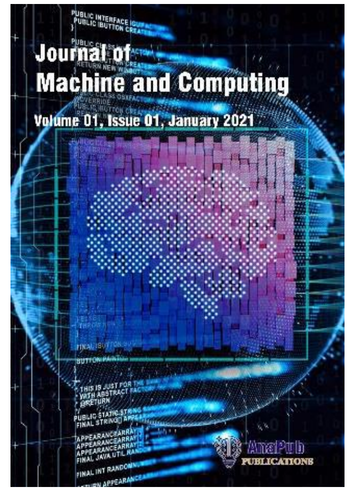
Journal Pre-proof



Blockchain-Based Machine Learning Model for Secure Data Transfer and Route Preservation in UAV Integrated VANET Systems

Divya Sree A and Kapil Sharma

DOI: 10.53759/7669/jmc202505182
Reference: JMC202505182
Journal: Journal of Machine and Computing.

Received 17 June 2025
Revised from 28 July 2025
Accepted 03 August 2025

Please cite this article as: Divya Sree A and Kapil Sharma, "Blockchain-Based Machine Learning Model for Secure Data Transfer and Route Preservation in UAV Integrated VANET Systems", Journal of Machine and Computing. (2025). Doi: https:// doi.org/10.53759/7669/jmc202505182.

AnaPub
PUBLICATIONS

Blockchain-Based Machine Learning Model for Secure Data Transfer and Route Preservation in UAV integrated VANET Systems

A.Divya Sree[1], Kapil Sharma[2]

Research Scholar[1], Department of Computer Science and Engineering[1,2]

Amity University[1,2],Madhya Pradesh, Gwalior, India.

a.sree@s.amity.edu[1*],ksharma@gwa.amity.edu[2]

Corresponding Author: a.sree@s.amity.edu

Abstract

The rise of driver assistance and automotive telecommunication systems shows great potential for adaptive transport solutions using vehicular ad hoc networks (VANET). Generally, the two main issues in vehicle ad hoc networks that malicious attackers can greatly affect are privacy and safety. Preventing the spread of harmful messages among vehicles is crucial to protecting the private properties of automobiles from potential threats. This research tackles these issues and proposes a new machine-learning-based message authentication method. This method can be integrated with interplanetary file systems and blockchain to ensure secure message distribution. The Inter Planetary File System (IPFS) is utilized by blockchain technology to create tamper-proof records in a distributed environment. This protocol stores events using content addressing. The source metadata from the IPFS is first stored in a smart contract and then in the distributed ledger technology. This framework makes use of the Iterative Import Vector Machine (IIVM) classifier and Non-overlapping K-means clustering in the event authentication process. It will be classified as malicious or not malicious in order to carry out the vehicle clustering. After clustering, the IIVM classifier works to identify harmful event messages. As a result, dropped messages are recognized as such and the secure messages are sent into the network. According to simulation results, the suggested approach increases event spoofing identification precision by 96.21%. This system's trust model of the occurrence does an excellent task of separating genuine instances from fake ones.

Keywords: Blockchain, Over-lapping, IIVM, Spoofing, Machine Learning and VANETs.

I.INTRODUCTION

India's transportation system is undergoing a significant transformation due to the country's fast-growing economy, increasing car ownership, and a poor and inefficient public transit infrastructure. The intelligent transportation system (ITS) addresses all these issues [1]. It has a significant impact and provides direction as well as management to reduce traffic congestion. Due to their self-organizing character and ad hoc nature, automobile ad hoc networks are receiving a lot of interest these days. Multi-hop routing is possible for cars that are outside of the scope. An internal vehicle component that analyzes data from multiple sensors is called an onboard unit. The sensor installed with the vehicle's circumstances performs the interface with the external networks. The Vehicle to Infrastructure Network (VANET) facilitates data transmission between vehicles and between vehicles with ease. It isconsidered a potent tool for improving traffic efficiency. Figure 1 illustrates the VANET communication model.

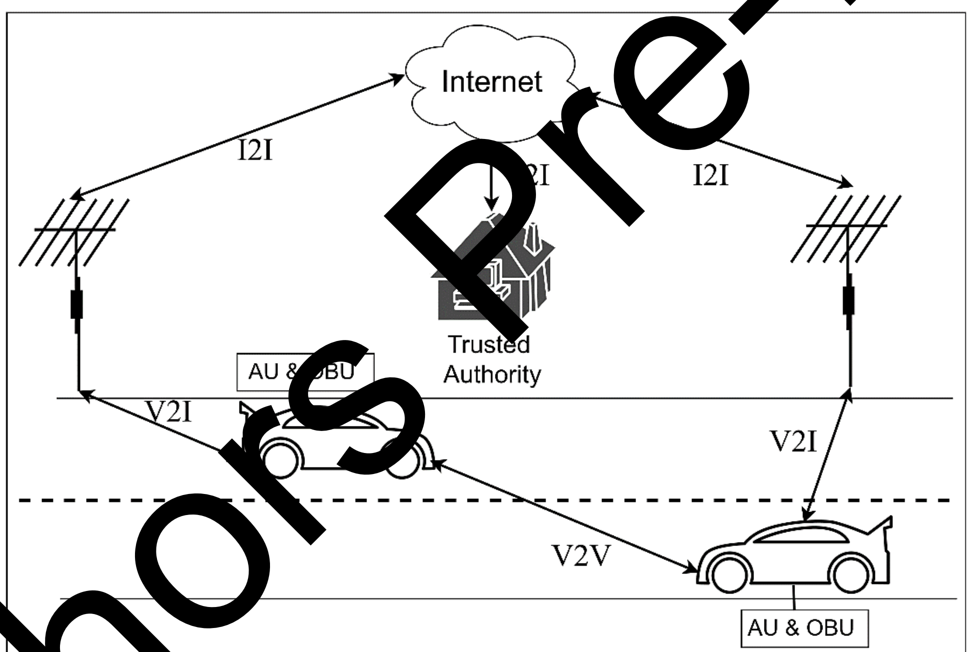


Figure 1. VANET communication model

VANET-enabled vehicles can gather data about conditions such as traffic jams and slick roads as well as their own driving status [2-4]. The data collected aids in improving driver comfort and safety in VANET vehicles. It is distinguished by high node mobility, communication link maintenance across a constrained range, and the absence of power issues.

Information is transferred between a car and a roadside unit (RSU) and between other vehicles inside a VANET via an open wireless channel [5]. This simplifies the task for attackers to carry out their nefarious objectives, such as traffic monitoring. Insider attackers can also send fake messages to report fraudulent activities. While increased connectivity and the number of communication channels have led to various breakthroughs, data security and reliability remain the most critical challenges in designing automotive solutions [6-8]. As a result, the main issues are the vehicles' secrecy and the safeguarding of data exchanges, that is accomplished by confirming the reliability, legitimacy, and integrity of event data.

Previous research has used numerous centralized solutions involving cloud computing [9,10]. While cloud computing improves computational efficiency and resource use in automotive contexts, it is not suitable for VANET applications due to latency sensitivity and vehicle mobility requirements. Vehicle networks are susceptible to various threats, leading to the use of numerous cryptographic techniques in the past [11-13]. Authentication is carried out by traditional security mechanisms, including password protection and biometric security with key-based authentication. However, these methods do not verify the accuracy of the data being supplied. The current solution uses edge service providers and multimedia data sharing to detect events before recording them on the blockchain, but the authentication process is lengthy [14-16]. The proposed solution resolves the problems with existing techniques. Blockchain is a decentralized network made up of several blocks with different kinds of information that function as an open ledger for every user on the network. Blockchain is featured in our recommended work partly due to its tamper-proof nature, consensus mechanism, and immutability of data storage, which makes alterations extremely difficult.

This research suggests a novel machine-learning-based data authorization approach that combines IPFS and blockchain to address these problems. Blockchain is integrated in the implementation of neural network parts, which utilise information from automotive sensors to make decisions and interpret situations creatively to improve the safety of on-road driving[20–21]. The information gathered by RSU are first preserved in IPFS, after the completion of an intelligent contract to create a neural network transaction authenticity mechanism and categorise events as dangerous or not. Initially, two clusters are created from the events gathered at RSU using the non-overlapped K-means clustering technique. By extracting the vehicle's true identity and verifying its validity in line with the database, RSU reduces the computing load on the vehicle. The data is anticipated using a domain expert. The vehicle retrieves the most recent decision rules from IPFS via a smart contract to validate the event. If the decision rules determine that the event is harmful, the vehicle removes the message. This ensures only authentic communications are transmitted over the network. Before forwarding messages to the next hop, the vehicle frequency verifies them using the decision rules derived from the execution of the smart contract.

The highlights of the work are as follows:

- This method enhances the security of message distribution by integrating interplanetary file systems (IPFS) and blockchain technology, ensuring tamper-proof records in a distributed environment.
- The proposed system employs the Iterative Import Vector Machine (IIVM) classifier and Non-overlapped K-means clustering to effectively classify and identify malicious event messages. Simulation results show that this approach improves event spoofing detection accuracy by 96.21%, significantly enhancing the reliability and safety of communication within VANETs.
- This approach not only prevents the spread of harmful messages but also protects the privacy and safety of vehicles from potential threats, addressing critical issues in VANET security.

