Engineered Science
DOI: https://dx.doi.org/10.30919/es1073

Privacy Preserving Blockchain Based Authentication Scheme for Vanet

Chindika Mulambia,* Sudeep Varshney and Amrit Suman

Abstract

Vehicular Ad-Hoc Networks are very necessary in Intelligent Transport Systems whose primary goal is to enhance safety in transportation by transmitting real time messages on accident notifications and traffic status. The dynamic nature of the vehicular networks makes them susceptible to malicious vehicles as these vehicles exploit and disseminate messages that have false information. It is imperative to identify and prevent these malicious actors so that integrity is preserved in the network. Another important aspect is privacy preservation whereby the real identities are not exposed and misused. To address these concerns a Privacy Preservation Blockchain Based Authentication Scheme approach is proposed. The solution is executed in Linux environment running Ubuntu 20.04 within a Docker Container that stimulates the network. The approach leverages Blockchain Technology that is known for its tamper resistant ledger which is managed via a peer-to-peer network. The approach assigns pseudo IDs to authenticated vehicles which ensures privacy for users. Every transaction saved in the Blockchain is hashed and subsequent transactions are built on the previous hash which makes tampered data easily detectable; this maintains data integrity and prevents unauthorised transactions. Results demonstrate the scheme's effectiveness as it promotes faster authentication and encryption as compared to alternative methods especially in scenarios where there's increase in vehicle density.

Keywords: Vehicular Ad-Hoc Networks (Vanet); Message Authentication; Road Side Unit (RSU); Authentication Manager; Blockchain.
Received: 25 October 2023; Revised: 27 November 2023; Accepted: 27 November 2023.
Article type: Research article.

1. Introduction

Vehicular Ad-Hoc Networks(Vanets) are a crucial component in Intelligent Transport Systems(ITS).ITS aims to achieve safe and efficient transport systems. Vanets are a network of continuously moving nodes that connect in an AdHoc manner.[1] The Vanet emerges as the vehicles connect and this type of network serves as a crucial component of Intelligent Transport Systems(ITS). Vanets facilitates achievement of ITS' objectives by disseminating information regarding road accidents and traffic conditions within the area.[2] If a vehicle sends a message to other vehicles of an accident that has occurred then the other vehicles can decide to change their routes and avoid that route. A message can also be about traffic conditions for instance if there's a lot of congestion in a particular route then the vehicles can also opt for another route. Fig. 1 shows a vehicle reporting to other vehicles that an accident has occurred.

Due to increase in the numbers of vehicles in the network, security and privacy concerns need to be addressed.[3] Vanets due to network structure promotes security concerns. It is a wireless network and any vehicle within the range can transmit messages and also find out the real identities of vehicles. Some of the attacks found in Vanet are:

Sybil Attack: The attacker creates many vehicles with similar identity or can steal multiple identities in the network and mislead others by sending misleading or wrong messages in the network that benefit the attacker.[4]

Replay Attack: The attacker will listen to messages that are being passed in an established connection. The attacker then replays the messages that were sent between them. The attacker makes them think that they are communicating with each other.[4]

Message Alteration: This is when the attacker changes the

Department of Computer Science and Engineering, Sharda University, Greater Noida 201310, UP, India.
**Email:* chindikachitalo@gmail.com (C. Mulambia)

contents of a message that has been sent in the network.[4]

1.1 Problem statement and motivation

Securing a Vanet is very key and authentication and privacy schemes are very vital in securing a Vanet. Authentication is a process that will allow only authorized or legitimate entities. Authentication is the first step to prevent malicious vehicles from joining the network. In the process the transmitter signs the message and then the recipient verifies the message.[5] Messages are very vital in Vanet so securing these messages is very important. Authentication helps us to be sure of the source of the message that has sent and it also confirm integrity. Privacy also ensures security in a Vanet by providing anonymity. Privacy protects the individual by hiding the identity of the user. In a vehicular network it is vital not to expose the real IDs of the vehicles so that malicious vehicles cannot steal the IDs of the users and perform certain attacks like the Sybil attack. In order to have a secure and efficient communication a reliable solution is required. Blockchain technology is the central technology behind Bitcoin.[6] The e-cash system uses a peer to peer method. The approach is decentralized and has a ledger where every node a copy of the database is managed by a node from the network. This technology is a good solution for Vanets because it provides a good data sharing platform whereby authenticated vehicles, activities in the network and messages will be shared.[6] Since the technology is peer to peer it allows a distributed network architecture that supports vehicles moving at high speed which is one of the characteristics in a vehicular network and the distributed architecture also supports the frequently changing network topology of a vehicular network. The nodes operate in such a way that they are able to accept or deny information sent by the other nodes and this makes them not waste resources by accepting unverifiable information. This process makes it improve network delay in the vehicular network.[6] In a vehicular network large amounts of data is transmitted between the vehicles and RSUs and one of the main concerns is large data storage. Blockchain is a solution to these scalable networks in that it is able to handle large amounts of data by applying data management schemes to the blockchain unlike traditional centralised methods that will be over swamped by too much data and cause a single point of failure.[6]

The proposed approach is a Privacy Preserving Authentication Approach that verifies the real identities of vehicles. The approach allows a vehicle to present their vehicle ID to the Authentication Manager and this is verified against the list of already known Vehicle IDs.

The approach promotes privacy preservation in that once a vehicle is authenticated it is given a pseudo ID that will be used it will use when communicating in the network and this can not be traced to the real Identity of the vehicle. This also prevents the malicious users from stealing the IDs of the legit vehicles and use them in the network.

A blockchain is also used in this approach that saves every transaction like vehicle authentication in the chain. Each transaction is hashed and given a timestamp. Any transaction that is done after that particular transaction is also hashed and the hash is built from the previous hash. Any manipulation of data will be detected because previous hashes are already recorded in the chain. This promotes message integrity and

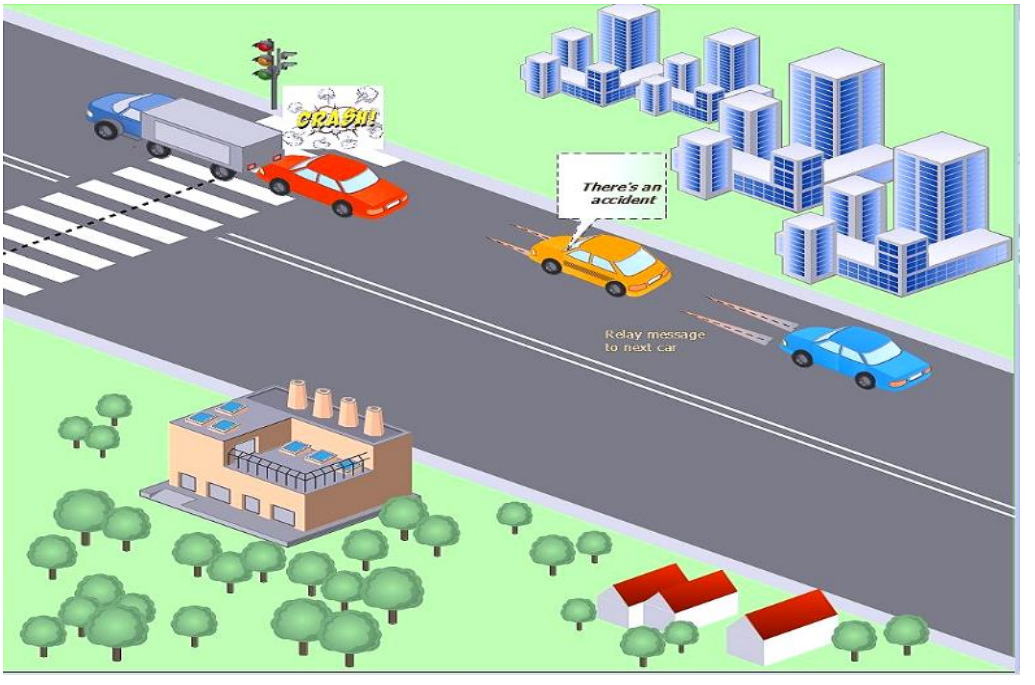

Fig. 1 Typical Vanet Scenario with vehicles announcing an accident.

