
Scalable Computing: Practice and Experience, ISSN 1895-1767, http://www.scpe.org
© 2024 SCPE. Volume 25, Issues 1, pp. 593–605, DOI 10.12694/scpe.v25i1.2406

NOVEL AUTHENTICATED STRATEGY FOR SECURITY ENHANCEMENT IN VANET SYSTEM USING BLOCK CHAIN ASSISTED NOVEL ROUTING PROTOCOL

ANAND N PATIL*AND SUJATA V MALLAPUR†

Abstract. In recent days, the fast growth of Vehicular Ad-Hoc Network has made smart driving practicable. The VANET performs communication with other vehicles with the intention of improving traffic flow and eliminating accidents and road hazards. VANET is nonetheless susceptible to security attacks by malicious users because of the open wireless nature of the communication channels. As a result, in this proposed system, the novel authenticated strategy for security enhancement in VANET system using block chain assisted novel routing protocol is implemented to prevent from vulnerable attacks. When vehicle enters a new roadside zone, it must continue the reauthentication procedure using the current RSU, which lowers the VANET system's overall effectiveness. Consequently, those mentioned problems are solved via blockchain technology. Reauthentication is effectively accomplished through safe authentication code transmission between the succeeding RSUs thanks to the decentralized nature of blockchain technology. The proposed system's reliability robustness against numerous harmful threats assures that it provides superior security. Furthermore, the Horse Optimization Algorithm based routing protocol assisted with blockchain technology used in this approach significantly reduce the computational and communication cost when compared to traditional approaches. To evaluate the effectiveness of blockchain assisted routing protocol, performance parameters such as PDR, routing overhead, throughput, communication and computational cost with varying scalabilities are measured. According to the findings, the proposed system works better than other existing approaches. In addition to this, our proposed framework substantially guarantees a secure and trustworthy vehicular environment with user privacy preserved.

Key words: Vehicular Ad-hoc Network (VANET), Blockchain, Roadside units (RSU), Horse Optimization Algorithm (HOA)

1. Introduction. VANET is gaining great attention in the exchange of information on smart cars and smart public transit systems. The advent of Vehicular Ad-hoc Networks (VANETs) offers consumers a more practical as well as comfortable driving experience [1]. However, with VANETs, authentication and user privacy continue to be important challenges. Internal vehicle broadcasting of bogus messages must be stopped in order to safeguard vehicles' confidentiality from sneaky attacks. As a result of the interacting channels between wireless nodes being public and unprotected by any form of security measures, VANET is subject to a variety of safety and transparency problems. Furthermore, the traditional manner of transactional data storage lacks distributed and decentralised security, making it possible for a third party to start being dishonest. In order to prevent assaults like physical and eavesdropping attacks, an individual's confidentiality and delicate details, such as actual identity-related data, must be securely protected [2-6]. One of the most harmful attacks is Data Poisoning attacks, which act to reduce the trustworthiness of data interchange [7]. Hence to enhance the trustworthiness, secure and efficient message authentication protocol is used [8]. It tries to achieve mutual authentication across vehicles and roadside units (RSUs). But they fail to meet the need of authenticating hundreds of messages each second in VANETs [9]. In general, the architecture of VANET consist of two layers. The bottom layer involves onboard units and roadside units. The onboard units in the top layer affixed to the vehicles enables wireless communication and the roadside units act as an intermediary-nodes put on roadsides, which act as a link from the top layer and the OBUs. Each vehicle utilizes the OBU to periodically transmit messages about the flow of traffic, including its speed, position, and current road conditions. The RSU gets traffic-related informations from vehicles within its communication range and transmits valid messages to the application server for further analysis.

In an effort to meet the VANETs security standards, several security solutions or systems have been offered in numerous studies, particularly in the previous ten years. Even while such initiatives can meet many

*Assistant Professor, Dept. of CSE, Sharnbasva University, Kalaburagi, Karnataka 585102, India (corresponding author: patilanand1990@gmail.com)
†Professor, Dept.of AI& ML, Sharnbasva University, Kalaburagi, 585102, India (sujatamallapur@gmail.com)

of the security and effectiveness requirements for VANETs, they are prone to a variety of serious reliability, safety, and confidentiality issues. Additionally, most of the strategies proposed are based on the assumption that perpetual delicate data should be stored in a perfect tamperproof device (TPD), that shouldn't ever be breached, physically cloneable, or vulnerable to attacks via side channels by an adversary party [10]. But in reality, this assumption's viability could not be feasible. The confidentiality and safety aspects of the information distribution process in VANETs are significantly impacted by the authentication system. With its plentiful storage and processing resources, certain common technologies, such as cloud computing [11, 12] is utilized which enhances the efficiency. The OBUs that store sensitive data typically validate 1000 to 5000 messages per second for 100 to 500 automobiles are within their contact radius. In this situation, cloud-assisted VANET has substantially helped OBUs to handle the significant processing task load while enhancing traffic efficiency and road safety. However, relational databases, which are typically used by cloud providers to store metadata, are open to privacy violations from the perspective of users' data [13]. In order to solve this, encryption is utilized to safeguard the secrecy of the user, but the inquiry may reveal the user's information and location [14]. Hence, the soft computing approach such as machine learning and deep learning approaches were used. Despite the fact that these two approaches function well in intrusion detection systems [15], the machine learning strategy fails to identify attacks when there are a large number of vehicle nodes in the VANET system [16], and the most intrusion detection system employing deep learning has a longer detection time [17]. To address this aforementioned problem, Block chain is used in this system. The blockchain network's main advantage is that, due to its extremely cheap computational costs, it can successfully address problems with unidentified authentication [18].

