CPAAS: an efficient conditional privacy-preservation anonymous authentication scheme using signcryption in VANET

Meenakshi Gupta*, Poonam Gera and Bharavi Mishra

LNM Institute of Information Technology,
LNMIIT Deemed University,
Rajasthan, Jaipur, India
Email: y14pg929@lnmiit.ac.in
Email: poonamgera@lnmiit.ac.in
Email: bharavi@lnmiit.ac.in
*Corresponding author

Abstract: Vehicular Ad-Hoc Network (VANET) is a tremendously promising innovation in the field of Intelligent Transportation System (ITS). It facilitates a vehicle to communicate on the road with infrastructure or OBU to increase road safety and driving conditions. Further, to deliver the same requires a secure network build-up through a legitimate entity. However, in an open network, any of the participating entities may be malicious. Therefore we need a proper solution to mitigate the effects of such entities by authenticating them, and it should also preserve the privacy of entity and integrity of message so that the impact of any malicious entity can be nullified. The existing solutions focus on any of the above aspects, but not all, further they are not computationally efficient. Inspired by this, we propose a computationally efficient approach that achieves most of the security requirements with less communication overhead. We have used distributed pseudo_id for preserving the privacy of vehicle and the ID-based Certificateless Signcryption scheme based on elliptic curve cryptography to provide an effective way to achieve mutual authentication, integrity, non-repudiation, and confidentiality. The security analysis of our approach demonstrates the efficiency and effectiveness of our proposed scheme.

Keywords: authentication; security; conditional privacy preservation; vehicular ad-hoc network; pseudonyms; signcryption.

Reference to this paper should be made as follows: Gupta, M., Gera, P. and Mishra, B. (2021) 'CPAAS: an efficient conditional privacy-preservation anonymous authentication scheme using signcryption in VANET', *Int. J. Vehicle Information and Communication Systems*, Vol. 6, No. 1, pp.88–105.

Biographical notes: Meenakshi Gupta received her Master's degree in Computer Engineering from RTU in 2010. Currently, she is a PhD Scholar at LNMIIT, Jaipur. Her research interests include computer networking, security and vehicular ad-hoc network.

Poonam Gera received her PhD degree in the Department of E&CE from IIT Roorkee in 2013. She is currently an Assistant Professor of Computer Science and Engineering at LNMIIT, Jaipur. Her research interests include security in MANET, VANET, IoT security, cloud computing.

Bharavi Mishra received his PhD degree in Computer Engineering from IIT BHU in 2013. He is currently an Assistant Professor of Computer Science and Engineering at the LNMIIT, Jaipur. His research interests include data mining and network security.

1 Introduction

Vehicular Ad-Hoc Networks (VANETs) is an embryonic innovation that integrates ad-hoc networks and wireless LAN (WLAN), for enhancing road security and driving conditions through inter-vehicle and intra-vehicle communication. VANET is a subgroup of a mobile ad-hoc network (MANET) in which nodes are the vehicles and free to move independently in a dynamic infrastructure. The main reason for developing an enthusiasm for VANET is due to the many services offered by it. These services fall into two categories namely safety-related services such as weather forecasting, blind curve warning, accident warning and non-safety related services like location-based services, internet access (Li and Wang, 2007).

In a typical VANET, three sorts of entities named Regional Trusted Authority (RTA), Road Side Unit (RSU) and vehicles, play essential roles. RTA is a central trusted authority that registers, authenticates and controls all the vehicles and RSUs. RTA assigns public-private key pair and certificate to RSUs and vehicles, for communication. RSUs are mounted at a critical point of the road, such as traffic light at the road intersection, parking, and so on. Vehicles are the essential entity of the VANET, and they use all the services provided by the VANET system. It is mounted with communicating devices such as Onboard Unit (OBU), location tracking device, display, GPRS, etc. OBU is a wireless communication device that uses dedicated short-range communication (DSRC) standard, which facilitates a vehicle to communicate with other vehicles (V2V) and with infrastructure (V2I) such as RSU (Li and Wang, 2007).

Unique characteristics like dynamic infrastructure and high mobility of VANETs make it susceptible to security and privacy threats, which may cause increasing malevolent attacks and service exploitations. According to the DSRC protocol, vehicle or RSU broadcasts alarm messages or real-time safety-related messages called beacons to enhance the driving experience and make driving safe. Alarm messages are sent by RSU to inform others about the already happened event on the road like car accidents. Beacons contain sensitive information of vehicles such as traffic events, location, direction, speed, real identity, current time, etc. and broadcast within the time interval of 100–300 ms. The beacons are broadcast to make aware neighboring vehicles about their presence and road condition so that drivers can avoid possible damage or choose the better route that evades traffic jam (Li and Wang, 2007). As beacons contain sensitive information like the real identity of vehicles, any illegitimate entity can track the vehicle resulting in privacy breaching. Therefore, to preserve privacy, anonymous identities called pseudonyms are preferred over real identities (Song et al., 2010). These pseudonyms help legitimate vehicles to become anonymous. However, when some severe unplanned condition like accidents and crime occurs, it requires the real identity of the vehicle to be revealed. Therefore to meet such conditions vehicle's real identity may be conditionally revealed through trusted authority, termed as conditional privacy or conditional anonymity. Conditional anonymity is desirable with privacy to handle unpredicted conditions in VANETs.

The insecure and open communication channel in VANET incorporates various security threats like impersonate attack, Sybil attack, etc. In VANET, any malicious node can be part of the network. These nodes impersonate as a legitimate vehicle; they may spread the false beacons, which can cause any severe damage even loss of life of a person in the vehicle. For instance, a vehicle impersonates an emergency vehicle to take benefit of a clear road. Further, a malicious node in a network may work in a collision with multiple identities and broadcast fake messages (such as false road traffic). To mitigate these attacks, we require a proper authentication mechanism which forbids a malicious node to be part of the network. Further preserving the integrity of the message may also avoid spreading the bogus or false message in the network.

