticate itself to the nearby RSU to get pseudonym token. This pseudonym token contains only the credentials for the vehicle to generate pseudonyms. The vehicle then uses this token to generate its own pseudonyms. After generating pseudonyms, the vehicles use ID-based encryption [45] for exchanging messages securely with other vehicles. RSUs cannot revoke the certificate of malicious vehicles because they do not have private information (such as ID) of the vehicles. The TA is responsible for revoking the certificate of malicious vehicles. A vehicle can send a report about malicious vehicles to nearby RSU and the RSU will send that report to the TA, based on which the TA can revoke the certificate of the vehicle.

Table 6
Summary of protocols using bilinear pairing based cryptography.

Paper	Year published	Focus area(s) of the paper	Method(s) used	Strengths and weaknesses
Lin et al. [103]	2007	Privacy, security and authentication	PKI-based authentication; Group signatures	OBUs have to save all the third party certificates from the neighboring vehicles which has associated overheads; if the group leader is malicious and reveals the key, the entire group is compromised; cannot efficiently deal with compromised vehicles; group-signatures generally have high signature verification and revocation costs.
Lu et al. [32]	2008	Privacy, security and authentication	Bilinear pairing based cryptography, RSU generated pseudonyms	Resolves RSU compromise attack; addresses the overhead related to pre-loading the OBUs with a large number of pseudonyms and certificates; latency that arises from generation of pseudonym keys by the RSUs; frequent interactions with the RSUs are required; requires dense deployment of RSUs; no clear revocation scheme.
Huang et al. [104]	2011	Authentication, security and privacy	Bilinear pairing, ID-based encryption [45]	Can handle message replay/modification attacks, impersonation attacks and deal with compromised RSUs; the use of ECC has associated overhead.
Zhang et al. [105]	2013	Privacy, security and authentication	Self-certified public keys [106] and bilinear pairing	Proved to be conditional privacy-preserving under random oracle model.
Azees et al. [107]	2017	Privacy, security and authentication	Bilinear pairing based cryptography	The authors claim that their scheme for verification of certificates and signatures is faster and more efficient than some of the schemes proposed in the literature.

The protocol proposed by Azees et al. [107] is based on bilinear pairing based cryptography; the authors claim that it can track malicious/compromised vehicles and RSUs. Although bilinear pairing based cryptography generally has high computation overhead, their performance analysis shows that their approach performs better than seven other protocols with respect to certificate and signature verification costs. The TA generates pseudonyms (the authors call them dummy ids) for vehicles and RSUs for preserving anonymity. Distributing CRLs to vehicles and RSUs is still the responsibility of the TA. Given the large number of pseudonyms and the associated certificates allocated to the vehicles, overheads associated with distributing CRLs as well as verifying the authenticity of messages using CRLs could be high. However, the authors do not discuss this overhead.

Table 6 summarizes the strengths and weaknesses of the protocols discussed in this section.

3.5. Protocols that can cope with compromised RSUs and vehicles

Jung et al. [109] propose a conditional privacy-preserving authentication protocol. They claim it is better than the one presented by Lu et al. [32], because it is robust against compromised RSUs. They use a TA (called membership manager) to assign Message Authentication Code (MAC) keys to OBUs and a group signing key to each RSU. The RSUs generate anonymous certificates for vehicles within its region. The TA stores the MAC keys and the IDs of the vehicles for tracing vehicles in case of disputes. An OBU requests the nearby RSU for anonymous certificates for a given time period; the RSU authenticates the OBU and generates multiple short-term certificates and sends them to the OBU. The OBU authenticates the RSU using CRL issued by the TA, accepts the certificates issued by the RSU, and uses them for sending authenticated messages. In contrast to many other protocols in the literature, the conditional privacy-preserving authentication protocol presented by Wang et al. [110] uses decentralized certificate authorities and two factor authentication for ensuring privacy and non-repudiation. This ensures a vehicle's privacy even if all RSUs are compromised; this protocol also incurs low computation and communication overheads compared with some of the existing protocols.

The primary goal of the pseudonymous authentication scheme with strong privacy preservation (PASS) presented by Sun et al. [111] is to keep the length of the CRL linear in terms of the number of vehicles revoked, not in terms of the number of pseudonyms assigned as in many other protocols. To accomplish this, they use hash chain based two-layered pseudonym generation method. This scheme uses a decentralized approach based on proxy re-signatures for updating the certificates of vehicles using RSUs and not the TA. This scheme can also handle compromised RSUs. Raya et al. [112] present a distributed solution for identifying and evicting misbehaving or faulty nodes in VANETs. Sedjelmaci et al. [113] also propose an intrusion detection scheme based on game theory to detect as well as predict the vehicles that are likely to misbehave in the future. They claim that their scheme can detect false alerts and Sybil attacks. Table 7 summarizes the protocols discussed in this section.

Next, we discuss some of the protocols that assume the installation of a tamper-proof device or smart card on each vehicle to store relevant information such as keys and passwords securely.

3.6. Protocols based on smart cards and tamper-proof devices

Conventional PKI [120] based schemes require each vehicle to verify the signatures of each of the other vehicles sending messages to it; this results in computational overhead for the OBUs of the vehicles. To overcome this drawback of PKI based approach, ID-based Batch Verification (IBV) [119] scheme was proposed. Under IBV scheme, an RSU can verify the signatures of multiple messages all at once; so signature verification is more efficient under this approach. The authors use ID-based cryptography for generating private keys associated with pseudo-identities. However, the IBV [119] scheme depends on the availability of a tamper-proof hardware device on each vehicle to securely store the system-wide secret key. Since the system wide secret key is stored on tamper-proof hardware of each vehicle, if one of these devices is compromised, the whole system is compromised. Moreover, this does not ensure privacy of vehicles because real ID of a vehicle could be traced by other vehicles.

The authentication protocol presented by Ying and Nayak [117, 118] uses dynamic login IDs to preserve privacy. The user gets a smart card loaded with the vehicle's pseudonym and password.

Table 7

Summary of the protocols that can deal with compromised RSUs and/or vehicles.

Paper	Year published	Focus area(s) of the paper	Method(s) used	Strengths and weaknesses
Jung et al. [109]	2009	Privacy and authentication	Bilinear pairing, ID-based group signature scheme [108] and universal re-encryption scheme [114]	Robust against compromised RSUs; incurs involved in issuing certificates, and CRLs; group-signatures generally have high signature verification and revocation costs.
Sun et al. [111]	2010	Authentication, security and privacy	Bilinear pairing, hash chains, Schnorr signatures [115]	Ensures authentication and privacy; centralized approach, although RSUs are involved in re-keying; requires dense deployment of RSUs; the pseudonym generation method used reduces key management overhead; bilinear pairing based operations have associated overhead.
Wang et al. [110]	2016	Privacy, security and authentication	Decentralized certificate authority and two-factor authentication; bilinear pairing based cryptography	Reduced communication overhead; bilinear pairing based cryptography incurs high overhead.

Table 8

Summary of protocols that make use of smart-cards and tamper-proof devices.

Paper	Year published	Focus area(s) of the paper	Method(s) used	Strengths and weaknesses
Paruchuri and Durresi [116]	2010	Authentication, privacy, and security	Smart cards to store keys and perform encryption/decryption	Requires the use of smart cards.
Ying and Nayak [117]	2014	Privacy, security and authentication	Login ids are generated dynamically for ensuring privacy	Smart cards are used for generating login ids dynamically; it can resist password attacks, and impersonation attacks; can tolerate smart card loss; can handle compromised RSUs.
Ying and Nayak [118]	2017	Privacy, security and authentication	Diffie-Helman protocol; smart cards; hash functions; centralized trusted authority for loading smart-cards with login id and password	Can resist smart card loss attack; can also resist impersonation and password guessing attack.
[119]	2008	Authentication, batch verification	ID-based cryptography; Camenisch-Lysyanskaya (CL) signature [52]; tamper-proof device	The real ID of the vehicles could be tracked; vulnerable to impersonation attack.