To perform optimal route selection to transfer the packet from source to destination node. Routing protocol is used in the VANET system. Due to the resilient nature of vehicle mobility, traditional optimisation algorithms are locked with limited optimal paths [19]. To manage this IoT-based route-discovery process, many optimisation techniques such as the genetic algorithm (GA), particle swarm optimisation (PSO), and cuckoo search optimisation (CSO) [20-23] have been converted from continuous to discrete space. Algorithms' poor convergence has been produced by parameter tweaking and the conversion from continuous to discrete space, which are out of balance with intensification and diversity. Furthermore, its search procedure fails to have exclusivity and selectivity. So, an effective optimization-based routing technique is used in this approach to sort out this problem. Several privacy preserving authentication schemes [24-26] are used to improve security in the VANET system. However, it provides better security, it possess high computational and communication cost.

To sort out all these problems, in this proposed system, a novel authenticated strategy for security enhancement in VANET system using blockchain assisted novel routing protocol is employed. The contribution of our work are as follows:

1. An authentication scheme followed by vehicle initialization and registration is established for the security in VANET system
2. Blockchain-enabled exchange protocol that makes it possible to transfer possession of a vehicle in a distributed, safe manner
3. Detection of malicious node in VANET is developed with enhanced security
4. Lightweight pseudonym management scheme for VANET legitimacy via block chain is developed

The paper is constructed accordingly: An authentication scheme followed by vehicle initialization and registration is done. After authentication, an algorithm is developed to detect the malicious node with enhanced security and finally the section 2 is finished with the pseudonym management scheme The findings and analysis are finished in part 3, and the section's conclusion is made in section 4.

2. Proposed system. The motivation of the proposed system is to facilitate secure and reliable mechanisms for data forwarding. In the proposed system, initially drivers of the vehicles must enter their confidential details about the vehicle directly to the closest Trusted Authority (TA). Only the TA maintains the data with the highest level of security in its database. The TA will track the genuine identity of the vehicle from the fictious identities using this sensitive information in the event disputes. The RSUs and motor units effectively finish their first-time verification with the TA to get an authentication key and the pseudonym identification. After the first step of authentication in the TA is complete according to the authentication code, the RSU

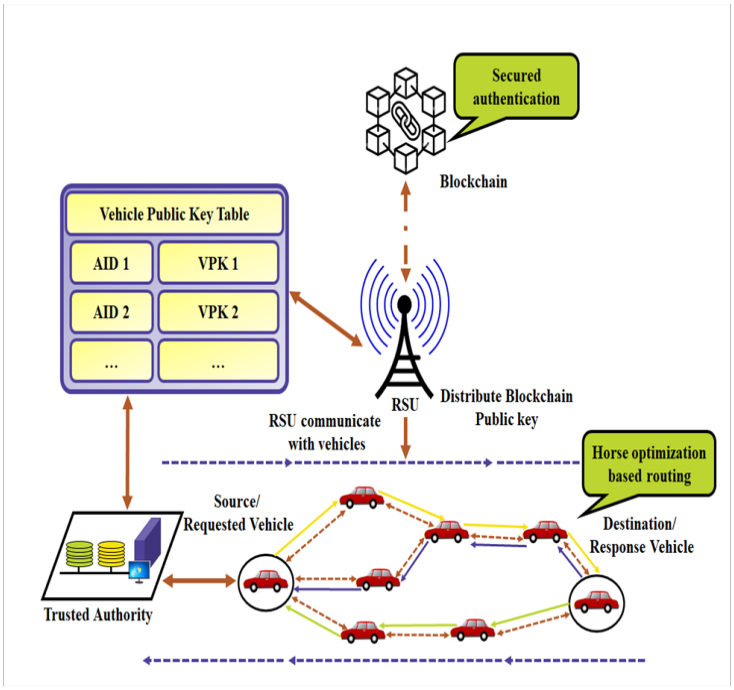

Fig. 2.1: Block diagram of proposed system

executes authentication process in the vehicle using the blockchain network as users enter the service zone of RSU. Then, when the vehicles enter into the communication range of current RSU, the current RSU performs authentication depending upon the handover certificate provided by the former RSU. The vehicle will be given the authentication token after the procedure is accomplished.

After the completion of authentication procedure, routing is performed to select the optimal path when transmission takes place from one user to another. To perform transmission in a secured way, a pseudonym management scheme is performed after the malicious node detection. Hence, in this proposed system, the high level security is achieved with better efficiency.

2.1. Authentication . This section describes the three steps of the envisioned authentication strategy, initialization, registration, and authentication.

2.1.1. Initialization Phase. The system seeks to generate private keys for the trusted authority during its initial setup. The TA results in two looping groupings which is represented as G_1 and G_2. It is generated with order p which fulfills the bilinear map relation $e : G_1 * G_2 \rightarrow G_T$. g_1 and g_2 are considered as the producers of the cyclic groups G_1, G_2 respectively. Furthermore, the trusted authority selects three cryptographics such as H_1, H_2 and H_3, where H_1, H_2 and H_3 is represented by:

$$H_1 : G_1 \rightarrow \{0,1\}^* \tag{2.1}$$

$$H_2\{0,1\}^* \rightarrow Z_q^* \tag{2.2}$$

$$H_3 : \{0,1\}.^* \rightarrow Z_q^* \tag{2.3}$$

The TA generates its public key $(Q_T A)$ by randomly selecting the private key β, where $Q_T A$ is computed as

$$Q_T A = g_1^{\beta} \tag{2.4}$$

Also, these TA generates system parameters such as $p, g_1, g_2, G_1, G_2, G_T, e, H_1, H_2, H_3, Q_T A$.

