EURASIP Journal on Wireless Communications and Networking

RESEARCH Open Access

Authentication strategies in vehicular communications: a taxonomy and framework

Mir Ali Rezazadeh Baee[1*], Leonie Simpson[1], Xavier Boyen[1], Ernest Foo[1,2] and Josef Pieprzyk[1,3,4]

*Correspondence:
info@baee.co
[1] School of Computer Science, Queensland University of Technology, 2 George Street, Brisbane, QLD 4000, Australia
Full list of author information is available at the end of the article

Abstract

In intelligent vehicular networks, vehicles have enhanced sensing capabilities and carry computing and communication platforms to enable new versatile systems known as Vehicular Communication (VC) systems. Vehicles communicate with other vehicles and with nearby fixed equipment to support different applications, including those which increase driver awareness of the surroundings. This should result in improved safety and may optimize traffic. However, VC systems are vulnerable to cyber attacks involving message manipulation. Research aimed at tackling this problem has resulted in the proposal of multiple authentication protocols. Several existing survey papers have attempted to classify some of these protocols based on a limited set of characteristics. However, to date there is no generic framework to support the comparison of these protocols and provide guidance for design and evaluation. Most existing classifications either use computation complexity of cryptographic techniques as a criterion, or they fail to make connections between different important aspects of authentication. This paper provides such a framework, proposing a new taxonomy to enable a consistent means of classifying authentication schemes based upon seven main criteria. The main contribution of this study is a framework to enable protocol designers and investigators to adequately compare and select authentication schemes when deciding on particular protocols to implement in an application. Our framework can be applied in design, making choices appropriate for the intended context in both intra-vehicle and inter-vehicle communications. We demonstrate the application of our framework using two different types of case study: individual analysis and hypothetical design. Additionally, this work makes several related contributions. We present the network model, outline the applications, list the communication patterns and the underlying standards, and discuss the necessity of using cryptography and key management in VC systems. We also review the threats, authentication, and privacy requirements in vehicular networks.

Keywords: Cryptography, Authentication, Vehicular communication systems, Taxonomy, Framework

1 Introduction

Car accidents kill or injure millions of people every year. The road safety report published by the World Health Organization (WHO) in 2015 [1], collecting information from 180 countries, shows total fatalities connected with street traffic stabilized at 1.25 million a year. Vehicular communication systems have the potential to improve current

vehicular safety services. For example, by using periodic safety message broadcasting, vehicles can be informed about environmental conditions and neighboring vehicles [2].

Historically, road vehicles were independent and mostly mechanical systems. Current vehicles increasingly use built-in networks of sensors, actuators and electronic control systems. Many of these functions are related to safety. For example, anti-lock braking, sophisticated emergency braking, automated stability control, and adaptive cruise control are vehicle systems that use technology to assist drivers.

To take the vehicular technology a little further, automated highway systems and Intelligent Transportation Systems (ITS) were introduced. The term ITS refers to use of Information and Communication Technologies (ICT) intelligently to increase road safety and reducing the number of accidents. In fact, ITS comprise a wide range of technologies, controls, systems, and applications to save lives, time, and money by preventing crashes [3]. Current examples of ITS include vehicle safety systems such as collision avoidance systems, roadway safety systems such as intersection collision avoidance systems, and incident response such as automatic crash notification systems. There are additional benefits for ITS, such as allowing drivers to avoid vehicular congestion, finding the optimal path to a destination by processing real-time data, vehicle behavior analysis, examining road capacity, pedestrian flow rate analysis, and so on.

The ITS platforms are now being established globally. The primary advancements come from USA, Europe, and Japan [4]. Each of these territories has defined a group of new standards that specify different aspects of the C-ITS communications, such as Physical layer (PHY) and Medium Access Control layer (MAC), data structures, and security.

While ITS focus on digital technologies providing intelligence placed at the roadside or in vehicles, Cooperative Intelligent Transportation Systems (C-ITS) focus on the communication between those systems. This includes a vehicle communicating with another vehicle, with the infrastructure, or with other C-ITS systems [5]. Standards are necessary for the C-ITS elements created by different companies to operate together. The Institute of Electrical and Electronics Engineers (IEEE) in USA, the European Telecommunications Standards Institute (ETSI) in Europe, and Association of Radio Industries and Businesses (ARIB) in Japan are well-known sources with defined C-ITS standards.

The American IEEE 1609, European ETSI ITS-G5, and Japanese ARIB STD-T109 standards aim to establish C-ITS by enabling a self-organizing network called a Vehicular Ad-hoc Network (VANET). The capability of this technology in very low-latency (latency critical) broadcast communications to use in hazardous situations has emerged as a promising approach toward increasing road safety and efficiency, as well as improving driving experience. Latency defines an allowable time frame between when information is generated for transmission and when it is received.

One of the main elements of C-ITS is the capability for heterogeneous vehicles and infrastructure to communicate with one another in an interoperable manner. Car manufacturers embed devices such as IEEE 802.11p, known as Wireless Access in Vehicular Environments (WAVE) in vehicles to enable wireless communication with other vehicles and nearby fixed electronic equipment, such as Road-Side Units (RSUs).

The WAVE enabled vehicles can synchronize and handshake via beacons (beacon messages) which periodically share the vehicle's mobility characteristics with its neighbors [6]. The beacon messages are short network packets containing the

identification and context information for a vehicle, such as vehicle location, speed, braking status, traffic conditions, and traffic events [7]. The detected data, such as road conditions, driving status, and traffic info, is processed and shared with vehicles and RSUs using beacons within required latency for different purposes such as collision avoidance.

This system is useful if all messages are legitimate. Safety messages are broadcast to reach all network entities within communication range. However, malicious entities could manipulate messages. Without the use of security mechanisms, activities such as the injection of false messages can be performed without detection. For this reason, mechanisms should be applied to ensure both identification of the data source (entity authentication) and authentication of the message (assurance of data origin and data integrity).

1.1 Authentication between network entities

Authentication is a vital part of trust establishment between network entities. It ensures that received messages come from the legitimate entities. Without this security service, messages transmitted by network entities can be altered by an attacker, or a bogus message can be generated by an impersonator. Also, a sender can later deny the message generation.

A message can be authenticated at two levels, including node level and the message level. Node level authentication refers to entity authentication (identification) and ensures that the message is received from a legitimate source. The message level authentication or data-origin authentication ensures the integrity of a message, and plays an important role in enhancing security [8]. This section outlines different types of authentication, including entity authentication and message authentication.

Entity authentication or identification is a technique designed to assure one party (the verifier) that the identity of another (the prover or claimant) is as claimed, and as a result, preventing impersonation [9]. From the verifier's point of view, the result of an identification protocol is either acceptance of the prover's identity as authentic, or rejection (termination without acceptance). Entity authentication techniques can be based on something known such as a password, something possessed like a passport, or something inherent (to a human individual) such as a handwritten signature [10].

Message authentication provides data origin authentication. It ensures the original message source and data integrity. An authentication type is called data origin authentication where a party is verified as the original source of data created at some time in the past. A property in which data has not been altered in an unauthorized manner is called data integrity. This property must be kept since the time data was created, transmitted, or stored by an authorized source. For any received message, it is required to ensure data actually came from its reputed source (data origin authentication), and it is unaltered (data integrity). The above-mentioned issues (data origin authentication, and data integrity) cannot be separated. If data is altered, it effectively has a new source, and if the source is not determined, then the investigation for alteration cannot be settled (data cannot be linked to a source). Thus, integrity mechanisms implicitly provide data origin authentication, and vice versa [10].

1.2 Research challenge

Many authentication schemes have been proposed to secure VC systems; examples include [11–60]. Existing studies [61–69] have attempted to classify some of these schemes based on a limited set of characteristics. However, to date there is no generic framework to support the comparison of these protocols and provide guidance for design and evaluation.

Most existing classifications either use the computational complexity of the cryptographic techniques as a criterion, or they fail to make connections between different important aspects of authentication, such as digital signatures. For example, Riley et al. [62] and Qu et al. [63] classify authentication protocols based on the computational complexity of cryptographic approaches involved: symmetric or asymmetric. Petit et al. [64] and Manvi et al. [65] classify authentication strategies into different categories. However, neither of these classifications includes the Identity-based (ID-based) approach as a subcategory of the asymmetric cryptography category. Similarly, Lu et al. [67] classify authentication schemes, but include ID-based and certificate-less approaches in different categories, although both are certificate-less strategies.

1.3 Research contribution

This research specifically addresses the development and evaluation of a taxonomy and framework to provide comprehensive guidance on the design, evaluation, and analysis of authentication protocols in the public literature and future proposals. This enables designers and investigators to adequately compare and select authentication schemes when deciding on particular protocols to implement in an application. Besides, this work makes several related contributions. We present the network model, outline the applications, list the communication patterns and the underlying standards, and discuss the necessity of using cryptography in vehicular networks. We also review the security standards and analyze multiple well-known authentication schemes. The main contributions are summarized as follows:

1. A new comprehensive taxonomy for authentication strategies in VC systems is provided. This generic taxonomy will enable identification of the similarities and differences between sets of related protocols. It helps to identify common structural elements for each class aiding both design and analysis. Based on extensive review of the public literature [11–60], this research has identified seven different criteria that form the backbone of many authentication schemes proposed for securing VC systems. The identified criteria used in the taxonomy proposed in this research include: cryptographic method, credential type, verification approach, secure hardware, privacy principle, network domain, and application latency.
2. Based on the proposed taxonomy, a framework is generated to facilitate comparisons of new and existing protocols, provide guidance for the design, evaluation, and analysis, and highlight common elements that could allow reuse of a given analysis.
3. A case study approach is employed to demonstrate the usefulness of the proposed taxonomy and framework. Through two types of case study, this research provides

individual analysis of seven well-known authentication protocols and presents a hypothetical authentication protocol design.

1.4 Research scope

Please note that this manuscript does have its limitation. This is not a survey paper on this area, and the reader will necessarily have to use other sources to get a 'big picture' overview. The aim is to systematize the study by grouping different authentication strategies using the proposed taxonomy, while providing related examples for each group. Thus, no attempt is made to write a survey paper covering all emerging authentication methods.

The remainder of this paper is organized as follows. Section 2 reviews different cryptographic techniques for authentication, cryptography for certification of network entities, key-management technique for cryptographic authentication, and outlines some basic definitions. Section 3 provides an overview on the vehicular networks, applications, the key features of European, American, and Japanese C-ITS standards, and the network simulation tools. The IEEE 1609.2 C-ITS security standard is also outlined. Section 4 discusses the threats, and outlines the efficiency and privacy requirements for authentication in vehicular networks. The necessity of using key-management mechanism is also covered. Section 5 reviews previous work on classifying authentication protocols. Section 6 presents our taxonomy for authentication strategies. Section 7 introduces our framework. In Sect. 8, we illustrate the use of our framework by case studies provided. We discuss our framework in Sect. 9 and conclude the paper in Sect. 10. Please note that all the abbreviations used throughout the paper are summarized in Table 1.

2 Preliminaries in cryptography

Before the underlying cryptographic primitives for authentication protocols in VC systems can be discussed, a brief introduction to cryptography is necessary.

The method in which advanced mathematical principles are used to store and transmit data in a secure way is called Cryptography [10]. A cryptographic algorithm uses a string of bits to transform a plain text into a cipher text (encryption) or vice versa (decryption). This string of bits is called a cryptographic key which remains private to ensure a secure communication. The length of a key is normally expressed in bits. A longer key makes exhaustive key search more difficult to perform (makes an encrypted data more difficult to crack). It may also result in longer time periods to perform encryption and decryption processes. Cryptographic keys can be used for different purposes, such as data encryption, decryption, identification, and message authentication.

Basically, there are two major categories of encryption, called symmetric encryption (also known as secret-key encryption), and asymmetric encryption (also known as public-key encryption) [10].

Symmetric encryption (also known as symmetric-key cryptography) uses a secret key such as a string of random letters to change the content of a message in a particular way. Both sender and recipient can encrypt and decrypt all messages using the same secret key. It is highly efficient in terms of computational overhead, and offers the benefits of short encryption and decryption time [10].

Table 1 List of abbreviations

Abbreviation	Meaning
AES	Advanced Encryption Standard
ARIB	Association of Radio Industries and Businesses
BP	Baseline Pseudonymous
Brainpool	Brainpool Standard Curves and Curve Generation
CA	Certification Authority
CAN	Controller Area Network
CCH	Control Channel
C-ITS	Cooperative Intelligent Transportation Systems
CRL	Certificate Revocation List
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
DoS	Denial of Service
DOT	Department of Transportation
DSRC	Dedicated Short-Range Communications
DSSS	Direct Sequence Spread Spectrum
ECC	Elliptic Curve Cryptography
ECDLP	Elliptic Curve Discrete Logarithm Problem
ECDSA	Elliptic Curve Digital Signature Algorithm
ECIES	Elliptic Curve Integrated Encryption Scheme
ECQV	Elliptic Curve Qu-Vanstone
EDCA	Enhanced Distributed Channel Access
ETSI	European Telecommunications Standards Institute
FHSS	Frequency-Hopping Spread Spectrum
GHz	GigaHertz
GPS	Global Positioning System
HMAC	Hash-based Message Authentication Code
I2V	Infrastructure-to-Vehicle
ICT	Information and Communication Technologies
ID-based	Identity-based
IEEE	Institute of Electrical and Electronics Engineers
ITS	Intelligent Transportation Systems
ITS-RS	Intelligent Transportation Systems Radio Service
MAC	Message Authentication Code
MAC	Medium Access Control layer
MANET	Mobile Ad-hoc Network
MHz	MegaHertz
NIST	National Institute of Standards and Technology
OBU	On-Board Unit
PHY	Physical layer
PKI	Public-Key Infrastructure
RF	Radio Frequency
RL	Revocation List
RSSI	Received Signal Strength Indication
RSU	Road-Side Unit
SCH	Service Channels
SHA	Secure Hash Algorithms
SNR	Signal to Noise Ratio
TA	Trusted Authority
TDMA	Time Division Multiple Access
TESLA	Timed Efficient Stream Loss-tolerant Authentication

Table 1 (continued)

Abbreviation	Meaning
TPD	Tamper Proof Device
TSVC	Timed efficient and Secure Vehicular Communication
U.S.	United States
V2I	Vehicle-to-Infrastructure
V2V	Vehicle-to-Vehicle
VANET	Vehicular Ad-hoc Networks
VAST	VANET Authentication using Signatures and TESLA++
VC	Vehicular Communication
VIN	Vehicle Identification Number
WHO	World Health Organization
WLAN	Wireless Local Area Network

One of the main drawbacks of symmetric encryption technique is exchanging secret keys over the network. As any party who knows the secret keys can decrypt the message, it is vital to prevent them from falling into the wrong hands. One solution is asymmetric encryption [10].

Asymmetric encryption (also known as public-key cryptography) consists of two mathematically related keys (a key pair), including a public key and a private key. Any party or a certificate authority can generate public/private key pairs. A public key is available to anyone who may want to encrypt and send a message to you, while a private key must be kept secret to decrypt the message. In secure systems, computing private key given public key is computationally infeasible. Any encrypted message using a public key can only be decrypted by applying the same algorithm and the matching private key. Using this method, we are not concerned about exchanging public keys over the networks [10].

One of the main drawbacks of asymmetric encryption technique is high computational overhead. Asymmetric encryption requires far more processing power for both encryption and decryption, and as a result, it is slower than symmetric encryption [10].

This section briefly reviews different cryptographic techniques for authentication, cryptography for certification of network entities, key management for cryptographic authentication, and outlines some basic definitions.

2.1 Cryptography for authentication

There are three methods to provide data origin authentication, including Message Authentication Codes (MACs), digital signature schemes, and appending (adding a secret authenticator value to an encrypted text).

Unlike digital signatures, other mechanisms for data origin authentication based on shared secret keys such as MACs do not provide non-repudiation of data origin. Non-repudiation ensures that a dishonest party cannot deny its action, such as the time of generating and transmitting a message. The reason is that using the shared key, any party can equally originate a message. In cryptography, a shared secret is a piece of data such as a password, a pass phrase, a big number, or a randomly chosen array of bytes. In a secure communication, a shared secret is known only to the involved parties.

This section reviews some basic cryptographic primitives for authentication, including: hash functions, MACs, hash-based MACs, and digital signatures.

A Cryptographic hash function

A cryptographic hash function is a one-way function (infeasible to invert) that is used for data integrity assurance. It takes a message as input and produces an output referred to as a hash value. A cryptographic hash implies an un-keyed hash function [10].

B Message authentication code (MAC)

A MAC is a short piece of information used to confirm that a message comes from the stated sender (its authenticity), and has not been changed. Different symmetric cryptographic primitives such as cryptographic hash functions, or block cipher algorithms can be used to construct MAC algorithms [10].

C Hash-based message authentication code (HMAC)

An HMAC implies a keyed-hash function that takes two functionally distinct inputs, a message and a secret key, and produces a fixed-size output. In practice, it should be infeasible to produce the same output without knowledge of the key. HMACs can be constructed using Secure Hash Algorithms (SHA), such as SHA-256 or SHA3-256 cryptographic hash functions. HMACs can be used to provide both data integrity assurance and symmetric data origin authentication, as well as identification in symmetric-key schemes [10]. Note that any communicating node with knowledge of shared secret key can be an originator of data.

Hash-based authentication is highly efficient in terms of computational and communication overhead. It offers the benefits of short generation and verification time as well as less communication overhead. The security of HMACs depends on the cryptographic strength of the underlying hash function, and the size and quality of the key used [10].

D Digital signature

A digital signature is a number generated on the content of a message using a secret that is known only to the signer, and must be verifiable. In information security, digital signatures have many applications. They are used for ensuring authentication, data integrity, and non-repudiation. Also, digital signatures are significantly applied for the certification of public keys in large networks. Certification is a mechanism to bind a user identity to a public key by a trusted party. This public key later can be authenticated by other entities without assistance from a TA. In this regard, many studies propose authentication mechanisms using digital signatures and cryptographic techniques [10].