The remaining sections are arranged as follows: Section II provides a brief overview of the suggested task and relevant current methods. The recommended procedure for event confirmation, approval, and safe event transmission is covered in Section III. The outcomes of the planned effort are covered in Section IV, and a conclusion is given in Section V.

II. Related works

The effects of the VANET blockchain system owing to mobility were presented in [22]. They examined three metrics: the volume of traded blocks during the rendezvous, the dependability of a rendezvous, and the contingency of a feasible block addition. A method for sharing secure information between cars using static and dynamic attributes with an attribute-based cryptography technique was demonstrated in [23]. This method uses a new group signature called CP-ABE in conjunction with ciphertext to provide verifiability and integrity, which requires pairing procedures. However, it is disadvantageous as an attacker may simply predict attribute values. An information restriction technique for transferring information over a virtual area networking (VANET) among many cloud storage platforms with automobile mobile services was suggested in [24]. Despite slower identification, this solution protects confidentiality and safety against harmful assaults and scales efficiently.

A broadcast encryption system based on identity was proposed in [25]. This method reduces redundancies, increases the trustworthy authority's work effectiveness, and compares the length of the encrypted text and the sender's ciphertext overhead. A blockchain depending on biometrics to protect vehicle transmission data, safeguarding the identity of the authorized user while preserving anonymity, was proposed in [26]. This approach combines blockchain technology with biometrics to ensure reliable data with computing cost. However, issues arise when combining several biometric features. The BCPPA method for transmission encryption, combining the key derivation process with blockchain technology, was suggested in [27]. Additionally, PKI-based signatures are utilized with batch verification to maximize throughput.

Privacy-preserving authenticating methods for VANETs to improve the abandoned unit's and the tamper-resistant device-aided CPPA's efficacy and security were offered in [28]. Using the chance oracle idea demonstrates reliability. Necessary security measures include identifying and ejecting rule breakers, detecting spoof communications, and safeguarding other vehicles' identities from un-linkability and untraceability. However, this significantly slows down traffic when approaching an RSU. The interaction between security, QoS, and safety awareness was examined in [29]. Extra care was taken to ascertain that crucial neighbors were included in the computation of awareness using vehicle heading-based filtration. Although this might make other drivers more cautious, it could be viewed as a safer strategy if there has previously been a history of moving offenses. The ability of automated automobiles to identify hostile vehicles and their misbehaving chauffeurs, who are subsequently removed from the safe car schedule, was enhanced in [30] by introducing a centralised man-in-the-middle operation with a significant amount of certainty. This method works in two stages: first, it finds counterfeit networks early on, and then it adds plausible constraints to the networking so that entity-centric confidence evaluations may be carried out. If a node meets certain characteristics, it might be deemed malevolent. After identifying a legitimate node, a data-centric credibility analysis can be conducted. The trust model's disadvantage is that it adds overhead by obtaining the sender's reputation from many sources.

The use of chameleon hashing to transmit data securely in cars was suggested in [31]. This methodology requires far less computational power to accomplish the authentication procedure for both vehicle-to-vehicle and vehicle-to-roadside traffic, working exceptionally well in actual vehicular contexts. The use of statistical classifiers for hybrid and complex attacks, enabling the detection of complicated attacks, was introduced in [32]. This proposed architecture is situation-aware, utilizing an environment references in lieu of pre-established dynamic privacy standards. Communications vehicles' movement information is context-referenced using Kalman and Hampel filters for both temporal and spatial synchronization. The results of these cluster models were lower for benign and misbehaving vehicle identification models, DCA-MDS and HCA-MDS, respectively, and less accurate in differentiating between the two types of cars. A multi-view fuzzy consensual cluster method for malware risk identification was suggested in [33-35]. This method applies 12 alternative extracted views for attribution and five categories of advanced persistent threats. Although it takes longer and has a 95% accuracy rate, the fuzzy criteria help effectively handle the threat attribution problem by differentiating between existing overlaps between various types of hostile states.

Research gaps identified

Despite significant advancements in secure communication for VANETs using blockchain and machine learning, several research gaps remain. Scalability and performance issues persist, as many existing methods struggle with efficiency when scaling, highlighted by the slower identification processes noted in [24]. The integration of biometrics with blockchain, as discussed in [26], presents challenges in managing multiple biometric features efficiently, requiring further research to develop seamless integration methods. Real-time authentication and communication in high-mobility environments like VANETs are often overlooked, necessitating low-latency solutions. Techniques like those in [23] using CP-ABE are vulnerable to attribute value prediction, indicating a need for more robust cryptographic techniques. Additionally, the centralised approach for identifying malicious vehicles in [30] introduces overhead, suggesting a gap in decentralised methods with lower overhead. Complex attack detection, as introduced in [32], still faces limitations in accurately differentiating between benign and misbehaving vehicles, calling for improved models and algorithms. Energy efficiency is another concern, with many solutions not considering the energy consumption of involved devices, as noted in [31]. Dynamic privacy standards, discussed in [32], require further development to adapt to changing conditions in VANETs. Trust models, such as the one in [30], introduce significant overhead, highlighting the need for more efficient models. Lastly, hybrid approaches integrating multiple security measures remain an open area of research, aiming to create more robust and resilient security frameworks for VANETs. Addressing these gaps is crucial for developing secure, efficient, and scalable solutions, enhancing the reliability and safety of vehicular communication systems.

III. Proposed trusted model

Vehicular ad hoc networks, which use wireless sensors to sense, analyze, and interact with the outside world, are a burgeoning field in intelligent transportation systems in the modern era. This proposed method ensures reliable and secure data sharing by integrating IPFS, blockchain technology, and a cutting-edge machine learning-driven verification method. It functions as follows: events that the RSU retrieves are first stored in IPFS. A contract with intelligence then determines if the event is hazardous based on the machine learning event verification model. Using the K-means clustering technique, each vehicle in the proposed system is first assigned to a cluster. This strategy groups the vehicles together, and the cluster head is selected based on the node with the highest performance capabilities. The cluster head is essential because it keeps an eye on how nearby cars are acting. Upon entering the network, every vehicle is assigned a mistrust value of 1.0, which helps to classify them as malicious, aberrant, or normal. The car is blocked and deemed dangerous if the distrust value rises above a predetermined level.

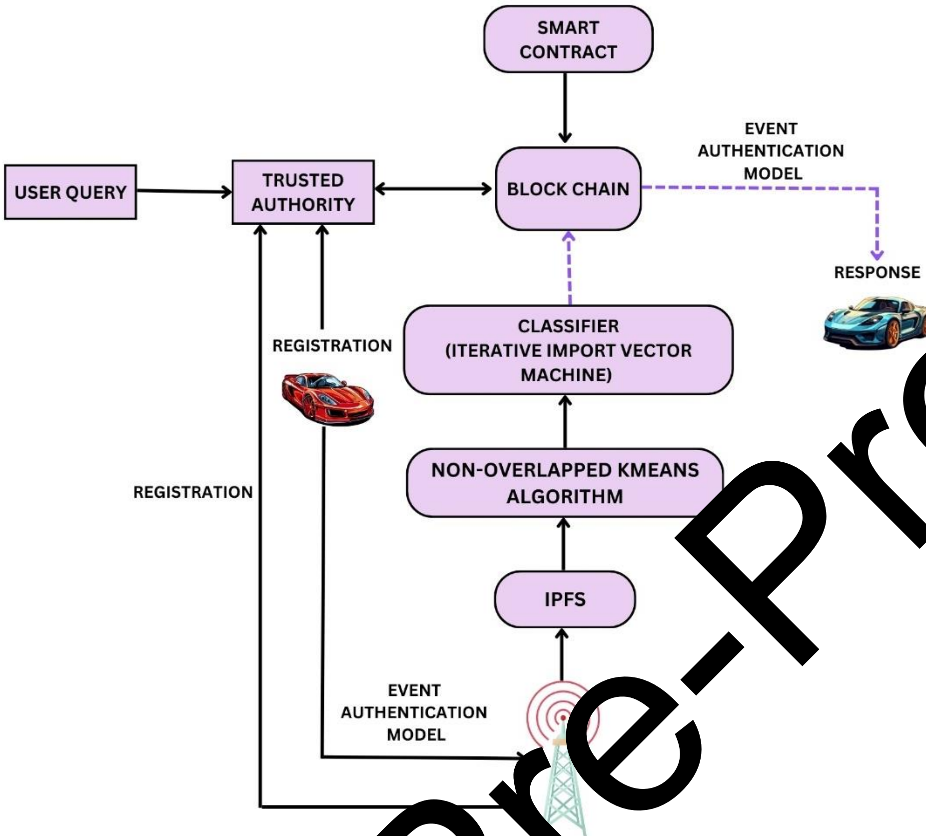


Figure 2. Proposed model taxonomy

Vehicles are characterized as malicious or non-malicious based on the mistrust value. After this classification, a support vector machine classifier—which has been trained on samples—is employed to identify harmful event signals and translate them into decision rules. These decision rules are saved in IPFS following each update and are subsequently accessed to verify events. The vehicle instantly drops an event that the decision rules determine to be harmful. By doing this, the network is guaranteed to forward only legitimate messages. Figure 2 displays the suggested system's functioning diagram. Because it saves time and money on communication expenses while certifying vehicles and events, the proposed solution is more efficient than traditional approaches. When it comes to accurately and efficiently identifying harmful events, the proposed strategy performs better than other traditional approaches. The entities involved in the proposed system include the trustworthy authority, RSU, IPFS, smart contracts, and blockchain. Below is a description of the system's workflow.

