Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.18576/amis/140602

NE-CPPA: A New and Efficient Conditional Privacy-Preserving Authentication Scheme for Vehicular Ad Hoc Networks (VANETs)

Mahmood A. Al-shareeda [1], *Mohammed Anbar*[1,*], *Selvakumar Manickam*[1], *Iznan H. Hasbullah*[1], *Nibras Abdullah*[2], *Mustafa Maad Hamdi*[3] *and Ahmed Shakir Al-Hiti*[4]

[1]National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia, 11800 USM, Penang, Malaysia
[2]Faculty of Computer Science and Engineering, Hodeidah University, Hodeidah, Yemen
[3]Faculty of Electrical and Electronic Engineering, Universiti Tun Hussein Onn Malaysia 86400 Parit Raja, Batu Pahat, Johor, Malaysia
[4]Department of Electrical Engineering, Faculty of Engineering, University of Malaya, Kuala Lumpur 50630, Malaysia

Received: 23 Jun. 2020, Revised: 2 Aug. 2020, Accepted: 10 Sep. 2020
Published online: 1 Nov. 2020

Abstract: Vehicular ad-hoc networks (VANETs) are the fundamental technology for the Intelligent Transportation System (ITS) that provides drivers with a safe and comfortable driving environment. However, the inherent openness of the VANETs wireless communication channel calls for careful scrutiny of its security, privacy and efficiency. This paper proposed a New and Efficient Conditional Privacy-Preserving Authentication (NE-CPPA) scheme to secure the communication in VANETs. NE-CPPA uses the Elliptic Curve Cryptography (ECC) algorithm to fulfil the security and privacy requirements. The security analysis of the proposed scheme under various attack scenarios are presented. Then, the computation and communication costs analysis is conducted to show its feasibility and robustness. Performance evaluation showed that the NE-CPPA scheme has a lower system overhead in terms of computation and communication costs than existing schemes. Thus, the proposed NE-CPPA scheme is appropriate for securing the deployment and adoption of VANETs.

Keywords: Authentication, Identity-based Cryptography, Privacy-Preserving,Vehicular Ad Hoc Networks (VANETs).

1 Introduction

Lately, Vehicular Ad-hoc Networks (VANETs) have received considerable attention from academia, industry, and government sectors for its many benefits to road users, such as improved road safety and increased traffic management efficiency. They also provide numerous of entertainment facilities to drivers and passengers [1–4]. Since the vehicles in VANETs are similar to mobile nodes in mobile ad-hoc networks (MANETs), it is safe to consider VANETs as a subgroup of MANETs [5, 6]. Every VANET-enabled vehicle comes with an On-Board Unit (OBU) responsible for exchanging road and traffic-related information with other vehicles or Road-Side Units (RSUs) deployed along the road. This information improves the driver's awareness of the surrounding environment [7].

There are two communication modes in VANETs: vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication modes. Both modes of communication operate via the Dedicated Short-Range Communication (DSRC) protocol [8, 9]. DSRC is a short-to-medium range wireless protocol channel that allows highly critical data transmission in VANETs [10]. By the aforementioned communications, VANETs provide not only safety services for drivers, but also unprecedented comfort applications. For example, they help the driver make decision on alternative travel routes. Vehicles or nodes in VANETs collect and process useful information on driving conditions, such as weather information, emergency warnings as well as traffic information, which other vehicles need to increase the awareness of the road [11, 12].

Nowadays, VANETs have become promising technology for intelligent transportation system (ITS)

* Corresponding author e-mail: anbar@nav6.usm.my

because of the above-mentioned advantages. Nevertheless, advantages always involve challenges; for example, VANETs should consider challenges related to communication security and privacy [13–15]. First, security requirement is very critical in VANETs, which are susceptible to various security attacks [16, 17]. Thus, the attackers can easily alter or modify broadcasted messages and control of the VANET channel. Since RSUs and vehicles make decisions based on the traffic-related message received, fake messages could result in faulty decision and cause critical road incidents. Thus, to guarantee secure communication [18–21], the authentication and integrity of the received messages must be ensured before further assessment or decision are made. Second, privacy-preserving problem has also become critical. An attacker can acquire a vehicle's original identity and then track its traveling routes by evaluating the content of certain captured messages in VANETs [22–25]. However, since the personal information of drivers would be known to others, drivers are reluctant to use the emerging technology for VANETs. Therefore, anonymous communication and unlinkability features are required to protect the privacy of vehicles. In addition to the requirements of security and privacy, performance efficiency is important in VANETs. Despite the capability of the vehicle with a powerful device, its principal aim emphasizes on mobility rather than computation [26–30].

Several schemes that address VANET's secure authentication and privacy-preserving requirements have been proposed. Although some existing schemes were able to satisfy most of these VANET requirements, they are not completely safe. They also have huge overhead in terms of computation and communication costs. Contributions of this paper are defined, as follows:

- A new and efficient conditional privacy-preserving authentication (NE-CPPA) scheme to guarantee secure communication in VANET using the Elliptic Curve Cryptography (ECC) algorithm to fulfill the security and privacy requirements
- A scheme with lower computation and communication costs compared to other existing schemes by not using the bilinear pairing.

The rest of the paper is organized as follows: Section 2 introduces the related work for VANETs. The preliminaries on the basis of a detailed description of the proposed scheme are presented in Section 3. Sections 4 presents the proposed scheme on VANETs. Discussion is presented in Section 5. Section 6 is devoted to the proposed NE-CPPA.

