frontiers | Frontiers in Computer Science

TYPE Original Research
PUBLISHED 01 May 2024
DOI 10.3389/fcomp.2024.1384515

OPEN ACCESS

EDITED BY
Lexi Xu,
China United Network Communications Group, China

REVIEWED BY
Liang Zhao,
Shenyang Aerospace University, China
Yue Cao,
Wuhan University, China
Akshat Gaurav,
Ronin Institute, United States

*CORRESPONDENCE
M. Gayathri
✉ gm0717@srmist.edu.in

RECEIVED 09 February 2024
ACCEPTED 11 April 2024
PUBLISHED 01 May 2024

CITATION
Gayathri M and Gomathy C (2024) Design of CSKAS-VANET model for stable clustering and authentication scheme using RBMA and signcryption. *Front. Comput. Sci.* 6:1384515. doi: 10.3389/fcomp.2024.1384515

Design of CSKAS-VANET model for stable clustering and authentication scheme using RBMA and signcryption

M. Gayathri* and C. Gomathy

Department of Electronics and Communication Engineering, College of Engineering and Technology, SRM Institute of Science and Technology, Vadapalani Campus, Chennai, India

A public key infrastructure-enabled system authentication model is developed to provide essential security functions for Vehicular *ad hoc* networks (VANETs). An intelligent transportation system is provided by VANET, an emerging technology. Dedicated short-range communication is used to disseminate messages wirelessly. Communications may be hacked, and messages can be stolen or fabricated. Hence, authenticated communication is crucial in the VANET environment. Some parameters such as trust, authentication, privacy, and security are at high risk. This article suggests a VANET with secure authentication and trust-based clustering mechanisms to provide stable and secure communication. Initially, the Restricted Boltzmann Machine learning algorithm (RBMA) is used to select the cluster head, which depends upon trust, vehicle lifetime, and buffer level. Then, cluster members are formed, followed by grouping. Diffie–Hellman Hyperelliptic Curve Cryptography and cryptographic hash functions are used by signcryption for secure communication in VANET. Therefore, the essential component of the key agreement strategy that will give superior authentication is this signcryption mechanism. Over the medium access protocol layer, all of these security characteristics are updated. The proposed method of clustering signcryption key agreement scheme (CSKAS) approach reduces time complexity and increases packet delivery ratio which is vital in providing stable, secure communication.

KEYWORDS

hyper elliptic curve cryptography, encryption, vehicular *ad hoc* network, signcryption, public key

1 Introduction

Vehicular *Ad hoc* Network extensively uses vehicle nodes to ensure an intelligent transportation system (ITS). Most currently available suggestions only consider a single component, making the connection easy to break, even though VANETs are the subject of multiple excellent geographic routing protocols. This study focuses on an RMFD-based multi-featured routing algorithm (Mukhtaruzzaman and Atiquzzaman, 2020). Vehicles serve as the primary communication participants in VANETs, a subset of mobile *ad hoc* networks. Two ways interact the VANET system: vehicle-to-infrastructure (V2I) and vehicle-to-vehicle (V2V) communication; in contrast to MANETs, VANETs stand out for their remarkable adaptability (Kosuru et al., 2022).

Consequently, VANETs' network topology is constantly changing (Mirsadeghi et al., 2021). Connection link conditions between cars frequently shift due to vehicle movement, occasionally resulting in network disconnection. However, GPS data on the vehicle's location, speed, and the presence of obstacles on either side of the main road can be used to predict vehicle movement. Due to the requirements of a relatively high ratio to

the final destination in a relatively short time, designing an appropriate routing protocol for VANETs remains challenging. Data packets are transported along road segments in VANETs, and at junctions, decisions are made regarding where to transmit them (Tan and Chung, 2020). Consequently, in the event of a link failure, the payload will be transcoded to the final intersection node to choose a new path. Accordingly, Source nodes at intersections verify connectivity by examining the link of nearby nodes. As a result, cars choose areas of the road where data packets can be transferred. The decision of a vehicle among the potential vehicles to work as the next jump interfacing two nodes is a basic test that should be tended to.

The primary contribution of the study is as follows:

- Innovative clustering with RBM: implements clustering methods using the Restricted Boltzmann Machine algorithm to select cluster heads based on trust, lifetime, and buffer level, enhancing communication efficiency and reliability in VANETs.
- Trust-based security enhancement: incorporates a trust parameter in cluster management, significantly reducing security risks and ensuring stable communication links.
- HEC-based signcryption scheme: adopts a hyperelliptic curve-based signcryption key agreement scheme for robust, scalable, and resilient communication, protecting against a wide range of cryptographic attacks.
- Optimal security-stable performance: achieves stable communication through clustering of vehicles and secure mechanism eliminates the malicious node entering into communication link, which is essential for the high-speed environment of VANETs.

When choosing the cluster head and cluster members in a VANET, an AI-based model restricted Boltzmann machine algorithm can aid in effective communication, maximize packet delivery ratio, increase throughput, and boost overall network performance. The proposed RBMA with HECC method provides an effective framework for clustering and secure communication in VANET because it can provide dynamic selection, self-organization, real-time updates, and secure communication.

In Section 2 of the article, a thorough literature review is mentioned. Section 3 covers the technique for employing the constrained Boltzmann machine algorithm to choose the optimal cluster head in the proposed approach. Authentication methods and a discussion of secure routing are illustrated in Section 4. Section 5 discusses the security analysis of the proposed system, followed by results, discussion, and conclusion.

2 Related works

The dynamic environment of vehicles is a challenge to provide stable communication. To provide stable communication, clustering of vehicles is done based on their similar behavior of the vehicle. Clustering schemes can be divided into intelligent-based, mobility-based, and multihop-based. Apart from these clustering techniques, trust-based clustering should be done to provide a trusted and stable communication (Mukhtaruzzaman and Atiquzzaman, 2020). Energy efficient clustering techniques have been proposed by authors but in VANET since vehicles move around and their energy gets stored automatically in vehicles, since VANET communicates wirelessly, hackers may hack the communication hence trusted communication plays a significant role (Kosuru et al., 2022). Trusted cluster communication is proposed by the authors but strong encryption and decryption of the message will provide high end to end secure communication between vehicles (Mirsadeghi et al., 2021). The author created a novel VANET system model, which includes a safe key management and identification method. It provides the necessary storage and computing capacity and focuses on edge cloud computing (Tan and Chung, 2020).

The article discusses privacy and trust in the network that connects vehicles that presents a system with a mechanism in the blockchain-based anonymous authentication scheme (BARS) that safeguards the confidentiality of vehicle identification and prevents the transmission of fraudulent communications between automobiles, but system complexity could occur (Cheng et al., 2022). Using mobility prediction, the author created a centralized routing strategy for the connecting network of vehicles. Authors used machine learning techniques to predict the mobility of nodes; likewise, machine learning algorithms could be used to provide a trusted clustering in VANET (Tang et al., 2019). The article discussed various challenges in the dynamic resource allocation system in VANETs. The proposed framework is based on 5G network-based VANET models. The presented system formulates privacy-preserving VANET using the BAN model with the SUMO tool (Li et al., 2020). A privacy-preserving cloud-controlled vehicular *ad-hoc* network considers various roadside units. It frames the cloud-assisted feedback model for privacy-preserving VANETs. A strong authentication protocol could increase the efficiency of vehicle communication (Wei et al., 2019).

Trust aware clustering routing protocol was proposed by the author (Kadam et al., 2023). Ant Colony Optimization technique is used for the formation of the cluster, to avoid routing attacks; strong encryption algorithms are needed (Kadam et al., 2023). An improved RSU authentication was discussed by authors (Cheng and Liu, 2020), but if RSU gets compromised, there would be chaos in the whole system. A secure and privacy-preserving authentication technique was proposed by the authors (Alfadhli et al., 2020). This approach utilizes a blend of physically unclonable functions (PUF) and dynamically generated one-time pseudo-identities for authentication purposes. ECC-based novel authentication is been discussed by the authors to provide secure communication but the highly dynamic nature and stability of the vehicle have not been discussed (Godse and Mahalle, 2018). HPBS scheme was proposed to reduce malicious node communication, and public key infrastructure is used to authenticate vehicles, but a trust metric is not introduced to classify genuine and malicious nodes which would reduce the complexity of the system (Liu et al., 2020).

This study introduces a lightweight and efficient authentication technique named LESPP, which is designed to ensure good privacy preservation for secure VANET communication. The proposed scheme uses a self-generated pseudo-identity to ensure privacy and traceability, but the stability of vehicles is not concentrated

(Nandy et al., 2021). Using mobility prediction, the author might devise a centralized routing strategy for the vehicle-connecting network. Various understandings of VANET architecture in the existing articles are beneficial to derive a novel system for archiving better throughput and reduced data loss (Fonseca and Festag, 2006; Wang et al., 2006; Sun et al., 2010; Wasef et al., 2010; Mershad and Artail, 2013; Bhoi and Khilar, 2014; Chim et al., 2014; Dhurandher et al., 2014; Woo et al., 2014; Bitam et al., 2015; Janani and Manikandan, 2018). To provide a good authentication scheme, use of one-way hash functions and lightweight bitwise XOR operations in a two-tiered method that includes a trusted authority and vehicles for establishing authentication is established (Rawat et al., 2022). There are various methods discussed to provide trust-based authentication schemes in VANET. The proposed method deals with providing a stable and secure communication scheme.

A comprehensive review of the literature reveals that one of the primary challenges in vehicular networks is the dynamic mobility of vehicles. Given that messages are transmitted wirelessly, there is a risk of hackers intercepting and manipulating the communication, leading to potential diversions for users. Therefore, establishing a stable and secure communication system is crucial in vehicular *ad-hoc* networks, a key focus of the proposed solution in this article.