3.1 Registration and validation

Intelligent vehicles (IVs) are among the modern technologies that have seen significant growth and adoption in all aspects of life connected to the internet. Through their interaction and integration with RSUs, these IVs create a virtual network. An IV sends a request message to a reliable authority if it wants to join the network. The trustworthy authority serves as a registrar in this system, compiling all IV-related data and providing a public key. Vehicles can communicate with one another using this certificate. The trusted authority is also utilized for data authentication to preserve data integrity.

3.2 Analysis of algorithm

Inthis approach, a car cannot enter the network without first registering. To obtain a registration certificate, the car uploads its data to a reliable authority. The issued certificate is cryptographically connected and digitally secure. The car communicates with the reliable source and obtains the ID pseudonym, which occurs only once. By using the MAC address and real ID as inputs for registration, less processing power and time are used. Vehicles connect for the first time across the network with the provided pseudonym ID, verifying innovative IVs, and the certification process is safe.

Algorithm I Registration and validation

```
Initialization
Inputs: MAC address, No. of vehicles.
Outputs: IVregistration,MAC address validation, stores in IPFS.
While IV is in connection with network do
Registration
Check IV_owner, Real_ID, MAC_address
Returnregistered IV
"Validation of ID"
if hash1=hash2 then
"Requested IV is authentic"
Else
"Requested IV is non-authentic"
end if
"MAC validation"
    MAC1= Address on IV
    MAC2=Address on IPFS
if MAC1 = MAC2then
"MACisvalid.IVsuccessfullyregisteredonthenetwork"
Else
"MACisinvalid.IVfailedtoregisteronthenetwork"
end if
"Storedon IPFS"
  "forward data to IPFS"
IPFS response
"returnhashofdata"
end while
END
```

3.3 Road side unit (RSU)

Packet routing between distant locations is done by RSUs. These customized wireless devices are used for V2I (Vehicle-to-Infrastructure) and V2V (Vehicle-to-Vehicle) communications and are positioned beside highways. They link roaming vehicles to the internet and transfer data to other RSUs as a permanent infrastructure. RSUs and cars can collaborate on processing, communication, and coordination, facilitating distributed and cooperative applications. This architecture stores events collected by roadside devices in IPFS, where they are subsequently processed by a smart contract .

3.4 Interplanetary file system

An interplanetary file system, a decentralized technique for data interchange and storage, is the means by which the suggested system prioritizes effective storage management. Data is posted to the blockchain as hashes, kept there, and mapped using a distributed hash table. Upon entering the system, data is partitioned into chunks of 256 KB each. The blockchain records the hash value of each segment after it has been computed and posted to the distributed hash table. This technique offers distributed and independent hash storage, ensuring effective system maintenance. It also determines the vehicle's reputation scores.

3.5 Cluster formation using Non-overlapped K-means clustering

Using a K-means clustering approach, each automobile is allocated to a cluster with the relationship dependability model taken into consideration as an objective function. Considerations include traffic volume, relative velocity, and node proximity. Automobiles are arranged into clusters to facilitate successful interaction; the head of the group is the nodes with the most capacity. The K-means algorithm groups cars using the link reliability model. By considering factors such as relative speed (ΔV) and traffic density (λ), the connection dependability model is calculated as follows:

$$P_t(t) = \frac{4.D_r}{\sigma \Delta v \sqrt{2\pi}} \times \frac{1}{t^2} \times e^{-\frac{\left(\left(\frac{2Dr}{t} - \mu \Delta v\right)^2\right)}{2\sigma \Delta v^2}} \quad (1)$$

Where $D_r[m]$indicates the vehicle transmission area and Δv stands for relative speed. Their mobility is shown by their relative speed[km/h]. On the other hand, traffic density [vehicle/km] is used to describe how many cars are on a given road section. Let V_j represent a vehicle with position $(x_j, y_j)$and velocityV_j for $1 < j < N$.Centroid c_i is defined as $1 < i < k$, with position (x_i, y_i) and velocity v_i. Equation (2) calculates the connection reliability model in light of this

$$p_{ij}(T_{ij}, \lambda) = \begin{cases} \frac{\delta.\lambda}{\lambda_c} \int_{t_o}^{t_o+T_{ij}} T_{ij} p(t)dt, & \text{if } \delta, \lambda < \lambda_c \\ \int_{t_o}^{t_o+T_{ij}} T_{ij} p(t)dt & \text{otherwise} \end{cases} \quad (2)$$

where T_{ij}in the equation stands for the likelihood, as calculated using, that the vehicle's connection to the centroidc_i will remain functional and is determined using

$$T_{ij} = \frac{L_{ij}}{\Delta v_{ij}} = \frac{(y_i - y_j)^2 + (x_i - x_j)^2}{\underset{v_i - v_j}{\vec{j}}} \quad (3)$$

Based on the matching cluster head and the connection reliability model, each vehicle is assigned to a cluster. This model takes positional changes and acceleration into account while estimating the vehicle's maximum time inside the cluster. As such, the likelihood of an automobile leaving a cluster is affected by changes in velocity and traffic volume, in addition to the separation between the vehicle and the cluster center. As a result, the K-means algorithm's objective function F, which is defined as, depends on network dependability.

$$F = \text{avgmax}_c \sum_{i=1}^{k} \sum_{x_j \in C_i} p_{ij}(T_{ij}, \lambda) \qquad (4)$$

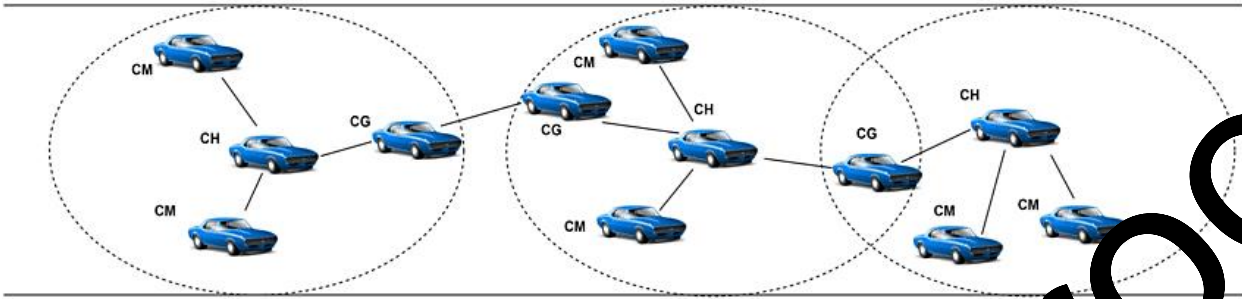


Figure 3. Clustering of vehicles

Figure 3 shows that the cluster members are represented in red, then yellow in CHs. The CA has the authority to renew the term of a cluster leader who has served for a considerable amount of time. When a vehicle joins the VANET, its distrust value is set to 1.0. The nearest vehicle receives the transmission with the vehicle's first distrust value, recognises it, and adds it to the whitelist. The automobile gets blacklisted if mistrust exceeds a specific level. The mean amount of automobiles in the communication area has to be ascertained in order to establish the minimum threshold.

$$N_v = \frac{Navg}{Ravg} \qquad (5)$$

Mean vehicles (N avg) and automobiles (R avg) within the communication range are used to compute the threshold value. The most reliable car in the network serves as the cluster head. Monitoring refers to the process of tracking data about a vehicle's behavior. The car that patrols the area and observes other cars is called the verifier. The verifier's mistrust value is equal to or less than that of the other vehicle. The verifier classifies cars as malicious, normal, or abnormal based on their mistrust value. This classification helps the SVM classifier identify malicious event signals. Instead of inspecting every vehicle on the network, it focuses solely on the malicious ones, detecting any non-genuine event messages and discarding them immediately

3.6 IIVM classifier

IIVM classifiers guard each automobile against fake data injection attacks by executing authentication, confirming that the communication is authentic. Once authenticity is determined, it is transformed into decision rules. These decision rules are stored in IPFS with a timestamp until they are ultimately modified. The most recent IPFS decision rules are retrieved and verified through the smart contract's execution If the event is determined to be malevolent, the automobile discards the decision rule immediately. This ensures that only real messages spread throughout the network.