In VANET, V2I messages are communicated in a simple format. An attacker can eavesdrop these messages further, resulting in active attacks such as message modification attacks, replay attacks, etc. Therefore, these messages should be encrypted to preserve them from these attacks. However, encrypting all the messages may incur a huge cost. Therefore the best approach is to encrypt a message which carries crucial information.

Conventional digital signature-then-encryption in public key infrastructure (PKI) is a well-suited way to ensure the legitimacy of a vehicle along with preserving message integrity and confidentiality. However, this approach introduces substantial communication and computational overhead (Shamir, 1984) and may not satisfy the stringent time requirement of VANET. Consequently, there is a requirement of a cost-effective scheme that incorporates all security requirements with conditional privacy in VANET.

Keeping above in mind, we propose a scheme centred on ID-based signcryption cryptography (Zheng, 1997a) that ensures to achieve all the above security requirements and also has a small signature size with less communication overhead to make it cost-effective. Further to ensure the privacy of vehicles conditional privacy-preserving approach is incorporated. It preserves the privacy of vehicles through pseudo_id, making them untraceable by an attacker.

The organisation of the paper follows. Section 2 contains the existing security and privacy schemes in VANET. Section 3 presents the system components and proposes an approach. The security analysis of our approach is presented in Section 4. Performance evaluation is presented in Section 5. Section 6 presents conclusions.

2 Related work

This section presents the existing schemes which ensure security and maintain the privacy with traceability of anonymous vehicles.

Raya and Hubaux (2007), Wang et al. (2008) and Lu et al. (2008) proposed PKI-based privacy-preserving authentication schemes. In these approaches, a trusted authority (TA) assigns some pseudonym identities with their corresponding certificate to each vehicle and also maintains a Certificate Revocation List (CRL). A vehicle selects a pseudo_id with its corresponding certificate from the list and sends it to the neighboring vehicles or RSU to prove their legitimacy. Authors guarantee that their scheme ensures authentication with conditional privacy. However, in this scenario, each vehicle broadcasts safety messages every 100–300 ms. Authenticating a large number of signatures becomes a time-consuming process that creates a traffic jam at the RSU, and maintenance of the public key certificate also incurs computational and communication overhead.

Hu et al. (2012) proposed an efficient, secure group communication scheme that replaces signature with Hash-based Message Authentication Code (HMAC) for VANET that ensures authentication, integrity, and privacy with faster verification. However, this scheme using bilinear pairing operation, which required extra computations and signature size is also extensive (more than 200 bytes). So, ID-based cryptography (Shamir, 1984) may be suitable for VANET, as this required less transmission overhead and verifying a batch of signatures within a necessary time frame.

Kamat et al. (2006) proposed identity-based security framework for VANETs. In this scheme, the requirement of ample memory space to store pseudonyms on OBU, avoids computing pseudo-identity through RSU whenever a vehicle required. RSU generates it by using the master key of Certificate Authority (CA). The authors claim that the scheme can achieve all the security aspects, including confidentiality, authentication, integrity, non-repudiation, and privacy for VANET.

Gamage et al. (2003) introduced an ID-based ring signature scheme with an anonymous signer feature with preserving privacy in VANET. However, this scheme does not ensure conditional privacy or traceability of anonymous vehicles.

Later, to achieve traceability, a group-signature-based authentication scheme has been proposed in Sampigethaya (2005), Sun et al. (2010) and Shim (2012), in which a group manager can reveal the real identity of any group member. Shim (2012) proposed an efficient Conditional Privacy-preserving Authentication Scheme (CPAS) using a pseudo-identity-based signature for securing V2I communication. This scheme performs three bilinear pairing operations for verifying a signature, but the cost of bilinear pairing function is more in comparison to other functions. Therefore, the computation cost is increased. As stated by Liu et al. (2018) modification attack can be possible in Shim's IBS scheme, i.e., the adversary can generate a new legal message by modifying a previous message.

Lo and Tsai (2016) proposed a new conditional privacy-preserving scheme based on ID-based batch signature cryptography without using bilinear pairings. The proposed approach is secure against adaptively chosen message attack and chosen cipher attack under random oracle. It is an advancement of Shim (2012) and guarantees less computation and communication overhead. For this, the authors proposed their scheme based on elliptic curve cryptography. Besides all these features, traffic-related messages are transmitted between vehicles to infrastructure, still in a simple format. Therefore, this scheme is prone to location privacy attacks.

Azees et al. (2017) proposed an Efficient Anonymous Authentication scheme with conditional Privacy-preserving (EAAP) based on bilinear pairing. In the proposed method, CA does not require to store credentials and certificates for the vehicles or RSU. They can generate their credentials on their own because of privacy. However, scheme is vulnerable to sybil attack as all the pseudonyms and its corresponding key are genereated by vehicle simultaneously. vehicles can use multiple identities at a time to launch attacks. Alongwith, the computation cost and communication overhead of the scheme is too high.

Kazemi et al. (2018) claimed that EAAP protocol is vulnerable against various security attacks, i.e. message modification attack, reply attack, and impersonation attack.

The authors proposed a new authentication scheme that provides more security than EAAP without increasing computational and communication overhead.

Along with lots of advantages in the above ID-based scheme, they have a key escrow problem. Key escrow issues arise when a private key for entities is produced by the Trusted Third Party (TTP). If TTP is compromised, then the malicious entity would be able to use the vehicle's private key to breakdown the framework. Zhang et al. (2011) proposed the identity-based security system for user privacy. It is a threshold group signature-based scheme. In this, a group manager computes the aggregate master key by using the real identity of the group identity of all vehicles, and would be able to reveal the identity of any group member; the result is identity escrow problem. The proposed scheme is an efficient identity-based multi-receiver ring signcryption scheme. The limitation of this approach is, a vehicle that wishes to send a message to other vehicles used the real identity of them to compute a single identity. For this, every vehicle requires to know the identity of other vehicles. Therefore, in the proposed scheme, a vehicle’s privacy would be compromised. Key escrow problem also would be possible.