Johnson et al. [70] proposed the Elliptic Curve Digital Signature Algorithm (ECDSA) which is a digital signature scheme based on Elliptic Curve Cryptography (ECC), as described by Koblitz [71] and Miller [72]. The ECDSA is one of the most important underlying cryptographic primitives to design authentication schemes. In ECDSA, the message sender generates a signature with its own private key and the receiver verifies the signature with the sender's public key.

The security of the ECC-based algorithms is dependent on the difficulty of Elliptic Curve Discrete Logarithm Problem (ECDLP), if the elliptic curve group is selected properly. ECC offers similar security with smaller key sizes and memory requirements compared to other traditional DLP-based schemes in use today [73, 74].

2.2 Asymmetric public key certification

To benefit from asymmetric encryption, each communication party needs to obtain the recipient's public key. The most common approach to convey public keys is to use digital certificates (also known as certificates). A certificate consists of information to identify a party (a user or a server). This information might be the certificate owner's name, the certificate issuer organization, the owner's e-mail address, country, and public key. An entity's credential is embedded in a certificate which is either explicitly (signed by a trusted authority or self-signed) or implicitly (without attaching signature) certified. Using a copy of certificate, any party can extract the provided public key which is located in the certificate to uniquely identify the holder.

A Certification authority

The certification authority (CA) or trusted authority (TA) for certification is a managing authority that acts as the root of trust in a networked system [54, 75]. The CA can be a single point of trust (centralized), or multiple entities jointly working together (decentralized). For example, the department of motor vehicles or the department of transportation can provide everything related to authentication and key management in VANETs.

B Public-key explicit certificate

The public-key certificate is a data structure composed of two different parts, including a data part and a signature part. They can be used to store, distribute, or forward public keys over unsecured network without worrying about undetectable manipulation. A certificate makes one entity's authentic copy of public key available to others. Thus, others can verify the true public key of that entity and its validity.

The data part consists at least a public key and a unique string identifying the associated real-world entity. The signature part on the certificate contains a signature belonging to the CA that binds the subject entity's unique identity to the specified public key. Using this signature, an intended recipient can verify that the public key belongs to the subject entity. The CA is a trusted third party and responsible for signing the data part. During an authorized user registration, the authentic public key of the CA is made available to each party. The CA's public key enables system users to authenticate the public key in any certificate signed by that CA, and as a result, certificates transfer trust. The certificate's data part may carry additional information, for example the issuing CA's name, public key validity period, certificate serial number, the key identifier, subject entity's address, algorithm or intended use of key, key pair generation policies, signature algorithm identifier, or the status of the public key for revocation purpose [10].

The overall process in which a party B authenticates the public-key certificate of party A is summarized as follows:

1 (One-time) receiving the CA's authentic public key.
2 Receiving A's public-key certificate.
3 Verifying the certificate validity period (if any).
4 Verifying the current validity of the CA's public key.
5 Verifying the signature on A's certificate, using the CA's public key.
6 Verifying that the certificate is not revoked.
7 Accepting the A's public key as an authentic key [10].

C Implicitly certified public key

The implicitly certified public key or implicit certificate is another variation of digital certificates in public-key cryptography in which an explicit user's public key can be implicitly certified. The main difference is that here a public key must be reconstructed from public data, rather than transported by public-key certificates (explicit certificates) in certificate-based systems [76].

The Elliptic Curve Qu-Vanstone (ECQV) implicit certificate [76] is a variation of the digital certificates used with cryptography for which an explicit user's credential can be implicitly certified. The main difference is that here a credential must be reconstructed from public data, rather than transported within a certificate, as occurs with explicit certificates. An explicit certificate is composed of two different parts: a data part and a signature part. The data part contains a credential and a unique string identifying the associated entity. The signature part of the certificate contains the signature of the certificate owner or a trusted authority and that binds the subject entity's unique identity to the specified credential. An intended recipient can verify this signature and be assured that the credential belongs to the subject entity. During an authorized system user registration, the authentic public key of the trusted authority is made available to all communicating nodes. This public key enables communicating nodes to verify the certificates signed by that trusted authority, and as a result, transfers trust.

The implicit certificate is still comprised of the three main elements/parts (identifier, public credential, and digital signature), but superimposed into the same space as the size of a public credential, resulting in reduced data transfer. ECQV provides a more efficient alternative to traditional explicit certificates, as described in the document *Standards for Efficient Cryptography 4* [76]. The ECQV implicit certificate scheme is particularly well suited for application environments where resources such as bandwidth, computing power and storage are limited [17].

D Pseudonym certificate

A pseudonym or alias is an alternative identity that is verified by a third party (e.g., the CA) [77]. The pseudonym certificate is introduced to ensure that services can be used without disclosing the user's identity while the user is accountable for that use. For example, a government transportation authority or a vehicle manufacturer in liability-related cases may trace a vehicle that disrupts the network. In this case, a driver profile may be fetched to be used for legitimate reasons, such as providing emergency services or law enforcement with appropriate information. Designing an authentication mechanism that preserves driver privacy and also tracks dishonest vehicles is a major challenge.

E Certificate revocation list

A cryptographic key is compromised if an adversary gains knowledge of secret data. It is important to stop using or trusting the keying material which are no longer secure. The revocation for public-key certificates with long-term validity is a difficult task, as all distributed copies must be effectively retracted. One solution for this is use of Certificate Revocation List (CRL). A CRL is a list of public key entries subject to revoke. Each entry indicates the unique identifier of the associated certificate. The CA's signature on the CRL guarantees its authenticity. CRLs should be

issued at regular intervals even if there are no changes, to prevent new CRLs being maliciously replaced by old CRLs [10].

2.3 Key management for cryptographic authentication

Any cryptographic technique for authentication requires the use of a cryptographic key. Thus, a key-management mechanism is also required, to allow parties to establish and update the keys for security-sensitive operations [10]. Key management is very important, and it is necessary to protect keying material against threats in which:

1 Confidentiality of secret keys is compromised.
2 Authenticity of secret or public keys is compromised. This authentication mechanism is to verify the identity of a party which a key is associated with.
3 Authorized use of secret or public keys is compromised. For instance, using a key which is not intended to be used anymore, or no longer valid.

3 Overview of vehicular networks

This section first briefly reviews vehicular communication systems and VANETs. Next, the network model is presented and the VANET applications are outlined. Then, the communication patterns and the underlying C-ITS standards are listed. The C-ITS security standards are also discussed. Finally, the network simulation tools are briefly reviewed.

3.1 Vehicular communication systems and VANETs

Car manufacturers and industries embed devices known as On-Board Units (OBUs) in vehicles to facilitate Vehicular Communication (VC) systems. The VC systems have the potential to improve current vehicular safety services through periodic safety message broadcasting, to let vehicles know about environmental conditions and neighboring vehicles [78].

By connecting communicating nodes consisting of vehicles and Road-Side Units (RSUs), a self-organized network called Vehicular Ad-hoc Network (VANET) can be formed. A VANET is a type of Mobile Ad-hoc Network (MANET). VANETs have some unique characteristics, as the mobile nodes are vehicles equipped with OBUs. As the vehicles may move at high speeds, the VANET topology may change rapidly. Both the network density and the number of vehicles in one area of the road temporally fluctuate during the day.

Many modern vehicles use services such as localization, route selection, and accident avoidance using VC systems. These rely on inter-vehicle and intra-vehicle VANET communication services. The inter-vehicle transmission ensures Vehicle-to-Vehicle (V2V) and Vehicle-to/from-Infrastructure (V2I/I2V) wireless communications. The V2V communication is among nearby vehicles, and the V2I/I2V communication is between vehicles and infrastructure (e.g., RSU). Intra-vehicle communication consists of different components, such as sensors, actuators, devices, switches, displays, and other electronic

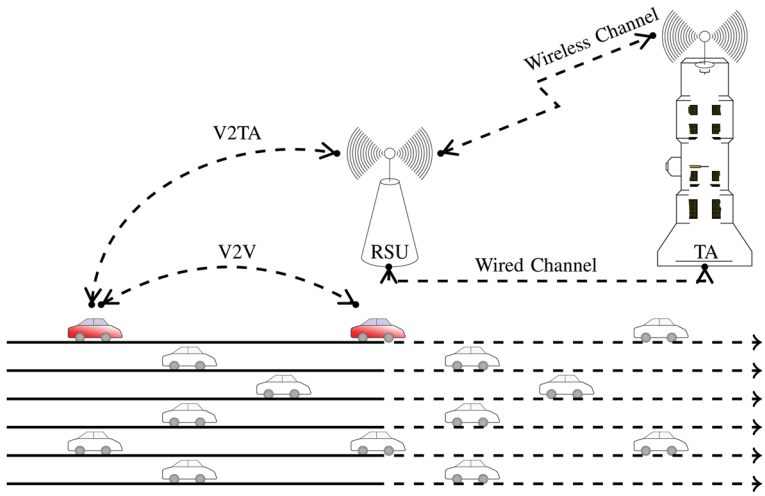

Fig. 1 Vehicular network model

components that are interconnected and act as communicating nodes over a serial communication bus called the Controller Area Network (CAN). This communication performs automotive functions inside a vehicle [78].

3.2 Network model

A potential vehicular network consists of a Trusted Authority (TA), RSUs along the roads, OBUs embedded in vehicles, and communication between these entities. This VANET architecture and communication model is illustrated in Fig. 1.

The TA is assumed to be always secure, trusted, and online. The TA can be implemented in a multi-layer structure, e.g., root TA and several sub-TAs. For sake of simplicity, here we show the TA as a single entity. The TA is a managing authority that can act as the root of trust to generate, update, and revoke credentials for other network entities, including vehicles. For example, the department of motor vehicles or the Department of Transportation (DOT) can act as the root TA. Further, the TA is the only one entity which can reveal a vehicle's real identifier in case of dispute.

The RSU is an access point, used along with vehicles, to allow information dissemination for the road user community. The RSUs are located along critical sections of roads, such as at traffic light intersections, or at stop signs. The RSUs are connected to the backbone network via high-speed network connections, and have data storing, computing, and routing capabilities for supporting the V2I communication [79] and increasing the V2V communication connectivity [80]. The distributed RSUs are equipped with a higher computational capability and transmission power than OBUs. The TA and RSUs can be connected to each other through wired connections or the Internet. The RSUs work as gateways to deliver data from the TA to roadside vehicles, and vice versa. The range of an RSU-to-vehicle communication can be larger than that of the V2V and vehicle-to-RSU communications to improve the network availability and performance [81].

Smart vehicles equipped with OBU, sensors, and Global Positioning System (GPS) move along the roads and communicate with other vehicles and RSUs according to a defined Intelligent Transportation Systems Radio Service (ITS-RS) standard, such as the

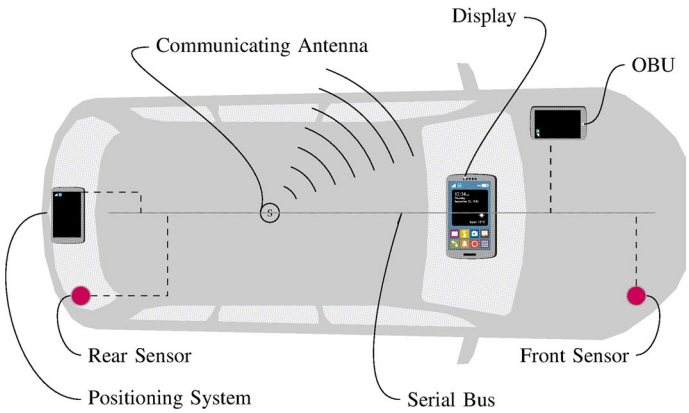

Fig. 2 Envisioned smart vehicle prototype

Dedicated Short-Range Communications (DSRC) protocol [81]. A Tamper Proof Device (TPD) is embedded in each OBU to store the user inaccessible cryptographic keying materials involved in cryptographic operations. Moreover, each vehicle has a unique barcode/identifier that can be known to the DOT. Figure 2 illustrates an envisioned smart vehicle prototype.

3.3 VANETs applications

Communications in VANETs aim to exchange information, such as traffic issues and road conditions. Thus, a wide range of applications can be deployed in VANETs. A potential classification of applications for VANET based on the safety objectives has classes, including: safety-critical, safety-related, and non-safety applications.

A Safety-critical application

Safety-critical applications (also known as latency critical) are the most important applications for hazardous situations, where the danger is high or imminent (e.g., intersection collision warning). Vehicles periodically (automatically at regular intervals) broadcast messages about events in their vicinity, such as collisions, road conditions, and emergency braking. The receiver vehicle can collect relevant information and inform the human driver about relevant events, depending on the context and situation. For this case, the communication requires high reliability and low latency to realize the safety function. The communication technology used in these applications can be V2V, V2I, and I2V. The latency required for most safety-critical applications is 100 ms (minimum update rate of 10 Hz) in a communication range of 150 to 500 m [7]. The system utility requires vehicles to receive updated information from surrounding vehicles within the required time frame before sending out a new safety message.

B Safety-related applications

Safety-related applications are event-driven (the transmission is triggered by an event) and are used in cases where the latency requirements are not as stringent as for safety-critical applications, and the danger is low, but still foreseeable (e.g., post-crash warning). The communication technology used in these applications can be V2V, V2I, and I2V. The latency required for most safety-related applications is between 500 and 1000 ms (update rate of 1 Hz) in a communication range of 250 to 1000 m [7]. The mechanisms

to generate safety-related messages are quite different than the other two classes. First, a vehicle's sensor detects an event, and local sensor information is aggregated. Then, in the case of a dangerous event, a message will be generated and broadcast by the vehicle. Also, a single car may not able to detect events such as traffic jam, which needs multiple cars location information to conclude that it is in or before a traffic jam. This example makes it easy to understand that matching the information received from different vehicles is critical for reliability.

C Non-safety applications

Non-safety applications provide periodic or event-driven traffic information and enhance driving comfort, such as traffic updates, electronic toll collection, and infotainment (the Internet, media, and entertainment). For example, information download at service stations or public hotspots, which can be served freely, or require a service subscription or a one-time payment. The latency required for most non-safety applications is 1000 ms (update rate of 1 Hz) in a communication range of 100 to 400 m [7]. The communication technology used in these applications can be V2V, V2I, and I2V. These services access the channels in the communication system in a low priority mode compared to safety-critical and safety-related applications [7]. A high priority message may contain crucial information regarding a crash that is about to occur.

In a VANET system, each safety message can carry information such as location, current time, direction of travel, speed, braking status, steering angle, turning signal, acceleration/deceleration, traffic conditions, and traffic events. RSUs can assist drivers in finding service centers, for example restaurants or gas stations, and broadcast traffic-related messages through V2I communications. For instance, a traffic light can remotely inform a vehicle about how many seconds are left before it turns to yellow or red. These advance-warning signs may be helpful to those drivers who are driving in bad weather conditions or unfamiliar areas.

However, when a vehicle's status and location information is linked to an identifiable individual, the data becomes personal information that may affect privacy. Thus, it is important to protect personal information during information exchange in the VANET applications. This issue is explained in detail in Sect. 4.4.

3.4 C-ITS standards

A standard is a document that provides specifications, requirements, guidelines or characteristics that may be used to make sure that materials, processes, products and services are fit for their purpose. The C-ITS standards are required for infrastructure and are intended to enable vehicles to talk to one another in an interoperable way [82]. The C-ITS criteria are required to specify general components such as:

- Which entities communicate, and to whom (e.g., vehicle, pedestrian, roadside infrastructure, central servers)
- What message set is used inside the communication
- What media and channel allocation (if applicable) is utilized (e.g., 5.9 GHz and the applicable station allocation)
- Which protocol is used (e.g., IPv6)

- What software is used, and how it is implemented.

Due to the VANETs highly dynamic topology and high data rate requirements, designing a proper protocol and application to use for message exchange in such environments is a challenging task. The Institute of Electrical and Electronics Engineers (IEEE) in USA, the European Telecommunications Standards Institute (ETSI) in Europe, and Association of Radio Industries and Businesses (ARIB) in Japan are the most well-known sources for defining C-ITS standards. The standards establish communication rules which assure transportation agencies that components from different manufacturers will work together. Results include efficiency, compatibility and interoperability, security, and mobility within the industry [82]. Some ITS standards are adopted around the world. Numerous countries and areas (e.g., European Union) are now developing the C-ITS platforms for deployment. The developments are emerging in Europe [83], the USA [3], and Japan [84].

Standards published by technical groups such as IEEE 802.11p, IEEE 1609, ETSI, and ARIB STD-T109 are intended to help VANETs to reduce transportation problems such as traffic congestion and traffic accidents. This section reviews the standards to understand the current state and progress of the development technologies behind the research problem.

A IEEE 802.11p

One of the most important standards is IEEE 802.11p [85] which is an amendment of IEEE 802.11 Wireless Local Area Network (WLAN) standard to support vehicular communications. It has different characteristics than usual wireless communications, for example short connection times. It uses IEEE 802.11a conventional Orthogonal Frequency Division Multiplexing-based (OFDM-based) physical layer and high quality of service improvements of IEEE 802.11e to work in high-performance systems. The Physical layer (PHY) and wireless LAN Medium Access Control layer (MAC) specifications are defined in the original IEEE 802.11p standard, published in 1997. The fundamental access method for the MAC realization is Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). Three different propagation modes are defined in IEEE 802.11 standard, including 2.4 GHz Frequency-Hopping Spread Spectrum (FHSS), the 2.4 GHz Direct Sequence Spread Spectrum (DSSS) and the infrared system [86]. The IEEE 802.11p utilizes an Enhanced Distributed Channel Access (EDCA) MAC sublayer protocol built into IEEE 802.11e, with a few modifications to the transmission parameters.

B C-ITS standard in the U.S.

IEEE 1609 standard has defined the first version of WAVE protocol stack using IEEE 802.11p. The WAVE protocol [81] reserves bandwidth of 75 MegaHertz (MHz) (in frequency range 5.850 to 5.925 GHz) to use in the U.S. DSRC spectrum band, known as Intelligent Transportation Systems Radio Service (ITS-RS). The 75 MHz band includes one central Control Channel (CCH) and Six Service Channels (SCH).