In this study, given a set of practice examples, a SVM classifier classifier seeks to derive a division hyperplanes from the sampling space.

$$D = \{(X_1, Y_1), (X_2, Y_2), \dots (X_n, Y_n)\} \text{ and } Y_i \in (-1, +1) \qquad (6)$$

$$W^T \vec{x} + b = 0 \qquad (7)$$

Equation (7) can be utilized to model the hyperplane, in which b represents the distance of the hyperplane from the coordinate source and, $W = w_1, w_2, \dots, w_d$ is the normal vector that determines the direction of the hyperplane.

$$r = \frac{|w^T x + b|}{\| w \|} \qquad (8)$$

The aircraft categorizes the training sample according to specific restrictions.

$$w^T x_i + b \geq +1, y_i = +1 \qquad (9)$$

$$w^T x_i + b \leq -1, y_i = -1 \qquad (10)$$

For (x_i, y_i) in training sample D.

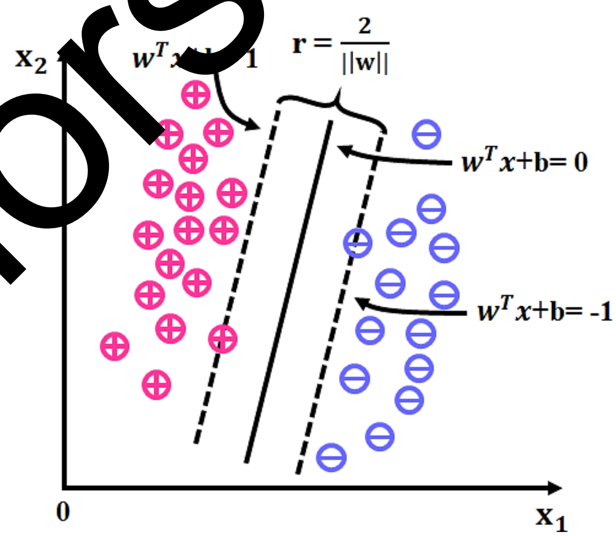


Figure 4. Training samples

The training point samples nearest to the plane are called support vectors (Figure 4). The entire length between two different kinds of heterogeneity help vectors and the plane of motion is calculated using a simple formula:

$$r = \frac{2}{\| w \|} \qquad (11)$$

Although SVM is a cutting-edge data mining model, its non-linearity is regarded as an opaque black box model. However, simple rules that can be used for classification without requiring bulk store upkeep can be extracted from the SVM model.The conversion process from malicious event identification to decision rules is depicted in Figure 5.

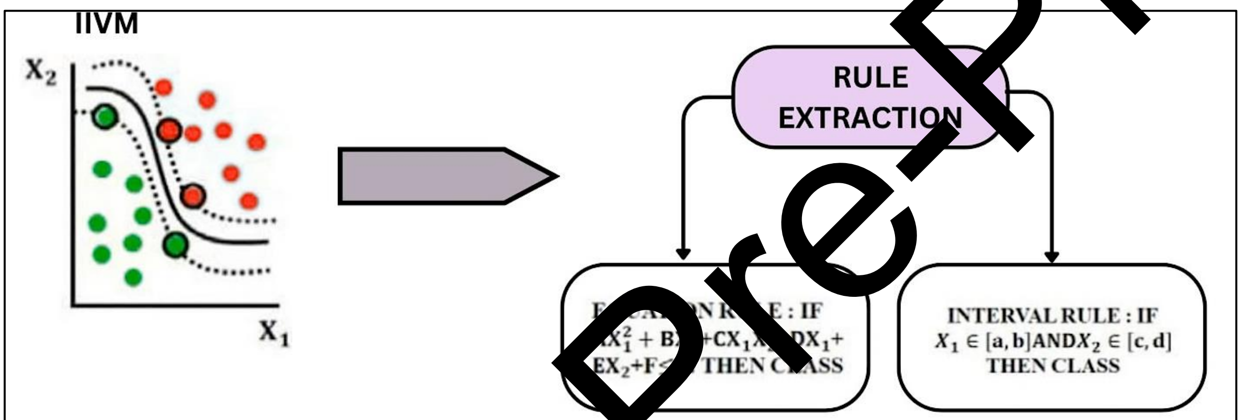


Figure 5. SVM to decision rule conversion

The RSU uploads the event to IPFS. The smart contract upgrades IPFS and generates the selection guidelines in addition to processing these stored events. The vehicle periodically retrieves the decision criteria via an executed electronic contract, implements them to the data messages, and verifies them before proceeding to a subsequent hop.

3.7 Smart contract

Smart contracts use if/then logic over a blockchain network to assess potentially hazardous occurrences found by ML Approach. These contracts can be executed without the use of a middleman because their code is examined by each participant in the blockchain network. By cutting out the intermediary, significant cost savings are achieved while improving sustainability, accuracy, security, and dependability.

3.8 Blockchain integration

Every vehicle that is linked downloads and updates blockchain technology. Blockchain stores reports of incidents and vehicle reliability history. Figure 6 illustrates the blockchain's operation process. When a vehicle encounters an event in the blockchain network, such as a collision, it broadcasts event alerts, along with different parameters, to other cars. The automobiles first analyze the event message to see if it is location-specific. The cars in the vicinity then check the other criteria in the event message. Every vehicle individually confirms that denial-of-service assaults, spam, and other invasive systemic threats have stopped while disseminating an incident notification further. Automobiles that acquire the event communication first assess the sender car's blockchain credibility before confirming it. When a message is accepted as trustworthy, it is saved in the local memory pool. From an untrusted incident message pool, mining machines gather a variety of event signals and confirm the accuracy of the sent variables. If the received event notification is authentic and reliable. the degree of confidence in it is adjusted. The degree of trust varies over time based on how trustworthy or deceptive messages remain. By using blockchain, the main issues with message dissemination are resolved. This ensures that the automobile can access the required data efficiently.

IV. Trusted Networking Reconfigured with Blockchain

Assuring trust, identifying untrustworthy networks and eliminating them from the task network, and choosing the best location to create the upper network in order to facilitate inter-zone forwarding and reach compromise are the principal objectives of the blockchain integrated into the UAV network. Adding blocks finishes drone network reconfiguring. Distribution of the present position throughout the sub-zone centre is necessary to reduce the duplication. In order to be chosen, the most appropriate node has to meet two criteria: it needs to be dependable, and aided intra-zone transit needs to prevent picking ineffective nodes.