also message alteration or tampering is avoided.

The blockchain also enhances decentralised architecture which prevents a single point of failure in the network.

1.2 Related work

Vanets due to its structure of open access brings a lot of challenges in security and privacy so these issues need to be dealt with before implementation in the real world. Feng *et al* (2021) uses a centralised method where by the TA which is a Law Enforcement Authority (LEA) distributes certificates for RSU's and vehicles.[7] SEMA model approach by Wang *et al* (2021) has groups and the RSU generates keys for the local group. TA manages the global group and distributes real identities of the vehicles and the RSU's and also the pseudonyms.[8] Lee *et al* (2021)[9] approach has a TA that authenticates keys for the users. Aghabagherloo *et al* (2022) approach uses a bit of decentralised method but has high computational overhead.[10] Luo *et al* (2022) also uses a centralised structure in which TA comes up with keys for users.[11] While all these approaches are able to solve the security challenge. The security is not distributed across the network which promotes one point of failure. This approach also puts a lot of computational overhead on the central device. Blockchain arranges data in order that they are created and the nodes in the network share this data.[6] An example of is Bitcoin which is a decentralised system used in e-cash. Fig. 2 shows how the transaction processes happen in Blockchain technology. Each transaction is inserted with a hash. The Hash is unique to each block and any modification causes change to the hash.[6] The technology promotes a decentralised, distributed and immutable network. These characteristics that enhance security are some reasons why researchers are implementing it in Vanets. Lu *et al* (2019)[12] uses blockchain technology and implements a privacy-based authentication scheme. It uses a distributed authentication with the data structure that it implements. For privacy it gives a vehicle multiple certificates and it links these certificates to the real identity. The disadvantage with the approach is that there are too many certificates for vehicles. A traceable system for authentication based on blockchain including preservation of privacy is used by Zheng *et al* (2019).[6] It makes use of pseudonyms to employ anonymity among the vehicles. Only the CA knows the identity of the vehicle and CA is highly secure. Disadvantage is that if less RSU's than malicious nodes then transactions will be changed. Liu *et al* (2019)[13] proposes an approach that uses group signatures for authentication and the every message sent in the group has to be verified by other witnesses in the network using a method called trust calculation. This verification does not reveal the identities of the users. Malicious vehicles are identified by checking the public addresses in the blockchain. The drawback of the approach is that parameters of the scheme not completely set. Wang *et al* (2020)[14] approach makes a vehicle generate an encrypted message and transmits to RSU who verifies that message inside the blockchain. The scheme also allows the vehicle to search for a service in the network and this search uses keywords. A ciphertext is created for the search and the reply of this service is re-encrypted using an attribute-based proxy. Drawback is computation and communication costs. These a bit higher than other approaches. A trust management scheme based on block chain approach is used by Zhao *et al* (2021).[15] The approach uses an identity-based group signature and also employs calculation of reputation of vehicles which is the most effective thing in the approach. The drawback is slightly high communication overhead especially on the signature in comparison with other schemes. A secure message handling approach is proposed by Muhammed, Javed *et al* (2022)[16] using blockchain. They also introduce an artificial intelligent file system that is implemented that reduces storage cost and improves data availability. It also employs usage of pseudonyms that are updated after some time. Drawback is computation overhead. Yang *et al* (2022)[17] introduces an approach that uses multidomain authentication instead of having a single administrative domain. The multidomain uses blockchain technology and this enhances dispersed sharing of information in different domains. Drawback is that as number of domains increases the delay in vehicle enrolment also increases. In order to assist miner nodes verify and identify such messages, an approach is developed by Khatri N et al 2023 with a unique clustering method for handling event messages in VANETs using Blockchain Technology. This method improves K-value selection, reduces computational costs, and solves issues with K-Means clustering. The results obtained show that this algorithm performs more effectively than K-Means and other clustering approaches in terms of accuracy, precision, recall, and computing cost.[18]

Subramani *et al* 2023[19] with the goal to enhance security and privacy proposes an innovative approach to authentication that utilises fog computing using blockchain. By taking benefit of mobility support, decreasing latency, and tracking locations, it effectively addresses these issues. Physical security is enhanced by the decentralised blockchain, that secures vehicle data without maintaining secret keys. Compared with other methods of a similar kind, this one provides adequate safety with fewer requirements for computing, storage, and communication.[19]

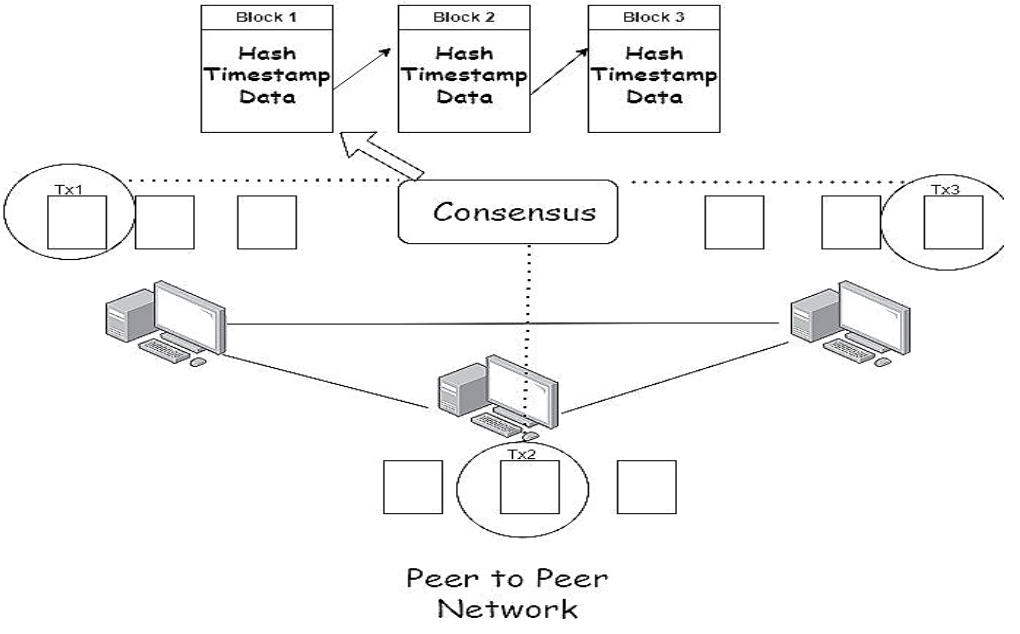

Fig. 2 Transaction process in blockchain.

