EURASIP Journal on Wireless Communications and Networking

RESEARCH Open Access

Robust cryptographic scheme for reliable data communication in VANET (RCSRC) using clustering approach

Wajid Ali[1], Shalini Z. Ninoria[1], Gulista Khan[1] and Kamal Kumar Gola[2*]

*Correspondence:
kkgolaa1503@gmail.com

[1] Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India
[2] COER University, Roorkee, Uttarakhand, India

Abstract

In contemporary times, as accident rates continue to rise, there is a growing interest in vehicular ad hoc networks (VANETs) as a means to reduce accidents and vehicle damage, as well as enhance public safety. VANETs facilitate the transmission of messages within predefined areas to ensure system safety and efficiency. However, ensuring message authenticity in such a dynamic environment presents a significant challenge, with previous research focusing less on security aspects. Some previous protocols send plain message, which leads to the compromise of the message confidentiality. Although few algorithms work on security, they involve the communication to the trusted authority, which lead to increased latency. Thus, in this paper we propose a robust cryptographic scheme for reliable data communication in VANET which minimizes the involvement of trusted authority and uses communication ID of vehicle for communication in place of real entities. Security analysis of the proposed scheme is showing the sturdiness of the proposed protocol again various types of safety spasms. The evaluation of its performance includes assessing communication cost and time, revealing the proposed algorithm's efficiency compared to others.

Keywords: Trust model, Authentication, Reliability, Security

1 Introduction

The increasing popularity of smart mobility aligns with the rise of smart cities, characterized by features such as monitoring of traffic flow and mobbing management. The rise in traffic mobbing incidents and inefficient wireless communication systems for traffic management has spurred the development of intelligent transportation systems (ITS) [1]. Recent advancements in communication and information, particularly mobile communications, have transformed modern lifestyles, enabling data exchange anytime and anywhere. Cellular networks like 3G and 4G facilitate data exchange in vehicles, and vehicular ad hoc networks (VANETs) can effectively achieve intelligent transportation system (ITS) goals such as enhancing road safety, controlling traffic congestion, and optimizing infrastructure utilization [2].

VANETs establish an intelligent environment for vehicle-to-vehicle communications, integral to ITS, offering a large number of secure and non-secure requests, including

automated toll collection, vehicle safety, enhanced navigation, traffic management, location-based services, and entertainment applications. Unlike traditional networks, VANET relies on smart vehicles for network functionality, with each moving vehicle acting as a node and On Board Unit (OBU) to establish a mobile network. VANET communication is done in two ways. Vehicle-to-infrastructure communication and direct data transfer between vehicle-to-vehicle communication.

Dynamic connectivity and self-organizing are inherent properties of VANET nodes [3]. However, frequent topology changes due to vehicles' high mobility reduce network lifespan and increase routing overhead. Clustering is a common solution wherein vehicles are organized based on certain rules, criteria, or common aspects. Data transmission (DT) protocols are developed to ensure privacy and truthfulness safety of data transmitted between road side units (RSUs) and vehicles, albeit facing computational cost challenges due to high-speed traffic and short communication range.

Privacy and security [4] in VANETs have gained significant attention post vehicle safety communication (VSC). Pseudonym certificates are introduced to vehicles to secure communications within the network, covering both safety and non-safety services. Despite advancements, challenges persist in VANET management and deployment, especially in ensuring secure communication. Artificial intelligence (AI) techniques are increasingly employed to enhance VANET security by leveraging experience to make informed decisions in dynamic environments. However, VANET's high mobility and susceptibility to attacks, including Sybil, Black hole, and wormhole attacks, present ongoing challenges for secure communication [5–10].

Several flaws exist in current research efforts within VANET, as outlined below:

- Existing research methods fail to detect certain malevolent activities or prevent them effectively.
- Key management centers (KMC) are central to VANET communication in current research works, rendering the entire scheme ineffective if the KMC is compromised.
- Clustering-based systems often choose cluster heads (CH) based on location and velocity, which may not be optimal due to rapid changes in the chosen vehicle's location relative to other vehicles in the network.
- Some top-notch works rely on one or two metrics for cluster formation, which may not be the most optimal choice.

The proposed research aims to tackle several challenges in VANET security [11–15]

Several authentication and privacy preservation methods exist for VANETs, often involving plaintext message transmission alongside digital signatures, which can compromise confidentiality. Further authentication is crucial for defending against attackers, ensuring the privacy of non-safety-related messages is equally important. Therefore, a critical demand for an scheme to authenticate nodes VANETs that safeguards vehicle privacy while ensuring the privacy, truthfulness, and availability of exchanged messages.

1.1 Problem statement

Recent studies have revealed shortcomings in existing authentication schemes for VANET.

i. Many existing schemes concentrate on authenticating vehicles using identifications recognized during registering. However, once authenticated, messages are often transferred openly in plaintext [16–22]. This vulnerability leaves private communications susceptible to compromise by malicious entities. Therefore, there is an urgent requirement to develop a scheme that not only facilitates mutual authentication among parties but also establishes secure associations capable of preserving the confidentiality of exchanged messages.
ii. In vehicular ad hoc networks, vehicles need to communicate while in motion, necessitating low latency in signaling message exchanges. This can be completed by making use of lightweight cryptographic methods and minimizing message size and number.
iii. Most recent authentication schemes for VANETs require continuous connection with a trusted authority, which delays authentication and needs to be minimized for faster signaling.
iv. Recent privacy-preserving schemes in VANETs rely on digital signatures, involving steps like generating pseudo-IDs, creating secret keys, and verifying messages with computationally intensive bilinear pairing operations. There is a need to explore lightweight cryptographic techniques that offer efficient privacy protection without the computational overhead of numerical signs and pairings.

1.2 Contribution of the work

Considering the identified areas for improvement, we introduce an innovative authentication scheme tailored for VANETs. Our scheme aims to authenticate communications between RSUs and on board units (OBUs), while safeguarding vehicle privacy. The key features of our proposed scheme differ from existing works in the following aspects:

i. Our scheme offers two-way authentication and secrecy to vehicles. Only the trusted authority (TA) possesses the actual vehicle ID, while RSUs identify vehicles using communication IDs provided by the agent of TA.
ii. In contrast to other schemes relying on TA, we proposed a cluster-based model in which RSU will act as the cluster head and work of allocating credentials like symmetric and group keys, delegated to ATA and RSUs. RSUs distribute Cluster keys to vehicles, allowing them to communicate and authenticate others within their cluster. Cluster keys are updated each time a new vehicle joins.
iii. Our scheme employs the use of lightweight cryptographic practices to attain its goals with minimal signaling dormancy. Vehicles in the VANET can request new communication ID once their current validity period expires.

2 Related work

This section elaborated the related work done in the context of authenticate and securing the communication between the vehicle and vehicle to infrastructure. Reliability analysis is also done in this chapter.

2.1 Cryptography-based Protocols

Wu et al. in [23] introduce the public key cryptography which does not use certificates. In this scheme instead of certificates, semi-private key generated by the key generation center in coordination with the user.

Liu et al. in [24] proposed the authentication scheme that was based in the Lattice. However, this scheme suffers from high communication cost along with lack of energy efficiency.

Canhuang Dai et al. [25] introduced an indirect mutuality security approach where each OBU is assigned a scalar reputation to evaluate its threat level within VANET. They utilized consensus techniques and encryption procedures to safeguard information from tampering, employing blockchain techniques for recording other OBUs' activities. Additionally, they developed a reinforcement learning (RL) technique for OBUs to select reliable relays or choose should they follow source OBUs' requests. Employing a hot boot mechanism enhanced learning speed, leveraging prior knowledge. The results comes up with improved packet delivery ratio (PDR), status, and usage of OBU through action selection methodology with built-in prior knowledge.

Sowmya Kudva et al. [26] proposed to randomize the selection of honest miners for block production in block chain-based VANET applications by using the proof of driving (POD) method. They also deployed a riddling method based on vehicular nodes service standard score to identify and remove malicious nodes, enhancing consensus adaptability and honest miner selection. This approach addressed fairness and efficiency concerns related to proof of work (POW) and proof of stake (POS). Achieving lower agreement overheads while enhancing quality and scalability.

Parul Tyagi and Deepak Dembla [27] introduced a secured AODV routing technique. Elliptic curve cryptography (ECC) is utilized to detect malevolent nodes, prevent black hole attacks, and ensure secure Data Transfer (DT) in VANETs. Although it enhanced road safety by providing timely and authenticated traffic-related messages, it lacked provisions for attack confrontation and malicious node removal.

J. Jenefa et al. [28] proposed a proxy vehicle-based message authentication scheme (ID-MAP) to reduce road side unit (RSU) overhead by validating multiple messages simultaneously. However, it incurred high computational costs for signature generation and lacked privacy preservation guarantees, making it vulnerable to privacy-based attacks.

Ayan Roy et al. [29] proposed a dispersed incentive-based system with a protected event detection design, employing Byzantine fault-tolerant Paxos technique and game theory. Unlike previous methods, this model verified information accuracy even in the presence of malicious vehicles, ensuring system feasibility and efficacy under various use-case scenarios. However, it faced challenges in managing communication between more than one nodes.