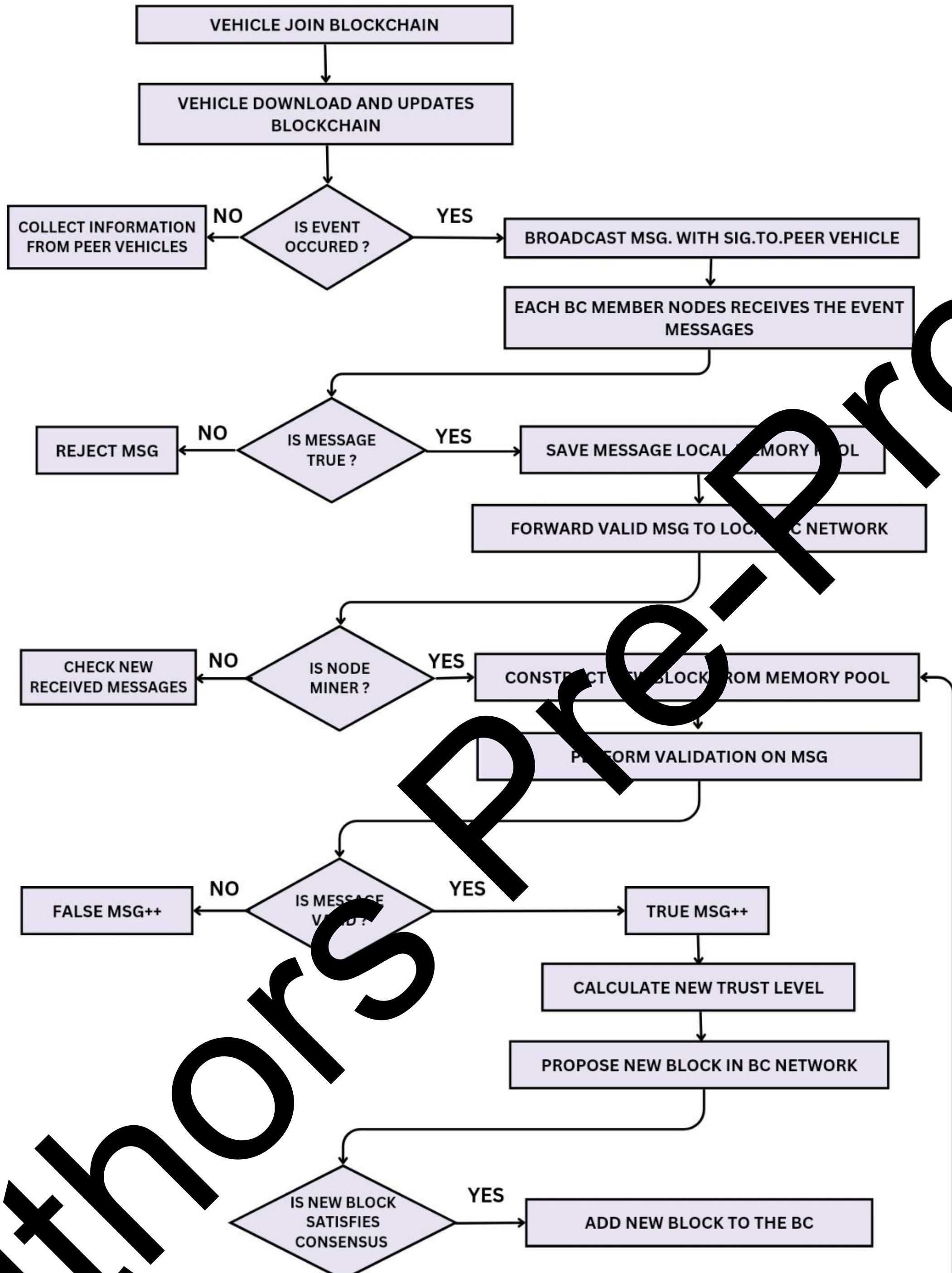


Figure 6. Workflow of blockchain integrated IIVM

4.1 Node Global Trustworthiness

In data consensus, all nodes produce an asynchronous generic subset (ACS) that includes StateData $_i = \{ID_i, [ID]_i, [ID_i^j\text{: CurScore }_{i-j}^{bc-height}], \text{cdots}\}$, The node's local state assessment (LSA) is discovered by counting the asynchronous generic subset ACS, representing the node's trustworthiness evaluation by all neighboring nodes: $LSA_i = \{ID_i, [ID]_i, [ID_j^i \text{ CurScore }_{j-i}^{bc-height}], \ldots\}$. As a distributed Byzantine system, does not allow the computational method indicated above to properly evaluate collusive or selfish conduct.

Using the global statistical computational technique helps to find nodes that are self-serving or collaborating and to modify discount. D_x is represented by the expected value of the local discount of all surrounding nodes GDiscount ^{x}, with a variance of σ^x, using :

$$\text{GDiscount }^x = \frac{\left(\sum_{i=0}^{n} \text{ CurScore }_{x-i}^{bcheight}\right)}{n} \tag{12}$$

$$\sigma^x = \sqrt{\sum_{i}^{n} \left(\text{CurScore }_{x-i}^{bcheight} - \text{GDiscount}^x\right) / n} \tag{13}$$

where i is one of node x 's n neighbors. Table 1 displays the guidelines for determining the worldwide trust degree discount.

Table 1. The guidelines for global dimension decrement

Reasons for Trust Discount	Global Discount
Discount $_\sigma(\mid \text{CurScore }_{x\mid i}^{bcheight} \mid < 5\sigma^x)$	0
Discount $_\sigma^x(\mid \text{CurScore }_{x\mid i}^{bcheight} \mid \geq 5\sigma^x)$	-0.5
Selfish node Discount $_{error}^x$	-1

Equation (14) in node x in accordance with the rule. The present global trustworthiness is determined by Equation (15).

$$\text{GDiscount }^x = \text{ GDiscount }^x + \text{ Discount }_\sigma^x + \text{ Discount }_{\text{error}}^x \tag{14}$$

$$\text{GReputation}_{x}^{bcheight} = \text{GReputaion}_{x}^{bcheight-1} + \text{GDiscount}^{x} \quad (15)$$

Algorithm II: Global Trust Assessment

```
Function: Global_Trust_Assess(LSD, IDx)
Initialize LSA[N] as empty
# Running in a Delegated Agent UAV IDx
# LSD already contains local state transactions for 2/3 of the total nodes in the network
if Nodes_Received(State_Data_x) ≥ 2/3 then
    # Extract corresponding decentralized transaction message blocks
    DRBCx ← Build_My_RBC_Packet()
    # Multicast its own DRBCx to the delegate agent nodes
    Multicast(DRBCx, {ID_A})
    while true do
        DRBCother ← Receive_DBC_From_Other_Agents()
        # Translate DRBCother to the delegate agent nodes
        Multicast(DRBCother, {ID_A})
        # If 2/3 DRBCs are acknowledged, consensus is reached
        ACS ← Build_ACS_from_State_Data(LSD)
        # Exit loop
        break
    end while
end if
# Statistical local assessment of all nodes
# ACS contains trustworthiness scores of each node for all neighbors
# LSA contains trustworthiness scores of all neighbors for each node
LSA ← Statistical_LSA(ACS)
# Compute assessment of IDx by all neighboring nodes from LSA
```

```
GDiscount_x ← (sum of CurScore_xi_bcheight for i = 0 to n) / n
# Compute confidence variance of IDx
sigma_x ← sqrt((sum of (CurScore_xi_bcheight - GDiscount_x)^2) / n)
# Amend global trustworthiness assessment
if |CurScore_ix_bcheight| > (5 * sigma_i) then
    Discount_sigma_x ← -0.5
end if
if No_Record_From_Neighbor(IDx) then
    Discount_error_x ← -1
end if
GDiscount_x ← GDiscount_x + Discount_sigma_x + Discount_error_x
GReputation_x_bcheight ← GReputation_x_bcheight-1 + GDiscount_x
return GReputation_x_bcheight
```

4.2 Zone Center Node Elections

The The dynamic nature of the UAV network necessitates a time-varying top layer management network, with dependable constituent nodes that accurately reflect their respective regions. The representation of the feature in node $\vec{N}_i = [ID_{i1}, ID_{i2}, \dots, ID_{im}]$,. If there are less than m neighbors, zeros are added to the missing part.

The number of UAVs in network, represented by the feature vector $\vec{U} = [\vec{N_1}, \vec{N_2}, \dots, \vec{N_n}]$, is used to represent the UAV network [33]. The feature vectors used for clustering are lists that are used for categorization, not numerical vectors.

$$d(\vec{N}_i, \vec{N}_j) = \sum_{x=1}^{m} \sum_{y=1}^{m} \delta(ID_{ix}, ID_{iy}) \qquad (16)$$

where $\delta(ID_{ix}, ID_{iy}) = 0$, if $ID_{ix} \neq ID_{iy}$; $\delta(ID_{ix}, ID_{iy}) = 0$, if $ID_{ix} = ID_{iy}$

Let $U^k = [\vec{N}_{k1}, \vec{N}_{k2}, \dots, \vec{N}_{kn}]$represent a UAV network sub-zone.

Definition 1: The mode of the UAV network U^k is represented by the feature vector $Q = [ID_1, ID_2, \dots, ID_m]$ if it satisfies function (17).

$$D(Q, \vec{N}_i) = \sum_{i=1}^{m} d(\vec{N}_i, Q) \qquad (17)$$

Before select $Q \in U^k$, pick the least value.

By computing n_{ID_x}, or the number of times the neighbor node ID_x appears in all lists of neighbors, one can determine the frequency of ID_x in the zone U^k.

$$f(ID = ID_x \mid U^k) = \frac{n_{ID_x}}{m} \qquad (18)$$

Theorem 1 states that the function $D(Q, N_i)$ reaches a minimum when and only if the mode update mechanism for k-modes of UAV networks is such that the following condition holds:

$$f(ID = ID_x \mid U^k) \geq f(ID = ID_j \mid U^k) \qquad (19)$$

where $ID_x \neq ID_j, \forall j = (1,2, \ldots, m)$. Thetheorem's relevant proofs are found in Algorithm

Algorithm III Poof of updated techniques for for k-modes of UAV

while $(m - -)$ do
if $f(ID = ID_x \mid U^k) \geq f(ID = ID_j \mid U^k)$ then
if $n_{ID_x} > n_{ID_j}, j \neq x, \forall j = (1,2, \ldots, m)$ then
$Q \cup ID_x$
end if
end if
end while
$D(Q, N_i)$ reaches a minimum

4.2 Blockchain Synchronization and Updations

This system's two-stage consensus data consensual achieves an unchanging consensus outcome, a common fraction of local status events (ACS), at delegation agent endpoints using decentralised consistent transfer of DRBCs and externally verifiable smart contract agreements. Any agent network that has been authorised may now generate blocks, harmonise decision-making, and produce configuration information. While broadcasting fresh blocks in accordance with the verified nodes on the present-day blockchain, the delegated agents nodes update the local currency. Every time a node receives a new block and it calculates its height. If it is taller than the authorised agent network that contributed the block, the node updates the local blockchain. If not, it requests that they synchronise the blockchain with it.

After the information's consensus is done, the upper layer networks tells the agent at the node to find the neighbourhood central node, and update the nodes' trust levels, and re-set up the trusted drone network in its current state. This is done utilising statistics and clustering to process the neighbour list and global trust discount tables. Any participant node may explicitly request, at any point throughout a cycle, that the top layer networks initiate consensus if it observes notable changes to the physical configuration or poor local credibility of neighbouring nodes. Reconfiguring the dependable infrastructure is necessary for the blockchain's ongoing confirmation operation. In Figure 7, the consensus flow is shown.