2.2. Registration phase. For vehicle and RSUs, in-person registration is completed in the TA as detailed below. To perform registration, users of the vehicle have to provide all required personal details, comprising of their contact details, email and postal address. Following the successful submission and validation of the private information by the TA, which selects a random integer $u_i \epsilon Z_q^*$ for every vehicle owner and estimates $PK_v = g_1^(u_j)$ to be the user's public key. Following the automobile's successful registration in the TA, The vehicle user is then covertly given both the private and public key while offline. Additionally, the TA creates a code of authentication for every single user according to the time as given below:

$$AC(t) = \frac{\sum_{i=1}^{n} v_i a_i}{nn} \tag{2.5}$$

Here $v_i \epsilon Z_q^*$ indicates the value of identity selected by the trusted authority for each vehicle user, $a_1 \epsilon Z_q^*$ denotes the identity value which is provided by automobile owner to the TA at the period of registration, and n represents the total amount of vehicles. Once the Authentication code is produced, the TA encrypts the vehicle transaction information with session keys that have been mutually agreed upon by the TAs before broadcasting it to all the trusted authorities. After receiving the transmitted message from the neighbourhood TA, every TA is committed to resolving the riddle. A confirmed authentication code along with the pseudonym is then added as a new block to the end of the block chain when the minor has successfully solved the riddle. In order to protect each vehicle's genuine identity from other network entities, the TA also generates a pseudonym identity for it. The TA aids in performing updation and storing the every vehicle's owner authorization code in the blockchain. Finally, each TA and RSU maintains a duplicate of the most current blockchain in its database as soon as the verified AC has been connected to the block chain in order to examine the new RSUs in the VANET. These values for each vehicle are updated in the block chain.

2.2.1. Authentication phase. This stage of the authentication procedure is done in the vehicle by the RSU and this process is done by using the authentication code which TA generates while the registration procedure is underway. In the authentication phase, As the automobile approaches the RSUs network coverage region, an RSU is needed to verify a vehicle user's validity in an anonymous manner. The vehicle user will provide the pseudonym ID and node number to the RSU once he has arrived at the first RSU region. RSU validates the pseudonym's authentication code and identity. This phase creates a session key between the RSU and the vehicle, as seen below. The car proprietor calculates session key as given in equation

$$SK_v = PK_r^{u_i} \tag{2.6}$$

where $PK_r = g_2^k i$ and k_i represents the public and private key of the RSU. In the same way, the RSU computes session key as given in equation:

$$SK_{r,1} = PK_v^{K_i} \tag{2.7}$$

where $PK_v = g_1^{u_i}$ indicates the vehicle user's public key. After this process, the RSU chooses a master key $r_i \epsilon Z_q^*$ and computes:

$$K_r = g_1^{r_i} \tag{2.8}$$

The value of SK_r is maintained secretly by the RSU. Moreover, the RSU computes:

$$PK_{r,1} = g_2^{r_i} \tag{2.9}$$

The calculated value is delivered to the owner along with a timestamp value T_1.

The driver of the vehicle then confirms the youthfulness of the time-stamp T_1 thereby calculating $SK_{v,1}$ accordingly:

$$SK_{v,1} = PK_{r,1}.SK_V^{(H_2(ID|(|AC|)|T_1||H_1(SK_v)))} \tag{2.10}$$

where, ID identifies the user of the vehicle using a pseudonym. Afterwards, the session key created using the vehicle is computed as follows:

$$SK = e(SK_{v,1}, g_1) \tag{2.11}$$

Following that, the RSU determines the session key accordingly:

$$SK_{r,2} = SK_r.SK_{r,1}^{H_2(ID|(|AC|)|T_1||H_1(SK_r,1))} \tag{2.12}$$

The vehicle is deemed to be outlawed and the RSU fails to provide services if the vehicle's Authentication Code is classified as zero. The blockchain's tamper-resistance capability prevents revoked vehicle consumers from passing for regular vehicles and forbids them exchanging information involving the RSU. The RSU generates the session key as shown below:

$$SK = e(g_2, SK_{r,2}) \tag{2.13}$$

Verification

$$SK = e(g_2, SK_{r,2}) = e(SK_{v,1}, g_1) \tag{2.14}$$

After performing authentication, routing is performed to select the most efficient way to transfer the data between sources and destinations. In this system, HOA based routing technique is used with blockchain technology to perform efficient routing approach that occurs during a safe and evenly dispersed handover of control from one automobile user to another.

2.3. Blockchain assisted HOA based routing protocol. To carry out the routing process, HOA is implemented. The hierarchical structure of horse herds serves as the primary source of inspiration for HOA. Horses favour living in herds. Since many animals coexist in big groups, it is crucial to establish a stable hierarchy in order to promote social cohesion and reduce aggressiveness. The conduct of the horses adopts a hierarchical structure after they form a herd; the animals in the herd with the highest status tend to drink and eat first. Low-status herd members eat later, and occasionally some may not receive enough food. High-ranking horses may have prohibited lower-ranking horses from eating at all in the event that there was little available feed. Horse herds contain a dominant mare and the hierarchy of the horses within a herd determines which horses have priority access to resources. The primary stage of the strategy determines a horse's position in a herd by taking into account its fitness value for that particular herd. Assume there are k horses in the herd, and P stands for a function.