Jitendra Bhatia et al. [30] suggested a strategy combining Software Defined Networking (SDN) technology with network coding and multi-generation mixing (MGM) functionalities are employed to improve data transfer reliability and security in vehicular networks. Their protocol demonstrated efficient performance and resilience against various attacks compared to traditional network coding protocols.

2.2 Batch verification-based protocols

Various algorithms [31–34] proposed the authentication schemes which were based on the batch verification codes. These codes do not require certificates management. However, these algorithms are not suitable for privacy and data security. Few certificate-based batch verification techniques are produced [32] but it again includes burden of verifying the certificates. To avoid this burden, few ID-based techniques were proposed as [34]. This technique should verify multiple IDs at a time which introduces the reply attack. Ciu et al. in [12] improved this work to some extent by improving the vehicle privacy by introducing the 2 ID-based privacy authentication without bilinear pairings.

2.3 Group communication-based protocols

Various schemes have been proposed based on group communication [35–40]. Yang et.al in [38] introduces Anonymous credential and group signature-based technique, but it does not explain proof of knowledge and it claimed to address the unforgeability and anonymity. Algorithm [16] introduces by Houmer et al. employed ECC (elliptic curve cryptography) it improved the key agreement protocol and address integrity and confidentiality issue in communication. Tan et al. in [6] introduces secure authentication by the use of ECC and it does not use certificates. It deals with the authentication and reply attacks.

2.4 Trust management protocols

Existing trust schemes are categorized in two categories mainly object oriented and information oriented. Object oriented trust scheme explains that trust of any node is calculated based on the behavior of the entity. It is based on the historical data available regarding the entity. In [25] Qin Li et.al mentioned a scheme based on reputation announcement. TA evaluates the reputation of any vehicle which is calculated based on the data provided by pother vehicles. Likewise, reliability of any message is ensured by considering the message is received by the node having higher reputation.

In reference [13], the authors introduced a method for calculating object trust in a VANET by using recommendation from other objects. The trustworthiness of information does not always correlate with the trustworthiness of the object providing it. Our approach ensures that the trust evaluation process is independent of the reputation of the information source or sender, thus preventing errors when assessing fraudulent information from high-reputation entities. Additionally, our method addresses the cold start problem by not immediately classifying information from newly added entities as unreliable due to their low reputation.

Saneeha Ahmed et al.[27] discussed about a trust framework for VANET that includes a process for evaluating entity trust [27]. They employed the resemblance between the trustor and the trustee to assess the trustee's commendation faith. The overall trust value of the trustee is then determined by integrating the subjective sum of established commendations with the trustor's direct trust.

A method for creating a trust presenter for a reliable parking application was presented in [4], relying on physical encounters between vehicles. The practicality of

approaches such as [27] and [4] depends on the frequency of interactions between the trustor and the trustee.

Current secure authentication algorithms in VANETs face several challenges. They often struggle with scalability as the count of vehicles rises, leading to high computational overhead and latency issues. Many algorithms are vulnerable to Sybil attacks and insider threats, and managing cryptographic keys in a dynamic environment is complex. Privacy concerns also arise as vehicles need to disclose sensitive information. Additionally, existing methods may not adapt well to network changes and can suffer from interoperability issues among different systems and standards. Addressing these flaws requires advancements in robustness, efficiency, and adaptability. For the same we have focused on Reliability, Authentication and Trustiness of nodes in the proposed work.

i. Our scheme offers two-way authentication and privacy to vehicles. Only the trusted authority (TA) possesses the actual vehicle ID, while RSUs identify vehicles using communication IDs provided by the agent of TA.
ii. In contrast to other schemes relying on TA, we proposed a cluster-based model in which RSU will act as the cluster head and work of allocating credentials like symmetric and group keys, delegated to ATA and RSUs. RSUs distribute Cluster keys to vehicles, allowing them to communicate and authenticate others within their Cluster. Cluster keys are updated each time a new vehicle joins.
iii. Our scheme employs the use of lightweight cryptographic practices to attain its goals with minimal signaling dormancy. Vehicles in the VANET can request new communication ID once their current validity period expires.
iv. All the communication among vehicles done through the RSU so our scheme is considered as the reliable scheme.

Table 1 gives the comparison of various authentication schemes with the proposed schemes in terms of various security requirements and computation cost.

Table 1 Comparison of various Authentication schemes

Requirement	Preserve in following algorithms	Proposed Algorithm
Privacy	[15, 20–22, 29–32, 35, 47–50]	✓
Non-repudiation	[20–22, 31, 32, 35, 41, 49]	✓
Message authentication	[15, 20–22, 29–32, 35, 47–50]	✓
Sybil attack	[20–22, 31, 32, 49]	✓
Modification attack	[20–22, 31, 32, 35, 49, 50–52]	✓
DoS	[20–22, 31, 32, 35, 50]	✓
Impersonation attack	[15, 20–22, 29–32, 35, 47–50]	✓
Replay attack	[20–22, 29–32, 35, 36, 49, 50]	✓
Location tracking	[21, 22, 32, 49, 50]	✓
Low communication	[20–22, 31, 32, 35, 48, 49]	✓
Low computational	[20, 21, 29, 41, 43, 47–49]	✓
Scalability	[20, 21, 31, 32, 35, 49]	✓

All these requirements preserved in the proposed algorithm. The proposed scheme very well provides the security using low computation cost and communication cost. Detailed analysis is presented in Sect. 7.

3 Proposed methodology

In the territory of intelligent transportation systems (ITS), VANET are emerging as a significant investigation area due to their impending to significant improvement in road protection and transportation management. Equipped with sophisticated communication tools, vehicles require robust power supplies, onboard computing devices, and data storage capabilities. However, this sophistication brings forth serious challenges in terms of concealment and safety within VANET. This information misuse could lead to accidents and even loss of hominid lives, underscoring the critical need for vehicle authentication.

Figure 1 shows the proposed architecture for RCSRC. This figure shows there are a one trusted authority. All vehicles registered with this TA. Agent of TA is also shown which is distributed area wise. TA forwards data of registered vehicles to the agent of TA, ATA is responsible to generate the shared keys for the Vehicles and assign them communication IDs. ATA maintains a mapping table containing communication IDs and Shared Keys of all the vehicles. Later in ATA shares this table to the RSUs. RSUs considered as the semi-secure so all the communication at the RSU level and the OBU level is done through the communication ID. All RSU Create Cluster and act as the cluster head. Once a Vehicle passes from one RSU it will send vehicles data to the next RSU in the way so that Next RSU will share Cluster key to Vehicles immediately and cluster formation process could be minimize.

3.1 System model

In vehicular ad hoc networks, all automobiles are equipped with the OBU, due to which each vehicle can broadcast and interconnect the messages for vehicle-to-vehicle (V2V)

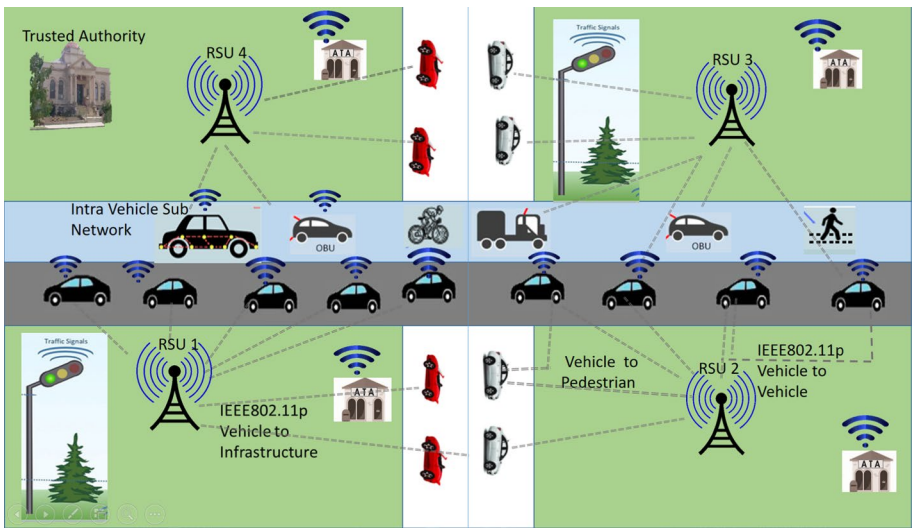

Fig. 1 Proposed architecture of RCSRC

and vehicle-to-infrastructure communication (V2I). The trusted authority (TA) through agent of TA (ATA) assigns a communication ID (CVi) all vehicles. Trusted authority is the highest trusted entity in the VANET. Its major work is to register various entities like RSUs, ATAs and vehicles. Agent of TA (ATA) is also the trusted entities, which are distributed area wise in a city; its major work is to map the communication ID to the vehicle's real ID. It maintains a table containing real IDs(Vi) and communication IDs (CVi) of the vehicles. For example, Vehicle 1 is assigned CV_1 as the communication ID, Vehicle 2 is assigned as $CV_2$and CV_3, CV_4, *and* $CV5$ and so on. All communication through vehicles will be now done using only communication ID. This communication ID could be changed on the request to the ATA. Figure 2 depicts the system model of proposed algorithm. Trusted authority has multiple ATAs area wise. One ATA will be serving for multiple RSUs. RSUs works as the cluster head of the cluster made up of vehicles for the communication. All the communication is done using the RSU as cluster head by this approach proposed algorithm turns out to be more reliable. For more understanding of the work, two tables are presented. Table 2 defines the abbreviations using in this paper. Table 3 indicates the definition of the symbols used in this paper.