Smart card inserted into the vehicle's OBU, authenticates its owner by asking for the real ID and password and generates dynamic login identity for the user and sends it to the nearby RSU. Upon receiving this message, the RSU verifies if it is valid, computes its own dynamic login id and sends its dynamic login id and the dynamic login id of the vehicle to the TA. The TA computes the anonymous keys and the corresponding certificates for the vehicle and sends them to the RSU securely. The RSU then broadcasts the keys and certificates securely to the vehicles in the region and the corresponding vehicles receive them and use them for communication. Their privacy-preserving anonymous authentication scheme not only authenticates received messages but also verifies the legitimacy of the senders of the messages (i.e., it checks if the sender is a malicious node which forged the ID of some legitimate node). In addition, to reduce the computational complexity, they do not use bilinear pairing based cryptography. It allows the user's password to be changed dynamically. So, this scheme can resist smart card loss attack, impersonation attack, and password guessing attack.

The protocol presented by Paruchuri and Durresi [116] also uses smart cards to generate anonymous keys on-the-fly for establishing secure V2V as well as V2I communication. The TA issues smart cards as well as the keys to the vehicles and certificates to RSUs. The vehicle's ID, required cryptographic keys, and driver information are stored on the smart card. To send a message to vehicles within its group, first a vehicle needs to get a session key securely from the nearby RSU. To send a message m to a vehicle within its group, it encrypts the message m and the ID of the OBU and the signature of m (hash of m encrypted with its private key V_{Pr}) encrypted with the public key $E_{RSU_{Pu}}$ of the RSU using the session key K_e as follows and sends it:

$$E_{K_e}(m, E_{RSU_{Pu}}(OBU_{ID}, E_{V_{Pr}}(H(m))))$$

A receiving vehicle can decrypt the message using the session key issued by the RSU. However, it cannot decrypt the second part because the private Key of the RSU is needed for decrypting the second part. The second part is used by the RSU to trace misbehaving nodes, when necessary. Table 8 summarizes the strengths and weaknesses of protocols discussed in this section.

Next, we discuss some of the protocols that minimize the overhead involved in using the Public Key Infrastructure (PKI) for generating and assigning keys, pseudonyms, certificates, and CRLs to vehicles and/or RSUs.

3.7. Minimizing the overhead involved in public key infrastructure (PKI) based protocols

The anonymous authentication protocol presented by Wang et al. [121] uses the TA to assign each vehicle and each RSU a long term certificate during registration. Each RSU is responsible for assigning a master key to each vehicle entering its region after authenticating the vehicle based on its long term certificate. Then the vehicle uses the master key to generate pseudonyms locally and uses them to sign messages to preserve anonymity. This approach has lower signature verification overhead compared to the protocols presented in [73] and [122]. Moreover, it supports both single and batch authentication of messages.

The Secure and Authenticated Key Management Protocol (SA-KMP) presented by Hengchuan et al. [133], combines the idea of the Public Key Regime (PKR) (which delegates the distribution of public keys to the RSUs, eliminating the need to distribute digital certificates) proposed by Shen et al. [134] and the idea of 3-D matrix key distribution scheme (which generates the keys dynamically instead of preloading the keys), proposed by Hamid et

al. [135,136]. Wasef et al. [123] propose a mechanism based on PKI which supports not only location privacy but also authentication; it also uses a distributed approach for certificate revocation. They use the Message Authentication Acceleration (MAAC) [72] protocol to make the revocation checking process faster without checking the CRLs. However, their solution can only preserve the location privacy of vehicles within its group. They also propose a method for mitigating Denial of Service (DoS) attacks.

Biswas and Misis [124], [125], [126] use proxy signatures for privacy-preserving authentication. One drawback of this solution is that it requires larger keys for generating and verifying signatures. As a result, it incurs higher computational cost compared to other competitive schemes such as Elliptic Curve Cryptosystems (ECC) to provide similar security strength.

Dong et al. [127] propose a privacy-preserving data forwarding scheme for service oriented VANETs based on Lite-TA-based public key cryptography and on-path onion encryption scheme. This scheme has lower encryption cost and public key management complexity compared to conventional public key encryption schemes. However, since this approach requires relaying nodes to encrypt the message before forwarding to prevent adversaries from tracing message flows, it incurs higher computation overhead for forwarding packets.

Haas et al. [128] propose a method for quick, organized and efficient distribution of CRLs through V2V communication [137]. This scheme ensures backward privacy of revoked vehicles prior to their revocation. They use the probabilistic data structure Bloom filters [75] for quickly checking CRLs. However, false positives may occur. But they claim that, false positives can be avoided by discarding the certificate of the vehicles that may trigger a false positive. The use of Bloom filters reduces the overhead incurred for checking CRLs. It is observed that the distribution of CRLs through V2V communication is more efficient and cost effective than the RSU-based distribution scheme because it does not require widespread deployment of RSUs.

Many of the research works based on chameleon hash signature [130] using fixed public keys for authentication do not guarantee message unlinkability. Shen et al. [129] address this problem and propose a light weight privacy-preserving protocol that relies on Elliptic Curve based chameleon hash signature and dynamic public keys. They consider the registration phase and the mutual authentication phase between OBUs and RSUs in their protocol. They also considered the TA tracking phase to ensure authenticity and traceability. Whenever any suspicious event occurs, the TA can recover the real identity of the OBU that created the event by executing the TA tracking phase. The use of chameleon hash-based signature for messages helps in preventing replay attacks and impersonation attacks. However, V2V authentication is not addressed in this protocol.

The Security Credential Management System (SCMS) proposed by Whyte et al. [131] is based on PKI; it was developed under a cooperative agreement with the United States Department of Transportation (USDOT), the leading candidate for V2V security backend design in the United States. This scheme adds some additional features such as the number of vehicles it supports and tries to achieve a tradeoff between security, privacy and efficiency of traditional PKI based approaches. Additionally, they propose (i) a frequent certificate changing (e.g., every 5 minutes) scheme to enhance protection against attackers outside of the SCMS and (ii) organizational separation of operations of SCMS to protect against attackers inside the SCMS.

Alshaer [132] proposed a secure connection model based on the Vehicular Public Key Infrastructure (VPKI) that utilizes trusted RSUs to establish secure connections and distribute secret keys to vehicles within their transmission range. The probability of the number of reachable neighboring vehicles that a Communi-

cation Enabled Vehicle (CEV) can reach has been derived using Exponential distribution of time and space headways with a Robustness Factor (EwRF). They claim that suitable statistical distribution (e.g., exponential distribution, Generalized Extreme Value (GEV) distribution) that characterizes inter-vehicle spacing can accurately contribute to secure connectivity. This approach requires the widespread deployment of RSUs and RSUs are assumed to be reliable. Table 9 summarizes the strengths and weaknesses of the protocols discussed in this section.

3.8. Message aggregation and cooperative message authentication

Multiple vehicles could observe the same phenomena on the road and try to disseminate it to other vehicles which wastes bandwidth. To address this problem, message aggregation (as has been proposed for sensor networks earlier) has been proposed. Moreover, to reduce the overhead involved in message authentication, cooperative message authentication wherein vehicles share the overhead due to message authentication, has been proposed. We discuss the protocols in these categories in this subsection.

3.8.1. Protocols using message aggregation

The Aggregated Emergency Message Authentication (AEMA) scheme proposed by Zhu et al. [138] is based on bilinear pairing. Under AEMA, each vehicle registers with the TA (they call it an Offline Security Manager (OSM)) and obtains its public key certificate. Then, when a vehicle needs to send an emergency message, it uses the following format (*Type*, *Loc*, *ID*, *Time*, *Sig*, *Cert*) to send it. Here, *Type* indicates the type of the event, *Loc* is the location where the event occurred, *ID* is the pseudo ID of the vehicle, *Time* is the time when the event occurred, *Sig* denotes the signature of the message, and *Cert* is the certificate. The receiver verifies the validity of the certificate *Cert* and the signature *Sig* and accepts the message. The authors assume that each event is uniquely determined by *Type*, *Loc*, and *Time*. Hence, an intermediate node receiving the message can eliminate duplicates and aggregate the messages. The overhead involved in computing the signature based on bilinear pairing is of some concern. In addition, the algorithm depends on the central OSM for issuing certificates. The authors assume that each observed event has a unique type. This scheme does not ensure location privacy of vehicles because each message carries the location information of vehicles.

