Enhancing Privacy and Trust in VANETs with Blockchain Authentication

M.Karuna[1], E.Rupa[2], PH.Swarna Rekha[3]

[1]Assistant Professor, Department of CSE, Sri Indu Institute of Engineering & Technology, Hyderabad

[2]Assistant Professor, Department of CSE, Sri Indu Institute of Engineering & Technology, Hyderabad

[3]Assistant Professor, Department of CSE, Sri Indu Institute of Engineering & Technology, Hyderabad

Abstract

Vehicular Ad Hoc Networks (VANETs) are characterized by high mobility of nodes and volatility, which make privacy, trust management, and security challenging issues in VANETs' design. In such networks, data can be exposed to a variety of attacks, the most dangerous is false information dissemination, which threatens the safety and efficiency of transportation systems. False emergency messages can be injected by inside attackers to announce fake incidents such as traffic accidents, resulting in a false information attack. As the data in VANET is based on events, any trust mechanism must first identify the true events. To address these security challenges, a blockchain-based authentication scheme and trust management model are proposed for VANETs. Using the authenti- cation scheme, vehicles are enabled to send messages anonymously to the roadside units (RSUs) and the identity privacy of vehicles is protected. Besides, the proposed trust management model is designed to detect and deal with false information by evaluatingthe trustworthiness of vehicles and data. Using the trust model, when vehicles report anincident to the nearest RSU, the RSU is able to verify whether or not the incident took place. This mechanism ensures that RSUs send only verified event notifications. Finally, RSUs participate in updating the trust values of vehicles and store these values in the blockchain. The efficiency of the proposed authentication scheme is validated through analysis while the trust model is validated through simulations. The results obtained show that the proposed authentication scheme and the trust model provide better performance than other state-of-the-art models where malicious vehicles can be identified efficiently and RSUs are enabled to broadcast only legitimate events.

KEYW ORDS

authentication, blockchain, privacy-preserving, trust management, VANET

1 | INTRODUCTION

Vehicular Ad Hoc Network (VANET) provides a promising way for vehicles to communicate with each other via Vehicle- to-Vehicle (V2V) and with roadside units (RSUs) via Vehicle- to-Infrastructure (V2I) to facilitate road safety. Furthermore, RSUs can share the data with the backbone network via the Internet. A Dedicated Short-Range Communication protocol is used to facilitate communication between vehicles and RSUs in VANETs [1]. The information they exchange usually in- cludes alerts and reports about traffic accidents and othertraffic conditions. All of these traffic alerts and notificationswill provide vehicles with timely information about different traffic conditions. It will assist vehicles in effectively avoiding traffic congestion or potential traffic incidents by executing a timely response by changing the route to prevent traffic jams, thus improving transportation safety and efficiency [2]. Infor- mation shared in the context of VANETs must be reliable and trustworthy, as important decisions and people's lives may rely on it. However, if a malicious vehicle reports false information about vehicle position or the traffic condition, it may lead totraffic jams or road accidents [3–5]. Therefore, authentication and trust of the transmitted messages are essential requirements in VANETs. The other crucial issue for VANETs is privacy, which means only trusted authorities should only have access to private information of a vehicle (such as its real identity) and as a result, the driver's privacy will be protected from any third-party observer [6]. When bogus messages lead to accidents, the trusted authority (TA) can trace malicious vehicles, thus ensuring accountability.

Vehicles' privacy and authentication concerns are growing significantly [7]. For establishing an effective vehicular communication network, there are two essential requirements. Messages should be sent and forwarded anonymously as these messages usually contain private information of users, such as geographic location. However, messages sent anonymously cannot be guaranteed to be authentic. It is especially difficult to prevent false messages from being disseminated from internal vehicles. These false messages can cause disturbance to driver behaviour and consequently lead to accidents [8]. When bogus messages are noticed, the TA and RSUs should be able to trace the real identity of the malicious vehicle that spread the messages. We assume that the TA can be trusted completely. The duty of the TA is to register vehicles and RSUs. In addition, it generates private keys and security parameters for vehicles and RSUs. If RSUs and vehicles want to participate in the network, they must first register with TA. When these vehicles and RSUs are successfully registered, the security parameters generated by TA are loaded to them. Furthermore, TA generates pseudo-identity for each vehicle and stores its relationship with the real identity, this helps to trace the vehicle in case of malicious activity. To prevent false information attacks, the received data from vehicles must be analysed by RSUs for potential accuracy. RSUs should have the ability to identify and verify false information reports. Traditional cryptography and Public Key Infrastructure (PKI) are used in the majority of current security solutions. Most security issues are addressed to some extent by these solutions; for example, outsider attackers are easily detected by these solutions. However, insider attackers are not detected by PKI-based solutions since they are authenticated participants with valid credentials. To overcome the shortcomings of security solutions based on PKI, the concept of trust has been introduced as an additional security parameter that can detect insider attackers by analysing mutual messages. In a VANET, trust is described as the belief that one node has in another node(s) for the purpose of exchanging trustworthy, reliable, accurate, and authentic messages [9, 10]. Trust model as a security tool in VANETs is still relatively in its early stages. The trust models ensure that reliable information is broadcast across the network, that malicious vehicles are tracked, and that false messages are eliminated. Vehicles and RSUs have trust models installed to determine the reliability, accuracy, and authenticity of received messages.

A blockchain is seen as a useful tool for dealing with the aforementioned issues and helping in the development of a robust trust model [11]. A blockchain is a distributed ledger that keeps track of all completed and shared digital events among participating nodes. It keeps a complete and verified record of every single event that has ever happened. The consensus of the majority of nodes within the blockchain ensures that blockchain events are valid. It provides reliable and traceable data and facilitates value exchange among untrusted entities without reliance on centralized third parties. Due to these important features of the blockchain, it has the potential to create a desirable trust model in VANETs [12]. Blockchain technology has been suggested as a method of bringing ‘trust’ and ‘autocheck’ to VANETs. It is helpful in creating a suitable data-sharing platform in VANETs. Further, the pseudonyms and trust values of the vehicles will be recorded into an immutable, tamper-resistance, and decentralized ledger [13].The blockchain is adopted for secure storage because it has several key characteristics: decentralization, transparency, immutability, and anonymity. Decentralization allows controls and functions to be delegated to participants from a central authority. Each participant receives a copy of the transaction ledger. A new block is created after all participants have validated the transactions. As a result, the network runs in a decentralized environment on a peer-to-peer basis. The blockchain's data is accurate, reliable, consistent, timely, and broadly accessible because of its decentralized network. It is resistant to malicious attacks and has no single point of failure. In the blockchain network, all transactions and events are recorded, thus ensuring transparency. Transparency allows everybody in the network to view the transactions. Moreover, blockchain technology is characterized by immutability. Data is stored in blocks, which are immutable and tamper-proof. A successful attack can only be launched if the adversary acquires 51% of the legitimate nodes. Furthermore, blockchain technology ensures anonymity. Participant anonymity is preserved since only the blockchain address is required.

Considering the limitations of existing authentication schemes and trust management models, there is a lack of the authentication scheme that fulfils the security and privacy requirements of VANET, including entity and message authen-

tication, non-repudiation, traceability, preservation of privacy, and unlinkability, have low computational and communication overhead. Moreover, an effective trust model that can identify malicious vehicles (inside attackers) and the content they generate and revoke them from the network, identify true and false events, be highly resistant to malicious attacks, and can provide an accurate evaluation result is required.

To fill the security, privacy, and trust gaps in VANET, in this work, we propose an efficient and lightweight authenti- cation scheme that ensures authentication between RSUs andvehicles and protects vehicle identity privacy and withstand various attacks. In addition, we propose a trust model that enables the RSUs to evaluate received reports, identify mali- cious vehicles, remain robust regardless of the growing number of malicious vehicles and allow only true events to be broad- cast by the RSUs. The main contributions of our paper can besummarized below.

1. To secure the communication between vehicles and RSUs, we propose an authentication scheme based on blockchain that allows vehicles and RSUs to communicate anony- mously and provides the ability to trace malicious vehicles,

protects vehicle privacy, and satisfies the security requirements of VANET
2. To safeguard VANETs against bogus messages, we require that vehicles and RSUs be able to authenticate the message sender, the message itself, and the timeliness of the message. In addition, RSUs perform the trustworthiness check of received messages and compute the trust values of vehicles
3. We propose a blockchain-based trust management scheme that allows the broadcast of only true events messages by RSUs. The scheme identifies malicious nodes and revokes them and enables RSUs to eliminate bogus messages and broadcast only true events. It also allows all RSUs to take part in the decentralized update of trust values where the trust information of all vehicles is shared with all RSUs in the vehicular network

The remainder of the paper is organized as follows. An overview of related work is provided in Section 2. In Section 3, we present the system model. In Section 4, the adversary model is presented. Section 5 & 6 describe the proposed authentication scheme and trust model in detail. The security analysis is presented in Section 7. In Section 8, the results and discussion are presented. Open challenges and future research directions are provided in Section 9. Finally, we draw our conclusions in section 10.

2 | RELATED WORK

2.1 | Privacy-preserving authentication in VANETs

Raya and Hubaux [14] introduced the concept of conditional privacy-preserving authentication (CPPA) in order to overcome security and privacy issues in VANETs. They also demonstrated how to use a modified PKI to implement a practical CPPA protocol based on anonymous certificates. In their scheme, a large number of certificates and public/private key pairs are installed into vehicle onboard units (OBUs) in order to hide the vehicle's real identity and achieve anonymous authentication. The CPPA protocols proposed by Zhang et al. [15] require substantial storage costs for certificates. In fact, key/certificate management complexity is a common weakness in existing CPPA protocols. As a result, CPPA protocols that use ID-based signatures have been developed [16–18]. Each of these protocols aims at either enhancing existing solutions to meet security criteria or increasing CPPAs performance to support VANET applications. Zheng et al. [13] created an ID-based BCPPA protocol with traceable anonymity using pseudonym technology. By combining pseudonyms with a safe access authentication scheme between vehicles and RSU, the proposed scheme reduces reliance on TA, but it is limited by the need for ideal hardware and is vulnerable to a compromised certificate authority. Tan et al. [19] presented a certificateless authentication and message dissemination protocol for vehicle identity authentication in vehicle-to-RSUs communication and to improve user key protection in VANETs. Vijayakumar et al. [20] developed a secure authentication and key management mechanism. However, the proposed solutions do not provide distributed security because they rely on a trusted third party. Peng [21] proposed an on-board network certificateless signature scheme-based anonymous authentication protocol. Despite the fact that this protocol ensures user confidentiality and efficient authentication, it is unable to identify the malicious vehicle. Further, Feng et al. [22] proposed a blockchain-assisted privacy-preserving authentication system for VANETs, which protects vehicle privacy while also allowing automatic authentication. As part of the proposed system, the message credibility is checked, the behaviour of the vehicle is monitored, and the communication history is also tracked.

Alazzawi et al. [23] introduced a pseudo-identity-based scheme that is intended to secure communications within VANETs using pseudonyms. The scheme does not include bilinear pairing operation and is efficient and provides batch verification but does not satisfy all the security requirements, like unlinkability.

For V2V communication, Liu and Wang [24] proposed an efficient CPPA scheme based on a ring signature scheme using bilinear maps. The scheme performs batch signature verification efficiently. However, it is ineffective for signing and verifying single messages.

By using the data recovery property in the message recovery signature, Jian et al. [25] proposed a secure traffic data aggregation scheme for VANETs. Their scheme supports batch verification. However, it has some shortcomings. Pseudo-identities for vehicle communication are not used in this scheme, so the conditional privacy-preserving characteristic is not met. Secondly, there is a high computational and communication overhead in their scheme. Additionally, the proposed scheme requires a secure channel for signature transmission, which limits its practical application.

Ali et al. [26] used a bilinear map and pseudonyms to create an efficient Identity-based CPPA signature scheme with batch verification for V2I communication. The scheme performs better than related schemes. However, in identity-based schemes, the private key generator (PKG) has access to all users' private keys; therefore, if PKG is compromised, key escrow issues will appear.

Cui et al. [27] proposed a secure mutual authentication scheme that preserves privacy. By updating the TPD data regularly, malicious users will not be able to gain useful information that might be exploited in a side-channel attack to disrupt the VANET network. However, their scheme suffered from impersonation attacks and forgery attacks.

Ren et al. [28] presented an efficient and privacy-preserving certificateless public key signature technique. First, with their approach, a single signature can be verified with only two bilinear pairing operations while batch verification and signature aggregation are also supported. Second, to secure the vehicles' identity privacy, the scheme uses two blockchains. However, the key generator centre suffers from key escrow problems.

Different from existing works, our proposed scheme fulfils the security and privacy requirements of VANET, including entity and message authentication, non-repudiation, traceability, preservation of privacy, and unlinkability, resists impersonation, forgery, and other kinds of attacks, and provides low computational and communication overhead. With our scheme, the key escrow issues associated with identity-based systems and the complex certificate management problem associated with PKI are avoided.

2.2 | Trust management in VANETs

Trust is defined as a mechanism that allows the receiving node (RSU/vehicle) to determine with a degree of certainty whether the information from an arbitrary sender should be accepted or discarded. It is a measure of the quality (trustworthiness) of the received message. When a message is received, the receiver node needs to verify: (a) the message sender's legitimacy and trustworthiness, and (b) the message's content's legitimacy and trustworthiness. The former is met by authentication and node trust while the second is met by authentication and content trust. Using trust models, trusted content is propagated throughout the network. Trust management is crucial for identifying malicious vehicles and determining the reliability of traffic data [29].