3.2 VANET communication

In VANET infrastructure, major objects for communication are vehicles and RSU. Among these, automobiles are always on move across various roads and in different directions. In this scenario a safety mechanism is needed for the secure and reliable communication among the vehicles and the vehicle to RSU and ATA. Before the communication, authentication of the generated messages is also very important. So for this purpose secure cluster communication is proposed here.

Fig. 2 System model of proposed algorithm

Table 2 Details of abbreviations used in paper

Abbreviation	Name
VANET	Vehicular ad hoc networks
RCSRC	Robust cryptographic scheme for reliable data communication in VANET
TA	Trusted authority
ATA	Agent of TA
ITS	Intelligent transportation systems
OBU	On board unit
V2V	Vehicle to vehicle
DT	Data transmission
RSUs	Road side units
VSC	Vehicle safety communication
AI	Artificial intelligence
KMC	Key management centers
CH	Cluster heads
RL	Reinforcement learning
PDR	Packet delivery ratio
POD	Proof of driving
POW	Proof of work
PoS	Proof of stake
ECC	Elliptic curve cryptography
SDN	Software-defined networking
MGM	Multi-generation mixing
CIA	Confidentiality, integrity and availability
V2I	Vehicle to infrastructure

All the vehicles are allowed to do the communication with in the cluster. A cluster is formed from a group of vehicles. It is based on the geographical location. RSU is designated as the cluster head. RSU broadcast a message for cluster formation (RSUi as the ID of ith RSU). All the vehicles node who receives this message will join this cluster. Then, a cluster key is broadcasted to the cluster members for the secure communication. [41] [42]

3.3 Security requirements

There are few basic security requirements to be considered while designing the secure scheme for VANET are as follows:

- Message authentication

All the messages are communicated among the legitimate users only. The vehicles having the cluster key will be able to communication to all vehicles and RSU which are again the part of the cluster.

- Confidentiality, authentication and integrity

Another requirement of the secure communication is the integrity, confidentiality and authentication is preserved. In the proposed scheme, all the messages are encrypted and properly decrypt after reception to ensure the confidentiality, Hash

Table 3 Details of symbols used in paper

Symbol	Definition
CVi	Communication ID
Vi	Real IDs
G_{TA}*	Creates a group
RsK	Random number
Mas_V_L	Master list
V_L	Vehicle list
skV	Secret key
certVi	Certificate ID
$C_{sk}y$	Cluster secret key
H	Hash
m	Denotes the packets modified
d	Denotes the no. of dropped packets
f	Packets without modification
DT_y	Denotes the direct trust calculated for node y
IT_y	Denotes the node y's indirect trust
n	Denotes the recommendations from the neighbors
L_x	Calculate the distance
Pc	Denotes the position closeness
D	Denotes the distance between two nodes
2r	Denotes the perimeter of communication area
T_0	Represents the threshold
CT	Combined trust
IT	Indirect trust

function of used during the communication to ensure the integrity. To ensure authentication, each vehicle is authenticated with the communication ID provided by the ATA.

- Trustiness of nodes

Nodes used in the communication must be having the trust to be the legitimate nodes. Trustiness of the nodes is checked randomly using the trust management scheme in the proposed scheme.

- Privacy preservation

Node's identities must be protected during communication. For this proposed scheme is using communication IDs of the vehicles instead of the real IDs. All V2V and V2I communication is done using the mapped communication IDs of the vehicle.

- Vehicle traceability

Although privacy is necessary, in case of any vehicle that is sending any malicious message, this vehicle must be traceable so that some legal action could be taken against it. In our approach ATA, agent of TA is able to trace the vehicle through the table maintain aby ATA about mapping id Communicated IDs and the Real IDs.

- Non-repudiation

While communication non-repudiation could be managed by adding an acknowledgement number along with the message sent by the vehicles. So, later on it must not deny it has not sent the message.

- Key freshness

Key freshness must be ensured for the efficient communication. In the proposed approach, cluster key is changed every time the new vehicle joined the group.

- Resistance from attacks

Proposed communication model must be resisted from both active and passive attacks.

- Unlinkability

If any attacker receives any message, then it must be any scheme to reach the originator of the message.

4 Proposed algorithm

The proposed communication technique is not using the real IDs of the vehicles for communication; instead, it uses the communication IDs to have the secure communication and hide the actual authentication Identities of the vehicles from the outside world.

4.1 Proposed architecture for RCSRC

In VANET, all the vehicles are assumed to be equipped with facilities like enough memory, GPS, cameras, sensors for parking, capability of communication through radio interface.

Along with it, few more assumptions are done:

- Trusted authority (TA) is assumed fully trusted. All the vehicles are registered with this TA.
- ATA (agent of TA) is located at various places in city. It may be one or more than one with in a City. These agents are also considered to be trusted and their prime work is to allocate the communication IDs to the Vehicles correspond to their Real IDs.
- RSU (road side units) are considered as the semi-rusted. It is assumed that communication between TA and road side units has a trustworthy and safe communication. Communication among RSU and Vehicles is not done using Real IDs it is done using communication IDs being RSU as the semi-trusted.
- All vehicles are fortified with OBE, which are capable of having enough memory, GPS, Cameras, Sensors for parking, capability of Communication through Radio Interface.
- In case of any need vehicle can ask for a fresh communication ID from ATA by Registration update. Fresh ID will be allocated by ATA and same will be updated to the master database of the TA.
- RSU is considered to have the enough memory to save the communication IDS of the vehicles in the area.

4.2 Initialization

Initialization of the proposed protocol is performed in the following phases.

5 TA Initialization

At the very first time TA has been established. It creates a Group (G_{TA}*) containing large number of prime numbers of order q. q will be any large number. TA selects a random number k from the group G_{TA}*such that k belongs to G_{TA}*as its shared secret key.

6 Initialization of ATA

ATA are connected to the TA via a secured channel. Its work is to assign communication IDs to the vehicles.

7 Initialization of RSU

All the RSUs are registered with the TA. RSU is assigned an ID $RSU_{id.}$ by TA. Communication among TA and RSU is considered as secure. TA will select a random number *Rsk* as the RSU secret key such that *Rsk* belong to G_{TA}*. Along with key RSU key a certificate (Cert_{rsu}) is also shared to all the RSU. RSU is provided with ($RSU_{id.||}\text{Cert}_{\text{rsu}||}$ *Rsk*). ATA provides the master list (Mas_V_L) of the vehicles. Vehicles enlisted in this master list are registered for the services from VANET along with this another vehicle list (V_L) that is provided by the ATA which are in the area but not registered for VANET services. These two lists are shared by ATAs to the RSUs.

8 Initialization of OBU in vehicles

ATA provides shared secret key *skV* and communication ID to the vehicles. *skV* is generated from a pool of secret keys sent to ATA via TA from group G_{TA}*.A table is maintained at the ATA level like (V_1 assigned with skv_1 and CV_1, V_2 assigned with skv_2 and CV_2 and so on). It is shared using the certificate sent to OBU containing ($certVi$ || $CV_i||skV_i$)

9 Cluster formation

RSU is responsible to create the cluster. Process is as follows:

1. RSU being the cluster head broadcast its cluster formation message containing its ID and public key of RSU (RSU_{pu}).
2. All the vehicles in its area joined the group by sending its communication ID (CV_i) along with certificate ($certVi$) which is encrypted by RSU public key (RSU_{pu}).
3. RSU on receiving the request will share Cluster secret key ($C_{sk}y$) encrypted by Vehicles secret keys and broadcast.
4. All the vehicle upon receiving it decrypt the cluster key using their secret key by identifying using their communication ID.
5. Cluster key (C_{sky}) is refreshed when a new member enters to the cluster region and broadcast again to all the members.