2. Method

To enhance privacy and secure message authentication in a Vanet, the following model is used as in Fig. 3. The model consists of the following layers which are the message dispersal layer, management layer then the blockchain layer. In the message dispersal layer is where the vehicles generate messages and transmit to to the RSU's. Vehicles will first have to be authenticated by the Authentication manager that is in the Management layer.[20] Once authenticated then they can proceed to send messages. The last layer is the blockchain layer. This consists of different RSU's that have a peer to peer network. The RSU's oversee the whole network. Data that has been generated in the first layer is transmitted to this layer. The RSU that receives the data will create a transaction of that data and generate a hash for that particular transaction using Blockchain technology. Once the hash of that data has been created then the RSU broadcasts that data to the rest of the RSU's in the layer.[21] Table 1 shows the acronyms used in the document.

Table 1. Acronyms used in document.

Acronym	Description
$Cert_a$	Certificate for a
$Cert_b$	Certificate for b
PID_a	Pseudo ID a
PID_b	Pseudo ID b
VID_b	Vehicle ID for a
H	Hash
P_{ka}	Private Key for RSU
D_{ka}	Message
ConnM	Connection message

The proposed model as shown in Fig. 3 has the following components:

A. Vehicles

Vehicles generate messages and transmit these messages across the network. Messages created announce the traffic status. Vehicles firstly get authenticated with Authentication Manager as depicted by step 1. Once authenticated it is given PID and keys as in step 2. The vehicles are equipped with an OBU that stores the keys (public and private keys).[22] Another vehicle joining the network will also need to be authenticated as in Step 5. After authentication it can access the messages sent by other vehicles in the network as in step 6.

B. Authentication Manager/RSU

RSU is also an authentication manger in this model. Using the blockchain technology the RSUs are connected in a peer-to-peer setup. This means all the RSUs have access to the same information and no RSU is superior over the other RSUs. The RSU authenticates vehicles in the network and then saves that information in the blockchain and broadcasts that information to other nodes in the layer and these are shown by steps 3 and 4. If one RSU is not available the rest of the RSUs still have the information of the network.

C. Blockchain

To prevent altering of records and promote a decentralised system the blockchain is used. Blockchain has data blocks and a hash is used on each block.[23] Each information that the RSU saves to the blockchain is recorded in form of transactions.

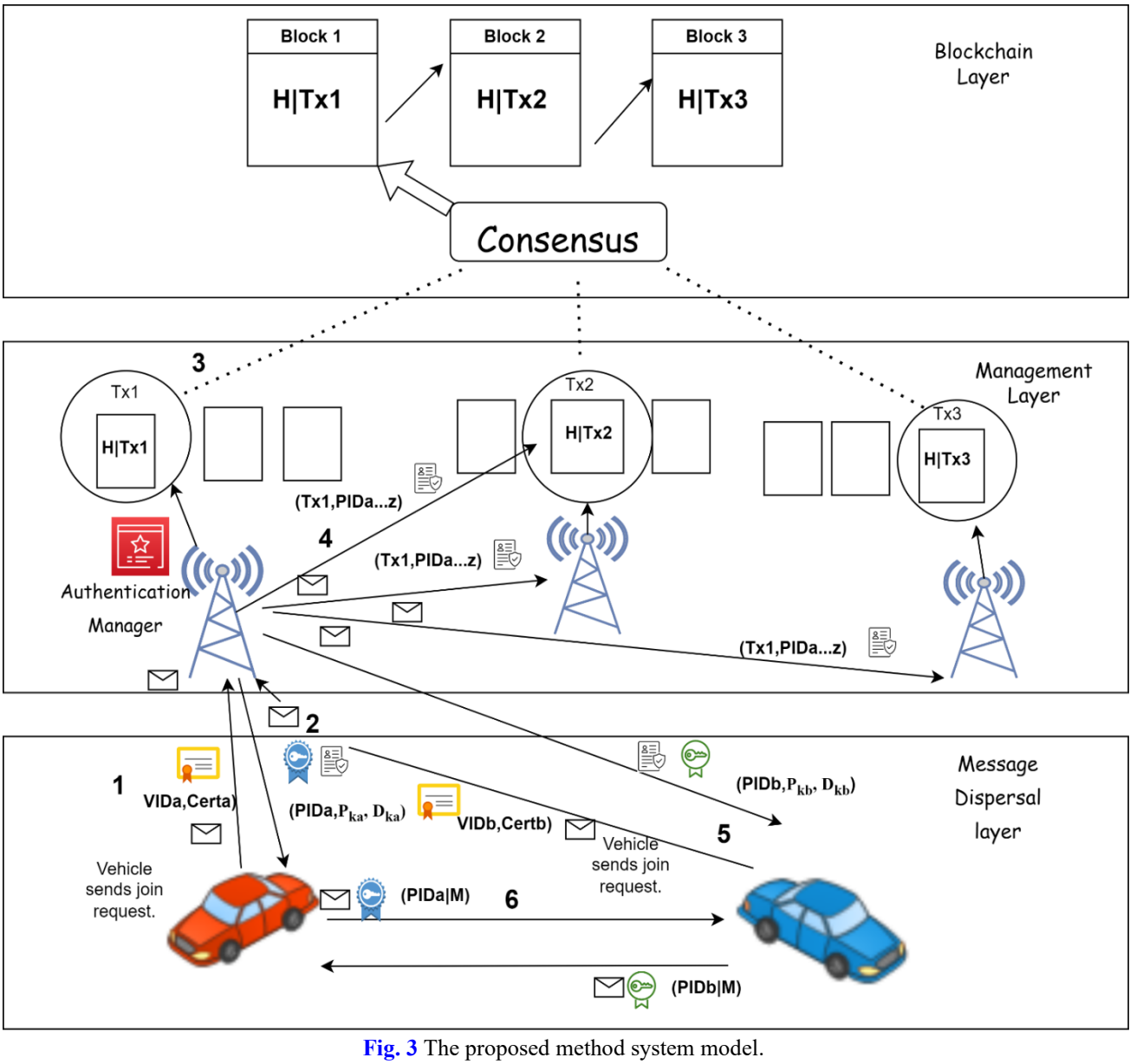

Fig. 3 The proposed method system model.