Certificateless cryptography (Gamage et al., 2003) is the best solution for key escrow issues. Certificateless public-key cryptography was introduced in Al-Riyami and Paterson (2003) and Malhi and Batra (2015) to solve the complicated certificate management problem in traditional public-key cryptography and the key escrow problem in identity-based cryptography. Al-Riyami and Paterson (2003) proposed a certificateless cryptography concept. In a certificateless public key scheme, the key generation process is divided between TTP and node. First, TTP computes a key pair, called partial private key, for node. Later, node computes a random secret key and performs some cryptographic operation to concatenate partial private key and randomly chosen the secret key to compute full private key pair. However, this is not well suited for the VANETs because of its high computation cost in signature generation and verification. Owing to the highly dynamic infrastructure, there is an urgent need for a scheme with less computation cost and bandwidth.

Authentication, integrity, and confidentiality are achieved by signature and encryption, respectively. Signcryption cryptographic approach is introduced by Zheng (1997a), which combines the functionality of both digital signature and encryption in a single step. Signcryption gives guarantee for authentication, confidentiality, non-repudiation, and integrity. As discuss in Zheng (1997b), signcryption costs 58% less in average computation time than signature-then-encryption. More work on signcryption is presented in Pradweap and Hansdah (2013); Han et al. (2014); Lu et al. (2018); Wahid and Mambo (2016) and Zhang et al. (2011). Han et al. (2014) presented a hybrid authentication protocol for VANET based on aggregate signcryption scheme. In this scheme, authors divide vehicles into public and private. Aggregate signcryption ensures the authenticity of a private vehicle with the confidentiality and integrity of the message. However, this scheme does not preserve the privacy of vehicles. Zhang et al. (2011) presented a Short Identity-based Signcryption Scheme in the Multi-PKG over the VANETs scheme. This scheme uses signcryption technique to ensure confidentiality, non-repudiation, authentication, and integrity in the system. A KGC computes public and private key for the vehicles, which may introduce key escrow problems in the network. Location privacy attack and replay attack can also be possible.

Pradweap and Hansdah (2013) proposed RSU-Aided Hybrid Architecture for Anonymous Authentication (RAHAA) in VANET, which uses a certificateless signcryption scheme without pairing. In this approach, the vehicle's user uses signatures to authenticate himself. The signature's size is 192 byte, which is quite large and gives results in a high computational cost.

Lu et al. (2018) proposed a signcryption-based authentication scheme with conditional privacy preservation for VANET (SACP). This scheme requires less computational time to generate and verifies signed messages. However, this scheme can be compromised with key escrow issues as the private key for vehicles is generated by TA.

After bunches of discourse, we came at a point that, in VANET, where thousands of messages broadcasted within a second, it becomes a herculean task to verify all the signatures in time and maintain the database by a single central authority. It required less time for signature verification and small signature size to reduce computational/ communication overhead. So, there is not a solitary approach proposed yet that ensures above all discussed security requirements with conditional privacy and ensures less transmission overhead.

2.1 Our contribution

Keeping above in mind, we have proposed an efficient conditional privacy-preserving anonymous authentication scheme using signcryption. Our scheme is based on ID-based certificateless signcryption cryptography that uses the elliptic curve (Kapoor et al. 2008) proposed by Wahid and Mambo (2016), which ensures less communication overhead. This scheme combines identity-based cryptography with a certificateless and signcryption cryptography scheme to take the advantages provided by all. Identity-based cryptography eliminates the requirement of public-key certificates. Further, certificateless cryptography eliminates inherent key escrow problem and key management problem. Signcryption ensures confidentiality, authentication, integrity, and non-repudiation. Additionally, for preserving privacy and unlinkability, we require RSU to generate pseudo-id for a limited time period for the vehicle whenever it come in the range of RSU, or a vehicle wants to change their pseudo_id. So, there is no need to have ample memory space at OBU and all pseudonyms will be valid for a small time frame. After timer expires pseudo-id will become invalid and cannot be used. The generation of random pseudo-id ensures that vehicles always use a single pseudonym for communication thus reduces the probability of Sybil attack. Our scheme also provides privacy with traceability at RTA which retains mapping between real identity and pseudo_id This ensures traceability of a misbehaving vehicle, if required.

3 Proposed scheme: an efficient conditional privacy-preservation anonymous authentication scheme using signcryption

This section represents system components and assumptions for the proposed approach. Later, proposed model is discussed.

3.1 System components and assumption

We considered three building blocks for the network: RTA, RSU, and vehicles. All vehicles need to be registered with the Regional Trusted Authority (RTA) during the registration process. RTA computes initial credentials for vehicles, by the vehicle's unique identity along with corresponding partial public-private key pair. It stores all initial credentials, global public parameters into the vehicle's OBU, over a secure channel. OBU is a tamper-proof device that is used to store vehicle's credentials and assumes that physical extraction of the information from it is impossible. After the registration, vehicles become part of the VANET and able to communicate with each other or with RSU.

RSU is the backbone of the proposed system. RSU has a stronger computational capability with broad communication area compare to vehicles. RTA produces a partial private key and partial public key for RSU. Here, we assume RSU's communication range is around 1 km whereas vehicle communication range is 300m. In our model, RSUs are responsible for assigning temporary credentials to the vehicles. We divide RSUs into two categories. Firstly, LRSU (Local RSU), where the vehicle verifies itself first and gets a pseudonym before starting communication. Second, RRSU (Remote RSU), all other RSUs except LRSU, are called RRSU. Here, we assume that both RTA and RSUs are fully trusted and can't be compromised. All the used notations are listed in Table 1.

Table 1 Notations and their description

Notations	*Descriptions*
RTA	Regional trusted authority
RSU	Roadside unit
V_i	Vehicle i
F_q	The finite field over a large prime order of q

3.2 Proposed scheme

We divide our scheme into seven stages: a detailed description of each stage is given next.