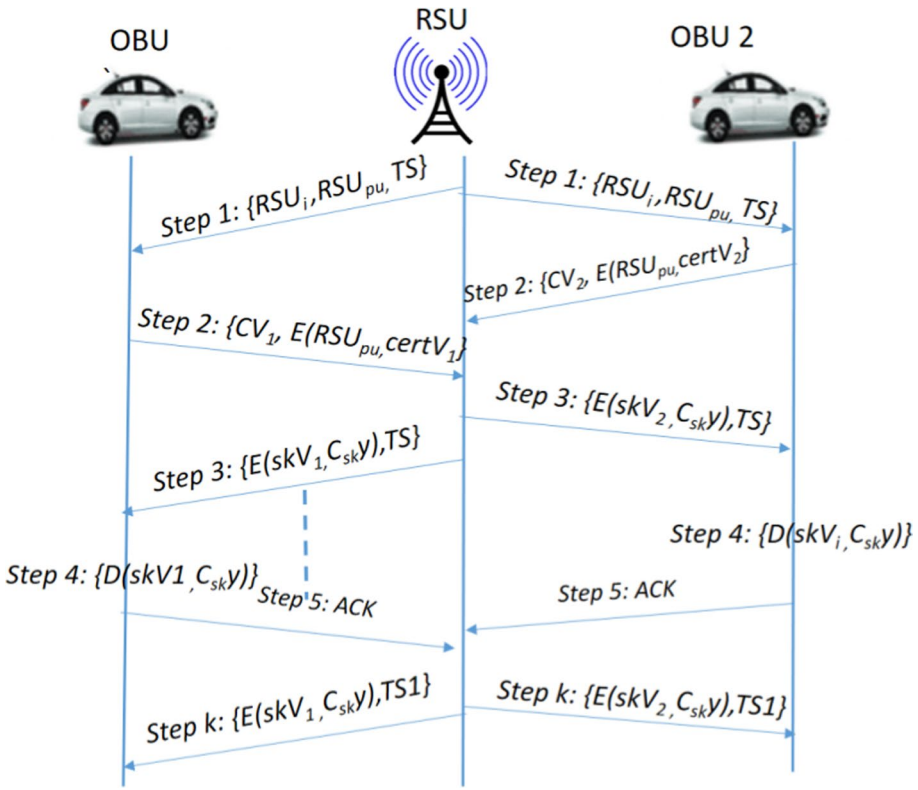

Fig. 3 Cluster formation process communication

Process 2 is done only one time when the journey starts after that RSU communicate and share the vehicles data on the route to their nearby RSU till the journey end assuming all the RSU are available on the route are in working condition. Figure 3 shows the process of cluster formation.

10 Proposed scheme for authentication

Vehicle will start the communication by receiving the cluster key from the RSU. Two types of communication are done in this scenario: V2V and V2I.

10.1 Vehicle-to-infrastructure authentication and communication

When a vehicle enters to first RSU on the route, it receives the cluster formation message sent via the RSU containing its ID and certificate (it contains public key of RSU (RSU_{pu}) and a shared key). Vehicle checks this message authenticity by using shared key. After the confirmation vehicle will share its certificate to RSU for joining the cluster. Vehicle certificate contains vehicle communication ID, time stamp and its public key. Upon receiving the reply message, RSU checks the communication ID of the vehicles and match it from the master list of vehicles available at ATA and fetch its shared key from the master list.

RSU generates a cluster key which will be used for the communication. After that, RSU encrypts this cluster key with all the vehicles public key and shared key and broadcasts

it. The vehicle upon receiving the broadcasting message will decrypt the part of the message intended to it and receive the cluster key.

10.1.1 Communication among V2I

Vehicle can communicate with TA, ATA and RSU.

1. Vehicle and TA communication is done at one time only at the time of vehicle registration. Registration is done using the vehicle registration number.
2. ATA is connected to the TA via a secured channel. Its work is to assign communication IDs to the vehicles. After the registration vehicle will receive its certificate containing its secret key and communication ID, which will be used for further communication.
3. Vehicle-to-RSU communication is done frequently. Vehicle communication with RSU for joining the cluster and some time to report the false information about any other node.

10.2 Vehicle-to-vehicle authentication and communication

V2V communication is done through RSU to ensure the reliability of the messages transfer. Vehicle can communicate with other vehicles by using the cluster key from RSU as cluster head. The type of messages they can share could be security message, universal message and communication related message. Hash (H_1) will be also created of message using the Cluster key and its Vehicle ID ($H_1 = H(Message||CV_i)$). Now whenever one vehicle wants to send this data to another vehicle it sends Message by encrypting the message with Cluster key (C_{sky}). Framekey is generated as $framekey = H(CV_i||CV_{i\_}key)$ Sender vehicle prepare message $M = (C_{sky}((Message)||H_1||CV_i||Ts||framekey||GP)$ and share it to RSU. All the vehicle-to-vehicle communication will be done using RSU to ensure the reliability. Here T_s is the time stamp and GP denotes the geographical position if the node, *Framekey* is verified at the RSU only to check the non-repudiation thus rest of the message will be unicast to intended Vehicle. After the recipient of the message $M = (C_{sky}((Message)||H_1||CV_i||Ts||framekey||GP)$.

Figure 4 explains the vehicle-to-vehicle communication transactions. During transmission, vehicle performs the following steps*:*

1. Decrypt this message by decrypting with the cluster-shared key (C_{sky}).
2. Check the freshness of the message by checking the Time stamp.
3. Check the GP of the vehicle if it belongs to same geographical location where it is located.
4. Calculate Hash of $H_1' = H(Message||CV_i)$.
5. Match whether $H_1 = H_1'$.
6. If yes, then it receives the message and manage to send the ACK to the Vehicle CV_i through RSU.

If any of the steps from above 2-4 steps failed, then receiving vehicle informed it to RSU. RSU takes action to trace the CV ID of the vehicle and inform about the situation to the ATA. ATA will trace real ID of vehicle to take further action.

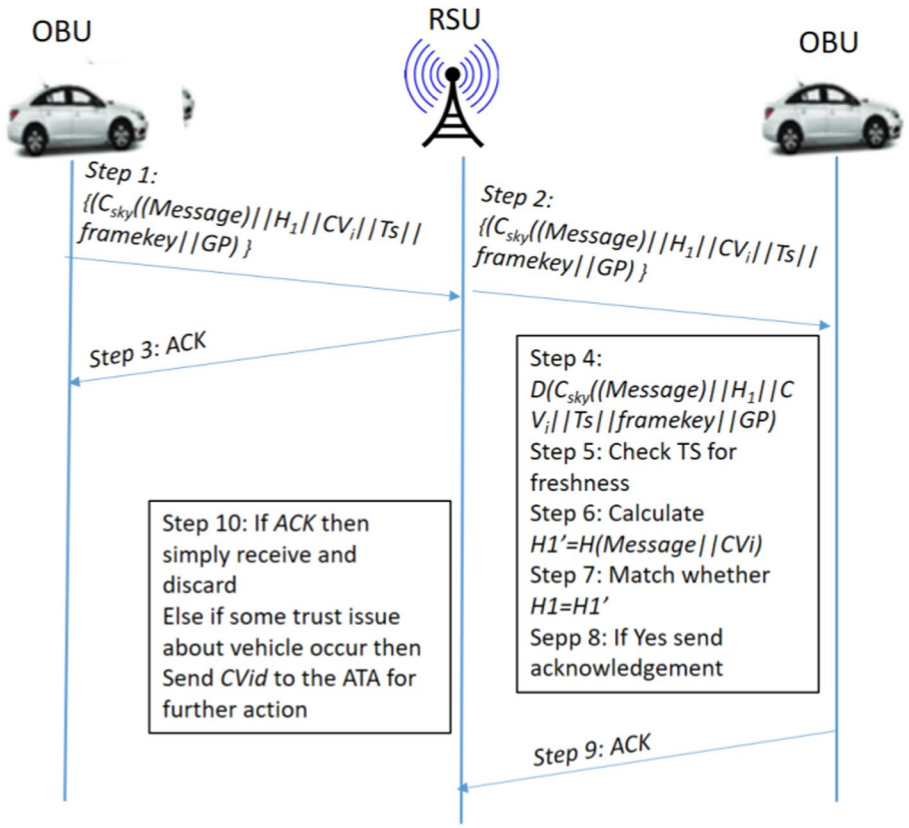

Fig. 4 Vehicle-to-vehicle communication

7. If Step 5 failed to match, then receiving vehicle discards the message and sends *ACK* about this failure of message to CV_i.

11 Trust calculation scheme

A trust management scheme for VANET (vehicular ad hoc networks) nodes is designed to assess and ensure the reliability of communications within the network. This trust management approach enhances the reliability and security of VANETs by ensuring that only trustworthy nodes participate in the network and share accurate information. By taking care of the communication cost in consideration, the proposed scheme is using only two values to assess the combined trust that are direct trust and indirect trust.

11.1 Direct trust

It is calculated by the below equation in which m denotes the packets modified, d denotes the no. of dropped packets, packets that are forwarded without modification are denoted by f, DT_y denotes the direct trust calculated for node y.

$$DTy = \frac{m+d}{m+d+f}$$

Flag values for the faith have been set based on the calculated trust. These Boolean flag values are decided after the comparison of trust values with threshold values. If the DT_y is greater than the threshold value, then T_y is set to 1; otherwise, it will be set to 0.

If $DTy > \partial$, then $\mathrm{Ty} = 1$ otherwise $\mathrm{T_y} = 0$.

11.2 Indirect trust

After the direct trust, indirect trust is calculated for node Y. Indirect trust is calculated by combining the trust values received from all the observer nodes.

$$ITy = \frac{\sum_{i=1}^{n} T(yi)}{n}$$

where $\mathrm{IT_y}$ denotes the node y's indirect trust. n denotes the recommendations from the neighbors (observer nodes).

