IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received August 15, 2021, accepted August 29, 2021, date of publication August 31, 2021, date of current version September 9, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3109264

Security and Privacy Schemes in Vehicular Ad-Hoc Network With Identity-Based Cryptography Approach: A Survey

MAHMOOD A. AL-SHAREEDA[1], MOHAMMED ANBAR[1], SELVAKUMAR MANICKAM[1], AYMAN KHALIL[2], AND IZNAN HUSAINY HASBULLAH[1]

[1]National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia (USM), Gelugor, Penang 11800, Malaysia
[2]Faculty of Engineering, Islamic University of Lebanon (IUL), Choueifat, Beirut 30014, Lebanon

Corresponding author: Mohammed Anbar (anbar@nav6.usm.my)

This work was supported by Universiti Sains Malaysia (USM) from external grant by UMobile Sdn Bhd number 304/PNAV/650958/U154.

ABSTRACT Vehicular Ad hoc Networks (VANET) broadcast messages regarding road and environmental conditions. Due to its design, VANET inadvertently introduced security and privacy issues. Many researchers have suggested various approaches to address these shortcomings as the deployment of VANET becomes more widespread. Nevertheless, these solutions could not address all the security and privacy shortcomings in VANET. Furthermore, the proposed approaches incur high costs in terms of computation due to the complexity involved in doing so sequentially. One of the significant approaches used in VANET security and privacy mitigation is identity-based schemes. This paper provides a comprehensive survey on VANETs and the entities involved, attack models, and an analysis of the security and privacy requirements for identity-based security and privacy schemes for VANETs.

INDEX TERMS VANET, cyber-attack, bilinear pair, elliptic curve cryptography, identity-based cryptography.

I. INTRODUCTION

Vehicular Ad-hoc Networks (VANETs) is a subclass of Mobile Ad-hoc Networks (MANETs), where a vehicle is considered a mobility node. VANET technology generally supports various functions such as intersection crash warning, cooperative forward collision, sensing cautioning, and [1]–[3]. In addition, a VANET technology offers the drivers and passengers services such as Internet access, location-based services, and entertainment content [4]–[7]. Nevertheless, the main goal of VANET is to improve transportation by preventing and mitigating road traffic and accident [8]–[15].

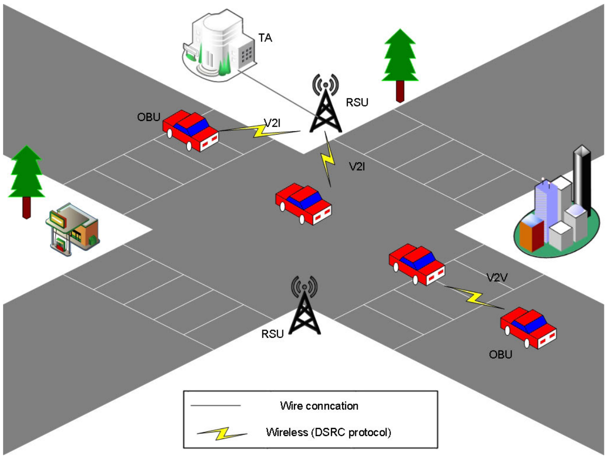


FIGURE 1. **The architecture of VANET.**

Typically, the architecture of VANET includes three components: trusted authority (TA), roadside units (RSUs), and onboard units (OBUs), as shown in Figure 1. TA is a fully trusted entity with large computation and communication resources than other components in the system. RSU is an infrastructure device located adjacent to an intersection that serves vehicles within its coverage area with services such as management and communication via the dedicated short-range communications (DSRC) standard [16]–[19]. Each vehicle has an OBU that shares the information of the driving circumstances with others or neighboring RSU via vehicle-to-vehicle (V2V) mode and

The associate editor coordinating the review of this manuscript and approving it for publication was Abderrezak Rachedi.

vehicle-to-infrastructure (V2I) mode. Each vehicle sends to neighboring vehicles via DSRC with information about the road condition using these communication modes. While RSUs ensure better control of traffic by sending messages to a vehicle within their coverage area.

As connectivity transcends computing devices to everyday objects and even vehicles, VANET's role has become more prominent with more research and development in this domain. As with any new technology, VANET also suffers from issues related to security and privacy. More accurately, the challenges of security and privacy issues on V2V and V2I communications should be carefully considered in VANET [20]–[23].

Vehicles in a VANET environment are prone to security and privacy issues due to the openness of VANET. Therefore, they need to be addressed to ensure VANET users do not suffer from the problems aforementioned. Much research has been carried out in VANET relating to providing authentication. Nevertheless, there are several limitations to the existing schemes.

Furthermore, most of these schemes have a massive overhead in terms of computation complexity involved in doing so sequentially. The main goal of this paper is to critically review identity-based security and privacy schemes based highlighting their strengths and weaknesses guided by security requirements, privacy requirements, resistance to cyberattack, and the evaluation metrics.

The rest of this paper is structured as follows: Section II presents the overview of VANET. Section III deals with the background of VANET and the security and privacy requirements. Section IV reviews a relevant survey on the existing work. The identity-based security and privacy are classified differently in Section V. Section VI discusses the existing schemes and presents a critical review of related work. Conclusions of this paper are provided in Section VII.

II. VEHICULAR AD HOC NETWORK

This section provides the overview of the VANET system, a description of the architecture VANET follows in terms of entities and communications. Lastly, the comfort and safety applications of VANET are provided.

A. OVERVIEW

Each year, approximately 1.3 million fatalities and 30 million are reported due to road accidents, respectively. Since it is considered the ninth leading cause of death globally, gross domestic product (GDP) loss is around 3% or USD 1 trillion. Furthermore, It is expected, by 2030, road accidents will climb to the fifth position for the cause of death [24].

An intelligent transportation system (ITS) plays a particularly critical role in the road and transportation system. Smart vehicles are fast becoming a norm leveraging the rapid growth of wireless communications [25]. Modern vehicle manufacturers have started integrating wireless devices in every vehicle, enabling them to share road status information with others or infrastructures [26]. These vehicles form an ad hoc network, where the vehicles are nodes of a network known as VANET. Thus, VANET has become one of the most promising research areas with applications [4], [27]. Vehicles have an important position for persons. Several researchers have been archived to assist drivers and passengers. Recently, industry, academia, and governments have attracted extensive research and attention to VANET due to its massive development and deployment [28].

B. ARCHITECTURE

In this subsection, we describe the typical architecture of VANET in terms of entities and communications, as follows.

1) ENTITIES

As shown in Figure 1, three entities are involved in the VANETs, namely the TA, RSU, and OBU. Table 1 presents the model descriptions of the major entities in detail.

TABLE 1. Description of VANET's major entities.