$$Herd = H_1, , H_k \tag{2.15}$$

$$P = Herd \rightarrow 1, , K \tag{2.16}$$

If fitness$(H_x) \leq$ fitness (H_y) where $x \neq$y and $x, y\epsilon 1, ..., k$ then $P(H_x) > P(H_y)$ If fitness H_x=fitness(H_y) where $x \neq y$ and $x, y\epsilon 1, ...k$ then $P(H_x) - P(H_y)](x - y) > 0$ For each horse, the rank is determined as follows:

$$H_x - Rankofeachhorse = (P(H_x))/K \tag{2.17}$$

Every herd has a centre, which is the weighted average of the horse's placement within the herd. The status of the horse is thus represented by the weight. The following formula is used to determine the herds' centre:

$$Herd_{center} = \frac{\sum_{x=1}^{k} z_x H_x.rank}{\sum_{x=1}^{k} H_x.rank} \tag{2.18}$$

Euclidean distance is computed to determine the location between the stallion and the horse herd's center:

$$Dim(stallion, herd) = \sqrt{\sum_{y=1}^{D} im(stallion_y - Herd_{center})^2} \tag{2.19}$$

where Dim is the totality of search space dimensions. If a horse is a member of a herd, its velocity is modified as follows:

$$Vel_{x,y}^{T+1} = Vel_{x,y}^{T} + H_{x.rank} * (Herd_{center,y}^{T} - Z_{x,y}^{T}) \tag{2.20}$$

$$Vel_{x,y}^{T+1} = Vel_{x,y}^{T} + H_{Rand} * (Herd_{center,y}^{T} - Z_{x,y}^{T}) \tag{2.21}$$

Rand is a random value ranging from 0 to 1. The current iteration is denoted by T, while the next iteration is denoted by $T+1$. The horse memory (Mem) is a matrix with the same number of rows as the HMP values in the D column and the horse.

$$Mem_{x}^{T+1} = \begin{bmatrix} Mem_{1,x,1}^{T+1} & .... & Mem_{1,x,D}^{T+1} \\ .... & .... & .... \\ Mem_{HMP,x,1}^{T+1} & .... & Mem_{Hmp,x,1}^{T+1} \end{bmatrix}$$

The memory matrix's cells are updated using this equation.

$$Mem_{k,x,y}^{T+1} = Z_{x,y}^{T+1} * N(0, SD) \tag{2.22}$$

where N stands for a normal distribution (SD) with a mean of zero. Every possible solution or path is assigned a fitness value by HOA. The HOA-based routing technique's objective is to select the route that requires the least amount of energy and travel time. The fitness function, which is illustrated as follows, can be thought of as a minimization function.

$$F - t = minRE_i * DIST_i \tag{2.23}$$

where F_i represents the fitness function of population i, RE_i is the energy required by the i^{th} population. $Dist_i$ represents the overall distance of i^{th} route. The pathways that already exist are initialized as principal populations in HOA. Following are the potential routes.

$$Sol = P_i, i = 1, 2, , N \tag{2.24}$$

The initial set of population is represented by Sol and N indicates the route count. The path's distance and overall energy expenditure are provided by,

$$P = RE, DIST \tag{2.25}$$

where DIST stands for the overall distance and RE stands for the node's remaining energy in the path.

$$RE = f_1 = \sigma_R E = \sqrt{(1/N) \sum_{i=1}^{n} \mu_{RE} - e(node_j)^2} \tag{2.26}$$

$$\mu_{RE} = 1/n \sum_{i=1}^{n} E(node_i) \tag{2.27}$$

when calculating the value of uniform load dispersion across sensors, the standard deviation for RE (σ_{RE}) is used. A routing technique determined by the Horse Optimisation Algorithm (HOA) is used for identifying the best routes depending on fitness function. Additionally, to enable shared memory across network points, the HOA-based routing approach uses blockchain technology.