In the proposed approach, the combination of the Restricted Boltzmann Machine Algorithm (RBMA) and Hyper Elliptic Curve Cryptography (HECC) with signcryption in vehicular *ad-hoc* networks constitutes a noteworthy breakthrough, especially due to the collaborative impact of these technologies in improving security and operational efficiency. RBMA, renowned for its strength in unsupervised learning, is particularly skilled at detecting patterns and anomalies in node, facilitating superior and dynamic clustering. This is vital for the effective management of VANETs, enhancing the organization and processing of network data. In contrast, HECC offers a potent security solution with smaller key sizes than the traditional Elliptic Curve Cryptography, ensuring a balance between high security and efficiency in signcryption tasks. This synergy offers a dual benefit: RBMA's effective clustering significantly reduces network processing load and delays, while HECC brings forth a robust, yet compact cryptographic framework, augmenting the overall performance and security of the network. The combined effectiveness of RBMA and HECC signcryption aptly meets the unique demands of VANETs, such as constant high-speed movement, varying network densities, and rigorous security needs, thus outstripping prior solutions that might not effectively address both efficiency and security simultaneously.

The model presented sets itself apart from existing methods by incorporating a Hyper Elliptic Curve Cryptography (HECC)-based signcryption scheme and ensuring secure authentication and key management between Road-Side Units (RSUs) and vehicles. This approach introduces a groundbreaking signcryption system within the realm of certificate-based cryptography, aimed at improving security and privacy in VANET networks. Beyond just facilitating secure communication, the model also guarantees communication stability through the application of clustering technique. Focusing on both the stability and security of communication, this innovative method greatly enhances the effectiveness of VANET communication, forging a path toward an Intelligent Transportation System, an aspect not previously explored in existing research.

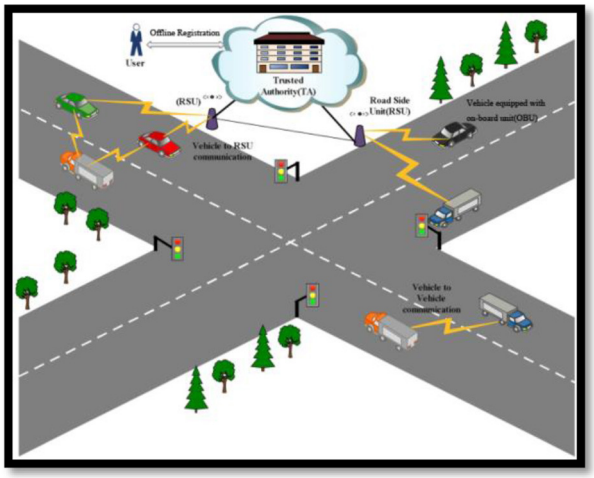

FIGURE 1
Proposed system—system architecture.

3 Proposed methodology

Three significant entities are present in our system model: certifying authority, vehicles, and roadside units. The novel architecture with hierarchical architecture is shown in Figure 1.

Certifying authority (CA): in vehicular networks, one crucial role is to trust. Centralized managing authority and power with adequate storage capability are considered CA. A certifying authority (CA) is used to register each RSU, followed by the attack of vehicular networks. It fails to negotiate by the attackers.

Roadside unit (RSU): CAs are connected wirelessly with the vehicles through this unit. It acts as a primary tool to build the VANET infrastructure. Its advantages include reliability, secured internal data storage, and easy installation. It is used on roads such as traffic signals, gas stations, and parking units. These units are directly interconnected with one another.

Vehicles: the three vehicle components are an onboard unit (OBU), sensors, and a global positioning system (GPS). Each node is triggered to communicate through the wireless medium by OBU. The vehicle communication range is 250 m.

3.1 Parameters required for cluster head selection based on restricted Boltzmann machine algorithm in proposed approach

Restricted Boltzmann Machines (RBMs) exhibit distinct characteristics and benefits when compared with other Artificial Neural Network (ANN) models. RBMs excel in efficiently managing the dynamic and frequently non-linear characteristics of VANET data, a task that is difficult for conventional ANNs. RBMs excel in feature identification and unsupervised learning, enabling them to effectively identify and react to the evolving patterns of vehicle movement and communication. Conversely, conventional artificial neural network models, which perform well

in supervised learning, may need a large amount of labeled data to produce comparable outcomes, a challenging requirement in the dynamic VANET setting. RBMs are well suited for VANETs due to their scalability and resistance to overfitting, which is important in handling the enormous and varied data volume in such networks. Certain artificial neural networks that may encounter challenges related to overfitting or scalability in similar situations. RBMs' generative nature offers a detailed insight into data distributions in VANETs, which is crucial for forming clusters effectively, as opposed to the discriminative approach of traditional ANNs. RBMs provide characteristics that make them a more versatile and effective option for cluster formation in the complicated and ever-changing environment of VANETs, hence restricted Boltzmann machine algorithm is used in the proposed approach for effectively grouping vehicles into clusters.

Initially, the Restricted Boltzmann machine learning algorithm (RBMA) is used to select cluster head which depends upon parameters such as trust, the lifetime of a vehicle, and buffer level. Secure authentication-based routing is processed, followed by choosing the best CH.

3.1.1 Buffer monitoring

Broadcast messages are those that are sent over the VANET. Basic safety messages, emergency communications, messages geared toward pleasure or entertainment, and messages encouraging information exchange are sent over the network. Since this communication scenario in VANET, there is a potential for congestion where messages must wait in line to be delivered, and packet overflows may also occur. Consequently, traffic load has to be observed. Let B be a neighboring node, let q_j be the jth sample value indicating the queue length at the current instant, and Q be the total number of samples collected throughout the interest. The average traffic load at node B can be formulated as shown in Equation (1).

$$LT\ (B) = \left(\frac{1}{Q}\right)^{*} \sum_{j=1}^{n} q_j \tag{1}$$

Traffic load intensity is expressed as mentioned in Equation (2).

$$LTI\ (B) = \left(LT\ (B)\ /qmax\right) \tag{2}$$

where, $qmax$ = maximum length, the traffic load intensity function at node B is followed by the interface queue of node B's maximum length, qmax, at the MAC layer.

Then, using the following Equation (3), the packet neighboring success probability concerning potential queue overflows denoted by PQ at node B can be modeled.

$$PQ\ =\ 1 -\ LTI\ (B)\,. \tag{3}$$

3.1.2 Lifetime of vehicle

Vehicles are highly dynamic since they move from one source to the other. The vehicle node's velocity determines the vehicle's lifetime. It is defined as the time it takes for a car to become available in that bandwidth as shown in Equation (4).

$$LT\ (i) = \frac{d_{ith}}{V\ (i)} \tag{4}$$

$LT\ (i)$–lifetime of vehicle i;
d_{ith}–distance from the sending/forwarding vehicle;
$V\ (i)$–velocity of vehicle i.

3.1.3 Node trustworthiness evolution

The local trust score is computed by analyzing vehicle behavior. A vehicle's proper behavior is shown when transmitting messages at consistent intervals, and vehicle trustworthiness is calculated by examining the control messages. Beacon messages transmitted during the transaction are saved and used for determining trust. The messages include information about the number of packets sent, delivered, and dropped. While exchanging messages, trusted nodes show an increased rate of effective message delivery compared with opponent nodes. On commencement of message exchange between node "i" and "j," acknowledgment is produced from them. From beacon messages, packet forwarding ratio (P_{Forw}) and delivery ratio (P_{Del}) are determined as shown in Equations (5, 6), respectively.

$$P_{Forw} = \frac{M_S^{Forw} - M_F^{Forw}}{M_S^{Forw} + M_F^{Forw}} \tag{5}$$

$$P_{Del} = \frac{M_S^{Del} - M_F^{Del}}{M_S^{Del} + M_F^{Del}} \tag{6}$$

M_S^{Forw}–effective forwarding rate; M_S^{Del}–effective delivery rate;
M_F^{Forw}–unsuccessful forwarding rate; M_F^{Del}–unsuccessful delivery rate.

From the ratio determined, node "i" finds the trust of "j" using the bayes theorem (Janani and Manikandan, 2018). A continuous random variable (φ) is computed at steady intervals in $0 \leq \varphi \leq 1$. The Probability Distribution Function (PDF) of "φ" at time "t" is given by Equation (7),

$$f_t\ (\varphi) = \frac{f_t\left(P_{Forw}^t \left|\varphi, P_{Del}^t\right.\right) f_{t-1}\ (\varphi)}{\int_0^1 f_t\left(P_{Forw}^t \left|\varphi, P_{Del}^t\right.\right) f_{t-1}\ (\varphi)\ .d\varphi} \tag{7}$$

where f_t current time and f_{t-1} previous time.

Equation (7) describes how the trustworthiness of node j can be calculated using the bayes theorem. The equation takes into account the probability distribution of φ at time t and the data from time $t-1$ $f_{t-1}\ (\varphi)$ to calculate the probability distribution of φ at time t ($f_t\ (\varphi)$). The equation is then integrated over φ to obtain the absolute trustworthiness of node j. As a result, it is determined using bayes theorem, and it may be a percentage where "φ" is distributed over a period [0, 1], and the best PDF to define this is beta distribution (BD). Binomial distribution at "t" is obtained from the likelihood function as shown below in Equation (8):

$$f_t\left(P_{Forw}^t \left|\varphi, P_{Del}^t\right.\right) = \begin{pmatrix} P_{Forw} \\ P_{Del} \end{pmatrix} \varphi^F\ (1-\varphi)^{F-\ D} \tag{8}$$

Equation (8) describes the probability of a forward progress (P^t_{Forw}) and a delivery (P^t_{Del}) occurring at time t, given a certain possibility ϕ. The equation is derived from the beta distribution and the binomial distribution. The beta distribution is used to describe the likelihood of ϕ being distributed over the period [0,1]. "φ" is found to be beta-distributed, "i" determines sequential random variable (φ_1, φ_2, ... φ_n) for "j" at fixed intervals. It is assumed that PDF "$f_t(\varphi)$" and "$f_{t-1}(\varphi)$" follow BD represented by "φ" in Equation (9):

$$Beta\ \varphi(\gamma,\delta) = \frac{\varphi^{\gamma-1}(1-\varphi)^{\delta-1}}{\int_0^1 \varphi^{\gamma-1}(1-\varphi)^{\delta-1}.d\varphi} \ where,\ \gamma,\delta - variables\ of\ BD,\ \gamma,\delta > 0 \quad (9)$$

At $t = 0$, nodes are not known to one another, and variables of BD should be neutral. It is assumed that $\gamma, \delta \in 1$. Furthermore, the node finds PDF iteratively, as shown below:

Finally, trust (T_i) for "i" is determined from BD mean as mentioned in Equation (10):

$$T_i = \omega(\gamma,\delta) = Beta\ \varphi(\gamma,\delta) = \frac{\gamma_{t-1} + P^t_{Forw}}{\gamma_{t-1} + P^t_{Forw} + \delta_{t-1} + P^t_{Del} - P^t_{Forw}} \quad (10)$$

where, $T_i \in [0,\ 1\ ]$.