Entity	Description
(TA)	It is responsible for managing and maintaining the entire VANET system. The TA has sufficient resources in terms of computation, communication, and storage. Moreover, it is also considered to be fully trusted by all entities in the VANET. Therefore, no adversary can compromise the TA.
(RSU)	It is stationary infrastructures located along the roadside. RSUs are the intermediate node between the OBUs and TA, which link with TA by secure wire communication and OBUs by wireless technologies. The RSUs receive the messages using the DSRC protocol and process them locally or forward them to TA for further use.
(OBU)	Each vehicle is fitted with an OBU, which enables the vehicle to exchange messages with other vehicles or nearby RSUs to increase driver awareness in the driving environment. Each OBU has a tamper-proof device (TPD) to store the secret, and personal information never revealed in VANETs.

2) COMMUNICATIONS

As shown in Figure 1, two types of communication are comprised in the VANETs, Vehicle-To-Vehicle (V2V), and Vehicle-To-Infrastructure (V2I) communications. These communication modes use the DSRC protocol during wireless communication. The two modes are described as follows:

- Vehicle-To-Vehicle (V2V) utilizes multi-hop wireless to broadcast messages to other entities in VANET via multiple hop nodes. In the communication of V2V, the OBU of vehicle issues message shares only with other OBUs. The vehicle utilizes this message to avert traffic accidents and disruption in the driving environment. For instance, when a traffic jam occurred, the vehicle transmits the status so that other vehicles closing the site could make changes to their journey to avert the congestion. The vehicle sends information to others every 100 to 300 ms using the protocol of DSRC [29], [30]. For example, VANET with 200 vehicles within the RSU range utilizing such a protocol means that 200 to 600 information is broadcasted every second. This must be checked by the verifying recipient [31].

- Vehicle-To-Infrastructure (V2I) communication utilizes single-hop wireless, sending a message from a fixed infrastructure located along the roadside. In the communication of V2I, the vehicle issues message share with other vehicles or nearby RSU by using DSRC protocol during the journey. The RSU provides the driver and passengers with internet access and downloading music or forwards the message to TA for further use.

C. APPLICATIONS

In VANET, the communication modes support a wide range of application development and provide the drivers and passengers with many convenience and entertainment information. VANET applications are categorized into (i) comfort and (ii) safety applications, as shown in Table 2.

TABLE 2. Applications of VANET.

Application	Description
comfort	It is part of non-safety applications. The major goal of these applications is to provide the driver and passenger with convenience and entertainment services such as weather condition, Internet access, details of the position of nearby gas stations, and download entertainment content [32], [33].
Safety	The main objective of these applications is to reduce accidents and traffic disruption in the driving environment. Utilizing the communication modes can enhance traffic management, blind-spot warning, signal violation warning, and averting collisions and accidents [32], [33].

III. BACKGROUND

A. OVERVIEW

VANET communication offers drivers and passengers many transportation applications and provides unprecedented non-safety information and safety services. For example, when the vehicle collects and processes the exchange information involving V2V and V2I communications, it can increase the driver's awareness of the driving environment, which enhances driving experiences and improve passenger comfort [20], [22], [34].

B. SECURITY AND PRIVACY REQUIREMENTS

In this section, the security and privacy requirements of VANET are discussed in detail.

1) SECURITY REQUIREMENTS

Due to the inherent characteristics of VANETs, it is vulnerable to different security attacks. Thus, the attacker is easy to launches several processes on sent messages even to control the communication channels [35], [36]. The security requirements should be satisfying per each scheme.

- **Authentication:** The receiver can check whether the receiving message is valid by verifying the signer's authenticity.
- **Integrity:** With periodically exchange the message in VANETs, the content of the legitimate message should be checked to guarantee that it has been broadcasted without being corrupted.
- **Non-repudiation:** The singer of messages should do not has the ability to deny that they have broadcasted messages.
- **Traceability:** TA-only entities of the VANET can disclose the original identity of any malicious vehicle.
- **Revocability:** Besides the traceability requirement, TA can also revoke the malicious vehicle from participating in the system.

2) PRIVACY REQUIREMENTS

Issues of privacy have become equally significant [37], [38]. During the communication, the attacker can perform actions that include (i) acquire the vehicle's true identity or even determine its traveling paths by examining the captured messages and (ii) cross-match multiple broadcasted messages that by the same source. Such an attack exposes the driver's personal and other vehicular details, and it can be leveraged to carry out other forms of attacks. The privacy requirements should be satisfying per each scheme.

- **Identity privacy-preservation:** This is a crucial privacy requirement. It offers privacy preservation in a VANET, which means that personal information about the driver and vehicles, such as the identity, should be securely transmitted.
- **Unlinkability:** The attacker cannot link whether the same source has signed multiple messages.
- **Unobservability:** Registered nodes in VANET can sign and verify messages without being observed in service utilization by the attacker.

C. ATTACK MODEL

The internal attackers and external attackers are commonly classified in VANETs. Compared to internal attackers, the external attackers cannot be part of the system, therefore, they are approved to be extremely robust attackers. The compromised entities of VANETs are called internal attackers. It can use sensitive information by internal attackers due to they are part of the system [5]. In some potential attack scenarios, various attacks on VANETs are carried out.

- **Replay attacks:** It is an extremely general security attack in VANETs. It is also known as a playback attack. If a legitimate message is maliciously replayed, which causes a delay in its effect, there is a higher possibility that a replay attacker occurred in the network.
- **Modification attacks:** It is a common attack to alter or modify the intercepted message in these two communication modes. The attacker could deliberately send a fake message to the system creating confusion among vehicles, leading to severe safety consequences. The recipient should verify all the messages from other nodes to avert falling victim to a modification attack.

- **Impersonation attacks:** In VANET, every node has a unique identity ID, and each node is identified in the VANET network and used to identify vehicles needing assistance, especially in case of an emergency or accident. Nevertheless, an attacker could alter his identity during an impersonation attack and act as an original identity of the message. An attacker receives the message from the sender, performs modification of the message for malicious intent, and then broadcasts this message to other nodes.
- **Man-In-The-Middle attacks (MITM):** In VANET, this attack risks communication and change messages sent among registered nodes. The MITM attack is a leading and highly damaging cyber-attack on VANET communication especially when the message contains important roads and other status. The attacker launches the MITM attack by following two scenarios, (i) the message containing critical information should be received by the adversary in VANET, and (ii) the adversary can interpret the information content [39].

D. EVALUATION METRICS

Due to high computation cost, the impact on scalability will not be withstanding as the number of vehicle joining VANET grows. The vehicle has equipped one strong capability of ample device, its main goals focus on movement instead of computation process. AS the number of vehicles increases, exchanging a large number of messages in VANET, the costs spent on computation should be reduced. Besides, the vehicle share information about the driving environment every 100–300 ms [19]. Within the area covered by the vehicle or RSU, if there are 150 vehicles, the recipient must authenticate 450–150 messages per second [31]. Also, the process of verification must be very fast to handle the velocity of the incoming messages. Thus, communications security should, therefore, be sufficiently effective.

