A fuzzy-based trust evaluation framework for efficient privacy preservation and secure authentication in VANET

N. Jyothi and Rekha Patil

ABSTRACT
The Vehicular Adhoc Network (VANET) is a newly added smart technique in vehicles to ensure safety and reduce time consumption. Even though it saves time and guarantees safe travel, security and privacy are the most difficult issues in the VANET. Moreover, this is due to the fact that the methods exploit public key infrastructure, group signature, etc. Meanwhile, the hackers can acquire the sensitive data’s which are usually kept in the tamper-proof devices by using side-channel attacks. The VANET also possesses several security-related issues. To circumvent this we propose an efficient privacy-preserving and fuzzy-based trust evaluation scheme. This method ensures the security and authenticity of the VANET. To ensure security our proposed method utilizes a modified Elliptical Curve cryptographic (ECC) method which also reduces the computational complexities created by the conventional ECC. In our proposed method the TPD parameters are renewed more often to eliminate the attacks and permits batch verification methods to reduce the time. The experimental analysis is conducted in Matlab simulator in terms of computational cost, communication cost, evaluation of trustworthiness, privacy protection. The experimental analysis shows that proposed method provides 94% of trustworthiness and time consumption and communication overheads are reduced to greater extent.

1. Introduction
A smart VANET is the self-assembled, self-established, and cheapest intercommunication network. It is the exact solution for the issues faced (traffic, location, direction) in transportation nowadays. Vehicular-Ad-Hoc Network (VANET) is a type of Mobile Ad-Hoc Network (MANET) in which the vehicles communicate with each other via transportation system and interchange the details about traffic, and other essential information (Aijaz et al., 2006; Chowdhury et al., 2018; Engoulou et al., 2014; Hartenstein & Laberteaux, 2010; Paikrao et al., 2021; Raya & Hubaux, 2007).
The VANET is a type of wireless communication system which utilizes IEEE 802.11p standard and dedicated short-range communication (DSRC) protocol to maintain communication between vehicle to vehicle, vehicles to infrastructure (Devangavi & Gupta, 2017; Durga et al., 2019; Getzi & Dinesh Peter, 2018). Moreover, the VANET promptly improves the trustworthiness and security of the exchanged information during transportation. By gathering the information the vehicle owner can understand the road conditions and make a decision based on that and enhances the transportation safety and travelling efficacy.

Generally, VANET is composed of three types of layers as (i) onboard units (OBUs), (ii) roadside units (RSUs), and (iii) top (CA) layer (Contreras-Castillo et al., 2017; Köłaczek & Mizera-Pietraszko, 2018; Mejri et al., 2014; Shanmugapriyan, 2014; Swathynathini & Jeeva, 2014; Vörös et al., 2020). The OBUs are usually installed in the vehicles to connect the vehicle to another vehicle or vehicle to infrastructure via a wireless connection. On the other hand, RSUs are usually, the nodes installed on the roadways that are used as a mediator to connect the OBUs and the top layer of the VANET. The top layer is a certificate authority (CA) that is used to manage the administrative works like initializing and organizing the system parameters, data (open and secret) for the OBUs (Tanuja et al., 2015).

Basically, the VANET broadcasts both open and secured data among the nodes, and hence the attackers seamlessly attack the network to access the information like location, direction, and speed of the transports. Henceforth the attackers can mislead the user for their convenience and can perform physically as well as cyber-attacks. Therefore it is mandatory to protect the information provided by the user (Alfadhli et al., 2019). Several research works have been conducted to encourage the authentic broadcasting of data among vehicles. Due to the secured and authentic scheme, there may exist computational complexity.

Hence to enhance the security and authenticity and trustworthiness as well as to reduce the computational complexity we proposed a novel method known as Efficient privacy preservation and Fuzzy based trust evaluation scheme for securely authenticate VANET.

The contribution of our work is listed below.

- The proposed method adopts modified ECC to circumvent the computational complexities. Since the traditional ECC possesses some of it.
- The proposed method involves several steps such as trust authority (TA) initialization, registration of all the OBUs and RSUs involved in the VANET system, the interconnection of all OBUs and RSUs, verification, trust evaluation, renewal of TPD parameters, and vehicle revocation stage.
- The trustworthiness of the safety or traffic-related messages is ensured by the fuzzy-based trust evaluation.
- The proposed method reduces the computational complexities and hones up the trustworthiness of the VANET system.

The remainder of this work is organized as, in section 2, the literature survey of the proposed work is delineated. The preliminaries of our proposed work are explained in section 3. Section 4 elucidates the proposed work in the wider context. The performance analysis
of our proposed work with other existing works is demonstrated in section 5. Finally, the conclusion and the suggested future work are in section 6.

2. Literature survey

To achieve privacy-preserving in the VANETs many research works have been done by several researchers. Wei et al. (2019) proposed a novel method known as the lightweight privacy-preserving protocol for VANETs. To safeguard the messages from the attackers, this method exploited identity-based signatures. Moreover, the computational complexity has been reduced by the two outsourced algorithms for the exponential operations. Hence this method effectively minimizes the computational complexities by improving anonymity, traceability, and privacy. Even though, it provides better privacy however the optimal privacy is yet to be achieved.

As a result, Al-Shareeda et al. (2020) proposed a new approach for ensuring content and contextual privacy through a VANET-based privacy-preserving communication scheme (VPPCS). The security of the VANET has been enabled with the aid of incorporating elliptic curve cryptography (ECC) and an identity-based encryption scheme. Thus this proposed method can be used to protect the messages from the replay, impersonation, modification, and man-in-the-middle attacks. On the other hand, there occurs storage overhead while replacing the existing pseudonym with new. Meanwhile, Zhou et al. (2019) presented an elliptic curve-based conditional privacy-preserving authentication and key agreement scheme for the VANET. This provides an authentic service between the vehicles via a pre-shared password. However, the security has been enabled by utilizing the hybrid game model. The computational cost has been reduced by exploiting this method; nevertheless, the computational cost on the client-side is higher than the other works.