2 Related works

The existing research related to security and privacy issues are have been classified into two main categories:

2.1 Group signature-based CPPA schemes

Chaum and Van Heyst [31] are the first to propose the idea of using group signature as a basis for a CPPA scheme for VANETs. A group member's signature could be anonymously generated on behalf of the whole group, and a secret group key could be utilized by the group manager to disclose the identifying information of the group member's signature. Many researchers have proposed security and privacy schemes for VANETs that fall under the group signature-based CPPA category [32–40]. In the Lin et al. [39] GSIS scheme, the Trusted Authority (TA) generates the public and private keys of the group and then stores them in the vehicle, which eliminates the burden of the certificates management. Moreover, since only the group manager knows the secret group key, other group members would not be able to disclose the identity information of the signature. However, if there exists a large number of revoked vehicles, the size of the certificate revocation list (CRL) also increased. Since every CRL operation involves two bilinear pairing operations, the computation overhead for the verifier will increase significantly. Moreover, the computation cost of group signature-based CPPA schemes is already higher than the general signature to begin with.

2.2 Identity-based CPPA schemes

Several researchers have suggested identity-based CPPA schemes to overcome the shortcoming of group signature-based CPPA schemes. In 1984, Shamir [41] first introduced identity-based CPPA scheme, where the identity information is used as the public key of the node, and the TA used the same identity information to generate a private key and then distributes it to nodes. The receivers authenticate the traffic-related message using the sender's public key, and the message is signed with the sender's private key.

Zhang et al. [42] proposed an identity-based CPPA scheme using bilinear mapping that can guarantee the security and privacy of VANET users. However, Lee and Lai [43] detected that [42] were not able to withstand some security attacks in VANETs. First, the verifier might repeat the checking of the signature that has already been checked because of lack of a required tool, which increases the computation overhead. This means that a replay attack could not be prevented. Second, the scheme in [42] cannot achieve non-repudiation. The signer may argue that a reputable institution has not sent the disputed messages to track identity information. Lee and Lai proposed an enhanced privacy preservation scheme [43] to resolve the security issues in [42]. J. Zhang [44] and Bayat et al. [45] discovered that Lee and Lai [43] scheme cannot withstand the impersonation attack. An attacker could broadcast false messages to gain the benefit and give himself some comfort considered as legal vehicle.

Two new and improved schemes have been proposed to overcome the present problems in [43]. Pournaghi et al. [46] proposed an authentication scheme, called NECPPA, which provides secure communications in VANET. In their scheme, the public parameters of the TA are kept in the Tamper Proof Device (TPD) of RSUs, which ensures security and provides fast communication link between the TA and RSU. Meanwhile, Bayat et al. [47] proposed an identity-based CPPA scheme that depends on an RSU, where the master key of the TA is kept within TPD of OBUs. Lei Zhang et al. [48] introduced a multiple trusted authority to propose an identity-based aggregate signature process. With this technique, a vehicle can authenticate a various messages at the same time. Zhong et al. [49] detected that Lei Zhang et al. scheme [48] does not define the sender in the verification process and has a large authentication signature overhead. Hence, an enhanced scheme to resolve the above-mentioned issues was proposed. We et al. [50] proposed an efficient CPPA scheme based on location without the bilinear pairing and tamper-proof device. However, He et al. [51] proposed an identity-based CPPA scheme without bilinear mapping. In their scheme, during message broadcast, an attacker may tamper with the vehicle's signature.

The existing CPPA schemes can be classified into two groups, each one addresses its own challenges in VANET. Both operations of bilinear pairing and map-to-point function are utilized in the first group [42–49] in the signature verification process, which create high computation and communication costs for the receiver. The schemes in the second group [50, 51] utilize the Elliptic Curve Cryptography (ECC), which is more efficient and makes the batch verification process possible. However, the four-point multiplication operations in [50] can lead to delay in a signature verification; while [51] uses three-point multiplication operations.

In the following sections, a new and efficient conditional privacy-preserving authentication (NE-CPPA) scheme is proposed to secure the communication channel in VANETs. NE-CPPA uses the Elliptic Curve Cryptography (ECC) algorithm to achieve security and privacy requirements. Furthermore, the NE-CPPA scheme will be compared with other schemes to show the improvement in terms of computation and communication costs.

3 preliminary

3.1 System model

This subsection presents the system model of the NE-CPPA scheme. NE-CPPA scheme comprises three main components: a Trusted Authority (TA), Road-Side Units (RSUs), and On-Board Units (OBUs), as shown in Figure 1.

–TA is a trustworthy third party with powerful capability responsible for the registration of other components in VANETs.
–RSUs are located along the neighboring road that operates as a proxy or intermediate entity between the vehicles and the application server.
–OBU is fitted on each VANET-enabled vehicle and communicates with other vehicles or RSUs using the DSRC protocol. In each OBU, a TPD prevents the attackers from obtaining the stored information.

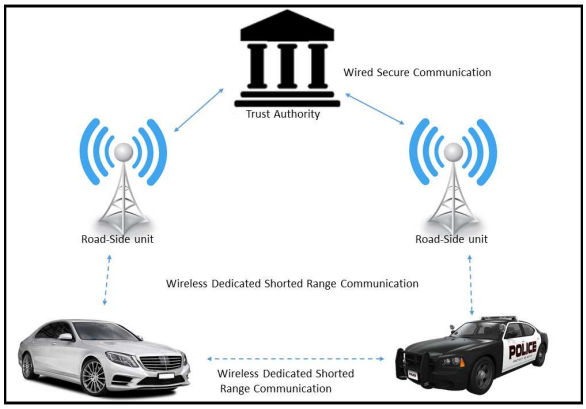

Fig. 1: Typical Structure of VANET

3.2 Security and privacy requirements

The proposed scheme should satisfy the following security and piracy requirements.