2.2.1 | Classification of trust management

There are essentially three types of trust management approaches currently in use:

Trust management based on entities

It focusses on the trust evaluation of each entity in the network. Usually, an entity has a trust value that evolves over time. Trust and reputation have been widely used in the literature to assess the trustworthiness of an entity [30]. Khan et al. [31] introduced an approach based on clusters in which the elected cluster head (CH) is in charge of calculating and evaluating network trust. In its neighbourhood, CH uses a watchdog system in which legitimate vehicles report the existence of misbehaving vehicles to CH. Once malicious vehicles have been detected, CH notifies the TA, who then removes them from the network. However, the high overhead caused by the CH's reports, which reduces network performance, is the major disadvantage of this strategy. Furthermore, this study lacks information on communication between vehicles, CH, and TA. Hu et al. [32] presented REPLACE, which is a reliable and trust-based batch service selection scheme to help consumer vehicles avoid selecting poorly behaving platoon head vehicles. In addition, the system allows platoon head vehicles to receive and model input from their user vehicles. It uses input from user vehicles to measure platoon head vehicle trust values. In addition, to deal with untrustworthy feedback from user vehicles, an iterative filtering algorithm was developed. Haddadou et al. [33] proposed the DTM2, an infrastructure-independent confidence model derived from the work market signalling model. DTM2 assigns credits to vehicles and secures their management. In this solution, each vehicle receives credit for receiving data, so that selfish vehicles are prompted to cooperate more. It employs a tamper-proof system to provide rewards and punishment while also preventing tampering attacks. Minhas et al. [34] designed a trust model based on four factors: (1) priority, (2) sender node experience, (3) majority opinion, and (4) position. When a message is sent, the evaluator node (EV) chooses and prioritizes local vehicles (VP) based on their reputation and knowledge, integrating position and experience-based trust. Then, it seeks feedback from the VP about the legitimacy of the event. VPs respond to it with their opinions based on proximity in time and place. EV uses a plurality rule to decide the vehicle's trustworthiness after all VP messages have been received. The EV accepts messages if a majority agrees; if not, vehicles with more experience on the network are asked for advice. Using PKI cryptography for role-based trust calculation leads to the need for central authorities to verify certificates, which makes this trust model disadvantageous.

Trust management based on data

It focusses on the assessment of data produced by an entity instead of the entity itself. In ephemeral networks such as VANET, data trust evaluation is more convenient than the entity's trust due to the absence of social connections between fast-moving entities [30]. Gurung et al. [35] in their trust model considered a number of factors such as context similarity, route similarity, and content conflict to evaluate the message's credibility. Liu et al. [36] proposed the LSOT data-oriented trust model, which calculates overall trust based on certificates and recommendations. A total of three weights (context, time decay, and number) were applied in order to measure overall trust accurately. Shaikh and Alzahrani [37] introduced a trust model that can identify fake messages in the network. The trustworthiness of a vehicle is determined in three stages. First, a trust value is determined for each piece of data based on four factors: time closeness, time verification, location closeness, and location verification. Then, trust is determined for each message, and finally, the message is subjected to fuzzy logic, where accepting or rejecting the information is made by a decision module. A message's trustworthiness rating is only acknowledged when it reaches a certain threshold. The delay imposed in the calculation of trust values makes this model not ideal for safety applications. In Ref. [2], the authors presented a context-aware trust management model that can authenticate a message by evaluating the sender's trust value. In this method, the level of trust is determined by both the available knowledge and the current assessment technique. In addition, integrated reinforcement learning techniques are used to dynamically evaluate different driving scenarios.

Hybrid trust management

In a hybrid trust, both trust managements based on entity and data are combined. In this class, the entity's trust value represents the input of the data trust model. The aim of hybrid

approaches is to provide a more efficient trust evaluation that considers both the message and entity's trustworthiness [30]. Sedjelmaci and Senouci [38] provided a trust model to evaluate message credibility. This trust model operates in two stages. The first stage identifies CH, which performs a completely distributed evaluation of message trustworthiness. In the second stage, a nearby RSU is used to measure the trust value on a global scale. As a result, stable clusters are assumed to be present in the vicinity of RSU, which is a major weakness in the model. Furthermore, choosing a CH and forming a cluster around an RSU are both time-consuming tasks that add to the network's overall complexity. To handle malicious attacks, Li and Song [39] proposed ART, data, and entities-based trust model. Entity trust is determined by recommendation and functional trust values. Data trust is determined in this model by information collected from multiple vehicles. Ahmad et al. [40] proposed MARINE, a trust Model, which detects and revokes malicious nodes' credentials when they execute man-in-the-middle attacks. Nodes in the MARINE system measure sender trust by performing multi-dimensional plausibility tests. The information obtained is then analysed both directly and indirectly.

2.3 | Trust management based on blockchain

The use of the blockchain for trust management is gaining more attention. Yang et al. [41] utilized the blockchain to ensure data credibility by having a reputation scheme that stores ratings from individual data receivers in the blockchain. A vehicle is randomly selected to perform the task of scoring the received message and storing it in a block. Once the selected vehicle broadcasts the block to neighbours, they confirm the ranking using their local knowledge. Adding a block to the blockchain happens once the majority of neighbours agree. However, it is not mentioned how the credibility of the received messages is evaluated. Bendiab et al. [42] proposed a blockchain-based identity management trust model where the trust relationships are controlled by cloud service providers with no third-party involvement. Another proposed model in [43] splits vehicles into clusters, with a CH appointed by an RSU to ensure message credibility. For checking the credibility of the messages, the miner will need the data about the behaviour of the vehicle as well as some fuzzy logic rules. Following that, a block is formed from the validated messages and is added to the blockchain. However, the cluster approach can be used in trust management in limited scenarios due to short-lived communication channels. Therefore, due to the limited number of neighbouring vehicles, this solution does not work in a highly mobile and sparse scenario.

Zhang et al. [44] presented AIT, which is a blockchain-based AI-enabled trust management system. First, each vehicle in the AIT system is able to detect, generate, and exchange messages with other vehicles. Then, nearby vehicles verify the messages that have been received. As they receive and validate messages from adjacent vehicles, vehicles will establish and manage the trust of those vehicles, which will be facilitated by the deep learning algorithm. Trust scores calculated locally by vehicles are shared with local RSU. Next, the following steps are performed: Calculation of the global trust level (GTL) by the local RSU, validation and archiving of trust by the blockchain, and voting and dissemination of the GTL by all the RSUs. When a vehicle detects an untrustworthy vehicle, it reports it to a nearby RSU, which verifies the authenticity of the report as well as the vehicle's identity using the blockchain. This system has the ability to revoke the security credentials of untrustworthy vehicles and the revocation is performed by the RSU. However, this system is not able to withstand a group of malicious vehicles cooperating together to tamper with or manipulate the trust value of a target vehicle.

Pu [45] proposed a blockchain-based trust management system that is based on multi-criteria decision making, also known as Trust-Block MCDM, in VANETs. The model evaluates the credibility of the received road safety message to determine the trust value of the message originator. It determines a message's credibility based on the opinions of neighbouring validators, the message originator's reputation value, and its own confidence in the event and then calculates a message originator's trust value. The trust values of each vehicle are periodically uploaded to a nearby RSU due to the limited storage capacity of vehicles. The RSU calculates a message originator's reputation value based on various trust values collected from vehicles, stores the reputation value in a block, and competes to add the block to the blockchain. This model can identify bogus messages and drop them from the network. The drawback of this model is that it suffers from unfair ratings sent to the RSU by malicious vehicles.

To evaluate the trustworthiness of vehicles, Wang et al. [46] propose a privacy-preserving trust management system based on the blockchain. The authors developed a trust evaluation blockchain in which distributed RSUs assess a vehicle's trustworthiness based on ratings from neighbouring vehicles. When a vehicle sends an event message to its neighbours and adjacent RSUs, neighbours generate feedback messages and send them to the RSU. Two smart contracts implement feedback message aggregation and trust evaluation with automated execution and validation by distributed RSUs. In order to protect vehicle privacy, Elliptic Curve Cryptography (ECC) is used for identity authentication. However, this system has the drawback of the high generated overhead needed to validate often numerous such pseudonyms within a short period.

Li et al. [47] developed ATM, a new local trust management system, to deal with trust inconsistencies between regions and fake trust values generated by a set of colluding malicious nodes. Active detection and blockchain techniques are used by ATMs. The surrounding malicious nodes are efficiently filtered by the active detection and their active cooperation is prevented and the neighbour reference is employed to remove outliers with median absolute deviation. At the same time, the blockchain ensures

that trust data is consistent across regions. However, this system uses a primary server for generating and maintaining the blockchain, which may lead to a single point of failure.

In Ref. [48], an HMM-based vehicle trust evaluation approach to improving the accuracy of malicious behaviour detection is presented. In addition, an alliance-based trust management method is developed with complete authority control, requires no authorization, improves data sharing, allows for easy branching and querying on the premise of security, and improves the efficiency of trust updating by requiring less time for consensus. However, this model suffers from unfair ratings sent to the RSU by malicious vehicles.

Kudva et al. [49] presented a blockchain-based decentralized trust score framework for participating nodes to proactively detect and blacklist insider attackers in the VANET and greatly improve the throughput of the vehicular network. The authors proposed a two-level detection scheme, in which neighbours calculate trust independently at the first level. The second level is a consortium-blockchain-based system that aggregates trust scores for vehicle nodes using authorized RSUs as validators. The blacklist node tables are then dynamically changed based on trust scores reported by surrounding nodes. However, these tables require processing overhead and additional communication overhead to be distributed.

In existing blockchain-based trust management schemes, vehicles evaluate the messages and submit the trust ratings to the RSU, which may be affected by the problem of unfair ratings submitted by malicious vehicles to manipulate the trust of other honest vehicles. Our method is different in that it relies on RSUs to evaluate the messages and compute the trust values of vehicles. Moreover, our trust model is highly resistant to false information attacks and can provide accurate evaluation results.

Table 1 presents a comparison of existing trust models for VANET.

3 | SYSTEM MODEL

Our proposed system model is presented in this section. The proposed solution consists of two components: an authentication scheme and a trust model. The authentication scheme enables vehicles to send messages anonymously and protect vehicle privacy. The trust model enables RSUs to calculate the trustworthiness of vehicles passing in VANET. When an event happens in the network, vehicles near the event send reports about the event to the reachable RSU. The RSU evaluates the credibility of the received reports, if the event is confirmed to be true, it broadcasts notifications to the vehicles in its communication range and stores the trust values of participating vehicles in a block. By using the consensus mechanism, RSUs can verify a block's correctness, and the correct block will be stored on the blockchain.

3.1 | Network model

Figure 1 illustrates the network model.

TA: TA is required at the registration phase and first-time authentication. The TA is responsible for making the transactions in the authentication blockchain, which is a private blockchain. The transactions are the information required for the authentication of vehicles when they join the network for the first time. The other RSUs have the right to read and check from the authentication blockchain the authenticity of a new vehicle. Vehicles do not need to contact the TA except for the first time registration and authentication. In this way, we reduce the dependency on the TA.

RSUs: RSUs are typically stationary and have large amounts of processing, storage, and communication capabilities. RSU collects messages from nearby vehicles, evaluates the trustworthiness of these messages, updates the trust values of the vehicles, and broadcast traffic events to the vicinity. They are able to keep track of all current trust levels of vehicles. In addition, all RSUs work together to construct a consistent ledger and perform consensus tasks. Therefore, the trust computation and update is performed in a fully distributed manner on the RSUs. This eliminates the dependence on centralized entities such as the TA.

Vehicles: Each vehicle has an OBU, which is a computing device with communication capabilities. OBUs make it possible for vehicles to communicate with each other and with RSUs. As compared to RSUs, vehicles are equipped with limited storage, computing, and communication capabilities. Vehicles send events information to the nearest RSU.

3.2 | Data structure of the proposed blockchains

We introduce the chronological Merkle tree (CMT), which is used in the authentication blockchain, and the Merkle Patricia Tree (MPT), which is used in the trust blockchain.

3.2.1 | Data structure of the authentication blockchain

Figure 2 shows the data structure of the proposed authentication blockchain with the CMT, which is the traditional blockchain's underlying data structure. In CMT, all transactions are hashed and sorted chronologically. The value of the root hash is stored in the blockchain while the internal hashes are not required to be stored [50]. Each transaction contains the value of the parameter N, which is calculated during the vehicle authentication phase. To preserve vehicles' privacy, no information that can be linked to a real identity is included in the transaction. The transactions issued by TA are stored permanently and immutably.

TABLE 1 Comparison of existing trust models for VANET

Reference	Type of model	Leverage blockchain	Privacy-preserving	Withstanding attacks
[31]	Entity-centric	No	No	Malicious vehicles
[32]	Entity-centric	No	No	Bad-mouthing, ballot-stuffing, newcomers, and on-off attacks
[33]	Entity-centric	No	No	Tampering attack
[34]	Entity-centric	No	No	Fake message attack
[35]	Data-centric	No	No	Tampering attack
[36]	Data-centric	No	No	Collusion attack
[37]	Data-centric	No	No	Fake location and time information
[38]	Hybrid	No	No	Black hole, selective forwarding, Sybil attacks, packet duplication, resource exhaustion, and wormhole.
[39]	Hybrid	No	No	Compromised nodes, Bad-mouthing attack, Zigzag attack
[40]	Hybrid	No		Man-in-the-middle attack
[2]	Data-centric	No	No	Malicious vehicles
[41]	Hybrid	Yes	No	Fake message, Bad-mouthing attack
[43]	Entity-centric	Yes	No	Tampering attack, Black hole attack
[44]	Hybrid	Yes	No	Compromised nodes, Bad-mouthing attack, Zigzag attack
[45]	Hybrid	Yes	No	Fake message attack
[46]	Entity-centric	Yes	Yes	Fake message attack, Bad-mouthing attack, Sybil attack, and compromised RSUs
[47]	Entity-centric	Yes	No	Malicious vehicles, Collusion attack
[48]	Entity-centric	Yes	No	Fake message attack, reject cooperative attack and compromised RSUs
[49]	Entity-centric	Yes	No	Bad-mouthing attack, identity Spoofing attack, data tampering, and compromised RSUs

Abbreviation: RSU, roadside unit.

