Peer-to-Peer Networking and Applications (2021) 14:3198–3212
https://doi.org/10.1007/s12083-021-01079-5

A Blockchain enabled location-privacy preserving scheme for vehicular ad-hoc networks

Bhawna Chaudhary[1] · Karan Singh[1]

Received: 20 September 2020 / Accepted: 13 January 2021 / Published online: 16 March 2021

Abstract
n the imminent future, with the immense need for improving road safety and demand for enhancing the overall driving experience, the utility of vehicular ad-hoc networks technology (VANET) becomes well pronounced. But, the major setbacks of VANET are centralized architecture and the lack of privacy-preserving mechanisms. As it is evident, blockchain technology is gaining attention because of the features like decentralization, distributive, cooperative maintenance and non-tampering nature. This paper presents a decentralized architecture of VANET comprising blockchain technology. The proposed blockchain-based model for VANET works in four stages: blockchain network initialization, vehicle registration, pseudonym upload, and blockchain maintenance. This can efficiently solve the problems emerging in centralized architectures and helps in resolving trust issues between the entities. We propose an algorithm for protecting location privacy and providing anonymity. Experimental analysis proves that the given architecture performs better than the existing solutions.

Keywords Blockchain · Intelligent transport system · Location privacy · Anonymity · VANET

1 Introduction

The number of vehicles production has reached up to 91.78 million and it is foretold that this number will reach 2 billion within the next 10 to 15 years [1].Hence, there is high probability that this will increase congestion and road fatalities that creates a demand for upgraded driving experience and amendments in road safety measures [2]. In a recent issue from the United States Department of Transportation states that approximately 1. 35 million people get injured every year as a result of road traffic crashes [3] and 84% of this can be avoided by implementing ITS (Intelligent transportation system) [4]. To fulfill this requirement, ITS has developed a technology, VANET (vehicular ad-hoc networks) which offers to improve the road conditions by establishing inter-vehicular communication (V2V) and intra-vehicular communication (V2I). These vehicles communicate via dedicated short-range communications (DSRC) radio by exchanging beacon messages [5] or cooperative awareness message (CAMs) or commonly known as pseudonyms. VANETs comprise of multiple nodes that frequently exchange messages with each other directly and indirectly. In indirect communication (V2R), vehicles use infrastructure that involves roadside units (RSU). These RSUs act as a base station in VANETs along with providing coverage to specific range [2, 6, 7]. To maintain a safer and efficient traffic environment RSU sends safety alert notifications to the nodes moving in their proximities and forwards the received messages to the intended recipients. In direct communication, vehicle (node) sends information via commonly known beacons [7]. These beacons carry complete information about the sending node, including its trajectories on the road, heading direction and the query or alert message delivered by the sending node. These safety messages are utilized to provide information such as Co-operative Collision avoidance, as well as by traffic controlling infrastructure to implement traffic efficiency applications [8].

As the communication in VANETs is fully wireless, a malicious node may disrupt the activities of the other nodes by modifying the content of beacons or may even physically harm the driver by following the targeted vehicle or may

This article is part of the Topical Collection: *Special Issue on Cognitive Models for Peer-to-Peer Networking in 5G and Beyond Networks and Systems*
Guest Editors: Anil Kumar Budati, George Ghinea, Dileep Kumar Yadav and R. Hafeez Basha

✉ Karan Singh
karan@mail.jnu.ac.in

Bhawna Chaudhary
bhawna.0101@gmail.com

[1] School of Computer and Systems Sciences, JNU, New Delhi, India

deceive a target vehicle towards the wrong direction by sending false alarms. Therefore, beacons content integrity and authentication must be ensured by the network administrators [9, 10]. The network is compelled to verify whether the content of the received message is reliable and is sent by an authentic node only. The ability to retrieve moving coordinates of a targeted vehicle from beacons disrupts the location privacy of the targeted vehicle. This is one of the significant challenges in VANETs because any node in the network would not like to reveal its location and personal information to any other node.

In order to provide a privacy-preserved environment, many works have been proposed exclusively. Existing privacy frameworks [11, 12] mainly concentrate on creating a central authority (CA) to establish trust and authentication between the participating nodes. The major flaw in these ideas is the centralized network, because if that fails nothing will work efficiently. Also, this makes it more manageable for the attacker to fulfill his malicious intentions by destroying or spoofing the central authority alone. Also, the centralized approaches proposed till date do not claim that CA is a tamper-proof entity. By performing few mining techniques on the pseudonyms, the attacker can find out the users' personal information (his identity, current location, societal status etc..), which will create disruption and insecurity for the life of targeted users'. Another flaw of the centralization system is that the volume of data is increasing drastically, which is building excessive pressure on central entities and leading to the bottleneck problem. Therefore, to ensure the safety of users', it is essential to transfer the VANET to decentralization architecture. The information present in the pseudonyms is encrypted, which does provide the guarantee that data cannot be revealed by the pseudonyms, during their transmission process. However, there is no guarantee that location information and other valuable details available with CA cannot be revealed. Moreover, in recent times users' are being attentive for their data privacy [32, 33]. For this reason, it is very significant to preserve the vehicles' location privacy and identity.

The purpose of this work is to present a model where user's privacy is protected by creating decentralized management and anonymous communication among the nodes, by incorporating the technology of blockchain. Due to data sharing among vehicles certain issues regarding authorization and data security has been raised. The characteristics of decentralized blockchain's architecture protect from security risks brought by centralized data storage. The centralized architecture is also at a risk of single point of failure disrupting the entire network that can be managed by adopting decentralization. Scalability is also a major concern in centralized networks and can be easily solved by decentralization. Recently, blockchain [14] is winning attention from academia and research field. The reason behind this increasing popularity of blockchain in VANETs is its properties namely decentralization, anonymity, and trustworthiness [15]. It works as a distributed public ledger in which encryption is performed using Merkel tree and by calculating hash functions. Also, it follows a consensus mechanism that works on Proof-of-Work (PoW) algorithm [14]. Due to such remarkable features of blockchain, it can be deployed to design a location privacy preserving model for vehicular ad-hoc networks. We also present a blockchain consensus mechanism based on federated blockchain. In vehicular federated blockchain, the consensus scheme performs a crucial decision-making function in determining the authentication and location privacy of a vehicle. We will concentrate on PoW [14] and PoL [16] consensus mechanisms, to provide the security and privacy of federated blockchain.

Key contribution: The key contribution of the work can be summarized as follows:

1. To highlights the problems of centralized architecture in VANET. This work utilizes the benefits of federated blockchain technology and present a decentralized architecture of VANET. The hash value of pseudonym is stored in blockchain, which helps in maintaining the integrity of the messages. Also decrease the processing time and required storage space.
2. We propose to utilize federated blockchain to establish authentication of nodes and maintaining the decentralization in the vehicular network.
3. We deploy smart contracts on the federated vehicular blockchain to accomplish privacy and anonymity in the network.
4. We present a 4-layer model to preserve the location of the vehicles by shredding the work into different layers.

The remaining paper is arranged as follows: Section 2 briefly addresses the previous work by dividing into two categories; one presents the privacy schemes in VANETs without blockchain and the next discusses the details of available schemes with blockchain. Network model overview and the intricate details of proposed scheme are illustrated in section 3. We describe model initialization, location privacy algorithm including blockchain and its contribution in maintaining privacy in section 4. In section 5, we provide privacy analysis and discussion of the experimental results and the conclusion are given in section 6.

2 Related work

This section includes the discussion of the existing schemes in the domain of privacy that mainly focuses on preserving location privacy by using various methods such as k-anonymity, ring signature and group signatures etc. in the first section. In the next section, few schemes are briefly mentioned that uses blockchain mechanism to maintain the privacy in VANETs.