If $T_i > 0.5$, node behavior can be trusted; when $T_i < 0.5$, The node is said to be malicious; when the network is initialized, initial trust will be substituted by the new trust over a period depending on the behavior of the conforming vehicle during message interchange. Trust is computed depending on direct experience providing consistent trust in the target node.

3.2 Restricted Boltzmann machine algorithm-based cluster head selection

The RBM neural network is a component of the energy-based model. This deep machine-learning technique is probabilistic, unsupervised, and generative. It is the goal of RBM to identify the joint probability distribution that maximizes the log-likelihood function. RBM contains two layers: the input layer, a visible layer, and the hidden layer, as shown in Figure 2. All nodes were connected in the original Boltzmann machine. The restricted Boltzmann machine is so named because it restricts intralayer connections. Since they are undirected, RBMs do not use gradient descent and backpropagation to modify their weights. Through a procedure known as contrastive divergence, they adjust their weights (MohanaPriya and Mercy Shalinie, 2017).

Equation (11) is a trust configuration of a restricted Boltzmann machine where $V = v1, \ldots, vn$ are visible nodes, while $h = h1, ..., h_n$ is "n" hidden units. The weight matrix (w_{nm}) and bias units a_{im} and b_{jn} of each node in the visible-hidden layer are connected to the edges of these layers. RBM's configuration may be represented by Equation (11).

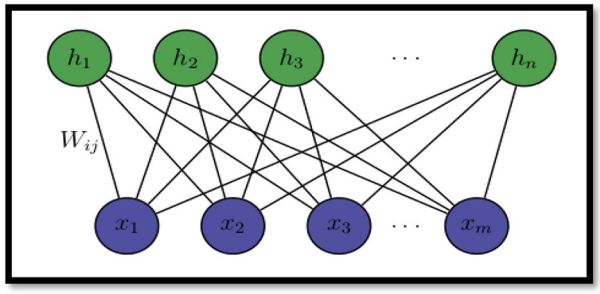

FIGURE 2
Structure of Restricted Boltzmann machine learning algorithm.

$$C(V,H) = \sum_{i=1}^{m}\sum_{j=1}^{n} S_{m,n}\, h_n\, v_m - \sum_{i=1}^{m} a_{im} v_m - \sum_{j=1}^{n} b_{jn}\, h_n \quad (11)$$

where $a\ C(V,H)$ = total weight of the RBM configuration;

$S_{m,n}$, strength of the connection between two nodes, m and n, in the network;

a_i, b_j bias units of visible and hidden layers;

v_m visible unit;

h_n hidden unit of the network.

The proposed protocol uses the RBM algorithm that self-learns the buffer, the lifetime of a vehicle, and trust metrics to provide an optimal cluster head (CH). The visible layer of RBM is trained with an input feature vector $(fv) = (senderip, destinationip, srcmac, destmac)$ and traffic parameter vector $(cv) = (Node_{buffer}, Node_{lifetime}, Node_{trust})$. The hidden layer learns and processes the feature and trust vectors to identify the malicious routes during the routing process in the RBM protocol. RBM's hidden layer is called a processing layer that maps the input with the incoming network traffic.

The joint probability distribution of visible and hidden layers at the training phase is represented as Equation (12).

$$J(V,H) = \left(\frac{1}{\phi}\right) * \exp\{-C(V,H)\} \quad (12)$$

where ϕ is the normalizing constant factor for visible and hidden layers, and it is given by Equation (13).

$$\phi = \sum_{v}\sum_{h} exp - C\left[fv, cv\right], H[fv, cv, NIT_{nt-tf}] \quad (13)$$

where NIT_{nt-tf} is the new incoming network traffic pattern.

At first, the model parameter fails at $\varphi = 0$. In that instance, iterative optimization based on an alternate iteration technique can be used to update the value of the model parameter. As a result, the value of φ_i may be estimated from sample Vi. It is possible to utilize the starting value of φ_{i+1}, which is produced from training the previous sample, as φ_i. The model parameter, φ_{i+1}, will be estimated using the following sample. The optimization procedures are carried out again until the

termination requirements are met. The hidden layer self-learns the input vectors to calculate the nearby success probability concerning potential queue overflows for all the participating nodes engaged in the RBM process. In contrast to previous unsupervised neural network learning techniques, the visible–visible and hidden–hidden layer constrained connections allow for a quick learning strategy. In any of the following two scenarios, the conditional probability distribution may be calculated using the joint probability distribution:

1. The hidden layer values are computed by feeding the input values to the visible layer as $P\left(h_{\mathrm{n}}/v_{\mathrm{m}}\right)$.
2. The values of the visible layer are computed by feeding the input values to the hidden layer as $P\left(v_{\mathrm{m}}/h_{\mathrm{n}}\right)$.

The same can be computed using the Gibbs sampling method, and the given input features in the visible layer are represented as Equation (14).

$$GS\left(\frac{h_n}{v_m}\right) = \sum_{v} sigmoid\left(b_{jn} + v^T w : j\right) \tag{14}$$

$PQ(i)$ *is the* packet neighboring success probability for possible queue overflows, $v\,(i)$ indicates vehicle's velocity, and T is the final trust factor. Here, the E_{VANET} efficient VANET node will be selected as the cluster head represented in Equation (15), and their range vehicles become cluster members by receiving CH messages.

$$E_{VANET} = -[w_1 .PQ\,(i) + w_2 .T\,(i) + w_3 \frac{d_{ith}}{V\,(i)}] \tag{15}$$

High mobility and rapid moving network topologies are characteristics of vehicular *ad hoc* networks. In VANETs, efficient clustering is crucial for improving overall network performance and communication. The aim is to integrate important parameters that represent the network's real-time state and use the Restricted Boltzmann Machine Algorithm (RBMA) for dynamic and effective cluster selection. The fitness function as in Equation (15) plays a pivotal role in determining the suitability of a node as cluster head and cluster member. The main components given as inputs are buffer monitoring that is used to analyze packet success probability rate (PQ) of node, indicating the efficiency of a node in handling network traffic, trust of a vehicle (T), assessing the reliability based on historical communication behavior of node, and velocity of the vehicle, relevant to the node's stability in the network due to mobility.

Input layer: PQ success probability rate mentioned in Equation (3), lifetime of a vehicle is calculated as in Equation (4), and trust as mentioned in Equations (5, 6). These characteristics are used to represent each VANET node.

Hidden layer: encodes complex interdependencies between these features.

Training process: RBMA is trained on historical data from the VANET, learning the probabilistic distribution of the node features as mentioned in Equation (12).

The training helps RBMA understand typical patterns and anomalies in node behavior.

Fitness evaluation: Nodes are evaluated based on the fitness function as in Equation (15).

Weights are optimized w_1 , w_2 , w_3 to reflect the significance of each feature in the VANET scenario.

Within VANETs, the Restricted Boltzmann Machine Algorithm (RBMA), real-time clustering mechanism is notable for its flexible and dynamic methodology. The RBMA rates each network node's fitness by continuously evaluating it in accordance with its updated Packet Success Probability Rate (PQ), Trustworthiness (T), and Life time (LT) of vehicle based on node's velocity range. These scores are then used to pick cluster head and members to reliably sustain communication and manage the network. The real strength of the system is its adaptability; the RBMA smoothly modifies its clustering decisions as VANET conditions change, whether because of differences in traffic load or changes in node mobility. This adaptability makes a more responsive and durable network architecture possible and is essential for maintaining network performance and efficiency in the constantly evolving VANET environment.

Figure 3 shows the flow diagram of the proposed approach. At the initial stage, nodes of VANET will be distributed. A cluster is formed to create stability. In the proposed approach, clusters are formed by a restricted Boltzmann machine algorithm using inputs such as buffer monitoring, lifetime of a vehicle, and trust metric. Buffer monitoring should be low, the success probability of the neighborhood for delivering packets should be high and trust factor should be high, and velocity of the vehicle should be low to maintain the lifetime of the vehicle. If all these conditions satisfy, grouping of vehicles is done, and then, secure communication is provided through hyperelliptic curve cryptography with signcryption. The packets are signcrypted at source and unsigncrypted at receiver side to provide stable and secure communication.

4 Secure routing and authentication scheme in proposed approach

Public-key cryptography, or hyperelliptic curve cryptography (HCC), is the Elliptic curve cryptography (ECC) successor. Every user has a set of private and public keys. While public keys are used for encryption and signature generation, private keys are utilized for decryption and unsigncryption. The main objective of the proposed approach is to bring an efficient key authentication scheme based on a signcryption system. It utilizes hyperelliptic curve cryptography and two one-way cryptographic hash functions. The significant advantage of using a hyperelliptic curve is its key size.

The proposed work procedure consists of six steps:

1. Setup phase.
2. RSU registration phase.
3. Registration phase of vehicles.
4. Key agreement phase between RSU, vehicles, and CA.
5. New Joining vehicles updating phase.
6. Cancellation of affected or failed vehicles.