3.2.1 System_Setup

In this phase, RTA selects all elliptic curve parameters. RTA also chooses a random number $MSK \epsilon Z_q$ and computes $P_{pub} = MSK.P$, where MSK, P_{pub} is the master secret key and master public key of RTA, respectively. After computing all parameters, RTA keeps MSK secret and publishes all parameters $\left(Fq, P, H_0, H_1, H_2, H_3, E / F_q, P_{pub}\right)$ globally.

3.2.2 Set_Secret_Key

At this step, vehicle picks a random number $x_i \epsilon Z_q$ and computes $VID_i = x_i.P$. Here, x_i is the vehicle's secret value, and VID_i is the public key for vehicle *i*.

3.2.3 Registration_and_Partial_Private_Key_Extraction

In the registration process, a vehicle submits their vehicle number and VID_i to the RTA as a unique identity. RTA verify and computes real identity RIDi by using them. Next, RTA chooses a random number $r_i \epsilon Z_q$ and computes $R_i = r_i.P$ along with it find $H_1(RID_i, R_i)$ and computes the partial private key for V_i.

$$pp_i = r_i + MSK.H_1(VID_i, R_i) \ mod \ q$$

Here, pp_i and R_i are the partial private key and partial public key respectively for vehicle '*i*.' RTA store RID_i, R_i, pp_i, $H_1(RID_i, R_i)$ to vehicle's OBU, over a secure channel. Simultaneously, RTA sends $H_1(RID_i, R_i)$ to LRSU, by encrypting public key of LRSU. RTA also maintains a database for future references, which contains the vehicle's number and their corresponding $H_1(RID_i, R_i)$.

3.2.4 Set_Full_Private_key

It is run by vehicle to compute full private key pair $< pp_i, x_i >$ and public key $< R_i, VID_i >$.

3.2.5 Pseudonym_Gen

In the proposed approach, a vehicle use pseudo_id for anonymous communication and this pseudo_id is updated by the RSU.

When a vehicle enters in the network first time, it verifies itself with the LRSU by sending $H(RID_i, R_i)$, and TS_i (timestamp) encrypted with public key of LRSU. TS_i is the timestamp that attached to the request to evade a replay attack. Now, LRSU decrypts it and check the similar entry in its database, the vehicle is valid if there is a match found. Then, LRSU computes pseudo_id and its corresponding partial public and private key (pp_i, R_i) and sends it to the vehicle, encrypted by the vehicle's public key. Table 2 presents the pseudonym format computed by LRSU:

$$PID_{i,1} = \left(H(RID_i, R_i) \| LRSU\_ID_r | random\_no \ || \ TTL\right)$$

Here, $LRSU\_ID_r$ represents the identity of LRSU and TTL (time to live) defines time in which a vehicle's pseudonyms is valid, as time expired, pseudonyms become invalid. After computing pseudonym, LRSU encrypts it with its private key and sends to the particular vehicle. At vehicle side, it decrypts it with the public key of LRSU. Also, LRSU sends $H(RID_i, R_i)$ and $H(PID_{i,1})$ to the RTA for traceability purposes. RTA makes an entry of $H(PID_{i,1})$ along with vehicle's previous entries into their database. Vehicle has to refresh with new pseudonyms before TTL expires. In many circumstances, if a vehicle becomes unable to update pseudonyms, it again verifies himself to give $H_1(RID_i, R_i)$ and $LRSU\_ID_r$, encrypted with public key of RRSUs. Now, RRSU decrypts it and sends $H_1(RID_i, R_i)$, encrypt to the public key of LRSU, to verifying it. After getting a positive response, RRSU accepts the request to generate a new pseudonym. LRSU maintains a database with $H(RID_i, R_i)$, $H(PID_{i,1})$ entries and each entry is encrypted with public key of LRSUs.

Table 2 Pseudonyms format

H(RID$_i$,R$_i$)	*LRSU_ID$_r$*	*random_no*	*TTL*
32 Bytes	10 Bytes	2 Byte	1 Byte

3.2.6 Signcryption

Whenever a vehicle wants to update its pseudo_id, it sends a signcrypted message request to RRSU. For that, it choose a random number $I_i \epsilon \left[1,2,3\ldots(q-1)\right]$, and computes $A = I_i.P$.

- $Y_r = R_r + H_1(VID_r, R_r).P_{pub}$. Here, Y_r is the partial public key
- $SK = H_2\left(I_i.\ (Y_r + VID_r), A, VID_r, R_r\right)$.
- $C = E_{SK}(M)$
- $S = \left(\left(pp_i + I_i.H_3\left(M, PID_{i,j,}TS_i\right) + x_i.H_3\left(M, PID_{i,j,}TS_i\right)\right) mod\ q\right)$
- So, signcrypted signature is $\Sigma = (C, S, A)$. Now, Vehicle send signcrypted message $\left(\Sigma, PID_{i,j}, TS_i\right)$ to RRSU, encrypted with public key of RRSU.

3.2.7 UnSigncryption

In this phase, RRSU authenticates a vehicle to verify the received message. RRSU decrypt it and ensure the validity of TS_i, if it is valid, then RRSU first computes the secret key for decrypting ciphertext C:

- $SK = H_2\left((pp_r + x_r).A,\ A, VID_r, R_r\right)$
- $M = D_{SK}(C)$. Now, RRSU verifies signature S.
- $Y_i = R_i + H_1(VID_i, R_i).P_{pub}$
- Now, If the following condition holds, RSU accept a request to change pseudonyms
- $S'.P = Y_i + A.H_3\left(M, PID_{i.j,}TS_i\right) + VIDi.H_3\left(M, PID_{i,j,}TS_i\right)$

$$\begin{aligned} S &= \left(pp_i + I_{i.}H_3\left(M, PID_{i,j,}TS_i\right) + x_i.H_3\left(M,\ PID_{i,j,}TS_i\right)\right).P \\ &= \left(ppi.P + I_i.PH_3\left(M, PID_{i,j,}TS_i\right) + x_i.PH_3\left(M, PID_{i,j,}TS_i\right)\right) \end{aligned} \tag{1}$$