Further, Singh et al. (2019) delineate an enhanced method known as Cooperative Pseudonym Exchange and Scheme Permutation (CPESP) in order to sustain the privacy among the users’ in the VANET. In this method, the pseudonym has been exchanged between the user and the service providers. The user can modify the pseudonym based on their requirements. Hence it is arduous to track the user location by the service providers. Moreover, there is no inclusion of trusted authority in this scheme, which reduces the computational overhead. Besides, Ali and Li (2020) stated an efficient Identity-based Conditional Privacy-Preserving Authentication (ID-CPPA) signature mechanism incorporated with a bilinear map for the communication between the vehicles and the RSUs. This method can be used to secure the messages from the adaptive chosen-message attack and adaptive chosen-identity attack among the Inverse Computational Diffie-Hellman (Inv-CDH) issues in the Random Oracle Model (ROM). Therefore, this method offers better security and minimizes the computational complexity; nevertheless, the inclusion of a bilinear map might have led to an intricate security process.

Recently, Blockchain-based privacy-preserving has been proposed by Li et al. (2020). This method enhances the trustworthiness and thereby enables the security of the messages in VANET. The trustworthiness can be enhanced with the trust management algorithm and data security can be accomplished by the proposed blockchain technique. However, the real-time application shows that this method doesn’t provide optimal security and trustworthiness when compared to other methods. Meanwhile, privacy-preserving has also been achieved by the evolution of blockchain-assisted privacy-preserving
authentication system (BPAS) which was proposed by Feng et al. (2019). It also provides
decentralized authenticate solutions. However, if multiple messages are received at the
same time, simultaneous verification of those messages was arduous. Hence it is manda-
tory to support batch verification to attain optimized security in the VANET.

3. Preliminaries

3.1. Elliptic curve cryptography

Let us consider that a vehicle $X$ is trying to transmit the encrypted plain data to vehicle $Y$.
Then the vehicle $X$ performs several operations which are listed below (Forouzan &
Mukhopadhyay, 2015).

- Vehicle $X$ chooses an elliptic curve $E$ with the base point $M$.
- Then the vehicle $X$ generates the public key $K = kM$ by exploiting the selected private key $k$.
- The generated public key $K$ along with the elliptic curve $E$ and $M$ are transmitted to
  vehicle $Y$.
- The vehicle $Y$ accepts the data and decrypt the encrypted plain text into the $N$ point in
  the elliptic curve $E$ and creates an arbitrary integer $r$ where $r < a$.
- The vehicle $Y$ estimates the $C1 = N + rK$ and $C2 = rM$.
- $C1$ and $C2$ are transmitted to the vehicle $X$ by the vehicle $Y$.
- Then the point $N$ is regenerated by the vehicle $X$ by the estimation of $C1 - kC2$. Then
  the extracted $N$ is decrypted to acquire the plaintext.

The inversion operation involved in this ECC creates computational complexities and
becomes a burden while transmitting the data (Chanti et al., 2018). Hence the traditional
ECC is modified into a new version by eliminating the inversion operation. The modified
ECC algorithm is elucidated below.

3.2. Modified ECC

The modified ECC involves the following steps

- To construct the data abstract, the hash function is incorporated with the signer.
- The elliptic curve parameters are defined by the signer and can be given as
  $F = (P, x, h, m, a, h)$ or $F = (n, f(s), x, h, m, a, h)$.
- The elliptic curve parameters are defined by the hash function which is determined by
  the signer.
- The key $s$ is selected by the Signer and it depends on the $M(P)$ the finite field and the
  chosen points of the Elliptic curve. Henceforth the public key $b = sm$ and public $b$.
- The arbitrary numbers $K$ are selected by the signer and it lies between 1 and $a-1$
- Moreover, it also estimates the $r = km$, if $r = 0$ and return to the previous step
- Henceforth the estimation of $l = nrs - k$ is made and acquired $(b,r)$ as the signature of
  $n$. after that the $(b,r)$ and $n$ are transmitted to the verifier for the further process.
- Verifier evaluates the new parameter value $r' = bm + nsr$. 
Then the verifier decides whether the signature is accurate or not and accepts the \( a' = r \) values and eliminates the other possibilities.

### 3.3. Network model

The VANET is composed of three units: Trusted Authority (TA), Road Side Unit (RSU), and Onboard Unit (OBU). The RSU is the on-roads unit and is a fixed framework. This is usually used as a mediator between the vehicles and the TA through wired or wireless channels. On the other hand, the OBU is installed in every smart vehicle, i.e. VANET-enabled vehicle. This helps the vehicle to broadcast and receive essential informations such as, traffic and safety-related data, and also it includes tamper-proof devices (TPD) which securely safeguard the personal identity data. However, the third-party unit TA is used to keep and manage the public system parameters from the attackers with respect to the other two units. The schematic framework of VANET is illustrated in Figure 1. The benefit of using this communication is to enhance safety, efficacy, and driver assistance.

To begin with, the RSU and OBU are registered on the TA. Following this, the mutual authentication of RSU and OBU has been performed in order to validate the identity. If the user is not an authentic one then the TA is used to identify the attacker, else the authentication process becomes a success and improves the trustworthiness of OBU. The parameter can be estimated by the RSU. After ensuring trustworthiness the OBU can interact with the neighbours within their constraints.

### 3.4. Common threats

The common threats in the VANET are replay, impersonation, modification, and side-channel attacks. Hence it is necessary to design the authentication mechanism to

![Figure 1. A typical VANET model.](image)
sustain and eliminate the above-mentioned attacks. The common attacks are elucidated below.

### 3.4.1. Replay attack
This is a kind of common attack in which the malicious vehicles replay the safety-related data which were created by the TA for the authenticate vehicle previously.

### 3.4.2. Impersonation attack
The malicious vehicle tries to act as the legitimate vehicle and steal the identity of the vehicle. Then it impacts distortion to the legitimate vehicle by the illegal access to the network. This attack is known as the Impersonation attack.