–Message Integrity and Authentication: The receiver should have the ability to authenticate the received message and ensure that the sender is authentic.
–Privacy-preserving: The attacker should not be able to disclose the identity of vehicles from the broadcasted messages.
–Non-repudiation: The message sent by a vehicle itself cannot be refuted by the sender.
–Unlinkability: The attacker should not be able to link multiple messages to a particular vehicle.
–Traceability: By analyzing the exchanged message during communication, only the TA should be able to track the identity of the vehicle that broadcasts false information in the VANETs.
–Resistance to Attacks: An effective security scheme in VANET should withstand common attacks such as impersonation, replay, and modification attacks.

Table 1: Notation and their description

Notation	Descriptions
E	An elliptic curve
G	An additive group based on E
a,b	Two large prime number
p	large prime number
P	The base generator P$\in$ G
h_1,h_2,h_3	Three one-way hash function
OID_i	Original identity of vehicle
PW	Password
s_{pri}^{TA}	The private master key of the system
P_{Pub}	The public key of the TA
r	Random integer
$\|$	Concatenation operation
$\oplus$	XOR operator

3.3 Attack model

The nature of the VANET environment renders the vehicle vulnerable to security attacks [52]. Some of the security attacks on VANETs are as follows:

–Reply Attack The attacker replays the legal signature previously received by the recipient.
–Impersonation Attack An attacker could falsify valid vehicle signatures and submit them to other nodes.
–Modification Attack An attacker can change and send a legitimate message to others [53].

4 The proposed scheme

The NE-CPPA scheme comprises five phases: initialization, registration, message signing, message verification, and identity tracking phases. Table 1 presents the basic notations used in describing NE-CPPA scheme.

4.1 System initialization Phase

The TA sets up in generating the public parameters of the system as follows:

–The TA randomly selects two large numbers (p and q). Then TA selects a non-singular elliptic curve E representing $y^2 = x^3 + b \bmod p$, where $a,b \in Fp$ is defined. Then the TA selects a group of elliptic curve points with a q prime order and a P generator of G.
–The TA randomly chooses secret value $s_{pri}^{TA} \in Z_q^*$ as the private master key of the system, and then computes its corresponding master public key as $P_{Pub} = s_{pri}^{TA}.P$.
–The TA chooses three secure cryptographic hash functions as: $h_1 : G \rightarrow Z_q^*$ $h_2 : \{0,1\}^* \times \{0,1\}^* \times G \rightarrow Z_q^*$ $h_3 : \{0,1\}^* \rightarrow Z_q^*$

4.2 Registration phase

In this phase, the authentication registration process takes place for the new participants.

4.2.1 RSU Registration

RSU are registered by the TA as follows:

–The TA preloads the public parameters parmas = $\{p, q, a, b, P, P_{Pub}, h_1, h_2, h_3\}$ for each RSU.

4.2.2 OBU Registration

Vehicle are registered by the TA as follows:

–The TA preloads the public parameters parmas = $\{p, q, a, b, P, P_{Pub}, h_1, h_2, h_3\}$ for each OBU.
–The TA stores the master private key s_{pri}^{TA} in TPD of OBU, which prevents the stored information from being disclosed to attackers.

4.3 Signing message phase

In this phase, for the OBU_i to sign a message Mi, the steps below must be executed, where OID_i is the original identity of the vehicle and T_i is the timestamp.

–OBU_i selects a random integer $z_i \in Z_q^*$ first.
–OBU_i generates the pseudo-ID $pID_i = \{pID_i^1 , pID_i^2 \}$ and its relevant private key as follows:
$pID_i^1 = z_i P$
$pID_i^2 = OID_i \oplus h_1(z_i P_{Pub})$
$SK_i = s_{pri}^{TA}.h_2(pID_i^1 \| pID_i^2 \| T_i)$.
–OBU_i computes the signature of message as follows:
$\delta_m = SK_i + z_i.h_3(M_i \| T_i)$
–OBU_i computes $\vartheta = h_3(M_i \| T_i).pID_i^1$ and sets $\sigma_m = \{\delta_m, \vartheta\}$
–OBU_i broadcasts the signature-message $\{M_i, T_i, pID_i, \sigma_m\}$ to nearby RSU or other vehicles.

4.4 Verification message phase

After the recipient receives the signature-message $\{M_i, T_i, pID_i, \sigma_m\}$, it first verifies the timestamps Ti validity. For example, assume T_r is the time of receipt, T_i is valid if ($T_I > T_r$ - T_∇), where T_∇ is the time delay predefined. If ok, the message continues with one of the next verification:

4.4.1 Single message verification

The receiver checks the Equation 1 and accepts the message if it holds.

$$\delta_m.P = h_2(pID_i^1 \| pID_i^2 \| T_i) P_{Pub} + \vartheta \quad (1)$$

The proof of Equation 1 is as follows:

$$\begin{aligned}\delta_m.P &= (SK_i + z_i.h_3(M_i \| T_i)).P \\ &= s_{pri}^{TA}.h_2(pID_i^1 \| pID_i^2 \| T_i) + z_i.h_3(M_i \| T_i).P \\ &= h_2(pID_i^1 \| pID_i^2 \| T_i) s_{pri}^{TA}.P + h_3(M_i \| T_i) z_i.P \\ &= h_2(pID_i^1 \| pID_i^2 \| T_i) P_{Pub} + h_3(M_i \| T_i) pID_i^1 \\ &= h_2(pID_i^1 \| pID_i^2 \| T_i) P_{Pub} + \vartheta\end{aligned}$$

4.4.2 Batch message verification

Verifier receives various signature-messages $\{M_i^1, T_i^1, pID_i^1, \sigma_m^1\}$; $\{M_i^2, T_i^2, pID_i^2, \sigma_m^2\}$;.....;$\{M_i^n, T_i^n, pID_i^n, \sigma_m^n\}$ can be simultaneously checked as below.

$$\sum_{i=1}^{n} (\delta_m).P = \sum_{i=1}^{n} \left(h_2(pID_i^1 \| pID_i^2 \| T_i) \right) P_{Pub} + \sum_{i=1}^{n} \vartheta \quad (2)$$