During the setup phase, the certificate authority (CA) creates the essential infrastructure and protocols, such as security measures and the deployment of roadside units (RSUs). During the RSU registration phase, each RSU undergoes authentication and

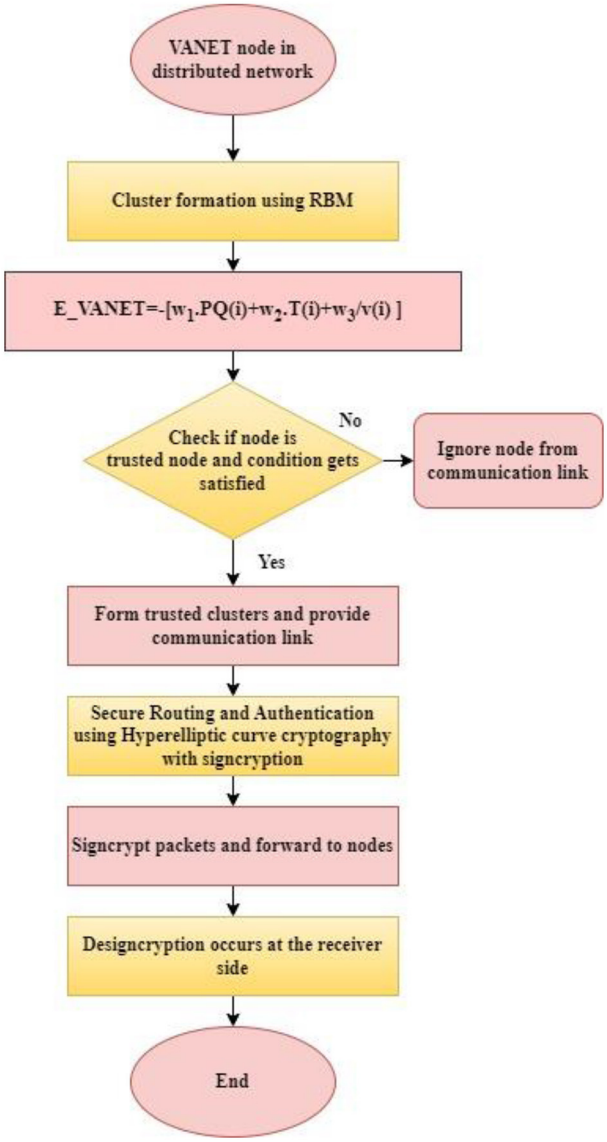

FIGURE 3
Flow diagram of the proposed approach.

registration with the CA to establish a secure network environment. During the registration phase for vehicles, vehicles undergo authentication and registration to enable secure and authorized network participation. The key agreement phase is essential for establishing safe communication protocols between roadside units, automobiles, and the certificate authority. It involves cryptographic key generation and exchange to ensure secure communication. The new joining vehicles updating phase ensures the expansion of the network and incorporation of new trusted vehicles seamlessly while maintaining a stable and trusted communication. Finally, the removal of affected or failed vehicles is crucial for network integrity. Non-operational or compromised vehicles are eliminated from the network to maintain security and efficiency. This thorough process guarantees a trusted, secure, and effective communication network in an intelligent transportation system.

TABLE 1 Notation used in the article.

Notation	Definition
CA_{st}	Certificate authority
D_{pk}	Private key
Υ_{st}	Public key
H_a and H_b.	Hash functions
RSU	Road side unit
E_i	RSU id
CH	Cluster head
Cluster head	CID_{new}
Member vehicles	MID_{New}
σ_i	Random number selected from $\sigma_i \in [1, 2, 3, \ldots (c-1)]$
ε_i	Secret key generation
α_i	To compute the private key with a public key
Nonce	Random or pseudo-random numbers

The subsection below will explain all the work phases in providing a secure routing and authentication scheme. Table 1 describes the notation used in this article.

4.1 Setup phase

Certificate authority CA_{st} will do this setup phase. This setup phase consists of creating public and private keys of node users, and the procedures are as follows.

a. To choose the private key D_{pk} . CA_{st} uses a hyperelliptic curve (HEC) in order of c with finite field F_c and selects the number from the set $\varphi_{st}, \varphi_{st} \in [1, 2, 3, \ldots (c-1)]$ uniformly.
b. CA_{st} generates the public key Υ_{st} as$\Upsilon_{st} = \varphi_{st}.J$. Here, J indicates the divisor of the hyperelliptic curve.
c. It chooses the two hash functions H_a andH_b.
d. Finally, it publishes the parameters.

$$K = \left[F_c, D_{pk}, HEC, J, \Upsilon_{st}, H_a, H_b\right]$$

4.2 Registration phase of RSU

CAst will handle this registration of RSU, and its process will be as follows:

a. CA_{st} will select the RSU id E_i;
b. Computes the private key for the RSU E_i as $X_i = \varphi.H_a(E_i) \; mod \; c$;
c. Computes the public key as $Y_i = X_i.J$;
d. Then, certificate for E_i is calculated as shown in Equation (16).

$$cert_i = \Upsilon_{st} + (X_i)\, H_a(E_i || Y_i) \tag{16}$$

e. *Finally*, CA_{st} *will update the memory of* E_i *as*

$$(E_i,\ cert_i, X_i, Y_i)$$

4.3 Registration phase of vehicles

Registering the vehicles is needed, which is deployed in that network. CAstand will handle this registration process. The process is as follows:

a. CA_{st} will select the vehicle id ID_i;
b. Computes the private key for the vehicle ID_i as $XV_i = \varphi.H_a\ (ID_i)\ mod\ c$;
c. Computes public key as $YV_i = XV_i.J$;
d. Then, certificate for ID_{ds} is calculated as in Equation (17).

$$certv_i = YV_i + (XV_i)\ H_a(ID_i||YV_i) \quad (17)$$

e. Finally, CA_{st} will update the memory of the vehicle node id ID_i as $(ID_i,\ certv_i,\ XV_i,\ YV_i\ )$.

4.4 Communication and key agreement phase between RSU, cluster head and member, and certificate authority

Let us consider cluster head CH vehicles CID_i and its member vehicles MID_i want to connect inside the network. It should have a key agreement and mutual authentication phase to be carried out.

4.4.1 Stage 1

If the RSU E_i is in the range of CH vehicle CID_i, the below process will be performed.

a. It selects $\sigma_i, \sigma_i \in [1, 2, 3, \ldots (c-1)\ ]$;
b. It computes $\varepsilon_i = \sigma_i.J$;
c. It computes $\alpha_i = \varepsilon_i.E_i.YV_i$;
d. Then, it encrypts $_i = E_{\alpha_i}(E_i||Nonce_i)$;
e. Then, it computes certificate as $\partial_i = certv_i + H_b\left(message\ ||E_i||\ Nonce_i\ \right)$;
f. The signature is computed as $\beta_i = \left(\frac{\sigma_i}{\partial_i + X_i} E_i\right)\ mod\ q$;
g. Finally, using the open network, it sends the key with necessary information as shown in Equation (18).

$$\Omega_1 = (\beta_i, \partial_{i,i}, \varepsilon_i, \alpha_i\ ) \quad (18)$$

to vehicle CID_i.

4.4.2 Stage 2

Suppose CH vehicle CID_i receives the key Ω_1 from the RSU E_i. In that case, it will check the validity of the key and add its cluster member information and sends it to the certificate authority via RSU to CA_{st}, and the following process will be performed:

a. It needs to decrypt $(E_i||Nonce_i = D_\alpha(_i)$ and verify the freshness of $Nonce_i$;
b. To check the certificate, E_i will check the condition as follows:

$$\Upsilon_{st} + Y_i.\ H_a(CID_i|\ |YV_i) = certv_i.J$$

c. Then, it checks the signature for validation as follows:

$$\beta_i\ (YV_i + \partial_i.J) = CID_i.\ \varepsilon_i.XV_i$$

d. If the signature is valid, it computes the $\varepsilon_i = \sigma_i.J$ Where $\sigma_i \in [1, 2, 3, \ldots (c-1)\ ]$
e. Then, it computes certificate ∂_i

$$\partial_i = certv_i + H_b(message_i||CID_i||MID_i||Nonce_i)(\sigma_i).$$

f. The following calculation will be performed for updating session key:

$$\vartheta_i = \sigma_i\varepsilon_i = \sigma_i.J$$

g. By using the above relation, it finds out the session key, and it needs to be shared with the cluster head and cluster member as follows:

$$v_i = H_b\left(message\ ||CID_i|\ |MID_i||Nonce_i||\ \vartheta_i\right)$$

h. The above session key can be verified as follows:

$$Hv_i = H_b(Nonce_i||v_i)$$

i Finally, using the open network, it sends the key of the cluster head and its members via RSU as mentioned in Equation (19).

$$\Omega_2 = (Hv_i, Nonce_i, \varepsilon_i, CID_i, MID_i\ X_i, \partial_i)\ \ to\ the\ CA_{st} \quad (19)$$

4.4.3 Stage 3

Once CA_{st} receives the key Ω_2, the keying procedure done in the cluster head and cluster member. For that, it will do the computations as follows:

a. It needs to decrypt $(message||\ MID_i||CID_i\ |\ |Nonce_i) = D_\alpha(_i)$ and verify the freshness of $Nonce_i$;
b. To check the certificate of the sender vehicle, it will check the condition as follows:

$$\Upsilon_{st} + Y_i.\ H_a(CID_i|\ \left|MID_i||YV_i\right) = certv_i.J$$

c. Then, it checks the signature for validation as follows:

$$\beta_i\ (Y_i + \partial_{is}.J) = CID_i.\ MID_i.\varepsilon_i.XV_i$$

d. If the signature is valid, it computes $\varepsilon_{CA_{st}} = \sigma_{CA_{st}}.J$ Where $\sigma_{CA_{st}} \in [1, 2, 3, \ldots (c-1)\ ]$

After verifying the cluster head and cluster member, certificate authority generates a certificate.

e. Then, it computes its certificate $\partial_{CA_{st}}$ as follows:

$$\partial_{CA_{st}} = cert_{CA_{st}} + H_b\left(message\,||CID_i||\,MID_i\,||CA_{st}||\,Nonce_{GC_{st}}\right)\left(\sigma_{CA_{st}}\right).$$

f. The following calculation will be performed to update the session key:

$$\vartheta_{iCA_{st}} = \sigma_i \varepsilon_{CA_{st}} = \sigma_i.\sigma_{CA_{st}}.J$$

g. To find out the relation of the nonce key, it computes as $_{iCA_{st}} = E_{\alpha_i}(Nonce_i||Nonce_{CA_{st}})$;

h. By using the above relation, it finds out the session key, and it needs to be shared with CID_{ds} as follows:

$$\nu_{drCA_{st}} = H_b\left(message\,||CID_i||\,MID_i\,||CA_{st}|\,|Nonce_{iCA_{st}}||\,\vartheta_{iCA_{st}}\right)$$

i The above session key can be verified as in Equation (20).

$$H\nu_{iCA_{st}} = H_b(Nonce_{iCA_{st}}||\nu_{iCA_{st}}). \quad (20)$$

j Finally, using the open network, it sends the key as follows:

$$\Omega_3 = \left(H\nu_{iCA_{st}}, Nonce_{iCA_{st}}, \varepsilon_i, CID_i, MID_i\ \varepsilon_i, X_i, \partial_{CA_{st}}\right)$$

to cluster head vehicle CID_i via RSU.