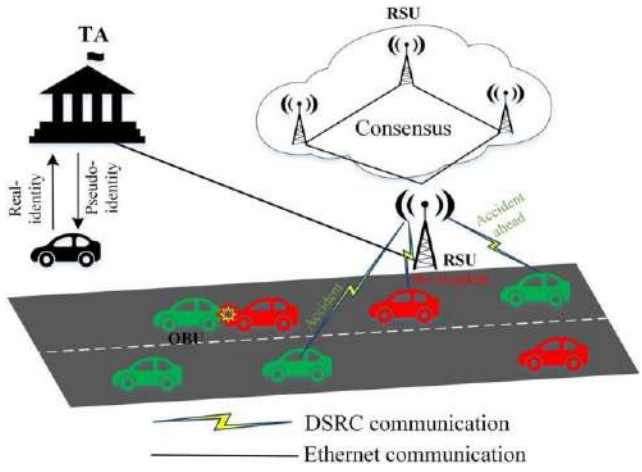

FIGURE 1 Network model. DSRC, dedicated short range communication; OBU, onboard unit; RSU, roadside unit

3.2.2 | Data structure of the trust blockchain

A distributed ledger transaction pool accumulates the unconfirmed transactions created by RSUs throughout the network over time. When the transactions pool has been processed, the system generates the list of vehicles and their trust values. A MPT structure [51] is introduced as part of the proposed system in order to improve efficiency. The data structure is shown in Figure 3. This is an enhanced MPT, which is a mixture of Merkle trees and Prefix trees, arranged chronologically, geographically, and hierarchically. MPT leaf nodes record two items, one is the vehicle public address and the other is the trust value. $Addr_i$ is the vehicle's public address, which is its pseudonym. Every leaf node is indexed by a branch node. The root node contains the RSU zone. The block header contains the previous block's hash, the timestamp, the nonce, the RSU ID, and the root hash of the corresponding MPT. The creator or miner of a new block is the first RSU to find the nonce in the same zone. Upon generating a new block, the miner broadcasts it to all RSUs in the same zone. Thus, every RSU within the same zone can verify the new block based on the nonce.

3.3 | Design goals

Authentication: Security services, such as authentication, integrity, and nonrepudiation, must be provided by the proposed scheme in order to cope with bogus message attacks, replay attacks, and other attacks [52]. A receiver should make sure that the received message has not been forged or replayed, and the sender's pseudonym has not

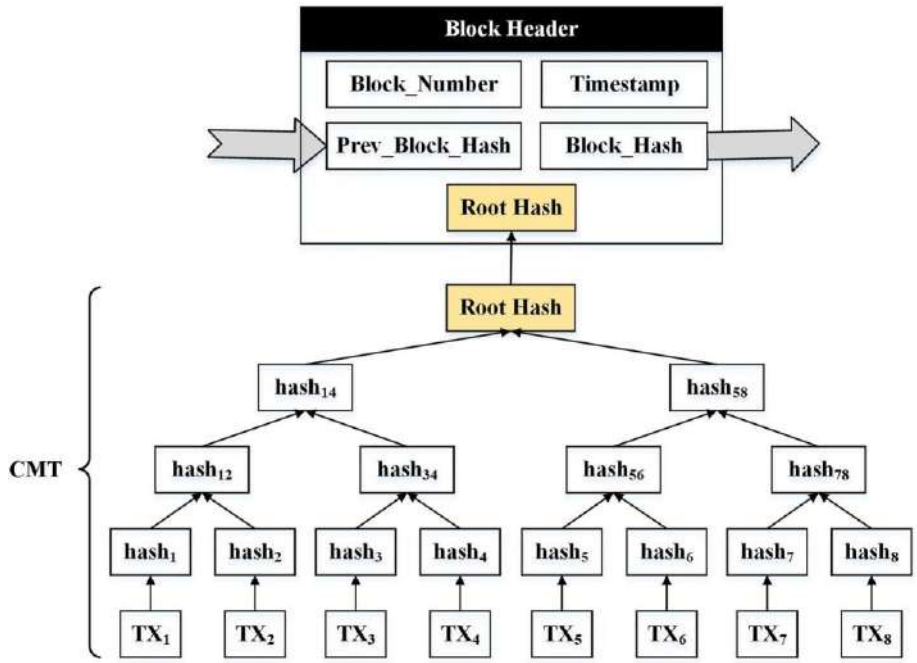

FIGURE 2 Data structure of the proposed authentication blockchain. CMT, chronological Merkle tree

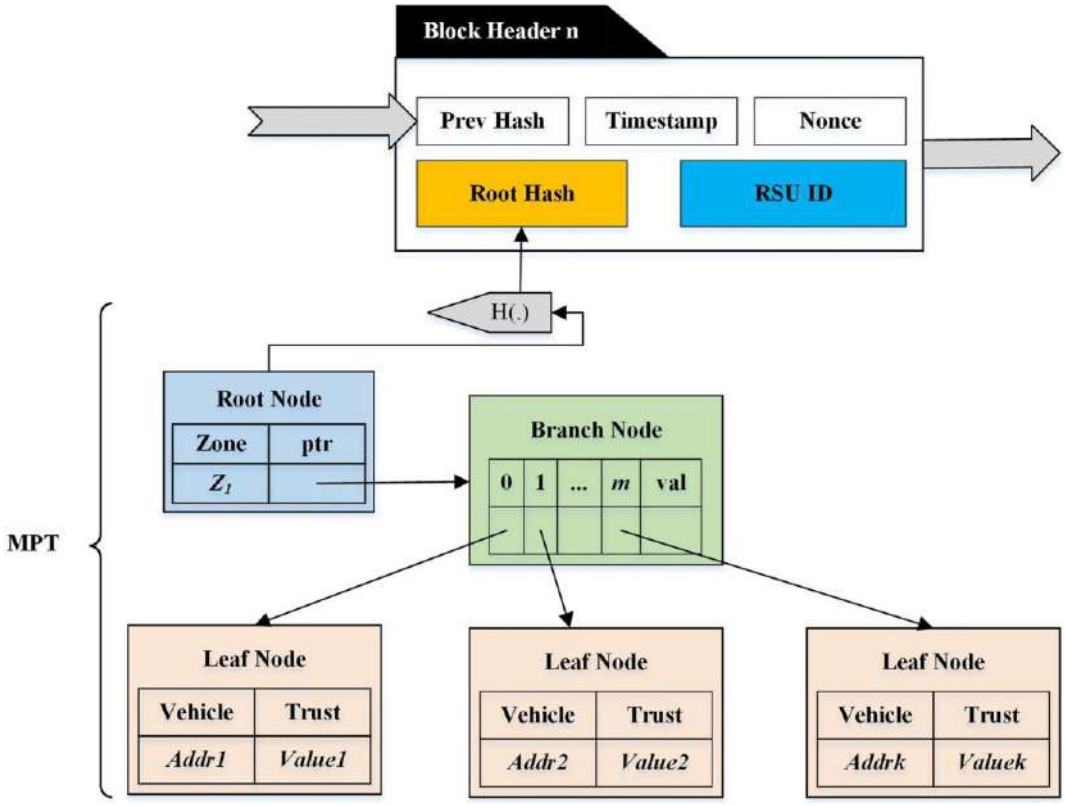

FIGURE 3 Data structure of the proposed trust blockchain. MPT, Merkle Patricia tree; RSU, roadside unit

been revoked by the TA. Furthermore, the sender should be unable to deny sending the message.

Conditional Privacy: First, the identity privacy of a vehicle needs to be protected so that an attacker cannot deduce the target vehicle's real identity from the broadcasted messages. Second, privacy should be conditional. If a malicious activity has been detected, the TA is capable of tracing and disclosing the malicious vehicles' real identity.

Efficiency and Robustness: The authentication scheme should have low computation and communication overhead. The authentication scheme and trust model

should be capable of efficiently determining the authenticity and reliability of reported event messages as well as being resilient to attacks such as false messages, replay, and impersonation.

4 | ADVERSARY MODEL

The adversary considered in this study is the malicious vehicle. The vehicular network may contain a large number of malicious vehicles. They usually have specific goals and attempt to disrupt the network's normal operation. Malicious vehicles may aim to intercept normal data transmissions, alter or forge data, mislead honest vehicles by sending bogus messages, and so on. The safety and efficiency of honest vehicles can be compromised by the misbehaviours of the malicious vehicles. This paper discusses four main categories of malicious vehicle behaviours:

(a) ***False message attacks:*** These attacks are performed by malicious vehicles (inside attackers) who have valid credentials. They launch a false message attack by distributing bogus alert messages claiming a non-existent accident [5, 53]
(b) ***Privacy attack:*** Attackers obtain vehicles' sensitive information by analysing the content of messages [5, 54]
(c) ***Impersonation:*** An attacker attempts to pass itself off as another node. To receive its messages or to gain access to privileges that it is not entitled to [5, 53]
(d) ***Message replay attack:*** Valid messages that have already been sent may repeatedly be reinjected by attackers to disrupt transportation [55]
(e) ***Sybil attack:*** In order to influence the trust assessment, the malicious vehicle generates multiple feedbacks on a single event using multiple pseudonyms [56]

Algorithm 4 depicts a formal adversary model with a false message attack.

Algorithm 4: Formal adversary model with a false message attack

$V = \{V_1, V_2, ..., V_n\}$, Set of n vehicles on road;
$A = \{A_1, A_2, ..., A_m\}$, Set of m malicious vehicles on the road;
Where $A \subset V$;
t_s =Start time of attack;
t_e =End time of attack;
for j =1 to m **do**
  for t = t_s to t_e **do**
    A_j creates False Message "M_F";
    A_j transmits M_F at time (t_{send});
  end for
end for

5 | AUTHENTICATION SCHEME

Figure 4 shows the sequence diagram of message exchange between vehicle, RSU and TA.

5.1 | System initialization

Our system is made of three participants, the TA, RSU, and the vehicles V_i where i = {1, 2, 3, …, n}. We adopt a blockchain namely authentication blockchain. The TA utilizes ECC to initialize the system and set up parameters as below.

1. TA takes generator P, cyclic group G of a large prime order q as input then generates elliptic curve $E : \delta y^2 \frac{1}{4} x^3 \text{ þ } ax \text{ þ } b\text{Þ} \bmod p$. Where $a; b \in Z_q^*$ and $\delta 4a^3\text{þ } 27b^2 \text{Þmod } p \neq 0$
2. Randomly chooses $s \in Z_q^*$ as the master secret key msk and calculates the public key as $T_{pub}\frac{1}{4}sP$
3. Finally, TA selects cryptographic hash functions $H_1; H_2; H_3 : \text{f0; 1g}^* \rightarrow Z_q^*$ and publishes $\text{f}H_1; H_2; H_3; p; q; P; G; E; T_{pub}\text{g}$ as system parameters

The notations used in this scheme are listed in Table 2.

5.2 | Vehicle registration

As part of registration, the vehicle V_i submits its real identity RID_i, as obtained from the motor vehicle's manufacturer (MVM) to TA through a secure channel. The TA confirms with MVM whether RID_i is genuine and if it is, TA will choose a random integer $t_i \in Z_q^*$ and generate a corresponding pseudonym $PID_i \frac{1}{4} \delta PID_{i1}; PID_{i2}\text{Þ}$ as below.

$PID_{i1} \frac{1}{4} t_i P$, $K_i \frac{1}{4} t_i T_{pub} \oplus RID_i$, $PID_{i2} \frac{1}{4} RID_i \oplus H_1 \delta PID_{i1}; T_i \text{Þ}$. After identity verification and pseudo-identity generation, the TA computes a hash function $h \frac{1}{4} H_1 \delta RID_i \oplus PID_i \oplus s \text{Þ}$ and store it together with RID_i and PID_i in its database. Next, TA selects a random integer $r_i \in Z_q^*$ and shares it with V_i and RSU_i, and then, the partial private key ppk_i for the vehicle V_i is calculated as follows. $R_i \frac{1}{4} r_i P$, $u_{1i} \frac{1}{4} H_1 \text{ } PID_i; R_i; T_{pub} \text{ }, ppk_i \frac{1}{4} \delta r_i \text{ þ} s\, u_{1i} \text{Þmod } p$. TA sends $\text{f}PID_i; ppk_i; R_i\text{g}$ to V_i and V_i saves it in its OBU. After receiving a partial private key ppk_i from TA, V_i selects a secret value $x_i \in Z_q^*$ and it generates both public key PK_i and private key SK_i by computing $X\frac{1}{4} x_i P$, $u_{2i}\frac{1}{4} H_2\delta X_i; PID_i\text{Þ}$, $D_i \text{ } \frac{1}{4} u_{2i} \text{ þ} x_i$. Finally, V_i sets public key $PK_i \text{ } D_i; R_i \text{ } \frac{1}{4} \delta \text{ þ}$ and private key $SK_i \frac{1}{4} p\delta pk_i; x_i \text{ þ}$ Similarly, The TA is responsible for RSU_i registration, generation and distribution of its public key PU_i and private key PR_i pairs. It does so by randomly picking a number $n_r \in Z_q^*$ and computes $N_r \frac{1}{4} n_r P$. It then sets $PU_r \frac{1}{4} N_r$ and $PR_r \frac{1}{4} n_r$.