2.1 Traditional privacy schemes without blockchain mechanism

In all the existing propositions, the pseudonym-based authentication mechanism is used to establish trust between the participating nodes. The main flaw in these approaches is that a centralized trust authority is required to maintain the logs of every pseudonym exchange, to safeguard the privacy of the vehicle and to secure the network from attacks. In [2], Lu et al. suggested a bilinear-pairing based protocol to provide the potential amount of conditional privacy for the vehicular nodes. The major contribution of this work is that the RSU has the capability to provide several anonymous keys for all the vehicles, to maintain the privacy of nodes participating in the network. Though, this protocol consumes more response time in the process of pseudonym generation. Also, RSU mandate to notify about the pseudonym to the trusted authority before allotting it to registered vehicles. Additionally, RSU can be swiftly compromised and hence it is not a genuine option to execute the process of pseudonym generation [35, 36]. Thereafter, the group signature-based algorithm was introduced [17], in which authentication process relies upon the signature of a cluster of vehicles. In their work [18], the OBU of a vehicle is not bound to manage a huge number of keys and trusted authority can effectively track down the targeted malicious vehicle. But, OBU are imposed to keep the list of revoked vehicles provided by trusted authority, to obviate to establish any communication with such vehicles. Due to this reason, it couldn't be an effective approach in large networks as process of verifying the vehicles increases consecutively with the enlarged number of revoked vehicles present on the revocation list. In [19], Gamage et al. presented an ID based ring signature approach for VANET to effectively eliminate the privacy concerns of a signing authority for applications of VANET. Still, vehicles can be traceable and conditional privacy issue remain unsolved in the respective method as well. Zhu et al. [20] presented a protocol for vehicular delay tolerant network (DTN) using social-based approach in which privacy-preserving is achieved using packet forwarding. In their model, they have given a packet forwarding protocol for privacy preserving to attain remarkably authentic and secure transmissions. The fundamental advantage of this scheme is that it promises to provide a high packet delivery ratio and thus, able to preserve privacy. However, the shortcoming is that the verification cost of a packet is too high. A distributed certificate service protocol for VANET was proposed by A. Jiang et al. [21]. In this paper, they presented a combined batch verification approach for authentication of signatures, specifically to reduce the authentication overhead in the network. In their work, the verification overhead is significantly decreased. Also, this is the first approach that highlights the assimilation among distributed generation of certificates with the help of RSUs and effective message authentication can be achieved by batch verification. Yet, the major disadvantage of using batch verification method is high packet verification cost is enforced. In recent work [38], a new pseudonym assignment scheme is presented in which two novel adversary placement strategies are deployed. The results given in the work proves that the vehicle traceability is maximum in the proposed work in comparison with the other existing pseudonym assignment methodologies. In [39], the solution of security and privacy is given by implementing the PKI scheme along with identity-based scheme. In the proposed model, a certificate has been issued by the intermediary trusted node and any node cannot enter into the network without carrying the long-term certificate. Identity based signatures are used in the place of bilinear pairing, to verify the certificate revocation lists. The proposed method is suitable for single vehicle or batch authentication and discussed results declares improvement over the other methodologies.

2.2 Privacy schemes using blockchain in VANETs

In [34], a novel automotive security architecture is proposed that employs embedded blockchain distributed feature to eliminate a centralized authority. This paper ensures that the privacy of users can be preserved by using changeable keys. The given model has capability to provide support to emerging automotive services by offering an inviolable and trustworthy way to exchange data, while guaranteeing the safety of the end user. Though, the article covers theoretical aspects of the blockchain but does not present any experimental validation. Another approach is proposed by Ali dorri et al. in [22]. This work gives a model imbibing blockchain technology involving the whole entity set in the life cycle of a vehicle, including insurance companies, software or hardware suppliers, and roadside infrastructure. All transactions between these parties are stored in the blockchain to receive high audibility. Possible attack scenarios are considered to prove the working of the model. In [23], the authors suggested to utilize blockchain technology for providing security to smart vehicles' inter communication using visible light and audible side channels. In their work, public keys of blockchain are used to validate the proposed model through session cryptographic keys, by using either side-channels or public key infrastructure of blockchain technology. This work presented various kinds of secure communication methods via blockchain technology. In [40], Pu et al. have presented an approach using PBFT consensus model for vehicular social networks (VSN). VSN consists various kinds of networks such as cloud networks, edge networks and on road networks. To overcome the privacy and security

flaw, this work analyze the impact of internal and external attacks by considering the two different scenarios. Pseudonyms are used to achieve the anonymization in the network. Results given in the study proves the efficiency of the proposed model. A conditional privacy preserving scheme using blockchain technology protocol is been proposed in [41], which combines the PKI with Ethereum to utilize the secure communication in VANETs. This scheme decreases the need of a large databases of keys required for authentication process by replacing the traditional ECDSA with the modified version of ECDSA (a scheme popularly used for digital signatures). The simulations results proves the feasibility and efficiency of the given model. The major variation between proposed model and the existing models is that this approach is comprehensively dedicated to location privacy of a user. Another vital advantage of proposed work is the decentralization of the vehicular ad-hoc network. While comparing with all the existing approaches, this work is distinctive in three aspects. First, this model does not demand any central authority to maintain the whole network. Secondly, pseudonym-generation and verification process time are slightly lessened. Finally, this model is capable of preserving privacy by applying blockchain technology on RSU's.

3 Background

3.1 Blockchain based vehicular network

Figure 1 depicts the proposed model, it comprises mainly of four layers as the user layer, RSU layer, repository layer and the blockchain network. On the user layer, OBU gathers data out of various pre-installed sensors and transfers them to the next layer i.e. RSU layer. It also communicates with RSUs to access various services. On this layer, the vehicles communicate with nearby RSU to access the existing information. The data taken from vehicles is momentarily stored at RSU and then passed to RA through wired connections. The RA acts as a data center to store large data permanently into blockchain and it performs complicated computing tasks for vehicles. The blockchain deployed RSUs perform the task of ledger management.

3.1.1 Federated blockchain and consensus mechanism

In this work, we use federated Blockchain (FBC) to provide privacy to the network public blockchain (BC). Unlike simple blockchain, FBC (also known as consortium or permissioned blockchain) is a special type of blockchain which works on a

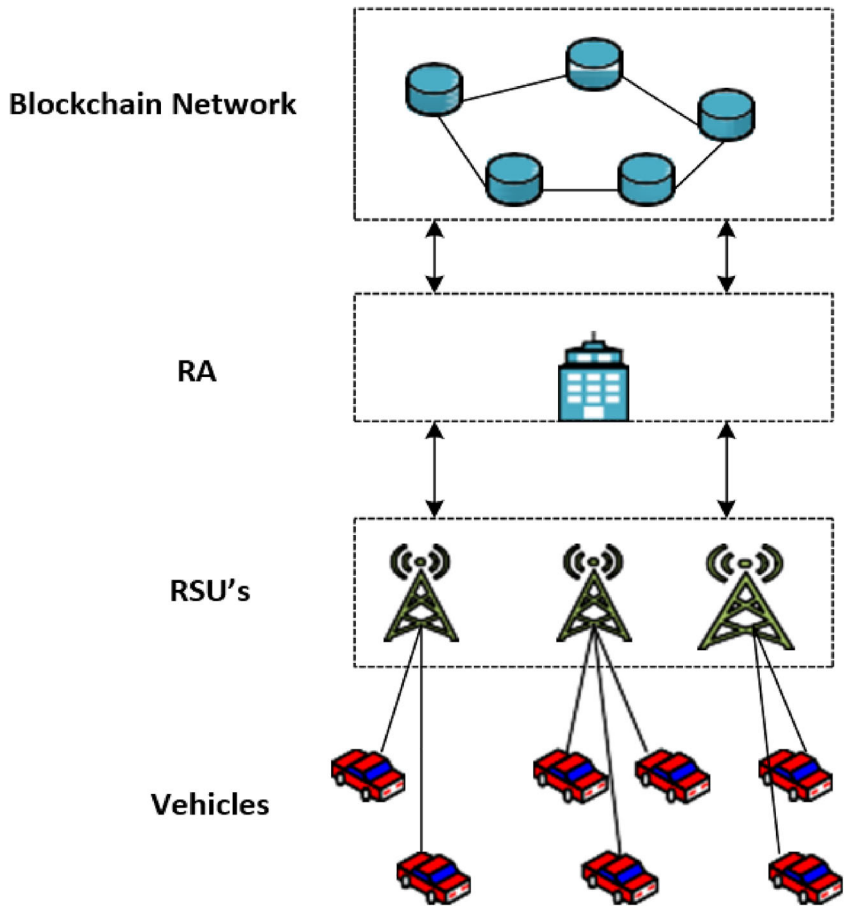

Fig. 1 The proposed architecture of blockchain-based VANET

set of preselected nodes that build distributed shared databases at minimum cost. To maintain the authentication in the network, FBC does not allow any person having access to the internet to participate in the BC network [24]. The consensus process in FBC works on some pre-selected set of RSUs. It is an essential auditing process in which information received from a group of vehicles is stored in the blockchain. Few RSUs are authorized to run the consensus process [25]. The pseudonym set of vehicles and the public/private keys of pseudonym have to be periodically updated. They must contact RA to get a new set of pseudo-identities for them. Whenever a new vehicle moves into the network it is mandatory for the vehicle to participate in the initial registration process. When a vehicle requests for a new pair of pseudonyms, it triggers a smart contract between RSU and the respective vehicle. Smart contracts are self-executing scripts stored on the blockchain, triggered with every transaction in a prescribed manner [16, 24]. Every RSU deployed in the network is required to download and implement smart contract into their blockchain. Whenever there is an occurrence of an event, the vehicle will alert its neighboring vehicles and will also send an alert notification to the nearest RSU BC network. After receiving the alert message, other vehicles verify the location certificate of the originator [26]. If the originator vehicle relates to the same network, then the neighboring node independently verifies the remaining parameters before forwarding it again to prohibit attacks against the network, else they discard the alert message [15]. To add new blocks into a blockchain following steps need to be executed:

Block generation In network abundance of un-analyzed data has been generated by the vehicle nodes. Vehicles use various pseudonyms to encrypt the whole data and to maintain variance between received data. The RSUs acting as data collectors will compile the received un-analyzed data from the vehicles at regular intervals to form a data block and broadcast these data blocks to the remaining RSU. Before embedding a newly created block into the immutable vehicular blockchain, a consensus mechanism shall be fulfilled between the chosen RSU via another process known as proof-of-work. Every newly constructed block consists a field name hash of previous block to remain connected and form a chain of blocks as briefly shown in Fig. 2. These transactions are further merged into the Merkle tree. The Merkle tree root ensures the integrity of the transactions, if any alterations made the value of the root will also change. The payload of the transactions can be calculated by the RSU collection within certain transaction period denoted t_{CP} and the other notations used to describe the time consumed by various process is given in Table 1.

Theoretically, the number of transactions can be defined by the number of moving vehicles in an hour (n_H) in the same block. We can calculate the value of number of transactions (n_T) by the given expression:

Table 1 Notations of time taken by different processes

Symbol	Description
t_{EN}	Time taken in encryption
t_{DE}	Time taken in decryption
t_{SI}	Time taken to sign message
t_{VE}	Signature verification time
n_T	Number of transactions
t_{CP}	Transaction period
t_{BC}	Block preparation time
t_{BT}	Back off time
t_{PO}	Network propagation time

$$n_T = n_H \times t_{CP} \tag{1}$$

The key transmission time taken by traditional structure includes encryption, decryption, signature and verification time. It can be calculated by the following equation:

$$t_{TS} = n_T \times (t_{EN} + t_{DE} + t_{SI} + t_{VE}) + (t_{BT} + t_{PO}) \times 2 \tag{2}$$

In blockchain only signature verification time is required for transactions. However, block creation time is also included in total processing time. It can be calculated by the following equation:

$$t_B = n_T \times t_{VE} + (t_{BT} + t_{PO}) \times 2 + t_{BC} \tag{3}$$

The network propagation time along with back off time is included both the equations and it has been calculated twice considering the two way communication of any message transmission along with the delays.

Proof-of-work for RSU Proof of work is an algorithm to validate the transactions and generate blocks in blockchain. Each RSU collects and validates all the data received from the vehicle nodes and shares the collected data with the other RSUs present in their vehicular blockchain. Every node constructs a new data block of consolidated data repeatedly after a certain period of time and attempts to find a hash value on the basis of criteria of the existing data blocks. As the traditional proof-of-work [14], the hash value should satisfy the predefined difficulty value audited by the blockchain system to modify the production speed of new construction of data blocks.

Proof-of-location for vehicular nodes Proof of location is blockchain's technological way of verifying vehicles location. A proof-of-location (PoL) certificate is used to validate the location of a vehicular node at any specific time [16]. Every vehicle participating in the network must carry a PoL certificate to affirm that the vehicle is placed close to an event spot. Moreover, this PoL certificate has capability to prove the location of a node in any event message to aid the federated

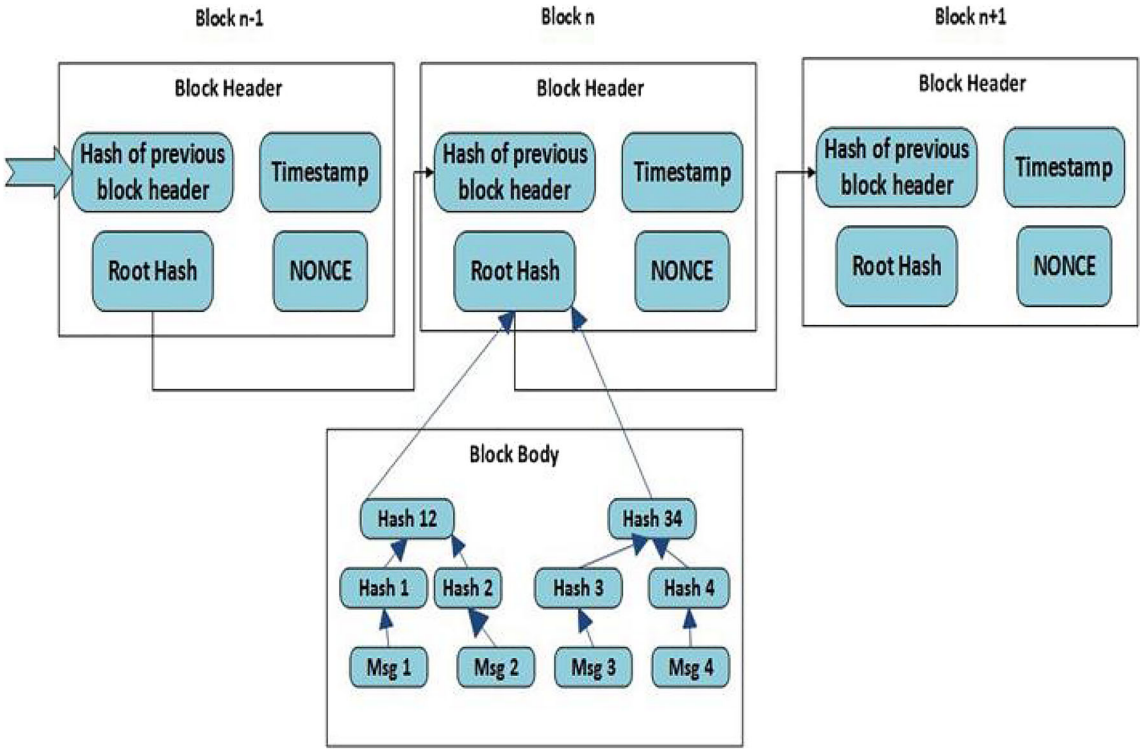

Fig. 2 The depiction of process of a block generation in a blockchain

blockchain. In proposed work, RSU acts as a location certificate validator inside its communication space. Here, we adopt that the vehicle and RSU keep their own set of public/private keys. The vehicle transmits a request message containing its public key (PK_{vi}) to the RSU and then the RSU provides a unique session id the requesting vehicle. Thereafter, the vehicle responds back to RSU with the signed session id. RSU authenticates the signature of the signed session id using the public key of the same vehicle and it also reviews the session-id exchange time. If the session id exchange time is lower than a few milliseconds, then a location certificate having the current location, timestamp and public key of vehicle are signed (using the private key of RSU) and issued by the RSU.

3.2 Location privacy objectives

An effective location privacy preserving model must have the following attributes [12, 27]:

1. **Minimum disclosure:** The measure of shared information by a respective user must be limited to the requisite information to safeguard VANET functionalities.
2. **Anonymity and Traceability:** The messages used in the network must remain anonymous. But this requirement conflicts with accountability i.e. another important security concern in VANET where accountability states that the receiver must have the capacity to verify the sender of a specific message.
3. **Unlinkability:** If communication is established between two nodes, it is complex to figure out if the consecutive messages are transmitted by the same vehicle and they cannot be linked with each other for a very long time except for the trusted authority.
4. **Identity Preserving:** The original identity of every active vehicle must remain unidentified from other cooperating entities of the vehicular ad-hoc networks to sustain the vehicle's privacy from plausible attacks.

3.3 Bilinear mapping

Bilinear mapping [28]: Let G_1 be a multiplicative group and G_2 be an additive group with the order $q = n \times r$ where q is a prime number and n is an integer. Let's take into consideration the higher difficulty of logarithm problem on above mentioned two groups. The e is said to be a bilinear pairing if the mapping of e satisfies for the below three characteristics, where e: G_2x G_2gives G_1.