4.4.4 Stage 4

a. The cluster head vehicle receives the key Ω_3.
b. Messages are again decrypted, and then, the certificate and signature are verified.
c. After mutual authentication between the roadside unit, vehicles with cluster heads, cluster members, and certificate authority, communication starts with a vehicle-to-vehicle, vehicle-to-RSU, and vehicle-to-certificate authority via RSU. If the certificate and signature are invalid in these three stages, the communication between those nodes is blocked.

4.4.5 New joining vehicles updating phase

If any new cluster head CID_{new} or member vehicle MID_{New} wants to join inside the cluster or the network, CA_{st} will add the network as follows:

a. CA_{st} will select the new cluster head CID_{new} or member vehicles MID_{New};
b. Computes the private key for the vehicle CID_{new} or MID_{New} ;
c. $XCH_{new} = \varphi.H_a\,(CID_i)\ mod\ c$;
d. $XMCH_{new} = \varphi.H_a\,(MID_i)\ mod\ c$;
e. Compute public key as $YCH_{new} = XCH_{new}.J$ and $YCM_{new} = XCM_{new}.J$;
f. Then, the certificate for CID_{new} is generated as mentioned in Equation (21).

$$cert_{cid} = \Upsilon_{st} + (XCH_{new})\,H_a(CID_{new}||YCH_{new}) \quad (21)$$

Same way for cluster members certificate is generated as in Equation (22).

$$cert_{mid} = \Upsilon_{st} + (XMCH_{new})\,H_a(MID_{new}||YMCH_{new}) \quad (22)$$

Finally, CA_{st}will update the memory of the cluster vehicle node id CID_{new} as $\left(CID_{new},\ cert_{cid},\ XCH_{new},\ YCH_{new}\right)$ and

g. MID_{New} as $\left(MID_{new},\ cert_{mid}, XMCH_{new}, YMCH_{new}\right)$.

4.4.6 Vehicles leaving the clusters and joining the clusters

When a vehicle within a cluster decides to exit, it submits a departure request to the cluster's leading vehicle. This head vehicle responds by acknowledging the request and proceeds to exclude the departing vehicle from the cluster. In cases where the head vehicle itself plans to leave, the responsibility of cluster head is transferred to another vehicle in the cluster, specifically one with a high trust rating. For a vehicle aiming to join a different cluster, it must first send a request to join the head vehicle of that new cluster. The head vehicle then evaluates the trustworthiness of the requesting vehicle. If deemed reliable, the head vehicle will approve the request, thereby incorporating the vehicle as a new member of the cluster.

In vehicular networks, clusters are dynamically formed based on the vehicles' speed and expected duration within a cluster, which is often influenced by their velocity. Vehicles continuously monitor their speed through their On-Board Units (OBUs) and compare it with the average speed of their current cluster. When a significant speed discrepancy arises, a vehicle may send a "leaving request" to its current cluster head and subsequently join a new cluster that better matches its velocity. This process, known as a handoff, is crucial for maintaining efficient and relevant network clustering. It ensures seamless communication and network integrity by aligning vehicles with similar movement patterns in the same clusters. The cluster head plays a vital role in this dynamic process, managing the entry and exit of vehicles to maintain stability and efficient communication within the cluster. Stability of vehicle is essential in vehicular *ad-hoc* networks (VANETs), where the rapid movement and changing positions of vehicles necessitate flexible and responsive network structuring.

4.4.7 Cancellation of affected or failed vehicles

The vehicle poses a threat if it is affected by intruders or hackers, or is controlled by an undesired entity when its information is stored in the CA_{st}. The danger stems from its unscrupulous use. As a result, if the system's connection is lost, the data must be safeguarded by wiping it away to maintain the central system running smoothly. The suggestion is provided for the aim of adding a private key X_k to a list set aside for storing the one-of-a-kind identification of a vehicle that has been crashed or compromised, subsequently deleting it from memory as $ID_{delete} = H_a\,(ID_{delete}\,||Y_{delete}||\,GC_{st})$ and removing from the memory $D_{delete} = \{ID_{delete},\ Y_{delete}\}$. CA_{st} checks the deleted ID by matching with ID_N with ID_{delete}. If it is reached, deletion is not successful. If it does not fit, deletion of the process is successful.

5 Security analysis of the proposed approach

This section explores the different types of attacks encountered in VANETs and briefs how the proposed approach is used to mitigate these attacks.

Consider $V = \{V_1, V_2, V_3 \ldots . V_n\}$–set of nodes in the networks, M—set of all possible messages,V_m–malicious vehicle in network, M_{ij}–message sent from V_i *vehicle i* to V_j *vehicle j*, $SC\left(m, K_{pri_i}, K_{pub_j}\right)$–signcryption of message m using the private key of sender K_{pri_i} and the public key of receiver K_{pub_j}, $DSC\left(SC_m, K_{pri_j}, K_{pub_i}\right)$–decryption and verification of signcrypted message, SC_m, $T(m)$–timestamp or sequence number of message m, C—set of clusters in the network, each with its own cluster head CH.

5.1 Man-in-the-middle attack

A Man-in-the-Middle (MitM) attack poses a significant security risk when an unauthorized party secretly intercepts, modifies, or transmits communication vehicles and roadside equipment. Critical information exchanged within the network may be compromised in terms of integrity and confidentiality by this kind of assault. An attacker may intercept and alter messages pertaining to route information, traffic conditions, or safety alerts, creating potentially hazardous driving circumstances.

If an attacker node A intercepts the message M_{ij} transmitted between V_i to V_j. Man in the middle attacker will try to intercept the message as M'_{ij}- Intercept (M_{ij}, A). The proposed approach uses signcrypting M_{ij} using the sender's private key and receiver's public key as $SC\left(m, K_{pri_i}, K_{pub_j}\right)$. The decryption and authentication process $DSC\left(SC_m, K_{pri_j}, K_{pub_i}\right)$ ensures that any altered message M'_{ij} by attacker A is detectable as attacker lacks the necessary key of signcrypted message. The use of HECC signcryption in proposed approach significantly enhances security by relying on the complexity of the discrete logarithm problem on hyperelliptic curves, a problem which is widely recognized as hard to solve, thereby providing strong protection against unauthorized access and attacks.

5.2 Malicious deployment attack

To interfere with operations or compromise data, malicious deployment attacks include inserting malicious nodes or software in a network. These rogue elements pose serious security concerns since they seem legitimate yet carry out harmful operations such as disseminating false information or interfering with communications.

If an attacker A deploys the malicious node in the communication zone, the impact of malicious node V_m can be quantifies as (V_m, A). The cluster-based defense mechanism utilizes trust evaluation

$Trust(V)$ to select cluster heads CH, minimizing the influence of V_m in the network. Signcryption ensures message integrity and authenticity within clusters, reducing the effectiveness of malicious nodes.

5.3 Denial of service attack

A denial of service (DoS) attack is a malevolent endeavor aimed at obstructing a targeted server, service, or network's regular operation by flooding it with an excessive amount of Internet traffic. The attacker of this assault sources traffic from a number of hacked networks. When an overflow of incoming messages, connection requests, or corrupted packets occurs, the targeted resource becomes unavailable to authorized users.

A DoS attack by A floods vehicle node V_i with many requests, which are modeled as $R_A(V_i)$. To mitigate this, the clustering model monitors buffer or traffic rate $R(V_i)$ and implements mitigation strategies as mitigate DoS(V_i) when traffic filtering or buffer exceeds the minimum threshold $R_{threshold}$.

5.4 Sybil attack

In Sybil attacks, a malevolent node assumes several fake identities in order to obtain excessive influence within the network. This may result in serious disruptions such as the dissemination of misleading information or the influencing of network choices. These types of attacks seriously jeopardize the dependability and integrity of VANET connections, affecting everything from safety procedures to traffic flow.

In a Sybil attack, A creates multiple fake identities as $\{V_{s_1}, V_{s_2}, V_{s_3}, \ldots V_{s_m}, \}$. The model for this attack influences (V_{s_i}, A). The countermeasure involves identity verification for each node *Verify ID*$(V_{s_i},)$ before it is allowed to join a cluster. Trust score of all vehicle node is checked; if its trust score is low, it is not allowed to join in the cluster, effectively reducing sybil nodes.

5.5 GPS spoofing

GPS spoofing is a deception approach used in VANETs whereby fake GPS signals are transmitted to spoof the GPS receivers in vehicles. This may result in the reporting of inaccurate location data, which could confuse traffic management procedures and throw navigational systems into chaos. There may be serious repercussions, such as clogged roads and compromised driver and passenger safety. GPS spoofing poses a serious threat to VANETs, where vehicles rely heavily on precise location data for a variety of purposes such as routing, safety alerts, and traffic optimization.

GPS spoofing involves A to broadcast false GPS signals $S_{fake,}$ impacting the location data $L(V_i)$ of nodes. The model is Error $(L_{true}(V_i), L_{fake}(V_i))$. The location provided is true or false is noted. Cluster-based cross-verification of GPS data *Verify GPS*$(L(V_i), C_k)$ can identify discrepancies in location information, mitigating the impact of spoofed signals.