### 3.4.3. Modification Attack
The malicious vehicle remolds the safety-related data that are transmitted between the VANET users.

### 3.4.4. Side-channel attack
This is a daunting attack since it gains sensitive data from the TPD. This can be achieved by hacking the master system key. If this attack is performed by the attackers then the entire system will be used to collapse.

Hence it is necessary to design the VANET to circumvent the above-mentioned attacks to safeguard the system. Some of the design goals are listed in the next section.

### 3.5. Design requirements
The goals that involve in the designing of the VANET system are listed below.

I. It is a must to sustain privacy in the VANET since it is an important parameter in this system. Once the privacy is broken it is easily hacked by the attackers.

II. Second, the verifier must ensure the message integrity and authentication in order to protect the safety-related messages from alteration by the attackers.

III. Third, the system must provide the trustworthiness traffic-related messages between OBU and RSUs. Sometimes, one OBU broadcast fault messages to the neighbour OBU. Hence it is a must to ensure the trust between the OBU to access data seamlessly.

IV. Moreover, the TA must be designed in such a way as to trace and revoke the attacker’s identity in order to circumvent the suspicion or discard of messages.

V. Meanwhile, it is necessary to subjugate the accessibility of two subsequent safety-related messages by the attackers transmitted by the same source, since it is easy to track the content.

VI. On the other hand, it is necessary to design a VANET that provides the identity-based conditional privacy-preserving authentication mechanism to avoid the common threats which were elucidated in the previous section.
4. Proposed method

Our proposed method utilizes the modified ECC to analyse the computation and communication cost of the VANET and the mutual authentication can be analysed by utilizing fuzzy which provides information about trustworthiness. Moreover, it can also be used to store the private key in the TPD of RSU which is used to take place during the registration stages of OBUs. However, these stored keys and pseudonyms are kept for only a short duration of time and after that, it will discard it and update the new version. This updation will take place during the renewal of the TPD parameters stage and is mostly carried out frequently. As a result, the attackers’ illegal attacks are avoided. Our proposed method also utilized batch message verification that can be allowed to perform concurrently during the verification stage. This is a good option during high traffic conditions.

The stages involved in the proposed method are TA initialization, registration, interconnecting, transmission and verification, measurement of trustworthiness, renewing the TPD parameters, and TPD parameters renewing, and vehicle revocation stages.

4.1. TA Initialization stage

The public parameters that are utilized for the VANET systems are created by the TA. The initialized parameters are then published to initiate the registration stages of other OBU and RSUs that are participating in the transmitting process. Steps involved in TA initialization are listed below.

- From the point $P$ of an additive group $M$, the TA chooses two large prime numbers such as $m$ and $n$. Here $n$ represents the order and the non-singular elliptic curve $E$ can be denoted as $F = (P, x, h, m, a, h)$ or $F = (n, f(s), x, h, m, a, h)$.
- The secret value is set by the TA arbitrarily and denoted as $\varepsilon \in \mathbb{Z}_n^*$. This value is selected as the master private key and the corresponding master public key can be evaluated $P_{pub} = \varepsilon.P$ by the TA.
- Henceforth the symmetric encryption function can be chosen by the TA and can be denoted as $E_{11}(.)/D_{11}(.)$. It also selects the three secure functions as a cryptographic hash function and can be indicated as $h_1: M \rightarrow \mathbb{Z}_n^*; h_2:[0, 1]^* \times [0, 1]^* \times M \rightarrow \mathbb{Z}_n^*; h_3:[0, 1]^* \rightarrow \mathbb{Z}_n^*$.

4.2. RSU and OBU registration stage

The registration process is carried out to authenticate the identity of all RSUs and OBUs. Moreover, the registration stage is classified into two stages (i) RSU registration and (ii) OBU registration.

- **RSU Registration**

  The steps followed in the RSU registration are listed below.
Based on the position of RSU, the original identity is chosen by the TA as RSU $OID_R$.

The public parameters are preloaded into each RSU by the TA and it is given as $\psi = \{m, n, u, z, P, P_{pub}, h_1, h_2, h_3\}$.

The $<OID_R>$ is stored into the registration list of RSUs by the TA and following this, the master private key $e$ is transmitted to the RSUs.

**OBU Registration**

The steps followed in OBU registration are listed below.

- The original identity $OID_v$ and the password $PS$ is capitulated to the TA via a secured channel by the driver of the subjected vehicle.
- The estimation of pseudonyms has been carried out by TA to verify the availability of the $OID_v$ in the valid period $VP_v$ and can be denoted as $P_s = h_3(OID_v||VP_v)$.
- The encryption key for the vehicles is evaluated by the TA along with the secret integer $l_i \in Z_q^*$ and the tuple $<\lambda_i, P_s, P_{pub}>$ is shifted into the TPD of every vehicle.
- The public parameters $\psi = \{m, n, u, z, P, P_{pub}, h_1, h_2, h_3\}$ are preloaded into every OBU along with the tuple $<OID_v, P_s, VP_v, \lambda_i>$ in the registration list of vehicles.

### 4.3. Interconnecting stage

The vehicles which hold OBU must have a link with the RSU followed by authenticating itself with the TA. The RSU analyses the requested OBU and provides a private key $MK$ to it. Hence the requested OBU becomes an authentic vehicle and can able to transmit data to the adjacent vehicles and RSUs. The interconnecting stage can be described as,

- The interconnection of OBU to RSU can be carried out when the OBU arbitrarily chooses integer $r \in Z_n^*$ and evaluates its pseudo-ID $PID_i = \{PID_i^1, PID_i^2\}$ as,

  $\begin{align*}
  PID_i^1 &= r.M \\
  PID_i^2 &= P_s \oplus h_1(r.P_{pub})
  \end{align*}$

  Here, $r.P_{pub}$ represents the point of the x-axis in an elliptic curve. Then the message $<R, PID_i, \mu_{OBU}>$ of OBU is transmitted to the RSU. Moreover, $\mu_{OBU}$ can be denoted as $\mu_{OBU} = h_3(R||PID_i||P_s)$.