The proof of Equation 2 is as follows:

$$\begin{aligned}&L.H.S \sum_{i=1}^{n} (\delta_m.P) \\ &= \sum_{i=1}^{n} \left(s_{pri}^{TA}.h_2(pID_i^1 \| pID_i^2 \| T_i) + z_i.h_3(M_i \| T_i) \right).P \\ &= \sum_{i=1}^{n} (h_2(pID_i^1 \| pID_i^2 \| T_i) s_{pri}^{TA}.P) + \sum_{i=1}^{n} (h_3(M_i \| T_i) z_i.P) \\ &= \sum_{i=1}^{n} (h_2(pID_i^1 \| pID_i^2 \| T_i) P_{Pub}) + \sum_{i=1}^{n} (h_3(M_i \| T_i) pID_i^1) \\ &= \sum_{i=1}^{n} (h_2(pID_i^1 \| pID_i^2 \| T_i) P_{Pub}) + \sum_{i=1}^{n} (\vartheta) \\ &= R.H.S\end{aligned}$$

4.5 Original identity tracking phase

When a malicious vehicle report is received, the TA can easily trace the malicious vehicle by disclosing the original identity of the vehicle as follows:

$$OID_i = pID_i^2 \oplus h_1(s_{pri}^{TA}.pID_i^1) \quad (3)$$

5 Discussion

5.1 Security Analysis

This section presents a part of NE-CPPA scheme that ensures security and privacy requirements are achieved.

5.1.1 Message authentication and integrity

An adversary cannot modify a valid signature-message in NE-CPPA scheme, and a recipient can verify that the message $\{M_i, T_i, pID_i, \sigma_m\}$ has integrity and legality by verifying whether $\delta_m.P = h_2(pID_i^1 \| pID_i^2 \| T_i) P_{Pub} + \vartheta$ holds. Therefore, the NE-CPPA scheme has satisfied the message authentication and integrity requirements.

5.1.2 Privacy-preserving

The vehicle uses OID_i to create the pID_i that are included in the signature-message, where $pID_i^1 = z_i.P$, $pID_i^2 = OID_i \oplus h_1(z_i P_{Pub})$, and $z_i \in Z_q^*$ is a random integer number. It is very difficult for an adversary to link the rapidly changing pseudonyms with the vehicle, and it is impossible for the attacker to obtain the vehicle location. Thus, the NE-CPPA scheme has satisfied the privacy-preserving requirement.

5.1.3 Unlinkability

During the signing message phase, a pseudo-ID $pID_i = \{pID_i^1, pID_i^2\}$ is used to create the signature. An anonymous description of the vehicle in the other message is rendered by different random numerals z_i. NE-CPPA scheme also utilizes a present timestamp and expired time to calculate the signature. The attacker that attempts to link two signature-messages may fail because of the difference in their pseudo-ID and timestamp. Hence, the NE-CPPA scheme has satisfied the unlinkability requirement.

5.1.4 Non-repudiation

This process occurs when the TA traces the OID_i of a signature-message broadcasted to the system, where $pID_i^2 = OID_i \oplus h_1(z_i P_{Pub})$. This signature-message $\{M_i, T_i, pID_i, \sigma_m\}$ prevents denial by the sender as the OBUs sent messages based on their own unique OID_i. Therefore, the NE-CPPA scheme has satisfied the non-repudiation requirement.

5.1.5 Traceability

Even though there is no information about OID_i in the NE-CPPA scheme, as specified in Section 4.5, the TA can trace a malicious vehicle. Consequently, the NE-CPPA scheme has satisfied the traceability.

5.2 Attack scenarios

5.2.1 Theorem 1. The NE-CPPA scheme resists the replay attack

In accordance with the content of signature-message $\{M_i, T_i, pID_i, \sigma_m\}$, where $\sigma_m = \{\delta_m, \vartheta\}$ and $\delta_m = SK_i + z_i.h_3(M_i\|T_i)$, another timestamp cannot be used because the attack resulted in different values of σ_m. Furthermore, the recipient first verifies the timestamp. If ok, then it rejects it. Therefore, the replay attack fails in NE-CPPA scheme.

5.2.2 Theorem 2. The NE-CPPA scheme resists the modification attack

By σ_m that is embedded in each signature-message, the system can identify that the message changed if the adversary changes a message. Thus, modification attack fails in the NE-CPPA scheme.

5.2.3 Theorem 3. The NE-CPPA scheme resists the impersonation attacks

The attacker must have the master private key of the system s_{pri}^{TA} to send a valid signature-message by impersonating an authentic vehicle. According to the signature-message content $\{M_i, T_i, pID_i, \sigma_m\}$, the attacker cannot compute the signature $SK_i = s_{pri}^{TA}.h_2(pID_i^1\|pID_i^2\|T_i)$ without knowing s_{pri}^{TA}. Therefore, the NE-CPPA scheme successfully prevents the impersonation attack.

5.3 Performance evaluation

5.3.1 Comparison of computation costs

This subsection analyzes the results of the comparison between NE-CPPA scheme and Pournaghi et al. [46], Bayat et al. [47], We et al. [50], and He et al. [51] schemes in terms of computation cost. The operation of cryptography in [46, 47] are established on bilinear pairings. However, [50, 51] and the NE-CPPA scheme are established on ECC.

This research has been implemented using MIRACL's [54] cryptographic library to calculate the time required for various cryptographic operations. The hardware platform runs on an Intel® Core™ 2 Quad 2.66 GHz processor with 4 GB memory and running Windows 7 operating system. Table 2 shows the definition of and execution times for each associated cryptographic operation.

