BLOCKCHAIN-BASED SECURE AND SCALABLE ROUTING MECHANISMS FOR VANETS APPLICATIONS

Hariharasudhan V and Dr.P.Vetrivelan

School of Electronics Engineering (SENSE), VIT, Chennai, TamilNadu 600127, India

ABSTRACT

The VANET has seen a boom in the distribution of significant source data,enabling connected vehicle communications to enhance roadway safety.Despite the potential for interesting applications invehicle networks,thereare still unresolved issues that have the potential to hinder bandwidth utilization once deployed. Specifically, insider assaults on VANET platforms such as Blackhole attemptscan completely stop vehicle-to-vehicle communications and impair the networks' performance level. In this study, we provide the blockchain-based decentralized trust scoring architecture for the participants in the network to identify existing and blacklisted insider adversaries in VANET. To address this concern, we suggest a two-level detection technique, in the first level neighboring nodes determine theirtrustworthiness and in the second level it aggregates trust scores for vehicle nodes using a consortium blockchain-based mechanism that uses authorized Road Side Units (RSUs) as consensus mechanism. The blacklisted node records are then periodically changed based on the trust scores supplied by the nearby nodes. In regards to the practical scope of the network, the experimental study demonstrates that the suggested solution is effective and sustainable. To improve packet delivery ratio and vehicle node security in the VANET, the blockchain-based Trust-LEACH routing technique has also been created. The performance analysis has been carried out for Computational cost analysis, Computational time for block creation, Network analysis, SecurityAnalysis, and MITM attack analysis. Additionally, we provide proof that the suggested approach enhances VANET reliability by thwarting and removing insider threat initiation nodes from its blacklist.

KEYWORDS

Blockchain Technology, VANET Security, Secure Routing, Insider AttacksBlockchain-based consensus algorithms.

1. INTRODUCTION

Through Vehicle-to-Everything (V2X) connections, Vehicular Ad-hoc Networks (VANETs) hold enormous promise for improving Intelligence Transportation Infrastructure (ITS). Because VANET technology has such significant promise for improving transportation infrastructure, researchers are paying close attention to it [1]. Vehicle communications are set up via wireless transmission devices. VANET uses vehicle communications to transmit sensitive information. Intruders or malicious actors may try to follow or steal information from vehicle communication. As a result, it becomes extremely important to consider the integrity of automotive the secrecy through anonymized authentication. Identifiers are essential in VANETs for maintaining secrecy and deterring unauthorized vehicle observation. There are many different ideas about how to switch pseudonyms. These approaches, the centralized authority for administering various aliases (broadcast, annulment, and changing), summarize the authors' main strategies for ensuring anonymity in VANET [2]. The author of [3] proposes the decentralized management of false identities using blind signatures in VANET. The majority of the services and activities available

to VANET subscribers are oriented around enhancing driving safety, news and entertainment, and routing [4]. Safety information (vehicle and curve speed warning) and non-safety information (comfort application) are the two categories of information that are sent in the VANET [5].Informational pamphlets alert drivers to potential dangers to permit a quick response, but they are configured to have a greater priority in VANET than non-safety signals. Although VANET has benefits, it also has disadvantages, particularly concerning subscriber privacy and the security of transmitted data [5]. Vehicles entering and exiting highways need safety awareness indications, including commuter traffic and wet roads, to select which routes to take to reach their intended destination.The suggested CFRS-CP technique is used to evaluate the likelihood of congestion at each node based on the network quality, MAC overheadneighbor density, and vehicle velocity. The projected likelihood of congestion is then used to evaluate the route[6]. Long delays or even tragedies may result when rogue nodes improperly modify protective notifications before sending them to the requestor, whether deliberately or accidentally. Pseudonyms and anonymized verification [7] are two techniques for protecting privacy that has been developed by a number of researchers. As long as they aren't used to identify the user, they can be used to protect security and privacy. Vehicles do not change their pseudonyms when transmitting information, however, this makes these systems less secure because unreported traffic data can be used to identify user pseudonyms [8].Although technologies that may establish secure lines of communication vs various threats are available, consensus mechanisms and data confidentiality for vehicles remain unresolved difficulties for VANETs [8,9]. To lessen or completely prevent intrusion attempts, security, anonymity, and trustworthiness [9] must be considered when developing a secured VANET.

1.1. Blockchain in VANETs

A decentralized peer-to-peer system called Blockchain [10] was initially developed to run the virtual money Bitcoin. In recent years, blockchain has started to offer additional services to a variety of applications, including those in financial services, medical services, supply chains, the Industrial IoT, 5G networks, and Smart Cities [11]. The blockchain without the parent/root node is named the genesis block. Every block must contain the following previous hash value, timestamp, and nonce value mentioned in [10].

Figure 1 shows an example of transactions in a VANET network. A new block is created by a vehicle node and sent to the vehicle network. Other vehicle nodes try to solve the PoW problem, known as mining. A block became legitimate when the PoW was solved, and it will be included in the chain. Blockchain has so many unique features compared to recent technologies like distributed nature, immutability, security, privacy, and also transparency. From the above features, we are motivated to give a solution for routing mechanisms for VANET’s applications by incorporating blockchain concepts over VANETs.

1.2. Contributions of the Proposed Method

The primary significance of our research article is highlighted below :

a. To overcome the traditional VANET’s issues by applying the blockchain concepts to develop a blockchain-based secure trust system to identify and blacklist numerous black hole nodes from the network.
b. To create the processing logic for a VANET system's decentralized execution of transactional operations and trust rating accumulation.
c. To introduce the Blockchain-based Trust-LEACH protocol to perform the scalable routing mechanisms.

d. By using simulation, to show the findings on the effect of the developed blockchain-based trust model on network metrics in terms of computational time, throughput rate, delay, and packet loss ratio.

This remaining article is organized as follows:

Some related work is reviewed in Section 2. The designed methodology paradigm for the identification and eradication of internal attacks from the networks is described in Section 3. The experimental findings as well as some perspectives are described in Section 4. Results and Discussions are explained in section 5.