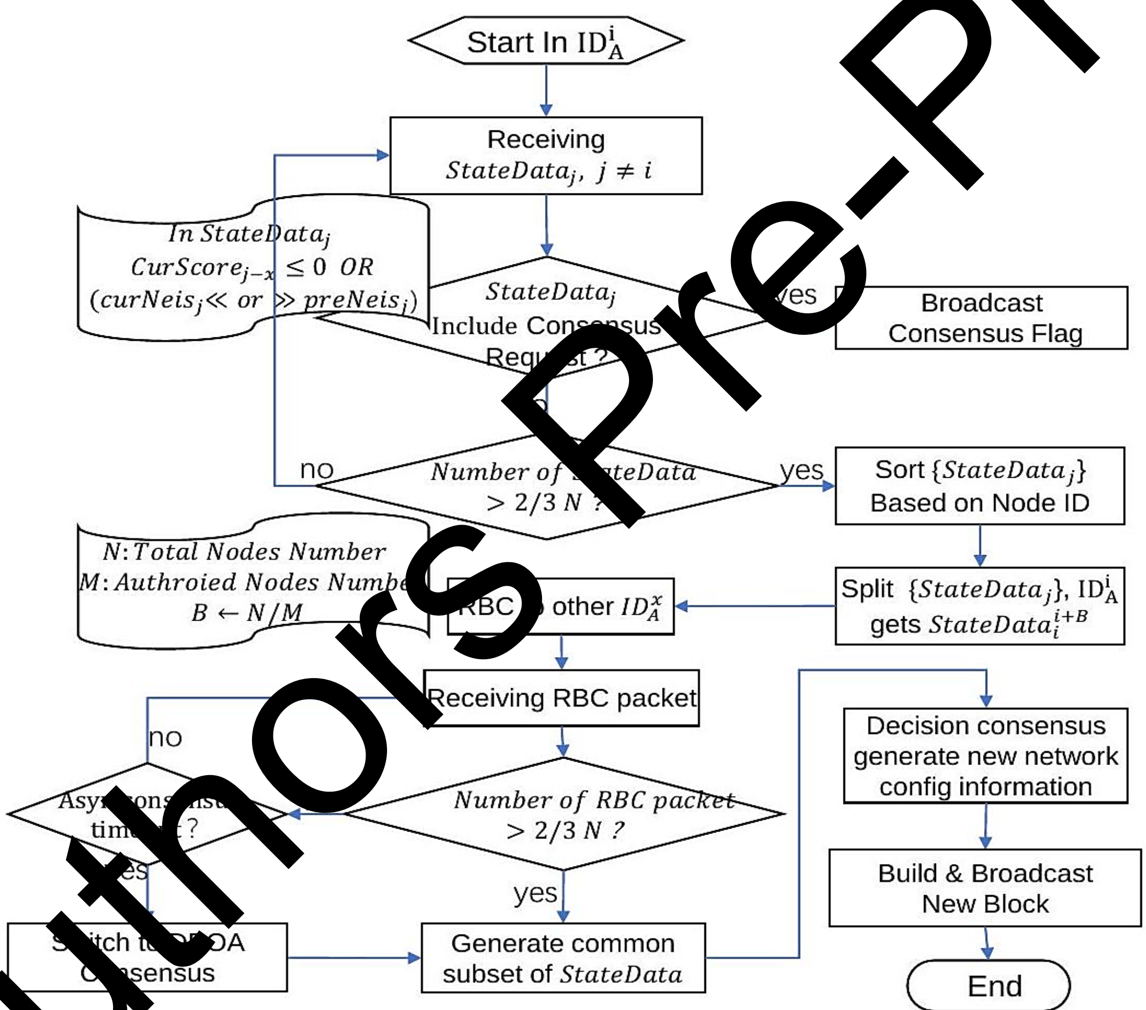


Figure 7. Two-phase consensus procedure in a node with authorization ID_A^i

The rate at which new blockchain blocks are added depends on how long it takes for data consensus to reach a decision. Even though the drone network frequently experiences network partitioning, a deterministic consensus can eventually be reached by an asynchronous consensus technique. Nevertheless, this strategy's original objective was to dynamically reorganize the network to preserve its general credibility. When the asynchronous consensus fails, the multi-point proof of authority (DPOA) compromise technique is instantly initiated for real-world applications. Both DPOA and proof-of-authority consensus employ chosen best state nodes to reach agreement each cycle. As a result, if more than two stations gain agreement, the information unanimity might be finished after the asynchronously decision delay. Reconfiguring the UAV connection within a secure time is ensured.

V. Simulation Experiments and Effect of Evaluation

UAV trustworthy networks dynamically reconfigure using the blockchain-assisted trusted Zone Routing Programme (proposed), which is formed when new blocks chain together during blockchain creation. Efficiency is measured using the delivery of packets rate, route overhead, and information transfer delay. The OSI seven-layer model architecture is used by Qualnet network simulation software, which is designed specifically for wireless mobile communication networks. Every network node's activity is estimated independently during the simulation to mimic real-world network functioning and provide a wide range of complex statistical data analysis functions.

This study aims to generate mission scenarios. The 1000 × 1000 m² scene, 100 UAV nodes, 30 data lines, 210 seconds for the simulation to run, 0–30 m/s for node movement speed, 30 seconds for dwell time, 500 ms for packet sending interval, and 0,5, 10, 15, 20, 25, and 30 malevolent nodes are all included in the simulation experiment. We employ 802.11b MAC layer technique and 400-meter wireless communication range. Every test procedure was executed three times using distinct randomised numbers, and the assessment was based on the mean of each of the trials. Finally, distinct randomised numbers in the system correspond to distinct node trajectories. Message Delivery Rate: The message delivery rate is the number of properly accepted frames by the target node and sent to the originating node. Figure 8 shows how the promised delivery percentages of the four route methods change as the number of broken nodes rises.

AODV has the greatest delivery rate without error nodes, whereas the other protocols have comparable rates. However, the blockchain-assisted trustworthy area routing methods don't really alter when new error nodes emerge. Deliveries rates, on the other hand, abruptly decline and finally collapse for OLSR, AODV, and ZRP. This is because, by continuously redesigning the upper logical networks utilised for agreement, BC-TZRP has high tolerance for failure and can separate the largest number of unstable locations from the entire network. The pace of delivery decline is also greatly accelerated by the network's inaccurate routed data; roadway routes under the remaining three technologies need to be updated and rearranged on a regular basis as the proportion of defective locations rises.

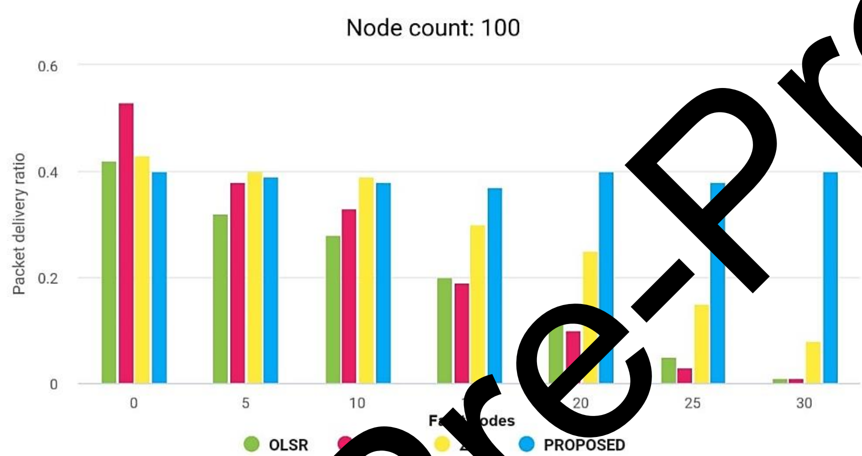


Figure 8. Packet arrival rate for a number of failed nodes

Overhead in Route: In the identical case, all nodes send out route command messages, which is the route overhead. Figure 9 demonstrates the routing overhead related to every method at different error locations. The biggest routing overhead is attributed to OLSR, which is adhered to by ZRP and AODV in the absence of irregular nodes. But as errant networks start to show up, OLSR, AODV, and ZRP's excess increases quickly, leading OLSR to fail first because the routing load uses cellular resources. On the other hand, BC_TZRP shows a consistent dropping trend and stays low due to the isolation of faulty nodes. The routing overhead of conventional routing systems is increased by the quantity of inaccurate routing information generated by erroneous nodes. However, the routing overhead is mostly constant since the nodes in BC_TZRP that are engaged in route creation and maintenance.