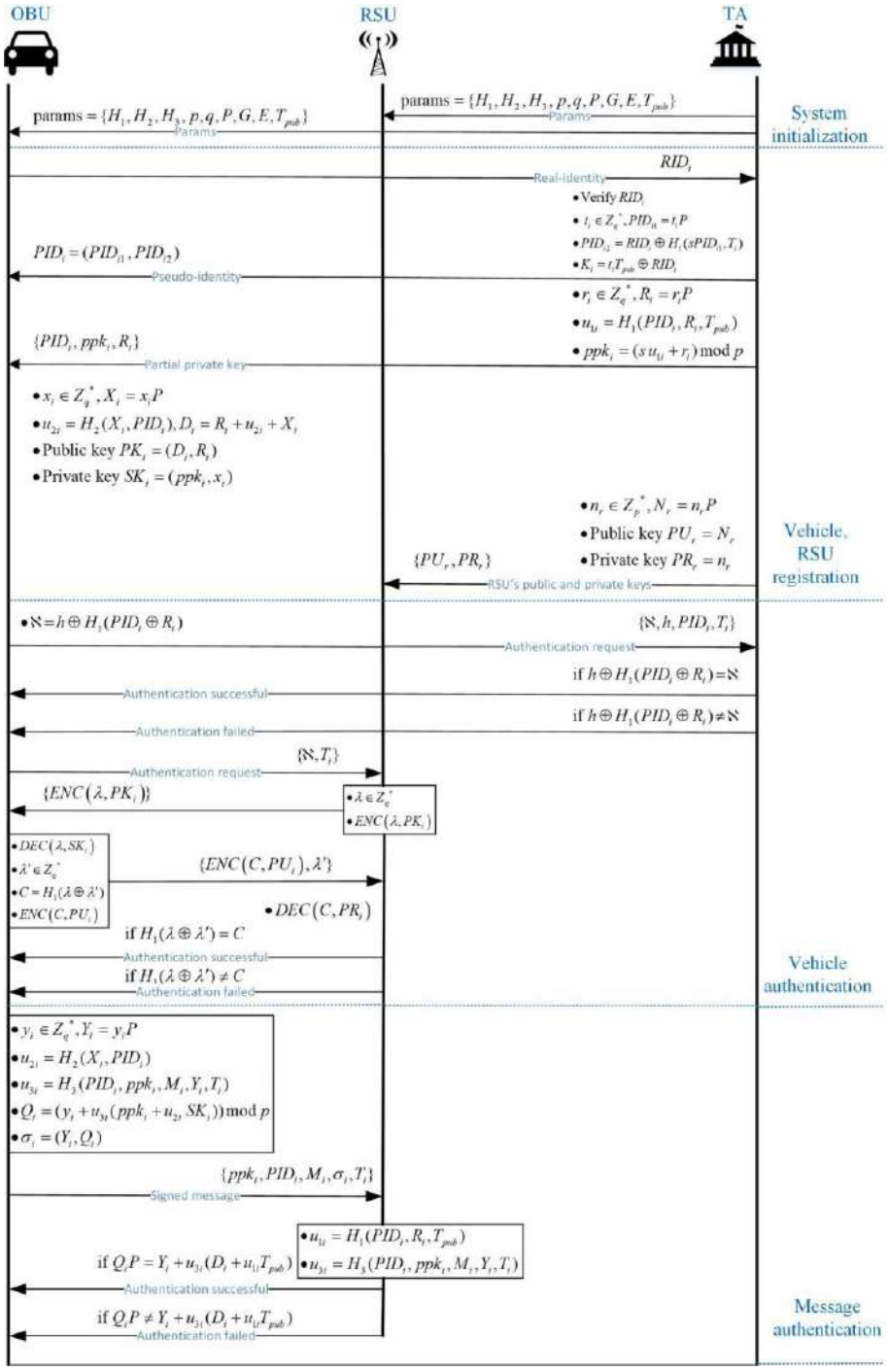

FIGURE 4 Sequence diagram of message exchange between vehicle, RSU and TA. OBU, onboard unit; RSU, roadside unit; TA, trusted authority

5.3 | Vehicle authentication

To ensure only legitimate vehicles participate in communication, the vehicle V_i must be authenticated by TA at the time of joining the network as follows: V_i calculates a value $N = h \oplus H_1(PID_i \oplus R_i)$ and sends a message containing N, h, PID_i and timestamp T_i to TA requesting for authentication. Upon receiving the message, TA checks the timestamp T_i to confirm the freshness of the request. Then, it verifies if h and PID_i corresponds to the same vehicle as recorded in its database. If the details match, it checks if $h \oplus H_1(PID_i \oplus R_i) = N$ holds. If the equation holds, the authentication of the vehicle V_i is successful else the vehicle is revoked and a revocation tag is added to its PID_i. After V_i is authenticated successfully, TA stores $N = h \oplus H_1(PID_i \oplus R_i)$ as a new transaction in its memory pool, later these transactions are mined and added to the authentication blockchain. Whenever vehicle V_i enters the range of a new RSU, it will again be authenticated using the steps below.

TABLE 2 Notations

Notation	Description
RSU_i	Roadside unit i
V_i	Vehicle i
G	The cyclic additive group formed on elliptic curve cryptography
G_1	The cyclic additive group formed on bilinear pairing
P	G-Generator
E	An elliptic curve
$p; q$	Two large and secure prime numbers
RID_i	The real identity of the vehicle V_i
PID_i	Pseudo-identity of the vehicle V_i
$T_{pub}; s$	Public and master secret keys of trusted authority
$PK_i; SK_i$	Public and private keys of V_i
$PU_i; PR_i$	Public and private keys of RSU_i
ppk_i	The partial private key of V_i
$H_i(:); i = 1; 2; 3$	The cryptographic one-way hash function
T_i	Timestamp
M_i	Event message from V_i
σ_i	Signature from V_i on M_i
λ	A challenging integer between V_i and RSU_i
$\oplus$	Exclusive OR operator

Abbreviation: RSU, roadside unit.

- V_i will send a message $\{N; T_i\}$ to RSU requesting authentication
- After receiving the message, RSU checks if N exists in the authentication blockchain as updated by TA. If yes, the RSU choses a random integer λ as a challenger, then encrypts λ using V_i public key PK_i as $ENC(\lambda; PK_i)$ and send it to V_i
- When V_i receive the challenger, it decrypts it using its private key as $DEC(\lambda; SK_i)$, generates another random challenger λ^0, and calculates the hash value of the two random challengers as $C = H_1(\lambda \oplus \lambda^0)$. Next, V_i encrypt a hash value C using RSU public key PU_i and send $\{ENC(C; PU_i); \lambda^0\}$ to RSU
- The RSU decrypts the received ciphertext using its private key PR_i as $DEC(C; PR_i)$ and check if $H_1(\lambda \oplus \lambda^0) = C$ holds. If true, vehicle V_i is authenticated and can participate in communication within the RSU range

5.4 | Message authentication

In order to ensure message integrity, the vehicle V_i must sign every message M_i before it is forwarded to any vehicle or RSU. On inputs of pseudo-identity PID_i, partial private key ppk_i, private key SK_i message M_i, and current timestamp T_i, vehicle V_i output a signature σ_i as below.

Vehicle V_i chooses a random integer $y_i \in Z_q^*$ and computes $Y_i = y_i P$, $u_{2i} = H_2(X_i; PID_i)$, $u_{3i} = H_3(PID_i; ppk_i; M_i; Y_i; T_i)$, $Q_i = (y_i + u_{3i}(ppk_i + u_{2i} SK_i)) \bmod p$, $\sigma_i = (Y_i; Q_i)$.

V_i sends $\{ppk_i; PID_i; M_i; \sigma_i; T_i\}$ to a nearby node that is, RSU_i for authentication. As soon as RSU_i receives the message, it authenticates it by checking T_i for freshness. If this condition is met, then it calculates $u_{1i} = H_1(PID_i; R_i; T_{pub})$, $u_{3i} = H_3(PID_i; ppk_i; M_i; Y_i; T_i)$ and verifies $Q_i P = Y_i + (u_{3i} D_i + u_{1i} T_{pub})$. If the equation holds the verifier accepts the message, otherwise it is discarded.

6 | TRUST MODEL

6.1 | Application scenario

VANETs enable vehicles to share road-related messages such as accidents and traffic congestion to the nearest RSU to timely inform nearby vehicles. When a vehicle encounters a traffic accident, it sends a message to the nearest RSU. However, unreliable messages may be generated by vehicles. RSUs must evaluate these messages for trustworthiness, calculate direct and indirect trust between participants, and verify the reliability of the messages. Next, the RSU checks

the correctness of this event. Based on this scenario, no accident exists. Therefore, any vehicle that reports the accident to the system is either defective or malicious. If the message's credibility is not properly evaluated, road accidents or traffic jams may occur because most vehicles could be misled and incorrectly redirected to the same route if bogus traffic alerts go undetected and thus have a negative impact on VANETs. Therefore, it is of primary importance to secure VANETs so that they can better support intelligent transportation applications.

6.2 | Details of the trust model

Step 1: Calculating the trust of the sender

Three metrics are used to calculate the trust score: old trust, direct trust, and recommendation trust. The old trust is collected from the trust blockchain, the second one is based on reports sent by each vehicle to the RSU, and the last is the recommendation trust, which is defined as the ratio of vehicles that agree with the message. A proof of work distributed consensus mechanism will be performed to guarantee consistency of data accessed by RSUs.

The RSU calculates the direct trust and recommendation trust of the sender and retrieves its old trust value from the blockchain. Recommendation trust is also referred to as indirect trust. Direct trust represents a ratio between the number of true messages A_s and the total number of messages B_s reported by a vehicle V_i in a given period of time. The current direct trust is given by

$$T_{dir} = \frac{A_s}{B_s} \quad (1)$$

The recommendation degree $\mathrm{Re}\, c_s(RSU_i; V_i)$ is given by

$$\mathrm{Re}\, c_s(RSU_i; V_i) = \frac{Affirm_s(V_i)}{Affirm_s(V_i) + Contradict_s(V_i) + 1} \quad (2)$$

$Affirm_s(V_i)$ is the number of vehicles that affirm the message sent by the vehicle V_i to the RSU. $Contradict_s(V_i)$ is the number of vehicles that contradict the message sent by the vehicle V_i to the RSU.

The trust value of the vehicle V_i is computed by RSU_i as follows:

$$t_s(RSU_i; V_i) = \sqrt{T_{dir} \cdot T_{old}} \cdot \mathrm{Re}\, c \quad (3)$$

We summarize the trust computation within the proposed trust model in Algorithm 1.

Step 2: Calculating the trustworthiness of report

The RSU receives event reports from different vehicles. It assesses the credibility of the reported event whether it is true or not. Once the information about an event is received, the RSU creates two sets and name them as event set-1 or no-event set-0. Set-1 contains the reports claiming the event is true, whereas set-0 contains the reports claiming that the event has not occurred. Let us say that the RSU has L vehicles in set-1 and K vehicles in set-0 with the trust value of each vehicle obtained from Equation (3) as $t_s(RSU; V_i)$ at the time s. The average trust of sets is given by

$$T_1 = \frac{\sum_{i \in L} t_s(RSU; i)}{L + 1}; \; T_0 = \frac{\sum_{j \in K} t_s(RSU; j)}{K + 1} \quad (4)$$

The weight, W, of the ith and jth vehicles in L and K, respectively, is calculated as

$$W_s(i) = \frac{t_s(RSU; i)}{T_1} \; ; \; W_s(j) = \frac{t_s(RSU; j)}{T_0} \quad (5)$$

The weighted mean of senders' trust values in set-1 is determined by

$$T_{avg1} = \frac{W_s(i) \cdot t_s(RSU; i)}{L} \quad (6)$$

Similarly, the weighted mean of trust values of senders in Set-0 is given by

$$T_{avg0} = \frac{W_s(j) \cdot t_s(RSU; j)}{K} \quad (7)$$

If the following decision rule holds, the event is considered to have occurred

$$T_{avg1} - T_{avg0} > 0 \quad (8)$$

where $0 \le T_{avg0}$ Or $T_{avg1} \le 1$. The RSU will announce the event to the vehicles within its communication range. Once the correct event has been identified by the RSU, it calculates the anomaly ratio (AR) of any sender with whom it interacted. AR is a measure of a sender's behaviour based on the ratio of anomalies introduced by that sender. If the vehicle V_i sends I_s incorrect messages out of total B_s messages sent by the vehicle V_i till the current time. The current anomaly ratio AR_S is given by

$$AR_s = \frac{I_s}{B_s} \quad (9)$$

Therefore, the receiving RSU will check the AR value and classify the sender as malicious or honest accordingly. If the calculated AR is greater than a threshold λ and its trust value $t_s(RSU; V_i) < T_{thr}$, the sender is considered malicious. Then, the RSU puts malicious vehicles on the warning list. Finally, RSU attempts to store the trust values of the senders into the

blockchain. We summarize event report trustworthiness evaluation performed in this step in Algorithm 2.

Step 3: The mining process

This process allows all RSUs to compete for trust updates, that is, adding a trust block. Once the RSU has calculated the trust value for a message sender, it adds the new trust value into a block and tries to add it into the blockchain. If multiple RSUs attempt to add their blocks at the same time, the mining process will begin to determine who will add the block to the blockchain. In order for an RSU to be elected as the miner, it must obtain the following hash value: criterion Hash (timestamp, prevHash, nonce) < C. Where timestamp is the current time in the system, prevHash is the hash value of the previous block, the nonce is an arbitrary hexadecimal number and C is the target difficulty that controls block generation speed. Immediately after finding a nonce that meets the target criterion, the RSU will be elected as the miner. The miner creates a block of trust values and digital signatures, then adds the block to the blockchain. The blockchain uses a consensus mechanism to allow the miners to ensure data consistency. To reach a consensus, the new block will be accepted by other RSUs and added to their blockchains if it meets the target criterion and the attached digital signatures are verified. Other than that, the block is discarded and another miner is chosen. Further, Algorithm 3 summarizes the mining process to generate a block to be added to the blockchain.

Step 4: Revocation

RSUs take certain actions against vehicles whose trust values are lower than a threshold (e.g. warning and revocation). Therefore, vehicles having trust values lower than τ and their AR is greater than the threshold λ will be put into the warning list. If the vehicle still sends bogus messages, it will be put into the revocation list and TA takes action according to the revocation list. The vehicular network will not provide any services to any revoked vehicles.