1. Bilinearity: For any $Q \in G_2$, $R \in G_2$ and a_1, $a_2 \in Zr*$, there exist e(a_1Q, a_2R) = e (Q,R)a_1a_2.

2. Non-degeneracy: The two point Q,$S \in G_2$ must be there such that e (Q,S) =1 or e (S, R) = e (Q,Q), Where the identity element $1 \in G_1$.

3. Computability: An efficient algorithm to calculate e (Q,R) $\in G_1$, where $Q \in G_2$,$R \in G_2$must be there.

4 System model

In this paper, federated blockchain is harnessed to gain decentralization, anonymity and privacy in VANET. The federated blockchain is equipped with smart contracts which help in the establishment of a decentralized environment. The ledgers present in the blocks keep the whole network aware of the updated information. In this section, we present BELP (Blockchain Enabled Location Privacy) model and briefly explain the functioning of the scheme.

4.1 Network model

We focus exclusively on a system of VANET technology in which each vehicle is equipped with a wireless communication module. In proposed model, we include three entities: Registered Authority (RA), Road-Side Unit (RSU), and a vehicle equipped with an On-board Unit (OBU) [14].

1. Vehicle: The vehicle is equipped with On-board Units, computational devices and communication devices that capacitates gathering data from various sources, data processing, and additional sharing. Vehicles may establish their link after pseudonym exchange.
2. OBU: An On-board unit is a combination of software and hardware, developed to deploy a low-cost device, integrated by combining readily available hardware modules from the electronic market, and capable of effectively linking vehicles and road-side networks. These OBU devices aid the vehicle to automatically detect traffic-related events and send warning messages to others using V2V infrastructure, for e.g. the Long-Term Evolution Vehicle-to-Vehicle (LTE-V2V) or dedicated short-range communications (DSRC) [5, 29].
3. RSU: The RSU is located on the roadsides and it can establish a communication link with the vehicles. Also, the RSU acts as a path between vehicles and RA. The main responsibility of RSU is to authenticate the vehicle, process their output locally and then forward the results to traffic management devices. Additionally, they act as access points in the network and keep the vehicles notified about traffic and climate changes.
4. RA: The registered authority (RA) behaves as a repository center of RSU's and the main role is to provide key materials and credentials to vehicles present inside a network. It has the capacity to detect and trace the original identity of vehicles. The data available at RA will present in encrypted form, so no unauthorized node can access the data. For secure communication, RA is directly linked to RSUs via a wired connection.
5. Blockchain Network: To protect the privacy in federated-blockchain VANET, each participating node requires strict management. Thus, this paper uses a private chain to set up a blockchain network. The hash value generated by the whole data will be stored in a blockchain network. This hash value provides certainty that the data cannot be altered or spoofed by any malicious attackers as whenever a data change occurs, its hash value will be recalculated. The federated blockchain is auditable so that any modification can be traced. Additionally, the storage of hash values reduces the need of a larger storing device and lowers down the response time.

This proposed federated blockchain network does not include tokens, we consider the consensus of well-known approach Practical Byzantine Fault Tolerance (PBFT) can be utilized for transaction verification process. Every participating node can vote as per its calculation capability. Before appending a new data block into the blockchain, multiple RSUs (out of pre-selected) need to agree by consensus. Each RSU collects and verifies all the data of vehicles such as pseudonyms, available storage, current speed and moving direction etc. Thereafter, all RSUs broadcast their collected data to the other RSUs and also add this data into their own data blocks periodically (Fig. 3).

4.2 System interconnection

The blockchain based VANET interconnections are shown in 4. 1. This interconnection between the entities happens in four phases given below.

1. Blockchain network initialization: During this step, the system is initialized. Every registered RA gathers to form a blockchain network. Every RA in the network has the same rights and can utilize equally the benefits of blockchain. Smart contract rules are made at this stage. For all the successful rules address will be received from smart contracts.
2. Vehicles registration: When a vehicle joins the network, the vehicle sends a registration request to the nearest RSU and then to RA. Thereafter, RA will forward the request to the smart contract and these contracts will check for its authenticity by the set of predefined authentication rules. If a valid vehicle is requesting, it maintains the validity. If not, it discards the request and sends notification to all the participating nodes and creates a record in blockchain making VANET aware that the vehicle is not valid. The pseudonym token has been sent back to valid vehicles.
3. Pseudonyms upload: For preserving the location privacy and providing anonymity random encryption periods are used in the network. The complete explanation of pseudonyms generation is given in the next section.

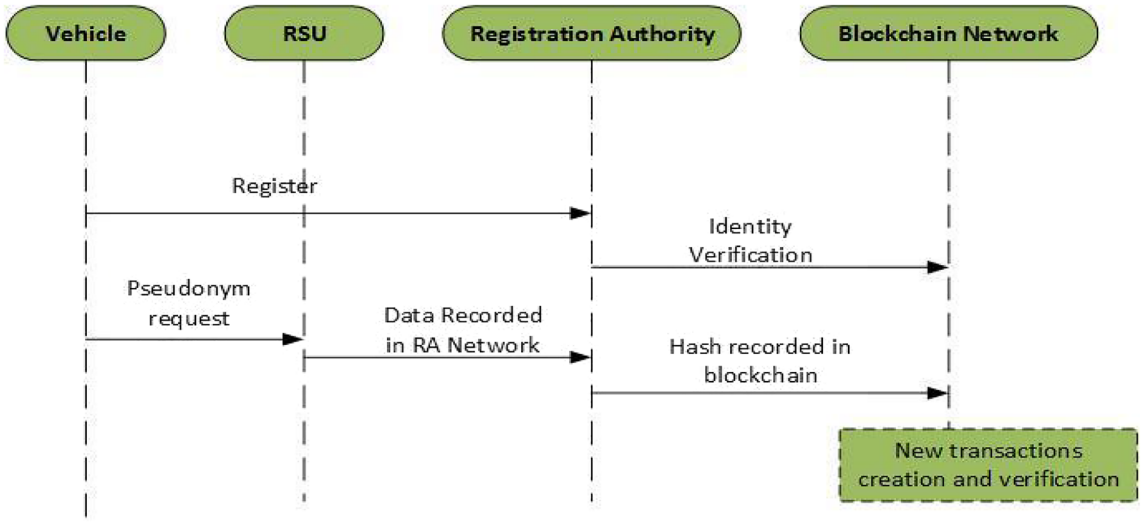

Fig. 3 The interconnection of Federated blockchain VANET

4. Blockchain record: As we know that the processing of each message is a transaction, and its calculated hash value is stored in the blockchain network. Therefore, the calculated hash value of every transaction during a period T is received by blockchain. The agent node of the blockchain broadcasts every newly formed block and finds out that the block has reached the PBFT consensus. It then broadcasts the new block into the network. The newly formed block is considered as valid only if all the transactions entered are valid, otherwise not. Backups of the blocks get created and updated in blockchain only when all the transactions in block are valid and does not exist before.

4.3 System initialization

In this phase, since the vehicles are registered with RA, RA will generate the ticket λ_a as per real identity r_{ID} of the vehicle node and produce the equivalent private key S_a. Thereafter, RA install λ_a and chosen system parameters into tamper proof device of the vehicle V_a. Also, the same information is provided to all RSUs memory. All the notations used in this phase are mentioned in Table 2. The RSU and RA are connected via a secured wired connection, the parameter transmission can happen anytime.

These steps need to be followed for system initialization:

1. V_a submits the r_{ID} to RA and then RA validates the credentials received, if they are valid then it proceeds to next
2. A random number *rnd* is chosen by RA such that *rnd* $\in Z^*q$ and thus determines the private key S_a for the vehicle OBU by using Bilinear pair mapping.
3. RA generates $S_a = H_1\ (r_{IDa}, rnd) \in \{0, 1\}^n$ and provides S_a to the OBU.
4. RA calculates the public key λ_a of the OBU by using $\lambda_a = S_aP \in G_1$.
5. For authenticity, RA signs λ_a as the public key with its own private key i.e. $SIG(\lambda_a, SK_{ra})$.
6. Then RA keeps the mapping of r_{IDa} and tickets given to the vehicle $<\lambda_a, r_{IDa}>$ using bilinear mapping into its database.
7. RA assigns the $<\lambda_a, SIG(\lambda_a, SK_{ra}), S_a>$ as private information of each vehicle V_a and stores the information into TPD of the vehicle.
8. RA communicates the private key SK_x to the RSU.
9. RA publishes public parameters of system $\{rnd, \lambda_i\}$ to the RSU and to all the vehicles.