Dietzel et al. [139] proposed selective attestation and trust fusion to detect attacks as well as mitigate their effects for semantic aggregation in VANETs. Their approach is based on a generic data aggregation model, which makes it extensible and suitable for the existing data aggregation schemes. In the trust fusion mechanism, multiple warnings of the same event are linked to alleviate the need for a Global Unique Identifier system (GUID) by using a fuzzy logic technique. However, the bandwidth needed for selective attestation could slow down the message dissemination process. Many of the existing message aggregation techniques require roads to be segmented into small fixed-size regions for aggregating messages originating from these regions. However, messages originating across regions cannot be aggregated using these approaches. Van der Heijden et al. [140] address this problem and present a scheme that allows more dynamic aggregation of messages.

Next, we discuss protocols in which vehicles cooperate to authenticate messages in order to reduce the overhead involved in message authentication.

3.8.2. Protocols that use cooperative message authentication or batch verification

Hao et al.'s [141] distributed key management and Co-operative Message Authentication Protocol (CMAP) based on short group signature [142] can detect compromised RSUs and the malicious vehi-

Table 9

Summary of the protocols that address the overhead involved in PKI based protocols.

Paper	Year published	Focus area(s) of the paper	Method(s) used	Strengths and weaknesses
Wasef et al. [123]	2010	Location privacy, authentication, and certificate revocation	PKI and Message Authentication Acceleration (MAAC) protocol	Fast revocation check process and mitigates DoS attacks; location privacy may not be ensured against outsider attacks.
Biswas and Mistic [124–126]	2010	Self authentication and anonymous message delivery	PKI, proxy signatures	Preserves message integrity and anonymity; RSU assisted proxy signatures.
Dong et al. [127]	2011	Privacy-preserving data forwarding; specifically designed for service oriented VANETs	Lite-TA-based public key cryptography; on-path onion encryption scheme	Efficient, robust and ensures higher trust level; high computational overhead.
Haas et al. [128]	2011	Distribution of CRLs	PKI and Bloom filters [75]	Does not require ubiquitous deployment of RSUs; false positives can be prevented; computational overhead is somewhat low.
Shen et al. [129]	2012	Secure communication	Chameleon hash signature [130]	Ensures unlinkability, traceability and defense against replay attack; V2V authentication is not addressed.
Whyte et al. [131]	2013	Security credential management system; V2V communication	Public Key Infrastructure	The authors try to achieve a tradeoff between privacy, security and efficiency; decentralized certificate distribution; frequent certificate changes could cause high overhead.
Alshaer [132]	2015	Securing VANETs connectivity with the support of RSUs	Vehicular Public Key Infrastructure (VPKI)	Can predict uplink and downlink connectivity probabilities in VANETs; assumes RSUs are trustworthy.
Hengchuan et al. [133]	2016	Authenticated key management	Public key regime (PKR) [134]; the 3-D matrix key distribution scheme [135,136]	This approach is more scalable than PKI based approaches; key generation takes less time compared to Elliptic Curve Diffie-Hellman and Diffie-Hellman protocols.
Wang et al. [121]	2017	Privacy, security and authentication	Does not use PKI for generating pseudonyms and the related certificates to vehicles; vehicles generate their own pseudonyms	This approach has less signature verification overhead compared to the protocols presented in [73] and [122]; it supports both single and batch authentication.

cles colluding with them. Vehicles getting keys from the same RSU form a group. To ensure reliable key distribution, messages are encrypted using Elliptic Curve Integrated Encryption Scheme (ECIES) and are transmitted using the Transmission Control Protocol (TCP). This scheme allows the cooperative verifiers to cooperatively authenticate messages. Cooperative verifiers are selected dynamically and distributively based on their own geographic locations relative to the sender of the message. However, a malicious vehicle can pretend to be a cooperative verifier by creating many Sybil nodes within its transmission range, which makes this scheme vulnerable to Sybil attack.

Most of the research work on secure incentive schemes focus only on cooperative packet forwarding; but due to the high mobility of vehicles, packets could be lost. To address this problem, Lai et al. [143] propose a Secure Incentive scheme for Reliable Cooperative downloading in highway VANETs (SIRC) that uses two phases, namely, cooperative downloading and cooperative forwarding which encourage vehicles to cooperate through an incentive scheme; SIRC utilizes aggregated Camenisch-Lysyanskaya (CL) signature [52] to cooperate with others in securely downloading-and-forwarding packets. In this scheme, a reputation system is implemented to reward the cooperating vehicles and punish the malicious vehicles. In addition, a partial prepayment strategy is used to minimize the payment risk to client vehicles. This scheme can resist various attacks such as free riding attack, DoS attacks and packet injection/removing attack. The performance evaluation of SIRC shows that it has high download success rate, low download delay, and moderate computation and communication overhead. A disadvantage of this approach is that the reputation information about vehicles which have high variability in their spatial distribution need to be calculated and stored.

Wang and Liu [144] proposed a scheme that satisfies the security requirements in Vehicular Heterogeneous Networks (VHNs)

wherein support for cooperative communication among various types of networks such as networks based on DSRC-based on IEEE 802.11p, Device to Device (D2D) communication and cellular communication needs to be provided. A mode selection algorithm that allows the OBUs to check the remaining lifetime of a packet and switch between three different modes (DSRC, D2D-V and cellular networks) is also presented. They found that sufficient power and vehicle density are the main factors for the successful transmission of messages securely in such networks.

Lin and Li [145] presented a cooperative message authentication scheme to reduce not only the overhead involved in message authentication but also the authentication delay. This scheme tries to minimize the authentication overhead on the same message by different vehicles when vehicles are allowed to cooperatively authenticate messages. To encourage vehicles to cooperate in message authentication, vehicles are issued evidence tokens. An evidence token issued to a vehicle reflects its contribution to authentication in the past; this encourages vehicles to participate in the message authentication process, which helps in distributing the authentication load among many vehicles. Evidence tokens are obtained from the TA via the RSU in its current region. It also uses a large number of pseudonyms, which could result in long CRLs. Jiang et al. [146] also propose an authentication scheme under which requests from multiple vehicles can be authenticated in batches rather than one by one. Cheon and Yi [147] proposed a method for batch verification of multiple signatures generated by different signers as well as a single signer. They showed how this technique can be applied to the modified DSA and ECDSA based signatures. They also show that their batch verification approach is seven times faster than individual verification. Wasef et al. [148,149] proposed a flexible certificate distribution scheme and an efficient way for vehicles to update their certificates. To decrease the message authentication overhead, they also proposed

Table 10

Brief summary of protocols that support message aggregation, cooperative message authentication, and/or batch verification.

Paper	Year published	Focus area(s) of the paper	Method(s) used	Strengths and weaknesses
Zhu et al. [138]	2008	Emergency message authentication	Bilinear pairing; message aggregation	Does not ensure location privacy; useful for propagation of short emergency messages only.
Dietzel et al. [139]	2010	Secure data aggregation	Generic aggregation model and Fuzzy logic methodology	Extensible and alleviates the need of a Global Unique Identifier system (GUID); bandwidth overhead could decrease dissemination speed.
Hao et al. [141]	2011	Authentication, security and privacy	Bilinear pairing; short group signatures [142]	Cooperative message authentication to speed up authentication; does not ensure location privacy of vehicles; vehicles in different regions cannot securely exchange messages; group-signatures generally have high signature verification and revocation costs; RSUs are assumed to be trustworthy; cooperative authentication would work only if the density of vehicles is high; susceptible to location modification because messages are selected for verification based on location information.
Jiang et al. [146]	2013	Privacy, security and authentication	Pseudonyms and ID-based signature, hash message authentication code	Supports batch authentication of requests; Tamper-proof devices (TPDs) are needed to store pseudonyms; TPDs could be susceptible to side-channel attacks.
Lin and Li [145]	2013	Privacy, security and authentication	Cooperative message authentication; uses large number of pseudonyms for ensuring anonymity	Due to the large number of pseudonyms issued to vehicles, CRLs could grow.
Lai et al. [143]	2017	Reliable cooperative downloading	PKI; incentive scheme based on reputation	Can resist different types of attacks including DoS attacks; can be difficult to calculate and store reputation information correctly.
Wang and Liu [144]	2018	Secure cooperative communication in heterogeneous vehicular networks	PKI, stochastic geometry theory and optimization	Flexible; allows to switch between DSRC, D2D-V and cellular networks modes; Requires OBUs with high computation power.

a method for verifying certificate-based signatures of messages in batches. Zhang and Zhang [150] developed a method for aggregating signatures in a certificate-less public key setting.