C C-ITS standard in Europe

IEEE 802.11p as an access layer is used in the European ETSI ITS-G5 family of standards [87, 88] to provide V2V and V2I communications. It describes the PHY and MAC sub-layer of ITS stations operating in the 5.9 GHz frequency band, covering

the G5A in frequency range 5.875 GHz to 5.905 GHz (dedicated for safety and safety-related applications), the G5B in frequency range 5.855 GHz to 5.875 GHz, and the G5C in frequency range 5.470 GHz to 5.725 GHz (for other applications). The PHY layer of G5A defines three 10 MHz channels including CCH, SCH1 and SCH2. Unlike IEEE 1609, ITS G5 uses a model including state machines and different tunable parameters to control MAC.

D C-ITS standard in Japan

In parallel to the American and European C-ITS standards, the Japanese ARIB STD-T109 [89] mandates operating of ITS in the 700 MHz frequency band to inform vehicles and drivers about traffic status in order to reduce the number of traffic accidents. ARIB STD-T109 specifies a PHY similar to IEEE 802.11p, but operating on a center frequency of 760 MHz. The MAC layer described in this standard employs Time Division Multiple Access (TDMA) protocol to ensure that all the vehicles have enough time to send safety messages without collision and delay.

E C-ITS security standards

The IEEE 1609.2 security standard [90] describes security services for applications and messages in the vehicular environments. It specifies use of the MACs [91] and ECDSA [70], as specified in the (U.S.) *Federal Information Processing Standard* (FIPS) 186-4 [92] to authenticate messages. IEEE 1609.2 also specifies use of ECDSA or ECQV [76] to ensure that a legitimate entity of VANET is the source of data communicated. Both the ECDSA and ECQV algorithms rely on ECC, as described by Koblitz [71] and Miller [72]. For any offered data, the Secure Hash Algorithms (SHA) approved to use in this standard are SHA-256 and SHA-384, as specified in the FIPS 180-4 [93]. However, the issues related to authentication, such as defining driver identification, and privacy protection are not addressed in the current IEEE 1609.2 standard, and left many open problems.

There are several different standards covering selection of curves to use in ECC, such as the National Institute of Standards and Technology (NIST) and the Brainpool Standard Curves and Curve Generation (Brainpool). These standards define three elliptic curves for the cryptographic processes, including: NIST P-256, BrainpoolP256r1, and BrainpoolP384r1 [94, 95].

The IEEE 1609.2 recommends these curves to use in the vehicular environments, and restricts the secret key size to become 256 bits (for NIST P-256 and BrainpoolP256r1) and 384 bits for (BrainpoolP384r1). Many security standards such as European ETSI TS 103 097 reference IEEE 1609.2 to ensure that the connected vehicles will operate safely, securely and efficiently.

3.5 Vehicular network simulation tools

Experimental studies on VANETs require the use of a mobility modeling tool to simulate vehicle movement patterns. For example, the commercial simulation software VISSIM [96] can be used together with a network simulator, such as the network simulator 3 (ns-3) [97] to model VANET communications. The purpose for using simulation tools is to evaluate communication performance in situations very similar to real-world scenarios, and to highlight existing issues.

Veins *Vehicles in Network Simulation* [98] is an open source vehicular network simulation framework. The Veins contains a fully functioning implementation of IEEE 802.11p

[99]. It relies on fully detailed models of IEEE 1609.4 DSRC/WAVE network layers, including noise and interference effects, and is frequently used in academic research. As of today, over 1100 publications relied on the Veins, such as the simulation study presented by Baee et al. [17]. The Veins utilizes the models provided in the OMNeT++ discrete event simulator [100] and SUMO *Simulation of Urban Mobility* [101] for network simulation and vehicular movement, respectively.

By contrast with ns-3, OMNeT++ has very good visualization support. It also provides high level architecture, and allows the interaction between SUMO and other network simulators.

Unlike the VISSIM, SUMO is free and open source software. It is highly portable, and allows simulations of multi-modal traffic in city-scale networks efficiently [102].

4 Authentication in VANETs

One of the main security requirements for VANETs is message authentication. This ensures that the received safety messages were generated by a trusted source, and have not been tampered with or altered after generation. In a VANET system, each vehicle broadcasts periodic safety messages to let other vehicles know about environmental conditions and their neighboring vehicles. Each safety message can carry critical information such as location, speed, braking status, traffic conditions, and traffic events. Any malicious activity, such as alteration and replaying of the disseminated messages, can be disastrous to drivers. Thus, it is necessary to ensure that the received safety messages come from legitimate vehicles, and are not altered by attackers. Also, a sender can later deny the message generation.

In this section, the security attacks on authentication and the related security requirements are discussed. The section also looks into efficient authentication requirements of VANETs, because cryptographic operations are compute-intensive and do have an impact on overall application performance. Most of the VANET safety applications are low latency (100 ms). Thus, an efficient mechanism required to authenticate received messages in a short period (100 ms), before broadcasting a new safety message.

4.1 Threats and attacks in VANETs

Threats exist for communication necessary for the VANETs operation. Malicious vehicles can make use of VANET to broadcast fraudulent messages to other vehicles in the vicinity for their own profit, or just to jeopardize the traffic system. Hence, the system must be designed to ensure that the transmission comes from a trusted source and has not been tampered with since transmission. We define a node to be adversary if it captures, injects, or deliberately alters any messages [103]. The most often encountered attacks concerning authentication are outlined as follows [13]:

- GPS spoofing attack: A location table containing the geographic location information about all the vehicles in the VANETs is saved in the GPS satellite. A GPS satellite simulator may be used by an attacker to generate false GPS signals, which are stronger than those generated by the actual satellite system. The attacker deceives the nodes by giving falsified GPS coordinates. Thus, the nodes position themselves in wrong locations.

- Replay attack: This attack is known as a play back attack (also known as re-transmitted or postponed attack) where a message is captured, and is replayed at a later time or in a different location. The VANET requires resources such as memory and time to compare and verify new and previously received messages.
- Free-riding attack: This attack is created through a malicious user who pretends to participate in cooperative authentication by incorporating neighbor users authentication attempts into its own integrated message authentication tag. By utilizing this attack, the forged authentication tag is verifiable by others while the malicious user does not actually contribute in the authentication of any original message [22, 104].
- Impersonation attack: By utilizing a fake or stolen identity of a valid user, an attacker gets the privilege of an authenticated user inside the VANET and can perform many malicious activities. For example, an attacker cheats the valid nodes to reduce their speed by pretending to be an emergency vehicle.
- Computational Denial of Service (DoS) attack: Where a receiver is flooded with invalid authentication requests (e.g., digital signatures) designed to consume the vehicles computing resources.
- Message tampering attack: The attacker sends fake response or counterfeit requests by altering exchanged messages in the VANET communications [105].

4.2 Authentication requirements in VANETs

A safety message has to be authenticated at two levels, including node level, and the message level. Node level authentication refers to entity authentication (identification), and ensures that the safety message is received from a legitimate vehicle. The message level authentication or data-origin authentication ensures the integrity of a message, and plays an important role in enhancing security in VANET [8]. For the interested reader, additional information related to message authentication is presented in Sect. 2.1.

In summary, to ensure security against those threats and attacks, the following requirements must be satisfied [14, 106]:

1 Entity authentication, to verify legitimacy of sender vehicle.
2 Message authentication, to detect message tampering and ensure data consistency.
3 Non-repudiation, to ensure the sender of a message cannot deny the message transmission.

4.3 Efficiency requirements for VANETs authentication

The embedded OBUs in vehicles use processors with limited computation ability to make VANETs economically viable. Therefore, the cryptographic operations used in VANETs should perform limited computational overhead (should be lightweight) [54]. The most important requirements for supplying efficient and dependable authentication [105] are listed below:

- Overhead: For verifying an authentication request, the number of cryptographic operations to be performed by RSU or from an automobile node or TA should be minimized.
- Bandwidth utilization: The bandwidth needs to be effectively used by vehicles (in bytes per second) for an authentication request, in the case of exchanging cryptographic keys and credentials.
- Response time: The time taken to respond to an authentication request must be reduced.
- Reliability: Authentication methods need to be stiff enough against attackers.
- Scalability: Authentication mechanism should be scalable.

4.4 Privacy-preserving authentication in VANETs

This section outlines the information privacy and its importance in VC systems and VANETs.

A Information privacy

Westin [107] explains *"privacy is the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others"*. Schoeman [108] explains privacy as *"control we have over information about ourselves"*.

Information privacy refers to control of personal information. For systems containing private information, it is important to assess the risks associated with collection, use and disclosure of that information. Personal information refers to information which is directly linked to an identifiable individual.

Private information can be a name, address, driver's license, or license plate and registration [109]. Personal information can also lead to an identifiable individual when combined.

B The importance of privacy in VANETs

In VANETs, vehicles broadcast unencrypted messages on a regular basis, containing a Vehicle Identifier Number (VIN) along with the vehicle's location information (using GPS), speed, and direction of traveling [110].

In a VANET system, protection of driver's identity should be guaranteed [111, 112]. Identity Privacy in VANETs refers to the ability to prevent others from learning and linking an identifier to a driver/vehicle. An adversary can capture communications and link the identifiers to specific vehicles, and consequently to the drivers (ID disclosure), providing a means for surveillance. The vehicle size attribute, acceleration, speed, steering angle, and position within a beacon message helps an observer to decide which beacon to link to a single vehicle. For example, in areas where a specific size vehicle is not frequent, two beacons can be linked to a single vehicle with high confidence [113].

From a legal perspective, it can be assumed that information privacy will not be harmed if there is no personally identifiable information [114]. However, many proposals for securing VANETs demonstrated that in some circumstances, non-personally identifiable information can be linked to individuals and transformed into personally identifiable information.

It is possible for an adversary to track a vehicle by installing cameras or physical tracking equipment on the road. Also, it is possible for an adversary to follow a vehicle using another vehicle to discover the driver's location. Such physical attacks may only trace specific targets, and are much more expensive than capturing the communications in VANETs [115]. This research addresses the issue associated with malicious capturing of wireless traffic in the VANET communications. The knowledge of a driver's route, or tracking a vehicle based on Radio Frequency Fingerprinting (RF Fingerprinting) [116] are outside the scope of this research.

C Privacy issues in VANETs

Privacy can often conflict with authentication requirements. A unique identifier (e.g., the VIN) is provided to a vehicle for authentication purposes. The fact is that sensitive personal information, such as the locations of our home, office, and other places can be revealed by tracking our vehicles using the shared critical information and the unique identifiers for authentication.

This vehicle unique identifier can be associated with an identifiable individual (e.g., driver or vehicle owner). In this case, the data becomes personal information whose protection and confidentiality would fall under stringent requirements. This is important in terms of information privacy. An adversary can capture the communications and link the identifiers to the vehicles, and consequently to the drivers (ID disclosure).

To avoid this, protection of the driver's identity during authentication must be guaranteed. A mechanism is required to provide message anonymity while also enabling identification by a trusted party (e.g., the department of motor vehicles or the department of transportation). For example, a government transportation authority or a vehicle manufacturer in liability-related cases may trace a vehicle that disrupts the network. In this case, a driver profile may be fetched to be used for legitimate reasons, such as providing emergency services or law enforcement with appropriate information. Designing an authentication mechanism that preserves driver privacy and also tracks dishonest vehicles is a major challenge.

The beacon content confidentiality is another concern. The vehicle size attribute, acceleration, speed, steering angle, and position within a beacon message helps an observer to decide which beacon to link to a single vehicle. For example, in areas where a specific size vehicle is not frequent, two beacons can be linked to a single vehicle with high confidence [113].

4.5 Key management in VANETs

A cryptographic system requires key-management techniques to control the distribution, use, update, and revocation of cryptographic keys, as well as protocols to manage certificates in certificate-based systems. The embedded OBU in a vehicle requires a key-management mechanism in which a number of properties should be fulfilled [54]. Ideally, an OBU key-management mechanism should provide the following desirable properties:

1. Long-term Unlinkability: A basic privacy requirement is that it should be impossible for any observer to learn if a specific vehicle has transmitted or will transmit a message (more generally, take an action according to a VC protocol), and it should

be impossible to link any two or more messages sent from the same vehicle [117]. If an observer tried to guess which vehicle transmitted a particular message, there should be only a low probability of linking a vehicle's actions or identifying it among the set of all vehicles. Messages contain parameters for identification of their senders (authentication), and messages generated by the same vehicle should be difficult to link to each other [118]. The digital certificates used for authentication purpose can lack identifying information. Regarding this important issue, public keys should change in such a way that an eavesdropper cannot link an old key with a new key.

2. Traceability and Revocation: In VC systems, each vehicle relies on messages received from other vehicles. To satisfy the aforementioned requirements in authentication, a mechanism should be designed that keeps messages to be anonymous to other vehicles, while enables identification by CA in liability-related cases to trace an OBU that abuses the VANET. In addition, once a malicious OBU has been detected, the authority should efficiently notify the VANET to revoke the misbehaving OBU's identifier (to prevent any further damage).
3. Efficiency: The embedded OBUs in vehicles use processors with limited computation ability to make VANETs economically viable. Therefore, the cryptographic operations used in VANETs should perform limited computational overhead (should be lightweight) [54].
4. Perfect Forward Secrecy: If a cryptographic secret key for current session is revealed, an adversary must be unable to use this to recover past and future ciphertexts [10, §12.16]. An authentication protocol needs a mechanism to automatically and frequently regenerate the keys it uses, such that if the latest key is compromised, it exposes only a small portion of sensitive data. A protocol is vulnerable to a known-key attack if perfect forward secrecy is not provided. Hence, compromise of past session keys allows an adversary to compromise future session keys [10, §12.17]. The more frequently the keys are updated, the less data is processed with any given key, and as a result, the less impact the leak will have. This is regardless of the purpose of the key (e.g., authentication, or encryption).

5 Existing classifications for authentication in VANETs

Several existing studies [62–69] attempt to classify existing authentication schemes in vehicular networks. These works are reviewed in this section.

Hasrouny et al. [66] present an extensive overview of the most of VANET security challenges and their causes as well as the existing solutions in a comprehensive manner. They review the recent security architectures, the security standards, and multiple security protocols in detail. However, they focus on the classification of the different attacks on vehicular communications and their corresponding solutions.

Singh et al. [68] survey the state of the art architecture, applications, emerging radio access technologies, standardization, and project activities, as well as reviewing the protocol stacks of the ITS in the USA, Japan, and Europe. Their work is presented as a tutorial in the emerging radio access technologies for connected and autonomous vehicles and their associated challenges.

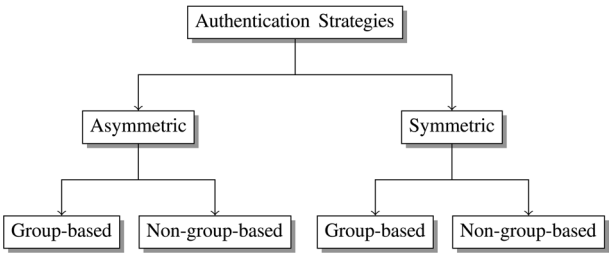

Fig. 3 Classification based on Riley et al. [62]

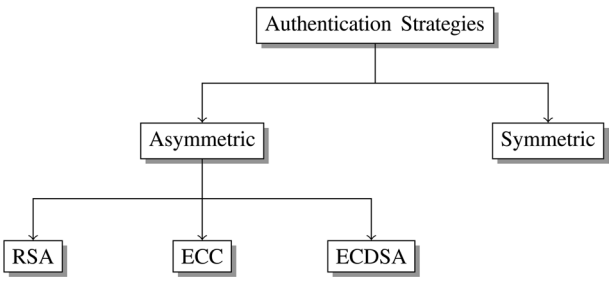

Fig. 4 Classification based on Qu et al. [63]

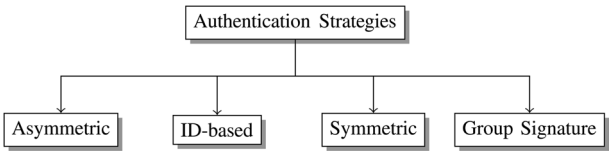

Fig. 5 Classification based on Petit et al. [64]

Manivannan et al. [69] classify multiple authentication schemes into two categories based on the problems addressed and the techniques used to solve these problems, and discuss their strengths and weaknesses.

Riley et al. [62] examine several proposed authentication schemes and classify them using two criteria. Firstly, they note the type of cryptographic algorithm the schemes use: symmetric or asymmetric. Then, each of these categories is divided into two subcategories: group-based schemes and non-group-based schemes (refer to Fig. 3).

Qu et al. [63] survey authentication protocols and also classify the schemes according to the type of cryptographic algorithms involved: symmetric or asymmetric (refer to Fig. 4). However, both of the classification schemes Riley et al. [62] and Qu et al. [63] rely on the computational complexity of cryptographic approaches.

Petit et al. [64] classify authentication schemes into one of four categories: asymmetric, symmetric, group signature, and identity-based. However, this single layer structure fails connect the identity-based and group signature approaches to asymmetric cryptography, which is the underlying primitive in both cases (refer to Fig. 5).