The computation overhead of each scheme is dependent on the evaluation metrics used. Using the MIRACLE library [40], we can calculate the cost needed for cryptography security operations for bilinear pairing and ECC algorithm. The hardware platform utilized is powered by an Intel(R) Core 2 Quad 2.66 GHz processor in the Microsoft Windows 7 operating system with 4 GB memory. The average execution time of operations based on cryptography is presented in Table 3. Operations based cryptography of bilinear pairing and ECC are presented as bellow:

- T_{sm-ecc} indicates the execution operation of scalar multiplication regarding the ECC in an additive group G.
- T_{pa-ecc} indicates the execution operation of point addition regarding the ECC in an additive group G.
- T_h indicates the execution function of secure hash cryptography.
- T_{bp} indicates the execution of a bilinear pairing operation.
- T_{sm-bp} indicates the execution operation of scalar multiplication about the bilinear pairing in G_1.
- T_{pa-bp} indicates the execution operation of point addition about the bilinear pairing in G_1.
- T_{mtp} indicates the execution function of map-to-point regarding the bilinear pairing in G_1.

TABLE 3. Time cost of several operations based on cryptography.

Cryptography operation	Time (ms)
T_{pa-ecc}	0.0031
T_{sm-ecc}	0.6718
T_h	0.001
T_{bp}	5.811
T_{pa-bp}	0.0106
T_{sm-bp}	1.5654
T_{mtp}	4.1724

To evaluate communication overhead, to require the same security level in both bilinear pair and ECC algorithm, we use the parameters listed in Table 4. The suppositions in this paper are the same for both ECC and bilinear pair schemes that the result sizes of the secure hash function and timestamp are 20 bytes and 4 bytes, respectively.

E. IDENTITY BASED SECURITY AND PRIVACY (ID-SP)

To reduce the burden preload a large number of certificate management and the corresponding key pairs raised from the conventional Public Key Infrastructure (PKI), Shamir proposed the Identify technology in 1984 [41]. The main idea of this approach is the public key is directly derived from identity information such as Id card, model, and contact number. Thus, this approach removes the need for certificate management and corresponding the key pairs with PKI as it does not utilize any certificate for the traffic information authentication, minimizing the overhead. So, this approach can somewhat improve the efficiency of VANETs. Four algorithms are involved in the identity-based scheme. They are Setup, Extract, Sign, and Verify [42], as follows.

- **Setup algorithm:** The main idea of this algorithm is to generate the public parameter of the system by TA which chooses s as the private key of the system and then computes the corresponding public key as $P_{Pub} = sP$, where $P \in G_1$ indicate to the generator of the group G_1. Finally, The TA store the private key s of the system.
- **Extract algorithm:** The main idea of this algorithm is to implement upon the request of the registered sender for a private key related to its identity $\in \{0, 1\}^*$. The TA calculates the private key for the identity as $PID = sH(ID)$. Then, the TA preloads PID to the registered sender.
- **Sign algorithm:** The main idea of this algorithm is to sign the traffic-related message $m \in \{0, 1\}^*$ by the sender during the broadcasting process. The sender selects $Z \in G_1$, chooses a random integer $w \in Z_q^*$ and calculates as $\eta = \mathrm{e}\ (Q, P)$, $\sigma = h(m, \eta)$ and $\delta = \sigma PID + wZ$. Therefore, the signature $(\sigma, \delta) \in Z_q^*$ on message m.
- **Verify algorithm:** The main idea of this algorithm is to verify the signature $(\sigma, \delta) \in Z_q^*$ on message m by

TABLE 4. Execution time of several cryptography operations.

Scheme	Curve type	Pairing	Cyclic Gr.	Size of p	G (bits)	Length of group
ECC	E:$y^2 = x^3 + ax + b \bmod p$, where $a, b \in Z_q^*$	Pairing-free	$G(p)$	160 bits	q = 160	$\|G\|$= 40 bytes
Bilinear Pairing	E:$y^2 = x^3 + x \bmod p$	$G_1 * G_1 \rightarrow G_2$	$G_1(p)$	521 bits	q = 160	$\|G_1\|$= 128 bytes

the verifying recipient after the paymasters is received. Therefore, the verifier calculates as η = e (δ, P). e(H(ID)), $-$ $P_{pub})^{\sigma}$. If the equation σ = h(m, η)holds, the recipient accepts the signature; otherwise, it does not accept it.

In the previous work [43], VANET taxonomy schemes comprise public-key, infrastructure-based security and privacy schemes, group-signature-based security and privacy schemes, and ID-SP schemes. This survey paper mainly focuses on ID-SP schemes since several researchers proposed schemes to address conditional privacy-preserving authentication issues.

IV. RELEVANT SURVEYS

There are relevant surveys in the existing surveys in the literature, such as [19], [44]–[48].

Rahim *et al.* [44] surveyed the aware social services of VANET, dissemination of data, and modeling of mobility. Boualouche *et al.* [45] surveyed and compared pseudonym-changing schemes based on relevant metrics for the VANETs system. Sharma and Ajay [46] designed intrusion detection systems (IDSs) reviewed existing VANET schemes thoroughly Wang *et al.* [47] introduced a survey on vehicle-to-everything (V2X) system requirements. This boundary survey requires checking issues along with the summarized investigation on the testing process in terms of the view architectural stage for V2X communication. Sewalker and Seitz [48] reviewed the planning parameters of the vehicle-to-pedestrian (V2P) application. They surveyed the arising V2P schemes for safety services and their purpose investigation. Moreover, this survey discussed the combination of vulnerable road users (VRUs) challenges and the V2X system. Lu et al [19] surveyed the developments in the VANET system to discuss the basic architecture and features in VANETs.

These surveys comprehensively covered the features and security issues of VANET. Nevertheless, the main aim of this survey is to focus on the identity-based security and privacy schemes of VANETs in detail. This paper differed from the previous surveys by discussing (i) the identity-based security and privacy requirements of a VANET for each scheme, (ii) the security attacks resistance that affects security and privacy schemes, and (iii) the evaluation metrics in terms of computation and communication costs.

V. CLASSIFICATION OF THE IDENTITY BASED SECURITY AND PRIVACY (ID-SP)

We classify these schemes according to the modern cryptography algorithms utilized, such as bilinear pair-based-ID-SP and Elliptic Curve Cryptography (ECC) based-ID-SP since widely used in the identity approach. The main aims of this survey focus on security and privacy attacks, resistance to cyber-attack, and evaluation metrics for each scheme of bilinear pair based-ID-SP, Elliptic Curve Cryptography (ECC) based-ID-SP, and others.