The hash is used to verify data genuity by computing the hash. Data in this chain is also accessed by all the RSUs in the layer which enhances the peer-to-peer network.[24]

The flowchart in Fig. 4a show the process of a vehicle getting authenticated in the network. Vehicle sends a connection message and if authentication manager verifies vehicle, then it is given a pseudo-ID if not message is ignored. Sequence diagram in Fig. 4b shows the processes in the proposed model. When a vehicle is in the range it will send a connection message to the authentication manager. The authentication manager receives the ID of the vehicle and its certificate. The authentication manager verifies the details of the vehicle. In the model the assumption that the authentication manager has a list of valid vehicle IDs.[25] If the verification is successful the Authentication manger produces a pseudo ID for the vehicle and also keys sends to the vehicle. The vehicle stores this information in the OBU. If the verification is not successful then the authentication manager ignores the message. If the vehicle is legit then the message is resent otherwise the vehicle might be a malicious vehicle trying to get connection into the network.[26]

The privacy preserving scheme that has main entities which are a set of RSUs and these also play the role of authentication manager. The RSU use the blockchain network as they authenticate devices and broadcast messages. The set of vehicles in the network that range from {Va,Vb…….Vi}. The assumption is that the vehicles and RSU have already obtained their certificates. The blockchain builds the system for Elliptic Curve Cryptography (ECC) for the digital signatures and hashes (H0, H1…….He} for the transactions.[27] The RSU/Authentication Manager provides a place for vehicle identity authentication. Elliptic Curve Cryptography is a

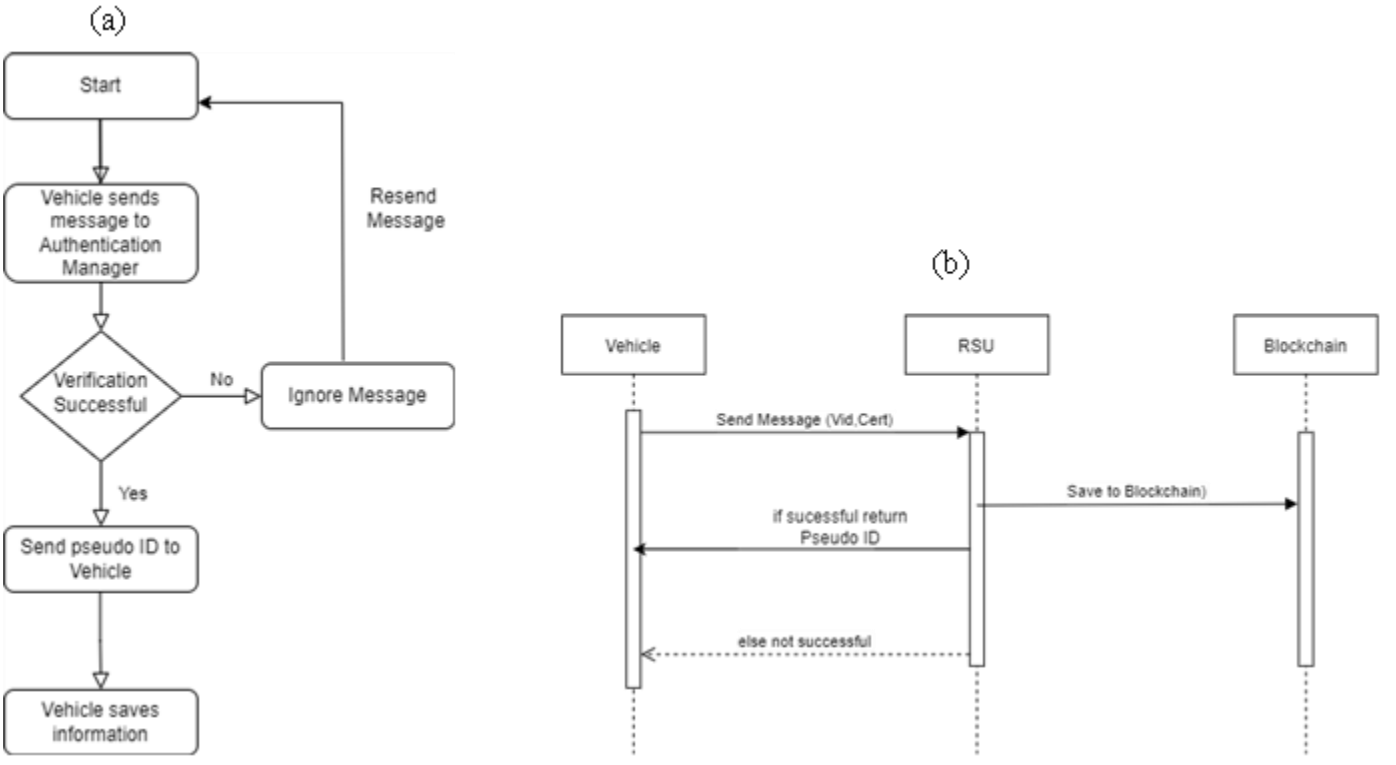

Fig. 4 Flowchart and Sequence diagrams of proposed approach.

technic based elliptic curves over finites fields. It can be applied to construct digital signatures.[28] An elliptic curve is written as follows:[29]

$y2 = \chi 3 + a\chi + b \pmod p$

In this case a and b are constants that qualify the properties of elliptic curve which is:

$4a3+27b2 \neq 0$

For key generation the sender selects k an integer randomly where (1<k< n-1) and this number randomly selected will be private key. For public key Psender the formula is:

Psender =k * q

where q is a fixed point on the curve.

To sign a document, compute the hash of the message and obtain a hash value. So, if the message is M the hash value is h(M).[30] A random number d is generated that is within the range of (1<d<n-1). Calculate another temporary point α which is α =d*q (α is the point on the curve too.)[31] The signature S is calculated as:

s=(h(M)+k*x(R))/d mod n

where x(α)) is the point α on the x coordinate. The digital signature (s,ϱ),where ϱ is also Point α the x coordinate.[32] Signature verification is done in the following way. Ensure that s and t are in the range of (1<t< n-1). Then calculate the message digest h'(M) and compare with received h(M). Compute a verification point E where,

E=(s-1)* h'(M)*q+(s-1)* ϱ *q.

If x-coordinate of E is equal to ϱ then signature is valid else no valid.[33]

The RSU's are peer nodes build the blockchain according to the proposed model. An authentication manager authenticates the vehicles as in the Table 2. In order to promote privacy of vehicles the Authentication manager generates a Pseudonym ID with a certificate attached to it. This is uniquely mapped to the vehicle's real ID and it the real ID cannot be extracted from this pseudonym.

Table 2. Steps for vehicle authentication process.

1	$V_a \longrightarrow$ Auth Ma01 n:<VID_a, $Cert_a$, other details>
2	Auth Man $\xrightarrow{verf}$ VID_a:<Verify (VID_a, $Cert_a$)
3	Auth Man $\xrightarrow{cal}$ Hash:<$H_0(PID_a \| P_{ka})$
4	Auth Man $\longrightarrow$ Blockchain: <$T_{x1}(H_0) \| PID_a \| P_{ka}$ >
5	Auth Man $\longrightarrow$ V_a:<PID_a‖cert‖ECC(P_{ka}, Dka>

The connection of a vehicle has the following steps:

Step 1: Vehicle transmits it ID and certificate to Authentication Manager.

Step2: Authentication manager authenticates this vehicle by verifying its ID and certificate. It then generates the pseudonym ID of the vehicle and also produces an ECC Public-Private keys Pka and Dka.

Step 3: Authentication manager calculates a hash H0 =PIDa||Pka to authenticate vehicle identity and to store this information to be used in the future.