Algorithm 1: System Initialization

Input: V_a, rnd, G_1, r_{ID}

Output : $\{rnd, \lambda_i\}$

1: V_a submits the r_{ID} to RA

2: if r_{ID} validated by RA then

3: Choose rnd

4: Generate $S_a = H_1\ (r_{ID_a}, rnd) \in \{0, 1\}^n$

5: calculate $\lambda_a = S_aP \in G_1$

6: Sign λ_a with SK_{ra} i.e. $SIG(\lambda_a, SK_{ra})$

7: Store Mapping of r_{ID} and $<\lambda_a, r_{ID_a}>$ using bilinear mapping

8: Store $<\lambda_a, SIG(\lambda_a, SK_{ra}), S_a>$ into TPD of V_a

9: Communicate SK_x to RSU

10: publishes $\{rnd, \lambda_i\}$ to RSU and Vehicles

11: end if

Table 2 Index for key notation

Symbol	Description
r_{ID_a}	The actual id of the vehicle a
P_{IDa}	The pseudo id of vehicle V_a
V_a	The vehicle a
PK_{vi}	The public key of vehicle i
SK_{vi}	The secure/private key of vehicle i
$Sig\ (M;K)$	Signature of message M by using key K
SK_{RA}	The private key of the registration authority
PK_{RA}	The public key of the registration authority
k_a	A key shared between vehicle and RSU
S_a	OBU private key issued by vehicle a
k_a	A group key, issued by every vehicular node participating in the proximity of similar RSU
λ_a	The ticket of a vehicle V_a, issued by RA as its public key
T_{sp}	The time duration of a Pseudonym allocation period

4.4 The generation phase of pseudonyms and access granted to vehicles

After obtaining the ticket λ_a, vehicle V_a approaches to the nearly available roadside unit RSU_i to acquire pseudonym token for itself. V_a sends its public key PK_{vi} to the RSU_i which in turn checks for the legality of vehicle by comparing its credentials (whether the vehicle is registered with RA). After validating from RA, RSU broadcast the status of vehicle (legitimate or not) in the network. Meanwhile, V_a sends λ_a to the RSU_i. After validating that vehicle is legally valid RSU_i issues pseudonym token T (a, i) with the timestamp validity t (a, i) and sends it to V_a including its group key k_g. To determine, the ticket of a vehicle based on its pseudonym, mapping between token and λ_a has been stored by RSU. Multiple tokens have been issued to Vehicle, based on the same ticket λ_a. The message carries all the information related to Token T,T's expiration time, Signature (sig(M,K)), Random number selected by RSU and group key k_g. The dynamic group key $k_g$establishes an encrypted area without interfering with the communication between vehicles. It is managed and updated by RSU and it helps to limit attackers from getting the privacy information from a vehicle.

4.5 The location privacy algorithm

A large number of pseudonyms are obtained by vehicle from RSU along with a group key k_g. To preserve the location privacy by changing the pseudonym, the vehicle starts a random encryption period. During this period if any vehicle prefers to change its pseudonym, the respective vehicle also needs to change other parameters like its speed and driving lane, so that attackers will not be able to trace the trajectory and pseudonym of the vehicle. The specific steps involved in this process are:

1. The vehicle V_a which wishes to replace its pseudonym, submits a request message $M = REQ_{rep}, PS, T_{rep}$ to initiate the random encryption period (rep) to its nearest placed RSU. The V_a encrypts M with its group key k_g and PS is taken as pseudonym-id used by the vehicle and T_{rep} is the length of random encryption period.
2. The vehicles present in the same vicinity decrypt the message M with the group key k_g. If decryption is valid, the vehicle will take part in the process of encrypting its broadcast messages with the same key k_g . All the participating vehicles will form a group i.e., an encrypted group. In case of failed decryption, the remaining vehicles decline the request.
3. During the encryption period, V_a will change its pseudonym along with speed or direction and also monitors the vehicles of the encrypted group.
4. Vehicles of the encrypted group can check their certificate validity. If the remaining time $<=T_{rep}$, the vehicle will change its pseudonym and trajectory.
5. At every pseudonym change, the vehicle must broadcast a response message.
6. V_a monitors that all the vehicles present in the group of encrypted vehicles satisfies the given two conditions: (i) The number of Vehicles who change the pseudonym should not be less than two. (ii) If any vehicle changes pseudonym then it is mandatory to change its speed and direction.

If any of the above conditions is violated before the ending of T_{rep}, a new encryption period will be opened by V_a by broadcasting a request to preserve its own location privacy. This way we can stop external attackers from eavesdropping during a pseudonym change period as the group key is mandatory to participate in the process. If the terminating condition of encryption period is not fulfilled before T_{rep}, V_a will

further send another request message demanding to provide a new encryption slot to preserve its own location privacy.

Algorithm 2 : Algorithm for Location Privacy

Input: $REQ_{rep}, PS, T_{rep}, k_g, t, V$

Output: Encrypted Vehicle Group EN_g

1: $V_a \in$ V encrypt $M = REQ_{rep}, PS, T_{rep}$ with k_g
2: V_a submits M to RSU
3: for M_{resp} do
4: V_i decrypt M with k_g
5: if D_i is valid then
6: Vehicles participates to form EN_g
7: else
Vehicles decline the request
8: end if
9: end for
10: while T_{rep} do
11: V_a changes its pseudonym along with speed and direction
12: V_a monitors vehicle of EN_g
13: V_{en} check certificate validity
14: if $t \leq T_{rep}$ then
15: Vehicle change its pseudonym and trajectory
16: if Pseudonym Change then
17: Vehicle Broadcast M_{resp}
18: end if
19: for V_i belongs to V_{en} do
20: V_a Monitors
21: if $V_{cp} \leq 2$ and V_i Changes pseudonym with speed and direction
22: Get EN_g;
23: else
New Encryption Period Started by broadcasting message;
24: end for
25: end if
26: end while

5 Simulation setup and result analysis

The performance evaluation of the proposed architecture BELP is presented in this section. The next subsection gives details about the simulation environment and thereafter the last subsection discusses the results of the experiments. To understand the improvement suggested by proposed approach, we present a comparison of proposed architecture with a centralized architecture [30]. The centralized architecture used for comparison in this work utilize a method in which a dynamic mix zone is formed on the request of a vehicle. To gain the unlinkability and untraceability in the network this method encrypts the messages in the mix zones. The main difference in the proposed and centralized approach [30] lies in the system designing. In centralized architecture the values are stored directly while in BELP we utilize the advantages of blockchain technology to store the calculated hash value.

5.1 Simulation environment

In the following section, we measure the realizable location privacy considering different traffic scenarios by dividing the given architecture into two parts: Vehicular network and blockchain network. For vehicular network simulation, OPNET [31] is used not only to evaluate the efficiency and performance of the given network but also for generating vehicle mobility to evaluate the normal distribution of vehicles and Poisson arrival rate of incoming vehicles [18]. Ethereum is used to simulate the blockchain network and has the capacity to implement the power of smart contracts, the PoL, and the PoW consensus mechanisms [16]. Therefore, in the conducted experiment, we utilize the ethereum platform to define rules (authentication, revocation, and certificate validation) into smart contracts. The new data block is verified using the PoW and PoL consensus.