Algorithm 1: Trust calculation

Input: RSU receives event reports from different vehicles.
Output: Trust $t(RSU, V_i)$ of vehicle V_i;
1 Create two event sets: Event Set-1 and No-Event Set-0;
2 Calculate the direct trust T_{dir} using Equation (1);
3 Calculate the recommendation trust $Re\ c_s(RSU, V_i)$ using Equation (2);
4 Retrieve the old trust value T_{old} of V_i from the blockchain;
5 Calculate the total trust of V_i using Equation (3);

Algorithm 2: Event report trustworthiness evaluation

Input: RSU receives event reports from different vehicles, Trust value $t_s(RSU, V_i)$, Trust threshold(T_{thr}), the anomaly ratio threshold (λ);
Output: Event Verification;
1 Create two event sets: Event Set-1 and No-Event Set-0;
2 Calculate the average trust of No-Event Set-0 and Event Set-1 using equation 4;
3 Calculate the weight of the i^{th} and j^{th} senders' trust in No-Event Set-0 and Event Set-1 using equation 5;
4 Calculate the WEIGHTED_MEAN of senders' trust values in Set-1 using equation 6;
5 Calculate the WEIGHTED_MEAN of senders' trust values in Set-0 using equation 7;
6 **If** *(The decision rule in equation 8 holds)* **then**
7 Announce event notifications to the vehicles within its communication range;
8 **end**
9 Calculate the anomaly ratio of every sender using equation 9;
10 **If** $(AR(V_i) > \lambda$ *and* $t_s(RSU_i, V_i) < T_{thr})$ **then**
11 The sender is considered malicious;
12 Put malicious vehicles on the warning list;
13 Send warning list to TA;
14 **end**

Algorithm 3: Mining process and Consensus

```
Input: previousBlock, RSU_ID, Transactions: Tx1, Tx2, …,Txn, target criterion: C; Result: Block;
Timestamp = T;
prevHash = Hash(previousBlock);
Root_Hash = create_MPT_Tree (transaction_pool.getAllTransactions);
do
    nonce = random_number();
    Cond = Hash (Timestamp, prevHash, nonce);
    if Cond < C then
        Node = miner;
        block = create_Block(Timestamp, prevHash, Root_Hash, RSU_ID, nonce);
        blockchain.add(block);
        RSU_Sig = sign_block(block);
        publish_Block(block, nonce, RSU_Sig);
    end
Until Node = = miner;
if Node ! = miner then
    receive_Block(block, nonce, RSU_Sig);
    verify_Signature(RSU_Sig);
    if Hash (timestamp, prevHash, nonce) < C then
        block_status = valid;
        blockchain.add(block);
    else
        block_status = not_valid;
        discard_Block(block);
    end
end
```

7 | SECURITY ANALYSIS

7.1 | Privacy-preserving

In our scheme, TA is the only one who knows the vehicle's real identity RID_i. V2V and V2I communications are performed using pseudo-identities PID_i. These pseudo-identities are generated using secret values s and t_i are only known by TA ensuring no malicious vehicle or RSU can extract RID_i from PID_i.

7.2 | Traceability

Although our scheme preserves the privacy of vehicles using their pseudo-identities PID_i, this privacy is conditional. In case of malicious activities (e.g. attacks) and accidents, the TA can determine the real identity of a vehicle from TA's $PID_i - RID_i$ database or from its pseudo-identity as $RID_i = K_i \oplus sPID_{i1}$. Thus, TA can trace the real identity of any vehicle if the need arises.

7.3 | Authentication

The RSU in our scheme is capable of determining whether a vehicle is malicious or not by checking the presence of $N = H_1(PID_i \oplus R$ in the authentication blockchain maintained by TA. If the N is present, the sending vehicle is legitimate otherwise the sender is a malicious vehicle and legal action is taken on it. Therefore, our scheme supports source authentication by authenticating vehicles using authentication blockchain.

7.4 | Integrity

The proposed scheme requires every message to be signed $\{PID_i, ppk_i, M_i, \sigma_i, T$ by the sender before it is broadcasted within the network. Subsequently, every receiver must verify the signature on the message as $Q_iP = Y_i + u_{3i}D_i = u_iP + T_{pub}$ before taking action. Since the signature σ_i is generated using the secret key SK_i and random integer $y_i \in Z_q^*$ only known to the sender, no attacker can forge a valid signature. Therefore, our scheme assures that messages sent by a legitimate sender have not been tampered with.

7.5 | Non-repudiation

Since TA can link a message's real and pseudo-identities, it would not be possible for any vehicle to deny that it has signed the message.

7.6 | Unlinkability

The verifier V_i in our scheme sends $\{ppk_i, PID_i, M_i, \sigma_i, T_i\}$ to a nearby RSU. Due to the signature of σ_i has a random value of y_i, no attacker can link two messages from the same vehicle. Therefore, the proposed scheme meets the requirement of unlinkability.

7.7 | Anti-false message attack

Malicious event messages can be generated and sent to the RSU by malicious vehicles. The trust model on the RSU ensures only true event messages are broadcasted to the vicinity.

7.8 | Sybil attack

Multiple submissions of feedback from the same vehicle of the same message to the RSU will be prevented by pseudonym authentication. Therefore, Sybil will not be successful.

7.9 | Resistance to other attacks

The proposed scheme can resist both replay attacks and impersonation attacks by applying time stamps T_i, random secret values, and signatures on each message sent, and also the use of authentication blockchain.

8 | RESULTS AND DISCUSSION

We evaluated the efficiency of the authentication scheme in terms of computation and communication overhead, which are widely used metrics in the literature. To make VANETs economically viable, embedded OBUs in vehicles use processors with limited computation capability. Therefore, in VANETs, cryptographic operations should perform a limited computational overhead (should be lightweight) [57]. Low computational and communication overhead are two of the most important requirements for providing efficient authentication.

We evaluated the trust model from the perspective of accuracy since the trust model is designed to assist RSUs to distribute authentic, accurate, and trustworthy information within the network. Therefore, we have used three metrics (precision, recall, f-measure for evaluating accuracy), which are considered to be the most essential criteria for evaluating trust in highly mobile networks, such as VANET. Moreover, we considered the false positive rate (FPR) metric. The vehicle's trust value or status within the network can be adversely affected by false positives. The accuracy of assessment and evaluation results would be improved if there is a method to

detect false positives within trust models. Furthermore, when RSU receives event messages, it is necessary to establish a level of confidence as to whether the event in question has actually occurred. Therefore, true and bogus events should be identified correctly in the network [58]. We used the event detection probability (EDP) metric for this purpose. These metrics determine the efficiency and robustness of the trust model in identifying the malicious vehicles and the content they generate, identifying true and false events, and remaining robust despite the growing number of malicious vehicles.

8.1 | Efficiency analysis

To evaluate the efficiency of the authentication scheme, we analyse and compare the computation cost and communication overhead for our scheme and four of the recent interesting VANET schemes.

8.1.1 | Computation cost

To evaluate the computational cost, we consider the time spent signing and verifying a message. The proposed scheme is compared with other closely related schemes [1, 59, 60], and [61] as shown in Table 2. For the analysis of schemes [59, 61], bilinear pairing is defined as $e : G_1 \times G_1 \rightarrow G_T$ where G_1 is an additive group of order q generated by a point P on an elliptic curve $E : y^2 = x^3 + x \bmod p$, p is a 512-bit, and q are 160-bit prime numbers that satisfy the equation $12qr = p + 1$. For the analysis of schemes [1, 60], and proposed, an elliptic curve $E : y^2 = x^3 + ax + b \bmod p$ is used where p, q, a and b are all 160-bit prime numbers. The main cryptographic operations that we consider are bilinear pairing, scalar multiplication and point addition based bilinear pairing, scalar multiplication and point addition based on ECC, and hash functions denoted as T_{bp}; $T_{bp\rightarrow sm}$; $T_{pb\rightarrow pa}$; $T_{ecc\rightarrow sm}$; $T_{ecc\rightarrow pa}$; T_h, respectively. It is assumed that encryption and decryption operations are lightweight; thus, we do not account for them. We utilize the same execution times recorded in the scheme [62], which is based on the well-known MIRACL crypto library [63], to do the analysis. For convenience, the operations are given in Table 3.

To sign a single message, a vehicle in Zhong et al's scheme [59] requires $3T_{bp\rightarrow sm} = 5.127$ ms, He et al's scheme [1] requires $3T_{ecc\rightarrow sm} + T_h = 1.3263$ ms, Kamil et al's scheme [60] needs $3T_{ecc\rightarrow sm} + 2T_{ecc\rightarrow pa} + T_h = 1.3297$ ms, Bayat et al's scheme [61] requires $3T_{bp\rightarrow sm} + 1T_{bp\rightarrow pa} = 5.1341$ ms while our proposed scheme needs $1T_{ecc\rightarrow sm} + 1T_h = 0.4422$ ms, which is much less time compared to other schemes. To verify a single message, scheme [59] requires $3T_{bp} + T_h + 2T_{bp\rightarrow sm} = 16.0511$ ms, scheme [1] requires $3T_{ecc\rightarrow sm} + T_h + 2T_{ecc\rightarrow pa} = 1.3298$ ms, scheme [60] requires $2T_{ecc\rightarrow sm} + T_{ecc\rightarrow pa} + T_h = 0.8859$ ms, scheme [61] requires $3T_{bp} + T_{bp\rightarrow pa} = 12.6401$ ms, whereas the proposed scheme needs $3T_{ecc\rightarrow sm} + 2T_{ecc\rightarrow pa} + T_h = 1.3298$ ms. According to Table 3, it takes 1.7716 ms to sign and verify a single message by the proposed scheme, which is 91.63%, 33.29%, 20.02% and 90.03% more efficient than schemes [1, 59], [60, 61] respectively. Therefore, the proposed scheme is more effective than other schemes. Table 4 shows the comparative analysis.

8.1.2 | Communication overhead

Our computation of communication overhead for the schemes is based upon evaluating the following parameters: the type of curve used in the scheme, the size of elements in the group, and the order of the cyclic group. As defined earlier, p in a bilinear pairing-based scheme is 512 bits while p in ECC-based schemes is 160 bits. Meaning, the size of elements in G_1 is $p = 512 \div 8 = 128$ bytes and G is $p = 160 \div 8 = 40$ bytes. We assume the size of the one-way hash function is 20 bytes and the size of the timestamp is 4 bytes. The Communication overhead is calculated by adding the size of pseudo-identity, partial private key, private key, signature, and timestamp only but excluding message since it is of constant size in all the schemes. A message in Ref. [59] comprises $\{PID_i, vpk_i, t_i, \sigma_i\}$ where $PID_i = \{PID_{i1}, PID_{i2}, t_i\}$, $PID_{i1} \in G$, $vpk_i \in G$, $\sigma_i = \{R_i, T_i\} \in Z^*_q$ and t_i is a timestamp. Hence, its overhead is $128 + 2 \times 20 + 4 = 320$ bytes. The message in [1] is made of $\{AID_i, T_i, R_i, \sigma\}$ where $AID_i = \{AID_{i1}, AID_{i2}\}$, $AID_{i1}, AID_{i2}, R_i \in G$, $\sigma_i \in Z^*_q$ and T_i is a timestamp. Therefore, its overhead is $3 \times 40 + 20 + 4 = 144$ bytes. In Ref. [60], a message sent to verifier is $\{PID_{y;k}, PK_k, \omega_k, \sigma_k = (R_k, v_k), T_k\}$ where $PK_k, R_k \in G$, $PID_{y;k}, \omega_k, v_k \in Z^*_q$ and T_k is a timestamp. Hence, its overhead is $2 \times 40 + 3 \times 20 + 4 = 144$ bytes. The size of a single message in the scheme [61] is $\{V, r, T_{i1}, T_{i2}, T_{i3}, PID_i, ts_i\}$ where $r \in G_1$ $V, T_{i1}, T_{i2}, T_{i3}$, $PID_i \in Z^*_q$ and ts_i is a timestamp. Thus, its overhead is $128 + 5 \times 20 + 4 = 232$ bytes. In the proposed scheme, a message consists of $\{PID_i, ppk_i, T_i, \sigma_i = (Y_i, S_i)\}$ where $PID_i = \{PID_{i1}, PID_{i2}, T_i\}$, $PID_{i1} \in G$, $PID_{i2}, ppk_i, Y_i, S_i \in Z^*_q$ and T_i is a timestamp. Thus, our scheme has a communication overhead of $40 + 4 \times 20 + 4 = 124$ bytes. A summary of the comparisons is listed in Table 5.

As can be seen from the above analysis, the proposed scheme incurs the lowest communication cost. Compared with schemes [1, 59–61], it decreases communication overhead with 61.25%, 13.8%, 13.8% and 46.55%, respectively.

8.2 | Simulation results and discussion

Our simulation environment is built using Veins [64], OMNet ++ [65], and SUMO [66]. In this work, we use precision, recall, F-measure, false-positive rate, and EDP evaluation metrics in order to evaluate the proposed trust model's performance. These evaluation metrics are well-known metrics for validating the results [67, 68].

On the road map, 100 vehicles were deployed. As depicted in Figure 5, 10 RSUs are randomly distributed across the map at fixed points. Each vehicle was given a trust value of 0.3 at the beginning of the experiment, and the reason is that it takes

Notation	Cryptographic operation	Execution time (ms)
T_{bp}	Bilinear pairing	4.2110
$T_{bp\to sm}$	Scalar multiplication based on bilinear pairing	1.7090
$T_{bp\to pa}$	Point addition based on bilinear pairing	0.0071
$T_{ecc\to sm}$	Scalar multiplication based on ECC	0.4420
$T_{ecc\to pa}$	Point addition based on ECC	0.0018
T_h	One-way hash function	0.0001

Abbreviation: ECC, elliptic curve cryptography.