A. BILINEAR PAIR BASED

Consider G_1 and G_2 indicate to a cyclic additive group and a cyclic multiplicative group respectively. In these groups use the same prime order q. The point $P \in G_1$ computes the G_1. Consider e: G_1 * $G_1 \rightarrow G_2$ be a bilinear pairing which fulfills the critical characteristic as follows [56], [57]:

- **Bilinearity:** For all P, S,R $\in$ G_1, e(P + S, R) = e(P, R)e(S, R) and e(P, S + R) = e(P, S)e(P, R). Likewise, with all a, b $\in$ Z_q^*, e(aP, bP) = e(P, P)ab = e(P, abP) = e(abP, P).
- **Non-degeneracy:** Given two points P, S $\in$ G_1 such that e(P, S) $\neq$ 1 or e(S, R) $\neq$ e(P, P), where 1 refer to the item of identity in group G_2.
- **Computability:** There should be a robustness method to calculate e(P, S) with all P, S $\in$ G_1.

Jianhong *et al.* [49] highlighted that the scheme of Lee and Lai [58] does not address the non-repudiation and tractability issues in VANET. Therefore, they proposed an enhanced authentication scheme with batch verification to solve the shortcomings of Lee and Lai scheme [58]. The vehicle submits its real identity RID_i and password PWD_i to start the process of pseudo-identity creation. After verifying the validity of RID_i and PWD_i, the TPD of the vehicle computes the pseudo-identity and the respective private key. Thus vehicle uses to sign messages during the broadcasting process.

Zhang *et al.* [50] proposed Distributed Aggregate Privacy Preserving Authentication (DAPPA) protocol without requiring an ideal TPD. This scheme is based on a new multiple TA one-time identity-based aggregate signature technique for secure VANET communication.

Wang and Yao designed a local Identity-based anonymous message in Authentication Protocol (LIAP) to increase authentication efficiency in VANET [51]. In this protocol, the nodes obtain the long-term certificate from a certificate authority (CA) in the registration phase. With an expired long-term certificate, the vehicle will not be able to join the network again.

Pournaghi *et al.* [52] proposed A Novel and Efficient Conditional Privacy-Preserving Authentication (NECPPA) scheme based on RSU for V2V and V2I communication. This scheme stores the system's private key into the TPD

TABLE 5. Security requirements achieved by bilinear pair based.

	Security Requirements				
Papers	**Authentication**	**Integrity**	**Non-repudiation**	**Traceability**	**Revocability**
[49]	✓	✓	✓	✓	✓
[50]	✓	✓	✓	✓	✓
[51]	✓	✓	✓	✓	✓
[52]	✓	✓	✓	✓	✓
[53]	✓	✓	✓	✓	✓
[54]	✓	✓	✗	✓	✓
[55]	✓	✓	✗	✓	✓

TABLE 6. Privacy requirements achieved by bilinear pair based.

	Privacy Requirements		
Papers	**Privacy-preserving**	**Unlinkability**	**Unobservability**
[49]	✓	✓	✗
[50]	✓	✓	✗
[51]	✗	✗	✗
[52]	✓	✓	✗
[53]	✓	✓	✗
[54]	✓	✗	✗
[55]	✓	✓	✗

TABLE 7. Controlled bilinear pair based resistance to security attack.

	resistance to security attack			
Papers	**Replay**	**Modification**	**Impersonation**	**MITM**
[49]	✗	✓	✓	✓
[50]	✓	✓	✓	✓
[51]	✓	✓	✓	✓
[52]	✗	✓	✓	✓
[53]	✗	✓	✓	✓
[54]	✓	✓	✓	✓
[55]	✓	✓	✓	✓

TABLE 8. Bilinear pair based overhead for computation and communication.

	computation (ms)		**communication**
Papers	**Singing**	**Verifying**	**(Bytes)**
[49]	13.59	3.1444	388
[50]	8.3478	11.4786	148
[51]	0.4013	12.5432	308
[52]	5.554	10.343	140
[53]	4.1724	14.1708	120
[54]	8.6962	10.5654	308
[55]	4.6962	1.5654	408

of RSU rather than the TPD of the vehicle during the registration phase. Moreover, after the TA assigns the private key of an RSU, it also stores in the TPD of RSU. The vehicle receives the private key of RSU to sign a message within the coverage range of RSU for a short time. The verifying recipient uses the public key of the RSU to authentic the message in VANET.

Baya *et al.* [53] introduced a New and Efficient RSU based Authentication (NERA) scheme to secure V2V and V2I communications. This scheme embeds the master key of the system in a TPD provided at the RSUs during the registration phase. Before the vehicle exchanges information, it has to authenticate itself when a vehicle joins the communication when it is in the range of an RSU. The RSU transmits the n pseudo-IDs and the respective private keys, where n is an anonymous security level that a vehicle can unrepeatable use in the communication range of RSU [59]. The RSU uses the HMAC as an asymmetric encryption algorithm to encrypt the set of pseudo-ID and the respective private key. After the vehicle receives the encrypted parameters from the RSU, it signs the message during the broadcasting phase.

The same author, Baya *et al.* [54], introduced an efficient authentication scheme that does not require any online-RSU or equipped vehicle equipped with TPD to store the private key of TA. Therefore, the entire system is not compromised when only one vehicle OBU is affected. Besides, to avoid the storage management burden put on the vehicle, the TA does not preload the pool of anonymous identities and the respective private keys on each OBU. After the TA receives the vehicle's identity, it computes the secret key SID_i and a pseudo-identity x_i and preloads them into the vehicle via a secure channel.

Ali and Li [55] designed an Identity-based Conditional Privacy-Preserving Authentication (ID-CPPA) signature scheme using a bilinear map to speed up the authentication process of the message at the RSU for V2I communication. This scheme requires less processing power because it utilizes general one-way hash functions instead of map-to-point hash functions.

Tables 5 and 6 summarize the security and privacy requirements achieved by the bilinear pair algorithm. Table 7 presents the level of resistance to security attack is achieved by bilinear pair based. Table 8 shows a bilinear pair-based evaluation metric in terms of computation and communication costs.

B. ELLIPTIC CURVE CRYPTOGRAPHY BASED

To present the foundations of Elliptic Curve Cryptography (ECC) briefly and the corresponding computation hardness which guarantees requirements of security and withstands various types of threats [60], [61] as.