Where,

$$\begin{aligned} pp_i.P &= \left(r_i +\ MSK.H_1\left(VID_i,\ R_i\right)\right).P \\ &= \left(r_i.P\ +\ MSK.H_1\left(VID_i,\ R_i\right).P\right) \\ &= \left(R_i + H_1\left(VID_i,\ R_i\right).P_{pub}\right)Yi \end{aligned} \tag{2}$$

- Now, put value of "$pp_i.P$" from equation (2) to equation (1)

$$S = Y_i + A.H_3\left(M, PID_{i,j,} TS_i\right) + VID_i.H_3(M, PID_{i,j,} TS_i))$$

- Otherwise, rejects and gives an error.
- Afterward, RRSU computes pseudo_id for the authenticate vehicle.

$$PID_{i,j} = \left(H\left(PID_{i,1}\right) \| RSU\_ID_r \| random\_no \| TTL\right) .$$

- For e.g. RSU2 computes

$$PID_{i,2} = (H\left(PID_{i,1}\right) \| RSU\_ID_2 \| random\_no \| TTL) .$$

- RSUn computes:

$$PID_{i,n} = \left(H\left(PID_{i,1}\right) \| RSU\_ID_n \| random\_no \| TTL\right).$$

3.3 Correctness analysis

At this point, we analysed the correctness of the ID-based certificateless signcryption authentication scheme. The correctness of approach can be analysed by examining the equality of the following equation

The equation $SK = H_2\left(I_i\left(Y_r + VID_r\right), A, VID_r, R_r\right)$ at sender side and $SK = H_2\left(\left(pp_r + x_r\right).A, \left(A, VID_r, R_r\right)\right)$ at receiver side must be equal. This means that, $I_i \cdot \left(Y_r + VID_r\right)$; moreover, $\left(pp_r + x_r\right).A$' must be similar.

- We know,

$$A = I_i.P$$
$$pp_r = r_r + MSK.H_1\left(VIDr, R_r\right) .$$
$$Y_r = R_r + H_1\left(VIDr, R_r\right).P_{pub}$$

- Now,

$$\begin{aligned}\left(pp_r + x_r\right).A' &= \left(r_r + MSK.H_1\left(VIDr, R_r\right) + x_r\right).Ii.P \\ &= I_i\left(r_r.P + MSK.H_1\left(VIDr,\ R_r\right).P + x_r.P\right) \\ &= I_i\left(R_r + H_1\left(VIDr,\ R_r\right).P_{pub} + VIDr\right) \\ &= I_i\left(Y_r + VIDr\right)\end{aligned}$$

4 Security analysis of the proposed approach

Security of public-private key pair relies on the elliptic curve discrete logarithm problem. Partial public key $Y_i = R_i + H_1\left(VID_i,\ R_i\right).P_{pub} = pp_i.P$, where VID_i, R_i and P, are a point on the elliptic curve over a finite field and pp_i is a quite large integer value. It is feasible to compute the value of Y_i if a value of pp_i and P is given. On the other side, it is infeasible to compute partial private key pp_i even if Y_i and P are given, where P is the generator of the group. In the same way, if secret key $x_i \epsilon Z_q$ and P are given, it will be possible to find a value of public key VID_i. However, it is difficult to compute the value of x_i, even if the value of VID_i and P are given. In this way, it is hard to compute the private key of the vehicles. Our scheme confirms confidentiality, privacy, integrity, authentication, non-repudiation, in one stroke.

4.1 *Proof for authentication*

In VANETs, two types of authentication are required, namely, message authentication and user authentication. Message authentication ensures that messages sent by a genuine person. In proposed system, a vehicle signed message with their private key (pp_i, x_i) and send a signature $S = \left(pp_i + I_i.H_3\left(M,\ PID_{i,j,}TS_i\right) + \ x_i.H_3\left(M, PID_{i,j,}TS_i\right)\right)$ to the RSU. After receiving a signature, the RSU verifies the message by using signature *S*. If $S.P = S'.P = Y_i + A.H_3\left(M, PID_{i,j,}TS_i\right)\ +\ VIDi.H_3\left(M, PID_{i,j,}TS_i\right)$ is held, this will ensure that the data comes from an authenticated vehicle. Entity authentication ensures that only authenticated vehicles can access the network. In propose approach, LRSU can authenticate a vehicle through $H\left(RID_i, R_i\right)$ and signature *S*.

4.2 *Poorf of integrity*

In our scheme, RSU can confirms integrity of message by computing signature $S = \left(pp_i + I_i.H_3\left(M, PID_{i,j,}TS_i\right) + \ x_i.H_3\left(M,\ PID_{i,j,}TS_i\right)\right)$. Suppose that if an attacker changed the ciphertext from C to C1 and sent to RSU. Now, RSU computes SK to decrypt ciphertext C1 to get a message 'M1'. This 'M1' differs from the original message. After getting M1, RSU computes $S'.P = Y_i + A.H_3\left(M1,\ PID_{i,j,}TS_i\right)$ $+VIDi\ .H_3\left(M1, PID_{i,j,}TS_i\right)$ to get signature *S* of vehicle. As a result, computed *S*' is not similar to the vehicle's signature. Therefore, the proposed scheme gives guarantees to the integrity of messages.

4.3 *Proof of privacy*

Our proposed scheme uses distributed pseudonyms to preserves the privacy of a vehicle. Distributed pseudonyms mean a vehicle's pseudonyms are updated periodically whenever it comes in the range of a new RSU' autonomous network.