For simplicity, Let *MSP*, *SMVP*, and *BMVP* denote the message signing phase, single message verification phase, and batch message verification phase, respectively.

Table 2: Definitions and time of cryptographic operation [55,56]

Abbr.	Execution time(ms)	Definition
T_{bp}	5.811	Bilinear pairing operation
T_{bp}^{sm}	1.5654	Scalar multiplication operation in a group based on bilinear pairing
T_{bp}^{pa}	0.0106	Point addition operation in a group based on bilinear pairing
T_{mtp}	4.1724	Map-to-point hash function
T_{ecc}^{sm}	0.6718	Scalar multiplication operation in a group based on ECC
T_{ecc}^{pa}	0.0031	Point addition operation in a group based on ECC
T_h	0.001	General hash function operation

In Bayat et al. [47], *MSP* includes only one map-to-point hash function. Thus, *MSP* overall computation cost is $1T_{mtp} \approx 4.1724$ ms. This scheme has three operations of bilinear pairing: a scalar multiplication, and a map-to-point hash function, which gives the *SMVP* an overall computation cost of $3T_{bp} + 1T_{bp}^{sm} + 1T_{mtp} \approx 23.1708$ ms. While *BMVP* in this scheme includes three operations bilinear pairing: n scalar multiplications, and n map-to-point hash functions. The overall computation cost for *BMVP* is $3T_{bp} + nT_{bp}^{sm} + nT_{mtp} \approx 5.7378$n+17.4333 ms.

In NE-CPPA scheme, *MSP* consists of three scalar multiplications, one point addition operation and two secure hash functions, so $3T_{ecc}^{sm} + 1T_{ecc}^{pa} + 2T_h$= 2.0205 ms is the total computation cost for *MSP*. *SMVP* consists of two scalar multiplications, one point addition and one secure hash function, so $2T_{ecc}^{sm} + 1T_h + 1T_{ecc}^{pa} \approx 1.3477$ ms is the total computation cost for *SMVP*. *BMVP* (2) scalar multiplications, (n+1) point additions, and (2n) secure hash functions, so $2T_{ecc}^{sm} + (n+1)T_{ecc}^{pa} + (n)T_h \approx 0.0041$n + 1.3436 ms is the total computation cost for *BMVP*. The computation cost of other schemes is performed in the same method.

Table 3 compares the cost of computation of the NE-CPPA scheme with the four other identity-based CPPA schemes for *MSP*, *SMVP*, *BMVP* and *BMVP*. Figure 2 shows that the NE-CPPA scheme has a significant advantage over the four schemes for *MSP*, *SMVP* and *BMVP*.

5.3.2 Comparison of communication costs

This subsection analyzes the results of the comparison between NE-CPPA scheme and Pournaghi et al. [46], Bayat et al. [47], We et al. [50] and He et al. [51] schemes in terms of communication cost.

In G $\{PID_{il}^1, PID_{il}^2, \sigma \in G\}$, the traffic-related message contents are three items. The size of the traffic-related message in solution in [47] is (40*3) = 120 bytes. In NE-CPPA scheme, the vehicle sends a

Table 3: cost of computation comparison

Schemes	MSP(ms)	SMVP(ms)	BMVP(ms)
Pournaghi et al. [46]	$3T_{bp}^{sm} + 1T_{mtp} + T_{bp}^{pa} \approx$ 8.8826	$3T_{bp} + 1T_{bp}^{sm} + 1T_{mtp} \approx 23.1708$	$3T_{bp} + nT_{bp}^{sm} + nT_{mtp} +$ 5.7378n+17.433
Bayat et al. [47]	$1T_{mtp} \approx 4.1724$	$3T_{bp} + 1T_{bp}^{sm} + 1T_{mtp} \approx 23.1708$	$3T_{bp} + nT_{bp}^{sm} + nT_{mtp} \approx$ 5.7378n+17.4333
Wu et al. [50]	$2T_{ecc}^{sm} + 2T_h \approx 1.3456$	$(4)T_{ecc}^{sm} + (2)T_h + (2)T_{ecc}^{pa} \approx 2.6954$	$(n + 2)T_{ecc}^{sm} + (2n + 1)T_{ecc}^{pa} + (2n)T_h \approx$ 0.6800n + 1.3467
He et al. [51]	$3T_{ecc}^{sm} + 3T_h \approx 2.0174$	$(3)T_{ecc}^{sm} + (2)T_h + (2)T_{ecc}^{pa} \approx 2.0236$	$(n + 2)T_{ecc}^{sm} + (2n - 1)T_{ecc}^{pa} + (2n)T_h \approx$0.6800n + 1.3405
NE-CPPA	$3T_{ecc}^{sm} + 1T_{ecc}^{pa} + 2T_h$= 2.0205	$2T_{ecc}^{sm} + 1T_h + 1T_{ecc}^{pa} \approx 1.3477$	$2T_{ecc}^{sm} + (n + 1)T_{ecc}^{pa} + (n)T_h \approx$ 0.0041n + 1.3436

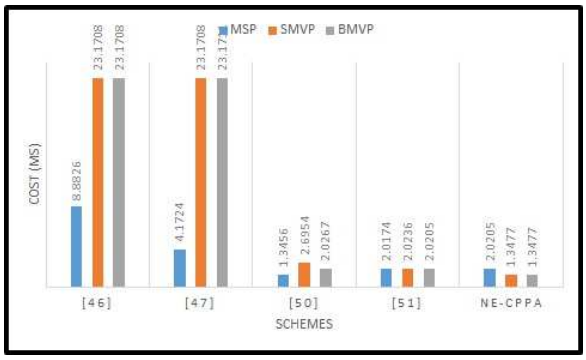

Fig. 2: Computation costs of *MSP*, *SMVP* and *BMVP*.

traffic-related message with size (40 + 20 * 3 + 4) = 104 bytes and the traffic-related message content is one element in $\{pID^1 \in G\}$, two elements in $\{pID^2, \delta_m, \vartheta \in z_q\}$, and one timestamp. The communication cost of the other scheme is executed in the same method. The overall overhead communication is illustrated in Table 4.