Let F_p be a finite field with prime order p. The definition of the non-singular with the following equation elliptic curve E $y^2 = x^3 + ax +$ b mod p, where $4a^3$ $+27b^2 \neq 0$ and a, b $\in F_p$. Consider O be the point at infinity. All the points make an additive group G with order q and generator P. The critical characteristic of the group G in ECC, as bellow:

- **Point Addition:** Consider P and S be two random points such that $(P, S) \in G$ based ECC, where the point P computes the group G with enormous prime order q. When $P \neq S$ then $R = P + S$ can be calculated, where R indicate to the point of intersection in ECC and the line which joins P and S. When $P = S$ then $R = P + S$, and when $P = -S$ then $P + S = O$.
- **Scalar multiplication:** The explanation of the ECC as $LP = P + P + P.... + P$ For L times, where $L \in Z_q^*$ and $L > 0$.
- **Elliptic Curve Discrete Logarithm problem (ECDLP):** There exists two random points P and S such that $(P, S) \in G$, on ECC, where $P \in G$ computes the G with large prime order q. The main idea of the ECDL problem is to calculate an integer x from $S = xP \in G$, where $x \in Z_q^*$ is an unknown integer.

He *et al.* [62] designed a Conditional Privacy-Preserving Authentication (CPPA) scheme without utilizing bilinear pairing to support mutual authentication and privacy preservation at the same time for V2V and V2I communications. For each vehicle, the TA chooses a real identity *RID* and a password *PWD*. The TA then preloads them with private key x of the system into the vehicle's Tamper-Proof Device (TPD). Before the vehicle broadcasts the message to nearby RSUs and vehicles, it computes an anonymous identity and a digital signature by using the vehicle's TPD.

To develop faster user authentication with a user privacy preservation scheme for vehicular sensor network (VSN) environments, Lo and Tasi [63] proposed a conditional privacy-preserving authentication scheme. It uses ECC instead of bilinear pair for drivers and passengers willing to utilize these services and applications in VSN. After the TA receives the original identity *RID* of the vehicle, it computes the pseudo-IDs and their respective private keys back to the vehicle through a secure channel.

Wu *et al.* [64] adapted the random short-term pseudonyms to propose a location-based-conditional privacy-preserving authentication scheme by and without utilizing any special device, such as ideal TPD. Within the RSU communication area, this scheme allows a vehicle to obtain short-term pseudonyms from a new RSU. The vehicle communicates with others by helping new pseudonyms within the coverage area of the RSU.

Alazzawi *et al.* [65] proposed a robust pseudo-identity-based scheme for V2V and V2I communications in VANET. The TA preloads the pseudonym instead of the vehicle's real identity during the registration process in this scheme. After the vehicle computes the pseudo-IDs PID_v1 and PID_v2, it sends them to RSU to authenticate itself with TA. When the vehicle is considered authentic, the RSU encrypts and sends the signature key *Sk* of pseudo-IDs of the vehicle by using XOR-operations during the mutual authentication process. In this scheme, the signer computes w to migrate the verification time for the verifying recipient.

Ali *et al.* [66] designed Identity-Based Signature with Conditional Privacy-Preserving Authentication (IBS-CPPA) scheme to secure V2V communication in VANET. After the TA takes an original identity OID_i of a vehicle, it checks the weather match stored in the registration list of vehicles. If it's right, the TA computes the pool of anonymous-identities AID_i and private keys for the vehicle to join the system. The vehicle uses the anonymous-identities AID_i and private keys to sign the message during a short time. When the timestamp closes to expired, the vehicle sends an updated request to TA in obtaining a new pool of the anonymous-identities AID_i and private keys. To verify multiple messages simultaneously, this scheme supports the batch verification process on the verifying recipient side.

Cui *et al.* [67] designed an authentication scheme with privacy preservation to address the security issues and reduce the system's overhead for VANET communication. The vehicle implements the mutual authentication process with the TA to authentic itself. Therefore any adversary could not imitate the registered vehicle to broadcast fake messages. After the vehicle obtains the authentication code AC from RSU, it considers to be an authentic vehicle and allows to sign the message during the broadcasting process in VANET.

Tables 9 and 10 show a summary of the security and privacy requirements that are achieved by ECC algorithm based, respectively. Table 11 presents the level of resistance to security attack is achieved by ECC based. Table 12 presents an ECC-based evaluation metric in terms of computation and communication costs.

VI. CRITICAL DISCUSSION

Recently, researchers use the ID-SP, in which the sender signs the message by using its public key of which is derived from identity information. In contrast, the verifying recipient uses a private key to generate a TA to verify the number of messages. In this approach, the researchers use bilinear pair or ECC cryptography to sign and verify the message during the broadcasting. Besides, they also use the map-to-point and general way hash function in their scheme. Therefore, an attacker cannot enter the system as an authentic node or modify the message.

They considered the security requirements such as non-repudiation, integrity, authentication, traceability, and revocability in their schemes to achieve a high level of security in VANET. Therefore, many of the schemes in bilinear pair-based achieves the security requirements, as presented in Table 5. The scheme introduced in [51], [54] does not fulfill most privacy requirements, such as unobservability and unlinkability compared with other bilinear pair-based schemes, as presented in Table 6. The schemes introduced in [52], [53] are vulnerable from resistance to replay attacks, as presented in Table 7. The scheme introduced in [55] has low overhead in terms of communication overhead compared with others. In comparison, the scheme introduced in [53] has a low communication overhead compared with others, as presented in Table 8.

In the second class, the schemes such as [62], [63] save the system's private key on the TPD of the vehicle.

TABLE 9. Security requirements achieved by ECC based.

	Security Requirements				
Papers	**Authentication**	**Integrity**	**Non-repudiation**	**Traceability**	**Revocability**
[62]	✓	✓	✓	✓	✗
[63]	✓	✓	✓	✓	✗
[64]	✓	✓	✓	✓	✓
[65]	✓	✓	✓	✓	✓
[66]	✓	✓	✓	✓	✓
[67]	✗	✗	✗	✓	✓

TABLE 10. Privacy requirements achieved by ECC based.

	Privacy Requirements		
Papers	**Privacy-preserving**	**Unlinkability**	**Unobservability**
[62]	✓	✓	✗
[63]	✓	✓	✗
[64]	✓	✗	✗
[65]	✓	✗	✗
[66]	✓	✓	✗
[67]	✓	✓	✗

TABLE 11. Controlled ECC resistance to security attack.

resistance to security attack				
Papers	**Replay**	**Modification**	**Impersonation**	**MITM**
[62]	✓	✓	✓	✓
[63]	✓	✓	✓	✓
[64]	✓	✓	✓	✓
[65]	✓	✓	✓	✓
[66]	✓	✓	✓	✓
[67]	✗	✗	✗	✓

TABLE 12. ECC based overhead for computation and communication.

	computation (ms)		**communication**
Papers	**Singing**	**Verifying**	**(Bytes)**
[62]	2.0184	2.0216	144
[63]	0.6718	2.0154	105
[64]	1.3456	2.0236	148
[65]	0.6738	1.3477	148
[66]	2.0154	0.6749	124
[67]	1.3436	0.001	100

Thus, the signer uses it to sign a message during the broadcasting message. However, the TA cannot revoke the malicious vehicle, which leads to revocability is ignored in schemes [62], [63], as presented in Table 9. The scheme introduced in [64], [65] does not fulfil most of the privacy requirements, such as unlinkability and unobservability compared to other ECC-based schemes, as presented in Table 10. The scheme introduced in [67] is vulnerable to resistance to replay attacks, modification, and impersonation, as shown in Table 11. The scheme introduced in [67] has low communication and communication overhead compared with others, as presented in Table 12.