Manvi et al. [65] classify authentication strategies into three main categories: cryptography, signature, and verification. Each of these categories is further divided into several

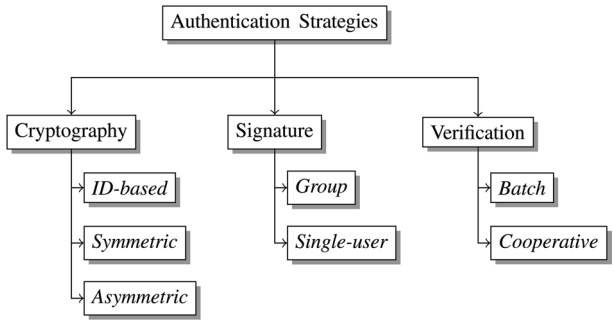

Fig. 6 Classification based on Manvi et al. [65]

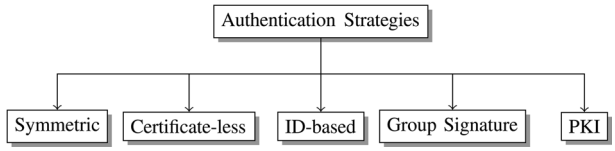

Fig. 7 Classification based on Lu et al. [67]

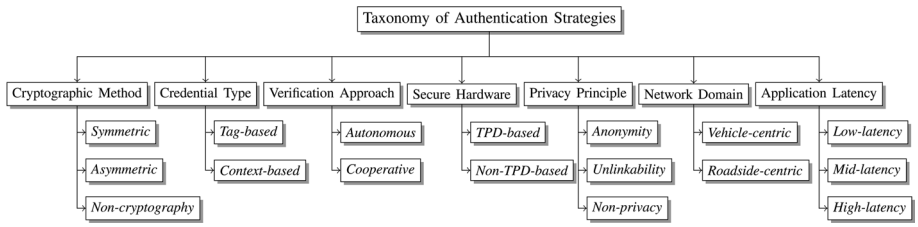

Fig. 8 Classification based on this paper

different subcategories such as asymmetric, group signature, and batch verification. Similar to [64], this structure does not include the identity-based approach as a subcategory of the asymmetric cryptography category (refer to Fig. 6).

Lu et al. [67] classify authentication schemes into five categories based on the mechanism used: symmetric cryptography, Public-Key Infrastructure (PKI), identity-based signature, certificate-less signature, and group signature. This single layer structure does not group identity-based and certificate-less approaches in the same category, although both are certificate-less strategies (refer to Fig. 7).

The classification schemes reviewed in this section categorize authentication protocols based on just a few criteria. They are mainly based on the underlying cryptographic technique used, or they fail to make connections between different important aspects of authentication, such as digital signatures. These gaps are filled in this research by providing a generic and comprehensive taxonomy that enables identifying common structural elements for each class. Based on this taxonomy, a framework is generated to facilitate design, analysis, and comparisons of new and existing protocols.

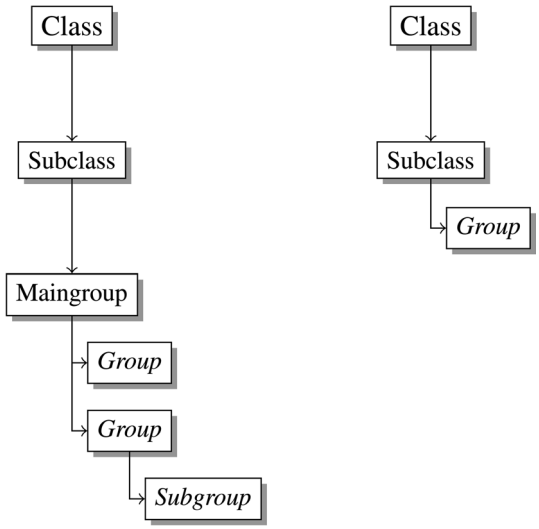

Fig. 9 The structures used in our taxonomy

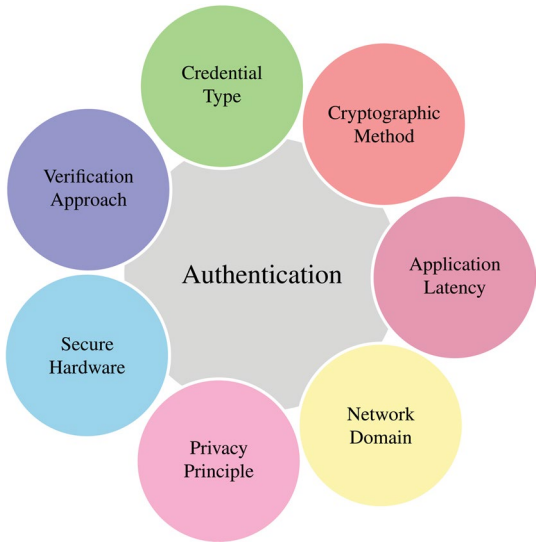

Fig. 10 The seven criteria, which are the bases for our taxonomy

6 The proposed taxonomy of authentication strategies in VC systems

This section presents a comprehensive taxonomy, based on seven criteria (as shown in Fig. 8): cryptographic method, credential type, verification approach, secure hardware, privacy principle, network domain, and application latency (see Fig. 10). These criteria are derived from observations of many authentication protocols. The following structures are used to describe the taxonomy. Each criterion is a class comprising at least a subclass, and group (or main group with subgroup), as shown in Fig. 9.

The first criterion of this taxonomy recognizes the cryptographic method used for authentication. In VC systems, cryptographic primitives can be applied to solve many authentication issues, such as message manipulation. Cryptographic algorithms can be

used for different purposes, such as identification and message authentication. For the interested reader, additional information related to cryptography and authentication is presented in Sect. 2. There are three cryptographic method subclasses: symmetric, asymmetric, and non-cryptography.

The second criterion is based on the credential type used for authentication. A credential is a unique possession provided to a communicating node to be used as a proof of identity to identify the node as authentic with high confidence. There are two subclasses: tag-based and context-based.

The third criterion is based on the verification approach used to verify (or reject) an authentication request in the network. Vehicles can authenticate each authentication request independently, or rely on information from other communicating nodes to make an authentication decision. There are two subclasses: autonomous and cooperative.

The fourth criterion of this taxonomy is based on the hardware requirements for authentication. Some schemes rely on a Tamper Proof Device (TPD) to store and protect cryptographic keying materials, while others do not. Based on that, protocols can be classified into two subclasses: TPD-based and Non-TPD-based.

The fifth criterion of this taxonomy is the privacy principle. Authentication protocols use different approaches to provide conditional privacy for vehicles/drivers in VC systems. For both identification and message authentication, protection of the driver's identity during authentication should be guaranteed. Identity privacy refers to the ability to prevent others from learning and linking a VC system identifier to a driver/vehicle. When a unique identifier is provided to a vehicle and its embedded communicating nodes for authentication purpose, this information can be associated with an identifiable individual. In this case, the data becomes personal information. An adversary can capture the communications and link the identifiers to the vehicles, and consequently to the drivers (ID disclosure), providing a means for surveillance. Based on the principle used, the class categorizes authentication strategies into one of three subclasses: anonymity, unlinkability, and non-privacy.

The sixth criterion is based on the network domain. The domains may be either intra-vehicle, inter-vehicle, or vehicle-RSU. A protocol is designed to provide authentication in a specific network domain, and may not be applicable to other domains. For example, an intra-vehicle protocol authenticates different communicating parts within a vehicle, but may not be applied for inter-vehicle authentication. There are two subclasses: vehicle-centric and roadside-centric.

The seventh criterion is based on the application latency for which the scheme can be used. Latency defines the time frame from when information is generated for transmission and when it is received. Different applications have different latency requirements. Examples include safety-critical, safety-related, or non-safety applications. Some protocols may satisfy the latency required by a non-safety application, but may not be fast enough to be used in safety-critical applications. Authentication protocols can be classified into three subclasses: low-latency, mid-latency, and high-latency, based on application time.

There may be other criteria in the literature for classification of authentication strategies in VC systems. The taxonomy includes the most important authentication criteria,

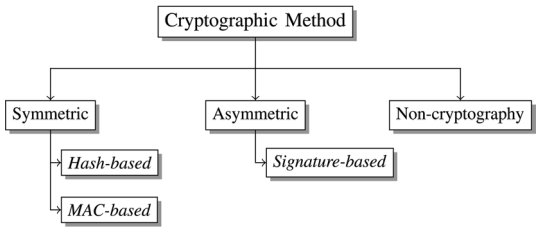

Fig. 11 Cryptographic method class in expanded form

and will enable classification of a variety of protocols in the public literature and future proposals.

6.1 Cryptographic method class

This class recognizes the cryptographic method used for authentication. There are three subclasses: symmetric, asymmetric, and non-cryptography. Figure 11 shows the cryptographic method class in expanded form.

A Symmetric subclass

The first subclass is those authentication schemes relying on symmetric cryptographic primitives. Symmetric algorithms make use of a secret key, and both sender and recipient perform message encryption and message decryption operations using the same secret key. One of the main drawbacks of the application of symmetric techniques is the secure distribution of secret keys to nodes in vehicular networks. As any communicating node with knowledge of the secret keys can decrypt the message, it is vital to prevent keys from falling into the wrong hands. The symmetric subclass can be further classified into two groups: Hash-based and MAC-based.

A.1 Hash-based group

This group of protocols perform authentication using hash functions. A cryptographic hash function is a one-way function (infeasible to invert) that is used for data integrity assurance. It takes a message as input and produces an output referred to as a hash value. A cryptographic hash implies an unkeyed hash function. The study presented by Han et al. [36] proposes a three-step authentication protocol using cryptographic hash value to provide data integrity assurance between the intra-vehicle network and an external network (mobile device).

A.2 MAC-based group

This group of protocols under symmetric subclass perform authentication using a distinct class of cryptographic primitives called Message Authentication Codes (MACs). The output of a MAC algorithm is referred to as a MAC, and is a short piece of information used to confirm that a message comes from the stated sender (its authenticity), and has not been changed [10] (refer to Sect. 2.1).

Different symmetric cryptographic primitives such as cryptographic hash functions, or block cipher algorithms can be used to construct MAC algorithms. An HMAC implies a keyed-hash function that takes two functionally distinct inputs, a message and a secret key, and produces a fixed-size output. In practice, it should be infeasible to produce the same output without knowledge of the key [10].

HMACs can be constructed from dedicated cryptographic hash functions, such as SHA-256 or SHA3-256 secure hash algorithms. In VANETs, HMACs can provide both data integrity assurance and symmetric data origin authentication, as well as identification in symmetric-key schemes. Note that any communicating node with knowledge of shared secret key can be an originator of data (refer to Sect. 2.1). Hence, it does not offer non-repudiation.

Hash-based authentication is highly efficient in terms of computational and communication overhead. It offers the benefits of short generation and verification time as well as less communication overhead. The security of HMACs depends on the cryptographic strength of the underlying hash function, and the size and quality of the key used [10]. An example of this is the authentication protocol proposed by Choi et al. [37] that enables vehicles and RSUs to generate/verify MACs in V2I/I2V communications, resulting in less reliance on availability of bandwidth, and high degree of efficiency.

Wang et al. [31] propose *A Two-Factor Lightweight Privacy Preserving Authentication Scheme for VANET*, named 2FLIP. In 2FLIP, all vehicles are equipped with a same copy of system key to generate MACs on the broadcast messages. Recipient TPDs can verify the messages by creating MACs of the received messages with the same system key. This only requires one hash computation and one MAC operation to accomplish the message verification. Hence, the protocol is very efficient in terms of computation. However, the same copy of system key must be stored in all TPDs. This viewed as a single point of failure [34]. If a single vehicle's system key is compromised, all vehicles in the network will be affected, and all will need to be updated with a new system key. However, a CA encrypts a new system key under the previous system key. In case of compromise of past system key, the new system key is very easily compromised (see [10, §12.2.3] regarding perfect forward secrecy and known-key attacks).

Huang et al. [34] propose a similar efficient scheme to address the system-key problem in the scheme presented by Wang et al. [31]. However, the scheme is not scalable. For a new vehicle that joins into the network, the TA generates a list of pseudo identifiers along with a list of hashed values of the pseudo identifiers, and sends to the vehicle. Then, the TA updates all other vehicles with the hash of pseudo identifiers that are generated for the new vehicle. This means that all vehicles must store each other's hashed values of pseudo identifiers. In case of a revocation, all vehicles must be updated with a new list of pseudo identifiers and hashed values.

Recently, Camenisch et al. [35] introduce the novel concept of zone encryption as a practical means to authentically and confidentially transmit data in vehicular communications. The zone encryption idea relies on symmetric authenticated encryption using temporary keys that are exchanged among vehicles. However, the scheme does not provide non-repudiation in V2V communication, and as a result, no proper traceability and revocation could be performed in case of malicious activity.

B Asymmetric subclass

The second subclass relies on asymmetric cryptographic primitives. Asymmetric algorithms make use of two mathematically related keys (a key pair), referred as a public key, and a private key. Any sender node can encrypt a message using the receiver's public key. The corresponding private key must be kept secret, only known by the receiver.

Any message encrypted using a public key can only be decrypted by applying the same algorithm and the matching private key. This method can be used to provide confidentiality, and thus securely distribute symmetric secret keys over vehicular networks. Asymmetric techniques can also be used for authentication [10]. Asymmetric cryptographic primitives require far more processing power for both encryption and decryption, and as a result, they are slower than symmetric techniques. The asymmetric subclass can be further divided into signature-based Group.

B.1 Signature-based group

This group of protocols provides authentication using digital signatures. In cryptography, a digital signature is a number generated from the content of a message using an algorithm and a private key that is known only to the signer. The signature must be verifiable using the corresponding public key [10]. In VC systems, digital signatures are used to ensure authentication, data integrity, non-repudiation, and for certification of public keys. In this regard, many studies propose authentication mechanisms using digital signature schemes.

Johnson et al. [70] proposed the ECDSA scheme which is a digital signature algorithm based on ECC. Gollan and Meinel [11] propose the use of digital signatures for authentication in vehicular environments. To use in vehicular communications, each message broadcast/sent is signed. Recipients must verify the signatures before accepting the messages. Raya and Hubaux [14] show that in terms of speed and compactness, ECDSA is fit for message authentication in V2V communications.

However, Baee et al. [17] demonstrate that care is needed when using the ECDSA for authentication of a high volume of received messages and credentials in V2V communication. The verification results in a delay in driver notification and allows insufficient driver reaction time, resulting in potential collisions and serious injuries (assuming the driver does not react independently).

There are other types of signature schemes used for authentication in VC systems. The group signature scheme applied by Calandriello et al. [25], ring signature scheme applied by Xiong et al. [38], and blind signature scheme applied by Fischer et al. [39] are other examples that fall into signature-based subclass.

C Non-cryptography subclass

Protocols in this subclass do not employ any cryptographic mechanism to provide authentication, and the network nodes do not perform basic input validation, which raises the possibility of remote spoofing of the messages transmitted. The study presented by Rouf et al. [40] experimentally validated that several protocols for state-of-the-art commercial tire pressure monitoring systems do not employ cryptographic authentication. Authors showed that using a customized software radio attack platform located in a nearby vehicle they can easily trigger the tire pressure warning messages in a moving vehicle.

6.2 Credential type class

This class recognizes the type of credential used for authentication. There are two subclasses: tag-based and context-based. Figure 12 shows the credential type class in expanded form.

A Tag-based subclass

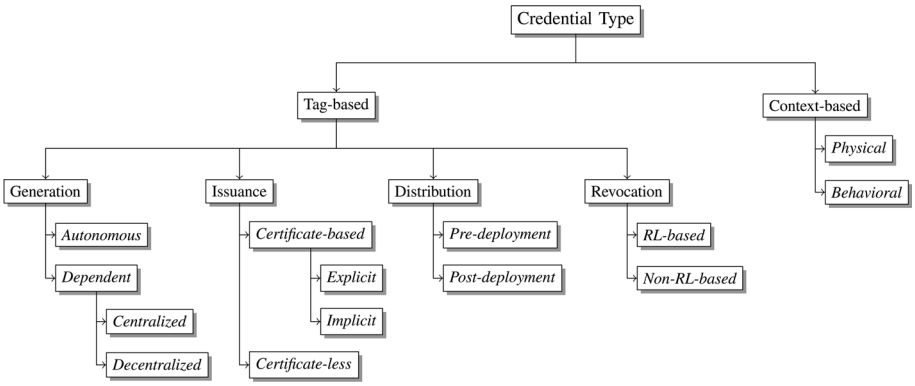

Fig. 12 Credential type class in expanded form

In this subclass, the credential can take the form of a key (for example, a public key) that is known to be unique to a network communicating node, and used for establishing its identity when communicating with other nodes. Any node holding a credential is usually given secret knowledge (e.g., a private or secret key) as proof of owning that credential. A node that wishes to communicate to the other nodes in the network is referred to as a *supplicant*. A node that receives and responds to the authentication requests is referred to as an *authenticator*. The supplicant can assure the authenticator about its credential (identity) if it is certain that the supplicant possesses a cryptographic private/secret key corresponding to that credential. Four main groups are defined under this subclass based on the process applied: credential generation, credential issuance, credential distribution, and credential revocation. Each main group can be further classified into different groups as follows.

A.1 Generation main group

This main group categorizes authentication protocols based on the approach used to generate credentials for the communicating nodes in the network, with respect to the authentication operation. This main group can be further classified into two groups based on the party that generates the credentials (the communicating node itself or a trusted party): these are autonomous and dependent.

A.1.1 Autonomous group

In this group of authentication protocols, a node generates credentials autonomously, removing the need for recurring communication with a trusted party. The scheme presented by Calandriello et al. [25] is an example where vehicles generate certified credentials autonomously which significantly reduces the communication overhead.

A.1.2 Dependent group

Authentication protocols in this group rely on a trusted party to generate credentials. It can be a single point of trust (centralized authority), or consist of multiple entities jointly working together (decentralized authorities) [75]. In this case, the dependent group of credential generation can be further classified into two subgroups: centralized and decentralized.

A.1.2.1 Centralized subgroup

Under this group of authentication protocols, a centralized trusted authority with full knowledge of system parameters is responsible for generating credentials.

Communicating nodes send their credential requests and receive the corresponding credentials. The scheme presented by Raya and Hubaux [13] is an example where vehicles receive certified credentials from a centralized trust; a governmental transportation authority or a vehicle manufacturer. This makes management and handling of credentials easier in terms of installation, deployment, and monitoring within the network.

A.1.2.2 Decentralized subgroup

The underlying service for credential generation in this group of protocols has no central authority, and distributed trusted parties such as RSUs act as credential generators in the network. Park et al. [41] propose delegating responsibility of credential generation to the RSUs in order to reduce the communication and storage overhead on the centralized authority.