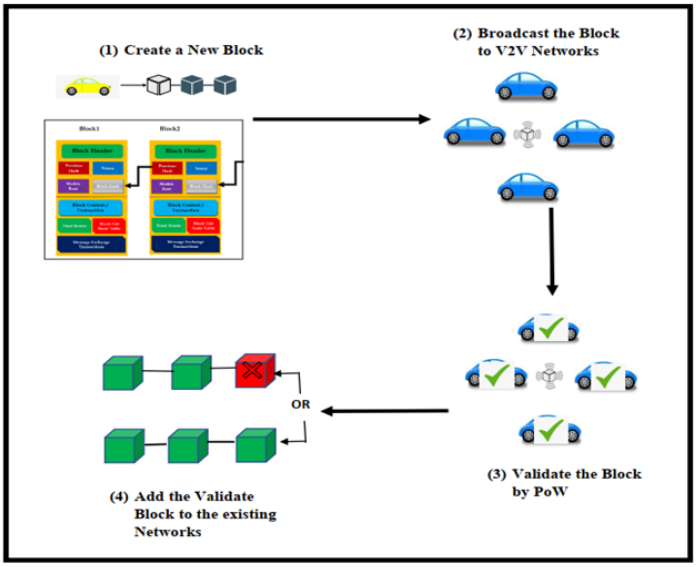


Figure 1. Example of Blockchain-based transaction in VANETs

2. RELATED WORKS

Ahmed et al [12], proposed a model that is put into practice and contrasted with the most recent VANET-based QoS and fault-tolerant approaches by a customized simulator. The outcome demonstrates the effectiveness of the suggested strategy which by utilizing the edge server SDN controller decreased the average message transmission time of both normal and urgent communications by 55%. Additionally, the suggested approach utilizes the edge server, cloud server,and blockchain architecture to decrease processing time, possible threats, and as well as communication loss ratio.

In addition, Zhang et al [13], introduced an adaptable threshold multi-signature methodology. It necessitates numerous users to jointly verify the message's legitimacy, much like crowdfunding. The effectiveness of secure communication is increased by aggregate cryptographic signatures. TCoin, a trustworthiness instrument, is designed to pique reporters' interest in taking part in transportation engineering. The outcomes of the security evaluation and simulation demonstrate how secure and successful our plan is in the smart transportation system.

Li et al [14], suggested an innovative local trust management mechanism called ATM. Active recognition and blockchain algorithms are used by ATMs. In particular, the blockchain assures the reliability of trustworthiness data between different locations, while the active detecting

efficiently eliminates the nearby bad nodes and prohibits their effective involvement. They undertake mathematical solutions to assess the effectiveness of ATMs. According to the findings of our experiment, ATM outperforms the other two tested trust methods. From the perspective of a 95% accuracy rate and 90% delivery proportion, it can successfully detect malicious behaviors. A blockchain-based methodology is presented to resolve security threats, particularly to assure safe crisis message delivery. One blockchain will be used to maintain the vehicle's identification information and the other will be used to maintain and disseminate blockchain applications. According to experimental investigation, the suggested blockchain-based procedures outperform the current ones in a few measures by Moustafa et al [15].

Son et al [16], proposed methods to maximize bandwidth utilization. They also do a thorough evaluation of the suggested protocol using Burrows-Abadi-Needham (BAN) logic, a Real-Or-Random (ROR) arbitrary architecture, and a demonstration using the Automatic Validation of Internet Security Methods and Applications (AVISPA). To make sure that the proposed communication is feasible, they simulated it using network simulator 3 (NS-3). They compare the computational overhead and privacy features of the proposed communication with those of earlier approaches to show that the suggested approach is more efficient and secure than those used previously. The decentralized blockchain architecture guarantees the benefit of data integrity to the agreement between two parties. Additionally, they tested its network communication using the SUMO and NS-3 emulators. According to the findings of their simulations, BPSDQS's authorization latency is shorter compared to the currently used blockchain-based proxy re-encryption (PRE) technique. The simulated results also revealed that their plan can save up to 98% on the typical authorization latency [17].

Usha Rani et al [18], a VANET concept that emphasizes high-quality video transmission while utilizing data exchange among vehicles is given in the study. Eliminate multi-hop route discovery, which is accomplished by employing the best router in each ring, which is centered on the total number of cars accessible in the system. Blockchain is used to validate warning messages, improving the integrity of confidential documents. Also, an evaluation of the network applications such as AODV, OLSR, and DSDV is provided.

Wang et al [19], suggested a simple, blockchain-based secure routing mechanism in their research. They make use of the ultra-light Blockchain to improve the routing reliability of the 5G NR-based swarm UAS networks. In comparison to traditional clustering algorithms, the suggested method with compact Blockchain can identify harmful UASs, prevent dangerous UAS assaults, and eliminate fraudulent links from hackers. A huge implementation of swarming UAS networking is simultaneously extended by the suggested algorithm, which is swarm UAS orientated. They have assessed each UAS's traffic condition in swarm UAS networks, create confirmation for swarm UAS connectivity with Proof-of-Traffic (PoT), and proactively synchronize the modified blocks for lighter Blockchain within the bounds of energy utilization. The evaluation demonstrates that PoT can lower bandwidth utilization in the procedures of reaching a consensus and synchronizing modules.

Feng et al [20] offered an asynchronously accumulator-based Efficient Privacy-Preserving Authentication Model (EPAM) that enhances the working prototype. The time-consuming process of verifying the Certificate Revocation List is avoided by asynchronous aggregation, which provides effective member authentication (CRL). Importantly, they achieve confidentiality aspects like secrecy and confidentiality of information by creating a mutual authentication system while taking the semi-trust RSUs into account. The simulations demonstrate that in the EPAM experiment over 107 credentials, the validation time is around 0.157 milliseconds, reducing the authentication delay in VANETs.

Youssef et al [21], proposed a smart contract-based approach as a dependable and relatively secure solution to address OLSR security threats by incentivizing (rewarding) vehicle cooperation and eliminating redundant detection procedures. The simulation demonstrates how effective their technology is for use in contexts with constrained resources, such as VANET. As the detection method becomes more effective due to the removal of malicious users, the limited timeframe and complexity are decreased.

To solve the security and privacy concerns in VANETs, different security techniques have been put forth by different scientists. This section outlines a few of the previous strategies that addressed related VANET issues using methods related to the suggested remedy. Ying introduced the anonymized and compact smart card (ASC) enrolment technique to handle privacy-preserving issues including the authenticity of members and communications sent over the system [22]. Regarding communication and processing overhead cost, end-to-end latency, and average packet drop, VanetMobiSim was used to assess ASC's efficiency. The simulation revealed that ASC outperformed other baseline methods and had higher efficiency. However, a significant disadvantage of ASC is that it increases network computational costs by often updating login identification and user passwords.

One-way hashing mechanisms and bitwise exceptional OR (XOR) procedures are used in the decentralized lightweight authorization and key agreement protocol (LAKAP) that Wazid introduced for VANETs [23]. The presented lightweight protocol stands out for a few aspects, including the capacity to dynamically add new roadside units to the system after initialization, the provision of RSU-to-RSU requirements, as well as other capabilities like anonymity and intractability. In addition, the solution demonstrates three methods for establishing authorization: between cars, between a vehicle and its corresponding cluster-head (CHs), as well as between CHs and their RSUs. Using Ns2 Simulator 2.35 (NS-2.35) on a desktop with an Intel Xeon E5-1620 v2 processor and 16 GB of RAM offered by the University Malaysia Sarawak, the effectiveness of the proposed method was evaluated in terms of networks and computational overheads, bandwidth, network delay, and packet delivery rate (PDR).According to the investigation, there aren't many expenses associated with transmission and processing when using the lightweight authentication and key agreement technique.