As a result, the schemes in the second class utilized ECC operations, are more efficient when compared with first-class, which used bilinear pair operation to sign and verify messages during the phase of broadcasting. However, the bilinear pair operations are complicated because they use cryptography and are time-consuming. Thus, these operations create massive computation and communication overheads for signing and verifying messages during the broadcast process.

VII. CONCLUSION

A vehicle plays a critical role as it not only gets the passengers from one location to another, but it also must ensure the safety is not compromised in any way. Therefore, many studies suggested VANET for enhancing and improving traffic and road management. However, the attacker can delete, alter, replay and modify the exchange message on the driving environment, disrupting the system for V2V and V2I communication. Therefore, several researchers proposed a security and privacy scheme to address the above issues. In this paper, several schemes regarding identity-based security and privacy requirements have been classified into bilinear pair-based and ECC-based schemes. The security requirements, privacy requirements, resistance to cyber-attack, and evaluation metrics are reviewed and compared for each class. This paper aims to assist researchers and developers in determining and understanding the major requirements for security, privacy, and evaluation metrics in V2V and V2I communication of VANET.

REFERENCES

[1] M. A. Alazzawi, H. Lu, A. A. Yassin, and K. Chen, "Robust conditional privacy-preserving authentication based on pseudonym root with cuckoo filter in vehicular ad hoc networks," *KSII Trans. Internet Inf. Syst.*, vol. 13, no. 12, pp. 6121–6144, 2019.

[2] J. Zhang, J. Cui, H. Zhong, Z. Chen, and L. Liu, "PA-CRT: Chinese remainder theorem based conditional privacy-preserving authentication scheme in vehicular ad-hoc networks," *IEEE Trans. Dependable Secure Comput.*, vol. 18, no. 2, pp. 722–735, Mar. 2021.

[3] J. Cui, L. Wei, H. Zhong, J. Zhang, Y. Xu, and L. Liu, "Edge computing in VANETs—An efficient and privacy-preserving cooperative downloading scheme," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 6, pp. 1191–1204, Jun. 2020.

[4] D. Manivannan, S. S. Moni, and S. Zeadally, "Secure authentication and privacy-preserving techniques in vehicular ad-hoc NETworks (VANETs)," *Veh. Commun.*, vol. 25, Oct. 2020, Art. no. 100247.

[5] M. Azees, P. Vijayakumar, and L. J. Deboarh, "EAAP: Efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 9, pp. 2467–2476, Sep. 2017.

[6] J. Cui, J. Chen, H. Zhong, J. Zhang, and L. Liu, "Reliable and efficient content sharing for 5G-enabled vehicular networks," *IEEE Trans. Intell. Transp. Syst.*, early access, Sep. 24, 2020, doi: 10.1109/TITS.2020.3023797.

[7] P. Vijayakumar, M. Azees, and L. J. Deborah, "CPAV: Computationally efficient privacy preserving anonymous authentication scheme for vehicular ad hoc networks," in *Proc. IEEE 2nd Int. Conf. Cyber Secur. Cloud Comput.*, Nov. 2015, pp. 62–67.

[8] A. Kaci, T. Bouabana-Tebibel, A. Rachedi, and C. Yahiaoui, "Toward a big data approach for indexing encrypted data in cloud computing," *Secur. Privacy*, vol. 2, no. 3, p. e65, May 2019.

[9] Y. Yahiatene, D. E. Menacer, M. A. Riahla, A. Rachedi, and T. B. Tebibel, "Towards a distributed ABE based approach to protect privacy on online social networks," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2019, pp. 1–7.

[10] A. Kaci, A. Nacef, and A. Henni, "Mobile cloud system for road safety," in *Proc. Int. Conf. Geoinformat. Data Anal.*, Apr. 2018, pp. 132–136.

[11] A. Kaci and A. Rachedi, "Mc-Track: A cloud based data oriented vehicular tracking system with adaptive security," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2019, pp. 1–6.

[12] Y. Yahiatene, A. Rachedi, M. A. Riahla, D. E. Menacer, and F. Nait-Abdesselam, "A blockchain-based framework to secure vehicular social networks," *Trans. Emerg. Telecommun. Technol.*, vol. 30, no. 8, p. e3650, Aug. 2019.

[13] A. Alamer, Y. Deng, G. Wei, and X. Lin, "Collaborative security in vehicular cloud computing: A game theoretic view," *IEEE Netw.*, vol. 32, no. 3, pp. 72–77, May/Jun. 2018.

[14] A. Alamer and S. Basudan, "An efficient truthfulness privacy-preserving tendering framework for vehicular fog computing," *Eng. Appl. Artif. Intell.*, vol. 91, May 2020, Art. no. 103583.

[15] A. Alamer, S. Basudan, and X. Lin, "A privacy-preserving incentive framework for the vehicular cloud," in *Proc. IEEE Int. Conf. Internet Things (iThings), IEEE Green Comput. Commun. (GreenCom), IEEE Cyber, Phys. Social Comput. (CPSCom), IEEE Smart Data (SmartData)*, Jul. 2018, pp. 435–441.

[16] X. Li, T. Liu, M. S. Obaidat, F. Wu, P. Vijayakumar, and N. Kumar, "A lightweight privacy-preserving authentication protocol for VANETs," *IEEE Syst. J.*, vol. 14, no. 3, pp. 3547–3557, Sep. 2020.

[17] M. A. Al-Shareeda, M. Anbar, M. A. Alazzawi, S. Manickam, and A. S. Al-Hiti, "LSWBVM: A lightweight security without using batch verification method scheme for a vehicle ad hoc network," *IEEE Access*, vol. 8, pp. 170507–170518, 2020.

[18] S. H. Islam, M. S. Obaidat, P. Vijayakumar, E. Abdulhay, F. Li, and M. K. C. Reddy, "A robust and efficient password-based conditional privacy preserving authentication and group-key agreement protocol for VANETs," *Future Gener. Comput. Syst.*, vol. 84, pp. 216–227, Jul. 2018.