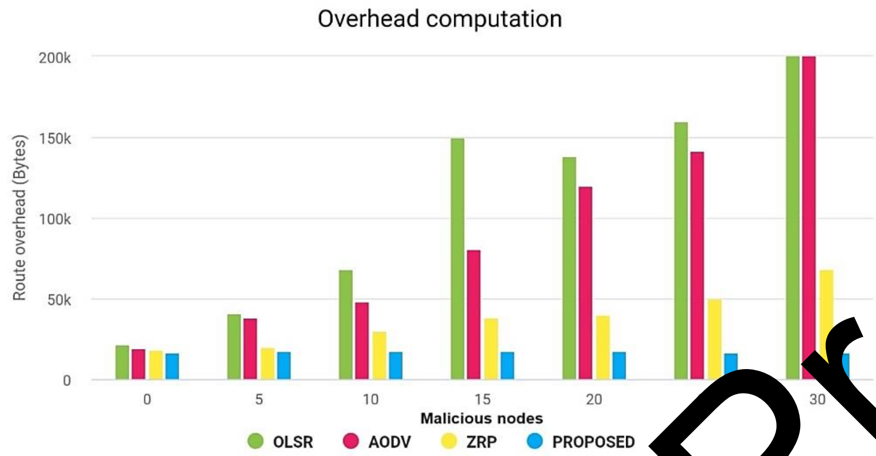


Figure 9. Routing overhead in the case of a steadily increasing number of failure nodes

The average end-to-end latency is the duration of time between a packet's departure from the source node and its arrival at the destination node. Figure 10 shows that ZRP has the shortest latency, OLSR the shortest, and AODV has the greatest without error connections. The average end-to-end delay of all three increases quickly because to the influence from malfunctioning routers. When there are more than 25 malfunctioning nodes, the communication system collapses and the delay goes to zero. The proposed work preserves the task's real trustworthiness while reducing mean end-to-end latency.

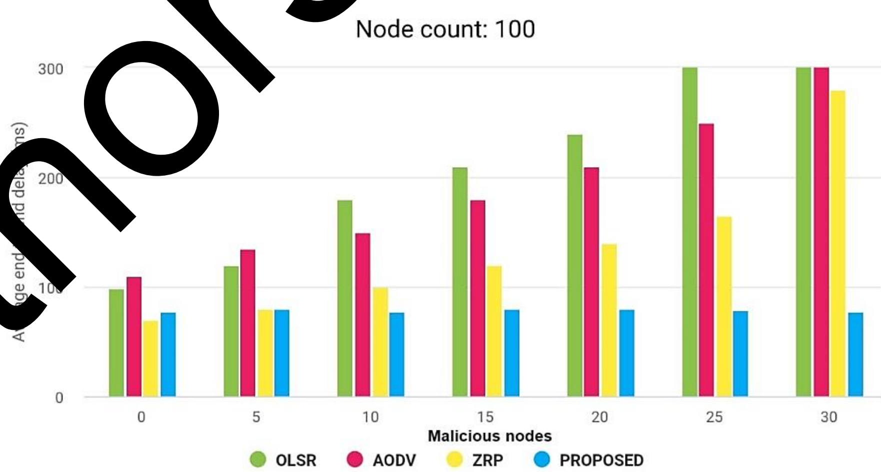


Figure 10. Average End-to-End latency in the scenario where the fault node is rising over time

By installing the proposed scheme, the new network will be reconfigured in accordance with the nodes' blockchain-recorded statuses. Reconfiguring the network primarily entails removing harmful nodes from it. The modifications in Figures 9 and 10 are minimal since these malicious nodes are not part of routing and data forwarding and are thus excluded from the new network. Furthermore, when a node discovers that an adjacent node is unreliable, it triggers the consensus process, asking the system to start consensus right once in order to isolate these problematic nodes as soon as possible. Malicious nodes in the experiment manipulate forwarding information, greatly undermining the reliability of the data they transmit. As a result, these nodes are promptly recognized as unreliable and removed from the task network. As a result, malicious nodes can only harm the network for a very brief time before being isolated and causing little to no damage.

While blockchain network technologies can authenticate UAV networks to keep malicious external nodes from accessing them without authorization, the complex mission environment also involves the possibility of node formation in addition to selfish and flawed nodes. This scenario involved setting up trials with varying percentages of false nodes (which made it possible for compromised internal nodes of drones impersonating real entities).

The most economical option for globally dependable management and economical network use of resources for dispersed drone networks functioning in intricate surroundings is the decentralised and de-trusted digital currency blockchain. Drones as blockchain servers are less resource-intensive than those in traditional a distributed ledger It must be adjusted to the desired asynchronous, lightweight, and dynamic error node production environment. The purpose of the upcoming wave of context design experiments is to address the low energy consumption and lightweight storage of blockchain technology.

Blockchain Storage: Blockchain nodes need a lot of storage because the blockchain is a shared chain database that is always expanding and uses unchangeable historical data to validate transactions. Utilising the decentralised Proof of Stakes (DPOS) voting process, 21 servers are tasked with keeping track while assessing the data retention utilisation of blockchains. Figure 11 displays the simulation experiment's outcomes.

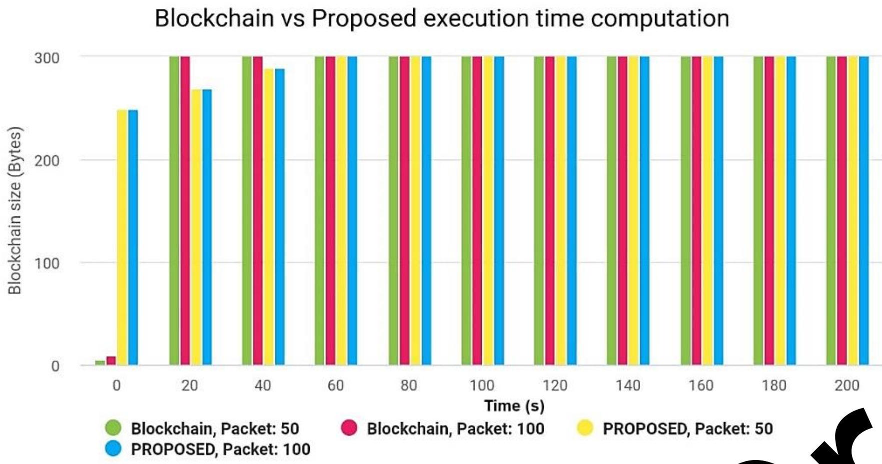


Figure 11. Time computation

Due to its two-stage support process and the reality that the digital ledger only retains the choice's agreement, it is evident that the BC_TZRP method has an average rate of expansion and remains devoid of transactions volume. Conversely, all transaction history data is stored on the standard DPOS blockchain, which needs more capacity as transaction traffic increases.

Energy Usage: One major problem with the drone system is its energy usage. The general opinion computation in the framework of blockchain consumes most of the power needed for transmission latency and execution. As opposed to using a conventional blockchain, ZRP routing coherence is used in a prototype situation with 100 swarm networks. POW consensus technique changes the amount of activities and zeros in in the required hash headers to match the evaluation setting, taking around 30 seconds to compute. Consensus times for PBFT and POS are guaranteed to be determined by the quantity of operations. If the specified asynchronously compromise method fails to achieve a contract in 20 seconds, the proof-of-authority consensus procedure is started. Using numerous faulty node locations, the evaluations measure the majority method's connection and computational latency and convert it into the consumption of energy. Applying compromise to ZRP's real-time relaying behaviour tracking local state transaction and analysing many experiment circumstances for the POW and PBFT consensus protocols calculates the network's energy usage. Figure 12 displays the simulation experiment's outcomes.

Although the POS consensus technique doesn't require any computational power, the growing number of rogue nodes also results in an increase in the amount of bandwidth used by the network due to incorrect routing. Because of the rise in malicious nodes and the frequency of view change during the consensus process, the PBFT also uses more energy. The BC_TZRP method substitutes agent nodes for consensus delegation and reconfigures the network on a regular basis to eliminate untrustworthy nodes and minimize the quantity of overlapping routes. The consensus overhead is essentially constant regardless of the quantity of malicious locations since each phase offers an extra fair distribution of resources for the infrastructure as a whole.

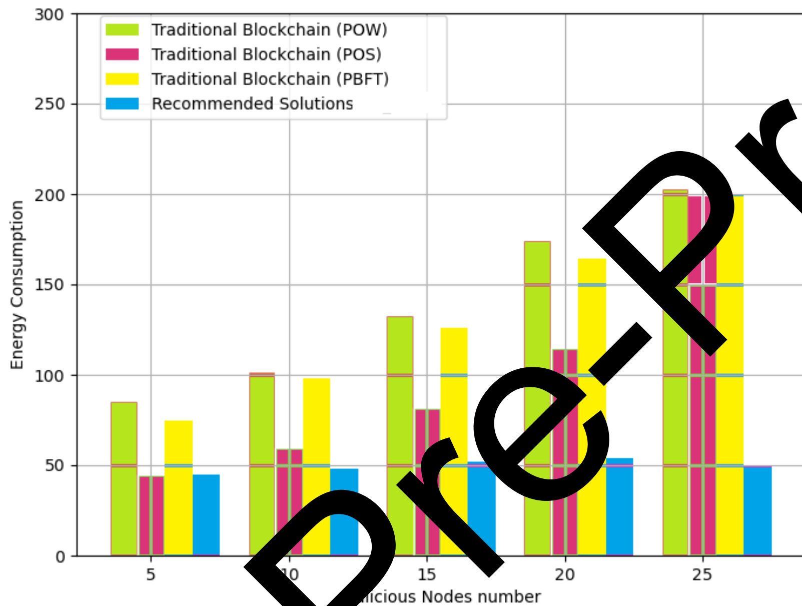


Figure 12. Energy required for consensus vs amounts of malicious routers

Attack prediction computation

This section summarizes the performance of the proposed system in detecting attacks compared to traditional approaches. The results demonstrate significant improvements in attack detection rates and event spotting detection accuracy under varying network densities and numbers of malicious vehicles. These findings highlight the effectiveness of the proposed system in challenging network environments.