A.2 Issuance main group

This subclass categorizes authentication protocols based on the approach used to issue credentials, with respect to the authentication operation. Communicating parties can exchange their credentials for the purpose of identification. The credentials can be transferred either using certificates or without certificates. A digital certificate (also known as certificate) is an electronic document that is used to bind a credential to an entity. Credential issuance can be further classified into two groups: certificate-based, and certificate-less.

A.2.1 Certificate-based group

In this group of protocols, most common approach to convey credentials (e.g., public keys) is to use digital certificates. A certificate consists of information to identify an entity. Each entity's credential is embedded in a certificate which is either explicitly (signed by a trusted authority or self-signed) or implicitly (without attaching signature) certified. Any party can use a copy of the certificate to extract the provided credential and use it to uniquely identify the holder [10]. To provide a more accurate discrimination, certificate-based credentials can be further classified into two subgroups: explicit and implicit.

A.2.1.1 Explicit subgroup

Protocols in this subgroup rely on explicit certificates to exchange credentials. An explicit certificate is a data structure used to store, distribute, or forward credentials (e.g., public keys) over unsecured networks without fear of undetectable manipulation. It is composed of two different parts: a data part and a signature part. The data part contains a credential and a unique string identifying the associated entity. The signature part of the certificate contains the signature of the certificate owner or a trusted authority. This binds the subject entity's unique identity to the specified credential. An intended recipient can verify this signature and be assured that the credential belongs to the subject entity. During an authorized system user registration, the authentic public key of the trusted authority is made available to all communicating nodes. This public key enables communicating nodes to verify the certificates signed by that trusted authority, and as a result, transfers trust. The scheme presented by Jung et al. [42] is an example where RSUs issue multiple explicit certificates to vehicles for authentication purposes.

A.2.1.2 Implicit subgroup

Protocols in this subgroup rely on implicit certificates to exchange credentials. An implicit certificate is a variation of the digital certificates used with cryptography for which an explicit user's credential can be implicitly certified. The main difference here is that a credential must be reconstructed from public data, rather than transported within a certificate, as occurs with explicit certificates. The implicit certificate is still comprised of the three main elements/parts (identifier, public credential, and digital signature), but superimposed into the same space as the size of a public credential, resulting in reduced data transfer. The ECQV implicit certificate is an example that falls into this subgroup. The IEEE 1609.2 security standard [90] recommends use of ECQV as a more efficient alternative to traditional certificates, as described in the document *Standards for Efficient Cryptography 4* [76].

A.2.2 Certificate-less group

The second group of authentication protocols under this subclass is for schemes where credentials are not presented in certificates. Unlike the certificate-based group of protocols, these have no dependence on signed certificates. The application of identity-based cryptography and signature schemes [119, 120] is common among protocols in this group. The study presented by Kamat et al. [43] is an example of schemes that fall into this group, where vehicles implicitly validate the identity-based signatures on the messages by verifying that the vehicle using the credential actually has the private key corresponding to it. This eliminates the need for certificate exchange between vehicles, resulting in reduced communication overhead.

A.3 Distribution main group

This main group categorizes authentication protocols based on the approach used to distribute credentials to the network communicating nodes. Regardless of which party generates the credentials (communicating node or trusted party), the distribution can be further classified into two groups: pre-deployment, and post-deployment.

A.3.1 Pre-deployment group

The first group of authentication protocols under this subclass assumes that credentials are distributed to the nodes during an offline phase, before deployment. The scheme presented by Papadimitratos et al. [44] is an example that assumes authentication using a large set of pre-loaded credentials, installed in the vehicle's on-board credential pool by the transportation authority or the manufacturer, resulting in reduced V2I communication to receive new credentials and less reliance on availability of infrastructure in all regions.

A.3.2 Post-deployment group

The second group of authentication protocols under this subclass assumes that credentials are distributed to the network nodes during an online phase, after deployment. Different parties may be involved in this group of credential deployment. For example, network nodes may form a group in which a unique node is responsible for distributing the credentials to other nodes. The work presented by Sampigethaya et al. [45] is an example that enables a group manager to derive credentials by interacting with a trusted party and distribute them to new group members, resulting in reduced unnecessary overhead and redundancy in neighbors broadcast. The scheme presented by Calandriello et al. [25] is another example where vehicles issue certified credentials by themselves which significantly reduces the communication overhead.

A.4 Revocation main group

This main group categorizes authentication protocols based on the approach taken to revoke credentials, with respect to the authentication operation. Credential revocation is an essential feature of authentication protocols. It is needed because authentication information changes over time. Revocation may minimize threats associated with a compromised secret key related to a credential. It is important to stop using or trusting keying material which is no longer secure. A key is compromised if an adversary gains access to it. The revocation of credentials with long-term validity is a difficult task, as all distributed copies of the credentials must be effectively retracted. One solution for this is use of a Revocation List (RL). A RL is a list of credentials which have been revoked, provided by a trusted party. Credential revocation can be further classified into two groups: RL-based, and non-RL-based.

A.4.1 RL-based group

The first group of authentication protocols under this subclass assumes distribution of credential revocation information using RL. The RLs should be issued at regular intervals even if there are no changes, to prevent new RLs being maliciously replaced by old RLs. The scheme presented by Papadimitratos et al. [46] is an example where all vehicles can obtain the latest RL with very low bandwidth used for transmissions.

A.4.2 Non-RL-based group

An alternative approach is to issue credentials with very short lifetimes, and require frequent installation of new credentials by the credential provider. In the case of revocation, further credential certification requests are denied. The work presented by Fischer et al. [39] uses a blind signature scheme to eliminate the need for RLs, and as a result, reduces the overall memory and bandwidth consumption.

B Context-based subclass

This subclass categorizes the authentication protocols based on the contextual attribute of the supplicant. This unique attribute can be used as a credential to authenticate an entity with high confidence. Two groups are defined under this subclass: physical, and behavioral.

B.1 Physical-based group

Authentication protocols under this group try to authenticate a communicating node based on a physical characteristic that uniquely identifies it. Physical attributes, such as GPS location, Received Signal Strength Indication (RSSI), or Signal to Noise Ratio (SNR) may be needed. For example, Li and Chigan [47] assume verification based on physical distance between vehicles, to efficiently and securely verify the massive messages in VC systems.

B.2 Behavioral-based group

Authentication protocols under this group of contextual credentials attempt to authenticate a communicating node based on its behavioral pattern. A supplicant may be monitored by the authenticator based on its pattern of behavior with respect to certain functionality and performance. For example, Golle et al. [48] rely on the vehicle sensor capabilities to distinguish the nodes in the network; hence identifying malicious nodes.

6.3 Verification approach class

This class aims to recognize the nature and behavior of different authentication schemes based on the approach used to verify an authentication request. There are two subclasses: autonomous and cooperative.

A Autonomous subclass

The first subclass under the verification-approach class of authentication protocols uses an approach that enables authenticators to verify each authentication request independently, with respect to the authentication operation. This reduces dependency on other parties, but requires more computation power to verify received messages in short time frames independently. In V2V communication, Raya and Hubaux [14] assume that each vehicle needs to verify the periodically received safety messages within intervals of 100 milliseconds. Vijayakumar et al. [24] propose a batch verification method to reduce the message verification delay. However, in case of receiving an altered or modified message, an additional operation is required to find the invalid signature in the batch.

B Cooperative subclass

The second subclass of authentication protocols assumes that authenticators rely on information from other entities to make an authentication decision. This reduces the time required to authenticate a message, and as a result, increases authentication speed. The network nodes cooperatively work with each other and simultaneously authenticate transmitted messages to share their results with each other. Different parties may be involved in this group of credential deployment. For example, Zhang et al. [49] assume that vehicles work cooperatively to verify authentication requests according to their computing capacity, resulting in lower computation and communication overheads.

The schemes presented by Zhang et al. [20] and Shim [50] are another examples that assume infrastructures such as RSUs are delegated by vehicles to authenticate the received messages, and report the authentication results to the vehicles. This approach can simultaneously verify multiple authentication requests, and hence, considerably reducing the total verification time.

However, these schemes need RSUs to be pervasive, otherwise, the scheme is ineffective. Moreover, in heavy traffic conditions, the performance significantly degrades, as the RSUs need to perform authentication for a high number of messages in a short time period, and send the results back to the vehicles.

In addition, cooperative authentication protocols proposed in the studies presented by Hao et al. [21], Lin and Li [22], and Zhu et al. [23] are inefficient for broadcast authentication in the latency-critical applications. Each vehicle needs to cooperate in the message verification processes, and report its own verification results to neighboring vehicles. In heavy traffic conditions, the computational and communication delay associated with cooperative authentication could result in insufficient time for a driver to receive an alert and react, resulting in a crash. Moreover, this approach requires availability of a reasonable number of honest vehicles to cooperate in authentication. In the case of low vehicle density, these protocols may not be reliable for authentication purposes. These protocols can also be exploited by modification attacks on location information, as they select messages for verification based on location information (refer to Sect. 4.1).

6.4 Secure hardware class

This class recognizes the secure hardware requirements used to store and protect cryptographic keying material or other important cryptographic elements for providing authentication. There are two subclasses: TPD-based and Non-TPD-based.

A TPD-based subclass

This subclass of authentication protocols proposes the integration of TPDs within network nodes. Thus, cryptographic keying material can securely be stored or managed inside the nodes, and cannot easily be extracted or transferred. Trusted device-based authentication protocols have been proposed by Vijayakumar et al. [51] and Wang et al. [31], to reduce the overhead caused by authentication and revocation management.

B Non-TPD-based subclass

In contrast to the TPD-based, authentication protocols in this subclass do not rely on secure hardware for authentication purposes. The RSU-aided authentication protocols have been proposed to perform message authentication without using a trusted device [20, 52, 53]. This eliminates the costs for embedding TPDs in vehicles, and reduces the risks associated with unauthorized access to the TPDs.

6.5 Privacy principle class

Parno and Perrig [12], and Raya and Hubaux [13] identify topics associated with privacy and authentication. Through this context, many protocols have been proposed to address privacy-preserving message authentication in VC systems.

This class recognizes the principles used to mask identity to provide for driver privacy during authentication. There are three subclasses: anonymity, unlinkability, and non-privacy. Figure 13 shows the privacy principle class in expanded form.

A Anonymity subclass

This subclass contains authentication protocols used to provide anonymity for communicating nodes. Ideally, to mitigate the surveillance risk, it should be impossible for any observer to learn if a specific node has transmitted or will transmit a message. In VC systems, each node relies on messages received from other nodes. To preserve a driver's privacy during authentication, a mechanism should be employed to keep messages anonymous to other nodes. This subclass can be further categorized into two groups: pseudonym-based and group signature-based.

A.1 Pseudonym-based group

Protocols under this group rely on pseudonymous tag-based credentials. A pseudonym or alias is an alternative identity that is verified by the node itself or a trusted party.

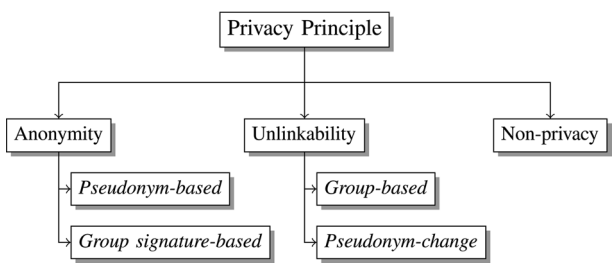

Fig. 13 Privacy principle class in expanded form

This ensures that services can be used without disclosing the driver's identity. Examples of schemes that fall into the pseudonym-based group are the studies presented by Fischer et al. [39], Calandriello et al. [25], and Jung et al. [42] that enable a vehicle to avoid being tracked by periodically creating new pseudonym certificates.

The schemes based on pseudonymous credentials achieve conditional anonymity by using pseudonym identifiers. In V2V communication, vehicles periodically sign messages using the currently active credential and broadcast them. Each broadcast message contains the resulting signature, as well as the corresponding pseudonym identifier. Once a vehicle receives the message, it can authenticate the message originator using the pseudonym identifier, without knowledge of the sender's real world identifier. This demands the use of CRLs, to manage revoked identifiers and present a protected and secured communication in VANETs. However, for anonymous communication, a static identifier is not sufficient: a vehicle using a single identifier can be very easily tracked during broadcast authentication. Thus, vehicles continuously need to be equipped with new pseudonyms to maintain anonymity.

Raya and Hubaux [14] propose a Baseline Pseudonymous (BP) authentication scheme that requires a large number of short-lived pseudonym certificates that are pre-loaded in a vehicle OBU by CA. Each broadcast message needs to be signed using a certificate from the vehicle certificate pool. A vehicle should change its anonymous certificate and private key only after having used it for a certain number of messages.

This pseudonym changing strategy alone is not sufficient for confusing an observer to link the new pseudonym to the vehicle [15]. Furthermore, the pseudonym refill frequency depends on pseudonym validity periods and pseudonym change rate. In case of a revocation, most of the pseudonyms need to be revoked. A revocation checking against CRLs needs to be performed before verification, when a vehicle receives a message from an unknown entity. The delay produced by revocation checking increases when the size of CRLs grows exponentially with the number of revoked vehicles. The delay caused by CRL transmission becomes longer as the size of CRLs becomes larger, which allows misbehaving vehicles to continuously compromise the network during this period. Besides, the CRLs should be issued at regular intervals even if there are no changes, to prevent new CRLs being maliciously replaced by old CRLs. The large communication overhead caused by broadcasting CRLs to vehicles may have negative impact on the availability of the network. Thus, most of the existing pseudonym-based authentication schemes are not scalable. A collection of schemes based on pseudonymous certificate along with their analysis concerning communication overheads is presented by Kortesniemi and Särelä [16]. For the interested reader, additional information related to the pseudonym changing strategies is presented by Boualouache et al. [121].

A.2 Group signature-based group

This group of protocols under anonymity subclass assumes that the network nodes form a group, and utilize a group-oriented signature scheme (e.g., group signature [122] or ring signature [123]) to provide anonymous authentication, while eliminating the issuance of certificates. On behalf of a group, any member of the group can sign a message using its private key, and the signature can be verified with a group-wide public key. Group-oriented signature schemes provide non-traceability,

unlinkability, and unforgeability. That is computationally infeasible for an adversary to learn whether two signatures on the message have been signed by the same group member, as only one public key is used for a group. The study presented by Studer et al. [54] is an example that uses a group signature scheme for anonymous authentication in vehicular communications.

However, in some schemes [18, 19], the CRL size of group signature is linear with the number of revoked vehicles. This would cause long authentication delays. At least two cryptographic pairing operations [124] are involved with the revocation checking. Furthermore, VANETs are highly dynamic environments and vehicles periodically join and leave highways using enter and exit ways. The distance between vehicles continuously changes and they join different groups unpredictably [17]. That is, a group leader has to continuously generate a new group public key which makes this type of schemes ineffective. In addition, the cryptographic pairing calculations used in group signature schemes are not computationally efficient for the VANETs latency-critical applications.

B Unlinkability subclass

The credentials are stripped of any identifying information. It should be impossible to link any two or more messages sent from the same node. The unlinkability property of pseudonyms prevents any observer from learning that the messages originated from a specific node. If an observer tried to guess which node transmitted a particular message, there should be only a low probability of linking a node's actions or identifying it among the set of all nodes. For example, Vijayakumar et al. [30] propose that a trusted authority generates a unique dummy identifier for each vehicle to use for authentication purposes. However, the scheme cannot satisfy the unlinkability requirement, as it allocates a single unique identifier for each vehicle.

Unlike the group signature-based protocols which provide unlinkability, protocols in this subclass utilize pseudonym-based credentials that need a strategy provide unlinkability. Based on the strategy providing unlinkable pseudonym, this subclass can be further categorized into two groups: group-based and pseudonym-change.

B.1 Group-based group

This group of protocols assumes that the network nodes form a group in which a unique node is responsible for distributing the credentials to other nodes. The scheme presented by Sampigethaya et al. [45] is an example that enables a group manager to derive credentials by interacting with a trusted party and distributing credentials to the new group members, resulting in increased driver privacy by mitigating the location tracking of vehicles.

B.2 Pseudonym-change group

Protocols under this group assume providing pseudonym unlinkability using a set or different sets of pseudonyms, where the credential holder can change pseudonyms over time or different contexts to break linkability. Examples of schemes that fall into the pseudonym-change group are the studies presented by Li et al. [55] and Lu et al. [56] that enable a vehicle to change pseudonyms with different strategies to break linkability between messages.

C Hybrid schemes

Multiple hybrid privacy-preserving authentication schemes have been proposed to secure VC systems. Hybrid schemes combine different authentication approaches, such as pseudonymous authentication protocols, digital signatures, Hashes, MACs, and other techniques to balance computational efficiency, CRL size, bandwidth consumption, and verification delay. This section briefly reviews the most relevant state-of-the-art research into hybrid authentication schemes for use in V2V communication.

A hybrid scheme is proposed by Calandriello et al. [25] that combines a pseudonym scheme with group signature. A vehicle can issue a self-signed certificate using its group private key, and then sign each message using a private key corresponding to the self-signed public-key certificate. This could reduce the average overhead of message authentication, but the expensive pairing calculations and group signature CRL checking still remains a problem.

Studer et al. [26] propose a new hybrid authentication mechanism, *VANET Authentication using Signatures and TESLA++* (VAST), which is based on ECDSA and a modified version of the *Timed Efficient Stream Loss-tolerant Authentication* (TESLA) [27]. The TESLA protocol uses symmetric cryptography with delayed key disclosure to prove the sender was the source of a message. Since symmetric cryptography has a faster computational speed compared to asymmetric cryptography, TESLA is resilient to computational DoS attacks. However, TESLA is vulnerable to memory-based DoS attacks, as receivers store data until the corresponding key is disclosed. Receivers can be flooded by malicious parties with invalid messages without a corresponding key disclosure which filled receiver's memory with junk data. Moreover, TESLA cannot provide non-repudiation, as no recipient vehicle can convince a third party that the sender indeed broadcast the message [26]. VAST is flexible, extensible, and efficient, but it does not provide privacy preservation and conditional traceability.