Furthermore, to test the performance of proposed model, we have considered a real-world road map of Jaipur city (India) as shown in Fig. 4. The movement of vehicles is fixed within 7 km on the straight suburban Highway from Jagatpura to Bombay Hospital. It has a two-way road with 3 lanes on each side and contains four exit points to leave/ enter the road. We consider two-vehicle movement cases: In case-1, the pseudonym change happens without vehicles switching into the lanes and case-2 enforces the change of pseudonym and lane, to compare the effectiveness of proposed algorithm. The acceleration factor is set to 2 m/s2 to consider red traffic light scenarios at intersections. Table 2 contains the simulation

Table 3 Simulation parameters

Name of parameters	Value
Rate of Arrival	0.008 to 0.200
Variance	1,3,5,7,9,11
Average speed of a vehicle (km/h)	50
Probability	0.08,0.2,0.4,0.6,0.8,0.96
Duration of Simulation(sec)	35,000
Number of Nodes	100
Acceleration factor (m/s^2)	2
Transaction Range	0 to 2000

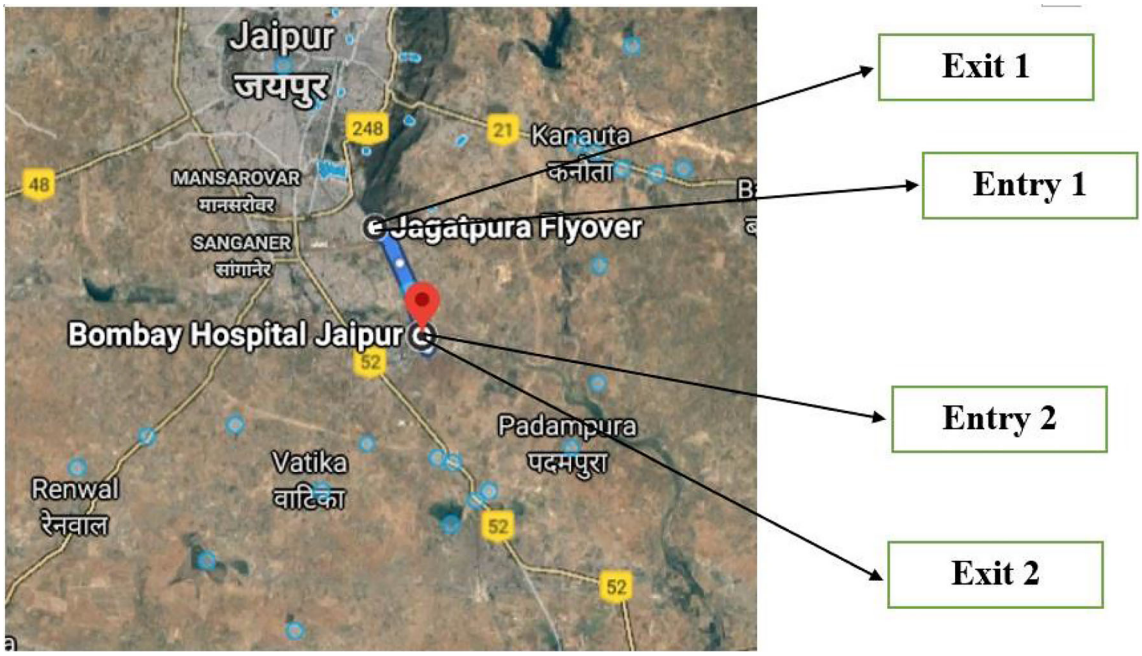

Fig. 4 Simulation setup (suburban highway of Jaipur city)

parameters used in proposed work. To do so, we have assumed the number of vehicular nodes to be 100, running on the average speed of 50 km/h, and simulation run time is 35,000 simulated seconds. The complete information of considered simulation parameters is given in Table 3. For medium access control, IEEE 802. 11 distributed coordination functions are used. We have done the simulations multiple times independently to calculate average system time and for the evaluation of the probability of efficient and fruitful tracking of a target node by an adversary.

5.2 Simulation results

First, we present the time consumed by the various cryptographic methods in proposed algorithm. We then elaborate on the comparison between the system time in the centralized scheme and the proposed scheme. The performance of cryptographic schemes and key distribution can be measured by the occurrence of the number of transactions. The final results vary on the complete set of number of transactions. Therefore, the simulation environment is comprised of the following mentioned steps: (a) in the end of every T_{cp}, a fixed number of transactions are performed in the range of one RSU. The vehicle movement is neglected in this calculation. (b) Transaction numbers ranging from 0 to 2000 are introduced in simulations to calculate the comparison of key transmission time between blockchain and traditional structures. The third simulation shows the assessment of finding efficient tracking of a node by a silent attacker or adversary.

Processing time First, we calculate the processing time consumed by cryptographic schemes. In Fig. 5, we present the processing time of the various cryptographic schemes that are mandated to participate in the key transfer process. The process of encryption and decryption costs approximately equal processing time. The signing and verification process consume the highest processing time as compared to the other methods. The estimation of these methods is essential because signature verification of a node is a significant task in key transfer time and it happens repeatedly in the network.

System time BELP calculates the system time based on two parameters: the blockchain processing time and pseudonym processing time. The Fig. 6 shown represent system time with respect to transaction numbers for both the centralized scheme and proposed scheme (BELP). The transaction range is taken from 1 to 2000 for testing system time calculation. The system time is directly proportional to the transaction number i.e. as the number of transactions increases system time also increases with respect to it. Even though the centralized architecture has only pseudonym processing time, it however consumes more system time as compared to BELP. The fundamental reason for this condition is more waiting time due to the presence of several central entities. And the system time of proposed approach is 3 times less than a centralized approach. In BELP we stored hash values of transactions in the blockchain network which saved a lot of time for larger transaction numbers. So, proposed scheme provides an improvement in scalability even with higher transaction numbers. Hence BELP gives lesser time consumption due to the decentralization property of blockchain.

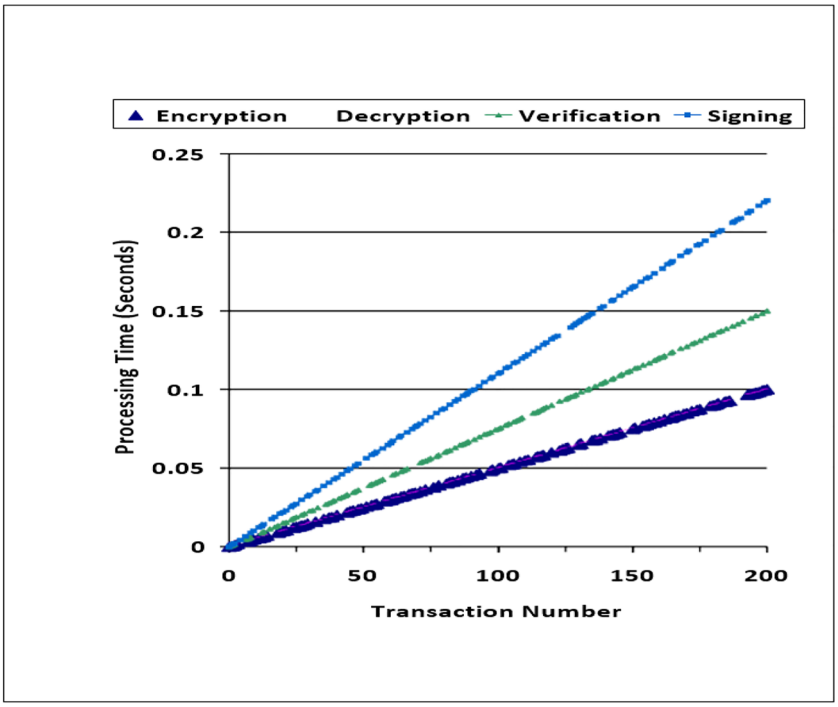

Fig. 5 The computation time required by the cryptographic schemes over transaction number

Probability of location tracking In Fig. 7, the success probability of location tracking is shown by considering different values of vehicle density and variance in speed. Each vehicle follows the proposed scheme (case1). In this simulation, for every vehicle leaving the network, the adversary may pick a node that may reduce the diversity between the average delays time to the leaving time of all the participating vehicles. Also, these vehicles communicate by using pseudonyms but do not switch the lanes after every pseudonym change. Results show that the success rate probability of the adversary declines with respect to the inclination of variance of the vehicular nodes. Also, the probability of location tracking of BELP is lower than DMLP taking the same variance in the account. BELP shows considerably lower tracking in case of both the variances. There is an improvement of 20% with every change of variance.