TABLE 3 Executior time of various cryptographic operations

TABLE 4 Comparative analysis of computation cost

Scheme	Signing cost	Cost of verifying a single message	Total execution time(ms)
Zhong et al. [59]	$3T_{bp\to sm} = 5.127$	$3T_{bp} \text{ þ } 1T_h \text{ þ } 2T_{bp\to sm} = 16.0511$	21.1781
He et al. [1]	$3T_{ecc\to sm} \text{ þ } 3T_h = 1.3263$	$3T_{ecc\to sm} \text{ þ } 2T_h \text{ þ } 2T_{ecc\to pa} = 1.3298$	2.6561
Kamil et al. [60]	$3T_{ecc\to sm} \text{ þ } 2T_{ecc\to pa} \text{ þ } 3T_h = 1.3297$	$2T_{ecc\to sm} \text{ þ } 1T_{ecc\to pa} \text{ þ } 1T_h = 0.8859$	2.2156
Bayat et al. [61]	$3T_{bp\to sm} \text{ þ } 1T_{pb\to pa} = 5.1341$	$3T_{bp} \text{ þ } 1T_{bp\to pa} = 12.6401$	17.7742
Proposed	$1T_{ecc\to sm} \text{ þ } 2T_h = 0.4422$	$3T_{ecc\to sm} \text{ þ } 2T_{ecc\to pa} \text{ þ } 2T_h = 1.3298$	1.7720

a long time to identify honest from malicious vehicles if the trust value is set as low as 0.1. Moreover, it will take more time to reduce a malicious vehicle's trust value if it has a high trust value, such as 0.8. As a result, detecting the malicious vehicle will take longer. We found that starting with 0.3 is appropriate because it takes less time to recognize honest vehicles from malicious ones. Each vehicle's communication range is 250 m and each vehicle is travelling at a speed of 10–25 m per second along the road, changing directions randomly at the intersection with no pause time. Furthermore, at a random location in the network, a road event (i.e. an accident) is generated during the movement of vehicles. Nearby vehicles will observe the event and begin sending messages to the nearest RSU within their communication range. However, malicious vehicles attack the network by sending false messages to the nearby RSU claiming there is no accident. Most of the vehicles in the network are legitimate and perform their tasks in a truthful manner. The number of legitimate vehicles is kept constant so we can investigate how the trust model will behave when malicious vehicles are present while increasing the number of malicious vehicles from 10% to 50% in order to validate the proposed trust model's efficiency in identifying malicious vehicles and their false data. RSU calculates each participating vehicle's trust value, identifies the legitimacy of the event, and broadcasts a notification about it to the vehicles in its communication range, and a block containing the vehicles' trust values is disseminated in the blockchain network. Each simulation scenario has 10 runs, each with a different random seed, ensuring that each run has a different initial node location. Each experimental result is the average of the 10 runs for each simulation scenario. Table 6 provides the details of the simulation parameters.

TABLE 5 Comparison of communication overhead

Scheme	Single message overhead	*n* messages overhead
Zhong et al. [59]	320 bytes	320 *n* bytes
He et al. [1]	144 bytes	144 *n* bytes
Kamil et al. [60]	144 bytes	144 *n* bytes
Bayat et al. [61]	232 bytes	232 *n* bytes
Proposed	124 bytes	124 *n* bytes

MARINE [40] evaluates vehicles' trust in two stages. First, the sender node's trustworthiness is evaluated. This is achieved by analysing past interactions with the vehicles and by considering feedback provided by nearby vehicles. Second, once node trust has been computed, data received is evaluated using three distinct factors, (1) the quality of information, (2) the capability of the node to forward messages, and (3) the opinions of neighbours. The sender node's data will only be accepted if both data and node-centric trust have been calculated successfully. Otherwise, the data will be dropped by the evaluator node.

ART [39] evaluates the trustworthiness of both data and nodes in VANETs. The trustworthiness of data is assessed and analysed using the data sensed and collected by various vehicles. Then, the evidence from the data analysis is used in trustworthiness evaluations. Various pieces of evidence that contain both trustworthy and untrustworthy information are combined using the Dempster-Shafer method in a suitable manner. Node trustworthiness is assessed on two levels: functional trust and recommendation trust, which indicate if a node can perform its functions and whether its recommendations to other nodes are trustworthy.

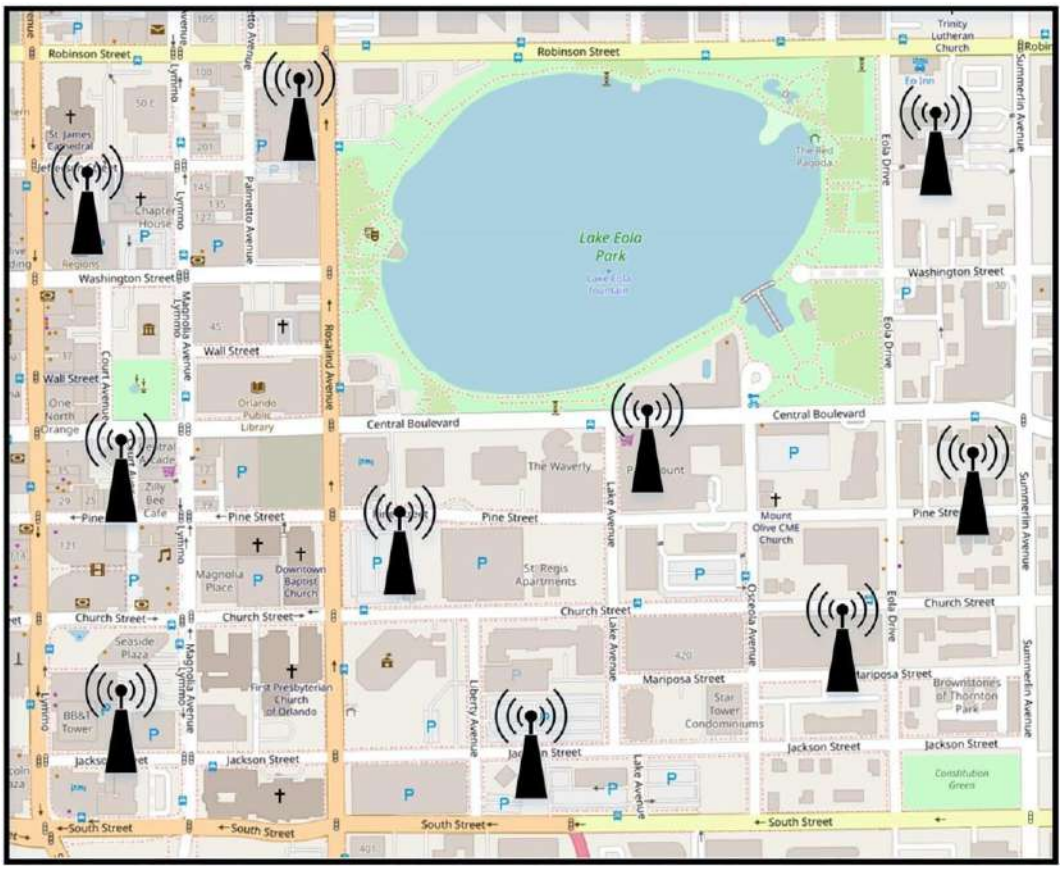

FIGURE 5 Extracted map of Orlando City, USA

TABLE 6 Simulation parameters

Parameter		Value
Simulation details	Simulation area (km ⨯km)	2 ⨯2
	Simulation Time	500 Sec
	Number of RSUs	10
	Communication range	250 m
Scenario	Legitimate vehicles	100
	Malicious vehicles (%)	10, 20, 30, 40, 50
Protocols	Network protocol	IEEE 1609.4
	MAC protocol	IEEE 802.11p
Trust model	Initial Trust(τ)	0.3
	Trust threshold(T_{thr})	0.5
	The anomaly ratio threshold (λ)	0.3
Adversary model	Actions	Create Fake messages

8.2.1 | Precision

Precision is the number of vehicles correctly identified as malicious over the total number of vehicles both correctly and incorrectly identified as malicious [68]. Precision is calculated as given below:

$$Precision = \frac{TP}{TP + FP} \quad (10)$$

where TP denotes the number of correctly identified malicious vehicles while FP denotes the number of incorrectly identified malicious vehicles.

The trust models' accuracy is expressed by precision, recall, and F-measure and shown in Figures 6 to 8. From the figures, it is clear that precision, recall, and F-measure decrease as the number of malicious vehicles in the network increases. The precision of the trust models is shown in Figure 6, showing that the three trust models attain a precision over 90% when the number of malicious vehicles is low, that is, all the trust models can identify malicious messages sent by these malicious vehicles.

In spite of that, this precision decreases below 85% when the network contains a large number of malicious vehicles. Further, the proposed trust model outperforms MARINE and ART by achieving higher precision values. When the network has 50% malicious vehicles, the proposed trust model achieves 9% and 17% higher precision values as compared with MARINE and ART, respectively. In fact, this is because in the proposed trust model, the trust is computed via old trust, direct trust, and recommendation trust. These methods ensure the correct identification of malicious vehicles in the network.

8.2.2 | Recall

The recall is the ratio of the number of vehicles correctly discovered as malicious vehicles, and the total number of malicious vehicles [68]. It is measured as shown below:

$$Recall = \frac{TP}{TP + FN} \quad (11)$$

where TP denotes the number of vehicles correctly identified as malicious vehicles and FN denotes the number of vehicles incorrectly identified as legitimate vehicles.

The proposed trust model outperforms both MARINE and ART with respect to recall as shown in Figure 7. When the network has 50% malicious vehicles, the proposed trust model achieves recall values that are 12% and 19% higher than MARINE and ART, respectively.

8.2.3 | F-measure

F-Measure is used to evaluate the accuracy of the trust models [69]. If the F-Measure is high, the trust model will be more accurate. F-Measure can be calculated as

$$F\_Measure = 2 * \frac{Precision * Recall}{Precision + Recall} \quad (12)$$

This metric can help in evaluating the trust model's accuracy in identifying malicious vehicles and the false messages they generate. Figure 8 illustrates that the proposed trust model can identify false messages with high accuracy even when there is a high number of malicious vehicles.

When 50% of malicious vehicles are present in the network, the proposed trust model achieves 11% and 18% higher accuracy than MARINE and ART, respectively. This is because of the usage of old trust, direct trust, recommendation trust, and the anomaly ratio that have the capability to identify malicious vehicles. Furthermore, the trust model ensures that true event messages are propagated in the network when there is a high number of malicious vehicles.

8.2.4 | False positive rate

FPR is the ratio of the number of legitimate vehicles that are incorrectly identified as malicious while detecting malicious vehicles over the total number of legitimate vehicles [70, 71]. The FPR is represented as

$$FPR = \frac{FP}{FP + TN} \quad (13)$$

where TN stands for the number of vehicles correctly identified as non-malicious and FP stands for the number of vehicles incorrectly identified as malicious. Hence, FPR is considered as

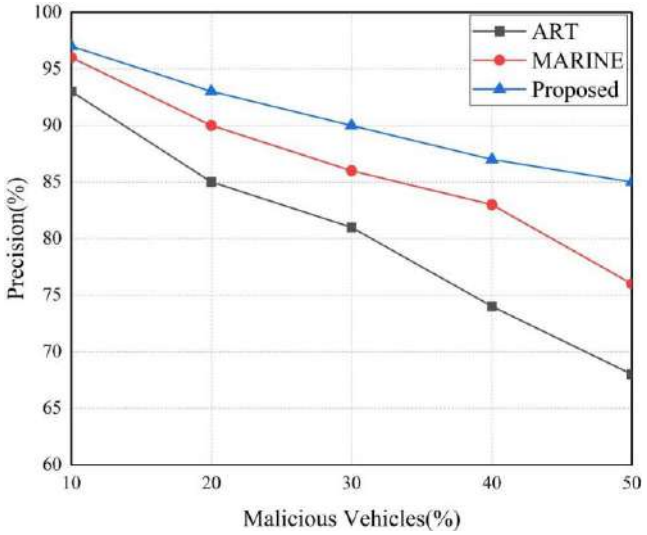

FIGURE 6 Impact of different percentages of malicious vehicles on precision

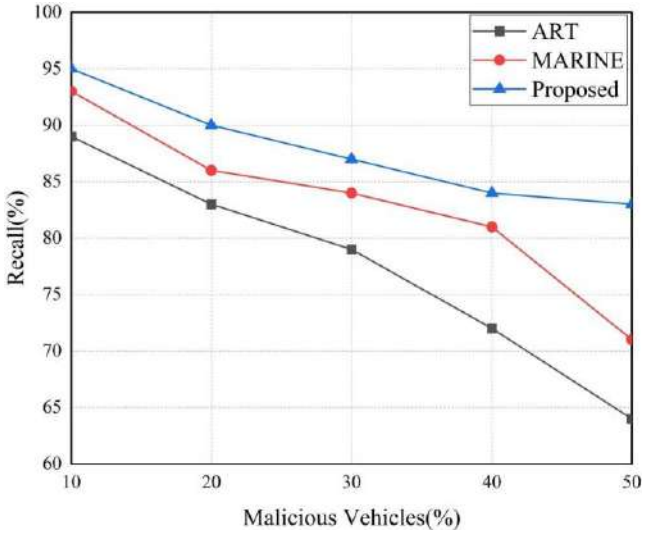

FIGURE 7 Impact of different percentages of malicious vehicles on recall

the error rate within the trust models. Due to the critical information involved in VANETs, trust models with low FPR values are suggested [72].

Figure 9 illustrates the FPR for the three trust models (the proposed trust model, MARINE, and ART). Trust models should maintain FPR at a minimum level in VANET.