Table 10 summarizes the strengths and weaknesses of the protocols discussed in this section.

4. Recommendations and open issues for further research

For the widespread deployment of VANETs, the following important issues need to be thoroughly addressed and efficient, scalable solutions for them need to be found: (i) authentication of vehicles and messages (ii) secure message dissemination and (iii) privacy of users need to be protected.

4.1. Scalable and distributed authentication and secure message dissemination protocols

VANETs could support various safety-related applications such as safe driving, collision avoidance, timely reporting of events such as accidents to law enforcement agencies, facilitating the law enforcement agencies to reconstruct events such as accidents and speeding violations, hazard awareness and many others. Moreover, VANET users could also benefit from infotainment and software download. For implementing these facilities, scalable solutions for authentication and secure message dissemination need to be designed. Most of the solutions presented in the literature for this problem are centralized. Few attempts have been made to solve these problems using decentralized approaches. Further research is needed to address this scalability issue. Cooperative message authentication has been proposed to distribute the burden of authentication among vehicles. Such protocols could be susceptible to Sybil attacks because a malicious node can create several Sybil nodes. These protocols, in general, use location information to select messages. So, these protocols could be susceptible to location modification attacks.

4.2. Privacy of vehicles

Ensuring the privacy of vehicles is an important issue in VANETs. Otherwise, vehicle owners' life could be jeopardized. So, in all communications, a vehicle should not use its real identity. To solve this problem, several solutions have been proposed. A vast majority of the solutions proposed use pseudonyms instead of the real ids of vehicles in the communication. This requires large number of pseudonyms to be loaded into the vehicles OBUs and they need to be kept secret. Moreover, to punish malicious vehicles (i.e., vehicles disseminating malicious messages or modifying the messages sent by other vehicles), vehicles' real ids need to be traced. Thus, even though privacy needs to be preserved, authorities should still be able to trace and punish malicious vehicles. Vehicles cannot use the same pseudonym for a long time, because then, based on the path traversed by vehicles, an intruder can associate the pseudonym with the real id. Thus pseudonyms should be changed frequently. Some authors suggest changing pseudonyms every five seconds to prevent an intruder from linking two messages to the same vehicles and tracking the vehicle. So, each vehicle needs to be assigned millions of pseudonyms during its lifetime and also a scalable mechanism for tracking which vehicle has been assigned what pseudonym needs to be designed and implemented. Moreover, when a vehicle is revoked, the certificates associated with the pseudonyms of the revoked vehicle need to be disseminated to all vehicles/RSUs. This could lead to an exponential growth of CRLs which could slow down the authentication of messages. So, centralized solutions are not scalable. Some solutions proposed for handling this problem allow the distribution of the task of creating and distributing the certificates as well as CRLs to the RSUs. However, more research needs to be done in devising highly efficient, scalable privacy-preserving methods to solve this problem.

4.3. Availability of roadside infrastructures

Many of the solutions presented assume the availability of RSUs. However, we will not see widespread deployment of RSUs in the near future. So, solutions proposed in the future should also consider the scenarios in which there is no widespread deployment of RSUs. Due to advances in new technologies and a growing number of vehicles, the design of reliable and scalable VANETs architectures that support multiple technologies (e.g., DSRC, D2D-V and Cellular Networks) is also important. In such a scenario, vehicles need to authenticate with entities in different networks. This is especially challenging because vehicles in VANETs use privacy-preserving authentication and other networks do not use privacy-preserving authentication.

4.4. Metrics for evaluating protocols designed for VANETs

Some researchers have proposed metrics for evaluating protocols for authentication and security in VANETs. However, these metrics do not capture all the requirements. Metrics need to be developed and standardized; moreover, simulators and testbeds for evaluating protocols based on these metrics need to be implemented.

5. Conclusion

In this paper, we presented a survey of papers published in the last ten years that address privacy, authentication and secure message dissemination in VANETs. Based on the tools and techniques used in the papers, we classified the papers into various categories. We made a comparative study of the protocols in each category and discussed their strengths and weaknesses. Then, we discussed some of the open issues that remain to be addressed. We hope this survey will serve as ready reference for other researchers working in these areas and also help in addressing some of the open issues.

Declaration of competing interest

The authors declare that there is no conflict of interest.

Acknowledgement

We thank the editor and the reviewers for their valuable comments, which helped us greatly in improving the content and presentation of the paper.