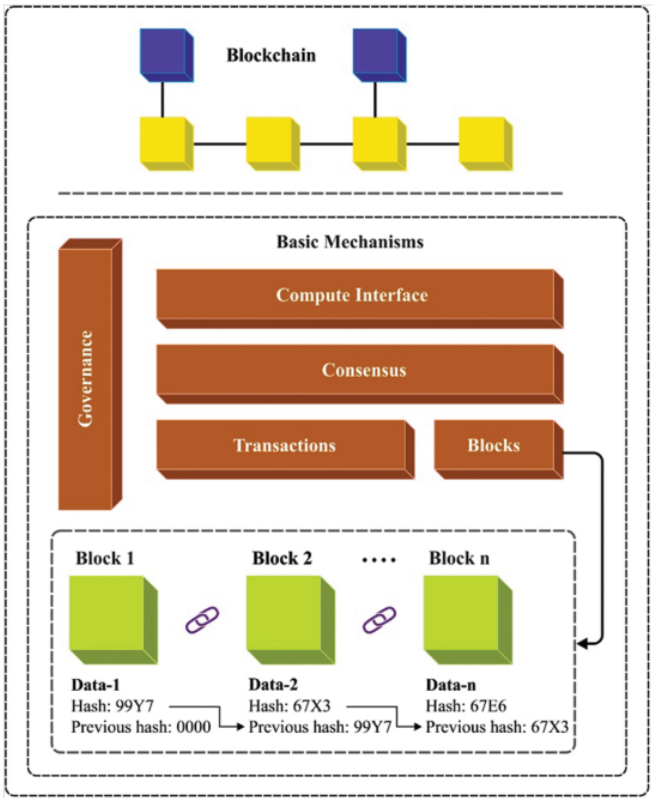

Fig. 2.2: Framework of Blockchain

2.3.1. Blockchain as a shared memory. The blockchain system relies on a ledger that records each transaction moving through a network. As a result, a specific method is needed to identify the nodes that are being moved and the path that they take. On this method, it is possible to save the routes of live, ongoing blockchain transactions. In order to carry out this, the network nodes are treated as coins. To be more precise, a message is transferred from a source to Base Station (BS) by particular nodes, and the originating node influences its proprietorship. Each node has a base Station at the beginning, and all the base station are considered to be inactive. In other words, none of the nodes have an active base station. Then it requests ownership's route node from the BS. The nodes are transferred via the chosen path once the transactions have been registered on the blockchain. The transferring nodes return possession of the route node to the BS, including themselves, once the data has been successfully transported to the BS. This is simply done to let the peer's network know that the communication was successful. Following this, these nodes are released. An origin node, in their opinion, has the capacity to be the owner of u nodes where $u \leq n$. Figure 2.2 illustrates the blockchain's structural components.

2.4. Detection of malicious node in VANET with enhanced security. A node serves as a source which is known to be information generator in VANET communication. Other intermediary nodes between the source and destination operate as relay nodes, while one more node serves as the message's destination. There are third parties in VANETs known as Trusted Authorities (TAs) who offer security. The administration of the network's vehicle identities and the verification of misbehaviour reports received by the verifier nodes fall within the purview of the TA. If the reports are determined to be true, the TAs will adjust the nodes' mistrust values appropriately. Every vehicle has a black list given by the TA that contains an inventory of dangerous nodes, as well as a white list provided by the cluster head for that particular vehicle. To detect the malicious node with enhanced security, following is a description of the Algorithm 1.

Algorithm 1 Algorithm for detection of malicious nodes

1: Initially, vehicle V_N enters the vehicular network.
2: Obtain the cluster keys
3: The parameters such as load, distrust value and distance of nodes in area V_n is to be computed for selecting the verifier.
4: For selecting the verifier, Compute the decision parameter D_p. $D_p = W_1 * L_D + W_2 * D_v + W_3 * D_s$
5: Where $W_1 + W_2 + W_3 = 1$
6: W_1, W_2, W_3 represents weight factors of parameters L_D, D_v, D_s which are Load, Distrust value and Distance accordingly.
7: The nodes are detected with the decision parameter value which is smaller than selection threshold i.e., $(D_p < T_{vs})$.
8: Distribute the nodes which is obtained as verifiers from step 5 to the newly entered vehicle V_N.
9: The vehicle's behaviour is monitored by verifiers
10: If (verifier notices vehicle V_N acting strangely)
11: Notify to the cluster head (CH)
12: jump to step 9;
13: else
14: jump to step 7;
15: Compute cluster head of a new distrust value of vehicle V_N.
16: If the distrust value falls below or equals to detection threshold i.e.,
17: If $(D_v \leq T_M D)$ then
18: the whitelist gets updated and jump to 7
19: else
20: jump to 11
21: alert message is transmitted to all other nodes
22: Perform updation in black list about the entry of vehicle V_N.
23: Remove the discovered malicious vehicle from the network

By this process, if any vehicle found to be acting strangely inside the network, a warning message is sent to all the nodes and update it in the black list about the vehicle's entry. So that the malicious vehicle gets detected and the other vehicle inside the network zone gets alerted.

2.5. Lightweight pseudonym management scheme. The network's vehicle V attaches its public key and uses pseudo id to denote the message's sender, digital signature of the message which was created using its private key and a local table is maintained along with it. This table comprises of valid (PID_v, PK_v)pairs and the termination time for each entry. We point out that performance is impacted by how long the data in a local table is valid for. If the period of time is very brief, the frequency at which the vehicles must check the RSU is increased, increasing the delay. if the time period is lengthy, the local table might have outdated or incorrect information. So, to get rid of this problem, at least once every five minutes, vehicles are required to change their pseudonyms. In order to ensure the freshness of data, a validity period in the LT is to be reasonable. We utilised a validity period of 5 s in our simulations. Every time a message is received, the authentication method is conducted, and the result is a binary value that indicates whether the message is legitimate or not. A message with a valid digital signature sent by an authorized sender is deemed "VALID". The message can be used. If not, the message is deemed false and is immediately deleted (Algorithm 2).

When the RSU receives a request for a (PID_v, PK_v) pair, it searches for the PIDv in the blockchain to confirm the validity of the current public key. The keys and associated pseudo-IDs for each vehicle may vary, and in order to maintain secrecy, these pseudonyms must be constantly altered. Because each item in the LTs has a limited validity period, it is important to make sure that the expired IDs are not being utilised. Additional details about a vehicle, such as misbehaviour complaints and reputation ratings, may also be seen on the blockchain. The proposed solution performs vehicle authentication as an immediate search in the blockchain for its PID. In order to reduce the computational effort significantly, we design an easy-to-use pseudonym

Algorithm 2 Algorithm for detection of malicious nodes

Input: Message retrieved from vehicle v, local table (LT) at receiving vehicle
Output: verification status of received message from v.
Verify the status of PID_v and PK_v in local table
if (PID_v, PK_v) ϵ LT and not terminated then
Sender v is authenticated
else
Fix random wait time t_w and wait
if status message is not retrieved for (PID_v, PK_v) during the time period t_w then
send request message to perform validation and wait for response.
end if
process RSU response
if response reveals 'the message is authentic' then
a. Add (PID_v, PK_v) to LT
b. displays the message 'sender v is authentic'
else
sender v is not authentic
displays received message is not VALID
end if
end if
if sender v is authenticated then
a. Validate digital signature using PK_v
if signature is valid then
received message is VALID
else
received message is not VALID
end if
end if

authentication method.