Step 4: The authentication manager creates a transaction

TX1(H0)|| PIDa||Pka and this is stored in the blockchain and all RSUs get that transaction.

Step 5: Connected vehicle gets the Certificate, Pseudo ID and the private and public key pair and stores this in the OBU.

The vehicle will want to communicate about the traffic conditions. It will generate a message M. The steps are in Table 3.

Table 3. Steps for sending messages.

1	$V_a \longrightarrow$ RSU:<$H_1(M\|\|PID_a\|\|M\|\| PID_a >$
2	RSU $\xrightarrow{cal}$ H'1:<Calculate H'1: ($M\|\|PID_a\|$)
3	RSU $\xrightarrow{com}$ H_1:<Compare H'1= H_1 if true, pack up T_{x2}
4	RSU $\xrightarrow{packs}$ T_{x2} : <$T_{x2}(H_1)\|\|$ M$\|\|PID_a\|\|$*timestamp* >
5	RSU $\xrightarrow{store}$ Blockchain:<calculate $H_3(T_{x2})$>

Step 1: Vehicle sends message M to RSU and hashes with pseudo ID.

Step 2: The RSUs only verify integrity of message since the vehicle has already been authenticated.

Step 3: If calculated hash is same as sent hash then the RSU creates a new Tx2.

Step4: RSU saves this message in the transaction and content is Tx2(H1)|| M||PIDa||timestamp.

Step 5. This transaction is hashed H3 and the saved in the chain and broadcasted to other peer nodes.

3. Results and discussion

3.1 Experiment setup

Real World: Real traffic scenario was extracted from Greater Noida, New Delhi on busy streets using Open Street Map and this scenario was imported into SUMO as shown in Fig. 5. This was then imported into sumo and the simulation results obtained. Fig. 6 shows the simulation in Sumo. The scheme was implemented in python 3.12 using laptop Intel core i7 processor 13thGen with 16GB RAM and on Linux environment running Ubuntu 20.04 in a docker container. The docker container simulated the network. For the authentication process a vehicle presents their VID and then the authentication manager verifies that ID and once the verification is done this vehicle is authenticated and that is the pseudo ID of the vehicle.

Figure 5 shows the real traffic scenario selected from Greater Noida in India from the busy streets in Greater Noida. The real traffic simulated in the SUMO software and shown in the Fig. 6.

3.2 Security analysis

Privacy Preserving: The vehicles are given pseudo IDs after they have been authenticated. These IDs are stored in the blockchain. The pseudo-IDs given cannot be traced to vehicles true identity. When vehicles are communicating they only use this pseudo ID and this prevents malicious vehicles from getting the real ID of the vehicle and get authenticated.

Replay Attack Prevention: The information stored in the blockchain contains a unique identifier called a transaction. All transactions have a unique identifier so any transaction that comes with a similar transaction number to the ones already stored will be rejected and this will avoid replay attack in the network.

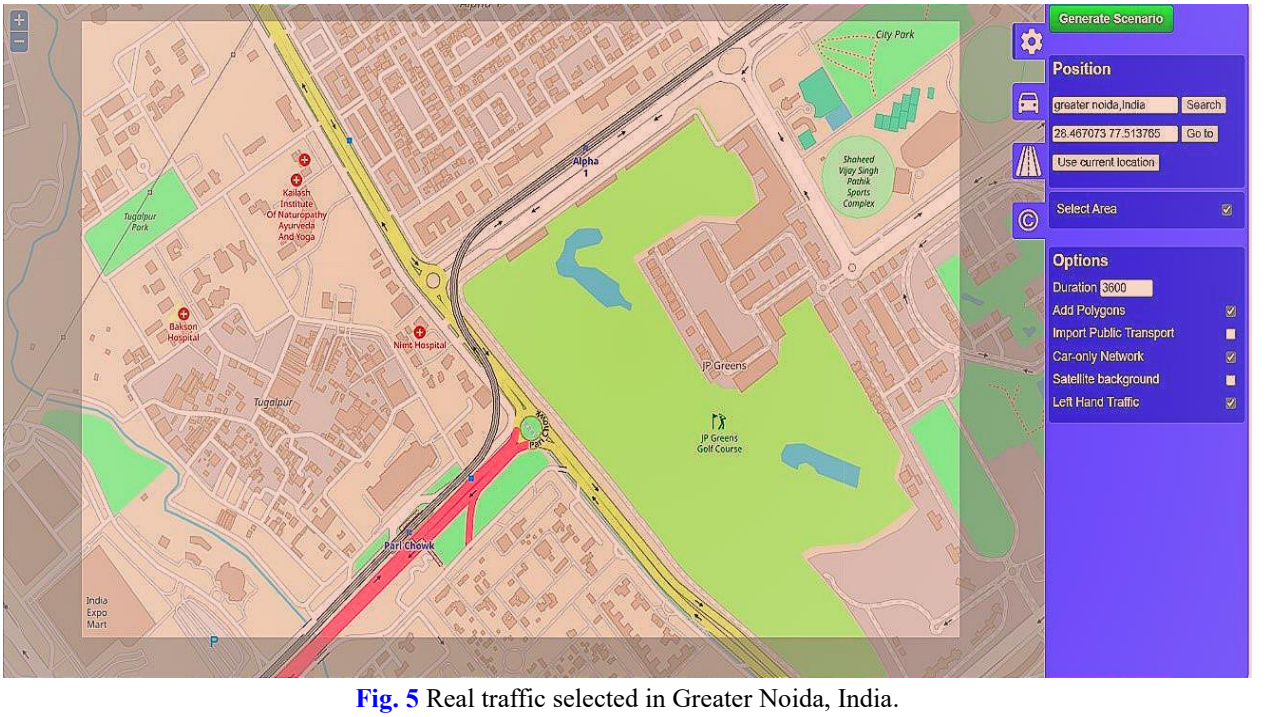

Fig. 5 Real traffic selected in Greater Noida, India.