References

- [1] H. Peng, L. Liang, X. Shen, G.Y. Li, Vehicular communications: a network layer perspective, *IEEE Trans. Veh. Technol.* (May 2018).
- [2] H. Hartenstein, L.P. Laberteaux, A tutorial survey on vehicular ad hoc networks, *IEEE Commun. Mag.* 46 (June 2008) 164–171.
- [3] P. Offor, Vehicle ad hoc network VANET: safety benefits and security challenges, 2012.
- [4] S. Al-Sultan, M.M. Al-Doorand, A.H. Al-Bayatti, H. Zedan, A comprehensive survey on vehicular ad hoc network, *J. Netw. Comput. Appl.* 37 (January 2014) 380–392.
- [5] S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, A. Hassan, Vehicular ad hoc networks (VANETs): status, results, and challenges, *Telecommun. Syst.* 50 (4) (2012) 217–241.
- [6] F.A. Teixeira, V.F. e Silva, J.L. Leoni, D.F. Macedo, J.M.S. Nogueira, Vehicular networks using the IEEE 802.11p standard: an experimental analysis, *Veh. Commun.* 1 (2) (April 2014) 91–96.
- [7] A. Studer, F. Bai, B. Bellur, A. Perrig, A flexible, extensible, and efficient VANET authentication, in: *Special Issue on Secure Wireless Networks*, *J. Commun. Netw.* 11 (6) (Dec. 2009) 574–588.
- [8] D. He, S. Zeadally, B. Xu, X. Huang, An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks, *IEEE Trans. Inf. Forensics Secur.* 10 (12) (2015) 2681–2691.
- [9] B. Mokhtar, M. Azab, Survey on security issues in vehicular ad hoc networks, *Alex. Eng. J.* 54 (2015) 1115–1126.
- [10] T. Willke, P. Tientrakool, N. Maxemchuk, A survey of inter-vehicle communication protocols and their applications, *IEEE Commun. Surv. Tutor.* 11 (2) (2009) 3–20.
- [11] G. Karagiannis, O. Altintas, E. Ekici, G. Heijenk, B. Jarupan, K. Lin, T. Weil, Vehicular networking: a survey and tutorial on requirements, architectures, challenges, standards and solutions, *IEEE Commun. Surv. Tutor.* 13 (4) (2011) 584–616.
- [12] M. Riley, K. Akkaya, K. Fong, A survey of authentication schemes for vehicular ad hoc networks, *Secur. Commun. Netw.* 4 (10) (2011) 1137–1152.
- [13] E.C. Eze, S. Zhang, E. Liu, Vehicular ad hoc networks (VANETs): current state, challenges, potentials and way forward, in: *Proceedings of 20th International Conference on Automation and Computing*, Cranfield University, Bedfordshire, UK, 2014, pp. 176–181.
- [14] M. Whaiduzzaman, M. Sookhak, A. Gani, R. Buyya, A survey on vehicular cloud computing, *J. Netw. Comput. Appl.* 40 (2014) 325–344.
- [15] J. Petit, F. Schaub, M. Feiri, F. Kargl, Pseudonym schemes in vehicular networks: a survey, *IEEE Commun. Surv. Tutor.* 17 (1) (2015) 228–255.
- [16] H. Lu, J. Li, Privacy-preserving authentication schemes for vehicular ad hoc networks: a survey, *Wirel. Commun. Mob. Comput.* 16 (6) (April 2016) 643–655.
- [17] M. Gerla, C. Wu, G. Pau, X. Zhu, Content distribution in VANETs, *Veh. Commun.* 1 (1) (January 2014) 3–12.
- [18] M. Azees, P. Vijayakumar, L. Deborah, Comprehensive survey on security services in vehicular ad-hoc networks, *IET Intell. Transp. Syst.* 10 (6) (August 2016) 379–388.
- [19] C. Bernardini, M.R. Asghar, B. Crispoc, Security and privacy in vehicular communications: challenges and opportunities, *Veh. Commun.* 10 (2017) 13–28.
- [20] AUTomotive open system ARchitecture, <https://www.autosar.org/>, 2019.
- [21] R.B. GmbH, Can with Flexible Data-Rate, Specification Version 1.0, 2012, Vector CANtech, Inc., Novi, MI, USA, 2012.
- [22] S. Woo, H.J. Jo, I.S. Kim, H.L. Dong, A practical security architecture for in-vehicle CAN-FD, *IEEE Trans. Intell. Transp. Syst.* 17 (8) (Aug. 2016) 2248–2261.
- [23] K. Taimur, A. Naveed, C. Yue, S.A. Jalal, A. Muhammad, S. ul Haq, C. Haitham, Certificate revocation in vehicular ad hoc networks techniques and protocols: a survey, *Sci. China Inf. Sci.* 60 (10) (2017).
- [24] F. Sakiz, S. Sen, A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV, *Ad Hoc Netw.* 61 (1) (June 2017) 33–50.
- [25] S.S. Manvi, S. Tangade, A survey on authentication schemes in VANETs for secured communication, *Veh. Commun.* 9 (July 2017) 19–30.
- [26] H. Hasrouny, A.E. Samhat, C. Bassil, A. Laouiti, VANET security challenges and solutions: a survey, *Veh. Commun.* 7 (2017) 7–20.
- [27] M.A. Ferrag, L. Maglaras, A. Ahmim, Privacy-preserving schemes for ad hoc social networks: a survey, *IEEE Commun. Surv. Tutor.* 19 (4) (Fourth Quarter 2017) 3015–3045.
- [28] P. Asuquo, H. Cruickshank, J. Morley, C.P.A. Ogah, A. Lei, W. Hathal, S. Bao, Z. Sun, Security and privacy in location-based services for vehicular and mobile communications: an overview, challenges and countermeasures, *IEEE Int. Things J. (Early Access)* XX (2018).
- [29] A. Boualouache, S.-M. Senouci, S. Moussaoui, A survey on pseudonym changing strategies for vehicular ad-hoc networks, *IEEE Commun. Surv. Tutor.* 20 (1) (2018) 770–790.
- [30] Z. Lu, G. Qu, Z. Liu, A survey on recent advances in vehicular network security, trust, and privacy, *IEEE Trans. Intell. Transp. Syst.* 20 (2) (Feb. 2019) 760–776.
- [31] J.L. Huang, L.Y. Yeh, H.Y. Chien, ABACA: an anonymous batch authenticated and key agreement scheme for value-added services in vehicular ad hoc networks, *IEEE Trans. Veh. Technol.* 60 (1) (Jan. 2011) 248–262.
- [32] R. Lu, X. Lin, H. Zhu, P.-H. Ho, X. Shen, ECPP: efficient conditional privacy preservation protocol for secure vehicular communications, in: *Proceedings of 27th IEEE Conference on Computer Communication (INFOCOM)*, 2008, IEEE, 2008, pp. 1229–1237.
- [33] F.-X. Standaert, T. Malkin, M. Yung, A Unified Framework for the Analysis of Side-Channel Key Recovery Attacks, *Lecture Notes in Computer Science: Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics*, vol. 5479, 2009, pp. 443–461.
- [34] S.-B. Lee, G. Pan, J.-S. Park, M. Gerla, S. Lu, Secure incentives for commercial ad dissemination in vehicular networks, *IEEE Trans. Veh. Technol.* 61 (6) (July 2012) 2715–2728.
- [35] S.B. Lee, G. Pan, J.S. Park, M. Gerla, S. Lu, Secure incentives for commercial ad dissemination in vehicular networks, in: *Proceedings of the 8th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, ACM, ACM, September 2007, pp. 150–159.
- [36] V.B.C. da Silva, M.E.M. Campista, L.H.M.K. Costa, TraC: a trajectory-aware content distribution strategy for vehicular networks, *Veh. Commun.* 5 (July 2016) 18–34.
- [37] J. Choi, J. Han, E. Cho, T. Kwon, Y. Choi, A survey on content-oriented networking for efficient content delivery, *IEEE Commun. Mag.* 49 (3) (March 2011) 121–127.