In Fig. 8, we have considered case 2 and the outcome depicts the success probability of tracking a location while both values of vehicular nodes and the speed of vehicles vary. Each vehicle uses the BELP scheme under case 2. Here, the adversary rule will remain the same as the first case. Each curvature corresponds to distinct values of sigma. The probability of location tracking decreases by 30% with the increase in variance which is more than that of case 1. The results clearly show that location tracking probability of BELP is slightly lower than DMLP. The result of this simulation shows that the case 2 outperforms case1. Therefore, we can conclude

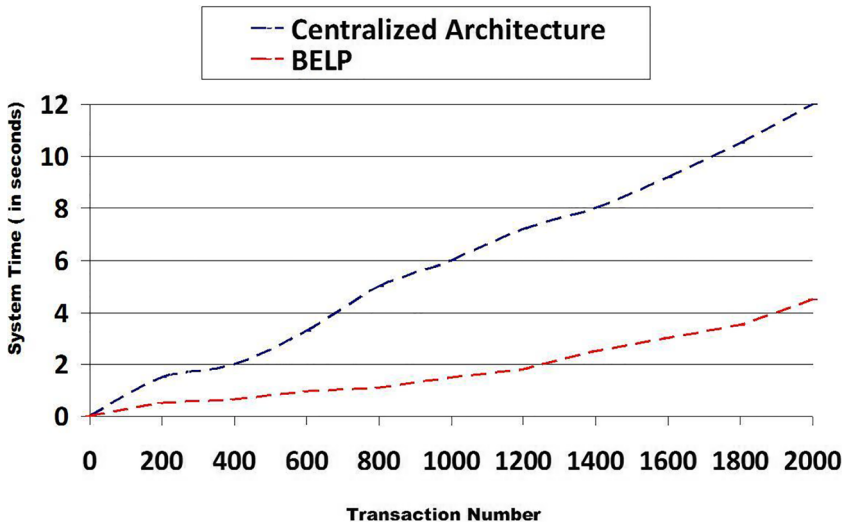

Fig. 6 The System time comparison between Centralized Architecture and BELP

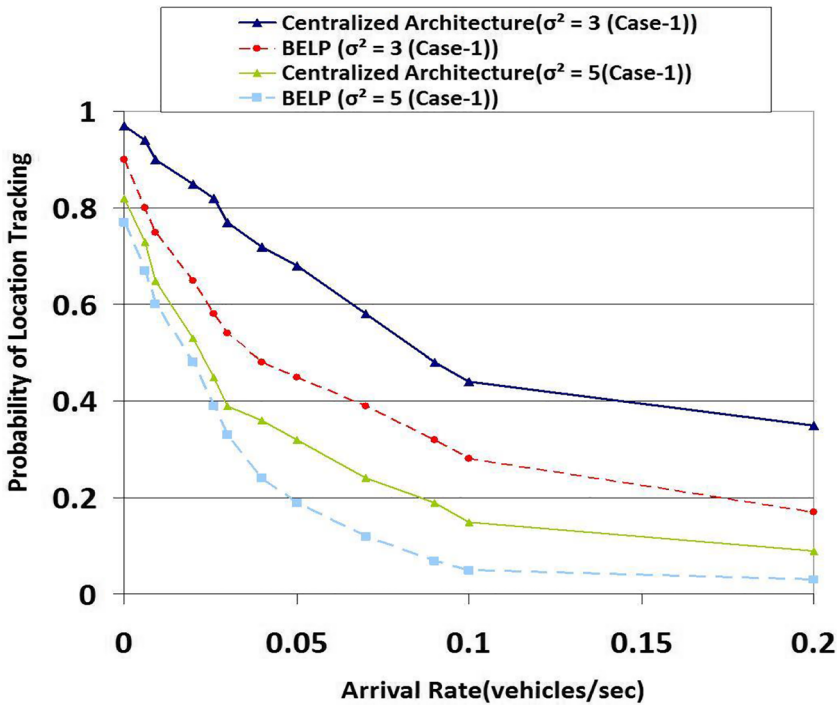

Fig. 7 The success probability tracking rate by an adversary in CASE 1 considering distinct arrival rate and variance

that ability to protect location privacy has been improved significantly using BELP.

On the basis of given algorithm, we have considered two scenarios to calculate the success probability of an adversary (in the first, vehicles cannot change the lanes and in the second, vehicles are allowed to change the lanes and speed) and compared with the traditional centralized approach. In our analysis,the success probability of an adversary has been calculated considering different values of variances and we have achieved that system time consumed by BELP is 3 times better than traditional centralized approach.

Comparative analysis In this section, we present the comparative analysis of proposed BELP scheme with the previously existing schemes. Zhang's scheme gives a model to check the authenticity of the message. In this work, edge computing is used by RSU's to validate the authentic messages. The scheme is capable to achieve the location privacy but fails to establish decentralization [9]. Wang et al. [17], presented the idea of using MAC tag, to reduce the computational overhead. The packet latency and overhead significantly reduced by calculating the hash value associated with the messages. In article [34], fog based vehicular computing framework has been discussed.

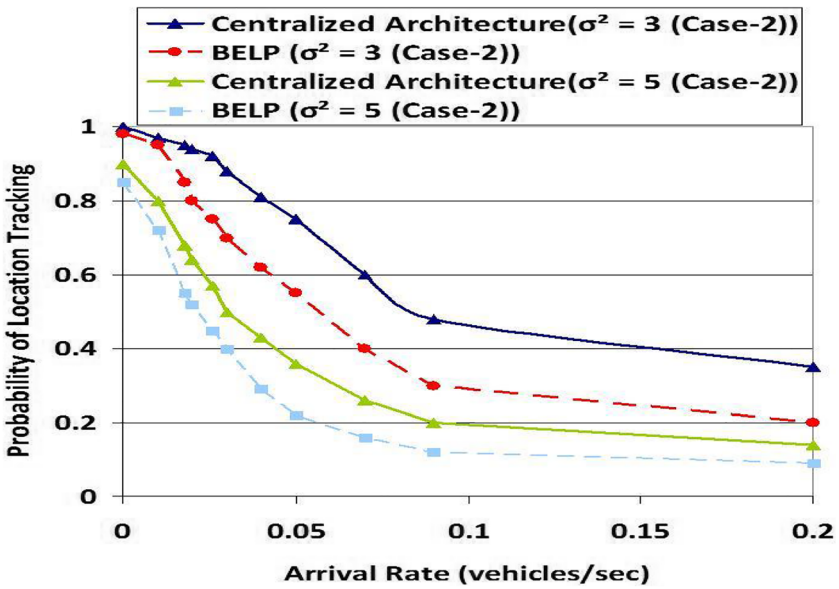

Fig. 8 The success probability tracking rate by an adversary in CASE 2 considering distinct arrival rate and variance

Table 4 The comparison table

Parameters Reference	Message Authentication	Identity Anonymity	Traceability	Unlink-ability	Decentralization	Location Privacy
Zhang's Scheme [9]	✓	✓	✓	✗	✗	✓
Wang's Scheme [17]	✓	✓	✓	✓	✗	✓
Ni's Scheme [34]	✓	✓	✓	✗	✗	✓
Azees Scheme [37]	✓	✓	✓	✓	✗	✓
BELP (Proposed Scheme)	✓	✓	✓	✓	✓	✓

This article highlights the requirement of security and preservation of privacy. Azees et al., presented a scheme for efficient authentication of the messages, which is capable to trace the malicious vehicles and RSU's, also it can prohibit those vehicles to participate in to the VANET [37]. The comparison analysis is shown in the Table 4 and it states that proposed scheme BELP is contained and well-suitable for vehicular ad-hoc networks.

6 Conclusions

In proposed work, we have presented BELP scheme that utilizes the federated blockchain technology to achieve decentralization and efficient computing environment. A system model of blockchain enabled vehicular network is given, including blockchain network initialization, vehicle registration, pseudonyms upload and blockchain maintenance phases. The blockchain enabled vehicular ad-hoc network provides maximum anonymity and unlink-ability in a suburban scenario. Introducing blockchain into the VANET removes the requirement of a central authority or third-party management. The hash value of the pseudonyms will be stored in the blockchain, which provides data integrity and improve the system processing time. Specifically, we have proposed an algorithm which consumes fewer pseudonyms exchange than other schemes to establish the secure communication. A number of simulations have been done to analyse the efficacy and performance of the BELP scheme. The simulation findings indicate that proposed scheme is efficient in providing location privacy preservation as compared to existing centralized architecture. Future work may aim to incorporate edge computing into the vehicular networks by permitting the RSU to mark the rankings of the misbehaving nodes present in their zone, to further improve the computation capability of the vehicular ad-hoc system.