Lin et al. [28] suggest a pseudonymous authentication scheme named *Timed Efficient and Secure Vehicular Communication* (TSVC), which is based on TESLA [27]. In TSVC, each vehicle has to generate a hash chain and shares it with its neighboring vehicles. Then, it uses the elements of the hash chain as shared secret keys to generate MACs on the broadcast messages. The fast speed of MAC verification in TSVC can reduce the message loss ratio. However, TSVC is not robust in large traffic scenarios, because a vehicle should broadcast its key chain commitment much more frequently, which results increased packet loss ratio [20]. Moreover, each vehicle is pre-loaded with a list of anonymous public-key certificates at the initialization stage, which makes revocation of compromised vehicles in TSVC problematic. In addition, the TESLA is directly used in TSVC, which makes the scheme vulnerable to memory-based DoS attacks, and increased verification delay. Also, message authentication starts after a period of waiting time, when the second packet is released. This makes the TSVC inefficient to be used in the VANETs latency-critical applications which require timely authentication [29].

Rajput et al. [32] propose a hybrid approach which caters to the individual flaws of pseudonym-based and group-signature based approaches, but still fails to provide privacy.

A two-layered pseudonym generation method based on a keyed hash chain is introduced by Jo et al. [33] for efficient revocation and the distribution and renewal of RL.

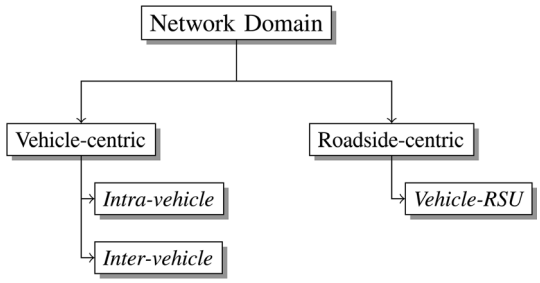

Fig. 14 Network domain class in expanded form

This protocol eliminates the authentication mode synchronization between non-cooperative and cooperative authentication. The proposed cooperative message authentication protocol requires each vehicle to share its verification result by reporting it. To verify a beacon message, each vehicle uses two processes: a beacon verification process and a report verification process. However, these are not applicable in broadcast authentication of low-latency safety applications of VANETs, as they are too time consuming.

D Non-privacy subclass

Protocols in this subclass do not employ any mechanism to provide anonymity for drivers/vehicles, and transmit a fixed node identifier in each data transmission, which raises the possibility of tracking vehicles through these identifiers. Rouf et al. [40] present security and privacy analysis of state-of-the-art commercial tire pressure monitoring systems. Authors showed that message eavesdropping was easily possible at a distance of approximately 40 meters from a passing vehicle, and that messages could be easily triggered remotely, resulting in raised privacy concerns as vehicles could be tracked through the communicating node's identifier.

6.6 Network domain class

This class recognizes the vehicular network domain that authentication protocol functions in. There are two subclasses: vehicle-centric and roadside-centric. Figure 14 shows the network domain class in expanded form.

A Vehicle-centric subclass

The first subclass categorizes authentication protocols specifically in two groups of network domains: intra-vehicle, and inter-vehicle.

A.1 Intra-vehicle group

Protocols under this group assume authentication for the intra-vehicle network. By attaching a gateway to the intra-vehicle network, information exchange between external parties and internal vehicle nodes become possible. This communication allows for remote diagnostics and firmware updates. However, allowing external parties to access the intra-vehicle network creates a potential entry-point for cyber attacks. Han et al. [36] propose a three-step authentication protocol that secures the communication between the intra-vehicle network and an external network (mobile device).

A.2 Inter-vehicle group

This group categorizes protocols which are supposed to provide authentication in a data exchange platform that shares information and warning messages between vehicles communicating in a VC system. It is imperative that safety-critical information is not inserted or modified by a malicious user or and adversary. Petit et al. [64] survey a range of authentication protocols under this group.

B Roadside-centric subclass

Information is also available from roadside sources. Protocols in this subclass provide authentication between the communicating nodes and infrastructure in vehicular networks. In this regard, the subclass can be further categorized in the vehicle-RSU group of protocols.

B.1 Vehicle-RSU group

Schemes in this group deal with the authentication portion of vehicle-to-RSU communication separated from vehicle-to-vehicle communication. For example, V2I authentication presented by Lin et al. [18] is a separate protocol that falls into this group.

6.7 Application latency class

This class recognizes the nature and behavior of different authentication schemes based on the speed with which a protocol can be deployed. A wide range of applications can be deployed in vehicular networks. From a safety point of view, applications can be classified as either safety-critical, safety-related, or non-safety-related. Each classification has latency requirements for the data transmissions. Safety-critical information should have lower latency than non-safety-related. There are three subclasses: low-latency, mid-latency, and high-latency.

A Low-latency subclass

The first subclass recognizes authentication protocols suitable for low-latency applications, such as safety critical. These are used in the case of hazardous situations, such as collisions, or any situations where the danger is high or imminent [17]. In this case, V2V and V2I communications require high reliability and low latency in realizing the safety function. Authentication protocols in such applications must satisfy the aforementioned requirements. The scheme presented by Lin et al. [58] falls into this subclass of authentication protocols.

B Mid-latency subclass

The second subclass recognizes authentication protocols that can be deployed in mid latency applications, such as safety-related. These are used in the cases where the latency requirements are not as stringent as safety-critical applications, and the danger is low, but still foreseeable. The communication technology used in these applications can be V2V or V2I/I2V. Authentication protocols that do not fit in the first subclass may satisfy the requirements for this category.

C High-latency subclass

The third subclass recognizes authentication protocols that can be deployed in high-latency applications, such as non-safety applications. These are used in applications providing traffic information and enhance driving comfort, such as traffic updates, electronic toll collection, and infotainment. They mostly involve in V2I/I2V communications. These services access the channels in the communication system in a low priority

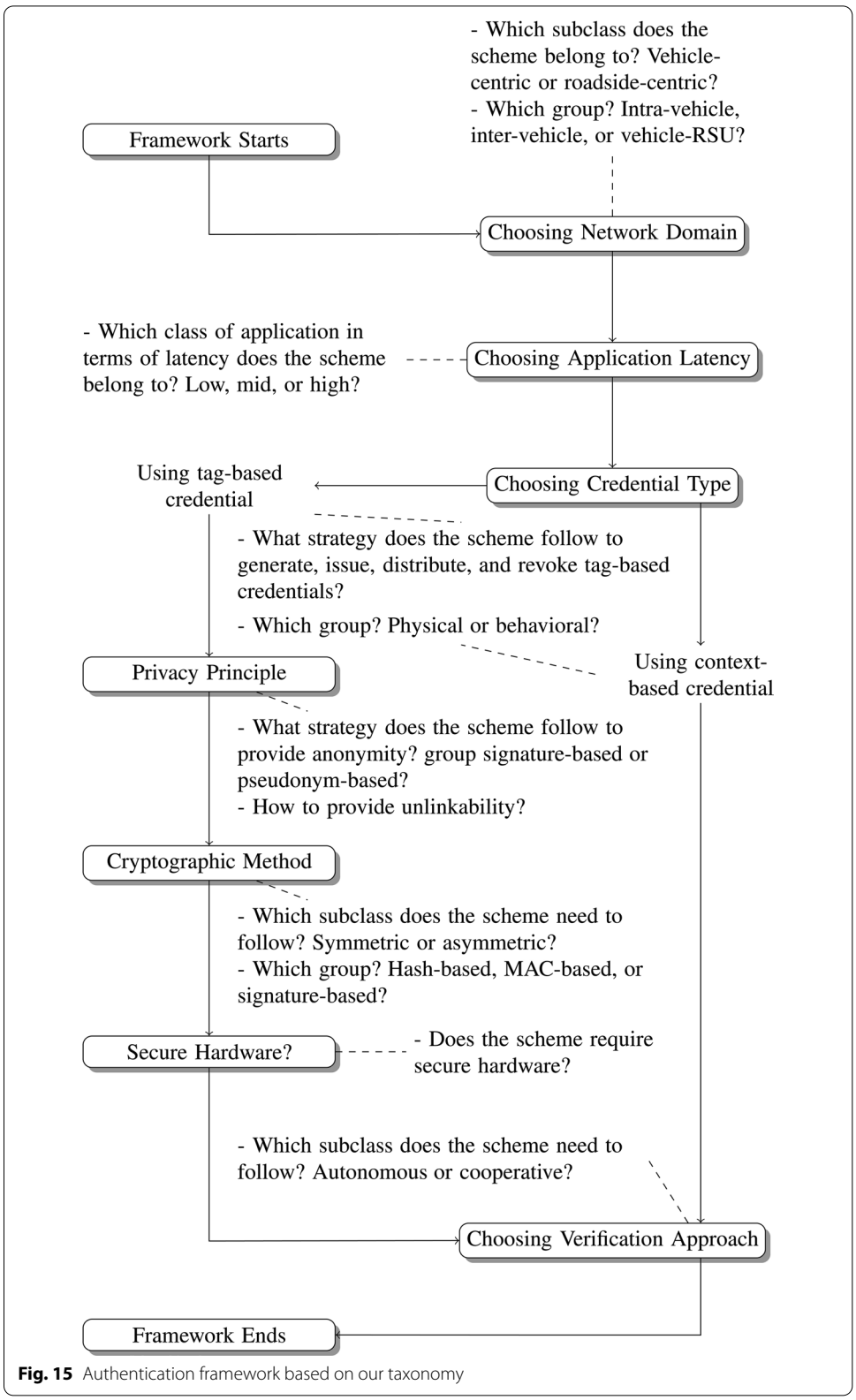

Fig. 15 Authentication framework based on our taxonomy

mode compared to safety-critical/safety-related applications. Authentication protocols that do not fit in the last two subclasses, may satisfy the requirements of this category.

7 The proposed framework for authentication in VC systems

This section introduces a framework that summarizes relations among different classes of the taxonomy. This can be used to provide guidance in selecting or designing an authentication scheme to use for a particular purpose.

The design and implementation of an authentication protocol is not a simple and straightforward process. Figure 15 shows the proposed framework for authentication in VC systems. For a particular situation the answers to a series of questions (shown by dashed links) identifies an appropriate authentication scheme. The framework presents possible stages of an authentication protocol's design. The framework uses this order, because each stage needs to be defined with respect to the previous stages requirements. Note that one can apply this framework to either intra-vehicle or inter-vehicle communications.

The first stage selects the network domain. In this stage, the authentication scheme is defined within a possible subclass of network domains to function in. This could be vehicle-centric or roadside-centric (refer to Sect. 6.6). Once a domain is selected, the next stage is to determine the application latency. In this stage, a protocol is defined within an appropriate class of application in terms of latency: low-latency, mid-latency, or high-latency (refer to Sect. 6.7). Following this stage is the selection of credential type, which defines a strategy for identification of communicating nodes. There are two subclasses: tag-based and context-based (refer to Sect. 6.2). Selecting the context-based subclass goes to the last stage. However, the tag-based subclass leads to three more stages before reaching the final stage. For the context-based subclass, the authentication scheme could be defined within physical or behavioral groups. For the tag-based subclass, strategies have to be defined for generation, issuance, distribution, and revocation of credentials. Following the tag-based stage, the privacy principle needs to be defined. Credentials contain identifiers of vehicles, and if these are captured, can possibly permit vehicle tracking and compromise the privacy of drivers. The privacy principle stage presents strategies to provide anonymity and unlinkability (refer to Sect. 6.5). The cryptographic method stage comes next. In this stage, an appropriate cryptographic method needs to be selected for the authentication scheme, with respect to the previous stages requirements. For example, a computationally heavy cryptographic technique may exceed the latency requirements selected in the second stage. The cryptographic method could be symmetric or asymmetric (refer to Sect. 6.1). The next stage is secure hardware. It indicates whether a secure device for storing cryptographic keying materials must be provided or not (refer to Sect. 6.4). In the last stage, the authentication scheme is provided an appropriate verification approach. This verification approach could be autonomous or cooperative (refer to Sect. 6.3). Once a verification approach is selected, the design phase concludes.

8 Case studies

A case study approach is employed to demonstrate the usefulness of the proposed taxonomy and framework. The research contribution is demonstrated using two different types of case study. The first type is based on analysis of seven well-known authentication protocols in public literature. The second type presents a hypothetical authentication protocol design.

8.1 Case study type 1: individual analysis

The proposed framework is applied for analysis of seven well-known authentication protocols. These are Calandriello et al. [25], Lin et al. [18], Zhang et al. [49], Shim [50], Horng et al. [59], Han et al. [36], and Wang et al. [31]. Please note that the aim is to systematize the study by grouping different authentication strategies using the proposed taxonomy, while providing related examples for each group. Thus, no attempt is made to survey all emerging authentication methods.

Calandriello et al. [25] combined multiple concepts to provide an authentication scheme for inter-vehicle domain (vehicle-centric). Vehicles transmit low-latency periodic messages (up to 10 messages per second) that enable safety applications. Authentication is provided using tag-based credentials. Vehicles generate their own credentials autonomously and issue their own explicit certificates during an online phase after deployment. This reduces the unnecessary communication overhead and redundancy in the neighbors broadcast message. The scheme relies on revocation lists requirements for distribution of credential revocation information. The scheme enables vehicles to avoid being tracked by periodically creating new pseudonym certificates, and as a result, vehicle/driver's privacy is preserved. Also, it uses a pseudonym change strategy to provide unlinkability that prevents any observer from learning that the messages originated from a specific vehicle. The underlying cryptographic primitive of this scheme is based on asymmetric cryptography, resulting in a higher computational overhead. It uses group signatures to support the issuance of explicit public key certificates. In a group signature scheme, an individual private key is provided for each vehicle to self-sign public key pairs to be used as pseudonyms for message authentication. The resulting message signature can be verified with one common group public key that is publicly known in the group. The scheme requires a TPD device to securely store cryptographic keying materials. The verification approach used in this study is autonomous to reduce dependency on other parties, but it requires more computation power to independently verify received messages within intervals of 100 milliseconds.

To summarize, Calandriello et al. [25] can be identified as: vehicle-centric, applicable in low-latency applications, uses tag-based credentials (autonomous credential issuance, certificate-based, post-deployment credential distribution, and RL-based), provides anonymity (using pseudonym-based credentials) and unlinkability (using a pseudonym-change strategy), applies asymmetric cryptography signature-based, is TPD-based, and performs an autonomous verification approach.

The stages represented in the framework (refer to Fig. 15) are repeated to analyze the next six authentication protocols: Lin et al. [18], Zhang et al. [49], Shim [50], Horng et al. [59], Han et al. [36], and Wang et al. [31]. The output of this analysis is shown in Table 2.

Table 2 Individual analysis of six different well-known authentication protocols

Stage	Case studies					
	Lin et al. [18]	**Zhang et al. [49]**	**Shim [50]**	**Horng et al. [59]**	**Han et al. [36]**	**Wang et al. [31]**
Network domain	Vehicle-centric Inter-vehicle	Vehicle-centric Inter-vehicle Roadside-centric Vehicle-RSU	Roadside-centric Vehicle-RSU	Vehicle-centric Inter-vehicle Roadside-centric Vehicle-RSU	Vehicle-centric Intra-vehicle	Vehicle-centric Inter-vehicle
Application latency	Low-latency	Low-latency	Low-latency	Low-latency	Low-latency	Low-latency
Credential type	Tag-based	Tag-based	Tag-based	Tag-based	Tag-based	Tag-based
Generation	Dependent Centralized	Dependent Decentralized	Dependent Centralized	Autonomous	Autonomous	Autonomous
Issuance	Certificate-less	Certificate-based Explicit	Certificate-less	Certificate-based Explicit	Certificate-based Implicit	Certificate-less
Distribution	Post-deployment	Post-deployment	Pre-deployment	Post-deployment	Post-deployment	Post-deployment
Revocation	RL-based	Not provided	Not provided	RL-based	Non-RL-based	Non-RL-based
Privacy principle	Anonymity Unlinkability Group-signature-based	Anonymity Pseudonym-based Unlinkability Pseudonym-change	Anonymity Pseudonym-based Unlinkability Pseudonym-change	Anonymity Pseudonym-based Unlinkability Pseudonym-change	Non-privacy	Anonymity Pseudonym-based Unlinkability Pseudonym-change
Cryptographic method	Asymmetric Signature-based	Symmetric MAC-based	Asymmetric Signature-based	Asymmetric Signature-based	Symmetric Hash-based	Symmetric MAC-based
Secure hardware	TPD-based	TPD-based	TPD-based	Non-TPD-based	Non-TPD-based	TPD-based
Verification approach	Autonomous	Cooperative	Cooperative	Cooperative	Autonomous	Autonomous

8.2 Case study type 2: hypothetical design

The protocol proposed for this hypothetical design is that of a low-latency safety application, considered for an inter-vehicle domain. The following stage is the selection of credential type. It defines a strategy for the identification of communicating nodes. There are three options. First, we can choose tag-based credentials and move to the next stage. Second, we can select context-based credentials, and move straight to the verification approach stage. Third, we can consider a hybrid strategy. Using hybrid strategy we only accept messages for verification which are relevant to a specific context (physical or behavioral). For example, we may just accept those messages for verification which are transmitted from within 50 meters of a vehicle. This is good in an extreme scenario with a high number of vehicles. Thus, after choosing a physical context-based credential, we need to properly design the next part which is the tag-based credential. Strategies have to be defined for generation, issuance, distribution, and revocation of credentials. These strategies have to be defined carefully with respect to the speed and time delay, as the protocol is considered for low-latency applications. Let's generate credentials using a centralized approach of dependent group. Issuance is certificate-based and explicit, while distribution is pre-deployed in

the vehicle's on-board credential pool by the transportation authority or the manufacturer. This results in a reduced V2I communication to receive new credentials and less reliance on availability of infrastructure in all regions. We use a RL-based approach to revoke certificates, when needed. Following the tag-based stage, the privacy principle needs to be defined. To provide anonymity, vehicles are provided pseudonym explicit certificates, with a changes strategy for unlinkability. The cryptographic method stage comes next, in which the authentication scheme needs to select an appropriate cryptographic strategy. We consider digital signatures in our protocol (asymmetric class). The next stage is secure hardware. We need to defines a TPD for storing pre-deployed certificates for our protocol. In the last stage, the authentication scheme is provided an appropriate verification approach. We choose autonomous which reduces dependency on other parties, but requires more computation power.