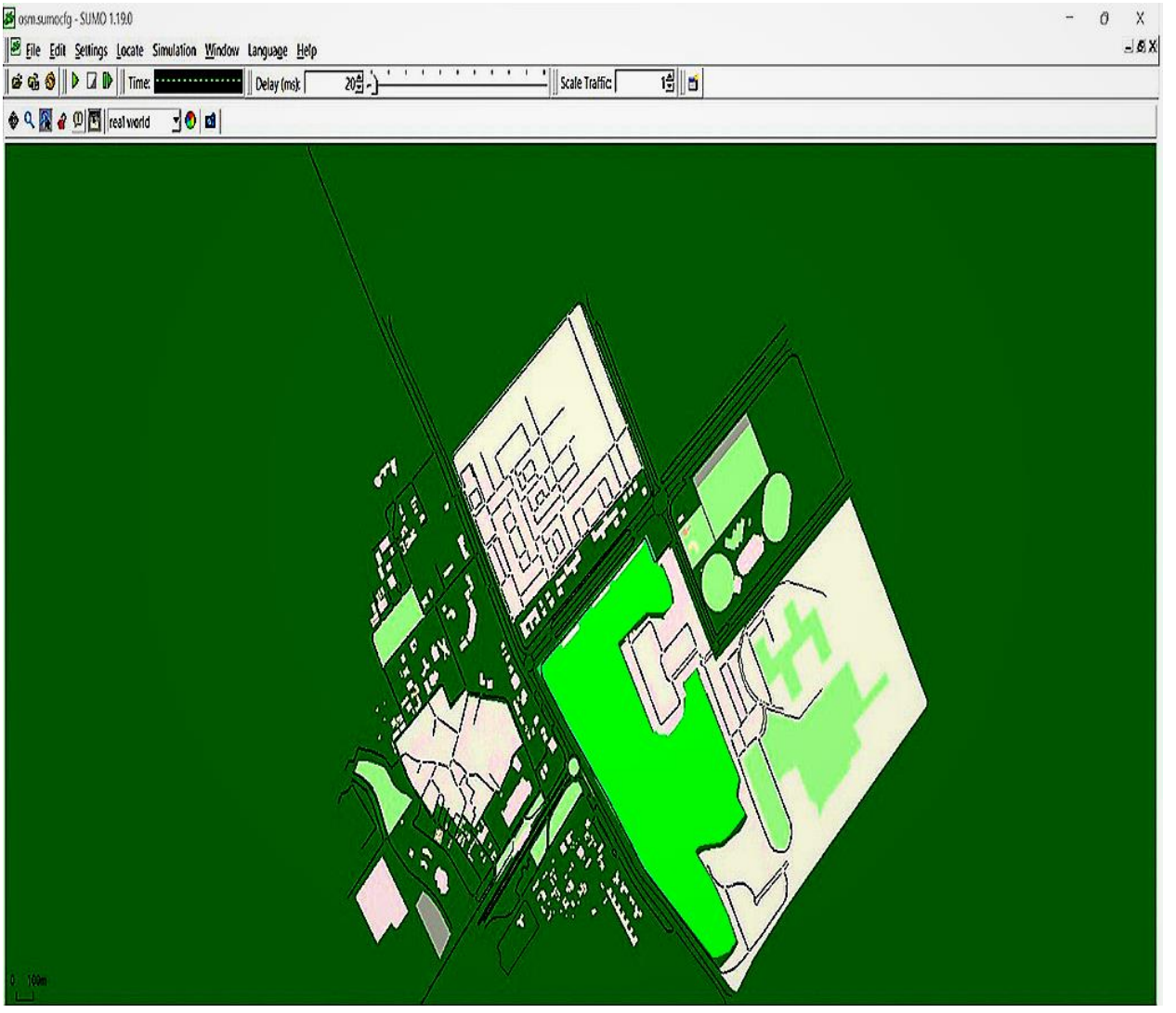

Fig. 6 Simulating the traffic in Sumo.

Message alteration Prevention: Each transaction is hashed. Any current hash is built from the previous hash. If there is any change in the information then the hash will be different so this will promote message integrity in that message will not be changed that have already been added to the blockchain.

3.3 Performance analysis

The performance is measured by calculating average delay in milliseconds(ms) that it takes for the vehicle to be authenticated and also given the pseudo ID. Fig. 5 shows the time it takes to do the authentication. The approach is compared with competitive scheme.[7,10,11]

To find the average delay of authentication process firstly the number of vehicles in a particular instance was calculated. To find number of vehicles in a given instance lets say in 100ms(milliseconds). TRi symbolises time received for ith node. Assumption is made to find number of nodes from 0ms to 100ms which is 0< TRi<100.Given TRi as the Time Received for the ith node.Then the number of nodes in an instance can be represented as:

$$\begin{cases} 1 \; if \; 0 < x < 100 \\ 0 \; otherwise \end{cases}$$

$$N = \sum_{i=1}^{z} I(TR_i)$$

N is number of vehicles which are found in an instance. For each vehicles in the network 1 to z time received is checked. If 0< TRi<100 then function contributes 1 to sum otherwise if condition not satisfied then 0 is returned.

During authentication some vehicles that are malicious will try to get authenticated. To calculate number of malicious vehicles an indicator function A that represents if a node is an attacker based on status S. Status is false if attacker vehicle. That means authentication is rejected because false node detected. Status is True if legit node and the vehicle is authenticated.

$$\begin{cases} 1 \; if \; S = False \\ 0 \; if \; S = True \end{cases}$$

The total number of malicious vehicles at a given time is calculated as:

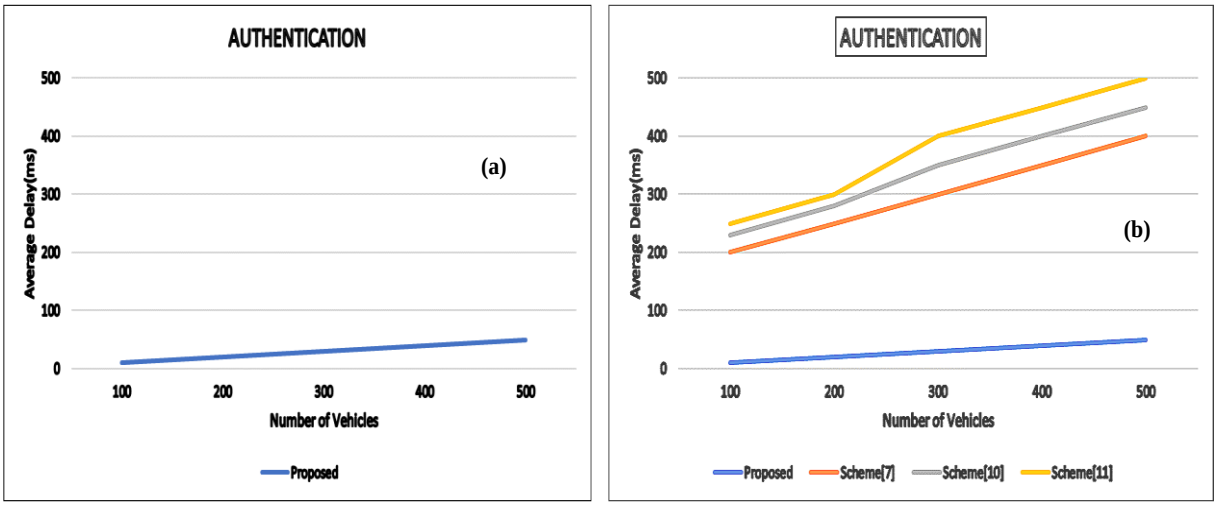

Fig. 7 Authentication process.

$T = \sum_{i=1}^{z} J(S_i) * I(TR_i)$

T is the number of malicious nodes. If status is false it means that there is false node and this contributes 1 to the sum. If status is true then it is not a malicious node therefore it contributes 0.

The Fig. 7a shows the proposed method average delay as the number of vehicles increase at a given time. The proposed method is compared with other approaches in Fig. 7b. The results show that as number of vehicles increase the authentication process is still faster than the other schemes.