5.6 Replay attack

A replay attack in VANETs is the capture and retransmission of legitimate signals or messages. This could manipulate the network into thinking that recently performed or ancient commands are entirely fresh. By disseminating inaccurate or out-of-date information, these assaults have the potential to hinder road safety and interfere with traffic control. As decision-making in VANETs depends on timely and accurate communication, thwarting these attacks is essential and usually entails steps such as time-stamping messages to guarantee their legitimacy and freshness.

In a replay attack, A capture and retransmits a message M_{ij} with old timestamp T_{old}. The mathematical model representation for attack is given by $M'_{ij} - Replay(M_{ij}, T_{old})$. Signcryption used in the proposed approach includes a timestamp or sequence number $T(M_{ij})$, enabling the receiving node to detect and reject replayed messages.

5.7 Non-repudiation attack

A non-repudiation attack occurs when a sender in a VANET denies sending a message or carrying out an action that they have already carried out. In safety-critical situations, in particular, this challenge to communication authenticity may breed distrust and uncertainty within the network. In VANETs, maintaining non-repudiation is essential to preserving trustworthy and responsible communication channels. This is typically accomplished by cryptographic approaches such as digital signatures.

In a non-repudiation attack, a sender V_i denies sending a message M_{ij}. This is represented as non-repudiation denial (V_i, M_{ij}). The signcryption mechanism ensures non-repudiation as the signature embedded in $SC(M_{ij})$ can only be generated by V_i's private key, which is verifiable by verify signature $(SC(M_{ij}), K_{pub_i})$, thus avoiding non-repudiation attack.

6 Results of the simulation and discussion

The system model is implemented using network simulator NS 3.26, where the vehicular *ad hoc* network model is created. The Simulation of Urban Mobility (SUMO) tool is used to get real-time traffic mobility, an open-source simulation platform for the mobility-based traffic verification system. It handles the toolset of large scenarios and employs the transportation map showing various location data. The mobility data contain traffic lights, junctions, and connecting nodes and bridges. The SUMO road network model is organized to form the northern location and can align the direction corresponding to the connections. Using the SUMO tool, the proposed approach considers the traffic data of Kathipara junction in Chennai, Tamil Nadu.

Vehicular *ad hoc* network efficiency increases with a good packet delivery ratio, throughput, low end-to-end delay, packet loss ratio, and stable communication. Table 2 shows the simulation parameter used in the proposed in the proposed study and Table 3 shows computation and communication overhead of the proposed approach. Figure 4 shows the SUMO view of the Kathipara junction in Chennai, Tamil Nadu. The proposed approach is compared with the existing approach ASCII-ECC and ECC. Using the Median-centered K-Means (MKM) approach, clusters are formed and cluster leaders are chosen. The shortest path is determined using an updated version of the Cockroach Swarm Optimization (MCSO) method. Additionally, the use of ASCII-ECC facilitates secure data exchange (Marry Anita, 2023). ECC, RSA, and ASCII-ECC are compared with the existing approach CSKAS. The proposed approach provides high efficiency when compared with the existing approach (Gayathri and Gomathy, 2022; Tulib and Malhotra, 2022; Husnain et al., 2023; Marry Anita, 2023).

TABLE 2 Simulation parameter.

Simulation tool	NS3.26
Topology	Guindy Kathipara map osm
VANET topology generation tool	SUMO
Number of nodes	100
Packet size	512bytes
Vehicle direction	Two-way
MAC protocol	802.11p standard
Simulation time	200s

TABLE 3 Computation cost and communication overhead of proposed approach.

CSKAS (proposed approach)		
Node density	Computation cost (ms)	Communication overhead (ms)
20	1.21	1.21 + 42.3 = 43.51
40	1.41	1.41 + 44.6 = 46.01
60	1.47	1.47 + 46.5 = 47.97
80	1.52	1.52 + 48.2 = 49.72
100	1.58	1.58 + 50.1 = 51.68

Packet delivery ratio (%):

The packet delivery ratio is the total packets created at the source node to the total packets generated at the destination node as mentioned in the Equation (23). Figures 5, 6 depict the performance analysis of the packet delivery and loss ratio.

$$PDR\,(in\,\%) = \frac{Packet\ Received}{Packet\ generated} * 100 \tag{23}$$

Packet loss ratio (%):

The packet loss ratio is the ratio of lost packets to received packets as shown in the Equation (24).

$$PLR\,(in\,\%) = \frac{Number\ of\ lost\ Packet}{Number\ of\ received\ Packet} * 100 \tag{24}$$

End-to-End delay (ms):

End-to-End delay, the total of all delays in the connection caused by intermediary nodes, is the overall amount of time

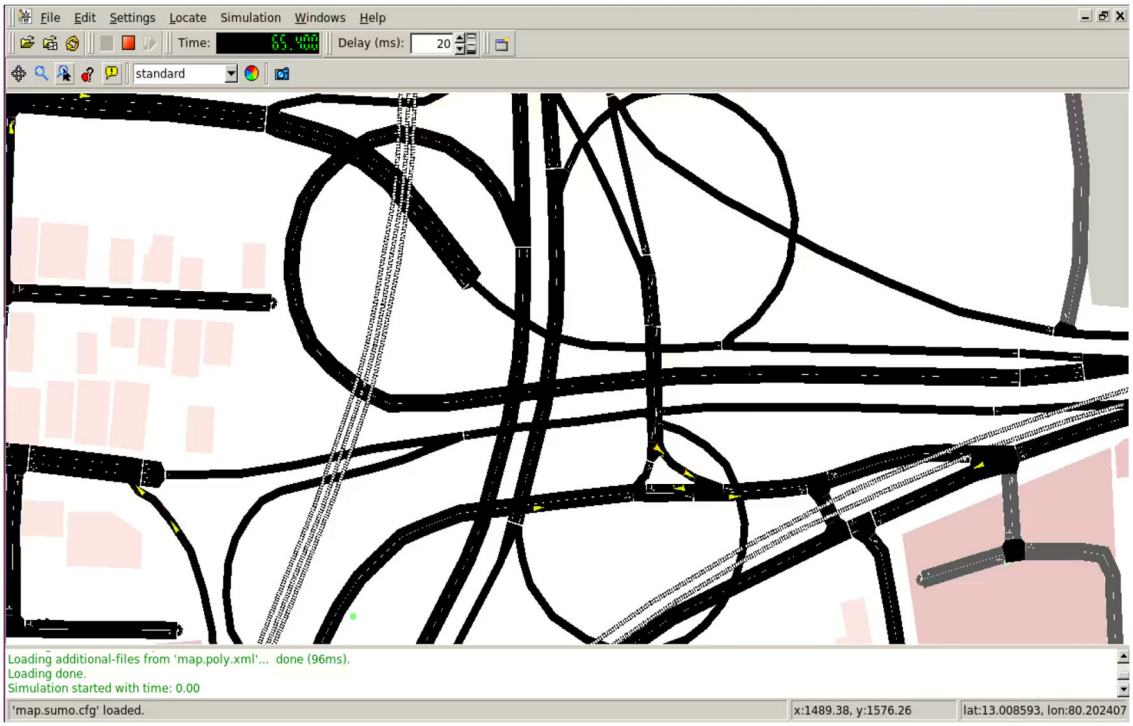

FIGURE 4
Sumo view of Guindy, Chennai.

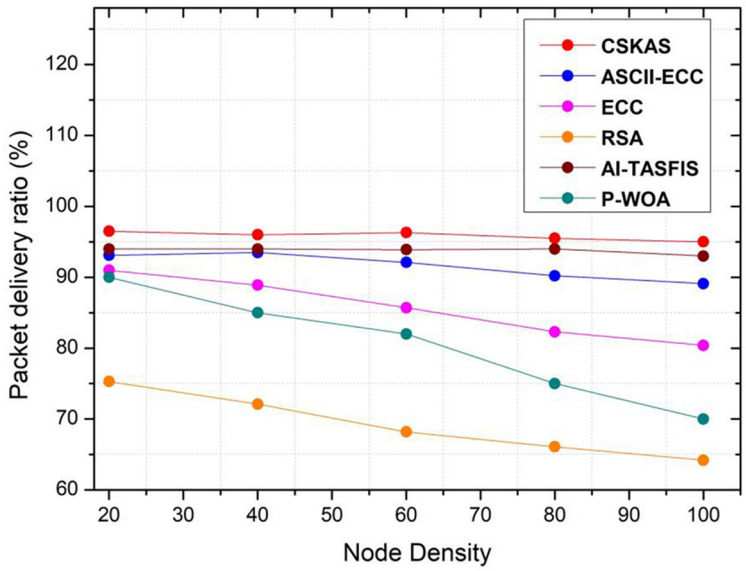

FIGURE 5
Performance analysis of packet delivery ratio.

required for a packet to go from its source to its destination. It is calculated by adding together all communication delays. Figure 7 displays the network's end-to-end delay performance analysis.

Computation cost (ms) (Tulib and Malhotra, 2022):

The proposed approach calculates the computation cost by calculating the total time required for signcryption and unsigncryption as shown in the Equation (25). Figure 8 shows the performance analysis of computation cost in milliseconds.

$$CC_{total} = t_{signcrypt} + t_{unsigncrypt} \quad (25)$$

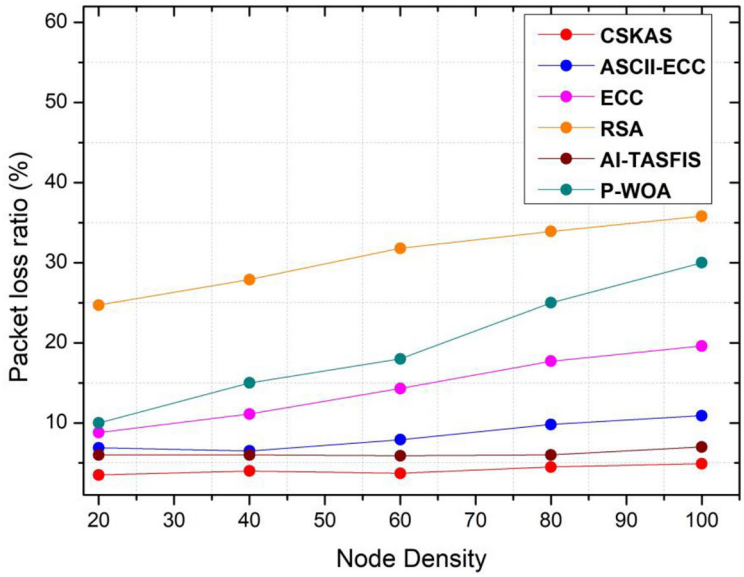

FIGURE 6
Performance analysis of packet loss ratio.