- The RSU can be interlinked to the TA by sending the message $\mu_{OBU}$ to the RSU. Henceforth, the RSU checks the timestamp $R$ to ensure validity. If there doesn’t have validity, i.e. $R_t - R > R_\Delta$ then it will discard the message. Here, $R_t$ represents the message received time, and $R_\Delta$ defines the predefined time delay. Then the $P_s$ can be estimated as,

  $P_s = PID_i^2 \oplus h_1(r.PID_i^1)$

  Then the RSU checks whether $\mu_{OBU} = h_3(R||PID_i||P_s)$ else it will discard the message and transmit $<R_t, OID_R, P_s>$ to the TA.
The transmission of the message from the TA to the RSU can be carried out when the message \( \langle \lambda_i, OID_R, P_s \rangle \) is received by the TA, and then the timestamp \( \lambda_i \) validity is checked. If it is the new entity the TA checks it with the registration list, if it is available then it transmits the message \(<\text{authentic}, \lambda_i>\) to the RSU else it will send the message \(<\text{not authentic}>\) and discard the messages.

The transmission of messages from RSU to OBU can be performed when the received message is \(<\text{authentic}, \lambda_i>\), otherwise it does not accept the messages. Then it estimates the secret value \( \psi_i \in Z_n^* \).

Henceforth the transmission between RSU and OBU can also perform when the RSU manages the private key as \( PK_i = \langle \psi_i, w_i \rangle \) for the OBU and exploits the encryption key of the node to encrypt the private key to access \( \text{Authentic}_{RSU} = E_{\lambda_i}(PK_i) \) and transmits the message \( \langle \lambda_2, \text{Authentic}_{RSU}, \mu_{RSU} \rangle \) to the OBU, and the \( \mu_{RSU} = h_3(\lambda_2 \parallel PK_i \parallel P_s) \).

Meanwhile, if the OBU receives the \( \langle \lambda_2, \text{Authentic}_{RSU}, \mu_{RSU} \rangle \) message, the time stamp validity is verified to analyse the life of the message. If the time stamp validity is available then the OBU decrypts the \( PK_i = D_{\lambda_i}(\text{Authentic}_{RSU}) \) in order to acquire the \( PK_i \) value. It also checks the \( \mu_{RSU} = h_3(\lambda_2 \parallel PK_i \parallel P_s) \) value to initiate the transmission with the aid of \( PK_i \).

In the meantime, the RSU uploads more pseudo-IDs and private keys into each node of OBU to attain the valid duration during the interconnection stage. These pseudo-IDs are updated within the expiry time of private keys while travelling the VANET (Li et al., 2019).

### 4.4. Transmission and verification stage

This stage involves two steps (i) message signing and (ii) verification

#### 4.4.1. Message signing
The safety-related messages are signed by the sender to provide security and authenticity. This can be performed to verify the message’s reliability, trustworthiness, and avoidance of modification of sensitive messages by the receiver and also ensures the signature is from the valid user OBU.

#### 4.4.2. Verification
This stage involves two types of verification (i) Single message verification and (ii) Batch message verification.

#### 4.4.3. Single message verification
This type of verification is performed by every VANET vehicle to ensure the authenticity and integrity of the arrived signature of the safety-related messages. This process is performed prior to the other processing steps to circumvent the entry of malicious effect. Usually, malicious vehicles act as authenticate vehicles and transmit fake messages to steal the original location details of the targeted vehicles.

#### 4.4.4. Batch message verification
This process is carried out to check the multiple safety-related messages concurrently by the verifier either RSU or OBU. Our proposed mechanism utilizes this verification method along
with the small exponent test technique (Liu et al., 2018) to reduce the computational time. The computational cost can be reduced by arbitrarily producing the integer value \( \gamma = \{ \gamma_1, \gamma_2, \ldots, \gamma_n \} \), here \( \gamma \in [1, 2^t] \) and \( t \) is a very small integer value. Moreover, the receiver receives several safety-related messages that can be considered as \( \{PID_1^1, m_1^1, R_1^1, \mu_1^1\}, \{PID_1^2, m_1^2, R_1^2, \mu_1^2\}, \ldots, \{PID_n^p, m_n^p, R_n^p, \mu_n^p\} \). Then the messages can be concurrently checked by using \( \mu_i^p \) of the message signature tuple \( \{PID_i^p, m_i^p, R_i^p, \mu_i^p\} \) and can be defined as,

\[
\left( \sum_{j=1}^{n} (\gamma, \delta) \right) P_{\text{pub}} = \left( \sum_{i=1}^{n} (\gamma, \omega_i) \right) + \left( \sum_{i=1}^{n} (\gamma, Q_i) \right)
\]

### 4.5. Measurement of trustworthiness

The VANET system follows transmitting data from one OBU to another OBU about various conditions and safety-related messages. The receiver OBU accepts the messages and acts accordingly. Sometimes, these transmitted data are not all reliable since the received message may have expired validity, or else illegal OBU can send messages to track the location of the corresponding OBU. This might have lead to serious issues. hence we adopted a fuzzy comprehensive strategy to tackle these consequences. Since the reliability of the message is totally agreed with the trustworthiness of the sender, the proposed fuzzy-based approach increases the trusted features of OBUs by employing a mechanism known as trustworthiness evaluation (Hasrouny et al., 2017). Each OBU access all its 1-hop adjacent OBUs and estimates the \( T \) value which is called direct trust of OBU. These estimated trust measurements \( T \) are broadcasted to other neighbours frequently by the OBU. Thus every OBU exhibits the direct trust measurement received from the neighbours and the indirect trust received from the OBU’s adjacent over \( i \) and it can be represented as:

- \( T_{OBU} \): <direct trust> opinion of OBU on \( i \)
- \( T_{OBU} \): <indirect trust> opinion of OBU on \( i \) based on the adjacent OBU
- \( T_{OBU} \): <total trust> opinions of both OBUs, i.e. calculation of both direct and indirect trust.
- \( T_{OBU} \): <global trust> initial trust given by the OBU \( i \) for the newly entering OBUs in the VANET system.
- \( T_{OBU} \): <global trust> that are stockpiled in the RSU for the OBU \( i \).