Rajput presented a hybrid technique for a privacy-preserving authentication mechanism (HEPPA), which blends conditioned anonymously with elements of pseudonym-based and shared signature-based techniques [24]. The genuine identification of an adversary may be discovered during the monitoring of harmful activities, claim the scientists. With this hybrid strategy, conditional privacy is provided through a straightforward, lightweight identity. A trapdoor technique offered by the pseudonym enables the identification of rogue networks and the consequent expulsion of such clients from the networks. For inter-vehicle connectivity, Tangade developed an efficient, customizable, and secrecy authentication (ESPA) framework using a hybrid cryptography methodology [25]. Stage I: V2I pre-authentication; Stage II: V2V authorization makes up the two phases of ESPA. Following offline registrations of cars and RSUs, every vehicle's beacon signal is pre-authenticated by the RSU throughout the transmission of data to determine whether it is an authorized vehicle or corresponds to one of the network's access points.

An intrusion detection system (IDS) based smart black hole attack monitoring system for VANETs was established by the authors in [26]. It also can recognize new attacks (blackhole attack variations). It takes longer and uses more computational power. The authors of [27] suggested combining trust tables with an opportunistic geospatial routing protocol to incorporate a durability measure for vehicle nodes. Unfortunately, their methodology is limited to low-density networks with straight-line travel for the car.

Perumal et al [31], introduced the blockchain-based communication architecture for completing the VANET-based clusters. Here, they have analyzed the latency, and packet delivery ratio, using the rainfall optimization approach. The proposed method is analyzed against different security attacks. The suggested MCRP-BWSN method seeks to derive from a heterogeneous network and use a shared memory subsystem and blockchain approach to identify the best routes to the endpoint [32].

Asmaa M.Morsi [33] prominently introduces an effective and secure hybrid clustering network for WSNs-based trustworthy mobile node-based malicious node detection model (ESMCH). Using the ESMCH model, we can prevent attacks like the Man-in-the-Middle Attack and the Black Hole Attack that WSNs are still vulnerable to.

3. THE PROPOSED METHODOLOGY

3.1. Adversary Model

We believe the suggested paradigm is vulnerable to both internal and external opponents, which could substantially harm how the commute program is designed to operate. In this article, specialized hostile opponents include both foreign adversaries who breach network components and domestic hostile vehicle nodes. In this example, these attacks can be intended to reduce the dependability of the ride-sharing service. However, considering that there are N total system components, we estimate that a sizable portion of the car nodes is secure and reliable. Additionally, due to the model's regular dependability checks, the compromised motorized vehicles node cannot be controlled by enemies for a very long time. Due to this characteristic, it is believed that an attacker could only target a small number of vehicles in a short length of time.

a. External Attacks:Even if we assumed that the majority is trustworthy, there is still a risk that some of them may be unscrupulous. Out of N total nodes, prospective miner vehicular nodes are legitimate but suspicious and could also be susceptible to being physically penetrated by adversaries and being opportunities for harmful miners. Such an adversary has control over many vehicle network nodes and can compromise the Nsc final consensus gathering in our scenario. The proposed method's quality of service may be endangered by exploited miner nodes, which can change or remove activities that should be included in the block.

b. Attacks that defame or antagonize others: This model is designed to detect attacks that defame or lambast others, which indicates that it might produce a fraudulent trust score for the authentic vehicle and publish the transactions to the decentralized system.

c. Tampering Blocklist Node Table: Dangerous nodes in the network may attempt to add, delete, or edit the prohibited neighbor’s table to compromise the device's trustworthiness.

d. RSUs will act as an Intruder: During the verification process, it's possible that a few of the RSUs will act fraudulently or will be in the hands of outside adversaries that want to harm the networks.

We create our model on the hypothesis that there are around 25% of hostile devices in the system and we construct countermeasures against the blackhole assault, even if we believe that the perpetrators do not manage each of the nodes in the system that is responsible for the eclipse attempt [24].

3.2. Design Goals

In a VANET system based on the stated adversary model, our goal is to establish a tamper-proof database of trust scores and banned nodes. This system must adhere to the following critical criteria to be successful and economical.

a. The proposed methodology should be (1) transparency so that each of the device's authorized users may acquire the same irreversible data, (2) adaptable to handle a very wide variety of nearby vehicles that connect to the network, (3) impervious to manipulation, ensuring the confidentiality of the node's databases and trustworthiness scores that are recorded and (4) Capable of providing tamper-proof information through auditing.

b. The proposed framework ought to be immune to single points of failure (SPOF). Decentralization must therefore be incorporated into our architecture to prevent a single body from being responsible for the entire ecosystem.

c. The proposed system's preparation and implementation speeds ought to be the equivalent of a few milliseconds to ensure that each transaction can be handled quickly, and an upgraded trust score can be released to the public to the integrated structure. As a result, the routing delay in VANETs must be reduced.

d. A very important design criterion is that the proposed system's file storage costs must be within an acceptable level.

3.3. System Model

The proposed system has the following entity to do the set of operations securely as clearly shown in Figure 2.

3.3.1. Registration Authority (RA)

RA is necessary during the registration system and first verification. The RA oversees performing the operations on the private verification chain. When a car integrates into the network for the very first time, the interactions contain the data needed for automobile verification. The other RSUs are permitted to examine and verify the validity of a new vehicle using the authenticating blockchain. Except for the introductory period and validation, vehicles don't need to get in touch with the RA. By doing this, we lessen our reliance on the RA.

3.3.2. Roadside Unit (RSU)

RSUs often have a lot of computational, storage, infrastructure and resources, and therefore are immovable. RSU receives communications from neighboring vehicles, analyses the reliability of these communications improves the trust ratings of the automobiles, and broadcasts traffic events to the neighborhood. Along with this, RSU plays an important role to monitor and manage the trust values of all the vehicles. All RSUs collaborate to develop a unified ledger and complete consensus duties. As a result, the evaluation and update of trust are fully transmitted across the RSUs. As a result, there is no longer any reliance on a centralized system like the RA.

3.3.3. Vehicles

An OBU, a computerized gadget with seamless connectivity, is a part of every vehicle. Here, OBU plays an important role to create a connection between vehicles and RSUs. Vehicles have

less storage, computation, and network connectivity than RSUs do. The closest RSU receives related data from moving vehicles.