Table 4: Comparison of communication cost

Schemes	**One message(byte)**	**n messages(byte)**
Pournaghi et al. [46]	140	140 n
Bayat et al. [47]	120	120 n
Wu et al. [50]	148	148 n
He et al. [51]	144	144 n
NE-CPPA	104	104 n

6 Conclusion

VANETs improves safety and comfort of road users during travel by exchanging traffic-related messages among the VANET-enabled vehicles as well as between the vehicles and road infrastructure. However, they encounter many challenges and problems because of their reliance on open wireless communication channel. The proposed scheme (NE-CPPA) guarantees secure communication and supports both V2V and V2I communication modes within VANET. Moreover, it uses elliptical curve parameter and identity-based CPPA schemes. It also reduces the computation cost in message signing and verification processes during broadcasting traffic-related message. Thus, security analysis showed that security and privacy requirements for VANETs could be satisfied in NE-CPPA scheme. In terms of computation and communication costs, the proposed scheme performed better than other identity-based conditional privacy-preserving authentication schemes. Thus, it is appropriate for securing VANET networks, especially the one with with several vehicles.

Acknowledgement

This paper is supported by an external grant from U Mobile Sdn Bhd [grant number: 304/PNAV/650958/U154].

Conflicts of Interest

The authors declare that there is no conflict of interest regarding the publication of this article.

References

[1] M. A. Al-Shareeda, M. Anbar, S. Manickam, and A. A. Yassin, "Vppcs: Vanet-based privacy-preserving communication scheme," *IEEE Access*, pp. 1–1, 2020.

[2] M. A. Al-Shareeda, M. Anbar, I. H. Hasbullah, S. Manickam, and S. M. Hanshi, "Efficient conditional privacy preservation with mutual authentication in vehicular ad hoc networks," *IEEE Access*, vol. 8, pp. 144 957–144 968, 2020.

[3] M. M. Hamdi, S. A. Rashid, M. Ismail, M. A. Altahrawi, M. F. Mansor, and M. K. AbuFoul, "Performance evaluation of active queue management algorithms in large network," in *2018 IEEE 4th International Symposium on Telecommunication Technologies (ISTT)*. IEEE, 2018, pp. 1–6.

[4] I. Ali, A. Hassan, and F. Li, "Authentication and privacy schemes for vehicular ad hoc networks (VANETs): A survey," *Vehicular Communications*, 2019.

[5] M. A. A. S. M. Mahmood A. Al-shareeda, Mohammed Anbar, "Security schemes based conditional privacy-preserving in vehicular ad hoc networks," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 21, no. 1, 2020.

[6] M. M. Hamdi, L. Audah, S. A. Rashid, S. Alani, M. A. Al-Mashhadani, and A. S. Mustafa, "Green communication networks challenges, opportunities and future role." *JCM*, vol. 15, no. 3, pp. 256–262, 2020.

[7] M. Al Shareeda, A. Khalil, and W. Fahs, "Realistic Heterogeneous Genetic-based RSU Placement Solution for V2I Networks," *International Arab Journal of Information Technology*, vol. 16, no. 3 A, pp. 540–547, 2019.

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

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

[10] M. Al Shareeda, A. Khalil, and W. Fahs, "Towards the Optimization of Road Side Unit Placement Using Genetic Algorithm," in *2018 International Arab Conference on Information Technology (ACIT)*. IEEE, 2018, pp. 1–5.

[11] 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," *Vehicular communications*, vol. 15, pp. 16–27, 2019.

[12] M. A. Aladaileh, M. Anbar, I. H. Hasbullah, Y.-W. Chong, and Y. K. Sanjalawe, "Detection techniques of distributed denial of service attacks on software-defined networking controller–a review," *IEEE Access*, vol. 8, pp. 143 985–143 995, 2020.

[13] M. Muhammad and G. A. Safdar, "Survey on existing authentication issues for cellular-assisted v2x communication," *Vehicular Communications*, vol. 12, pp. 50–65, 2018.

[14] 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, 2019.

[15] Z. Lu, G. Qu, and Z. Liu, "A survey on recent advances in vehicular network security, trust, and privacy," *IEEE Transactions on Intelligent Transportation Systems*, vol. 20, no. 2, pp. 760–776, 2018.

[16] M. Raya, P. Papadimitratos, and J.-P. Hubaux, "Securing vehicular communications," *IEEE wireless communications*, vol. 13, no. 5, pp. 8–15, 2006.

[17] M. A. Al-Adaileh, M. Anbar, Y.-W. Chong, and A. Al-Ani, "Proposed statistical-based approach for detecting distribute denial of service against the controller of software defined network (saddcs)," in *MATEC Web of Conferences*, vol. 218. EDP Sciences, 2018, p. 02012.

[18] S. A. Alfadhli, S. Lu, K. Chen, and M. Sebai, "Mfspv: A multi-factor secured and lightweight privacy-preserving authentication scheme for vanets," *IEEE Access*, vol. 8, pp. 142 858–142 874, 2020.

[19] A. H. Mohammed, M. M. Hamdi, S. A. Rashid, and A. M. Shantaf, "An optimum design of square microstrip patch antenna based on fuzzy logic rules," in *2020 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*. IEEE, 2020, pp. 1–7.

[20] S. A. Alfadhli, S. Alresheedi, S. Lu, A. Fatani, and M. Ince, "Elcph: An efficient lightweight conditional privacy-preserving authentication scheme based on hash function and local group secrete key for vanet," in *Proceedings of the 2019 The World Symposium on Software Engineering*, 2019, pp. 32–36.