It is clearly shown in Figure 9 that low FPR is achieved even when there is a high number of malicious vehicles. However, the proposed trust model performs better than both MARINE and ART where FPR is maintained at a minimum level. As shown in this figure, the average FPR of the proposed model is about 1.78%, whereas it is 3.22% and 4.54%, respectively, for MARINE and ART. This is due to the

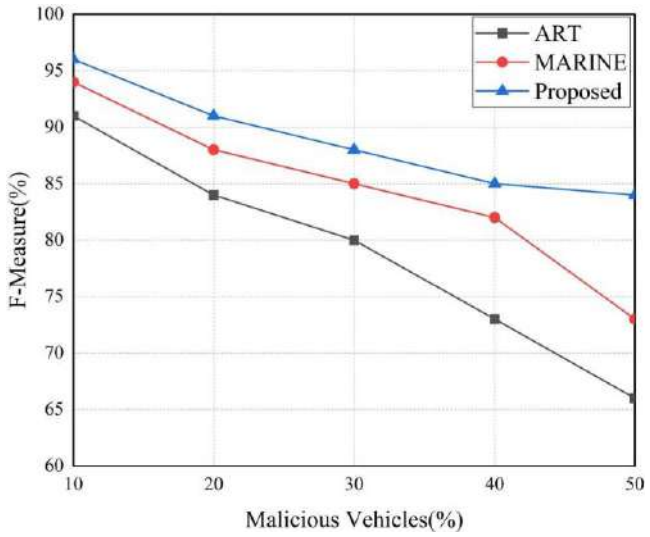

FIGURE 8 F-Measure

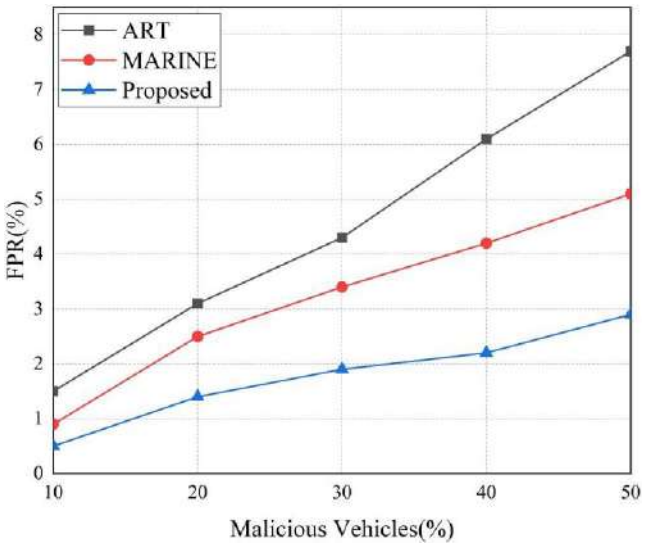

FIGURE 9 False positive rate

proposed trust model that is based on old trust, direct trust, and recommendation for trust computation in addition to adopting the anomaly ratio, therefore, enabling the trust model to efficiently evaluate the received messages and hence classify vehicles accordingly.

8.2.5 | Event detection probability

It has been defined as the ratio of true events to all events within the network. The ability of a trust model to identify true events can be determined by calculating EDP. Trust models should be capable of detecting true events efficiently [58]. The total events generated in the network are denoted by E_{Total}. True and bogus events are denoted by E_{True} and E_{Bogus}, respectively; then, EDP can be calculated by [72]

$$EDP = \frac{E_{Total} - E_{Bogus}}{E_{Total}} \quad (14)$$

When the trust model has a high event detection rate, it is considered to be effective and efficient [72]. There are two types of reports that are sent to the RSU in VANET: true reports that are sent by legitimate vehicles, and bogus reports, which are sent by malicious vehicles. Figure 10 shows the ability of the three trust models to identify true events, indicating that the proposed trust model outperforms MARINE and ART by identifying a high number of true events.

Since the proposed model adopts three measures to calculate trust, it has a high probability to provide accurate information, which results in higher detection rates. For a network with 50% malicious vehicles, the proposed trust model outperforms MARINE and ART and can detect 14% and 27% more events correctly than MARINE and ART, respectively.

8.2.6 | Time consumption of block creation and consensus

Time taken to generate a block determines the efficiency with which trust is evaluated. The difficulty of the consensus process and the number of RSUs are important factors that affect the time taken for reaching consensus. As can be seen in Figure 11, we can see the average time required to create each block and the time spent to reach consensus. The average time for creating blocks increases as the number of RSUs increases. It takes 4.54 ms to create a new block with a maximum of 10 RSUs for a network of 100 vehicle nodes. In our scenario, all remain at milliseconds, which is perfectly acceptable.

8.2.7 | Storage overhead

Figure 12 depicts the block size with a variety of network vehicles. Every 100 s, a block with an average size of 2 KB is created. The overall storage overhead for the entire blockchain is estimated to be 2 * (60/100) * 24 * 365, or 10,512 KB per year. As a result, the solutions proposed require very little storage in the blockchain.

We evaluated and compared the performance of the proposed authentication scheme and the trust model with the other related authentication schemes and trust models. The efficiency of the authentication scheme is evaluated in terms of computation and communication overhead and the accuracy of the trust model is evaluated based on precision, recall, f-measure, FPR, and EDP. It is clearly shown that the proposed authentication scheme outperforms the compared schemes in terms of achieving less computation time, and communication overhead, and the proposed trust model outperforms the compared models (MARINE and ART) by achieving high precision, recall, F-measure, and EDP, and

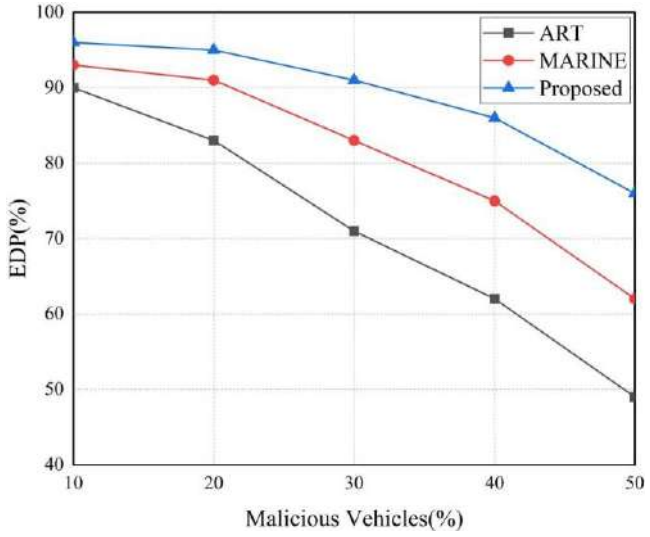

FIGURE 10 Event detection probability

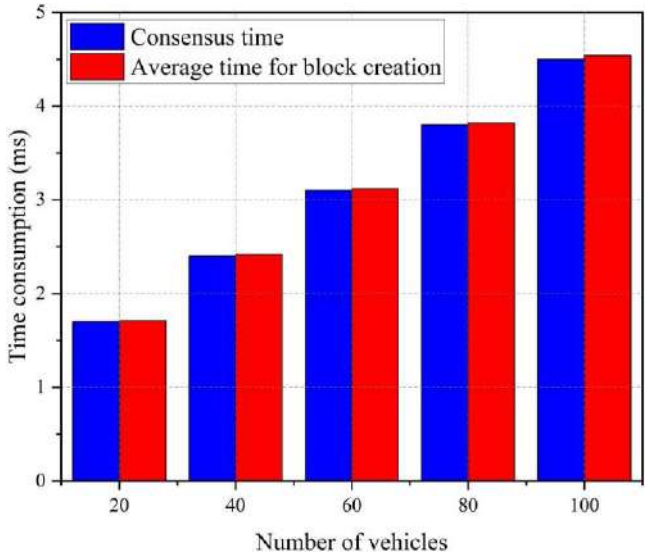

FIGURE 11 Time consumption of block creation and consensus

lower FPR. Moreover, we have analysed the performance of the system in terms of time consumption for block creation and consensus, and the storage overhead in the blockchain.

9 | OPEN CHALLENGES AND FUTURE RESEARCH DIRECTIONS

This section discusses some of the challenges related to trust management in vehicular networks that still need to be addressed in the future:

1. A solution to the 'node initialization' problem for trust management is required. An initial trust value must be assigned to every new node when they are joining the network. New vehicles do not have any historical interaction information, so it is impossible to calculate the trust score based on historical interactions. Existing solutions for trust management assume a static initial value for trust when a node is encountered. An important and challenging problem in trust management models is the allocation of initial trust values to new nodes in a vehicular network
2. Most trust management and establishment schemes compute trust based on the cooperation between nodes and/or authorities. Therefore, in order to encourage nodes to participate in the combined trust evaluation service, there is a need for efficient incentive mechanisms
3. VANET is characterized by random vehicle distribution across the network and high mobility, resulting in various contexts in VANET. For example, due to low vehicle mobility and a large number of RSUs, a large number of messages are present in one location. Other locations, on the other hand, are unable to guarantee RSU's persistent presence. Furthermore, the high mobility and the low number of vehicles in such areas result in a low number of messages. For a low number of vehicles scenario, trust models that rely on a large number of vehicles and RSUs for trust management will perform poorly. As a result, separate techniques for evaluating the trustworthiness of nodes and their messages are required in both scenarios. Only by ensuring secure and trusted messages in all contexts can VANET succeed. Trust management requires solutions that are context-aware in VANETs. Further research is needed in this direction for better solutions

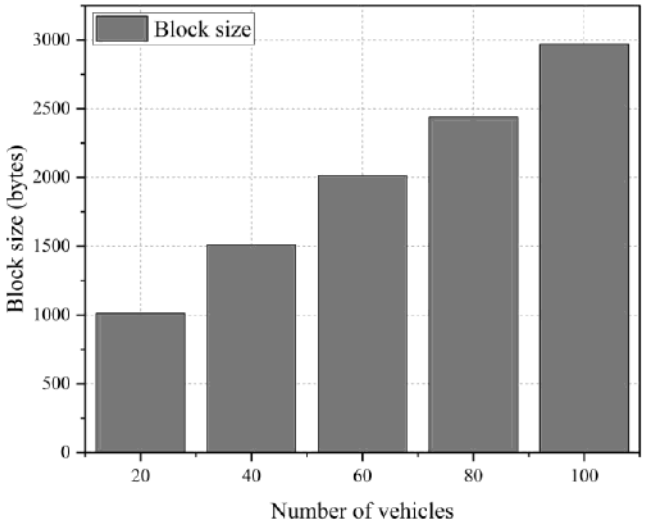

FIGURE 12 Storage overhead

10 | CONCLUSION

In this work, we propose a secure authentication scheme that allows vehicles to send anonymous messages to the RSU while preserving their privacy. In addition, it can also enable the TA

to trace anonymous malicious vehicles' identities and revoke them from the vehicular network. Additionally, a model of trust management is proposed so that the RSU can verify the trustworthiness of both vehicle nodes and traffic data. Therefore, the trust scheme allows the RSU to identify malicious vehicles sending false information, evaluate the received reports from vehicles, and broadcast only true events. RSU calculates the trust value of the sender vehicle and based on the trust value of the sender and the anomaly ratio, it can identify if the sender is malicious or honest. Then, trust values of the senders are stored in a block and the block is added to the blockchain, which represents the consensus of RSUs on each vehicle's trust. Moreover, RSU reports malicious vehicles to the TA to take action. The proposed trust model outperformed MARINE and ART due to the use of (1) direct trust (DT), (2) indirect trust/recommendation trust(Rec), and (3) old trust value from the blockchain for trust computation. The secure authentication scheme is validated through the efficiency analysis where results show it has a lower cost of authentication and less overhead than the compared schemes. To validate the proposed trust management scheme, numerous simulations have been conducted, and the accuracy of the trust model is evaluated using precision, recall, F-measure, FPR, and EDP. Moreover, the proposed system is analysed in terms of time consumption for block creation and consensus, and the storage overhead in the blockchain Experimental results show that the proposed trust model outperforms other related models as it accurately evaluates the trustworthiness of data as well as vehicles in VANETs, and it can also effectively identify malicious senders and allow only true events to be broadcasted.

CONFLICT OF INTEREST

No.

PERMISSION TO REPRODUCE MATERIALS FROM OTHER SOURCES

None.

DATA AVAILABILITY STATEMENT

Data sharing is not applicable to this article.

ORCID

Waheeb Ahmed https://orcid.org/0000-0003-4270-1422

REFERENCES

1. He, D., et al.: An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks. IEEE Trans. Inf. Forensics Secur. 10(12), 2681–2691 (2015). https://doi.org/10.1109/TIFS.2015.2473820
2. Guo, J., et al.: TROVE: a context-awareness trust model for VANETs using reinforcement learning. IEEE Internet Things J. 7(7), 6647–6662 (2020). https://doi.org/10.1109/JIOT.2020.2975084
3. Al-kahtani, M.S.: Survey on security attacks in vehicular ad hoc networks (VANETs). In: 2012 6th International Conference on Signal Processing and Communication Systems, pp. 1–9. (2012). https://doi.org/10.1109/ICSPCS.2012.6507953
4. Hezam Al Junaid, M.A., et al.: Classification of security attacks in VANET: a review of requirements and perspectives. MATEC Web Conf. 150, 1–7 (2018). https://doi.org/10.1051/matecconf/201815006038
5. Lu, Z., Qu, G., Liu, Z.: A survey on recent advances in vehicular network security, trust, and privacy. IEEE Trans. Intell. Transport. Syst. 20(2), 760–776 (2019). https://doi.org/10.1109/TITS.2018.2818888
6. Singh, K., Tomar, D.S.: Architecture, enabling technologies, security and privacy, and applications of internet of things: a survey. In: 2018 2nd International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2018 2nd International Conference on, vol. 4(5), pp. 642–646. (2018). https://doi.org/10.1109/I-SMAC.2018.8653708
7. Zhang, T., Zhu, Q.: Distributed privacy-preserving collaborative intrusion detection systems for VANETs. IEEE Trans. Signal Inf. Process. Netw. 4(1), 148–161 (2018). https://doi.org/10.1109/TSIPN.2018.2801622
8. Wei, Y.-C., Chen, Y.-M.: Efficient self-organized trust management in location privacy enhanced VANETs. In: Lee, D.H., Yong, M. (eds.) Information security applications. WISA 2012. Lecture notes in computer science, vol. 7690, pp. 328–344. Springer, Berlin (2012)
9. Grover, J., Gaur, M.S., Laxmi, V.: Trust establishment techniques in VANET. In: Khan, S., Khan Pathan, S. (eds.) Wireless networks and security. Signals and communication technology, pp. 273–301. Springer, Berlin (2013)
10. Ahmad, F., et al.: Trust management in vehicular ad-hoc networks and internet-of-vehicles. In: Outay, F., Yasar, A.-U.-H., Shakshuki, E. (eds.) Global advancements in connected and intelligent mobility: emerging research and opportunities, pp. 135–165. IGI Global (2020)
11. Nakamoto, S.: Bitcoin: a peer-to-peer electronic cash system (2008). http://bitcoin.org/bitcoin.pdf
12. Atzori, M.: Blockchain-based architectures for the internet of things: a survey. SSRN Electron. J (2017). https://doi.org/10.2139/ssrn.2846810
13. Zheng, D., et al.: A traceable blockchain-based access authentication system with privacy preservation in VANETs. IEEE Access. 7, 117716–117726 (2019). https://doi.org/10.1109/access.2019.2936575
14. Raya, M., Hubaux, J.P.: Securing vehicular ad hoc networks. J. Comput. Secur. 15(1), 39–68 (2007). https://doi.org/10.3233/JCS-2007-15103
15. Zhang, C., et al.: RAISE: an efficient RSU-aided message authentication scheme in vehicular communication networks. In: IEEE Int. Conf. Commun., no. Ivc, pp. 1451–1457. (2008). https://doi.org/10.1109/ICC.2008.281
16. Zhang, C., Ho, P.H., Tapolcai, J.: On batch verification with group testing for vehicular communications. Wireless Network. 17(8), 1851–1865 (2011). https://doi.org/10.1007/s11276-011-0383-2
17. Liu, J.K., et al.: Improvements on an authentication scheme for vehicular sensor networks. Expert Syst. Appl. 41(5), 2559–2564 (2014). https://doi.org/10.1016/j.eswa.2013.10.003
18. Jianhong, Z., Min, X., Liying, L.: On the security of a secure batch verification with group testing for VANET. Int. J. Netw. Secur. 16(5), 355–362 (2014)
19. Tan, H., et al.: Secure certificateless authentication and road message dissemination protocol in VANETs. Wireless Commun. Mobile Comput. 2018, 1–13 (2018). https://doi.org/10.1155/2018/7978027
20. Vijayakumar, P., et al.: Dual authentication and key management techniques for secure data transmission in vehicular ad hoc networks. IEEE Trans. Intell. Transport. Syst. 17(4), 1015–1028 (2016). https://doi.org/10.1109/TITS.2015.2492981
21. Peng, X.: A novel authentication protocol for vehicle network. In: 2016 3rd International Conference on Systems and Informatics (ICSAI), pp. 664–668. (2016). https://doi.org/10.1109/ICSAI.2016.7811036
22. Feng, Q., et al.: BPAS: blockchain-assisted privacy-preserving authentication system for vehicular ad hoc networks. IEEE Trans. Ind. Inf. 16(6), 4146–4155 (2020). https://doi.org/10.1109/TII.2019.2948053
23. Alazzawi, M.A., et al.: Efficient conditional anonymity with message integrity and authentication in a vehicular ad-hoc network. IEEE Access. 7, 71424–71435 (2019). https://doi.org/10.1109/ACCESS.2019.2919973
24. Liu, F., Wang, Q.: IBRS: an efficient identity-based batch verification scheme for VANETs based on ring signature. In: 2019 EEE Vehicular Networking Conference (VNC), pp. 1–8. (2019). https://doi.org/10.1109/VNC48660.2019.9062800