3.3.4. Vehicular Block Chain (VBC)

The essential component of our suggested system is the consortium decentralized system [Consortium Blockchain]. The networks that take part in the consensus on a decentralized network are pre-authorized and they decide how each block is generated. RSU is a pre-authorized component in this architecture. The ability to add data to the blockchain and take part in consensus is conferred to RSU. Here, we consider a lightweight vehicle node that may access the data replicated on the RSU. The RSU's local storage oversees gathering information shared through other RSUs in addition to data contributed by V2V communication. The issue of mutual understanding between both the system's components is resolved by the consensus algorithm.

i. Blocks: A block is composed of a block header and a block body.The Block header information includes the hash, timestamp, and Merkle root of operations from the preceding block. A collection of trust score notifications that function as transactions published by mobile nodes makes up the block contents. In addition, the body also maintains a table of banned nodes and consolidated trust rankings.

ii.Transactions (Tx): Records of messages sent, services used, etc. may be a component of each operation in a blockchain-based VANET. In our architecture, a transaction is defined as the transferring to the closest RSU, which is around 1000 meters away, of the trustworthiness ratings of nearby vehicles.

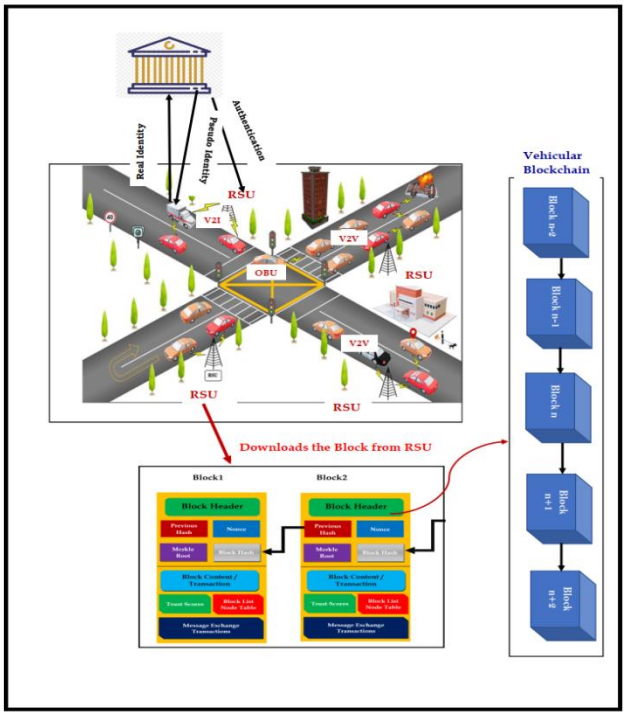


Figure 2. Consortium Blockchain-based VANET Architecture

Table1.Notations Used in the Proposed Method

Symbols	Meaning
V_i	Vehicle*i*
PK_{V_i}	PublicKeyofV*i*
SK_{V_i}	Private/SecretKeyofV*i*
$Cert_{V_i}$	CertificateofV*i*
$Cert_{BC}$	Blockchain Certificate
ID_{Vi}	IdentityofV*i*
Msg_{Vi}	Message*i* fromVehicle V
$Trust_{BC}$	TrustedBlockchain
Mes_{BC}	Message/input valueBlockchain
Di	Shortest Distance
X_i	Trust Score

4. PROPOSED SYSTEM METHODOLOGY

In this subsection, we describe the process of general modeling and simulation of our conceptual framework as shown in Figure 3.

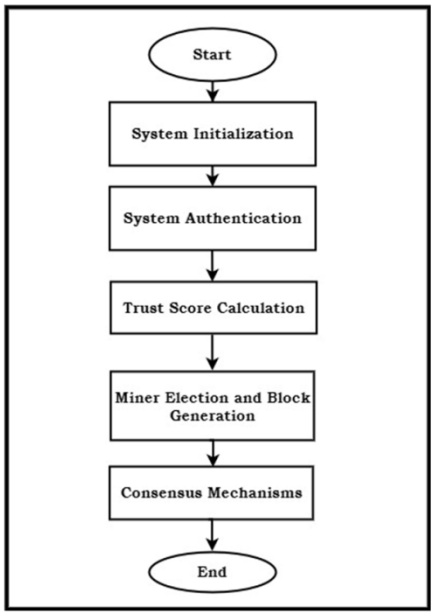


Figure 3. Process Flow of the Proposed Method

4.1. Initializing the System

When vehicle and passenger nodes join the blockchain network for the first time, the RA receives information about their names, addresses, Electronic License Plate (ELP) numbers for cars,

Personal Identity Numbers for people, and other necessary identification details. The key generation unit of RA uses the Elliptic-Curve Diffie-Hellman (ECDH) key setup technique to produce a public-private pair of keys and assign a pseudo identification, ID_{Vi} for vehicle nodes V_i and ID_{Pi} for passenger units Pi. The RSU generates a mapping list for each V_i, including ID_{Vi}, PK_{Vi}, SK_{Vi}, and RC_{Vi}. The identifying vector of the Vi is formed each time the vehicle re-joins the network, progressively raising the renewal count RCvi. Following the verification and acceptance of the PK_{Vi}, V_i enters step 2 of system authentication, as shown in Figure 4.

4.2. Authentication

The suggested method's next step is authentication between the networks of the vehicles so that they can share data with one another. When Vehicle A (V_A) wants to communicate with Vehicle B (V_B) on the same network to authenticate its identification, V_B will receive a $Cert_A$ from V_A as the first step in this process. To ensure that the $Cert_A$ provided at the delivery time and duration is still valid, V_B receives the certification from V_A. The certificate would include signatures, V_A's public key, and the expiration dates for $Cert_A$. Prior to verifying V_A's authenticity, V_B checks that $Cert_A$ has expired. The existence of $Cert_A$ in the blockchain certificate and whether it has expired are the two limitations that need to be checked. If both conditions are met, the public key is either valid or invalid. Using ID_{VB}, which is V_B's special identification number, RSU first confirms his authenticity. RSU ascertains the validity of the ID_{VB} after acquiring V_A's trust value through $Trust_{BC}$ and delivering it to V_B. Even if the ID_{VB} turns out to be false, the V_B is still denied. As shown in Figure 4, after determining the trust value, V_B will get in touch with V_A to get more details before proceeding to the third section.