4.4 *Proof of confidentiality*

The proposed scheme guarantees the confidentiality of message which is communicated between RSU and vehicles. An attacker will not be successful in accessing the message even if he knows the key SK. Suppose that an attacker tries to obtain

$SK = H_2\left(I_i.\left(Y_r + VID_r\right), A, VID_r, R_r\right)$ at the sender side. Here, I_i is a random number and hard for an attacker to find it. If an attacker tries to obtains $SK = H_2\left(\left(pp_r + x_r\right).A', A,'VID_r, R_r\right)$ at receiver side. This *SK* computes by using the private key of RSU and it is hard to get private key of an entity. So, scheme is confidentiality.

4.5 Proof of unlinkability

Unlinkability ensures that an attacker is not able to link the identity of a vehicle. Unlinkability is achieved through distributed pseudonyms which an individual vehicle has different and independent identities and vehicle uses these identities in different time intervals to send messages. So, it becomes infeasible for a malicious entity to link them.

4.6 Proof of non-repudiation

In the proposed scheme, vehicles cannot deny after sending a message. RSU can verify it by examine the signature $S = \left(pp_i + I_i.H_3\left(M,\ PID_{i,j,}TS_i\right) + x_i.H_3\left(M,\ PID_{i,j,}TS_i\right)\right)$, which is signed by the vehicle's private key. So non-repudiation can be achieved.

4.7 Proof of traceability

Traceability ensures that an RTA can trace the mapping between real identity and pseudonym identity of misbehaving vehicles.

Suppose an RSU finds that a particular vehicle sends a piece of bogus and misleading information, then it sends the vehicle's pseudo_id to the RTA. Now, RTA recovers the real identity of the vehicle as follows: Firstly, RTA extract $H\left(PID_{i,\,1}\right)$ from the $PID_{i,j}$. Then, search the similar match in his database if a similar entry found then RTA extract vehicle_no and $H\left(RID_i, R_i\right)$. RTA makes its credentials entry in the revocation list. Table 3 represents the comparative study of security requirements b/w propose an approach and existing approaches.

Table 3 Comparative study of security requirements

Schemes	*Authentication*	*Privacy*	*Confidentiality*	*Integrity*	*Non-repudiation*	*Traceability*
ECPP (Lu et al., 2008)	Yes	Yes	No	No	No`	Yes
A short identity-based signcryption scheme in multi-PKG (Zhang et al., 2011)	Yes	Yes	Yes	Yes	Yes	Yes
An identity-based security system for user-privacy (Sun et al., 2010)	Yes	No	Yes	No	Yes	Yes

Table 3 Comparative study of security requirements (continued)

Schemes	*Authentication*	*Privacy*	*Confidentiality*	*Integrity*	*Non-repudiation*	*Traceability*
CPAS (Shim, 2012)	Yes	Yes	No	Yes	Yes	Yes
An efficient conditional privacy-preserving authentication scheme for VSN without pairing (Lo and Tsai, 2016)	Yes	Yes	No	Yes	Yes	Yes
RAHAA (Pradweap and Hansdah, 2013)	Yes	Yes	Yes	Yes	Yes	Yes
EAAP(Azees et al., 2017)	Yes	Yes	No	No	No	Yes
SACP (Lu et al., 2018)	Yes	Yes	Yes	Yes	Yes	Yes
Our scheme	Yes	Yes	Yes	Yes	Yes	Yes

4.8 Impersonate attack

This attack happens in the lack of achieving authentication. In this, an entity that can be RSU, RTA, or a vehicle impersonating another entity with some of their benefit intentions. Our approach uses signcryption cryptography to ensure efficient authentication to reduce the chance of this attack in our system.

4.9 Sybil attack

This attack is possible in a network whenever a node forges multiple identities and broadcasts messages with them. In the proposed system, each vehicle is assigned with a temporary credential with a specific lifetime. Owing to the limited lifetime of credentials, a vehicle must update pseudo_id before its expiration. The newly assigned pseudo_id overwrites the existing ones. This makes sure that a vehicle has one pseudonym at a time. This approach saves the system from the Sybil attack.

4.10 Identity escrow attack

This attack takes place in the network when a user's private key is generated by a Trusted Third Party (TTP). TTP can use the user's private key on behalf of the private key's owner and send the information. In this non-repudiation can be compromised because the user can deny the message. In our proposed scheme, RTA must compute only partial credentials for vehicles or RSU, which makes RTA unaware of the private credentials of vehicles. So, the proposed scheme works against identity escrow problem and achieves non-repudiation.

4.11 ID disclosure and location tracking attack

These attacks are launched when an adversary continuously tracks the vehicles and links the sensitive information contained in the beacons. These attacks can be avoided by using distributed temporary credentials, and it must be updated periodically. The proposed approach using temporary pseudo_id and vehicles periodically updates it through RSU. A comparative analysis of security attacks preserved by the existing scheme and proposed scheme is depicted in Table 4.

Table 4 Comparative study of security attacks

Schemes	*Impersonate*	*Sybil*	*Modification*	*ID-disclosure*	*Replay*	*Identity escrow problem*
ECPP (Lu et al., 2008)	Yes	Yes	No	No	No	No
A short identity-based signcryption scheme in multi-PKG (Zhang et al., 2011)	Yes	No	No	Yes	No	No
An identity-based security system for user-privacy (Sun et al., 2010)	Yes	No	No	No	Yes	No
CPAS (Shim, 2012)	Yes	Yes	Yes	Yes	No	No
An efficient conditional privacy-preserving authentication scheme for VSN without pairing (Lo and Tsai, 2016)	Yes	Yes	Yes	Yes	No	No
RAHAA (Pradweap and Hansdah, 2013)	Yes	Yes	Yes	Yes	Yes	Yes
EAAP (Azees et al., 2017)	Yes	No	No	Yes	No	Yes
SACP (Lu et al., 2018)	Yes	Yes	Yes	Yes	Yes	No
Our scheme	Yes	Yes	Yes	Yes	Yes	Yes

Note: No – The scheme is prone to attack; Yes – The scheme is secure from the attack

5 Performance evaluation

In this section, we compute the computational and communication overhead of our approach and compare it with other existing approaches.