[19] Z. Lu, G. Qu, and Z. Liu, "A survey on recent advances in vehicular network security, trust, and privacy," *IEEE Trans. Intell. Transp. Syst.*, vol. 20, no. 2, pp. 760–776, Feb. 2018.

[20] M. Muhammad and G. A. Safdar, "Survey on existing authentication issues for cellular-assisted V2X communication," *Veh. Commun.*, vol. 12, pp. 50–65, Apr. 2018.

[21] M. A. Al-shareeda, M. Anbar, S. Manickam, and I. H. Hasbullah, "An efficient identity-based conditional privacy-preserving authentication scheme for secure communication in a vehicular ad hoc network," *Symmetry*, vol. 12, no. 10, p. 1687, Oct. 2020.

[22] S. S. Manvi and S. Tangade, "A survey on authentication schemes in VANETs for secured communication," *Veh. Commun.*, vol. 9, pp. 19–30, Jul. 2017.

[23] M. Azees and P. Vijayakumar, "CEKD: Computationally efficient key distribution scheme for vehicular ad-hoc networks," *Austral. J. Basic Appl. Sci.*, vol. 10, no. 2, pp. 171–175, 2016.

[24] *Global Status Report on Road Safety 2021*, World Health Org., Geneva, Switzerland, 2021.

[25] I. Ali, M. Faisal, and S. Abbas, "A survey on lightweight authentication schemes in vertical handoff," *Int. J. Cooperat. Inf. Syst.*, vol. 26, no. 1, Mar. 2017, Art. no. 1630001.

[26] C. Zhang, X. Zhu, Y. Song, and Y. Fang, "A formal study of trust-based routing in wireless ad hoc networks," in *Proc. IEEE INFOCOM*, Mar. 2010, pp. 1–9.

[27] M. A. Al-Shareeda, M. Anbar, S. Manickam, and A. A. Yassin, "VPPCS: VANET-based privacy-preserving communication scheme," *IEEE Access*, vol. 8, pp. 150914–150928, 2020.

[28] S. Wang, K. Mao, F. Zhan, and D. Liu, "Hybrid conditional privacy-preserving authentication scheme for VANETs," *Peer Peer Netw. Appl.*, vol. 13, no. 5, pp. 1–16, 2020.

[29] J. B. Kenney, "Dedicated short-range communications (DSRC) standards in the United States," *Proc. IEEE*, vol. 99, no. 7, pp. 1162–1182, Jul. 2011.

[30] D. Jiang, V. Taliwal, A. Meier, W. Holfelder, and R. Herrtwich, "Design of 5.9 GHz DSRC-based vehicular safety communication," *IEEE Wireless Commun.*, vol. 13, no. 5, pp. 36–43, Oct. 2006.

[31] X. Yang, X. Yi, I. Khalil, Y. Zeng, X. Huang, S. Nepal, X. Yang, and H. Cui, "A lightweight authentication scheme for vehicular ad hoc networks based on MSR," *Veh. Commun.*, vol. 15, pp. 16–27, Jan. 2019.

[32] J. Jakubiak and Y. Koucheryavy, "State of the art and research challenges for VANETs," in *Proc. 5th IEEE Consum. Commun. Netw. Conf.*, 2008, pp. 912–916.

[33] M. S. Sheikh, J. Liang, and W. Wang, "A survey of security services, attacks, and applications for vehicular ad hoc networks (VANETs)," *Sensors*, vol. 19, no. 16, p. 3589, Aug. 2019.

[34] M. R. Jabbarpour, H. Zarrabi, R. H. Khokhar, S. Shamshirband, and K.-K.-R. Choo, "Applications of computational intelligence in vehicle traffic congestion problem: A survey," *Soft Comput.*, vol. 22, no. 7, pp. 2299–2320, Apr. 2018.

[35] J. Cui, D. Wu, J. Zhang, Y. Xu, and H. Zhong, "An efficient authentication scheme based on semi-trusted authority in VANETs," *IEEE Trans. Veh. Technol.*, vol. 68, no. 3, pp. 2972–2986, Mar. 2019.

[36] M. Wazid, A. K. Das, R. Hussain, G. Succi, and J. J. P. C. Rodrigues, "Authentication in cloud-driven IoT-based big data environment: Survey and outlook," *J. Syst. Archit.*, vol. 97, pp. 185–196, Aug. 2019.

[37] F. Qu, Z. Wu, F.-Y. Wang, and W. Cho, "A security and privacy review of VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 6, pp. 2985–2996, Dec. 2015.

[38] I. Ali, A. Hassan, and F. Li, "Authentication and privacy schemes for vehicular ad hoc networks (VANETs): A survey," *Veh. Commun.*, vol. 16, pp. 45–61, Apr. 2019.

[39] F. Ahmad, A. Adnane, V. N. Franqueira, F. Kurugollu, and L. Liu, "Man-in-the-middle attacks in vehicular ad-hoc networks: Evaluating the impact of attackers' strategies," *Sensors*, vol. 18, no. 11, p. 4040, 2018.

[40] Scale Structures Limited. (2018). *Multi Precision Integer and Rational Arithmetic Cryptographic Library (MIRACL)*. [Online]. Available: http://www.certivox.com/miracl/

[41] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proc. Workshop Appl. Cryptograph. Techn.* Berlin, Germany: Springer, 1984, pp. 47–53.

[42] F. Hess, "Efficient identity based signature schemes based on pairings," in *Proc. Int. Workshop Sel. Areas Cryptogr.* Berlin, Germany: Springer, 2002, pp. 310–324.

[43] M. A. Al-Shareeda, M. Anbar, I. H. Hasbullah, and S. Manickam, "Survey of authentication and privacy schemes in vehicular ad hoc networks," *IEEE Sensors J.*, vol. 21, no. 2, pp. 2422–2433, Jan. 2021.

[44] A. Rahim, X. Kong, F. Xia, Z. Ning, N. Ullah, J. Wang, and S. K. Das, "Vehicular social networks: A survey," *Pervasive Mobile Comput.*, vol. 43, pp. 96–113, Jan. 2018.

[45] A. Boualouache, S.-M. Senouci, and S. Moussaoui, "A survey on pseudonym changing strategies for vehicular ad-hoc networks," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 1, pp. 770–790, 1st Quart., 2017.

[46] S. Sharma and A. Kaul, "A survey on intrusion detection systems and honeypot based proactive security mechanisms in VANETs and VANET cloud," *Veh. Commun.*, vol. 12, pp. 138–164, Apr. 2018.

[47] J. Wang, Y. Shao, Y. Ge, and R. Yu, "A survey of vehicle to everything (V2X) testing," *Sensors*, vol. 19, p. 334, Jan. 2019.

[48] P. Sewalkar and J. J. S. Seitz, "Vehicle-to-pedestrian communication for vulnerable road users: Survey, design considerations, and challenges," *Sensors*, vol. 19, no. 2, p. 358, 2019.