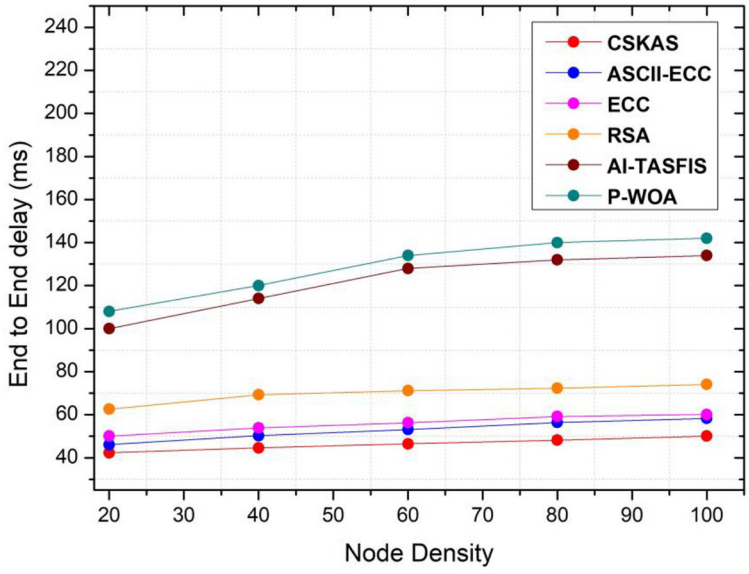

FIGURE 7
Performance analysis of end-to-end delay.

where CC_{total} is the total computation cost, $t_{signcrypt}$ and $t_{unsigncrypt}$ are the total time required to signcrypt and unsigncrypt a message in millisecond.

Average cluster lifetime (s):

The cluster lifetime specifies the length of time that a particular cluster is kept up and running. The sum of all cluster lifetimes is known as the average cluster lifespan.

Throughput (Mbps):

The total number of packets received at the destination divided by the processing time is known as throughput. Throughput is calculated by using the following Equation (26).

$$Throughput\ (Mbps) = \frac{Total\ number\ of\ packets\ received\ at\ the\ destination\ in\ bytes * 8}{End\ time - Start\ time} \quad (26)$$

Figures 9, 10 show the results obtained for average cluster lifetime and throughput for the proposed approach CSKAS by

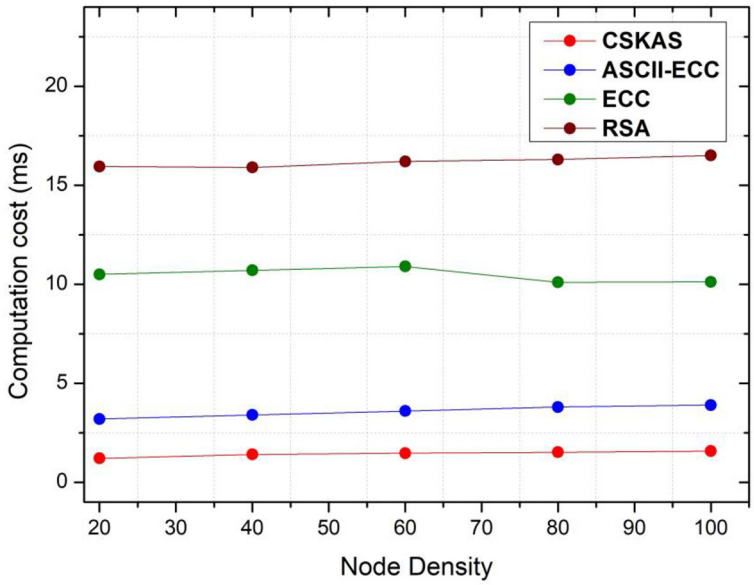

FIGURE 8
Performance analysis of computation cost.

varying the vehicle density. For 20 nodes, average cluster lifetime of a node is 102 s, and the throughput is 6.671 Mbps and is compared with the existing approaches. When the number of nodes increases, average cluster lifetime and throughput gradually decrease because of node density. For 100 nodes, the proposed approach still gives 75 s as the average cluster lifetime and a good throughput of 5.6 Mbps.

6.1 Communication overhead (ms)

The total of the computation cost and the additional factor delay is the communication overhead. The time needed for the signcryption and unsigncryption procedures is referred to as the computation cost. The extra time added by different network-related processes, such as data preparation, queuing, signal propagation, and processing at network nodes, is included in the additional factor delay or known as average end-to-end delay occurred for a packet to reach its destination. The total time used in computation cost and average end-to-end delay gives communication overhead. The proposed approach CSKAS achieves a low communication overhead across various node densities in the network. Specifically, for a network with 20 nodes, the overhead is just 0.04351 s. As the number of nodes increases, the overhead remains modest, with 0.04601 s for 40 nodes, 0.04797 s for 60 nodes, 0.04972 s for 80 nodes, and only 0.05168 s for a network comprising 100 nodes. This demonstrates the efficiency of the proposed method in maintaining minimal overhead even as the network scales.

The proposed approach provides high-end security performance by combining signcryption and Hyperelliptic Curve Cryptography (HECC) with a Restricted Boltzmann Machine (RBM) algorithm for clustering . This effectively balances computation cost and communication overhead. Strong security and reduced key lengths are two well-known advantages of HECC. Efficiency is especially important in high-speed vehicle networks. HECC's signcryption feature reduces computational complexity and overhead by combining encryption and signing in a single procedure. This integration reduces communication cost by reducing the size of cryptographic messages and cutting down on computation time. Concurrently, network organization is optimized by the RBM algorithm's skill at clustering. This improves data handling and routing effectiveness, which is vital in VANETs' dynamic environment.

A VANET system can analyze the correlation (Hanis and Amutha, 2019) between the data packet delivery rate (X) and packet loss rate (Y) for different network scenarios since the proposed study depends on packet-based clustering signcryption key agreement scheme, simulated PDR and PLR ratio are analyzed, and then, the correlation coefficient using a statistical method Pearson's correlation coefficient is calculated using Equation (27).

$$r = \frac{N\sum XY - (\sum X \sum Y)}{\sqrt{[N\sum x^2 - (\sum x)^2][N\sum y^2 - (\sum y)^2]}} \tag{27}$$

where N is the number of data points; X and Y are the two variables.

The Pearson correlation coefficient between PDR and PLR is ∼-0.964, indicating a strong negative correlation between the two variables. In the proposed approach increase in PDR results in a decrease in PLR; there is a strong negative correlation hence resistance to correlation attacks. This proves that encrypted packets are sent to the destination in a secure way.

The proposed approach uses key length of 128 bit. The Entropy E can be calculated as as shown in the Equation (28).

$$E = \log 2(2^{128}) \tag{28}$$

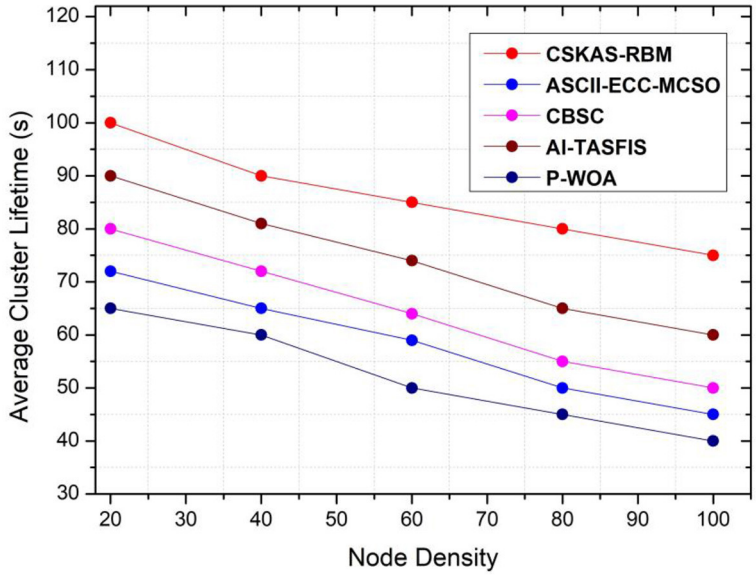

FIGURE 9
Performance analysis of average cluster lifetime.

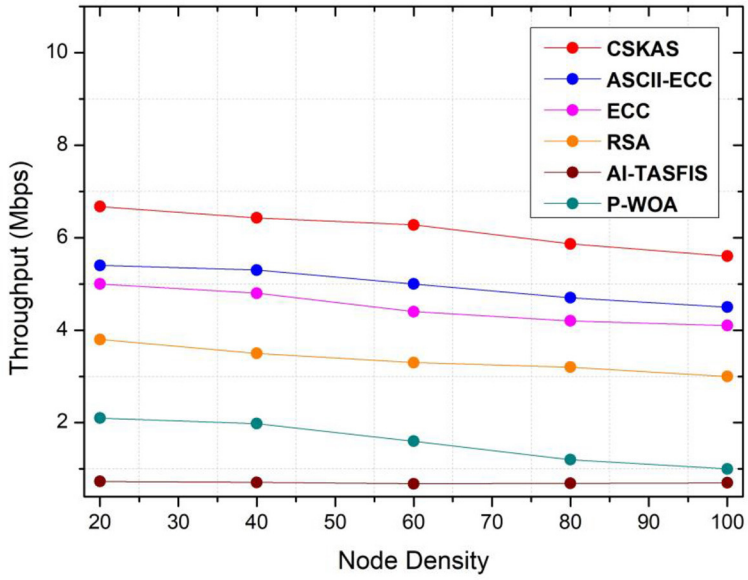

FIGURE 10
Performance analysis of throughput.