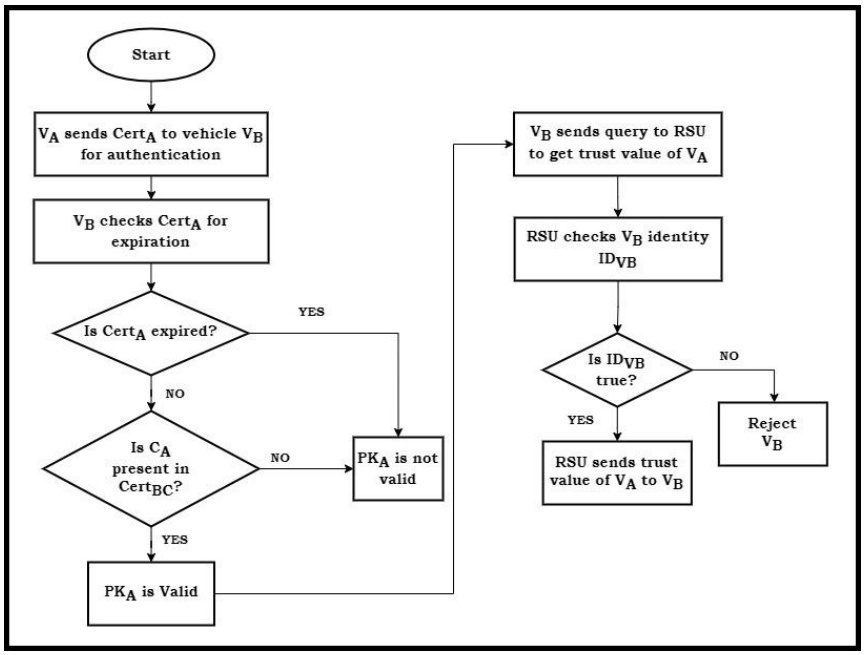


Figure 4. Authentication Mechanism for the Proposed Method

4.3. Calculation of Trust Score

The next stage of the proposed method begins when the RSU receives Mes_{BC} from the V_B. The trust value of each vehicle in the network is determined at this step. After receiving it, the RSU first checks to see if Mes_{BC} has been updated since the previous uploads. If Mes_{BC} is left

undisturbed, the trust value of V_A does not change. RSU, on the other hand, starts figuring out the trust offset for V_A if Mes_{BC} is upgraded. If V_B and V_A had communication, the amended V_A rating is given to RSU. The trust value in $Trust_{BC}$ is changed by RSU. Algorithm 1 displays the trust value computation for the suggested approach.

Algorithm1Calculation of Trust Score

Require:W_i:Updated ratingofV_i;X'_i:currenttrustvalueofV_i;
Ensure:X_i:Updatedtrust value of V_i
1: **if**(i=0)**then**
2: $X_i \leftarrow X'_i + 0$ **else**
foreachV_i**do**
3: **get**W_i
4: $X_i \leftarrow X'_i$
5: **endfor**

4.4. Block Generation & Mining Process

Block generation and mining process are the following steps in the proposed approach. Although it is the simplest operation, it is crucial to the success of the suggested strategy since it incorporates distributed ledger into the system. Moving on to the next RSU in the system requires repeating the process of selecting a miner RSU. Once elected as a miner RSU, the miner publishes its block into the blockchain. Due to distributed ledger technology's decentralized nature, a miner RSU is frequently elected to manage the system. Choosing a mining RSU ensures that data in the blockchain is updated on time.

4.5. Consensus Mechanism

Figure 5 illustrates how RSUs gather their longest blocks from the discarded parts and incorporate them into the distributed consensus when other portions are eliminated. By ensuring that every RSU in the network is utilizing the same blockchain, this approach ensures precision and consistency. The verifier networks in our architecture that create and distribute transactions using Practical Byzantine Fault Tolerance (PBFT) technology are called authorized RSUs. One of the RSUs is the main, or master node and the subordinate RSUs are chosen at random. The leader node of the car blockchain collects the transaction data supplied to it, generates a Merkle hash code for the records relevant to the previous block, and safely constructs a block. After a master creates a block, it is validated by the following nodes, and using the tyranny of the majority, all reliable nodes work to come to an agreement regarding the system.

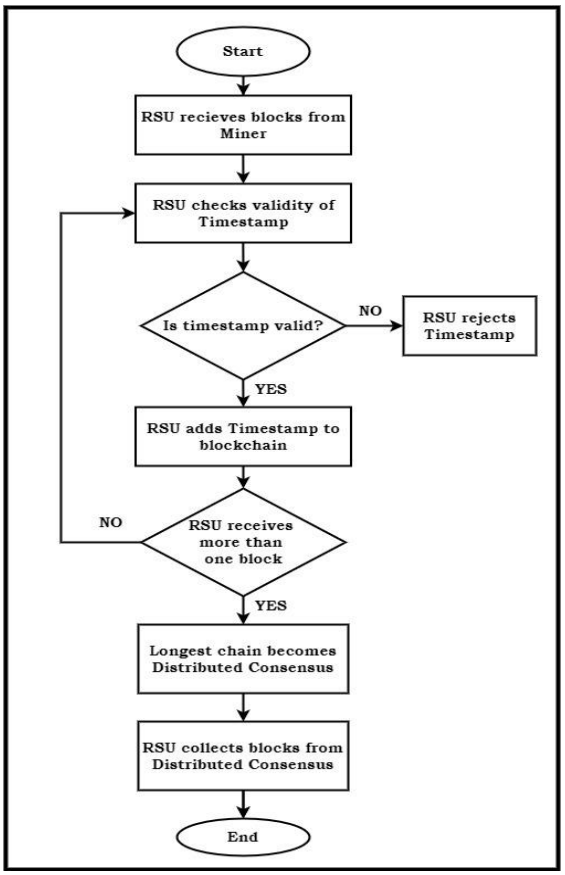


Figure 5. Proposed Consensus Mechanisms of the Proposed Method

4.6. Blockchain-based Trust-LEACH Protocol

With the help of the blockchain-based Trust-LEACH [34]protocol, the Cluster-Head (CH) of the suggested technique is chosen from the normal nodes. The shortest distance (Di) between base stations and a vehicle's trust score value are the two factors that determine how the cluster head is created (Xi). When a node satisfies both requirements, it is regarded as a CH; otherwise, the procedure will continue. The random function will be called for the selection of CHs if more than one node satisfies the requirements, as described in Algorithm 2.

Algorithm2 Trust Based Cluster Head Selection

Require:n_i:nodes ofV_i;*Base Station:* BS_i
Ensure: Cluster Head (CH)
a) *Choose a shortest distance (*D_i*) from* BS_i
b) *Trust value of node* X_i
1: **for**(*i:1 to*n_i)**do**
2: **if***CH = (MAX(*X_i*) && MIN(*D_i*))* **then**
3: *Select CH*
4: **endif**
5: Choose next node
6: **endfor**

4.7. Blacklist Node List

Each RSU updates its local network with the most recent transaction to represent the most transaction history. All vehicle nodes in the local system amended the new forbidden node list as well as the maximum DSN registered. Senders who are waiting for their messages to be delivered conjecture that the intermediate node sending the Response message might be forbidden. A fresh response is sent if so. Otherwise, as indicated in Algorithm 3, the found root is utilized to transmit the lead more effectively.

Algorithm3 Block Node List Identification

Require:n_i:nodes ofV_i;$Average_{Wi}$:Average rating value after registration
Ensure: AN_i:Active Node List of V_i
1: **for**($n_i \in N_i$)**do**
2: **if**$Average_{Wi} \leq Threshold$ **then**
3: $N_i.remove(n_i)$
4: **endif**
5: **endfor**
5: **return** N_i

4.8. Typical Scenario of the Proposed Method

The suggested method is used in various traffic situations, such as the use of traffic warning structures, the tracking of stolen vehicles, the tracking of known and unidentified offenders, and the detection and management of accidents. Figure 6 depicts the use case scenarios for employing blockchain technology to detect accidents and stolen cars.