[21] A. K. Al-Ani, M. Anbar, S. Manickam, C. Y. Wey, Y.-B. Leau, and A. Al-Ani, "Detection and defense mechanisms on duplicate address detection process in ipv6 link-local network: A survey on limitations and requirements," *Arabian Journal for Science and Engineering*, vol. 44, no. 4, pp. 3745–3763, 2019.

[22] M. A. Al-shareeda, M. Anbar, S. Manickam, and I. H. Hasbullah, "Review of Prevention Schemes for Man-In-The-Middle (MITM) Attack in Vehicular Ad hoc Networks," *International Journal of Engineering and Management Research*, vol. 10, no. 3, pp. 153–158, Jun. 2020.

[23] A. Al-Ani, M. Anbar, I. H. Hasbullah, R. Abdullah, and A. K. Al-Ani, "Authentication and privacy approach for dhcpv6," *IEEE Access*, vol. 7, pp. 73 144–73 156, 2019.

[24] M. Hamdi, L. Audah, S. Rashid, A. Mustafa, and M. Abood, "A survey on data dissemination and routing protocol in vanet: Types challenges opportunistic and future role," *Int. J. Adv. Sci. Technol*, vol. 29, no. 5, pp. 6473–6482, 2020.

[25] A. K. Al-Ani, M. Anbar, A. Al-Ani, and D. R. Ibrahim, "Match-prevention technique against denial-of-service attack on address resolution and duplicate address detection processes in ipv6 link-local network," *IEEE Access*, vol. 8, pp. 27 122–27 138, 2020.

[26] M. A. Saare, A. Hussain, and W. S. Yue, "Relationships between the older adult's cognitive decline and quality of life: The mediating role of the assistive mobile health applications," 2019.

[27] M. M. Hamdi, L. Audah, S. A. Rashid, A. H. Mohammed, S. Alani, and A. S. Mustafa, "A review of applications, characteristics and challenges in vehicular ad hoc networks (vanets)," in *2020 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*. IEEE, 2020, pp. 1–7.

[28] M. A. Saare, A. B. Hussain, O. M. Jasim, and A. A. Mahdi, "Usability evaluation of mobile tracking applications: A systematic review," *International Journal of Interactive Mobile Technologies (iJIM)*, vol. 14, no. 05, pp. 119–128, 2020.

[29] U. A. Khan, S. M. U. Din, S. A. Lashari, M. A. Saare, and M. Ilyas, "Cowbree: A novel dataset for fine-grained visual categorization," *Bulletin of Electrical Engineering and Informatics*, vol. 9, no. 5, pp. 1882–1889, 2020.

[30] A. S. Mustafa, M. M. Al-Heeti, M. M. Hamdi, and A. M. Shantaf, "Performance analyzing the effect of network size on routing protocols in manets," in *2020 International*

Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA). IEEE, 2020, pp. 1–5.
[31] D. Chaum and E. Van Heyst, "Group signatures," in *Workshop on the Theory and Application of of Cryptographic Techniques*. Springer, 1991, pp. 257–265.
[32] J. Guo, J. P. Baugh, and S. Wang, "A group signature based secure and privacy-preserving vehicular communication framework," in *2007 Mobile Networking for Vehicular Environments*. IEEE, 2007, pp. 103–108.
[33] R. Lu, X. Lin, X. Liang, and X. Shen, "A dynamic privacy-preserving key management scheme for location-based services in vanets," *IEEE Transactions on Intelligent Transportation Systems*, vol. 13, no. 1, pp. 127–139, 2011.
[34] J. Shao, X. Lin, R. Lu, and C. Zuo, "A Threshold Anonymous Authentication Protocol for VANETs," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 3, pp. 1711–1720, 2015.
[35] X. Sun, X. Lin, and P.-H. Ho, "Secure vehicular communications based on group signature and id-based signature scheme," in *2007 IEEE International Conference on Communications*. IEEE, 2007, pp. 1539–1545.
[36] Y. Wang, H. Zhong, Y. Xu, and J. Cui, "Ecpb: Efficient conditional privacy-preserving authentication scheme supporting batch verification for vanets." *IJ Network Security*, vol. 18, no. 2, pp. 374–382, 2016.
[37] J. Zhang, L. Ma, W. Su, and Y. Wang, "Privacy-preserving authentication based on short group signature in vehicular networks," in *The First International Symposium on Data, Privacy, and E-Commerce (ISDPE 2007)*. IEEE, 2007, pp. 138–142.
[38] A. Studer, E. Shi, F. Bai, and 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*. IEEE, 2009, pp. 1–9.
[39] X. Lin, X. Sun, P.-H. Ho, and X. Shen, "GSIS: A secure and privacy-preserving protocol for vehicular communications," *IEEE Transactions on vehicular technology*, vol. 56, no. 6, pp. 3442–3456, 2007.
[40] X. Lin, R. Lu, C. Zhang, H. Zhu, P.-H. Ho, and X. Shen, "Security in vehicular ad hoc networks," *IEEE communications magazine*, vol. 46, no. 4, pp. 88–95, 2008.
[41] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Workshop on the theory and application of cryptographic techniques*. Springer, 1984, pp. 47–53.
[42] C. Zhang, R. Lu, X. Lin, P. Ho, and X. Shen, "An efficient identity-based batch verification scheme for vehicular sensor networks," in *IEEE INFOCOM 2008-The 27th Conference on Computer Communications*. IEEE, 2008, pp. 246–250.
[43] C.-C. Lee and Y.-M. Lai, "Toward a Secure Batch Verification with Group Testing for VANET," *Wireless Networks*, vol. 19, no. 6, pp. 1441–1449, 2013.
[44] Z. Jianhong, X. Min, and L. Liying, "On The Security of a Secure Batch Verification With Group Testing for VANET," *International Journal of Network Security*, vol. 16, no. 5, pp. 351–358, 2014.
[45] M. Bayat, M. Barmshoory, M. Rahimi, and M. R. Aref, "A secure authentication scheme for vanets with batch verification," *Wireless networks*, vol. 21, no. 5, pp. 1733–1743, 2015.
[46] S. M. Pournaghi, B. Zahednejad, M. Bayat, and Y. Farjami, "Necppa: A novel and efficient conditional privacy-preserving authentication scheme for vanet," *Computer Networks*, vol. 134, pp. 78–92, 2018.
[47] M. Bayat, M. Pournaghi, M. Rahimi, and M. Barmshoory, "NERA: A New and Efficient RSU based Authentication Scheme for VANETs," *Wireless Networks*, pp. 1–16, 2019.
[48] L. Zhang, Q. Wu, J. Domingo-Ferrer, B. Qin, and C. Hu, "Distributed aggregate privacy-preserving authentication in VANETs," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 3, pp. 516–526, 2016.
[49] H. Zhong, S. Han, J. Cui, J. Zhang, and Y. Xu, "Privacy-preserving authentication scheme with full aggregation in vanet," *Information Sciences*, vol. 476, pp. 211–221, 2019.
[50] L. Wu, J. Fan, Y. Xie, J. Wang, and Q. Liu, "Efficient location-based conditional privacy-preserving authentication scheme for vehicle ad hoc networks," *International Journal of Distributed Sensor Networks*, vol. 13, no. 3, p. 1550147717700899, 2017.
[51] D. He, S. Zeadally, B. Xu, and X. Huang, "An Efficient Identity-based Conditional Privacy-preserving Authentication Scheme for Vehicular Ad hoc Networks," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 12, pp. 2681–2691, 2015.
[52] 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 Journal*, pp. 1–1, 2020.
[53] M. A. Al-shareeda, M. Anbar, S. Manickam, and I. H. Hasbullah, "Review of Prevention Schemes for Modification Attack in Vehicular Ad hoc Networks," *International Journal of Engineering and Management Research*, vol. 10, no. 3, pp. 149–152, Jun. 2020.
[54] S. S. Ltd, "Multi Precision Integer and Rational Arithmetic Cryptographic Library (MIRACL)," Http://www.certivox.com/miracl/, 2018.
[55] 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. 170 507–170 518, 2020.
[56] 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, 2020.