$ITy > \mu$, then $\mathrm{T}(\Sigma \mathrm{y_i}) = 1$ otherwise $\mathrm{T}(\Sigma \mathrm{y_i}) = 0$.

When nodes join the network trust of nodes are calculated by Direct and Indirect Trust calculation. Trust depends on the position closeness and the distance between the observe and observer node, for example, if we wish to take the trust of node V_i, then all other vehicle nodes could be the observer nodes based on their distance and position closeness. Observer nodes could be selected based on following steps:

1. Then Calculate the distance (L_x) from the observed node to the observer node using Euclidean Distance formula.
2. Calculate $\mathrm{P_c}$ (position closeness) as $Pc = 1 - (\frac{D}{2r})$. Here $\mathrm{P_c}$ denotes the position Closeness, D denotes the distance between x and y, 2r denotes the perimeter of communication area.
3. Calculate $N0 = \beta 1Lx + \beta 2Pc, where \beta 1 + \beta 2 = 1$.
4. If ($\mathrm{N_0} < \mathrm{T_0}$) then {$\mathrm{T_0}$ represents the threshold}.
5. Node x consider as the observer node.
6. Else.
7. Node x will not be considered as observer node.
8. End.

11.3 Combined trust

Combined trust of node y(CT_y) is calculated by adding direct DT_y and indirect trust IT_y.

$$\mathrm{CT_y} = \mathrm{DT_y} + \mathrm{IT_y}$$

RSU received the trust value of nodes from direct trust value form vehicle itself and Indirect trust values from neighboring values. Combined trust is calculated by the RSU which leads to knowing about the trustiness of the vehicle. If node was found to be trust node, then only it may join the cluster.

12 Analysis with respect to security

Here, we examine how resilient the suggested method is to potential security threats in communication among vehicles.

- Message authentication and integrity:

After the reception of broadcasted message from RSU for the formation of cluster, a vehicle shares its ID and certificate encrypted by RSU public key. The RSU on decrypting the request message check the communication ID from the list at ATA level authenticate the user and share Cluster key to it. The users who obtain the passwords from TA and RSU can receive the cluster keys from the cluster head. After that any user can authenticate itself and check the integrity of the messages.

- Conditional privacy conservation:

In the first phase, OBU registers itself to the TA. TA then registers the vehicle, issues a communication ID, and maintains a mapping table with real IDS of vehicle to the communication IDs and assigned secret keys. TA hides the real IDS of the vehicle from other vehicles and Infrastructures. TA shares the mapping table to the ATA for further dissemination to the RSUs. However, whenever OBU wants to change the Communications ID it will send the request message encrypted by its secret key to the ATA for changing it. This characteristic offers conditional privacy to the proposed scheme.

- Confidentiality, integrity and availability (CIA):

RCSRC is having integrity, privacy and availability. All the communication among vehicle-to-vehicle and vehicle-to-infrastructure is encrypted by the cluster key as well as the secret keys to make the communication confidential.

During communication, the sent message is also using the hashing technique. The data message involves computing the hash of the message using its secret key and transmitting it to the receiving device. At the receiving side, hash is again created and both the hashes matches. If *H1* matches to *H1'* inly, then message will be accepted; otherwise, message will be discarded.

In case of any malicious node present in the network, it will be tracked by the RSU and information will be shared to the TA for any legal action.

- Non-repudiation:

The cluster key encrypts data and the secret key of the automobile along with message times stamp is shared. Thus, vehicle sent this message could not deny with the sent message; thus, non-repudiation could not happen.

- Key freshness:

Cluster keys are refreshed after the new vehicle joined the cluster and whenever old vehicle leaves the cluster so in this way key is refreshed every time.

- Modification attack:

Modification attack is omitted through the hashing used in this technique.

- Replay Attack:

Replay attack is omitted by using the times stamp used during the message communication. Source vehicle generates a timestamp for the particular message and send it along with the message. On receiver side messages, freshness is considered based on the value of the timestamp.

- Resistance to Impersonation attack:

During vehicle-to-vehicle communication, the cluster key encodes the message, which is available with the authenticated vehicles only. After that, attacker must have the communicating ID of the authenticated vehicle and the secret key.

During vehicle-to-infrastructure communication, attacker must have the cluster key, communication ID and secret key to perform the Impersonation attack. It is not available to the attacker.

13 Simulation environment

To implement proposed algorithm in MATLAB, a system with intel core i5, CPU 2.40 GHz and 2.42 GHZ dual-core processors, 16 GB memory is used. To estimate the execution time of various schemes, Table 4 shows the execution time of various key cryptographic operations [43]:

14 Result and discussion

This section elaborates the comparison of our proposed scheme with various schemes mentioned in [16–22]. To calculate the implementation time of various algorithm, some cryptographic operation execution time and overhead are calculated. Elliptic curve cryptography is lightweight cryptographic technique. Cryptographic algorithms are taking the larger time than other XOR operations. So time calculation for performing the XOR operation is ignored in proposed algorithm.

14.1 Computation overhead at the vehicle during message exchange

Computation overhead is computed by calculating the execution time. These timings provide insights into the computational costs associated with different cryptographic operations used in the schemes.

Table 5 represents the time of message communication between OBUs and the RSU using encryption. Without encryption, execution time in transferring the data exchange between vehicles for the proposed scheme will be 0.114 ms. Figure 5 depicts the execution time for data transfer at vehicle without encryption.

Table 4 Execution time (ms) of various operations in cryptography

Operations	Execution Time
Scalar multiplication	Approximately 0.084 ms
Scalar multiplication based on bilinear pairing	Approximately 127.56 ms
Bilinear pairing operation	Approximately 1,617.77 ms
Hash function	Approximately 379.20 ms
Encryption	Approximately 77.64 ms
Decryption	Approximately 42.91 ms

Table 5 Computation overhead calculated at Vehicle (ms) during message exchange

Schemes	Exec. time during message exchange at OBU (ms)
A1- [16]	0.1881
A2- [17]	397.20
A3- [18]	0.181
A4- [19]	1036.68
A5- [20]	0.272
A6- [21]	4853.32
A7- [22]	0.278
A8-Proposed Scheme	71.17

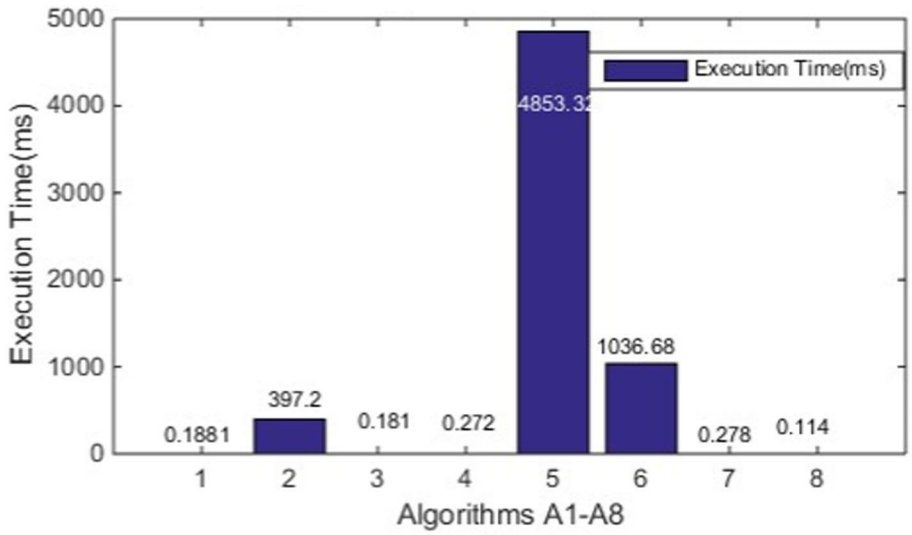

Fig. 5 Execution time for transferring data exchange at vehicle-without encryption

Table 6 Communication overhead during message verification at RSU (ms)

Schemes	Execution time during message Verification at RSU (ms)
A1-[16]	0.3494
A2-[17]	5611.88
A3-[18]	0.181
A4-[19]	255.13
A5-[20]	0.265
A6-[21]	0.362
A7-[22]	0.362
A8-Proposed Scheme	40.19

14.2 Computation overhead at the RSU during message verification:

This section outlines cost of execution of running cryptographic operations during the verification of the message at the receiver's end. Table 6 represents the Execution time