Thus the trustworthiness includes both the direct and indirect estimation of trust. The trustworthiness can be measured and compared with the threshold trust value. Fuzzy estimates the trustworthiness if the value exceeds the threshold value then the OBU is considered as a trusted one else they discard the OBU and marked as an untrusted OBU or malicious one.

### 4.6. Renewing of TPD parameters stage

The renewal of TPD parameters is done to preserve the OBU from the side-channel attack. The information that is stockpiled in TPD is pseudonym and encryption key and it should be updated frequently by inspecting it online. If the OBU fails to update the TPD
parameters, then the attackers can easily collapse the VANET system due to the long durability of data. The steps involved in the renewal of TPD parameters are listed below.

The OBU selects the \( l \) the arbitrary value from \( Z_n^* \) to estimate the \( \mathrm{PID}_1^i = l \cdot \mathrm{IP} \) and \( \mathrm{PID}_2^i = P_s \oplus h_1(l \cdot \mathrm{P}_{\text{pub}}) \). Then the OBU transmits the message \( \{ \mathrm{PID}^\text{new}_v, \mathcal{R}, \mu_{\text{OBU}} \} \) to the TA and the RSU. Here \( \mathrm{PID}^\text{new}_v \) can be denoted as \( \mathrm{PID}^\text{new}_v = \{ \mathrm{PID}_1^i = l \cdot \mathrm{IP}, \mathrm{PID}_2^i = P_s \oplus h_1(l \cdot \mathrm{P}_{\text{pub}}) \} \) and \( \mu_{\text{OBU}} \) can be represented as, \( \mu_{\text{OBU}} = h_3(\mathrm{PID}_1^i \| \mathrm{PID}_2^i \| \mathcal{R}) \). Henceforth, the validity of the timestamp \( \mathcal{R} \) can be checked after receiving the \( \{ \mathrm{PID}^\text{new}_v, \mathcal{R}, \mu_{\text{OBU}} \} \) message, the TA estimates the old pseudonym for the validity available timestamp. Moreover, it also checks the availability of \( \mu_{\text{OBU}} = h_3(\mathrm{PID}_1^i \| \mathrm{PID}_2^i \| \mathcal{R}) \) and analyses the tuple that whether the \( (\mathsf{OID}_v, P_s, \mathsf{VP}_v, \lambda_i) \) is still there in the registration list, else the \( \mathsf{VP}_v \) validation is verified. However, if the \( \mathsf{VP}_v \) expired then a new \( \mathsf{VP}^\text{new}_v \) is selected by the TA. Following this, the TA also estimates the new pseudonym for the registered vehicles to encrypt the messages. These generated pseudonyms are broadcasted to the vehicles and finally, the vehicles encrypt the received messages to access the newly generated pseudonym and the encryption key.

4.7. Vehicle revocation stage

The TA traces the illegal node and revokes it. After that, the TA publishes the identity from the signature message \( \{ \mathrm{PID}_i, m_i, \mathcal{R}, \mu_i \} \). Here, \( \mathrm{PID}_i = \{ \mathrm{PID}_1^i = s \cdot \mathrm{IP}, \mathrm{PID}_2^i = P_s \oplus h_1(s \cdot \mathrm{P}_{\text{pub}}) \} \). It can be denoted by the following equations.

\[
P_s = \mathrm{PID}_2^i \oplus h_1(r \cdot \mathrm{PID}_1^i)
\]
\[
= P_s \oplus h_1(s \cdot \mathrm{P}_{\text{pub}}) \oplus h_1(r \cdot \mathrm{PID}_1^i)
\]
\[
= P_s
\]

Thus the original identity of the malicious node is published with the knowledge obtained from the registration stage.

5. Performance analysis

The performance of our proposed method is analysed by comparing our work with existing works such as CPPAS (Al-shareeda et al., 2020), VITS (Zheng et al., 2017), ECVEPP (Cui et al., 2020) and LSV (Farouk et al., 2020). The simulations are carried out in a Matlab simulator. Moreover, our proposed method used fuzzy for the evaluation of trustworthiness, and also the private keys and pseudonyms are stored for a short duration of time both in OBU and RSU in order to sustain the connection between them and circumvent the attackers. Hence we focus to analyse the computational cost, communication cost, security, efficiency of the verification stage, and trustworthiness.

5.1. Security analysis

The security analysis is made on the design requirements of all the existing and proposed schemes. The different design requirements are resistance to replay attack, resistance to alteration attack, resistance to impersonation, resistance to side-channel attacks, identity privacy preservation, traceability and revocation, unlinkability,
integrity and authentication, and trustworthiness and can be denoted as DR1, DR2, DR3, DR4, DR5, DR6, DR7, DR8, and DR9 correspondingly. The outcomes are listed in Table 1.

From Table 1, the parameter trustworthiness is only achieved by the proposed method and other methods have not accomplished it. Moreover, the integrity and authentication requirements are fulfilled by the CPPAS (Liu et al., 2018), VITS (Hasrouny et al., 2017), and our proposed methods. However, the other methods fail to achieve it. Meanwhile, the resistance to side-channel attacks is accomplished by the methods VITS (Hasrouny et al., 2017) and our proposed method. Nevertheless, traceability and revocation have been accomplished by all methods. Hence from Table 1, it is evident that all design requirements are fulfilled only by our proposed method.