To summarize, the hypothetical protocol can be identified as: vehicle-centric, applicable in low-latency applications, uses tag-based credential along with context-based credential (dependent credential issuance, certificate-based, pre-deployment credential distribution, and RL-based), provides anonymity (using pseudonym-based credentials) and unlinkability (using a pseudonym-change strategy), applies asymmetric cryptography signature-based, is TPD-based, and performs autonomous verification approach.

9 Discussion and recommendation

There exists a rich variety of authentication protocols proposed for securing VC systems. The taxonomy developed in this research allows their grouping into categories for comparison and analysis. There is a great need, in the field of vehicular communications, for an authentication framework. A framework is necessary to structure future research, and provide direction to researchers and academia in the design of secure and efficient authentication protocols. The framework presented here can help in designing such effective protocols. The proposed framework classifies characteristics of authentication strategies into seven criteria: cryptographic method, credential type, verification approach, secure hardware, privacy principle, network domain, and application latency. It offers guidance to adapt each criterion to the appropriate design goals and objectives.

The framework also reveals stages for which no appropriate techniques have been developed yet. For example, Table 2 shows that the Revocation stage for both Zhang et al. [49] and Shim [50] is as "-not provided". That is, there is no Revocation technique provided in their schemes. Not providing an appropriate technique in a given category could stem from the fact that, inherently, the provided authentication mechanism is not attractive. Similarly, other shortcomings for authentication could be explored based on the proposed taxonomy and framework elements.

The framework also provides insights on unexplored avenues of research. It allows one to select and compare a set of possible techniques for a given application. For example, a researcher could identify viable techniques from the proposed framework in the context of Fig. 15 and Table 2, and consider a protocol for a low-latency application where a vehicle has to be authenticated using both tag-based and context-based credential types within custom setups. Another example is the ECQV implicit certificate. There have been no research efforts that use ECQV implicit certificate in the design of

authentication protocols for vehicular communications. This could be a potential avenue for future research.

Based on our extensive review of public literature, the communication overhead, security, and privacy aspects of authentication protocols in vehicular communications are widely addressed. However, the availability of a realistic testbed to evaluate the real computational overhead of authentication protocols on a large-scale network is a missing component. There is a great need for a model to evaluate impact of the delay on driver safety and discover any possible crash caused by the authentication delay in a large-scale VANET. There are many scenarios where a driver is relying completely on the safety messages to react on time, examples include: aggressive driver, distracted/inattentive driver, poor driver decision, impaired/drowsy driver, and rough/slick road. In such scenarios, the verification time must be less than driver reaction time, otherwise the system reliability is questionable.

10 Conclusion

Many authentication schemes have been proposed to secure VC systems; examples include [11–60]. Existing studies [61–69] have attempted to classify some of these schemes based on a limited set of characteristics. However, to date there is no generic framework to enable the comparison of these protocols and provide guidance for design and evaluation. Most existing classifications either use the computational complexity of the cryptographic techniques as a criterion, or they fail to make connections between different important aspects of authentication, such as digital signatures.

This paper specifically addressed the development and evaluation of a taxonomy and framework, to provide comprehensive guidance on the design, evaluation, and analysis of authentication protocols in the public literature and future proposals. The authentication framework was explicitly presented with clearly defined parameters. The application of the proposed taxonomy and framework was demonstrated through two different types of case study, for analysis and design, respectively. Seven different authentication protocols from the existing public literature were analyzed using the framework. This allows comparison between them. Similarly, the framework can be applied in design, making choices appropriate for the intended context.

We believe this taxonomy will be useful for researchers and designers to adequately compare and select authentication schemes when deciding on particular protocols to implement in an application. It is our hope that the taxonomy is broadly adopted.

Authors' contributions

M. A. R. Baee is the main author of the current paper. He contributed to the development of the ideas, design of the study, theory, analysis, and article writing. L. Simpson conceptualized the idea and contributed to the writing. X. Boyen supervised the study, and participated in its design. E. Foo supervised the study, and participated in its design. J. Pieprzyk supervised the study, and participated in its design and coordination. All authors read and approved the final manuscript.

Funding

The work of J. Pieprzyk was supported by the Australian Research Council under Grant DP180102199 and the Polish National Science Centre (Narodowe Centrum Nauki) under Grant 2018/31/B/ST6/03003. The work of M. A. R. Baee was supported by the Queensland University of Technology Postgraduate Research Award scholarship....

Availability of data and materials

Data sharing not applicable to this article as no datasets were generated or analyzed during the current study.

Declarations

Competing interests
The authors declare that they have no competing interests.

Author details
[1]School of Computer Science, Queensland University of Technology, 2 George Street, Brisbane, QLD 4000, Australia. [2]School of Information and Communication Technology, Griffith University, 170 Kessels Road, Nathan, QLD 4111, Australia. [3]Commonwealth Scientific and Industrial Research Organization, Data61, Corner Vimiera & Pembroke Road, Marsfield, NSW 2122, Australia. [4]Institute of Computer Science, Polish Academy of Sciences, 5 Jana Kazimierza Street, 01-248 Warsaw, Poland.

Received: 1 September 2020 Accepted: 25 March 2021
Published online: 21 May 2021

References

1. A. Paul, N. Chilamkurti, A. Daniel, S. Rho, Intelligent Vehicular Networks and Communications: Fundamentals, Architectures and Solutions, 1st edn. (Elsevier Science Publishers B. V, NLD, 2016)
2. B. Hassanabadi, S. Valaee, Reliable periodic safety message broadcasting in VANETs using network coding. IEEE Trans. Wirel. Commun. **13**(3), 1284–1297 (2014). https://doi.org/10.1109/TWC.2014.010214.122008
3. U.S.DOT: United States Department of Transportation: Intelligent Transportation Systems Safety Solutions: Preventing Crashes and Saving Lives, 1200 New Jersey Avenue, SE • Washington, DC 20590 • 800.853.1351 (2017). https://www.its.dot.gov/factsheets/jpo_safety_solutions.htm Accessed 2018-01-22
4. M. Annoni, B. Williams, in: Campolo, C., Molinaro, A., Scopigno, R. (eds.) The History of Vehicular Networks, pp. 3–21. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-15497-8_1
5. ETSC.Europa: European Transport Safety Council (ETSC): Briefing: Cooperative Intelligent Transport Systems (C-ITS). http://etsc.eu/wp-content/uploads/ETSC-Briefing-on-Cooperative-Intelligent-Transport-Systems-C-ITS.pdf, 20 Avenue des Celtes, Brussels B-1040, Belgium (2018). http://etsc.eu/briefing-cooperative-intelligent-transport-systems-c-its/ Accessed 2018-01-22
6. K.Z. Ghafoor, J. Lloret, K.A. Bakar, A.S. Sadiq, S.A.B. Mussa, Beaconing approaches in vehicular ad hoc networks: a survey. Wirel. Pers. Commun. **73**(3), 885–912 (2013). https://doi.org/10.1007/s11277-013-1222-9
7. CAMP: Vehicle Safety Communications Project: Task 3 Final Report - Identify Intelligent Vehicle Safety Applications Enabled by DSRC. Technical Report DOT HS 809 859, National Highway Traffic Safety Administration - U. S. Department of Transportation (USDOT) (March 2005). https://one.nhtsa.gov/DOT/NHTSA/NRD/Multimedia/PDFs/CrashAvoidance/2005/CAMP3scr.pdf
8. M. Bellare, P. Rogaway, Message authentication. M. Bellare, Introduction to Modern Cryptography, 155–175 (2005). cited By 1
9. D. Gollmann, What do we mean by entity authentication? In: Proceedings 1996 IEEE Symposium on Security and Privacy, pp. 46–54 (1996). https://doi.org/10.1109/SECPRI.1996.502668
10. A.J. Menezes, S.A. Vanstone, P.C.V. Oorschot, *Handbook of Applied Cryptography*, 1st edn. (CRC Press Inc, Boca Raton, 1996).
11. L. Gollan, C. Meinel, Digital signatures for automobiles?! in: Systemics, Cybernetics and Informatics (SCI) (2002). Citeseer
12. B. Parno, A. Perrig, Challenges in securing vehicular networks. In: Workshop on Hot Topics in Networks (HotNets-IV), pp. 1–6 (2005). Maryland, USA
13. M. Raya, J.-P. Hubaux, Securing vehicular ad hoc networks. J. Comput. Secur. **15**(1), 39–68 (2007)
14. M. Raya, J.-P. Hubaux, The security of vehicular ad hoc networks. In: Proceedings of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks. SASN '05, pp. 11–21. ACM, New York, NY, USA (2005). https://doi.org/10.1145/1102219.1102223
15. L. Buttyán, T. Holczer, I. Vajda, On the effectiveness of changing pseudonyms to provide location privacy in VANETs, in *Security and Privacy in Ad-hoc and Sensor Networks*. ed. by F. Stajano, C. Meadows, S. Capkun, T. Moore (Springer, Berlin, 2007), pp. 129–141
16. Y. Kortesniemi, M. Särelä, Survey of certificate usage in distributed access control. Comput. Secur. **44**, 16–32 (2014). https://doi.org/10.1016/j.cose.2014.03.013
17. M.A.R. Baee, L. Simpson, E. Foo, J. Pieprzyk, Broadcast authentication in latency-critical applications: on the efficiency of IEEE. IEEE Trans. Veh. Technol. **68**(12), 11577–11587 (2019). https://doi.org/10.1109/TVT.2019.2945339
18. X. Lin, X. Sun, P. Ho, X. Shen, GSIS: a secure and privacy-preserving protocol for vehicular communications. IEEE Trans. Veh. Technol. **56**(6), 3442–3456 (2007). https://doi.org/10.1109/TVT.2007.906878
19. L. Zhang, Q. Wu, A. Solanas, J. Domingo-Ferrer, A scalable robust authentication protocol for secure vehicular communications. IEEE Trans. Veh. Technol. **59**(4), 1606–1617 (2010). https://doi.org/10.1109/TVT.2009.2038222
20. C. Zhang, X. Lin, R. Lu, P.-Ho, RAISE: An efficient RSU-aided message authentication scheme in vehicular communication networks. In: 2008 IEEE International Conference on Communications, pp. 1451–1457 (2008). https://doi.org/10.1109/ICC.2008.281
21. Y. Hao, Y. Cheng, C. Zhou, W. Song, A distributed key management framework with cooperative message authentication in VANETs. IEEE J. Sel. Areas Commun. **29**(3), 616–629 (2011). https://doi.org/10.1109/JSAC.2011.110311
22. X. Lin, X. Li, Achieving efficient cooperative message authentication in vehicular ad hoc networks. IEEE Trans. Veh. Technol. **62**(7), 3339–3348 (2013). https://doi.org/10.1109/TVT.2013.2257188

23. X. Zhu, S. Jiang, L. Wang, H. Li, Efficient privacy-preserving authentication for vehicular ad hoc networks. IEEE Trans. Veh. Technol. **63**(2), 907–919 (2014). https://doi.org/10.1109/TVT.2013.2294032
24. P. Vijayakumar, S. Bose, A. Kannan, Improved harn batch digital signature algorithm for multicast authentication. J. Discrete Math. Sci. Cryptogr. **17**(5–6), 435–442 (2014). https://doi.org/10.1080/09720529.2013.858481
25. G. Calandriello, P. Papadimitratos, J.-P. Hubaux, A. Lioy, Efficient and robust pseudonymous authentication in VANET. In: Proceedings of the Fourth ACM International Workshop on Vehicular Ad Hoc Networks. VANET '07, pp. 19–28. ACM, New York, NY, USA (2007). https://doi.org/10.1145/1287748.1287752
26. A. Studer, F. Bai, B. Bellur, A. Perrig, Flexible, extensible, and efficient VANET authentication. J. Commun. Netw. **11**(6), 574–588 (2009). https://doi.org/10.1109/JCN.2009.6388411
27. A. Perrig, R. Canetti, J.D. Tygar, D. Song, The TESLA broadcast authentication protocol. RSA Cryptobytes **5**(2), 2–13 (2002)
28. 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), 4987–4998 (2008)
29. J. Zhou, Z. Cao, Z. Qin, X. Dong, K. Ren, LPPA: lightweight privacy-preserving authentication from efficient multi-key secure outsourced computation for location-based services in VANETs. IEEE Trans. Inf. Forensics Secur. **15**, 420–434 (2019)
30. P. Vijayakumar, M. Azees, A. Kannan, L.J. Deborah, Dual authentication and key management techniques for secure data transmission in vehicular ad hoc networks. IEEE Trans. Intell. Transp. Syst. **17**(4), 1015–1028 (2016). https://doi.org/10.1109/TITS.2015.2492981
31. 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), 896–911 (2016). https://doi.org/10.1109/TVT.2015.2402166
32. U. Rajput, F. Abbas, H. Eun, H. Oh, A hybrid approach for efficient privacy-preserving authentication in VANET. IEEE Access **5**, 12014–12030 (2017). https://doi.org/10.1109/ACCESS.2017.2717999
33. H.J. Jo, I.S. Kim, D.H. Lee, Reliable cooperative authentication for vehicular networks. IEEE Trans. Intell. Transp. Syst. **19**(4), 1065–1079 (2018). https://doi.org/10.1109/TITS.2017.2712772
34. J. Huang, Y. Qian, R.Q. Hu, Secure and efficient privacy-preserving authentication scheme for 5G software defined vehicular networks. IEEE Trans. Veh. Technol. (2020)
35. J. Camenisch, M. Drijvers, A. Lehmann, G. Neven, P. Towa, Zone encryption with anonymous authentication for V2V communication. In: 2020 IEEE European Symposium on Security and Privacy (EuroS P), pp. 405–424 (2020). https://doi.org/10.1109/EuroSP48549.2020.00033
36. K. Han, S.D. Potluri, K.G. Shin, On authentication in a connected vehicle: secure integration of mobile devices with vehicular networks. In: Proceedings of the ACM/IEEE 4th International Conference on Cyber-Physical Systems. ICCPS '13, pp. 160–169. ACM, New York, NY, USA (2013). https://doi.org/10.1145/2502524.2502546. http://doi.acm.org.ezp01.library.qut.edu.au/10.1145/2502524.2502546
37. Choi, J.Y., Jakobsson, M., Wetzel, S.: Balancing auditability and privacy in vehicular networks. In: Proceedings of the 1st ACM International Workshop on Quality of Service&Amp; Security in Wireless and Mobile Networks. Q2SWinet '05, pp. 79–87. ACM, New York, NY, USA (2005). https://doi.org/10.1145/1089761.1089775
38. H. Xiong, K. Beznosov, Z. Qin, M. Ripeanu, Efficient and spontaneous privacy-preserving protocol for secure vehicular communication. In: 2010 IEEE International Conference on Communications, pp. 1–6 (2010). https://doi.org/10.1109/ICC.2010.5502673
39. L. Fischer, A. Aijaz, C. Eckert, D. Vogt, Secure revocable anonymous authenticated inter-vehicle communication (SRAAC). In: 4th Conference on Embedded Security in Cars (ESCAR 2006), Berlin, Germany, pp. 1–9 (2006). Citeseer
40. I. Rouf, R. Miller, H. Mustafa, T. Taylor, S. Oh, W. Xu, M. Gruteser, W. Trappe, I. Seskar, Security and privacy vulnerabilities of in-car wireless networks: a tire pressure monitoring system case study. In: Proceedings of the 19th USENIX Conference on Security. USENIX Security'10, pp. 21–21. USENIX Association, Berkeley, CA, USA (2010). http://dl.acm.org/citation.cfm?id=1929820.1929848
41. M. Park, G. Gwon, S. Seo, H. Jeong, RSU-based distributed key management (RDKM) for secure vehicular multicast communications. IEEE J. Sel. Areas Commun. **29**(3), 644–658 (2011). https://doi.org/10.1109/JSAC.2011.110313
42. C.D. Jung, C. Sur, Y. Park, K.-H. Rhee, A robust conditional privacy-preserving authentication protocol in VANET, in *Security and Privacy in Mobile Information and Communication Systems*. ed. by A.U. Schmidt, S. Lian (Springer, Berlin, 2009), pp. 35–45
43. P. Kamat, A. Baliga, W. Trappe, An identity-based security framework for VANETs. in: Proceedings of the 3rd International Workshop on Vehicular Ad Hoc Networks. VANET '06, pp. 94–95. ACM, New York, NY, USA (2006). https://doi.org/10.1145/1161064.1161083
44. P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, J. Hubaux, Secure vehicular communication systems: design and architecture. IEEE Commun. Mag. **46**(11), 100–109 (2008). https://doi.org/10.1109/MCOM.2008.4689252
45. K. Sampigethaya, M. Li, L. Huang, R. Poovendran, AMOEBA: robust location privacy scheme for VANET. IEEE J. Sel. Areas Commun. **25**(8), 1569–1589 (2007). https://doi.org/10.1109/JSAC.2007.071007
46. P.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 '08, pp. 86–87. ACM, New York, NY, USA (2008). https://doi.org/10.1145/1410043.1410062
47. Z. Li, C. Chigan, On resource-aware message verification in VANETs. In: 2010 IEEE International Conference on Communications (ICC), pp. 1–6 (2010). https://doi.org/10.1109/ICC.2010.5502129
48. P. Golle, D. Greene, J. Staddon, Detecting and correcting malicious data in VANETs. In: Proceedings of the 1st ACM International Workshop on Vehicular Ad Hoc Networks. VANET '04, pp. 29–37. ACM, New York, NY, USA (2004). https://doi.org/10.1145/1023875.1023881. http://doi.acm.org.ezp01.library.qut.edu.au/10.1145/1023875.1023881
49. C. Zhang, X. Lin, R. Lu, P. Ho, X. Shen, An efficient message authentication scheme for vehicular communications. IEEE Trans. Veh. Technol. **57**(6), 3357–3368 (2008). https://doi.org/10.1109/TVT.2008.928581
50. K. Shim, *CPAS*: an efficient conditional privacy-preserving authentication scheme for vehicular sensor networks. IEEE Trans. Veh. Technol. **61**(4), 1874–1883 (2012). https://doi.org/10.1109/TVT.2012.2186992