- [38] V. Jacobson, D.K. Smetters, J.D. Thornton, M.F. Plass, N.H. Briggs, R.L. Braynard, Networking named content, in: Proceedings of the 5th International Conference on Emerging Networking Experiments and Technologies, ACM, ACM, December 2009, pp. 1–12.
- [39] S. Uppoor, M. Fiore, Large-scale urban vehicular mobility for networking research, in: Proceedings of Vehicular Networking Conference (VNC), IEEE, November 2011, pp. 62–69.
- [40] B. Ramakrishnan, R.B. Nishanth, M.M. Joe, M. Selvi, Cluster based emergency message broadcasting technique for vehicular ad hoc network, *Wirel. Netw.* 23 (1) (2017) 233–248.
- [41] L. Nkenyereye, Y. Park, K.H. Rhee, Secure vehicle traffic data dissemination and analysis protocol in vehicular cloud computing, *J. Supercomput.* 10 (June 2016) 1–21.
- [42] J. He, Y. Ni, L. Cai, J. Pan, C. Chen, Optimal dropbox deployment algorithm for data dissemination in vehicular networks, *IEEE Trans. Mob. Comput.* 17 (3) (March 2018) 632–645.
- [43] P. Barreto, B. Libert, N. McCullagh, J.-J. Quisquater, Efficient and provably-secure identity-based signatures and signcryption from bilinear maps, in: Proceedings of 11th International Conference on the Theory and Application of Cryptology and Information Security, Chennai, India, December 4–8, 2005, ASIACRYPT, 2005, in: Lecture Notes in Computer Science, vol. 3788, Springer, 2005, pp. 515–532.
- [44] A. Shamir, Identity-based cryptosystems and signature schemes, in: Proceedings of CRYPTO 84 on Advances in Cryptology, in: Lecture Notes in Computer Science: Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics, vol. 196, 1985, Springer-Verlag, Inc., New York, 1984, pp. 47–53.
- [45] D. Boneh, M. Franklin, Identity-based encryption from the Weil pairing, in: J. Kilian (Ed.), Advances in Cryptology – CRYPTO 2001, in: Lecture Notes in Computer Science, vol. 2139, Springer, Berlin, Heidelberg, 2001, pp. 213–229.
- [46] Y. Jiang, M. Shi, X. Shen, C. Lin, BAT: a robust signature scheme for vehicular networks using binary authentication tree, *IEEE Trans. Wirel. Commun.* 8 (4) (Apr. 2009) 1974–1983.
- [47] F. Hess, Efficient identity-based signature schemes based on pairings, in: K. Nyberg, H. Heys (Eds.), Selected Areas in Cryptography, SAC 2002, in: Lecture Notes in Computer Science, vol. 2595, Springer, Berlin, Heidelberg, 2002, pp. 310–324.
- [48] L. Zhang, Q. Wu, A. Solanas, J. Domingo-Ferrer, A scalable robust authentication protocol for secure vehicular communications, *IEEE Trans. Veh. Technol.* 59 (4) (2010) 1606–1617.
- [49] H. Xie, L. Kulik, E. Tanin, Privacy-aware traffic monitoring, *IEEE Trans. Intell. Transp. Syst.* 11 (1) (March 2010) 61–70.
- [50] L. Sweeney, K-ANONYMITY: a model for protecting privacy, *Int. J. Uncertain. Fuzziness Knowl.-Based Syst.* 10 (5) (2002) 557–570.
- [51] C. Zhang, P.-H. Ho, J. Topolcai, On batch verification with group testing for vehicular communications, *Wirel. Netw.* 17 (8) (2011) 1851–1865.
- [52] J. Camenisch, S. Hohenberger, M. Pedersen, Batch verification of short signatures, in: Advances in Cryptology-Eurocrypt, in: Lecture Notes in Computer Science, vol. 4515, Springer-Verlag, Berlin, Germany, 2007, pp. 246–263.
- [53] C.-C. Lee, Y.-M. Lai, Toward a secure batch verification with group testing for VANET, *Wirel. Netw.* 18 (6) (2013) 1441–1449.
- [54] M. Bayat, M. Barmshoory, M. Rahimi, M.R. Aref, A secure authentication scheme for VANETs with batch verification, *Wirel. Netw.* 21 (5) (2015) 1733–1743.
- [55] L. Zhang, Q. Wu, B. Qin, J. Domingo-Ferrer, Identity-based authenticated asymmetric group key agreement protocol, in: Proceedings of International Computing and Combinatorics Conference, 2010, pp. 510–519.
- [56] Y. Zheng, Digital signcryption or how to achieve $\text{cost}(\text{signature} \& \text{encryption}) < \text{cost}(\text{signature}) + \text{cost}(\text{encryption})$, in: Proceedings of 17th Annual International Cryptology Conference, Santa Barbara, California, USA, August 17–21, 1997, in: Lecture Notes in Computer Science, vol. 1294, Springer-Verlag, 1997, pp. 165–179.
- [57] A. Ferrara, M. Green, S. Hohenberger, M. Pedersen, Practical short signature batch verification, in: Proceedings of CT-RSA, in: Lecture Notes in Computer Science, vol. 5473, Springer-Verlag, Berlin, Germany, 2009, pp. 309–324.
- [58] T. Nakanishi, T. Fujiwara, H. Watanabe, A linkable group signature and its application to secret voting, *Trans. Inf. Process. Soc. Jpn.* 40 (7) (1999) 3085–3096.
- [59] Q. Wu, J. Domingo-Ferrer, Ú. González-Nicolàs, Balanced trustworthiness, safety and privacy in vehicle-to-vehicle communications, *IEEE Trans. Veh. Technol.* 59 (2) (Feb. 2010) 559–573.
- [60] H. Xiong, K. Beznosov, Z. Qin, M. Ripeanu, Efficient and spontaneous privacy-preserving protocol for secure vehicular communication, in: Proceedings of 2010 IEEE International Conference on Communications (ICC), May 2010, IEEE, 2010.
- [61] D.Y.W. Liu, J.K. Liu, Y. Mu, W. Susilo, D. Wong, Revocable ring signature, *J. Comput. Sci. Technol.* 22 (November 2007) 78–794.
- [62] N.W. Lo, J.L. Tsai, An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks without pairings, *IEEE Trans. Intell. Transp. Syst.* 17 (5) (May 2011) 1319–1328.
- [63] S. Biswas, J. Misic, V. Misic, ID-based safety message authentication for security and trust in vehicular networks, in: Proceedings of 31st ICDCS Workshops, IEEE, Minneapolis, MN, 2011, pp. 323–331.
- [64] I. 1609 2, Trial-Use Standard for Wireless Access in Vehicular Environments-Security Services for Applications and Management Messages, IEEE Standards, 2006.
- [65] T.W. Chim, S.M. Yiu, L. Hui, V. Li, SPECS: secure and privacy enhancing communications schemes for VANETs, *Ad Hoc Netw.* 9 (2) (Mar. 2011) 189–203.
- [66] H.-C. Hsiao, A. Studer, C. Chen, A. Perrig, F. Bai, B. Bellur, A. Iyer, Flooding-resilient broadcast authentication for VANETs, in: Proceedings of the 17th Annual International Conference on Mobile Computing and Networking (MOBICOM 2011), ACM, 2011, pp. 193–204.
- [67] P. Vijayakumar, M. Azees, A. Kannan, J.D. Lazarus, Dual authentication and key management techniques for secure data transmission in vehicular ad hoc networks, *IEEE Trans. Intell. Transp. Syst.* 17 (4) (Apr. 2016) 1015–1028.
- [68] J. Shao, X. Lin, R. Lu, C. Zuo, A threshold anonymous authentication protocol for VANETs, *IEEE Trans. Veh. Technol.* 65 (3) (March 2016) 1711–1720.
- [69] L. Zhang, Q. Wu, J. Domingo-Ferrer, B. Qin, C. Hu, Distributed aggregate privacy-preserving authentication in VANETs, *IEEE Trans. Intell. Transp. Syst.* 18 (3) (2017) 516–526.
- [70] L. Zhang, C. Hu, Q. Wu, J. Domingo-Ferrer, B. Qin, Privacy preserving vehicular communication authentication with hierarchical aggregation and fast response, *IEEE Trans. Comput.* 65 (8) (2016) 2562–2574.
- [71] C. Lai, H. Zhou, N. Cheng, X.S. Shen, Secure group communications in vehicular networks: a software-defined network-enabled architecture and solution, *IEEE Veh. Technol. Mag.* 12 (4) (2017) 40–49.
- [72] A. Wasef, X. Shen, MAAC: message authentication acceleration protocol for vehicular ad hoc networks, in: Proceedings of IEEE GlobeCom, Nov. 2009, IEEE, 2009.
- [73] A. Wasef, X. Shen, EMAP: expedite message authentication protocol for vehicular ad hoc networks, *IEEE Trans. Mob. Comput.* 12 (1) (2013) 78–89.
- [74] J. Cui, J. Zhang, H. Zhong, Y. Xu, SPACF: a secure privacy-preserving authentication scheme for VANET with cuckoo filter, *IEEE Trans. Veh. Technol.* 66 (11) (November 2017) 10283–10295.
- [75] B. Bloom, Space/time trade-offs in hash coding with allowable errors, *Commun. ACM* 13 (7) (July 1970) 422–426.
- [76] X.L. Zheng, C.T. Huang, M. Matthews, Chinese remainder theorem based group key management, in: Proceedings of 45th ACMSE, Winston-Salem, NC, USA, 2007, pp. 266–271.
- [77] Zhou, Y.H. Ou, Key tree and Chinese remainder theorem based group key distribution scheme, *J. Chin. Inst. Eng.* 32 (7) (Oct. 2009) 967–974.
- [78] L. Zhang, Q. Wu, B. Qin, J. Domingo-Ferrer, APPA: aggregate privacy-preserving authentication in vehicular ad hoc networks, in: Proceedings of ISC, 2011, in: Lecture Notes in Computer Science: Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics, vol. 7001, Springer-Verlag, Berlin, Germany, 2011, pp. 293–308.
- [79] C. Lai, R. Lu, D. Zheng, Achieving secure and seamless IP communications for group-oriented software defined vehicular networks, in: 12th International Conference on Wireless Algorithms, Systems, and Applications, Springer, June 2017, pp. 356–368.
- [80] C. Zhang, X. Lin, R. Lu, P. Ho, RAISE: an efficient RSU-aided message authentication scheme in vehicular communication networks, in: Proceedings of IEEE International Conference on Communications (ICC), IEEE, 2008, pp. 1451–1457.
- [81] C. Zhang, X. Lin, R. Lu, P.-H. Ho, X. Shen, An efficient message authentication scheme for vehicular communications, *IEEE Trans. Veh. Technol.* 57 (6) (Nov. 2008) 3357–3368.
- [82] Y. Hao, Y. Cheng, K. Ren, Distributed key management with protection against RSU compromise in group signature based VANETs, in: Proceedings of IEEE GLOBECOM, New Orleans, LA, USA, 2008, IEEE, 2008.
- [83] X. Sun, X. Lin, P.-H. Ho, Secure vehicular communications based on group signature and id-based signature scheme, in: Proceedings of IEEE International Conference on Communications, June 2007, IEEE, 2007, pp. 1539–1545.
- [84] P. Papadimitratos, G. Mezzour, J.-P. Hubaux, Certificate revocation list distribution in vehicular communication systems, in: Proceedings of the Fifth ACM International Workshop on Vehicular Inter-Networking (VANET 2008), San Francisco, CA, USA, September 15, 2008, ACM, 2008.
- [85] R. Lu, X. Lin, X. Shen, Spring: a social-based privacy-preserving packet forwarding protocol for vehicular delay tolerant networks, in: Proceedings of IEEE INFOCOM, San Diego, CA, Mar. 2010, 2010, pp. 1–9.
- [86] K.-A. Shim, CPAS: an efficient conditional privacy-preserving authentication scheme for vehicular sensor networks, *IEEE Trans. Veh. Technol.* 61 (4) (May 2012) 1874–1883.
- [87] H. Harney, C. Muckenhirn, Group key management protocol GKMP architecture, *ietf.org, Tech. Rep. RFC 2094*, July 1997.
- [88] A.T. Sherman, D.A. McGrew, Key establishment in large dynamic groups using one-way function trees, *IEEE Trans. Softw. Eng.* 29 (5) (May 2003) 444–458.
- [89] R. Canetti, J. Garay, G. Itkis, D. Micciancio, M. Naor, B. Pinkas, Multicast security: a taxonomy and some efficient construction, in: Proceedings of Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM'99), vol. 2, IEEE, IEEE, March 1999, pp. 708–716.