5.2. Storage overhead and Computation cost analysis

The storage overhead and time consumption are analysed for various approaches and listed in Tables 2 and 3. Since we utilizing the hash function, it will affect the storage capacity and lead to storage overhead. When compared to other approaches our proposed method has less storage capacity irrespective of the number of nodes. When the number of vehicles is equal to 1000, the storage overhead of our proposed method is equal to 375 bytes and for other approaches for VITs it is 893 bytes, CPPAS exhibits 798 bytes. Moreover for the number of vehicles is equal to 1000000, the storage overhead of our proposed method is 863 bytes.

Table 1. Comparative analysis of proposed method with the existing approaches for the security parameters.

| Methods     | DR1 | DR2 | DR3 | DR4 | DR5 | DR6 | DR7 | DR8 | DR9 |
|-------------|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| CPPAS [28]  | ✓   | ✓   | ×   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   |
| VITS [29]   | ✓   | ✓   | ×   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   |
| ECVEPP [30] | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   |
| LSV [31]    | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   |
| Proposed    | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   |

Table 2. Comparison of storage overhead in various approaches.

| Storage overhead (byte) per number of vehicles | 1000  | 10000 | 100000 | 1000000 |
|------------------------------------------------|-------|-------|--------|---------|
| CPPAS [28]                                     | 798   | 1592  | 2459   | 2867    |
| VITS [29]                                      | 893   | 1483  | 2178   | 2396    |
| ECVEPP [30]                                     | 753   | 1209  | 1983   | 2004    |
| LSV [31]                                       | 672   | 1001  | 1730   | 2196    |
| Proposed                                       | 375   | 562   | 732    | 863     |

Table 3. Comparison of time consumption in various approaches.

| Time consumption (ms) per number of vehicles | 1000  | 10000 | 100000 | 1000000 |
|---------------------------------------------|-------|-------|--------|---------|
| CPPAS [28]                                  | 0.165 | 0.189 | 0.231  | 0.264   |
| VITS [29]                                    | 0.175 | 0.243 | 0.359  | 0.321   |
| ECVEPP [30]                                  | 0.193 | 0.289 | 0.345  | 0.376   |
| LSV [31]                                     | 0.189 | 0.287 | 0.321  | 0.356   |
| Proposed                                     | 0.091 | 0.123 | 0.156  | 0.212   |
overhead of our proposed method is 863 bytes which is the lowest of all, whereas, CPPAS possesses 2867 bytes, VITS exhibits 2396 bytes, ECVEPP possesses 2004 bytes and the LSV exhibits 2196 bytes of storage overhead. Thus our proposed work has less storage overhead.

The time consumption of various methods vs our proposed method is depicted in Table 3. Table 3 shows our proposed method consumes less energy than the other irrespective of the number of vehicles. When the number of vehicles is 1000, the time consumed by our proposed method is 0.091 ms which is the least and the ECVEPP consumes the highest time of about 0.193 ms. Meanwhile, when the number of vehicles is 100000, the time consumed by our proposed method is 0.156 ms and the highest time consumption is by the method VITS about 0.359ms. However, the rise in the number of vehicles does not affect the proposed work. It takes less time than the other approaches.

Meanwhile, the comparative analysis of the proposed work in terms of computational cost with respect to the number of traffic-related messages received is depicted in Figure 2. From Figure 2 it is evident that state-of-art works such as VITS (Hasrouny et al., 2017), ECVEPP (Al-shareeda et al., 2020), and LSV (Zheng et al., 2017) depicts high consumption of time with respect to the number of traffic-related messages. Also, the time consumption increases with the number of messages received. Since enabling the accessing process takes more time than expected. However, the time consumption of method CPPAS (Liu et al., 2018) and our proposed method exhibits more or less similar and we analysed it in Figure 3.

From Figure 3 it is evident that the proposed method and CPPAS consume less time and the difference between the both is only a few milliseconds.

![Figure 2. Comparative analysis of proposed method with existing works in terms of computational cost vs the number of traffic-related messages.](image-url)
In the meantime, time overhead occurs during the authentication stage to provide authenticity to the user vehicle. Hence it is essential to analyse the time overhead both for onboard units and roadside units. Therefore, we analysed the time consumption of OBU and RSU during the authentication stage for the proposed and the other existing works as mentioned and depicted in Figure 4.

From Figure 4, it is evident that the VITS approach exhibits higher overheads for both OBU and RSU. Following it, ECVEPP (Al-shareeda et al., 2020) possesses a little lower time overhead for both cases than the VITS. However, our proposed method exhibits a lower time overhead than all other approaches, and moreover, the time overhead in the OBU is lesser than the RSU.

Figure 3. Time consumption comparison of the proposed method with the CPPAS method.

Figure 4. Time overhead occurs during the authentication stage for different methods.
5.3. Communication cost analysis

The communication cost is another parameter that impacts the effectiveness of the proposed method. Hence it is necessary to analyse the communication cost of the proposed method with the other existing approaches. We have made a comparative analysis and disclosed it in Table 2.

From Table 4, it is evident that the proposed method has the least communication cost whereas the method CPPAS (Liu et al., 2018) exhibits maximum communication cost, followed by VITS (Hasrouny et al., 2017), ECVEPP (Al-shareeda et al., 2020), and LSV (Zheng et al., 2017). Thus our proposed outperforms all the existing approaches we have taken.

5.4. Measurement of trustworthiness

Our main approach is to measure the trustworthiness of the messages received and broadcasted. For efficient communication between the vehicles, it is an important factor to analyse. Sometimes the vehicles receive time expired messages, fake messages, etc., Hence it is a must to measure the trustworthiness of traffic or safety-related messages. The percentages of trustworthiness provided by various methods are depicted in Figure 5. From the figure, it is evident that the proposed method ensures 94% of trust, and the method ECVEPP provides 84%, CPPAS provides 78%, LSV enables 70% of trustworthiness and the method VITS provides 64%.