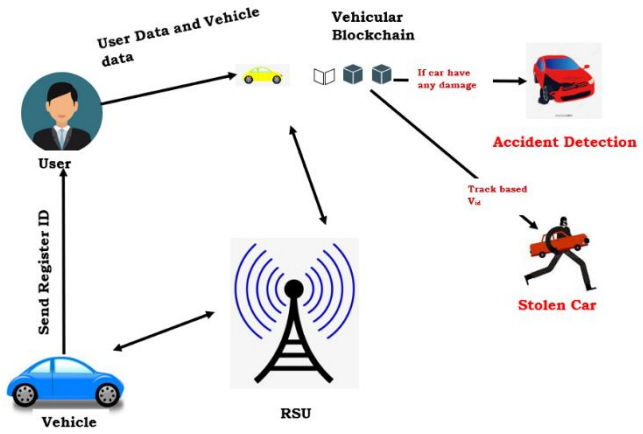


Figure 6. Accident detection and Stolen car scenario

5. RESULTS AND DISCUSSIONS

5.1. Simulation Settings

5.1.1. Simulation Setup for VANET

We use the NS-3 simulation program deployed on Virtualized Linux OS using Ubuntu 16.04 version containing 12 GB RAM to analyze the effects of insider threats and risks and analyze the system performance using the suggested blockchain-based trust score methodology in VANET.

We employed OpenStreetMaps (OSM) [28], which offers free customizable maps around the world, in our research to simulate real-time streets, intersections, and traffic signals. When creating convincing street architecture, OSM considers structures, traffic signals, two-way and four-way roads, and other factors. We employ the Simulations of Urban Movement platform (SUMO) [29] version 1.23 for vehicle movement. We also change the sources and destinations for various nodes such as 2 for 20, 3 for 40 & 60, 4 for 80 as well as 100 for total nodes. During the experiment, these networks delivered and acquired packets of data. The experiment was conducted was last 180 seconds (3 mins).

5.1.2. Simulation Setup for Blockchain

For enhancing the security of the proposed method, we have used blockchain-based trust management implemented using a laptop with a 2.3 GHz Intel Core i5 and 8 GB of RAM by JAVA. For aggregating trust scores, our model blockchain approach includes V2I communications to collect information on trust ratings from moving nodes. We believe that a minimum of 20% of the network's maximal effectiveness should serve as verification nodes within a network with N nodes. As a result, we run each test on 25 nodes in the network or RSUs. The consolidated trust values for each station are determined using a variety of techniques, and they are distributed throughout the blockchain network together with a list of nodes that have been prohibited.

5.2. Performance Evaluation

We primarily focus on the following analysis with some existing methods such as computational cost, time to create a block using consensus mechanisms, and protection from insider attack.

5.2.1. Computational Cost Analysis

In this research, we have used the information created by the NS-3 tool as a feed to the blockchain model-based trusted environment. Data on trust scores produced as an analysis to test was utilized to log events in the transactional group. This information was processed depending on the initialization of the mining process in our proposed method, and the computation time fordifferent-sized data streams was analyzed by varying the number of nodes in the NS-3 tool as well as calculating the size of the trust score stored in the transactions is shown in Figure 7. The proposed method needs 497KB of storage for 100 vehicle nodes. Figure 8 shows that the computational time for validation of the trust score, in the proposed methods takes only 0.576 secs.

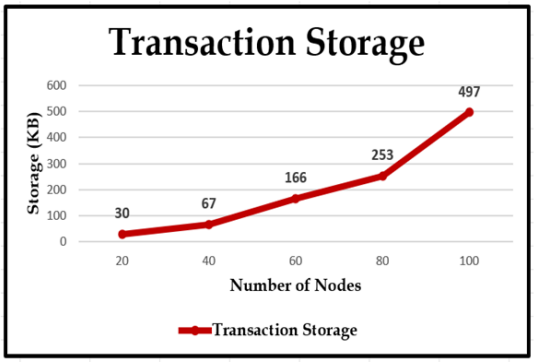


Figure 7. Transaction Storage Analysis

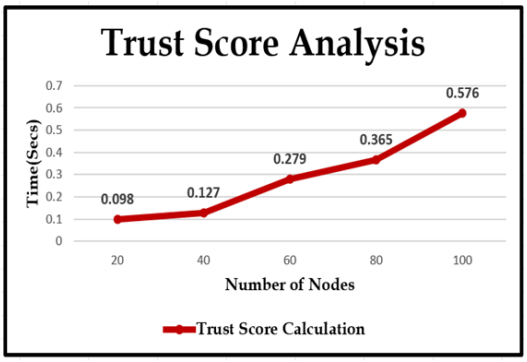
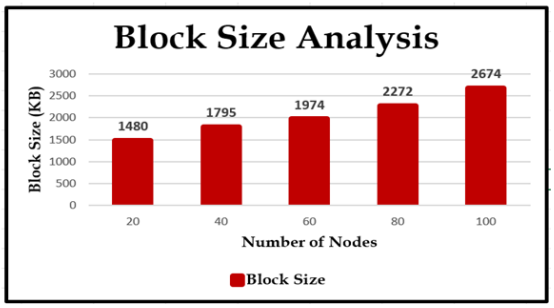


Figure 8. Trust Score Analysis

5.2.2. Computational time for Block Creation

In this research, we measure the presented model's performance in terms of how much time it takes to create a block with a prohibited node list and obtain PBFT consensus amongst verifiers on the status of operations. In this test, 25 validation nodes are used to process various blocks size shown in Figure9. The time needed to establish consensus and the overall amount of time needed to create each block is shown in Figure 10. It takes 7.942 seconds to construct a new block based on 25 verifiers by varying the number of nodes in the vehicle nodes.



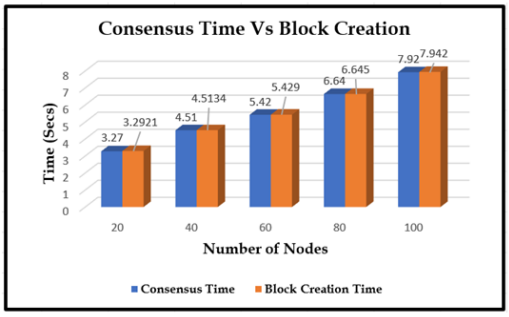
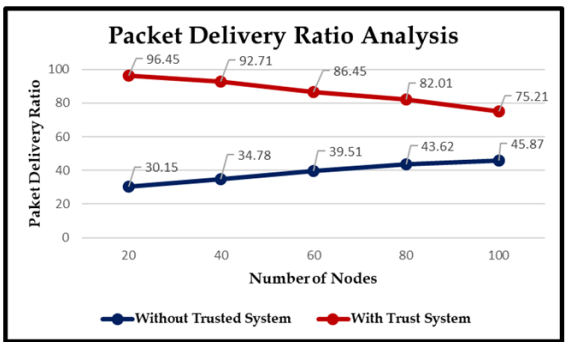