- [90] Y. Sun, W. Trappe, K.J.R. Liu, An efficient key management scheme for secure wireless multicast, in: *Proceedings of IEEE International Conference on Communications (ICC)*, vol. 2, 2002, IEEE, IEEE, April 2002, pp. 1236–1240.
- [91] Y. Sun, W. Trappe, K.J.R. Liu, Topology-aware key management schemes for wireless multicast, in: *Global Telecommunications Conference, GLOBECOM '03*, IEEE, December 2003, pp. 1471–1475.
- [92] Y. Sun, W. Trappe, K.J.R. Liu, A scalable multicast key management scheme for heterogeneous wireless networks, *IEEE/ACM Trans. Netw.* 12 (August 2004) 653–666.
- [93] M.-H. Park, G.-P. Gwon, S.-W. Seo, H.-Y. Jeong, RSU-based distributed key management (RDKM) for secure vehicular multicast communications, *IEEE J. Sel. Areas Commun.* 29 (3) (2011) 644–658.
- [94] G. Caronni, M. Waldvogel, D. Sun, B. Plattner, The versaKey framework: versatile group key management, *IEEE J. Sel. Areas Commun.* 17 (9) (September 1999) 1614–1631.
- [95] C.-T. Li, M.-S. Hwang, Y.P. Chu, A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks, *Comput. Commun.* 31 (12) (2008) 2803–2814.
- [96] X. Lin, X. Sun, X. Wang, C. Zhang, P.-H. Ho, X. Shen, TSVC: timed efficient and secure vehicular communications with privacy preserving, *IEEE Trans. Wirel. Commun.* 7 (12) (December 2008) 4987–4998.
- [97] A. Perrig, R. Canetti, J.D. Tygar, D. Song, The TESLA broadcast authentication protocol, *RSA CryptoBytes*, vol. 5. Available: <https://users.ece.cmu.edu/~adrian/projects/tesla-cryptobytes/paper/index.html>, Summer 2002.
- [98] T. Zhou, R. Choudhury, P. Ning, K. Chakrabarty, P^2 DAP - Sybil attacks detection in vehicular ad hoc networks, *IEEE J. Sel. Areas Commun.* 29 (3) (March 2011) 582–594.
- [99] S. Bao, W. Hathal, H. Cruickshank, Z. Sun, P. Asuquo, A. Lei, A lightweight authentication and privacy-preserving scheme for VANETs using TESLA and bloom filters, *ICT Express*, <https://doi.org/10.1016/j.ict.2017.12.001>, 2017.
- [100] Y.-C.L.M.-S. Hwang, C.-C. Lee, An untraceable blind signature scheme, *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.* E86-A (7) (2003) 1902–1906.
- [101] R.L.R.D. Chaum, A.T. Sherman (Eds.), *Blind Signatures for Untraceable Payments*, *Advances in Cryptology*, Springer, Boston, MA, 1983.
- [102] C. Lyu, D. Gu, Y. Zeng, P. Mohapatra, PBA: prediction-based authentication for vehicle-to-vehicle communications, *IEEE Trans. Dependable Secure Comput.* 13 (1) (Jan.–Feb. 2016) 71–83.
- [103] X. Lin, X. Sun, P.-H. Ho, X. Shen, GSIS: a secure and privacy preserving protocol for vehicular communications, *IEEE Trans. Veh. Technol.* 56 (6) (Nov. 2007) 3442–3456.
- [104] D. Huang, S. Misra, M. Verma, G. Xue, PACP: an efficient pseudonymous authentication-based conditional privacy protocol for VANETs, *IEEE Trans. Intell. Transp. Syst.* 12 (3) (2011) 736–746.
- [105] J. Zhang, W. Zhen, M. Xu, An efficient privacy-preserving authentication protocol in VANETs, in: *Proceedings of 2013 IEEE Ninth International Conference on Mobile Ad-hoc and Sensor Networks (MSN)*, IEEE, 2013.
- [106] M. Girault, Self-certified public keys, in: D.W. Davies (Ed.), *Advances in Cryptology – EUROCRYPT '91*, Springer Berlin Heidelberg, Berlin, Heidelberg, 1991, pp. 490–497.
- [107] M. Azees, P. Vijayakumar, L.J. Deboarh, EAAP: efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks, *IEEE Trans. Intell. Transp. Syst.* 18 (9) (2017) 2467–2476.
- [108] D. Boneh, H. Shacham, Group signatures with verifier-local revocation, in: *Proceedings of the ACM Conference on Computer and Communications Security*, ACM, 2004, pp. 168–177.
- [109] C.D. Jung, C. Sur, Y. Park, K.-H. Rhee, A robust conditional privacy-preserving authentication protocol in VANET, in: *Proceedings of Security and Privacy in Mobile Information and Communication Systems*, in: *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, vol. 17, Springer-Verlag, Berlin, Germany, 2009, pp. 35–45.
- [110] F. Wang, Y. Xu, H. Zhang, Y. Zhang, L. Zhu, 2FLIP: a two-factor lightweight privacy-preserving authentication scheme for VANET, *IEEE Trans. Veh. Technol.* 65 (2) (Feb. 2016) 896–911.
- [111] Y. Sun, R. Lu, X. Lin, X. Shen, J. Su, An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications, *IEEE Trans. Veh. Technol.* 59 (7) (2010) 3589–3603.
- [112] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, J.P. Hubaux, Eviction of misbehaving and faulty nodes in vehicular networks, *IEEE J. Sel. Areas Commun.* 25 (8) (2007) 1557–1568.
- [113] H. Sedjelmaci, S.M. Senouci, T. Bouali, Predict and prevent from misbehaving intruders in heterogeneous vehicular networks, *Veh. Commun.* 10 (October 2017) 74–83.
- [114] P. Golle, M. Jakobsson, A. Juels, P. Syverson, Universal re-encryption for mixnets, in: 2004, in: *Lecture Notes in Computer Science: Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics*, vol. 2964, Springer, 2004, pp. 163–178.
- [115] B. Libert, D. Vergnaud, Multi-use unidirectional proxy re-signatures, in: *Proceedings of the 15th ACM Conference on Computer and Communications Security*, 27 October 2008, ACM, 2008, pp. 511–520.
- [116] V. Paruchuri, A. Dursesi, PAAVE: protocol for anonymous authentication in vehicular networks using smart cards, in: *Proceedings of GLOBECOM*, IEEE, 2010.
- [117] B.D. Ying, A. Nayak, Efficient authentication protocol for secure vehicular communications, in: *Proceedings of IEEE 79th Vehicular Technology Conference*, IEEE, 2014.
- [118] B. Ying, A. Nayak, Anonymous and lightweight authentication for secure vehicular networks, *IEEE Trans. Veh. Technol.* 66 (12) (2017) 10626–10636.
- [119] C. Zhang, R. Lu, X. Lin, P.-H. Ho, X. Shen, An efficient identity-based batch verification scheme for vehicular sensor networks, in: *Proceedings of IEEE 27th Conference on Computer Communications (INFOCOM)*, IEEE, April 2008, pp. 246–250.
- [120] M. Raya, J.P. Hubaux, Securing vehicular ad hoc networks, *J. Comput. Secur.* 15 (1) (2007) 39–68.
- [121] S. Wang, N. Yao, LIAP: a local identity-based anonymous message authentication protocol in VANETs, *Comput. Commun.* 112 (November 2017) 154–164.
- [122] S. Jiang, X. Zhu, L. Wang, An efficient anonymous batch authentication scheme based on HMAC for VANETs, *IEEE Trans. Intell. Transp. Syst.* 17 (8) (Aug. 2016) 2193–2204.
- [123] A. Wasef, R. Lu, X. Lin, X. Shen, Complementing public key infrastructure to secure vehicular ad hoc networks, *IEEE Wirel. Commun.* 17 (5) (Oct. 2010) 22–28.
- [124] S. Biswas, J. Mistic, Establishing trust on VANET safety messages, in: *Proceedings of the Second International Conference on Ad Hoc Networks (ADHOC-NETS 2010)*, 2010, Springer, Victoria, BC, Canada, 2010.
- [125] S. Biswas, J. Mistic, Deploying proxy signature in VANETs, in: *Proceedings of the IEEE Global Telecommunications Conference GLOBECOM 2010 (GLOBECOM 2010)*, IEEE, 2010.
- [126] S. Biswas, J. Mistic, Proxy signature-based RSU message broadcasting in VANETs, in: *Proceedings of the 25th Biennial Symposium on Communications (QBSC)*, Kingston, ON, Canada: IEEE, 2010, IEEE, 2010, pp. 5–9.
- [127] X. Dong, L. Wei, H. Zhu, Z. Cao, L. Wang, EP2DF: an efficient privacy-preserving data-forwarding scheme for service-oriented vehicular ad hoc networks, *IEEE Trans. Veh. Technol.* 60 (2) (Feb. 2011) 580–591.
- [128] J.J. Haas, Y.-C. Hu, K.P. Laberteaux, Efficient certificate revocation list organization and distribution, *IEEE J. Sel. Areas Commun.* 29 (3) (2011) 595–604.
- [129] A.-N. Shen, S. Guo, D. Zeng, M. Guizani, A lightweight privacy preserving protocol using chameleon hashing for secure vehicular communications, in: *Proceedings of IEEE Wireless Communications and Networking Conference*, IEEE, 2012, pp. 2543–2548.
- [130] H. Krawczyk, T. Rabin, Chameleon signatures, in: *Network and Distributed System Security Symposium (NDSS)*, February 2000.
- [131] W. Whyte, A. Weimerskirch, V. Kumar, T. Hehn, A security credential management system for V2V communications, in: *Proceedings of the 5th IEEE Vehicular Networking Conference (VNC 2013)*, IEEE, 2013.
- [132] H. Alshaer, Securing vehicular ad-hoc networks connectivity with roadside units support, in: *Proceedings of IEEE 8th GCC Conference and Exhibition (GCCCE 2015)*, March 2015, IEEE, 2015.
- [133] H. Tan, M. Ma, H. Labiod, A. Boudguiga, J. Zhang, P.H.J. Chong, A secure and authenticated key management protocol (SA-KMP) for vehicular networks, *IEEE Trans. Veh. Technol.* 65 (12) (2016) 9570–9584.
- [134] P.-Y. Shen, V. Liu, M. Tang, C. William, An efficient public key management system: an application in vehicular ad hoc networks, in: *Proceedings of Pacific Asia Conf. Inf. Syst. (PACIS 2011)*, 2011.
- [135] M. Hamid, M.S. Islam, C.S. Hong, Developing security solutions for wireless mesh enterprise networks, in: *Proceedings of IEEE Wireless Communications and Networking Conference (WCNC)*, IEEE, 2008, pp. 2549–2554.
- [136] M.A. Hamid, M. Abdullah-Al-Wadud, C.S. Hong, O. Chae, S. Lee, A robust security scheme for wireless mesh enterprise networks, *Ann. Télécommun.* 64 (5–6) (June 2009) 401–413.
- [137] K. Laberteaux, J. Haas, Y.-C. Hu, Security certificate revocation list distribution for VANET, in: *Proceedings of the fifth ACM International Workshop on Vehicular Inter-Networking*, 15 September 2008, ACM, 2008, pp. 88–89.
- [138] X.L.H. Zhu, R. Lu, P. Ho, X. Shen, AEMA: an aggregated emergency message authentication scheme for enhancing the security of vehicular ad hoc networks, in: *Proceedings of IEEE International Conference on Communications (ICC)*, IEEE, 2008, pp. 1436–1440.
- [139] S. Dietzel, E. Schoch, F. Kargl, B. Könings, M. Weber, Resilient secure aggregation for vehicular networks, *IEEE Netw.* 24 (1) (Jan.–Feb. 2010) 26–31.
- [140] R. van der Heijden, S. Dietzel, F. Kargl, SeDyA: secure dynamic aggregation in VANETs, in: *Proceedings of ACM Conference on Security and Privacy in Wireless and Mobile Networks*, ACM, 2013, pp. 131–142.
- [141] Y. Hao, Y. Chen, C. Zhou, W. Song, A distributed key management framework with cooperative message authentication in VANETs, *IEEE J. Sel. Areas Commun.* 29 (3) (March 2011) 616–629.
- [142] D. Boneh, X. Boyen, H. Shacham, Short group signatures, in: *Advances in Cryptology—CRYPTO*, in: *Lecture Notes in Computer Science*, vol. 3152, Springer-Verlag, Berlin, Germany, 2004.
- [143] C. Lai, K. Zhang, N. Cheng, H. Li, X. Shen, SIRC: a secure incentive scheme for reliable cooperative downloading in highway VANETs, *IEEE Trans. Intell. Transp. Syst.* 18 (6) (June 2017) 1559–1574.