References

1. International Organization of Motor vehicle Manufacturers. Available at http://www.oica.net/category/production-statistics/2019-statistics/ (2019)
2. Wang J, Zhang X, Jia D, Lu K, Shen X (2015) A survey on platoon based vehicular cyber-physical systems. IEEE communications surveys tutorials 18:263–284
3. Department of Transportation. Report on road safety. Available at http://rspcb.safety.fhwa.dot.gov/dashboard/default.aspx (2018)
4. WHO. Global status report on road safety. Available at http://www.who.int/news-room/fact-sheets/detail/road-traffic-injuries (2018)
5. Kenney BJ (2019) Dedicated short-range communications (dsrc) standards in the United States. Proc IEEE 7:1162–1182
6. Semchedine F, Zidani F, Ayaida M (2018) Estimation of neighbours position privacy scheme with an adaptive beaconing approach for location privacy in vanets. Commericial and Electrical Engineering 71:359–371
7. Ruqayah Al-ani, Bo Zhou, Qi Shi, and Ali Sagheer (2018) A survey on secure safety applications in vanet. In 2018 IEEE 20th International Conference on High Performance Computing and Communications; IEEE 16th International Conference on Smart City; IEEE 4th International Conference on Data Science and Systems (HPCC/SmartCity/DSS), pages 1485–1490. IEEE
8. Saad S, Saini I, Jaekel A (2018) Identifying vulnerabilities and attacking capabilities against pseudonym changing schemes in vanet's. In IntConf on Intelligent, Secure, and Dependable Systems in Distributed and Cloud Environments, Springer, pages 1–15
9. Zhang J, Xu Y, Cui J, Wei L, Zhong H (2018) An efficient message authentication scheme based on edge computing for vehicular ad hoc networks. IEEE Trans Intell Transp Syst 99:1–12
10. Singh SK, K., Aziz A (2018) Congestion control in wireless sensor networks by hybrid multi-objective optimization algorithm. Comput Netw 138:90–127
11. Nzouonta J, Rajgure N, Wang N VANET routing on city roads using real-time vehicular traffic information. IEEE Transactions on Vehicular Technology 58:3609–3626
12. Raya M, Jean-Pierre H (2008) Securing vehicular ad hoc networks. Journal of computer security 15:39–68
14. Nakamoto S. Bitcoin: A peer to peer electronic cash system. Available at https://git.dhimmel.com/bitcoin-whitepaper/
15. Zyskind G, Nathan O (2015) Decentralizing privacy: using blockchain to protect personal data. In: IEEE Security and Privacy Workshops, pages 180–184
16. Eris industries documentation smart contracts. Available at http://docs.erisindustries.com/explainers/smart*contracts*/(2016/03/15)
17. Wang X, Ho CZPH, Lin X, Sun X, Shen X (2008) Tsvc: Timed efficient and secure vehicular communications with privacy preserving. IEEE Transactions on Wireless Communications 7:4987–4998
18. Singh K, Osamy W, Aziz A, Khedr AM (2019) Effective algorithm for optimizing compressive sensing in iot and periodic monitoring applications. Journal of Network and Computer Applications 126:12–28
19. Crispo B, Gamage C, Gras B, Tanenbaum AS (2006) An identitybased ring signature scheme with enhanced privacy. Securecomm and Workshops, IEEE, pages 1–5
20. Zhu S, Li Q, Cao G (2010) Routing in socially selfish delay tolerant networks. In Proceedings IEEE INFOCOM, pages 1–9

21. Jiang Y, Wasef A, Shen X (2009) Dcs: an efficient distributed certificate-service scheme for vehicular networks. IEEE Trans Veh Technol 59:533–549
22. Kanhere SS, Dorri A, Steger M, Jurdak R (2019) A blockchain-based Solution to automotive security and privacy. WILEY, 15 edition
23. Gerla M, Huggard M, Rowan S, Clear M, Goldrick CM (2017) Securing vehicle to vehicle communications using blockchain through visible light and acoustic side-channels. arXiv preprint: 1704. 02553
24. Yu R, Ye D, Deng Q, Li Z, Kang J, Zhang Y (2017) Consortium blockchain for secure energy trading in industrial internet of things. IEEE transactions on industrial informatics 14:3690–3700
25. Baliga A (2017) Understanding blockchain consensus models. Technical report
26. Bajracharya R, Shrestha R, Nam SY (2018) Blockchain-based message dissemination in vanet. In: 3rd Int'l Conf on Computing, Communication and Security (ICCCS), IEEE, pages 161–166
27. Ma Z, Schaub F, Kargl F (2009) Privacy requirements in vehicular communication systems. Int'l Conference on Computational Science and Engineering 3:139–145
28. Safavi-Naini R, Zhang F, Susilo W (2004) An efficient signature scheme from bilinear pairings and its applications. In Intl Workshop on Public Key Cryptography, pages 277–290
29. Stancil DD, Bai F, Chang L, Henty B, Mudalige P (2007) Mobile vehicle-to-vehicle narrow-band channel measurement and characterization of the 5. 9 ghz dedicated short range communication (dsrc) frequency band. IEEE Journal on Selected Areas in Communications 25:1501–1516
30. Ying DMB, Mouftah HT (2012) Dynamic mix-zone for location privacy in vehicular networks. IEEE Communications Letters 14:124–1527
31. Chang X (1999) Network simulations with OPNET. In WSC'99. 1999 Winter Simulation Conference Proceedings.'Simulation-A Bridge to the Future'(Cat. No. 99CH37038), pages: 307–314
32. Sun G, Liao D, Li H, Yu H, Chang V. (2017) L2P2: A location-label based approach for privacy preserving in LBS. Future Generation Computer Systems 74: 375–384
33. Liao D, Li H, Sun G (2015) Protecting user trajectory in location-based services. IEEE Globecom, pages 1-6
34. Kanhere SS, Dorri A, Steger M, Jurdak R (2017) Blockchain: a distributed solution to automotive security and privacy. IEEE Commun Mag 55:119–125
35. Ni J, Zhang A, Lin X, Shen X (2017) Security, privacy, and fairness in fog-based vehicular Crowdsensing. IEEE Communications Magazines, pages 146-152
36. Huang D, Mishra S, Verma M, Xue G (2011) PACP: an efficient pseudonymous authentication-based conditional privacy protocol for VANETs. IEEE Transactions on Intelligent Transportation Systems, pages 12:736–746
37. Azees M, Vijayakumar P, Deboarh LJ (2017) EAPP: efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks. IEEE Transactions on Intelligent Transportation Systems 18:2467–2476
38. Saini I, Amour B, Jaekel A (2020) Intelligent adversary placements for privacy evaluation in VANET, information, MDPI, pages: 11:443
39. Wang S, Mao K, Zhan F, Liu D (2020) Hybrid conditional privacy-preserving authentication scheme for VANETs. Peer-to-Peer Networking and Applications, Springer, pages 10:1–6
40. Pu Y, Xiang T, Hu C, Alrawais A, Yan H (2020) An efficient blockchain-based privacy preserving scheme for vehicular social networks. Information Sciences, Elsevier, pages 540:308–324
41. Lin C, He D, Huang X, Kumar N, Choo KK (2020) BCPPA: a blockchain-based conditional privacy-preserving authentication protocol for vehicular Ad Hoc Networks. IEEE Transactions on Intelligent Transportation Systems pages 1-13

Bhawna Chaudhary did her B. Tech in Computer Science and Engineering in 2008 from Univesity of Rajisthan, Jaipur, She did her M. Tech in Information Security in 2010 and is currently pursuing her PhD degree with Jawaharlal Nehru University of India. She have five yrars teaching experience and curntly working in SKIT, Jaipur. Her research interests are in the area of Computer Network, VANET, and Security networks

Karan Singh is working with School of Computer & Systems Sciences, Jawaharlal Nehru University, New Delhi. He work as proctor and many committee members at Gautam Buddha University. He is member of Admission and placement committee at school level. His primary research interests are in computer network, computer network security, Multicast communication and Software Define Network. He supervised six Ph.D. and thorty nine M.Tech. students. He is reviewer of IEEE & Elsevier conferences and reviewer of International Journals & IEEE Transactions. He is an Editorial Board Member of Journal of Communications and Network (CN), USA. He published eighty plus research papers in journal and good conference. He organized of various workshop, Session, Conference and training. Dr. Singh worked as General Chair of international conference (Qshine) in year 2013 at Gautam Buddha University. Recently, he organized a International Conference "NetCrypt 2019" at JNU, New Delhi. He was nominated for Who's who in World in year 2008. Dr. Singh has been joined as Professional member Association for Computing Machinery (ACM), New York, Computer Science Teachers Association (CSTA) U.S.A, Computer Society of India (CSI), Secunderabad, India, Cryptology Research Society of India (CRSI), Kolkata, India, Institute of Electrical and Electronics Engineers (IEEE), USA, International Association of Computer Science and Information Technology (IACSIT), Singapore, Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering (ICST), America, International Association of Engineers (IAENG), Hong Kong, Association of Computer Electronics and Electrical Engineers (ACEEE), India, Internet Society(ISOC), USA and Academy & Industry Research Collaboration Center (AIRCC), India