Mahmood A. Al-shareeda received his B.S degree in from communication Engineering in Iraq University College and MSc in Information Technology from Islamic University of Lebanon (IUL) in 2018. Currently, he is a Ph.D. candidate at National Advance IPv6 Center (NAv6), Universiti Sains Malaysia (USM). His research interests are security and privacy

issues in Vehicular Ad hoc Networks (VANETs) and Network Optimization.

Mohammed Anbar obtained his Ph.D. in Advanced Computer Network from University Sains Malaysia (USM). He is currently a senior lecturer at National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia. His current research interests include malware detection, web security, Intrusion Detection System (IDS), Intrusion Prevention System (IPS), network monitoring, Internet of Things (IoT), Vehicular Ad hoc Network (VANET) security and IPv6 security.

Selvakumar Manickam is an associate professor working in Cybersecurity, Internet of Things, Industry 4.0 and Machine Learning. He has authored and co-authored more than 160 articles in journals, conference proceedings and book reviews and graduated 13 PhDs. He has 10 years of industrial experience prior to joining the academia. He is a member of technical forums at national and international levels. He also has experience building IoT, embedded, server, mobile and web-based applications.

Iznan H. Hasbullah holds a Bachelor of Science degree in electrical engineering from Rensselaer Polytechnic Institute, Troy, NY, USA. He is currently pursuing his M.Sc. in advanced network security. He has experience working as software developer, R&D consultant, and network security auditor prior to joining National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia in 2010 as Research Officer. His research interest includes unified communication, telematics, network security, network protocols and next generation network.

Nibras Abdullah obtained his MSc and PhD in 2010 and 2017 from Universiti Sains Malaysia. He is a faculty member at Hodeidah University, Yemen. Currently, he is a visiting scholar at the National Advanced IPv6 Center, University Sains Malaysia, Penang, Malaysia. He is a member of IEEE, Yemeni Scientists groups (YSRG), Editorial board of Journal Insight - Engineering and Technology (Singapore), Associate Editor in International Journal of Cyber Forensics and Advanced Threat Investigations (UK), program committee and reviewer of several journals and international Conferences. He has published papers including journals and conferences. His interesting research areas includes Computer Networks, Internet Security, Information and Knowledge Engineering, Multimedia information System, Handwriting Recognition, Optimization, Internet of Things (IoT), Artificial Intelligence, and Artificial Neural Networks.

Mustafa Maad Hamdi was born in Al-Anbar, Iraq. He received the B.Eng. degree in Computer Engineering Technology from Al-Maarif University College, Iraq. and the M.Sc. degree in Communication and Computer Engineering from University Kebangsaan Malaysia (UKM), Malaysia. He is currently pursuing the Ph.D. degree in the department of communication engineering, University Tun Hussein Onn Malaysia (UTHM), Malaysia. His research interests include Wireless and Mobile Communications, VANET, MANET and Satellite Communication, and Cryptographic.

Ahmed Shakir Al-Hiti received his B.Eng in Electrical Engineering from the University of Baghdad, Iraq in 2008, computer Engineering from Al-Maarif University College, Iraq in 2012, and received his M.Sc. in communications and networks Engineering from University Putra Malaysia, Malaysia in 2017. He is currently working as a researcher in fiber lasers at the University of Malaya. His research interests include networks, control systems, wireless communications, photonics, and laser-plasma accelerators.