**Table 4.** Comparative analysis of different approaches in terms of communication cost.

| Methods  | Cost for a single message (bytes) | Cost for \( n \) Messages (bytes) |
|----------|----------------------------------|----------------------------------|
| CPPAS    | 436                              | 436 \( n \)                      |
| VITS     | 249                              | 249 \( n \)                      |
| ECVEPP   | 234                              | 234 \( n \)                      |
| LSV      | 126                              | 126 \( n \)                      |
| Proposed | **102**                          | **102** \( n \)                  |

**Figure 5.** Evaluation of trustworthiness for various approaches.
5.5. Location privacy protection

The next important factor is to analyse the probability of location identity leakage. Generally, the leakage of privacy details leads to the decrement of security. For the experimental purpose, we considered that only 30% of the malicious vehicles have the intention to attack the neighbours. Let all the other malicious nodes like normal nodes. The resultant outcome is plotted in Figure 6.

From Figure 6, it is evident that the proposed method provides high location privacy protection, i.e. up to 35 rounds it possesses little privacy leakage, henceforth it provides high security. Whereas, other methods depict less security than the proposed methods. Moreover, the presence of malicious nodes is unavoidable in every situation. Hence it is necessary to allocate better location privacy protection to ensure the security of the VANET system.

6. Conclusion

This paper presented a novel method to ensure security and authentication in the VANET. The safety or traffic-related data broadcasted between the OBUs, RSUs, and TA are encrypted by the cryptographic method known as modified ECC. To protect registered vehicles from malicious attacks, the method includes several stages such as trust authority (TA) initialization, registration of all OBUs and RSUs involved in the VANET system, the interconnection of all OBUs and RSUs, verification, trust evaluation, renewal of TPD parameters, and vehicle revocation. Moreover, the trustworthiness has been evaluated by utilizing fuzzy. The experimental analysis shows that the proposed method provides 94% of trustworthiness and the time consumption and communication overheads are reduced to a great extent. The storage overhead is also minimized in our method. Henceforth, the
probability of location privacy leakage was also analysed and our method ensures high security after the completion of 35 rounds. Thus concluded that our proposed method ensures high security and minimizes all the computational complexities when compared to other approaches. The limitations of any privacy preserving schemes in the VANETs include the high mobility and incomplete infrastructures which leads to vulnerability in provisioning the reliable services. However, in future the proposed work can be modified by utilizing a different cryptographic method to ensure the maximum security of the VANET system.

Disclosure statement
No potential conflict of interest was reported by the author(s).

Notes on contributors

N. Jyothi is an assistant professor in Computer Science & Engineering department, working in H.K.E Society’s S.L.N College of Engineering, Raichur. She is having teaching experience of more than five years. Currently she is carrying out research in Networking. Her research interest includes VANET, MANET, Cloud Computing and Big data.

Rekha Patil working as Professor in the department of Computer Science and Engineering at Poojya Doddappa Appa College of Engineering Kalaburagi. She has 26 years of teaching experience, She completed her Ph.D. at Jawaharlal Nehru Technological university Hyderabad Telangana state,2015.M-Tech(CSE) at KBN College of Engineering Kalaburagi, Gulbarga university Karnataka 1999 and BE(CSE) at Gulbarga university, Gulbarga Karnataka 1990. Her area of research interest includes Computer Networking, Big Data, Cloud Computing and Internet of things.

References

Aijaz, A., Bochow, B., Dtzer, F., Festag, A., Gerlach, M., Kroh, R., & Leinmuller, T. (2006). Attacks on inter-vehicle communication systems—an analysis. In Proceedings of the 3rd International Workshop on Intelligent transportation, WIT-2006 (pp. 189–194).

Alfadhli, S. A., Alresheedi, S., Lu, S., Fatani, A., & Ince, M. (2019). ELCPH: An efficient lightweight conditional privacy-preserving authentication scheme based on hash function and local group secret key for VANET. In Proceedings of the 2019 the World Symposium on Software Engineering (pp. 32–36).

Ali, I., & Li, F. (2020). An efficient conditional privacy-preserving authentication scheme for vehicle-to-infrastructure communication in VANETs. Vehicular Communications, 22, 100228. https://doi.org/10.1016/j.vehcom.2019.100228

Al-shareeda, M. A., Anbar, M., Manickam, S., & Hasbullah, I. H. (2020). An efficient identity-based conditional privacy-preserving authentication scheme for secure communication in a vehicular ad hoc network. Symmetry, 12(10), 1687. https://doi.org/10.3390/sym12101687

Al-Shareeda, M. A., Anbar, M., Manickam, S., & Yassin, A. A. (2020). Vppcs: Vanet-based privacy-preserving communication scheme. IEEE Access, 8, 150914–150928. https://doi.org/10.1109/ACCESS.2020.3017018

Chanti, Y., Naik, D. K. S., Mothe, R., Yamsani, N., & Balija, S. (2018). A modified elliptic curve cryptography technique for securing wireless sensor networks. International Journal of Engineering and Technology, 7(1.8), 230–232. https://doi.org/10.14419/ijet.v7i1.8.22959

Chowdhury, D. N., Agarwal, N., Laha, A. B., & Mukherjee, A. (2018). A vehicle-to-vehicle communication system using lot approach. In Second International Conference on Electronics. Communication and Aerospace Technology (ICECA) (pp. 915–919). https://doi.org/10.1109/ICECA.2018.8474909.
Contreras-Castillo, J., Zeadally, S., & Guerrero Ibáñez, J. A. (2017). A seven-layered model architecture for internet of vehicles. *Journal of Information and Telecommunication, 1*(1), 4–22. https://doi.org/10.1080/24751839.2017.1295601

Cui, J., Wei, L., Zhong, H., Zhang, J., Xu, Y., & Liu, L. (2020). Edge computing in VANETs—an efficient and privacy-preserving cooperative downloading scheme. *IEEE Journal on Selected Areas in Communications, 38*(6), 1191–1204. https://doi.org/10.1109/JSAC.2020.2986617

Devangavi, A. D., & Gupta, R. (2017). Routing protocols in VANET—A survey. In *International Conference on Smart Technologies For Smart Nation (SmartTechCon)* (pp. 163–167).