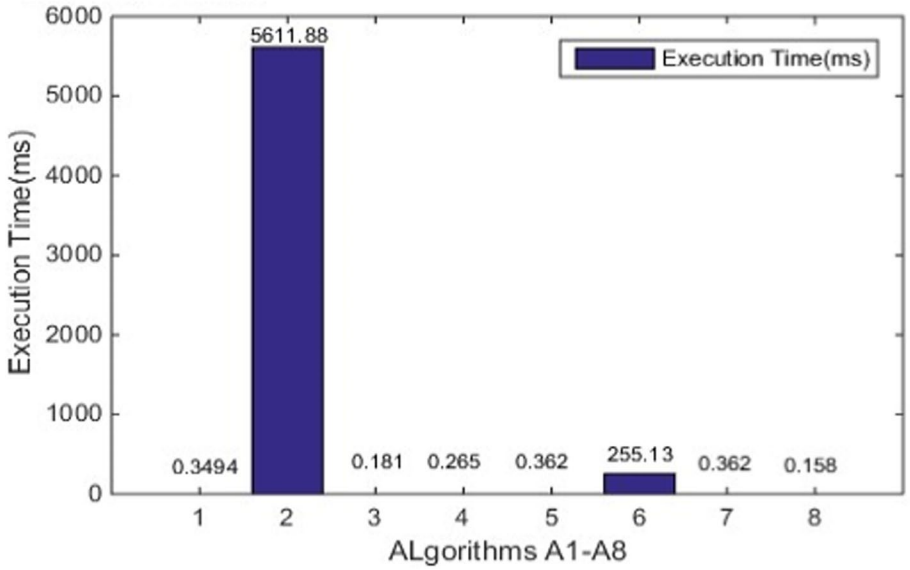

Fig. 6 Execution time during message verification at RSU-without encryption

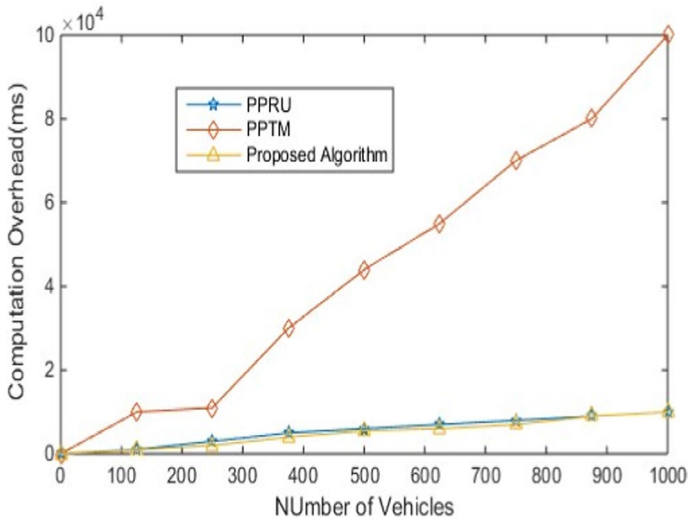

Fig. 7 Computation overhead at TA

taken at the RSU for the verification of the message with encryption its value is 40.19 ms. Execution time without encryption is also calculated and presented in Fig. 6, which is turned out to be 0.158 ms for proposed algorithm.

14.3 Computation overhead at TA

Figure 7 represents the computation overhead/cost at the trusted authority for PPRU [44] and PPTM [45] scheme including the proposed schemes. As it is mentioned, the proposed scheme deploys minimum overhead on TA, so figure shows computation overhead turns out to be minimum among all three algorithms. In PPRU and PPTM, reputation certificate is used. In PPRU, reputation certificate have 4 fields; on the other hand, in

PPTM reputation certificate have 5 fields. In the proposed algorithm, trust management is using just two parameters: direct trust and indirect trust. This is calculated at the vehicles level and sent to RSU. RSU calculates the combined trust by the addition of direct trust and indirect trust and thus identifies the trust node.

14.4 Communication overhead during message exchange

This section represents the evaluation of the communication cost during the message communication at vehicles and TA side.

15 Communication overhead at vehicle

As shown in Fig. 8, communication overhead is revealed on the vehicles side. It shown that communication cost for PPRU is higher than that of the PBTM and proposed algorithm. Figure 2b elaborates the communication cost at the trusted authority side. PPRU is showing the lower cost at TA side than the PBTM, but at the same it is greater than the proposed scheme. While taking the total number of vehicles varying from 1 to 1000. The reducing percentage of cost is approx. 85.37%

16 Communication overhead at TA

The proposed scheme is also compared with schemes [16, 17, 31, 32, 33, 34, and 35] in the context of communication cost. As per the recommendation of NIST to manage the strength of security of 16 bytes, we require key size of 32 bytes. For the same security strength, hash function could be SHA 256, 512 or256. Time stamp size can be 4 bytes. As per IEEE 1609.2, the length of the certificates is 125 bytes [46]. Communication ID of the OBUs is assumed to be 128 bits (Fig. 9).

By considering above requirements of security strength of 16 bytes, all schemes were compared and its result is shown in Tables 4 and 5.

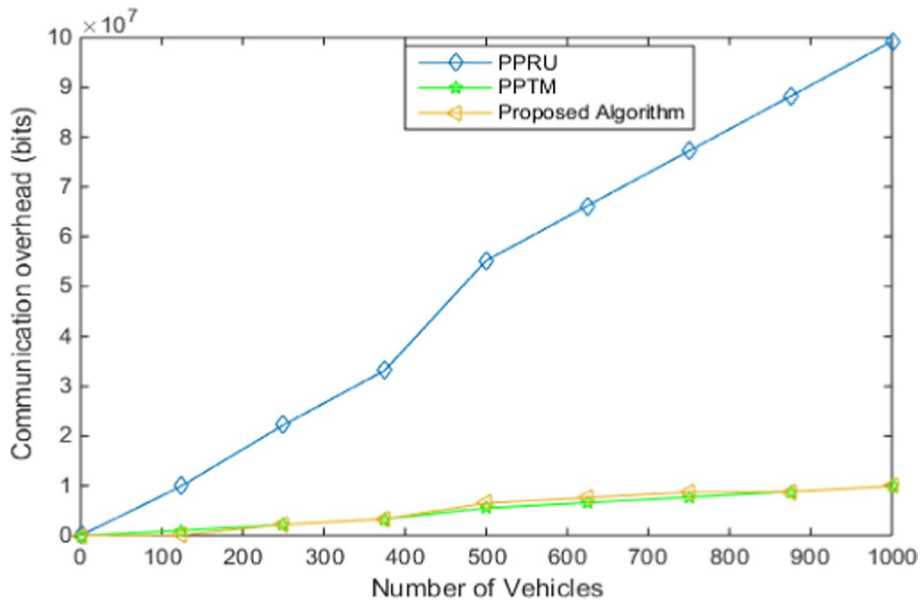

Fig. 8 Communication overhead at vehicle

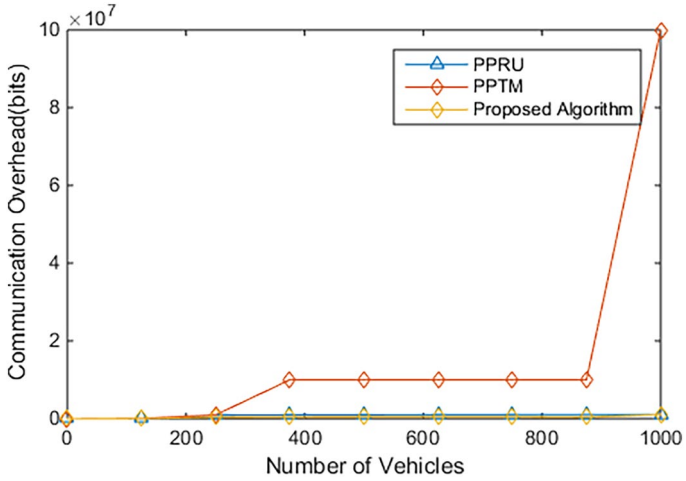

Fig. 9 Communication overhead at TA

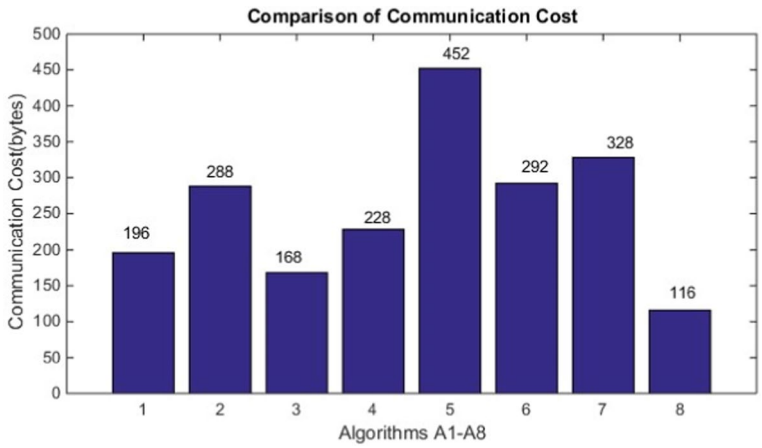

Fig. 10 Comparison of communication cost

Algorithm [16] communication cost in sending a single message will be 196 bytes, and sending the broadcasting message, it will be 196n bytes for sending n messages. Algorithm [17] consumes 288 bytes in sending a single message. 168 bytes' consumption in case of [18], 292 bytes in case of [19], 228 for [20], 452 for [21], 328 for [22]. Likewise, we calculate the communication cost for RCSRC scheme for sending a message to other vehicles ($C_{sky}((Message)||H_1||CV_i||Ts||framekey||GP)$.