Table 2: Attack Detection Rate vs. Network Density

Network Density (nodes/km²)	Proposed Detection Rate without Blockchain (%)	Proposed Detection Rate with Blockchain (%)
10	70	85
20	65	83

30	60	80
40	55	78
50	50	75

The table 2 shows how the attack detection rate changes with different network densities. The proposed system consistently outperforms the traditional approach, showing a higher detection rate across all levels of network density. As the network density increases, the detection rate decreases for both methods, but the proposed system maintains a significant advantage.

Table 3: Attack Detection Rate vs. Number of Malicious Vehicles

Number of Malicious Vehicles	Proposed Detection Rate without Blockchain (%)	Proposed Detection Rate with Blockchain (%)
5	68	90
10	60	85
15	52	80
20	45	75
25	40	70

The table 3 illustrates how the number of malicious vehicles impacts the attack detection rate. The proposed system using the SVM classifier shows a significantly higher detection rate compared to traditional techniques. As the number of malicious vehicles increases, the detection rate decreases for both methods, but the proposed system remains superior.

Table 4: Event Spoofing Detection Accuracy

Approach	Detection Accuracy (%)
Proposed system without Blockchain	70
Proposed system with Blockchain	96

This table 4 compares the event spoofing detection accuracy of traditional techniques with the proposed system. The proposed system achieves a much higher detection accuracy of 96%, compared to 70% for traditional methods. The high accuracy is due to the proposed system's confidence model, which effectively distinguishes genuine events from false occurrences through persistent monitoring and nodes scoring. Hence, the tables clearly illustrate that the proposed system has significantly improved attack detection rates and event spoofing detection accuracy compared to traditional approaches, even as network density and the number of malicious vehicles increase.

VI. Conclusion

The work that is being suggested incorporates blockchain technology with IPFS in order to build a novel machine-learning-based technique for message authentication. The goal of this approach is to prevent inner vehicles from spreading false information. In order to ensure that secured event sharing, authorization, and verification are carried out effectively amongst internal vehicles, this method is utilised. An effective defence against hostile attacks and identification of rogue cars is provided by the transaction storage mechanism that is based on distributed blockchain technology. In order to determine whether or not this access authentication system is effective, it is necessary to investigate the legitimacy and safety of the system that is being presented. The system is evaluated based on the amount of time it takes to verify vehicles, validation of events, and the amount of money spent on communication. It is able to carry out its procedures with a limited amount of time in comparison to other systems that are currently in use, and the event trust model that is utilised in this system is capable of achieving greater detection of harmful events. In comparison to the approaches that are now in use, it achieves a high level of security and safeguards automobiles against harmful intruders. It is possible that future studies in this area may concentrate on the creation of a novel, lightweight, and better neural networking-based message authorization system that is capable of successfully detecting network invaders.

REFERENCES

1. Zhu H, Yuen KV, Mihaylova L, et al. Overview of environment perception for intelligent vehicles. IEEE Transactions on Intelligent Transportation Systems 2017; 18(10): 2584–2601. doi: 10.1109/TITS.2017.2658662
2. Al-Shareeda MA, Anbar M, Hasbullah IH, et al. Survey of authentication and privacy schemes in vehicular ad hoc networks. IEEE Sensors Journal 2020; 21(2): 2422–2433. doi: 10.1109/JSEN.2020.3021731
3. Qu F, Wu Z, Wang FY, et al. A security and privacy review of VANETs. IEEE Transactions on Intelligent Transportation Systems 2015; 16(6): 2985–2996. doi: 10.1109/TITS.2015.2439292

4. Puneeth, R. P., & Parthasarathy, G. (2024). Blockchain-Based Framework for Privacy Preservation and Securing EHR with Patient-Centric Access Control. Acta Informatica Pragensia, 13(1), 1-23.
5. Verma S, Zeadally S, Kaur S, et al. Intelligent and secure clustering in Wireless Sensor Network (WSN)-based intelligent transportation systems. IEEE Transactions on Intelligent Transportation Systems 2021; 23(8): 13473– 13481. doi: 10.1109/TITS.2021.3124730
6. Elkhail AA, Refat RUD, Habre R, et al. Vehicle security: A survey of security issues and vulnerabilities, malware attacks and defenses. IEEE Access 2021; 9: 162401–162437. doi: 10.1109/ACCESS.2021.3130495
7. Yang A, Weng J, Cheng N, et al. DeQoS attack: Degrading quality of service in VANETs and its mitigation. IEEE Transactions on Vehicular Technology 2019; 68(5): 4834–4845. doi: 10.1109/TVT.2019.2905522
8. Jan S A, Amin NU, Othman M, et al. A survey on privacy-preserving authentication schemes in VANETs: Attacks, challenges and open issues. IEEE Access 2021; 9: 153701–153726. doi: 10.1109/ACCESS.2021.3125521
9. Puneeth, R. P., & Parthasarathy, G. (2024). A cross-chain-based approach for secure data sharing and interoperability in electronic health records using blockchain technology. Computers and Electrical Engineering, 120, 109676.
10. Alsayfi MS, Dahab MY, Eassa FE, et al. Securing real-time video surveillance data in vehicular cloud computing: A survey. IEEE Access 2022; 10: 51525–51547. doi: 10.1109/ACCESS.2022.3174554
11. Ribouh S, Phan H, Malawade AV, et al. Channel state information-based cryptographic key generation for intelligent transportation systems. IEEE Transactions on Intelligent Transportation Systems 2020; 22(12): 7496– 7507. doi: 10.1109/TITS.2020.3003577
12. Thoms GRW, Muresan R, Al-Dweik A. Chaotic encryption algorithm with key controlled neural networks for intelligent transportation systems. IEEE Access 2019; 7: 158697–158709. doi: 10.1109/ACCESS.2019.2950007
13. Tan H, Choi D, Kim P, et al. Comments on "dual authentication and key management techniques for secure data transmission in vehicular ad hoc networks". IEEE Transactions on Intelligent Transportation Systems 2017; 19(7): 2149–2151. doi: 10.1109/TITS.2017.2746880

14. Zhao Z, Guardalben L, Karimzadeh M, et al. Mobility prediction-assisted over-the-top edge prefetching for hierarchical VANETs. IEEE Journal on Selected Areas in Communications 2018; 36(8): 1786–1801. doi: 10.1109/JSAC.2018.2844681
15. Zhu C, Zhu X, Ren J, et al. Blockchain-enabled federated learning for UAV edge computing network: Issues and solutions. IEEE Access 2022; 10: 56591–56610. doi: 10.1109/ACCESS.2022.3174865
16. Li Q, Tian Y, Zhang Y, et al. Efficient privacy-preserving access control of mobile multimedia data in cloud computing. IEEE Access 2019; 7: 131534–131542. doi: 10.1109/ACCESS.2019.2939299
17. Li B, Liang R, Zhu D, et al. Blockchain-based trust management model for location privacy preserving in VANET. IEEE Transactions on Intelligent Transportation Systems 2020; 22(6): 3765–3775. doi: 10.1109/TITS.2020.3035869
18. Parthasarathy, G., & TOMAR, D. (2014). OPTIMIZED PRUNE BASED DATA MINING (OPBDM) FOR DISTRIBUTED DATABASES: AN ADAPTIVE APPROACH. Journal of Theoretical & Applied Information Technology, [illegible](3)
19. Xu R, Li C, Joshi J. Blockchain-based transparency framework for privacy preserving third-party services. IEEE Transactions on Dependable and Secure Computing 2022. doi: 10.1109/TDSC.2022.3179698
20. Liu T, Yang Y, Huang GB, et al. Driver distraction detection using semi-supervised machine learning. IEEE Transactions on Intelligent Transportation Systems 2015; 17(4): 1108–1120. doi: 10.1109/TITS.2015.2496157
21. Virupakshappa MM. An efficient vehicle traffic maintenance using road side units in VANET. Imperial Journal of Interdisciplinary Research 2016; 3(2016): 783–784.
22. Kim S. Impacts of mobility on performance of blockchain in VANET. IEEE Access 2019; 7: 68646–68655. doi: 10.1109/ACCESS.2019.2918411
23. Zhang L, Wang J, Mu Y. Secure and privacy-preserving attribute-based sharing framework in vehicles ad hoc networks. IEEE Access 2020; 8: 116781–116795. doi: 10.1109/ACCESS.2020.3004247
24. Puneeth, R. P., & Parthasarathy, G. (2023). Survey on Security and Interoperability of Electronic health record sharing using Blockchain Technology. Acta Informatica Pragensia, 12(1), 160-178.

25. Zhong H, Zhang S, Cui J, et al. Broadcast encryption scheme for V2I communication in VANETs. IEEE Transactions on Vehicular Technology 2021; 71(3): 2749–2760. doi: 10.1109/TVT.2021.3113660