- [144] L. Wang, X. Liu, Secure cooperative communication scheme for vehicular heterogeneous networks, *Veh. Commun.* 11 (January 2018) 46–56.
- [145] X. Lin, X. Li, Achieving efficient cooperative message authentication in vehicular ad hoc networks, *IEEE Trans. Veh. Technol.* 62 (7) (Sept. 2013) 3339–3348.
- [146] S. Jiang, X. Zhu, L. Wang, A conditional privacy scheme based on anonymized batch authentication in vehicular ad hoc networks, in: *Proceedings of IEEE WCNC, Shanghai, China, Apr. 2013*, IEEE, 2013, pp. 2375–2380.
- [147] J. Cheon, J. Yi, Fast batch verification of multiple signatures, in: *Public-Key Cryptography-PKC*, in: *Lecture Notes in Computer Science*, vol. 4450, Springer-Verlag, Berlin, Germany, 2007, pp. 442–457.
- [148] A. Wasef, Y. Jiang, X. Shen, DCS: an efficient distributed certificate service scheme for vehicular networks, *IEEE Trans. Veh. Technol.* 59 (2) (Feb. 2010) 533–549.
- [149] A. Wasef, Y. Jiang, X. Shen, ECMV: efficient certificate management scheme for vehicular networks, in: *Proceedings of IEEE Global Telecommunications Conference (GLOBECOM)*, 2008, IEEE, 2008.
- [150] L. Zhang, F. Zhang, A new certificateless aggregate signature scheme, *Comput. Commun.* 32 (6) (2009) 1079–1085.