3. Results and Discussion. The effectiveness of the proposed approach is examined in this section under various circumstances. In the following section, it provides the detailed comparison of proposed system with existing approaches considering packet delivery ratio, throughput, routing overhead. In addition to this, computational cost, communication and storage cost analogization is made in the graph to determine the enhancement in the proposed system.

3.1. Packet delivery ratio (PDR). Table 3.1 and graph representation in figure 3.1 depicts the results attained by proposed routing technique assisted with blockchain on the basis of PDR with various node counts. The novel routing assisted with blockchain shows maximum PDR value whereas, the techniques such as PSO, GA and GWO shows minimum PDR values. As an illustration, during 500 nodes, a maximum PDR of 0.971 is achieved with assist of proposed protocol and other routing protocols shows a minimum PDR value compared to proposed approach.

3.2. Throughput. The suggested approach's throughput analysis under different node counts is shown in Figure 3.2. The findings reveal that the suggested paradigm produces successful results with high throughput.

3.3. Routing overhead. Figure 3.3 compares the routing overhead of different approaches such PSO, GA, GWO and HOA. The overhead incurred in the transmission and reception of packets for the packet transfer rates inside the network is considered in this approach. GWO shows high level of overhead compared to other techniques whereas, the routing protocol used in this proposed approach incur lesser routing overhead. As this approach achieves low overhead, it is efficient in attaining maximum effective throughput.

Table 3.1: Ratio of Packet delivery

Number of nodes	PSO	GA	GWO	HOA
100	0.949	0.961	0.989	0.995
200	0.938	0.956	0.980	0.989
300	0.929	0.949	0.974	0.982
400	0.921	0.938	0.963	0.976
500	0.916	0.925	0.956	0.971

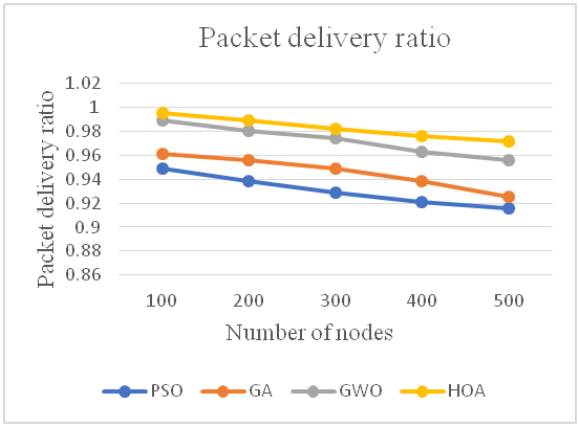

Fig. 3.1: Packet delivery ratio

Table 3.2: Throughput analysis

Number of nodes	PSO	GA	GWO	HOA
100	83.12	87.63	96.54	99.32
200	76.15	81.24	95.46	98.65
300	67.95	75.45	91.00	97.64
400	61.35	68.96	88.96	94.54
500	55.09	60.75	86.75	89.96

3.4. Computation cost. Figure 3.4 makes it clear that the proposed system requires less computational time for authentication than related schemes, as it only needs around 400 ms to authenticate 80 users compared to more than 450 ms for the other existing approaches to verify 80 vehicle users. Additionally, the computation time of the recommended method increases linearly as the number of vehicles increases.

3.5. Communication cost. Figure 3.5 represents the communication cost of proposed system. Comparison is made against existing approaches with varying number of users. The proposed system shows the minimum cost of communication compared to other existing approaches

The proposed system performs better than the conventional approaches with regard to PDR, throughput, routing overhead, communication and computational cost. In addition to this, it provides high level of security with efficient authentication scheme and routing protocol assisted with blockchain. In this study, the blockchain is used to store the nodes' credentials in order to protect network privacy and assure tamper resistance but the limitation of using blockchain is that it uses a lot of resources because there are more transactions happening simultaneously. With the assistance of blockchain based routing protocol, the optimal path is selected which enhances the efficiency of routing as well as the communication and computation cost gets reduced.