51. P. Vijayakumar, M. Azees, L.J. Deborah, CPAV: computationally efficient privacy preserving anonymous authentication scheme for vehicular ad hoc networks. in: 2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing, pp. 62–67 (2015). https://doi.org/10.1109/CSCloud.2015.32
52. 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), 1974–1983 (2009). https://doi.org/10.1109/T-WC.2008.080280
53. J. Shao, X. Lin, R. Lu, C. Zuo, A threshold anonymous authentication protocol for VANETs. IEEE Trans. Veh. Technol. **65**(3), 1711–1720 (2016). https://doi.org/10.1109/TVT.2015.2405853
54. A. Studer, E. Shi, F. Bai, A. Perrig, TACKing together efficient authentication, revocation, and privacy in VANETs. In: 2009 6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, pp. 1–9 (2009). https://doi.org/10.1109/SAHCN.2009.5168976
55. M. Li, K. Sampigethaya, L. Huang, R. Poovendran, Swing & swap: user-centric approaches towards maximizing location privacy. In: Proceedings of the 5th ACM Workshop on Privacy in Electronic Society. WPES '06, pp. 19–28. ACM, New York, NY, USA (2006). https://doi.org/10.1145/1179601.1179605
56. R. Lu, X. Lin, T.H. Luan, X. Liang, X. Shen, Pseudonym changing at social spots: an effective strategy for location privacy in VANETs. IEEE Trans. Veh. Technol. **61**(1), 86–96 (2012). https://doi.org/10.1109/TVT.2011.2162864
57. P.K. Singh, S.N.S.T. Gowtham, S. Nandi, CPESP: cooperative Pseudonym Exchange and Scheme Permutation to preserve location privacy in VANETs. Veh. Commun. **20**, 100183 (2019). https://doi.org/10.1016/j.vehcom.2019.100183
58. X. Lin, X. Sun, X. Wang, C. Zhang, P. Ho, X. Shen, TSVC: timed efficient and secure vehicular communications with privacy preserving. IEEE Trans. Wirel. Commun. **7**(12), 4987–4998 (2008). https://doi.org/10.1109/T-WC.2008.070773
59. S. Horng, S. Tzeng, Y. Pan, P. Fan, X. Wang, T. Li, M.K. Khan, b-SPECS+: batch verification for secure pseudonymous authentication in VANET. IEEE Trans. Inf. Forensics Secur. **8**(11), 1860–1875 (2013). https://doi.org/10.1109/TIFS.2013.2277471
60. B. Palaniswamy, S. Camtepe, E. Foo, L. Simpson, M.A. Rezazadeh Baee, J. Pieprzyk, Continuous authentication for VANET. Veh. Commun. **25**, 100255 (2020). https://doi.org/10.1016/j.vehcom.2020.100255
61. S. Goudarzi, A.H. Abdullah, S. Mandala, S.A. Soleymani, M.A.R. Baee, M.H. Anisi, M.S. Aliyu, A systematic review of security in vehicular ad hoc network. In: Proceedings of 2nd Symposium WSCN, pp. 1–10 (2013)
62. M. Riley, K. Akkaya, K. Fong, A survey of authentication schemes for vehicular ad hoc networks. Secur. Commun. Netw. **4**, 1137–1152 (2011). https://doi.org/10.1002/sec.239
63. F. Qu, Z. Wu, F. Wang, W. Cho, A security and privacy review of VANETs. IEEE Trans. Intell. Transp. Syst. **16**(6), 2985–2996 (2015). https://doi.org/10.1109/TITS.2015.2439292
64. J. Petit, F. Schaub, M. Feiri, F. Kargl, Pseudonym schemes in vehicular networks: a survey. IEEE Commun. Surv. Tutor. **17**(1), 228–255 (2015). https://doi.org/10.1109/COMST.2014.2345420
65. S.S. Manvi, S. Tangade, A survey on authentication schemes in VANETs for secured communication. Veh. Commun. **Supplement C**(1), 19–30 (2017). https://doi.org/10.1016/j.vehcom.2017.02.001
66. H. Hasrouny, A.E. Samhat, C. Bassil, A. Laouiti, VANET security challenges and solutions: a survey. Veh. Commun. **7**, 7–20 (2017). https://doi.org/10.1016/j.vehcom.2017.01.002
67. Z. Lu, G. Qu, Z. Liu, A survey on recent advances in vehicular network security, trust, and privacy. IEEE Trans. Intell. Transp. Syst. (2018). https://doi.org/10.1109/TITS.2018.2818888
68. P.K. Singh, S.K. Nandi, S. Nandi, A tutorial survey on vehicular communication state of the art, and future research directions. Veh. Commun. **18**, 100164 (2019). https://doi.org/10.1016/j.vehcom.2019.100164
69. D. Manivannan, S.S. Moni, S. Zeadally, Secure authentication and privacy-preserving techniques in vehicular ad-hoc networks (VANETs). Veh. Commun. **25**, 100247 (2020). https://doi.org/10.1016/j.vehcom.2020.100247
70. D. Johnson, A. Menezes, S. Vanstone, The elliptic curve digital signature algorithm (ECDSA). Int. J. Inf. Secur. **1**(1), 36–63 (2001)
71. N. Koblitz, Elliptic curve cryptosystems. Math. Comput. **48**, 203–209 (1987)
72. V.S. Miller, Use of elliptic curves in cryptography, in *Advances in Cryptology – CRYPTO '85 Proceedings*. ed. by H.C. Williams (Springer, Berlin, 1986), pp. 417–426
73. A.K. Lenstra, E.R. Verheul, Selecting cryptographic key sizes. J. Cryptol. **14**(4), 255–293 (2001). https://doi.org/10.1007/s00145-001-0009-4
74. S.S. Kumar, Elliptic curve cryptography for constrained devices. Ph.D. dissertation, Ruhr University Bochum (2006)
75. S.A. Soleymani, A.H. Abdullah, W.H. Hassan, M.H. Anisi, S. Goudarzi, M.A. Rezazadeh Baee, S. Mandala, Trust management in vehicular ad hoc network: a systematic review. EURASIP J. Wirel. Commun. Netw. **2015**(1), 146 (2015). https://doi.org/10.1186/s13638-015-0353-y
76. M. Campagna, Sec 4: elliptic curve qu-vanstone implicit certificate scheme (ECQV). Standards for Efficient Cryptography, Version **1** (2013)
77. S.W. Cadzow, Security and Privacy for ITS and C-ITS, pp. 283–306. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-15497-8_10
78. P. Papadimitratos, A.D. La Fortelle, K. Evenssen, R. Brignolo, S. Cosenza, Vehicular communication systems: enabling technologies, applications, and future outlook on intelligent transportation. IEEE Commun. Mag. **47**(11), 84–95 (2009). https://doi.org/10.1109/MCOM.2009.5307471
79. S.A. Soleymani, A.H. Abdullah, S. Mandala, M.A.R. Baee, S. Goudarzi, A hierarchical routing protocol for improving the quality of service in wireless sensor network. Life Sci. J. **10**(3) (2013)
80. L. Xue, Y. Yang, D. Dong, Roadside infrastructure planning scheme for the urban vehicular networks. Transportation Research Procedia 25, 1380–1396 (2017). https://doi.org/10.1016/j.trpro.2017.05.163. World Conference on Transport Research - WCTR 2016 Shanghai. 10–15 July 2016
81. R.A. Uzcategui, A.J.D. Sucre, G. Acosta-Marum, Wave: a tutorial. IEEE Commun. Mag. **47**(5), 126–133 (2009). https://doi.org/10.1109/MCOM.2009.4939288
82. EC.Europa: The European Commission's Directorate-General for Mobility and Transport: C-ITS Platform Final Report, January 2016. https://ec.europa.eu/transport/sites/transport/files/themes/its/doc/c-its-platform-final-report-janua

ry-2016.pdf, European Commission DG Mobility and Transport B – 1049 Brussels (2016). https://ec.europa.eu/transport/themes/its_en Accessed 2018-01-22
83. ETSI.Europa: European Telecommunications Standards Institute: Intelligent transport systems standards. http://www.etsi.org/standards, ETSI 650, Route des Lucioles Sophia Antipolis 06560 Valbonne FRANCE (2018). http://www.etsi.org/standards Accessed 2018-01-22
84. ITS.Japan: Japanese Ministry of Land, Infrastructure, Transport and Tourism, Road Bureau, ITS: Intelligent Transport Systems. http://www.mlit.go.jp/road/ITS/, Ministry of Land, Infrastructure, Transport and Tourism, Japan (2018). http://www.mlit.go.jp/road/ITS/ Accessed 2018-01-22
85. IEEE: IEEE standard for information technology– local and metropolitan area networks– specific requirements– part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications amendment 6: Wireless access in vehicular environments. IEEE Std 802.11p-2010 (Amendment to IEEE Std 802.11-2007), 1–51 (2010). https://doi.org/10.1109/IEEESTD.2010.5514475
86. G.R. Hiertz, D. Denteneer, L. Stibor, Y. Zang, X.P. Costa, B. Walke, The IEEE 802.11 universe. IEEE Commun. Mag. **48**(1), 62–70 (2010). https://doi.org/10.1109/MCOM.2010.5394032
87. ITS.Europa: Intelligent Transport Systems (ITS); European profile standard for the physical and medium access control layer of Intelligent Transport Systems operating in the 5 GHz frequency band. Standard ETSI - ES 202 663, European Telecommunications Standards Institute (November 2009). https://standards.globalspec.com/std/12101 75/etsi-es-202-663
88. ITS.Europa: Intelligent Transport Systems (ITS); European profile standard for the physical and medium access control layer of Intelligent Transport Systems operating in the 5 GHz frequency band. Standard ETSI - ES 202 663, European Telecommunications Standards Institute (January 2010). https://standards.globalspec.com/std/12157 38/etsi-es-202-663
89. ARIB.Japan: 700 MHz Band Intelligent Transport Systems. Standard ARIB STD-T109, Association of Radio Industries and Businesses (July 2017). https://www.arib.or.jp/english/html/overview/doc/5-STD-T109v1_3-E1.pdf
90. IEEE: IEEE standard for wireless access in vehicular environments–security services for applications and management messages - amendment 1. IEEE Std 1609.2a-2017 (Amendment to IEEE Std 1609.2-2016), 1–123 (2017). https://doi.org/10.1109/IEEESTD.2017.8065169
91. M. Bellare, C. Namprempre, Authenticated encryption: relations among notions and analysis of the generic composition paradigm, in *Advances in Cryptology – ASIACRYPT 2000*. ed. by T. Okamoto (Springer, Berlin, 2000), pp. 531–545
92. FIPS: Federal Information Processing Standard (FIPS) 186-4. National Institute of Science and Technology (2013)
93. Q. Dang, Changes in Federal Information Processing Standard (FIPS) 180–4, secure hash standard. Cryptologia **37**(1), 69–73 (2013). https://doi.org/10.1080/01611194.2012.687431
94. S. Turner, D. Brown, K. Yiu, R Housley, T. Polk, Elliptic Curve Cryptography Subject Public Key Information. RFC 5480, RFC Editor (March 2009). https://www.ietf.org/rfc/rfc5480.txt
95. M. Lochter, J. Merkle, Elliptic Curve Cryptography ECC Brainpool standard curves and curve generation. RFC 5639, RFC Editor (March 2010). https://tools.ietf.org/html/rfc5639
96. N.E. Lownes, R.B. Machemehl, VISSIM: a multi-parameter sensitivity analysis. In: Proceedings of the 2006 Winter Simulation Conference, pp. 1406–1413 (2006). IEEE
97. J.L. Font, P. Iñigo, M. Domínguez, J.L. Sevillano, C. Amaya, Architecture, design and source code comparison of ns-2 and ns-3 network simulators. In: Proceedings of the 2010 Spring Simulation Multiconference, pp. 1–8 (2010)
98. C. Sommer, Z. Yao, R. German, F. Dressler, Simulating the influence of IVC on road traffic using bidirectionally coupled simulators. IEEE INFOCOM Workshops **2008**, 1–6 (2008). https://doi.org/10.1109/INFOCOM.2008.4544655
99. D. Eckhoff, C. Sommer, F. Dressler, On the Necessity of Accurate IEEE 802.11p Models for IVC Protocol Simulation. In: 75th IEEE Vehicular Technology Conference (VTC2012-Spring), pp. 1–5. IEEE, Yokohama, Japan (2012). https://doi.org/10.1109/VETECS.2012.6240064
100. A. Varga, The OMNeT++ discrete event simulation system. In: In ESM'01 (2001)
101. D. Krajzewicz, J. Erdmann, M. Behrisch, L. Bieker, Recent development and applications of SUMO—simulation of urban mobility. Int. J. Adv. Syst. Meas. **5**(3 & 4), 128–138 (2012)
102. C. Sommer, J. Härri, F. Hrizi, B. Schünemann, F. Dressler, Simulation tools and techniques for vehicular communications and applications. In: Vehicular Ad Hoc Networks, pp. 365–392. Springer (2015)
103. X. Lin, R. Lu, C. Zhang, H. Zhu, P. Ho, X. Shen, Security in vehicular ad hoc networks. IEEE Commun. Mag. **46**(4), 88–95 (2008). https://doi.org/10.1109/MCOM.2008.4481346
104. X. Lin, R. Lu, Distributed Cooperative Message Authentication, pp. 137–151. Wiley-IEEE Press (2015). https://doi.org/10.1002/9781119082163.ch7
105. M. Azees, P. Vijayakumar, L.J. Deborah, Comprehensive survey on security services in vehicular ad-hoc networks. IET Intell. Transp. Syst. **10**(6), 379–388 (2016). https://doi.org/10.1049/iet-its.2015.0072
106. V.S. Yadav, S. Misra, M. Afaque, Security of wireless and self-organizing networks: security in vehicular ad hoc networks. Security of Wireless and Self-Organizing Networks: Security in Vehicular Ad Hoc Networks, 227–250 (2010). cited By 1
107. O.K. Fraenkel, Alan F.W, Privacy and freedom. pp. xvi. new york: Atheneum, 1967. \$10.00. The ANNALS of the American Academy of Political and Social Science 377(1), 196–197 (1968). https://doi.org/10.1177/000271626837700157
108. F. Schoeman, Privacy: philosophical dimensions. Am. Philos. Q. **21**(3), 199–213 (1984)
109. R. Akalu, Privacy, consent and vehicular ad hoc networks (VANETs). Comput. Law Secur. Rev. **34**(1), 37–46 (2018). https://doi.org/10.1016/j.clsr.2017.06.006
110. J.P. Hubaux, S. Capkun, J. Luo, The security and privacy of smart vehicles. IEEE Secur. Privacy **2**(3), 49–55 (2004). https://doi.org/10.1109/MSP.2004.26
111. F. Dötzer, Privacy issues in vehicular ad hoc networks. In: Proceedings of the 5th International Conference on Privacy Enhancing Technologies. PET'05, pp. 197–209. Springer, Berlin, Heidelberg (2006). https://doi.org/10.1007/11767831_13

112. P. Papadimitratos, A. Kung, J.-P. Hubaux, F. Kargl, Privacy and identity management for vehicular communication systems: a position paper. In: Workshop on Standards for Privacy in User-centric Identity Management (2006)
113. L. Reyzin, et al.: RE: Comments on NHTSA notice of proposed rule for FMVSS No. 150. V2V Communications (Docket No. NHTSA-2016-0126) (2017)
114. P.M. Schwartz, D.J. Solove, The PII problem: privacy and a new concept of personally identifiable information. NYUL Rev. **86**, 1814–1894 (2011)
115. J. Domingo-Ferrer, Q. Wu, in: Bettini, C., Jajodia, S., Samarati, P., Wang, X.S. (eds.) Safety and Privacy in Vehicular Communications, pp. 173–189. Springer, Berlin (2009). https://doi.org/10.1007/978-3-642-03511-1_8
116. O. Ureten, N. Serinken, Wireless security through RF fingerprinting. Can. J. Electr. Comput. Eng. **32**(1), 27–33 (2007). https://doi.org/10.1109/CJECE.2007.364330
117. P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, J.P. Hubaux, Secure vehicular communication systems: design and architecture. IEEE Commun. Mag. **46**(11), 100–109 (2008). https://doi.org/10.1109/MCOM.2008.4689252
118. A. Weimerskirch, J.J. Haas, Y.-C. Hu, Laberteaux, K.P.: Data Security in Vehicular Communication Networks, pp. 299–363. John Wiley and Sons, Ltd (2009). https://doi.org/10.1002/9780470740637.ch9
119. A. Shamir, Identity-based cryptosystems and signature schemes, in *Advances in Cryptology*. ed. by G.R. Blakley, D. Chaum (Springer, Berlin, 1985), pp. 47–53
120. M.A.R. Baee, Implementation and performance analysis of identity-based authentication in wireless sensor networks. Master's thesis, Universiti Teknologi Malaysia (2014)
121. A. Boualouache, S.-M. Senouci, S. Moussaoui, A survey on pseudonym changing strategies for vehicular ad-hoc networks. IEEE Commun. Surv. Tutor. **20**(1), 770–790 (2017)
122. D. Boneh, X. Boyen, H. Shacham, Short group signatures, in *Advances in Cryptology - CRYPTO 2004*. ed. by M. Franklin (Springer, Berlin, 2004), pp. 41–55
123. R.L. Rivest, A. Shamir, Y. Tauman, How to leak a secret, in *Advances in Cryptology – ASIACRYPT 2001*. ed. by C. Boyd (Springer, Berlin, 2001), pp. 552–565
124. V.S. Miller, *The Weil Pairing, and Its Efficient Calculation* (Springer, Berlin, 2004).

Publisher's Note