[49] Z. Jianhong, X. Min, and L. Liying, "On the security of a secure batch verification with group testing for VANET," *Int. J. Netw. Secur.*, vol. 16, no. 5, pp. 351–358, 2014.

[50] L. Zhang, Q. Wu, J. Domingo-Ferrer, B. Qin, and C. Hu, "Distributed aggregate privacy-preserving authentication in VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 3, pp. 516–526, Mar. 2016.

[51] S. Wang and N. Yao, "LIAP: A local identity-based anonymous message authentication protocol in VANETs," *Comput. Commun.*, vol. 112, pp. 154–164, Nov. 2017.

[52] S. M. Pournaghi, B. Zahednejad, M. Bayat, and Y. Farjami, "NECPPA: A novel and efficient conditional privacy-preserving authentication scheme for VANET," *Comput. Netw.*, vol. 134, pp. 78–92, Apr. 2018.

[53] M. Bayat, M. Pournaghi, M. Rahimi, and M. Barmshoory, "NERA: A new and efficient RSU based authentication scheme for VANETs," *Wireless Netw.*, vol. 26, pp. 1–16, Jul. 2019.

[54] M. Bayat, M. Barmshoory, S. M. Pournaghi, M. Rahimi, Y. Farjami, and M. R. Aref, "A new and efficient authentication scheme for vehicular ad hoc networks," *J. Intell. Transp. Syst.*, vol. 24, no. 2, pp. 171–183, 2020.

[55] I. Ali and F. Li, "An efficient conditional privacy-preserving authentication scheme for vehicle-to-infrastructure communication in VANETs," *Veh. Commun.*, vol. 22, Apr. 2020, Art. no. 100228.

[56] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," in *Proc. Annu. Int. Cryptol. Conf.* Berlin, Germany: Springer, 2001, pp. 213–229.

[57] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the Weil pairing," in *Proc. Int. Conf. Appl. Cryptol. Inf. Secur.* Berlin, Germany: Springer, 2001, pp. 514–532.

[58] C.-C. Lee and Y.-M. Lai, "Toward a secure batch verification with group testing for VANET," *Wireless Netw.*, vol. 19, no. 6, pp. 1441–1449, 2013.

[59] S. Biswas, M. M. Haque, and J. V. Misic, "Privacy and anonymity in VANETs: A contemporary study," *Ad Hoc Sensor Wireless Netw.*, vol. 10, nos. 2–3, pp. 177–192, 2010.

[60] V. Miller, "Use of elliptic curves in cryptography," in *Proc. Conf. Appl. Cryptograph. Techn.* Berlin, Germany: Springer, 1985, pp. 417–426.

[61] N. Koblitz, "Elliptic curve cryptosystems," *Math. Comput.*, vol. 48, no. 177, pp. 203–209, 1987.

[62] D. He, S. Zeadally, B. Xu, and X. Huang, "An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 12, pp. 2681–2691, Dec. 2015.

[63] N.-W. Lo and J.-L. Tsai, "An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks without pairings," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 5, pp. 1319–1328, May 2016.

[64] L. Wu, J. Fan, Y. Xie, J. Wang, and Q. Liu, "Efficient location-based conditional privacy-preserving authentication scheme for vehicle ad hoc networks," *Int. J. Distrib. Sensor Netw.*, vol. 13, no. 3, Mar. 2017, Art. no. 155014771770089.

[65] M. A. Alazzawi, H. Lu, A. A. Yassin, and K. Chen, "Efficient conditional anonymity with message integrity and authentication in a vehicular ad-hoc network," *IEEE Access*, vol. 7, pp. 71424–71435, 2019.

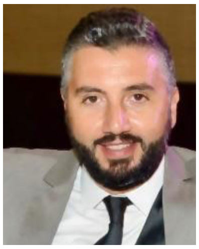
[66] I. Ali, T. Lawrence, and F. Li, "An efficient identity-based signature scheme without bilinear pairing for vehicle-to-vehicle communication in VANETs," *J. Syst. Archit.*, vol. 103, Feb. 2020, Art. no. 101692.

[67] J. Cui, W. Xu, Y. Han, J. Zhang, and H. Zhong, "Secure mutual authentication with privacy preservation in vehicular ad hoc networks," *Veh. Commun.*, vol. 21, Jan. 2020, Art. no. 100200.

MAHMOOD A. AL-SHAREEDA received the B.S. degree in communication engineering from Iraq University College and the M.Sc. degree in information technology from Islamic University of Lebanon (IUL), in 2018. He is currently pursuing the Ph.D. degree with the National Advance IPv6 Center (NAv6), Universiti Sains Malaysia (USM). His research interests include security and privacy issues in vehicular *ad-hoc* networks (VANETs) and network optimization.

MOHAMMED ANBAR received the Ph.D. degree in advanced computer network from University Sains Malaysia (USM). He is currently a Senior Lecturer with the National Advanced IPv6 Centre (NAv6), USM. His current research interests include malware detection, web security, intrusion detection systems (IDSs), intrusion prevention systems (IPSs), network monitoring, the Internet of Things (IoT), vehicular *ad-hoc* network (VANET) security, and IPv6 security.

SELVAKUMAR MANICKAM is currently working as an Associate Professor with the National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia. He has ten years of industrial experience prior to joining academia. He also has experience in building the IoT, embedded, server, mobile, and web-based applications. He has authored or coauthored more than 160 articles in journals, conference proceedings, and book reviews, and graduated 13 Ph.D. students. His research interests include cybersecurity, the Internet of Things, industry 4.0, and machine learning. He is a member of technical forums at national and international levels.



AYMAN KHALIL received the M.Sc. degree in networking and telecommunications from Lebanese University/Saint Joseph University, Beirut, Lebanon, in 2007, and the Ph.D. degree in telecommunications from the National Institute of Applied Sciences (INSA), Rennes, France, in 2010. During his Ph.D., he was with the Institute of Electronics and Telecommunications of Rennes (IETR), where he worked on the optimization of high data rate WPAN systems. He has been involved in supervising Ph.D. students in Lebanon and France. He has been involved in several European projects, including OMEGA, where he worked for three years in developing solutions and protocols for next generation home networks. His main research interests include next generation wireless systems, heterogeneous networks, network coding, cross-layer resource allocation, and optimization.

IZNAN HUSAINY HASBULLAH received the Bachelor of Science degree in electrical engineering from Rensselaer Polytechnic Institute, Troy, NY, USA. He is currently pursuing the M.Sc. degree in advanced network security. He has work experience as a Software Developer, Research and Development Consultant, and Network Security Auditor. Since 2010, he has been with the National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia, as a Research Officer. His research interests include unified communication, telematics, network security, network protocols, and next generation networks.