For computational process of authentication also processing of given messages at a particular time, the following parameters are used to calculate:

TS=Time Started, TF=Time Finished, WS=Work Size, S=Status (which is 1 if true and) if false)

Computational Process for a period of time is a vehicle is authenticated and sends a message in network.

$$\begin{cases} \dfrac{TF - TS}{WS} & if\ S = 1 \\ 0\ otherwise\ if\ S = 0 \end{cases}$$

If a vehicle is authenticated then S is true, the work done over the period of time is calculated as

$\frac{TF-TS}{WS}$

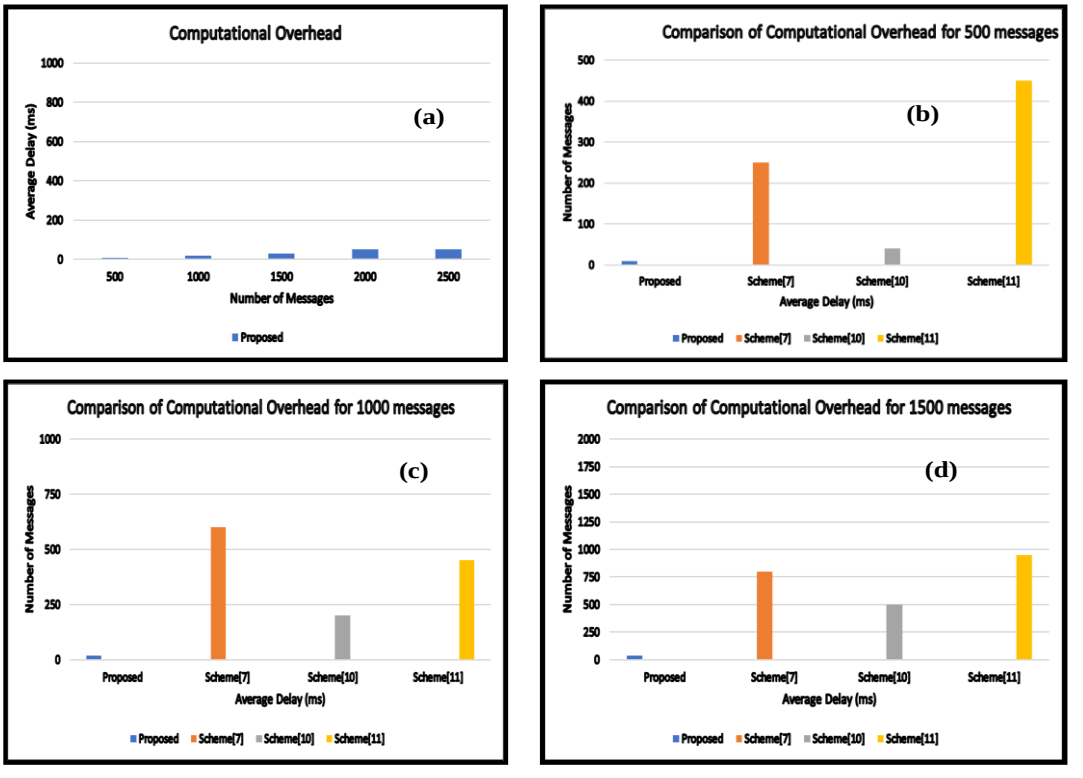

Fig. 8 Computational overhead as messages are processed.

If a vehicle is not authenticated then S is false and 0 is returned.

To calculate the average encryption time for messages the following are taken into consideration. The start time for encryption (Enc S) and the end time of the encryption (Enc F). For a given message M. The time to encrypt this message will be calculated as:

Enc F(M)-Enc S(M)

The average encryption time is calculated as:

$$\sum_{i=1}^{m} \frac{Enc\ F(M) - Enc\ S(M)}{WS * N}$$

The computational overhead was checked by number of messages being transmitted at a time and the average time in milliseconds(ms). The results are shown in Fig. 8.

4. Conclusions

Authentication plays a pivotal role in network security by thwarting unauthorized access attempts. Once a malevolent vehicle is identified, it mitigates the issue of malevolent nodes disseminating harmful messages. In the unlikely event that such messages manage to circumvent the security measures, the implemented blockchain system employs unique transaction identifiers, promptly rejecting any duplicates. Data blocks undergo hashing, with each block's hash generated from the preceding one. The identification of identical hashes results in message rejection, reinforcing the defense against malicious messages. The drawback of the approach is that as we keep increasing the number of transactions in a block then we find that the block creation is delayed than other methods. A tradeoff is required between security and computational overhead. Blockchain technology fosters decentralized and peer-to-peer network architectures, as evidenced by superior computational efficiency and faster authentication processing in the proposed approach. Future research will focus on optimizing blockchain performance within Vehicular Ad Hoc Networks (VANETs).

Conflict of Interest

There is no conflict of interest.

Supporting Information

Not applicable.

References

[1] T. Chatterjee, R. Karmakar, G. Kaddoum, S. Chattopadhyay, S. Chakraborty, A survey of VANET/V2X routing from the perspective of non-learning- and learning-based approaches, *IEEE Access*, 2022, **10**, 23022-23050, doi: 10.1109/ACCESS.2022.3152767.

[2] A. A. Ganin, A. C. Mersky, A. S. Jin, M. Kitsak, J. M. Keisler, I. Linkov, Resilience in intelligent transportation systems (ITS), *Transportation Research Part C: Emerging Technologies*, 2019, **100**, 318-329, doi: 10.1016/j.trc.2019.01.014.

[3] C. M. Chen, K. H. Wang, K. H. Yeh, B. Xiang, T. Y. Wu, Attacks and solutions on a three-party password-based authenticated key exchange protocol for wireless communications, *Journal of Ambient Intelligence and Humanized Computing*, 2019, **10**, 3133-3142, doi: 10.1007/s12652-018-1029-3.

[4] M. A. R. Baee, L. Simpson, E. Foo, J. Pieprzyk, The Security of "2FLIP" Authentication Scheme for VANETs: Attacks and Rectifications, *IEEE Open Journal of Vehicular Technology*, 2022, **4**, 101-113, 2023, doi: 10.1109/OJVT.2022.3217552.

[5] M. A. Al-Shareeda and S. Manickam, A Systematic Literature Review on Security of Vehicular Ad-Hoc Network (VANET) Based on VEINS Framework, *IEEE Access*, 2023, **11**, 46218-46228, 2023, doi: 10.1109/ACCESS.2023.3274774.

[6] D. Zheng, C. Jing, R. Guo, S. Gao, L. Wang, A traceable blockchain-based access authentication system with privacy preservation in VANETs, *IEEE Access*, 1809, **7**, 117716-117726, doi: 10.1109/ACCESS.2019.2936575.

[7] X. Feng, Q. Shi, Q. Xie, L. Wang, P2BA: A privacy-preserving protocol with batch authentication against semi-trusted RSUs in vehicular ad hoc networks, *IEEE Transactions on Information Forensics and Security*, 2021, **16**, 3888-3899, doi: 10.1109/TIFS.2021.3098971.

[8] P. Wang, Y. Liu, SEMA: secure and efficient message authentication protocol for VANETs, *IEEE Systems Journal*, 2021, **15**, 846-855, doi: 10.1109/JSYST.2021.3051435.