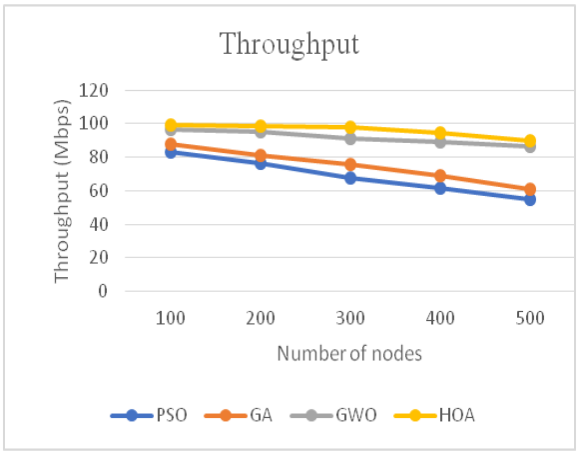

Fig. 3.2: Throughput

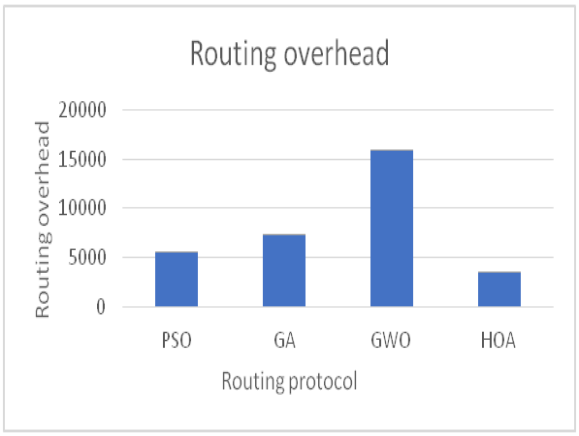

Fig. 3.3: Routing overhead

4. Conclusion. To achieve the best route selection and security in the vehicular ad-hoc network, a unique authenticated technique using block chain assisted routing protocol was developed in the current study. The proposed method involves two main phases, including the authentication and HOA-based routing processes. In order to share network information in real-time situations, the transactions are also kept in the blockchain. A thorough experimental investigation was performed, and the findings were evaluated using different metrics, in order to confirm the presented approach's superiority. The outcomes of the trial indicate that the proposed method outperformed other existing strategies significantly and offers high level security at a more affordable rate for computing and communication. As a part of future scope, we will simulate our proposed framework mechanism on real-time traffic data of vehicle information sharing scenarios.

REFERENCES

[1] Othman S. Al-Heety, Zahriladha Zakaria, Mahamod Ismail, Mohammed Mudhafar Shakir, Sameer Alani, Hussein Alsariera 2020, "A Comprehensive Survey: Benefits, Services, Recent Works, Challenges, Security, and Use Cases for SDN-VANET", IEEE Access, vol. 8, no. 5, pp. 91028-91047.

[2] Sagheer Ahmed Jan, Noor Ul Amin, Mohamed Othman, Mazhar Ali, Arif Iqbal Umar, Abdul Basir 2021, "A Survey on Privacy-Preserving Authentication Schemes in VANETs: Attacks, Challenges and Open Issues", IEEE Access, vol. 9, no.

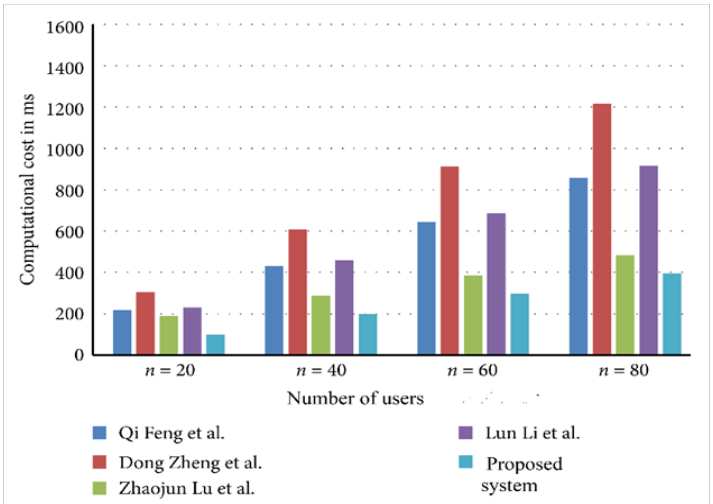

Fig. 3.4: Computational cost

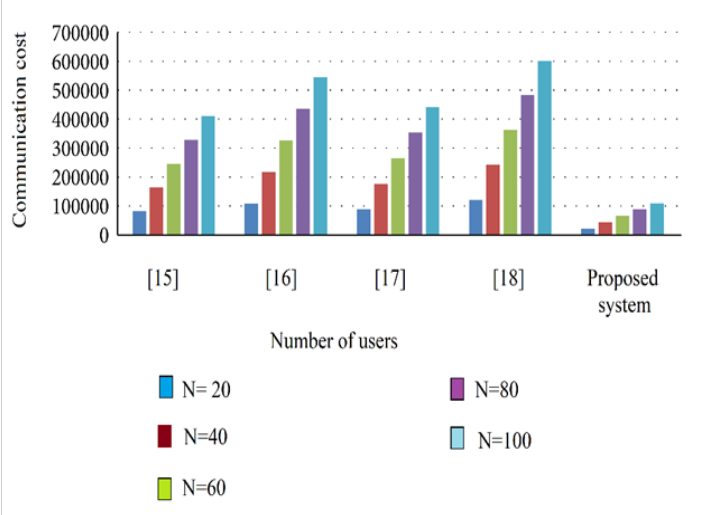

Fig. 3.5: Communication cost

11, pp. 153701-153726.
[3] Waqar Khalid, Naveed Ahmed, Suleman Khan, Zahid Ullah, Yasir Javed 2023, "Simulative Survey of Flooding Attacks in Intermittently Connected Vehicular Delay Tolerant Networks", IEEE Access, vol. 11, no. 7, pp. 75628-75656.
[4] Abdullahi Chowdhury, Gour Karmakar, Joarder Kamruzzaman, Alireza Jolfaei, Rajkumar Das 2020, "Attacks on Self-Driving Cars and Their Countermeasures: A Survey", IEEE Access, vol. 8, no. 11, pp. 207308-207342.
[5] Zhaojun Lu, Gang Qu, Zhenglin Liu 2019, "A Survey on Recent Advances in Vehicular Network Security, Trust, and Privacy", IEEE Transactions on Intelligent Transportation Systems, vol. 20, no.2, pp. 760-776.
[6] Fengzhong Qu, Zhihui Wu, Fei-Yue Wang, Woong Cho 2015, "A Security and Privacy Review of VANETs", IEEE Transactions on Intelligent Transportation Systems, vol. 16, no. 12, pp. 2985-2996.
[7] Carlos Pedroso, Thiago S. Gomides, Daniel L. Guidoni, Michele Nogueira, Aldri L. Santos 2022, "A Robust Traffic Information Management System Against Data Poisoning in Vehicular Networks", IEEE Latin America Transactions, vol. 10, no. 12, pp. 2421-2428.
[8] Peng Wang, Yining Liu 2021, "SEMA: Secure and Efficient Message Authentication Protocol for VANETs", IEEE Systems Journal, vol. 15, no. 1, pp. 846-855.