Figure 9. Block Size Analysis

Figure 10. Consensus Time vs Block Creation Analysis

5.2.3. Performance of Network Analysis

We executed the simulations frequently utilizing the same architecture, infiltrating 30% faulty nodes, to examine whether the efficiency might be optimized by including the developed framework. We first tested it using the conventional Routing protocol, and afterward, we tested the alternative AODV using a blockchain security framework. It should be noted that all these attacker nodes may be a solitary black hole attack station that drops messages or several nodes constructing tunneling that ingest the internet traffic. Without trust and with a 30% attacker node present in the first scenario, it is evident that perhaps the bandwidth utilization in bits per second and packets throughput significantly decreased, as depicted in Figure 11. From Figures 11 and 12, we can be concluded that integrating the suggested model into the VANET system will result in a large decrease in the packet delivery ratio and an increase in performance in bits per second.



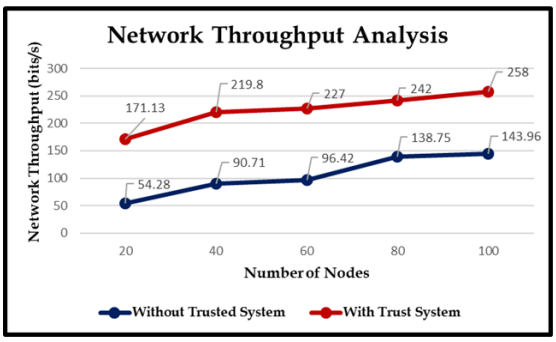


Figure 11. Packet Delivery Analysis

Figure 12. Network Throughput Analysis

Figure 13 shows that both strategies' initial network throughput is 0. The cause is that, at initial rounds, no data packet is transmitted. Due to the high volume of packets sent during these rounds, it keeps rising with the number of rounds. Due to full network participation, Trust-LEACH gradually increases the amount of data transferred from regular nodes to BS. Because Trust-

LEACH is used to choose CHs, and because there are many active nodes, the throughput is at its highest. As the number of rounds reduces, the amount of data packets grows.

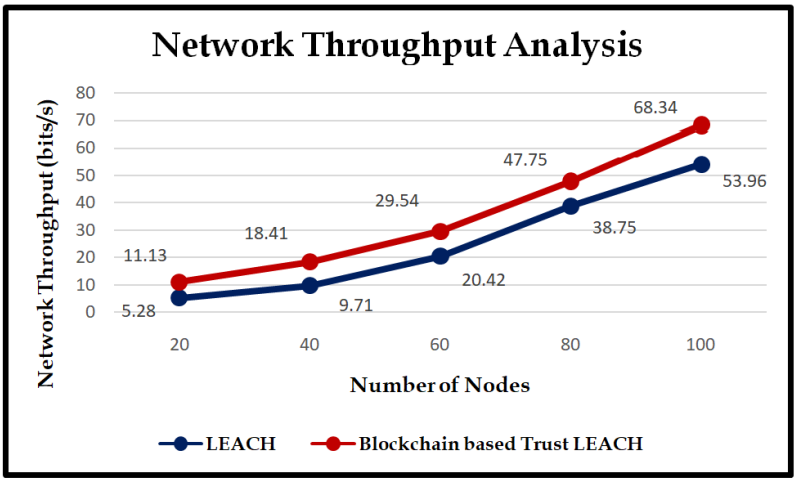


Figure 13. The Proposed Routing Method Network Throughput Analysis

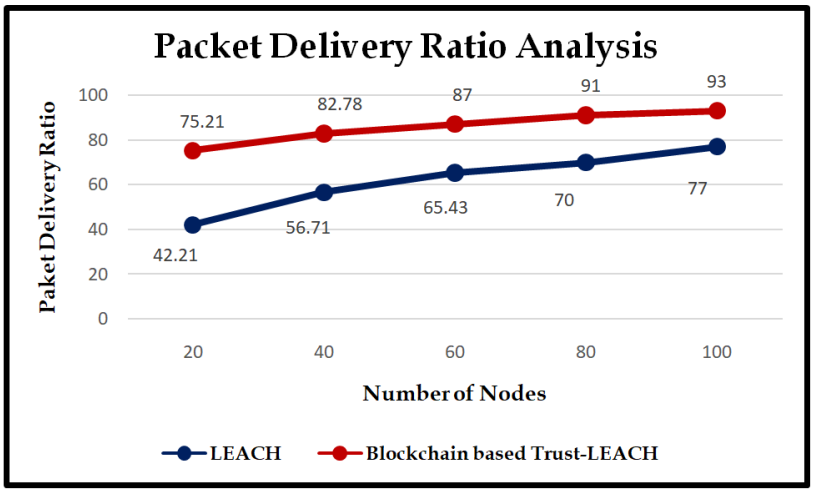


Figure 14. Comparison of packet delivery ratio with the existing LEACH protocol

The packet delivery ratio of the LEACH protocol is analyzed with our proposed blockchain-based trust-LEACH protocol as shown in Figure 14. For 20 nodes, the LEACH protocol can transfer 42KB per second, meanwhile, our proposed method transfers 75.21KB per second. This means that the proposed method has a high data transfer rate compared to the existing methods.

5.2.4. Security Analysis

To find fraudulent nodes throughout the network, a stringent security investigation is carried out. The authentication mechanism is used only to identify suspicious nodes. The Sybil and MITM attacks are tossed against the network to examine its flexibility. Additionally, the Oyente application [30] is used to analyze whether the sensitive information is safe or not, that is stored on the blockchain-based vehicular network. In the following sections, we are going to discuss the Man-in-the-Middle attack, against our proposed Trust-LEACH routing mechanisms.

5.2.5. MITM Attack Analysis

The MITM (Man In The Middle) assassination attempt, which disrupts the channel's ongoing conversions, is introduced into the blockchain-based Trust-LEACH mechanism. The authentication system of the networks is employed to safeguard the entire network from such kinds of assaults. Only nodes that have their identities recorded in the blockchain network are allowed to become participants in the vehicle network. Without authorization, they can't be eligible to communicate in the system, every node is validated at the time of registration itself. Figure 15 demonstrates how the hacker attempts to detect and tamper with the packets received during the conversation. In a MITM attack, the adversary carries out intrusion attempts by altering the packet header or delivering inaccurate info. Due to malicious activity, the actual packets are not transmitted whenever data are delivered from surrounding vehicles to CHs and BS respectively. The intruders repeatedly send malicious files in the direction of the destination node. The network's performance diminishes when intrusions are initiated since only fraudulent messages are delivered to the target point. The network performance is determined following the identification of intruders via simultaneous registrations and authorization. Whenever the system is clear of intruders, the system data transfer rate/throughput will increase tragically. The packet delivery ratio of the proposed method is analyzed against MITM attack nodes in Figure 16.