[9] J. Lee, G. Kim, A. K. Das, Y. Park, Secure and efficient honey list-based authentication protocol for vehicular ad hoc networks, *IEEE Transactions on Network Science and Engineering*, 2021, **8**, 2412-2425, doi: 10.1109/TNSE.2021.3093435.

[10] A. Aghabagherloo, M. Delavar, J. Mohajeri, M. Salmasizadeh, B. Preneel, An efficient and physically secure privacy-preserving authentication scheme for vehicular ad-hoc NETworks (VANETs), *IEEE Access*, 2022, **10**, 93831-93844, doi: 10.1109/ACCESS.2022.3203580.

[11] M. Luo, Y. Zhou, An efficient conditional privacy-preserving authentication protocol based on generalized ring signcryption for VANETs, *IEEE Transactions on Vehicular Technology*, 2022, **71**, 10001-10015, doi: 10.1109/TVT.2022.3179371.

[12] Z. Lu, Q. Wang, G. Qu, H. Zhang, Z. Liu, A Blockchain-Based Privacy-Preserving Authentication Scheme for VANETs, *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 2019, **27**, 2792-2801, doi: 10.1109/TVLSI.2019.2929420

[13] X. Liu, H. Huang, F. Xiao, Z. Ma, A Blockchain-Based Trust Management With Conditional Privacy-Preserving Announcement Scheme for VANETs, *IEEE Internet of Things Journal*, 2020, **7**, 4101-4112, doi: 10.1109/JIOT.2019.2957421.

[14] D. Wang, X. Zhang, Secure Data Sharing and Customized Services for Intelligent Transportation Based on a Consortium Blockchain, *IEEE Access*, 2020, **8**, 56045-56059, doi:

10.1109/ACCESS.2020.2981945.
[15] Y. Zhao, Y. Wang, P. Wang, H. Yu, PBTM: A Privacy-Preserving Announcement Protocol With Blockchain-Based Trust Management for IoV, *IEEE Systems Journal*, 2022, **16**, 3422-3432, doi: 10.1109/JSYST.2021.3078797
[16] M. U. Javed, A. Jamal, E. H. Alkhammash, M. Hadjouni, S. Ali Bahaj, N. Javaid, Secure message handling in vehicular energy networks using blockchain and artificially intelligent IPFS, *IEEE Access*, 2063, **10**, 82063-82075, doi: 10.1109/ACCESS.2022.3194513.
[17] Y. Yang, L. Wei, J. Wu, C. Long, B. Li, A blockchain-based multidomain authentication scheme for conditional privacy preserving in vehicular ad-hoc network, *IEEE Internet of Things Journal*, 2022, **9**, 8078-8090, doi: 10.1109/JIOT.2021.3107443.
[18] N. Khatri, S. Lee, A. Mateen, S. Y. Nam, Event message clustering algorithm for selection of majority message in VANETs, *IEEE Access*, 2023, **11**, 14621-14635, doi: 10.1109/ACCESS.2023.3244327.
[19] J. Subramani, A. Maria, A. S. Rajasekaran, F. Al-Turjman, M. Gopal, Blockchain-based physically secure and privacy-aware anonymous authentication scheme for fog-based vanets, *IEEE Access*, 1987, **11**, 17138-17150, doi: 10.1109/ACCESS.2022.3230448.
[20] S. Kim, "Impacts of Mobility on Performance of Blockchain in VANET," in *IEEE Access*, 2019, **7**, 68646-68655, doi: 10.1109/ACCESS.2019.2918411
[21] J. Chen, K. Li, P. S. Yu, Privacy-Preserving Deep Learning Model for Decentralized VANETs Using Fully Homomorphic Encryption and Blockchain, *IEEE Transactions on Intelligent Transportation Systems*, 2022, **23**, 11633-11642, doi: 10.1109/TITS.2021.3105682.
[22] G. D. Singh, M. Prateek, S. Kumar, M. Verma, D. Singh, H. -N. Lee, Hybrid Genetic Firefly Algorithm-Based Routing Protocol for VANETs, *IEEE Access*, 2022, **10**, 9142-9151, doi: 10.1109/ACCESS.2022.3142811.
[23] N. Khatri, S. Lee, A. Mateen S. Y. Nam, Event Message Clustering Algorithm for Selection of Majority Message in VANETs, *IEEE Access*, 2023, **11**, 14621-14635, doi: 10.1109/ACCESS.2023.3244327.
[24] J. Subramani, A. Maria, A. S. Rajasekaran, F. Al-Turjman and M. Gopal, "Blockchain-Based Physically Secure and Privacy-Aware Anonymous Authentication Scheme for Fog-Based Vanets," in *IEEE Access*, 2023, **11**, 17138-17150, doi: 10.1109/ACCESS.2022.3230448.
[25] H. Tan, I. Chung, Secure Authentication and Key Management With Blockchain in VANETs, *IEEE Access*, 2020, **8**, 2482-2498, doi: 10.1109/ACCESS.2019.2962387.
[26] Z. Ma, J. Zhang, Y. Guo, Y. Liu, X. Liu, W. He, An Efficient Decentralized Key Management Mechanism for VANET With Blockchain, *IEEE Transactions on Vehicular Technology*, 2020, **69**, 5836-5849, doi: 10.1109/TVT.2020.2972923.
[27] J. S. Alshudukhi, B. A. Mohammed, Z. G. Al-Mekhlafi, Conditional Privacy-Preserving Authentication Scheme Without Using Point Multiplication Operations Based on Elliptic Curve Cryptography (ECC), *IEEE Access*, 2020, **8**, 222032-222040, doi: 10.1109/ACCESS.2020.3044961.
[28] J. S. Alshudukhi, Z. G. Al-Mekhlafi, B. A. Mohammed, A Lightweight Authentication With Privacy-Preserving Scheme for Vehicular Ad Hoc Networks Based on Elliptic Curve Cryptography, *IEEE Access*, 2021, **9**, 15633-15642, doi: 10.1109/ACCESS.2021.3053043.
[29] M. A. Al-Shareeda, M. Anbar, S. Manickam, A. A. Yassin, VPPCS: VANET-Based Privacy-Preserving Communication Scheme, *IEEE Access*, 2020, **8**, 150914-150928, doi: 10.1109/ACCESS.2020.3017018.
[30] S. Sharma, B. Kaushik, M. K. I. Rahmani, M. E. Ahmed, Cryptographic Solution-Based Secure Elliptic Curve Cryptography Enabled Radio Frequency Identification Mutual Authentication Protocol for Internet of Vehicles, *IEEE Access*, 2021, **9**, 147114-147128, doi: 10.1109/ACCESS.2021.3124209.
[31] S. Ullah, J. Zheng, N. Din, M. T. Hussain, F. Ullah, M. Yousaf, Elliptic curve cryptography; Applications, challenges, recent advances, and future trends: a comprehensive survey, *Computer Science Review*, 2023, **47**, 100530, doi: 10.1016/j.cosrev.2022.100530.
[32] Q. Xie, Z. Ding, P. Zheng, Provably Secure and Anonymous V2I and V2V Authentication Protocol for VANETs, *IEEE Transactions on Intelligent Transportation Systems*, 2023, **24**, 7318-7327, doi: 10.1109/TITS.2023.3253710.