25. Shen, J., et al.: Secure real-time traffic data aggregation with batch verification for vehicular cloud in VANETs. IEEE Trans. Veh. Technol. 69(1), 807–817 (2020). https://doi.org/10.1109/TVT.2019.2946935
26. Ali, I., Li, F.: An efficient conditional privacy-preserving authentication scheme for Vehicle-To-Infrastructure communication in VANETs. Veh. Commun. 22, 100228 (2020). https://doi.org/10.1016/j.vehcom.2019.100228
27. Cui, J., et al.: Secure mutual authentication with privacy preservation in vehicular ad hoc networks. Veh. Commun. 21, 100200 (2020). https://doi.org/10.1016/j.vehcom.2019.100200
28. Ren, Y., et al.: Privacy-preserving batch verification signature scheme based on blockchain for vehicular ad-hoc networks. J. Inf. Secur. Appl. 58, 102698 (May 2021). https://doi.org/10.1016/j.jisa.2020.102698
29. Gazdar, T., Belghith, A., Abutair, H.: An enhanced distributed trust computing protocol for VANETs. IEEE Access. 6, 380–392 (2017). https://doi.org/10.1109/ACCESS.2017.2765303
30. Souissi, I., Ben Azzouna, N., Berradia, T.: Trust management in vehicular ad hoc networks: a survey. Int. J. Ad Hoc Ubiquitous Comput. 31(4), 230–243 (2019). https://doi.org/10.1504/IJAHUC.2019.101210
31. Khan, U., Agrawal, S., Silakari, S.: Detection of malicious nodes (DMN) in vehicular ad-hoc networks. Procedia Comput. Sci. 46, 965–972 (2014). https://doi.org/10.1016/j.procs.2015.01.006
32. Hu, H., et al.: REPLACE: a reliable trust-based platoon service recommendation scheme in VANET. IEEE Trans. Veh. Technol. 66(2), 1786–1797 (2017). https://doi.org/10.1109/TVT.2016.2565001
33. Haddadou, N., Rachedi, A., Ghamri-Doudane, Y.: A job market signaling scheme for incentive and trust management in vehicular ad hoc networks. IEEE Trans. Veh. Technol. 64(8), 3657–3674 (2015). https://doi.org/10.1109/TVT.2014.2360883
34. Minhas, U.F., et al.: A multifaceted approach to modeling agent trust for effective communication in the application of mobile Ad Hoc vehicular networks. IEEE Trans. Syst. Man Cybern. C Appl. Rev. 41(3), 407–420 (2011). https://doi.org/10.1109/TSMCC.2010.2084571
35. Gurung, S., et al.: Information-oriented trustworthiness evaluation in vehicular ad-hoc networks. In: Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 7873, pp. 94–108. LNCS (2013). https://doi.org/10.1007/978-3-642-38631-2_8
36. Liu, Z., et al.: LSOT: a lightweight self-organized trust model in VANETs. Mobile Inf. Syst. 2016, 18–15 (2016). https://doi.org/10.1155/2016/7628231
37. Shaikh, R.A., Alzahrani, A.S.: Intrusion-aware trust model for vehicular ad hoc networks. Secur. Commun. Network. 7(11), 1652–1669 (2014). https://doi.org/10.1002/sec.862
38. Sedjelmaci, H., Senouci, S.M.: An accurate and efficient collaborative intrusion detection framework to secure vehicular networks. Comput. Electr. Eng. 43, 33–47 (2015). https://doi.org/10.1016/j.compeleceng.2015.02.018
39. Li, W., Song, H.: ART: an attack-resistant trust management scheme for securing vehicular ad hoc networks. IEEE Trans. Intell. Transport. Syst. 17(4), 960–969 (2016). https://doi.org/10.1109/TITS.2015.2494017
40. Ahmad, F., et al.: MARINE: man-in-the-middle attack resistant trust model in connected vehicles. IEEE Internet Things J. 7(4), 3310–3322 (2020). https://doi.org/10.1109/JIOT.2020.2967568
41. Yang, Z., et al.: A blockchain-based reputation system for data credibility assessment in vehicular networks. IEEE Int. Symp. Pers. Indoor Mob. Radio Commun. PIMRC. 2017, 1–5 (2018). https://doi.org/10.1109/PIMRC.2017.8292724
42. Bendiab, K., et al.: WiP: a novel blockchain-based trust model for cloud identity management. Proc. - IEEE 16th Int. Conf. Dependable, Auton. Secur. Comput. IEEE 16th Int. Conf. Pervasive Intell. Comput. IEEE 4th Int. Conf. Big Data Intell. Comput. 3, 716–723 (2018). https://doi.org/10.1109/DASC/PiCom/DataCom/CyberSciTec.2018.00126
43. Kchaou, A., Abassi, R., Guemara, S.: Toward a distributed trust management scheme for VANET. ACM Int. Conf. Proceeding Ser. (2018). https://doi.org/10.1145/3230833.3232824
44. Zhang, C., et al.: AIT: an AI-enabled trust management system for vehicular networks using blockchain technology. IEEE Internet Things J. 8(5), 3157–3169 (2021). https://doi.org/10.1109/JIOT.2020.3044296
45. Pu, C.: A novel blockchain-based trust management scheme for vehicular networks. In: 2021 Wireless Telecommunications Symposium (WTS), pp. 1–6. (2021). https://doi.org/10.1109/WTS51064.2021.9433711
46. Wang, D., et al.: A privacy-preserving trust management system based on blockchain for vehicular networks. In: 2021 IEEE Wireless Communications and Networking Conference (WCNC), pp. 1–6. (2021). https://doi.org/10.1109/WCNC49053.2021.9417492
47. Li, F., et al.: ATM: an active-detection trust mechanism for VANETs based on blockchain. IEEE Trans. Veh. Technol. 70(5), 4011–4021 (2021). https://doi.org/10.1109/TVT.2021.3050007
48. Liu, H., Han, D., Li, D.: Behavior analysis and blockchain based trust management in VANETs. J. Parallel Distr. Comput. 151, 61–69 (2021). https://doi.org/10.1016/j.jpdc.2021.02.011
49. Kudva, S., et al.: A scalable blockchain based trust management in VANET routing protocol. J. Parallel Distr. Comput. 152, 144–156 (2021). https://doi.org/10.1016/j.jpdc.2021.02.024
50. Zhang, Y., et al.: Blockchain based efficient and robust fair payment for outsourcing services in cloud computing. Inf. Sci. (Ny). 462, 262–277 (2018). https://doi.org/10.1016/j.ins.2018.06.018
51. Wood, G.: Ethereum: a secure decentralised generalised transaction ledger. Ethereum Proj. Yellow Pap. Ethereum.org. 151, 1–32 (2018). https://ethereum.github.io/yellowpaper/paper.pdf
52. Li, H., Liu, Q., Chen, F.: Signal word-level statistical properties-based activation approach for hardware Trojan detection in DSP circuits. IET Comput. Digital Tech. 12(6), 258–267 (2018). https://doi.org/10.1049/iet-cdt.2018.5101
53. Hasrouny, H., et al.: VANet security challenges and solutions: a survey. Veh. Commun. 7, 7–20 (2017). https://doi.org/10.1016/j.vehcom.2017.01.002
54. Kerrache, C.A., et al.: Trust management for vehicular networks: an adversary-oriented overview. IEEE Access. 4, 9293–9307 (2016). https://doi.org/10.1109/ACCESS.2016.2645452
55. Arif, M., et al.: A survey on security attacks in VANETs : communication, applications and challenges. Veh. Commun. 19, 100179 (2019). https://doi.org/10.1016/j.vehcom.2019.100179
56. Zhou, T., et al.: Privacy-preserving detection of sybil attacks in vehicular ad hoc networks. In: 2007 Fourth Annual International Conference on Mobile and Ubiquitous Systems: Networking & Services (MobiQuitous), pp. 1–8. (2007). https://doi.org/10.1109/MOBIQ.2007.4451013
57. Rezazadeh Baee, M.A., et al.: Authentication strategies in vehicular communications: a taxonomy and framework. EURASIP J. Wirel. Commun. Netw. 2021(1), 129 (2021). https://doi.org/10.1186/s13638-021-01968-6
58. Ahmad, F., et al.: Faith in vehicles: a set of evaluation criteria for trust management in vehicular ad-hoc network. In: 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pp. 44–52. (2017). https://doi.org/10.1109/iThings-GreenCom-CPSCom-SmartData.2017.13
59. Zhong, H., et al.: Privacy-preserving authentication scheme with full aggregation in VANET. Inf. Sci. (Ny). 476, 211–221 (2019). https://doi.org/10.1016/j.ins.2018.10.021
60. Kamil, I.A., Ogundoyin, S.O.: An improved certificateless aggregate signature scheme without bilinear pairings for vehicular ad hoc networks. J. Inf. Secur. Appl. 44, 184–200 (2019). https://doi.org/10.1016/j.jisa.2018.12.004
61. Bayat, M., et al.: A new and efficient authentication scheme for vehicular ad hoc networks. J. Intell. Transport. Syst. Technol. Plann. Oper. 24(2), 171–183 (2020). https://doi.org/10.1080/15472450.2019.1625042
62. Zhang, J., et al.: PA-CRT: Chinese remainder theorem based conditional privacy-preserving authentication scheme in vehicular ad-hoc networks. IEEE Trans. Dependable Secure Comput. 18(2), 722–735 (2019). https://doi.org/10.1109/TDSC.2019.2904274

63. MIRACL. https://miracl.com/blog/evolving-the-miracl-core-library-4-min-read/. Accessed 05 April 2021
64. Veins. http://veins.car2x.org. Accessed 05 April 2021
65. OMNET. https://omnetpp.org/. Accessed 05 April 2021
66. Behrisch, M., et al.: SUMO – Simulation of urban MObility. Iaria (2011). https://www.eclipse.org/sumo/. Accessed 05 April 2021
67. Shah, S., et al.: Compromised user credentials detection in a digital enterprise using behavioral analytics. Future Generat. Comput. Syst. 93, 407–417 (2019). https://doi.org/10.1016/j.future.2018.09.064
68. Soleymani, S.A., et al.: A trust model using edge nodes and a cuckoo filter for securing VANET under the NLoS condition. Symmetry (Basel). 12(4), 609 (2020). https://doi.org/10.3390/sym12040609
69. Chen, Y.M., Wei, Y.C.: A beacon-based trust management system for enhancing user centric location privacy in VANETs. J. Commun. Netw. 15(2), 153–163 (2013). https://doi.org/10.1109/JCN.2013.000028
70. Sedjelmaci, H., Senouci, S.M., Abu-Rgheff, M.A.: An efficient and lightweight intrusion detection mechanism for service-oriented vehicular networks. IEEE Internet Things J. 1(6), 570–577 (2014). https://doi.org/10.1109/JIOT.2014.2366120
71. Arshad, M., et al.: Beacon trust management system and fake data detection in vehicular ad-hoc networks. IET Intell. Transp. Syst. 13(5), 780–788 (2019). https://doi.org/10.1049/iet-its.2018.5117
72. Ahmad, F., Franqueira, V.N.L., Adnane, A.: TEAM: a trust evaluation and management framework in context-enabled vehicular ad-hoc networks. IEEE Access. 6(3), 28643–28660 (2018). https://doi.org/10.1109/ACCESS.2018.2837887

How to cite this article: Ahmed, W., Di, W., Mukathe, D.: Privacy-preserving blockchain-based authentication and trust management in VANETs. IET Netw. 11(3-4), 89–111 (2022). https://doi.org/10.1049/ntw2.12036