5.1 Communication overhead

In the proposed system, we are using ECC256 for achieving 128 bits of security strength. ECC256 uses a key size of 256 bits and ensures the same level of security strength as provided by RSA 3072-bit. The size of the points in bilinear pairing is 128 byte and size of finite field Z_P^* is 20 byte. For symmetric encryption, AES 128 is used which takes input and uses a 128-bit key size to encrypt and decrypt the message.

In the proposed approach, a vehicle sends a signcrypted message $\Sigma = (C, S, A)$ where C is 32-byte long message, S is 32 bytes and 32 bytes for A. So, the total size of $\Sigma = (C, S, A)$ is 96 bytes. If we discard the message part, i.e., C from it, then total signcryption size will be 96–32=64 bytes.

In addition, total size of signcrypted message is 64+45+4=113 bytes. Table 5 represents the comparisons between proposed approach and existing approaches. The proposed scheme has a smaller size signcrypted message, which results in a lower communication overhead. So, our scheme is better than the previously proposed approaches.

Table 5 Comparisons of communication overhead

Scheme	*Signed message size*
CPAS (Shim, 2012)	209 bytes
RAHAA (Pradweap and Hansdah, 2013)	201 bytes
EAAP (Azees et al., 2017)	996 bytes
SACP (Lu et al., 2018)	136 bytes
Our scheme	113 bytes

5.2 Computational overhead

This section presents the comparison between the proposed scheme with existing approaches based on the computation overhead. Let T_P, T_E, T_{PM} define the time for computing pairing operation, exponent, and point multiplication, respectively. In our scheme, the vehicle is signer that requires two multiplication and three scalar multiplication operations for signature generation and requires four scalar multiplications for signature verification. Our signature verification and generation process does not require any pairing operation, which decreases the time delay by a significant amount. Tables 6 and 7 present a comparison of computational overhead between proposed approach and existing approaches. The execution time required for different cryptographic functions running on Intel Pentium 4 3.0 GHz machine with 1 GB RAM is 1.50 ms for point multiplication, 8.15 ms for pairing operations and 5.3 ms for exponent (Lo and Tsai, 2016).

In a broadcast environment, the receiver would verify more messages than signing, so there is a significant requirement for verification could to done in minimal time. If we compare signature verification in our scheme with (Shim, 2012), it performs three pairing operations and one scalar multiplication. Pairing operation has a relatively higher computational cost than an operation of ECC. So signature verification in Shim (2012) is very high. RAHAA (Pradweap and Hansdah, 2013) performs three exponents operation on 1024 bits prime number for signature generation. It gives a 40% higher computational cost in comparison to our scheme. EAAP (Azees et al., 2017), requires one exponent for signature generation which is acceptable in VANET. But, signature verification requires two bilinear pairing and five exponent operations which need 42.8 ms to verify a single message.

Table 6 Required time comparison

Proposed approach	*Signature generation time (ms)*	*Signature verification time (ms)*
Zang et al. (2011)	14.62	16.24
CPAS (Shim, 2012)	3	24.48
RAHAA (Pradweap and Hansdah, 2013)	16	10.6
EAAP (Azees et al., 2017)	5.3	42.8
SACP (Lu et al., 2018)	1.5	4.5
Our scheme	4.5	6

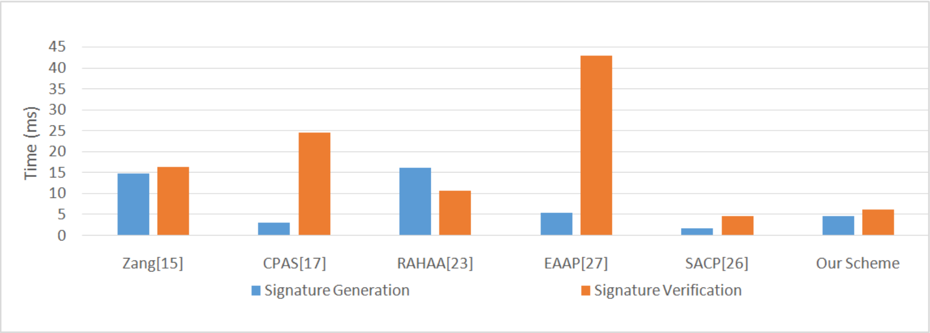
Table 7 Comparative study of computational overhead

Proposed approach	*Signature generation*	*Signature verification*
Zang et al. (2011)	$T_P + T_E + T_{PM}$	$2T_P$
CPAS (Shim, 2012)	$2T_{PM}$	$3T_P$
RAHAA (Pradweap and Hansdah, 2013)	$3\mathrm{T}_\mathrm{E}$	$2T_E$
EAAP (Azees et al., 2017)	T_E	$2\ T_P + 5T_E$
SACP (Lu et al., 2018)	T_{PM}	$3T_{PM}$
Our scheme	$\mathbf{3}T_{PM}$	$4T_{PM}$

SACP (Lu et al., 2018) has less computational cost in comparision to our scheme. However, this scheme is susceptible to identity escrow attack which is solved in our scheme.

Figure 1 presents the resultant graph for comparison of computational cost for signature generation and verification between proposed scheme and existing schemes.

Figure 1 Comparison of computational time required for different schemes



5 Conclusion

In this paper, we proposed an efficient anonymous authentication protocol centred on ID-based certificateless signcryption for achieving security and privacy in the VANET. The protocol has salient features like semi-trusted authorities, effective pseudonyms management, less communication overhead, etc. The proposed model uses certificateless signcryption to generate and verify the signcrypted messages, which improves bandwidth utilisation. Security analysis states that the proposed approach achieved most of the security requirements such as confidentiality, integrity, privacy, authentication, non-repudiation, etc. So, in brief, our proposed approach achieves most of the security requirements with a smaller communication overhead.