A 128-bit key offers incredibly high security and is challenging to crack with current technology. A 128-bit key has an entropy of 128 bits, meaning there are 2,128 potential keys, an astronomically enormous number that is challenging for an attacker to guess or brute-force.

The main limitation of signcryption system-based hyperelliptic curve cryptography in VANET is the increase in complexity of the system, which may increase latency. In the nb future, research will be carried out to reduce the complexity of the system.

7 Conclusion

Developing a system authentication model for critical public infrastructure is becoming increasingly crucial with the framework for providing vehicle *ad hoc* networks (VANETs) with essential security components. Trust, authentication, privacy, and security are among the high-risk factors. Safe authentication method and trust-based clustering are described in this article for VANET. At first, the confined Boltzmann AI approach is utilized to pick the trusted cluster head determination because of trust, the

lifetime of the vehicle, and buffer monitoring level using RBMA. After that, CH is made and clumping happens. Signcryption employs Diffie–Hellman hyperelliptic curve cryptography and cryptographic hash algorithms for secure VANET routing. The primary factor that contributes to the improved authenticity of the key establishment method is the system's signcryption. The medium access protocol layer has been updated to enhance these security measures. In addition, the CSKAS-clustering signcryption key agreement scheme, a signcryption-based approach to key establishment, reduces time and complexity that provides secure and trusted communication and secure routing protocol, which gives the solutions to issues with the secure routing.

Data availability statement

The original contributions presented in the study are included in the article/supplementary material, further inquiries can be directed to the corresponding author.

Author contributions

MG: Writing – original draft, Conceptualization, Methodology, Software. CG: Supervision, Methodology, Formal analysis, Writing – review & editing.

Funding

The author(s) declare that no financial support was received for the research, authorship, and/or publication of this article.

Acknowledgments

The authors would also like to thank the SRM Institute of science and Technology, Vadapalani to support them in providing good laboratory infrastructure to carry out the research.

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References

Alfadhli, S. A., Lu, S., Chen, K., and Sebai, M. (2020). MFSPV: a multi-factor secured and lightweight privacy-preserving authentication scheme for VANETs. *IEEE Access* 8, 142858–142874. doi: 10.1109/ACCESS.2020.3014038

Bhoi, S. K., and Khilar, P. M. (2014). Vehicular communication - a survey. *IET Netw.* 3, 204–217. doi: 10.1049/iet-net.2013.0065

Bitam, S., Mellouk, A., and Zeadally, S. (2015). VANET-cloud: a generic cloud computing model for vehicular *ad hoc* networks. *IEEE Wirel. Commun.* 22, 96–102. doi: 10.1109/MWC.2015.7054724

Cheng, H., and Liu, Y. (2020). An improved RSU-based authentication scheme for VANET. *J. Internet Technol.* 21, 1137–1150. doi: 10.3966/160792642020072104022

Cheng, H., Shojafar, M., Alazab, M., Tafazolli, R., and Liu, Y. (2022). PPVF: privacy-preserving protocol for vehicle feedback in cloud-assisted VANET. *IEEE Trans. Intell. Transp. Syst.* 23, 9391–9403. doi: 10.1109/TITS.2021.3117950

Chim, T. W., Yiu, S. M., Hui, L. C. K., and Li, V. O. K. (2014). VSPN VANET based secure and privacy-preserving navigation. *IEEE Trans. Comput.* 63, 510–524. doi: 10.1109/TC.2012.188

Dhurandher, S. K., Obaidat, M. S., Jaiswal, A., Tiwari, A., and Tyagi, A. (2014). Vehicular security through reputation and plausibility checks. *IEEE Syst. J.* 8, 384–394. doi: 10.1109/JSYST.2013.2245971

Fonseca, E., and Festag, A. (2006). *A survey of existing approaches for secure ad hoc routing and their applicability to VANETs, Vol. 1*. Heidelberg: NEC Network Laboratories, 1–28.

Gayathri, M., and Gomathy, C. (2022). AI-TASFIS: an approach to secure vehicle-to-vehicle communication. *Appl. Artif. Intell.* 36:2145636. doi: 10.1080/08839514.2022.2145636

Godse, S. P., and Mahalle, P. N. (2018). A computational analysis of ECC based novel authentication scheme in VANET. *Int. J. Electr. Comput. Eng.* 8:5268. doi: 10.11591/ijece.v8i6.pp5268-5277

Hanis, S., and Amutha, R. (2019). A fast double-keyed authenticated image encryption scheme using an improved chaotic map and a butterfly-like structure. *Nonlinear Dyn.* 95, 421–432. doi: 10.1007/s11071-018-4573-7

Husnain, G., Anwar, S., Sikander, C., Ali, A., and Lim, S. (2023). A bio-inspired cluster optimization schema for efficient routing in vehicular *Ad hoc* networks (VANETs). *Energies* 16:1456. doi: 10.3390/en16031456

Janani, V. S., and Manikandan, M. S. K. (2018). Efficient trust management with bayesian-evidence theorem to secure public key infrastructure-based mobile *ad hoc* networks. *EURASIP J Wireless Commun. Netw.* 25, 1–27. doi: 10.1186/s13638-017-1001-5

Kadam, M. V., Vaze, V. M., and Todmal, S. R. (2023). TACR: trust aware clustering-based routing for secure and reliable VANET communications. *Wireless Pers. Commun.* 132, 305–328. doi: 10.1007/s11277-023-10612-z

Kosuru, S., Suma, P., Alam, M. A., and Hussain, M. A. (2022). An intelligent cluster-based energy efficient optimization algorithm to improve the network performance in VANET. *Math Stat. Eng. Appl.* 71, 201–208.

Li, X., Liu, T., Obaidat, M. S., Wu, F., Vijayakumar, P., Kumar, N., et al. (2020). A lightweight privacy-preserving authentication protocol for VANETs. *IEEE Syst. J.* 14, 3547–3557. doi: 10.1109/JSYST.2020.2991168

Liu, H., Wang, H., and Gu, H. (2020). HPBS: a hybrid proxy based authentication scheme in VANETs. *IEEE Access* 8, 161655–161667. doi: 10.1109/ACCESS.2020.3021408

Marry Anita, S. E. A. J. (2023). Improved security of the data communication in VANET environment using ASCII-ECC algorithm. *Wireless Pers. Commun.* 128, 759–776. doi: 10.1007/s11277-022-09974-7

Mershad, K., and Artail, H. (2013). A framework for secure and efficient data acquisition in vehicular *ad hoc* networks. *IEEE Trans. Veh. Technol.* 62, 536–551. doi: 10.1109/TVT.2012.2226613

Mirsadeghi, F., Rafsanjani, M. K., and Gupta, B. (2021). A trust infrastructure-based authentication method for clustered vehicular *ad hoc* networks. *Peer-to-Peer Netw. Appl.* 14, 2537–2553. doi: 10.1007/s12083-020-01010-4

MohanaPriya, P., and Mercy Shalinie, S. (2017). Restricted Boltzmann machine-based cognitive protocol for secure routing in software defined wireless networks. *IET Netw.* 6, 162–168. doi: 10.1049/iet-net.2017.0054

Mukhtaruzzaman, M., and Atiquzzaman, M. (2020). Clustering in vehicular *ad hoc* network: algorithms and challenges. *Comput. Electr. Eng.* 88:106851. doi: 10.1016/j.compeleceng.2020.106851

Nandy, T., Idris, M. Y. I., Noor, R. M., Wahab, A. W. A., Bhattacharyya, S., Kolandaisamy, R., et al. (2021). A secure, privacy-preserving, and lightweight authentication scheme for VANETs. *IEEE Sens. J.* 21, 20998–21011. doi: 10.1109/JSEN.2021.3097172

Rawat, G. S., Singh, K., Arshad, N. I., Hadidi, K., and Ahmadian, A. (2022). A lightweight authentication scheme with privacy preservation for vehicular networks. *Comput. Electr. Eng.* 100, 1–10. doi: 10.1016/j.compeleceng.2022.108016

Sun, J., Zhang, C., Zhang, Y., and Fang, Y. (2010). An identity-based security system for user privacy in vehicular *ad hoc* networks. *IEEE Trans. Parallel Distrib. Syst.* 21, 1227–1239. doi: 10.1109/TPDS.2010.14

Tan, H., and Chung, I. (2020). Secure authentication and key management with blockchain in VANETs. *IEEE Access* 8, 2482–2498. doi: 10.1109/ACCESS.2019.2962387

Tang, Y., Cheng, N., Wu, W., Wang, M., Dai, Y., Shen, X., et al. (2019). Delay-minimization routing for heterogeneous VANETs with machine learning based mobility prediction. *IEEE Trans. Veh. Technol.* 68, 3967–3979. doi: 10.1109/TVT.2019.2899627

Tulib, K., and Malhotra, M. (2022). A hybrid approach for task scheduling in the cloud environment. *Int. J. Cloud Appl. Comput.* 12, 1–14. doi: 10.4018/IJCAC.305215

Wang, F., Zeng, D., and Yang, L. (2006). Smart cars on smart roads: an IEEE intelligent transportation systems society update. *IEEE Pervasive Comput.* 5, 68–69. doi: 10.1109/MPRV.2006.84

Wasef, A., Lu, R., Lin, X., and Shen, X. (2010). Complementing public key infrastructure to secure vehicular *ad hoc* networks. *IEEE Wireless Commun.* 17, 22–28. doi: 10.1109/MWC.2010.5601954

Wei, Z., Li, J., Wang, X., and Gao, C. Z. (2019). A lightweight privacy-preserving protocol for VANETs based on secure outsourcing computing. *IEEE Access* 7, 62785–62793. doi: 10.1109/ACCESS.2019.2915794

Woo, S., Jo, H. J., and Lee, D. H. (2014). A practical wireless attack on the connected car and security protocol for in-vehicle CAN. *IEEE Trans. Intell. Transp. Syst.* 16, 993–1006. doi: 10.1109/TITS.2014.2351612