[9] Kyung-Ah Shim 2023, "Security Analysis of Conditional Privacy-Preserving Authentication Schemes for VANETs", IEEE Access, vol. 11, no. 4, pp. 33956-33963.
[10] Tao Zhang, Quanyan Zhu 2018, "Distributed Privacy-Preserving Collaborative Intrusion Detection Systems for VANETs", IEEE Transactions on Signal and Information Processing over Networks, vol. 4, no. 3, pp. 148-161.
[11] Yujue Wang, Yong Ding, Qianhong Wu, Yongzhuang Wei, Bo Qin, Huiyong Wang 2019, "Privacy-Preserving Cloud-Based Road Condition Monitoring With Source Authentication in VANETs", IEEE Transactions on Information Forensics and Security, vol. 14, no. 7, pp. 1779-1790.
[12] Muthukumaran, V., Kumar, V. V., Joseph, R. B., Munirathanam, M., & Jeyakumar, B. (2021). Improving network security based on trust-aware routing protocols using long short-term memory-queuing segment-routing algorithms. International Journal of Information Technology Project Management (IJITPM), 12(4), 47-60.
[13] Ruba Awadallah, Azman Samsudin 2021, "Using Blockchain in Cloud Computing to Enhance Relational Database Security", IEEE Access, vol.9, no. 10, pp. 137353-137366.
[14] Sultan Almakdi, Brajendra Panda, Mohammed S. Alshehri, Abdulwahab Alazeb 2021, "An Efficient Secure System for Fetching Data From the Outsourced Encrypted Databases", IEEE Access, vol. 9, no. 5, pp. 137353-137366.
[15] Edivaldo Pastori Valentini, Geraldo Pereira Rocha Filho, Robson Eduardo De Grande, Caetano Mazzoni Ranieri, Lourenço Alves Pereira Júnior, Rodolfo Ipolito Meneguette 2023, "A Novel Mechanism for Misbehavior Detection in Vehicular Networks", IEEE Access, vol.11, no. 7, pp. 68113-68126.
[16] Aekta Sharma, Arunita Jaekel 2022, "Machine Learning Based Misbehaviour Detection in VANET Using Consecutive BSM Approach", IEEE Open Journal of Vehicular Technology, vol. 3, no.12, pp. 1-4.
[17] Natarajan, Rajesh, Gururaj Harinahallo Lokesh, Francesco Flammini, Anitha Premkumar, Vinoth Kumar Venkatesan, and Shashi Kant Gupta. "A Novel Framework on Security and Energy Enhancement Based on Internet of Medical Things for Healthcare 5.0." Infrastructures 8, no. 2 (2023): 22..
[18] Zhaojun Lu, Qian Wang, Gang Qu, Haichun Zhang, Zhenglin Liu 2019, "A Blockchain-Based Privacy-Preserving Authentication Scheme for VANETs", IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 27, no. 12, pp. 2792-2801.
[19] Maithili, K., Vinothkumar, V., & Latha, P. (2018). Analyzing the security mechanisms to prevent unauthorized access in cloud and network security. Journal of Computational and Theoretical Nanoscience, 15(6-7), 2059-2063.
[20] Meie Shen, Zhi-Hui Zhan, Wei-Neng Chen, Yue-Jiao Gong, Jun Zhang, Yun Li 2014, "Bi-Velocity Discrete Particle Swarm Optimization and Its Application to Multicast Routing Problem in Communication Networks", IEEE Transactions on Industrial Electronics, vol. 61, no. 12, pp. 7141-7151.
[21] Shahid Abbas, Nadeem Javaid, Ahmad Almogren, Sardar Muhammad Gulfam, Abrar Ahmed, Ayman Radwan 2021, "Securing Genetic Algorithm Enabled SDN Routing for Blockchain Based Internet of Things", IEEE Access, vol. 9, pp. 139739-139754.
[22] Muthukumaran, V., Vinoth Kumar, V., Joseph, R. B., Munirathnam, M., Beschi, I. S., & Niveditha, V. R. (2022, November). Efficient Authenticated Key Agreement Protocol for Cloud-Based Internet of Things. In International Conference on Innovative Computing and Communications: Proceedings of ICICC 2022, Volume 3 (pp. 365-373). Singapore: Springer Nature Singapore..
[23] Q. Feng, D. He, S. Zeadally, and K. Liang 2020, "BPAS: blockchain-assisted privacy-preserving authentication system for vehicular ad hoc networks," IEEE Transactions on Industrial Informatics, vol. 16, no. 6, pp. 4146–4155.
[24] D. Zheng, C. Jing, R. Guo, S. Gao, and L. Wang 2019, "A traceable blockchain-based access authentication system with privacy preservation in VANETs," IEEE Access, vol. 7, pp. 117716–117726.
[25] L. Li, J. Liu, L. Cheng et al 2018, "a privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles," IEEE Transactions on Intelligent Transportation Systems, vol. 19, no. 7, pp. 2204–2220.
[26] Z. Lu, Q. Wang, G. Qu, H. Zhang, and Z. Liu, "A blockchain-based privacy-preserving authentication scheme for VANETs," IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 27, no. 12, pp. 2792–2801, 2019.

Edited by: Polinpapilinho Katina
Special issue on: Scalable Dew Computing for Future Generation IoT Systems
Received: Jul 7, 2023
Accepted: Oct 9, 2023