References

Al-Riyami, S.S. and Paterson, K.G. (2003) 'Certificateless public key cryptography', Laih, C-S. (Ed.): *International Conference on the Theory and Application of Cryptology and Information Security*, Springer Berlin Heidelberg, pp.452–473.

Azees, M., Vijayakumar, P. and Deboarh, L.J. (2017) 'EAAP: efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks', *IEEE Transactions on Intelligent Transportation Systems*, Vol. 18, No. 9, pp.2467–2476.

Gamage, C., Gras, B., Crispo, B. and Tanenbaum, A.S. (2003) 'An identity-based ring signature scheme with enhanced privacy', *Proceedings of the SecureComm*, pp.1–5.

Han, Y., Fang, D., Yue, Z. and Zhang, J. (2014, September) 'SCHAP: the aggregate signcryption based hybrid authentication protocol for VANET', *International Conference on the Internet of Vehicles*, Springer, Cham, pp.218–226.

Hu, C., Chim, T.W., Yiu, S.M., Hui, L.C. and Li, V.O. (2012) 'Efficient HMAC-based secure communication for VANETs', *Computer Networks*, Vol. 56, No. 9, pp.2292–2303.

IEEE Trial-Use Standard for Wireless Access in Vehicular Environments (WAVE) (2006) *Security Services for Applications and Management Messages,* IEEE Std. 1609.2, July 2006.

Kamat, P., Baliga, A. and Trappe, W. (2006) 'An identity-based security framework for VANETs', *Proceedings of the 3rd International Workshop on Vehicular Ad Hoc Networks*, ACM, pp.94–95.

Kapoor, V., Abraham, V.S. and Singh, R. (2008) 'Elliptic curve cryptography', *ACM Ubiquity*, Vol. 9, pp.1–8.

Kazemi, M., Delavar, M., Mohajeri, J. and Salmasizadeh, M. (2018) 'On the security of an efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks', *Proceedings of the IEEE Iranian Conference on Electrical Engineering (ICEE)*, IEEE, pp.510–514.

Li, F. and Wang, Y. (2007) 'Routing in vehicular ad hoc networks: a survey', *IEEE Vehicular Technology Magazine*, Vol. 2, No. 2, pp.12–22.

Liu, J.K., Yuen, T.H., Au, M.H. and Su01silo, W. (2014) 'Improvements on an authentication scheme for vehicular sensor networks', *Expert Systems with Applications*, Vol. 41, No. 5, pp.2559–2564.

Lo, N.W. and Tsai, J.L. (2016) 'An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks without pairings', *IEEE Transactions on Intelligent Transportation Systems*, Vol. 17, No. 5, pp.1319–1328.

Lu, M., Wu, Y., Xu, Y., Yang, Y. and Wang, J. (2018) 'SACP: a signcryption-based authentication scheme with conditional privacy preservation for VANET', *Proceedings of the International Conference on Wireless Algorithms, Systems, and Applications*, Springer, Cham, pp.773–779.

Lu, R., Lin, X., Zhu, H., Ho, P.H. and Shen, X. (2008) 'ECPP: efficient conditional privacy-preservation protocol for secure vehicular communications', *Proceedings of the IEEE 27th Conference on Computer Communications*, pp.1229–1237.

Malhi, A.K. and Batra, S. (2015) 'An efficient certificateless aggregate signature scheme for vehicular ad-hoc networks', *Discrete Mathematics and Theoretical Computer Science*, Vol. 17, No. 1, pp.317–338.

Pradweap, R.V. and Hansdah, R.C. (2013) 'A novel RSU-aided hybrid architecture for anonymous authentication (RAHAA) in VANET', *Proceedings of the International Conference on Information Systems Security*, Springer, Berlin, Heidelberg, pp.314–328.

Raya, M. and Hubaux, J.P. (2007) 'Securing vehicular ad hoc networks', *Journal of Computer Security*, Vol. 15, No. 1, pp.39–68.

Sampigethaya, K. et al. (2005) 'Caravan, providing location privacy for VANET', *Proceedings of the ESCAR*, pp.1–15.

Shamir, A. (1984) 'Identity-based cryptosystems and signature schemes', *Proceedings of Advances in Cryptology (CRYPTO'84)*, Springer-Verlag, pp.47–53.

Shim, K-A. (2012) 'CPAS: an efficient conditional privacy-preserving authentication scheme for vehicular sensor networks', *IEEE Transactions on Vehicular Technology*, Vol. 61, No. 4, pp.1874–1883.

Song, J.H., Wong, V.W. and Leung, V.C. (2010) 'Wireless location privacy protection in vehicular ad-hoc networks', *Mobile Networks and Applications*, Vol. 15, No. 1, pp.160–171.

Sun, J., Zhang, C., Zhang, Y. and Fang, Y. (2010) 'An identity-based security system for user privacy in vehicular ad hoc networks', *IEEE Transactions on Parallel and Distributed Systems*, Vol. 21, No. 9, pp.1227–1239.

Wahid, A. and Mambo, M. (2016) 'Implementation of certificateless signcryption based on elliptic curve using JavaScript', *International Journal of Computing and Informatics (IJCANDI'16)*, Vol. 1, No. 3, pp.90–100.

Wang, N-W., Huang, Y-M. and Chen, W-M. (2008) 'A novel secure communication scheme in vehicular ad hoc networks', *Computer Communications*, Vol. 31, pp.2827–2837.

Zhang, J., Cui, Y. and Su, X. (2011) 'A short identity-based signcryption scheme in the multi-PKG over the VANETs', *Information Technology Journal*, Vol. 10, No. 11, pp.2098–2104.

Zheng, Y. (1997a) 'Signcryption and its applications in efficient public key solutions', *International Workshop on Information Security*, Springer, Berlin, Heidelberg, pp.291–312.

Zheng, Y. (1997b) 'Digital signcryption or how to achieve cost (signature & encryption)≪ cost (signature)+ cost (encryption) ', *Proceedings of Advances in Cryptology (CRYPTO'97)*, pp.165–179.