Message is encrypted so its encrypted. Here size of communication ID is 16 bytes, 4 bytes for timestamp, hash function 32 bytes, 32 bytes for encryption keys. So the communication cost is approx. 32*2 + 32 + 16 + 4 = 116 bytes shown in Fig. 10.

16.1 Robustness evaluation

This section represents the evaluation of robustness by having varying number of malicious nodes. Assume total number of vehicles as 1000. Percentage of law enforcement vehicles private and public vehicles are 5%, 85% and 10%. Commandment

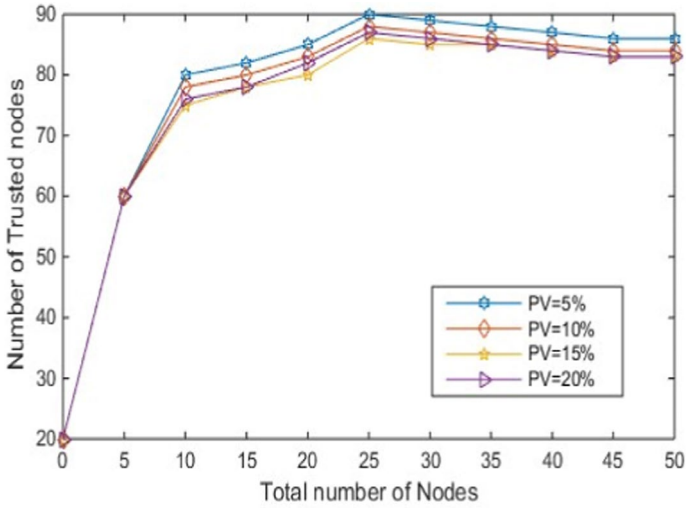

Fig. 11 Number of trusted nodes vs total number of nodes

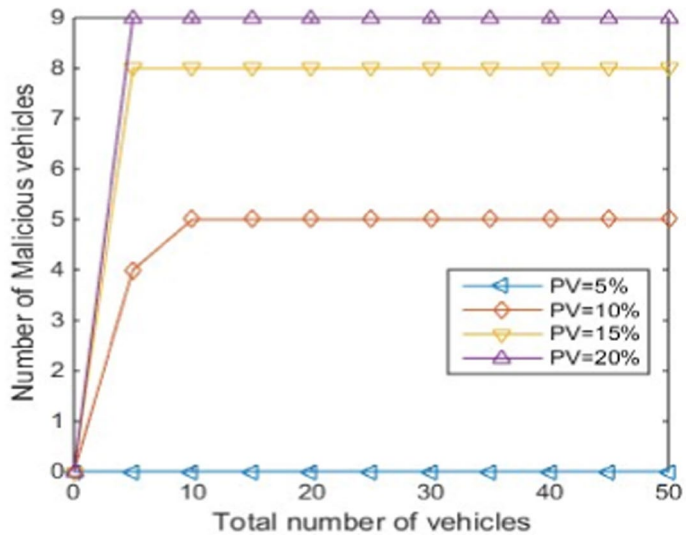

Fig. 12 Number of malicious nodes vs total number of nodes

enforcement and public vehicles are said to be trusted, and private vehicles could be trusted or malicious. For the experimental purpose, we are adjusting the malicious nodes from 5 to 20% for the private vehicles. Simulation is carried out 1000 times for each PV values. Figure is showing the average values of all 1000 times simulation. It is shown in figure initially the number of trusted vehicle are constant after the 20 rounds it drastically increase and stable. It is also shown in Fig. 11 that trusted nodes values decrease with the increase in the private vehicles.

In Fig. 12 for every PV value in starting 10 rounds, the malicious nodes increase, but it remains stable for every PV value after few rounds. Malicious nodes values increase with the increase in the number of vehicles. For different PV values, the number of

trusted vehicles is greater than the malicious vehicles; thus, it indicates that the proposed algorithm is robust.

The performance of the proposed scheme is mentioned in Tables 4 and 5. Compared to the other schemes, it is showing improved performance from few algorithm and its performance is declined from some others algorithms. It is showing 44.71% improvement from algorithm [16], 99.97% improved than [17], 42.54% improved than [18], 99.98% than [19], 61.76% than [20], 99.99% than [21] and 62.59% improved than [22].

During message verification process, it shows performance than [16, 17, 19, 21] and [22] with 24.06%, 99.99%, 99.89%, 26.79% and 26.79%. It is having similar performance with respect to [20]. During robust verification for varying number of private vehicles from 5 to 20%, the number of trusted vehicles is turned out to be more than the malicious nodes, which makes the proposed scheme robust.

17 Conclusion

A robust authentication algorithm is pivotal in safeguarding communication systems by verifying the identities of entities and ensuring the integrity and confidentiality of transmitted data. Authentication of various devices used in VANET is equally important than confidentiality of the message being sent over the VANET network. This paper explains a simple technique for authentication of the vehicle. Communication ID is used in the communication instead of real vehicle IDs. Latency is also taken care in this algorithm; for this purpose TA is involved only one time at the time of vehicle registration and later on assigning the communication IDs and secrets is done by ATA. All communication is done within the cluster using the cluster head, that is, RSU. In the proposed algorithm, RSU is acting as the cluster head; this approach makes it more reliable. Trustiness is also evaluated about the node using direct and indirect trust calculation. Additionally, the proposed scheme is also using the lightweight cryptography instead of complex cryptography techniques. Using authentication, trustiness and encryption feature proposed algorithm is showing the efficient behavior when compared in terms of communication time and the communication cost.

Acknowledgements
Not applicable.

Author contributions
All authors have equal contribution.

Funding
Nil.

Availability of data and materials
No new data are created.

Declarations

Competing interests
The authors declare that they have no conflict of interests

Received: 14 August 2024 Accepted: 1 October 2024
Published online: 10 October 2024