Durga, S., Mohan, S., Dinesh Peter, J., & Nittala, M. R. (2019). Towards benefiting both cloud users and service providers through resource provisioning. *International Journal of Information Technologies and Systems Approach (IJITSA), 12*(1), 1–19. https://doi.org/10.4018/IJITSA.2019010101

Engoulou, R. G., Belläche, M., Pierre, S., & Quintero, A. (2014). VANET security surveys. *Computer Communications, 44*, 1–13. https://doi.org/10.1016/j.comcom.2014.02.020

Farouk, F., Alkady, Y., & Rizk, R. (2020). Efficient privacy-preserving scheme for location based services in VANET system. *IEEE Access, 8*, 60101–60116. https://doi.org/10.1109/ACCESS.2020.2982636

Feng, Q., He, D., Zeadally, S., & Liang, K. (2019). BPAS: Blockchain-assisted privacy-preserving authentication system for vehicular ad hoc networks. *IEEE Transactions on Industrial Informatics, 16*(6), 4146–4155. https://doi.org/10.1109/TII.2019.2948053

Forouzan, B. A., & Mukhopadhyay, D. (2015). *Cryptography and network security*. Mc Graw Hill Education (India) Private Limited.

Getzi, S., & Dinesh Peter, I. (2018). A combined forecast-based virtual machine migration in cloud data centers. *Computers & Electrical Engineering, 69*, 287–300. https://doi.org/10.1016/j.compeleceng.2018.01.012

Hartenstein, H., & Laberteaux, K. (2010). VANET: Vehicular applications and inter-networking technologies. In *Intelligent transportation systems* (Vol. 1). Wiley.

Hasrouny, H., Bassil, C., EllatifSamhat, A., & Laouiti, A. (2017). Security risk analysis of a trust model for secure group leader-based communication in VANET. In A. Laouiti, A. Qayyum, & M. Mohamad Saad (Eds.), *Vehicular Ad-Hoc networks for smart cities. Advances in intelligent systems and computing* (Vol. 548, pp. 71–83). Springer. https://doi.org/10.1007/978-981-10-3503-6_6

Kolaczeck, G., & Mizera-Pietraszko, J. (2018). Security framework for dynamic service-oriented IT systems. *Journal of Information and Telecommunication, 2*(4), 428–448. https://doi.org/10.1080/24751839.2018.1479926

Li, B., Liang, R., Zhu, D., Chen, W., & Lin, Q. (2020). Blockchain-based trust management model for location privacy preserving in VANET. *IEEE Transactions on Intelligent Transportation Systems, 22*(6), 3765–3775. https://doi.org/10.1109/TITS.2020.3035869

Li, K., Au, M. H., HeiHo, W., & Wang, Y. L. (2019). An efficient conditional privacy-preserving authentication scheme for vehicular ad hoc networks using online/offline certificateless aggregate signature. In *International Conference on Provable Security* (pp. 59–76). Springer.

Liu, J., Yu, Y., Zhao, Y., Jia, J., & Wang, S. (2018). An efficient privacy preserving batch authentication scheme with degradable function for VANETs. In *International Conference on Network and system Security* (pp. 288–303). Springer.

Mejri, M. N., Ben-Othman, J., & Hamdi, M. (2014). Survey on VANET security challenges and possible cryptographic solutions. *Vehicular Communications, 1*(2), 53–66. https://doi.org/10.1016/j.vehcom.2014.05.001

Paikrao, P., Mukherjee, A., Jain, D. K., Chatterjee, P., & Alnumay, W. (2021). Smart emotion recognition framework: A secured IOVT perspective. *IEEE Consumer Electronics Magazine*. https://doi.org/10.1109/MCE3062802

Raya, M., & Hubaux, J. P. (2007). Securing vehicular ad hoc networks. *Journal of Computer Security, 15*(1), 39–68. https://doi.org/10.3233/JCS-2007-15103

Shanmugapriyan, M. D. (2014). Secured and highly reliable data transfer in MANET using position-based opportunistic routing protocol. *International Journal of Innovations in Scientific and Engineering Research (IJISER), 1*(2), 69–74.
Singh, P. K., Gowatham, S. N., Tamilselvan, S., & Nandi, S. (2019). CPESP: Cooperative pseudonym exchange and scheme permutation to preserve location privacy in VANETs. *Vehicular Communications*, 20, 100183. https://doi.org/10.1016/j.vehcom.2019.100183

Swathynathini, N., & Jeeva, K. (2014). Secure cluster formation and certificate revocation for adversary nodes in the MANET's. *International Journal of Innovations in Scientific and Engineering Research (IJISER)*, 1(3), 178–183.

TaNuja, K., Sushma, T. M., Bharathi, M., & Arun, K. H. (2015). A survey on VANET technologies, 121(18), 1–9.

Vörös, P., Csubák, D., Hudoba, P., & Kiss, A. (2020). Securing personal data in public cloud. *Journal of Information and Telecommunication*, 4(1), 51–66. https://doi.org/10.1080/24751839.2019.1686684

Wei, Z., Li, J., Wang, X., & Gao, C.-Z. (2019). A lightweight privacy-preserving protocol for vanets based on secure outsourcing computing. *IEEE Access*, 7, 62785–62793. https://doi.org/10.1109/ACCESS.2019.2915794

Zheng, B., Sayin, M. O., Lin, C.-W., Shiraishi, S., & Zhu, Q. (2017). Timing and security analysis of VANET-based intelligent transportation systems. In *IEEE/ACM International Conference on Computer-Aided Design (ICCAD)* (pp. 984–991).

Zhou, Y., Long, X., Chen, L., & Yang, Z. (2019). Conditional privacy-preserving authentication and key agreement scheme for roaming services in VANETs. *Journal of Information Security and Applications*, 47, 295–301. https://doi.org/10.1016/j.jisa.2019.05.018