References

1. N.K. Chaubey, Security Analysis of Vehicular Ad Hoc Networks (VANETs): A Comprehensive Study. Int. J. Secur Appl. **10**, 261–274 (2017)
2. H. Kaur, Meenakshi, "Analysis of VANET Geographic Routing Protocols on Real City Map". 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), pp. 895899, May 19–20, 2017
3. D. Jiang, V. Taliwal, A. Meier, W. Holfelder, R. Herrtwich, Design of 5.9 GHz DSRC-based vehicular safety communication. IEEE Wirel. Commun. **13**(5), 36–43 (2006)
4. L.M. Bernald, S.S. Sayana, Dual authentication and key management for secure transmission in Vanet. Int. Res. J. Eng. Technol. **05**(4), 3048–3051 (2018)
5. D. He, S. Zeadally, B. Xu, X. Huang, "An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks." IEEE Trans. Inf. Forensics Security **10**(12), 2681–2691 (2015)
6. L. Zhang, Q. Wu, J. Domingo-Ferrer, B. Qin, C. Hu, "Distributed aggregate privacy-preserving authentication in VANETs." IEEE Trans. Intell. Transp. Syst. **11**(10), 01–11 (2016)
7. V. Daza, J. Domingo-Ferrer, F. Seb, A. Viejo, "Trustworthy privacy preserving car-generated announcements in vehicular ad hoc networks." IEEE Trans. Veh. Technol. **58**(4), 1876–1886 (2009)
8. F. Qu, Z. Wu, F. Wang, W. Cho, "A security and privacy review of VANETs." IEEE Trans. Intell. Transp. Syst. **16**(6), 29582996 (2015)
9. C. Kerrache, C.T. Calafate, J. Cano, N. Lagraa, Pietro, Trust management for vehicular networks: an adversary-oriented overview. IEEE Access **4**, 9293–9307 (2016)
10. S. S. Manvi, and S. Tangade, "A survey on authentication schemes in VANETs for secured communication, Journal of Vehicular Communications", vol. 9, pp. 19–30, Mar. 2017
11. S. Tangade, S.S. Manvi, P. Lorenz, (2018) "Decentralized and scalable privacy-preserving authentication scheme in VANETs." IEEE Trans. Veh. Technol. **67**(9), 8647–8655 (2018)
12. S.A. Eftekhari, M. Nikooghadam, M. Rafighi, Security-enhanced three-party pairwise secret key agreement protocol for fog-based vehicular ad-hoc communications. Veh. Commun. **28**, 100306 (2021)
13. S. Sajini, E.A. Mary Anita, J. Janet, A block chain based authentication scheme in VANET for a secure data communication using SHAH algorithm. India. J. Sci. Technol. **16**(46), 4291–4299 (2023). https://doi.org/10.17485/IJST/v16i46.2010
14. R. Ramamoorthy, An enhanced location-aided ant colony routing for secure communication in vehicular ad hoc networks. Human-Centric Intell. Syst. **4**(1), 25–52 (2024)
15. M. Wang, D. Liu, L. Zhu, Y. Xu, F. Wang, LESPP: lightweight and efficient strong privacy preserving authentication scheme for secure VANET communication. Computing **98**(7), 685–708 (2016)
16. J. Zhang, J. Cui, H. Zhong, Z. Chen, L. Liu, PA-CRT: Chinese Remainder Theorem Based Conditional Privacy-Preserving Authentication Scheme in Vehicular Ad-Hoc Networks. IEEE Trans. Depend. Secure Comput. **18**(2), 722–735 (2019)
17. M. Bayat, M. Pournaghi, M. Rahimi, M. Barmshoory, NERA: A new and efficient RSU based authentication scheme for VANETs. Wirel. Netw. **26**, 3083–3098 (2020)
18. M.A. Alazzawi, H. Lu, A.A. Yassin, K. Chen, Efficient conditional anonymity with message integrity and authentication in a vehicular ad-hoc network. IEEE Access **7**, 71424–71435 (2019)
19. Z. Jianhong, X. Min, L. Liying, On the security of a secure batch verification with group testing for VANET. Int. J. Netw. Secur. **16**, 355–362 (2014)
20. D. He, S. Zeadally, B. Xu, X. Huang, An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks. IEEE Trans. Inf. Forensics Secur. **10**, 1–1 (2015). https://doi.org/10.1109/TIFS.2015.2473820
21. P. Wang, Y. Liu, SEMA: secure and efficient message authentication protocol for VANETs. IEEE Syst. J. **15**(1), 846–855 (2021). https://doi.org/10.1109/JSYST.2021.3051435
22. J. Alshudukhi, B. Al-Shaibani, Z. Al-Mekhlafi, Conditional privacy-preserving authentication scheme without using point multiplication operations based on elliptic curve cryptography (ECC). IEEE Access (2020). https://doi.org/10.1109/ACCESS.2020.3044961
23. T.Y. Wu, C.M. Chen, K.H. Wang, C. Meng, E.K. Wang, A provably secure certificate less public key encryption with keyword search. J. Chin. Inst. Eng. **42**, 20–28 (2019)
24. H. Liu, Y. Sun, Y. Xu, R. Xu, Z. Wei, A secure lattice-based anonymous authentication scheme for vanets. J. Chin. Inst. Eng. **42**(2019), 66–73 (2019)
25. M. Lee, T. Atkison, (2021) "Vanet applications: past, present, and future." Veh. Commun. **28**, 100310 (2021)
26. S. Kudva, S. Badsha, S. Sengupta, I. Khalil, A. Zomaya, Towards secure and practical consensus for blockchain based VANET. Inf. Sci. **545**, 170–187 (2020)
27. P. Tyagi, D. Dembla, Advanced secured routing algorithm of vehicular ad-hoc network. Wirel. Pers. Commun. **102**(1), 41–60 (2018)
28. J. Jenefa, E.M. Anita, Identity-based message authentication scheme using proxy vehicles for vehicular ad hoc networks. Wirel. Netw. **27**(5), 3093–3108 (2021)
29. A. Roy, S. Madria "Distributed incentive-based secured traffic monitoring in VANETs". In: 21st IEEE international conference on mobile data management (MDM), pp. 49–58, https:// doi. org/ 10. 1109/ MDM48 529. 2020. 00026. (2020)
30. J. Bhatia, P. Kakadia, M. Bhavsar, S. Tanwar "SDN-enabled network coding based secure data dissemination in VANET environment". IEEE Internet of Things Journal. https:// doi. org/ 10. 1109/ JIOT. 2019. 29569 64. (2019)
31. A. Ferdowsi, S. Ali, W. Saad, N.B. Mandayam, Cyber-physical security and safety of autonomous connected vehicles: optimal control meets multi-armed bandit learning. IEEE Trans. Commun. **67**(2019), 7228–7244 (2019)
32. S.J. Horng, C.C. Lu, W. Zhou, An identity-based and revocable data-sharing scheme in vanets. IEEE Trans. Veh. Technol. **69**, 15933–15946 (2020)
33. J. Cui, L.S. Liew, G. Sabaliauskaite, F. Zhou, (2019) "A review on safety failures, security attacks, and available countermeasures for autonomous vehicles." Ad Hoc Netw. **90**, 101823 (2019)

34. D. Manivannan, S.S. Moni, S. Zeadally, (2020) "Secure authentication and privacy preserving techniques in vehicular ad-hoc networks (vanets)."Veh. Commun. **25**, 100247 (2020)
35. P. Mundhe, S. Verma, S. Venkatesan, (2021) "A comprehensive survey on authentication and privacy-preserving schemes in vanets." Comput. Sci. Rev. **41**, 100411 (2021)
36. K. Lim, K.M. Tuladhar, X. Wang, W. Liu "A scalable and secure key distribution scheme for group signature based authentication in vanets", In: Proceedings of the 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON), IEEE, 2017, pp. 478–483
37. I. Ali, A. Hassan, F. Li, Authentication and privacy schemes for vehicular ad hoc networks (vanets): a survey. Veh. Commun. **16**, 45–61 (2019)
38. Y. Yang, Z. Wei, Y. Zhang, H. Lu, K.K.R. Choo, H. Cai, V2x security: a case study of anonymous authentication. Pervasive Mob. Comput. **41**, 259–269 (2017)
39. S.M. Farooq, S.S. Hussain, T.S. Ustun "Elliptic curve digital signature algorithm (ecdsa) certificate based authentication scheme for advanced metering infrastruc", In: Proceedings of the 2019 Innovations in Power and Advanced Computing Technologies (i-PACT), IEEE, 2019, pp. 1–6
40. K. Suganyadevi, V. Nandhalal, S. Palanisamy, S. Dhanasekaran "Data security and safety services using modified timed efficient stream loss-tolerant authentication in diverse models of vanet", In: Proceedings of the 2022 International Conference on Edge Computing and Applications (ICECAA), IEEE, 2022, pp. 417–422
41. C. Caballero-Gil, P. Caballero-Gil, J. Molina-Gil "Using Groups to Reduce Communication Overhead in VANETs". AP2PS 2010 - 2nd International Conference on Advances in P2P Systems. (2010)
42. S.H. Islam, M.S. Obaidat, P. Vijayakumar, E. Abdulhay, F. Li, M.K.C. Reddy, (2018)" A robust and efficient password-based conditional privacy preserving authentication and group key agreement protocol for VANETs", Future Gener. Comput. Syst. **84**, 216–227 (2018)
43. S. Li, R. Yang, J. Chen, A privacy-preserving authentication scheme for VANETs with exculpability. Secur. Commun. Netw. **2023**, 1–12 (2023). https://doi.org/10.1155/2023/8676929
44. Z. Liu, L. Wan, J. Guo, F. Huang, X. Feng, L. Wang, and J. Ma, (2023) "PPRU: A Privacy-Preserving Reputation Updating Scheme for Cloud-Assisted Vehicular Networks", IEEE TRANSACTIONS on vehicular technology, vol. 1, no. 1, October 2023
45. Z. Liu, J. Weng, J. Guo, J. Ma, F. Huang, H. Sun, Y. Cheng, (2022) "PPTM: A privacy-preserving trust management scheme for emergency message dissemination in space-air-ground integrated vehicular networks." IEEE Internet Things J. **9**(8), 5943–5956 (2022)
46. M. Zeng, H. Xu, Mix-context-based pseudonym changing privacy preserving authentication in vanets. Mob. Inform. Syst. **2019**, 1–9 (2019). https://doi.org/10.1155/2019/3109238
47. S. Ullah, G. Abbas, M. Waqas, Z.H. Abbas, A.U. Khan, RSU assisted reliable relay selection for emergency message routing in intermittently connected VANETs. Wirel Netw. **29**(3), 1311–1332 (2023)
48. R. Ramamoorthy, S. Kumar, R. C. A. Naidu, M. Sathya "Hybrid multihop routing mechanism with intelligent transportation system architecture for efficient routing in VANETs". In: 2022 international conference on disruptive technologies for multi-disciplinary research and applications (CENTCON), vol. 2. New York: IEEE; 2022, December. p. 69–74. (2022)
49. S. Harrabi, I.B. Jaafar, K. Ghedira, Survey on IoV routing protocols. Wirel. Pers. Commun. **128**(2), 791–811 (2023)
50. H. Ikhlef, S. Bourebia, A. Melit, Link state estimator for VANETs using neural networks. J. Netw. Syst. Manag. **32**(1), 10 (2024)
51. C. Dai, X. Xiao, Y. Ding, L. Xiao, Y. Tang, S. Zhou, "Learning based security for VANET with blockchain". In IEEE international conference on communication systems (ICCS), pp. 210–215, 2018
52. M. Farrell, M. Bradbury, M. Fisher, L.A. Dennis, H. Clare Dixon, C.M. Yuan, Using threat analysis techniques to guide formal verification: a case study of cooperative awareness messages, in *Software Engineering and Formal Methods: 17th International Conference, SEFM 2019, Oslo, Norway, September 18–20, 2019, Proceedings*. ed. by P.C. Ölveczky, G. Salaün (Springer International Publishing, Cham, 2019), pp.471–490. https://doi.org/10.1007/978-3-030-30446-1_25

Publisher's Note