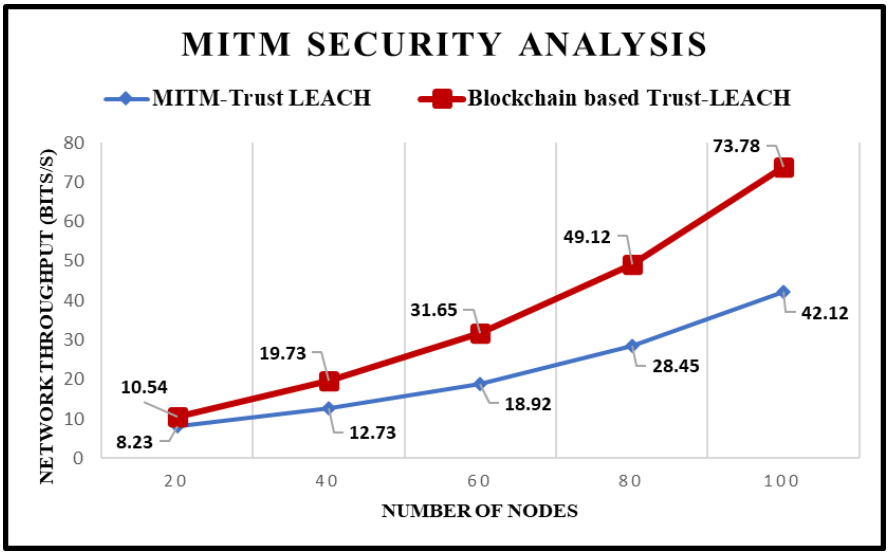


Figure 15. The Security Analysis Against MITM Attacks

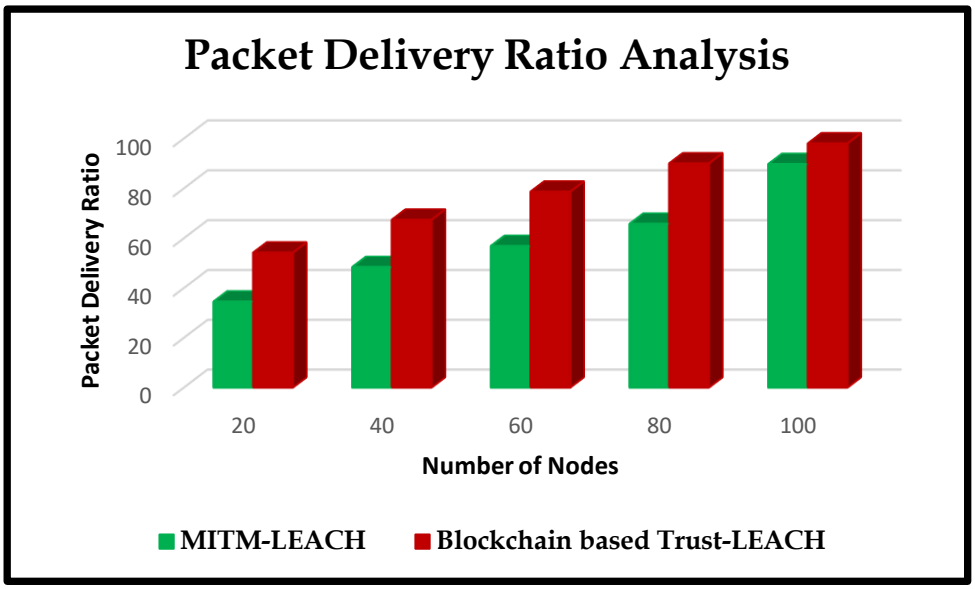


Figure 16. Packet Delivery Ratio Analysis vs MITM Attack

6. CONCLUSIONS

A blockchain-based Trusted LEACH protocol is used in this study's research to address insider threats on the VANET system. The vehicular nodes in this study outsource the extraction activity to the RSUs to speed up block production and make it compatible with the proposed VANET system. We use indiscriminate mode to assign a confidence level to nearby vehicular networks. Furthermore, we show how approved RSUs build up the threshold and examine how much block time is used for PBFT consensus. The results show that the inclusion of a blockchain-based VANET increased the network's throughput and packet transmission rate. It has been shown to be more effective for information propagation in the VANET by effectively removing the black hole attack nodes.

FUTURE SCOPE & LIMITATIONS

To enhance trust management, provide security against insider assaults and shorten the time needed to elect a blockchain node, a zero trust management, and deep learning approaches for VANET's secure data transmission utilizing the blockchain architecture may be developed in the future.

CONFLICTS OF INTEREST

The authors declare no conflict of interest.

REFERENCES

[1] Omar Dib, Kei-Leo Brousmiche, Antoine Durand, Eric Thea, Elyes BenHamida, Consortium blockchains: Overview, applications and challenges, Int. J. Adv. Telecommun. 11 (1&2) (2018).

[2] A.Boualouache,S.M.Senouci,andS.Moussaoui,"ASurveyonPseudonym Changing Strategies for Vehicular Ad-Hoc Networks," IEEECommunicationsSurveysandTutorials,vol.20,no.1,pp.770–790,2018

[3] D. Moussaoui, M. Feham, B. A. Bensaber, and B. Kadri, “Securing vehicular cloud networks,” International Journal of Electrical and Computer Engineering (IJECE), vol. 9, no. 5, pp. 4154–4162, 2019

[4] Bhoi,S.K.;Khillar,P.M.;Singh,M.;Sahoo,M.M.;Swain,R.R.Aroutingprotocolforurbanvehicularadhocnetworkstosupportnon-safetyapplications.*DigitalCommun.Networks***2018**,*4*,189–199.

[5] Azees,M.;Vijayakumar,P.;Deborah,L.J.Comprehensivesurveyonsecurityservicesinvehicularad-hocnetworks.*IETIntell.TransportSyst.***2016**,*10*,379–388

[6] Rashmi Patil and Dr. Rekha Patil: Cross Layer Based Congestion Free Route Selection in Vehicular Adhoc Networks.InternationalJournal of Computer Networks & Communications (IJCNC) Vol.14, No.4, July 2022

[7] Rabieh, K.; Mahmoud, M.M.E.A.; Guo, T.N.; Mohamed, M. Cross-layer scheme for detecting large-scalecolludingSybilattackinVANETs.InProceedingsofthe2015IEEEInternationalConferenceonCommunications,London,UK,8–12June2015.

[8] Zhang, Y.; Zheng, D.; Deng, R.H. Security and privacy in smart health: Efficient policy-hiding attribute-basedaccesscontrol.*IEEEInternetThingsJ.***2018**,*5*,2130–2145.

[9] Lu, Z.; Qu, G.; Li, Z. A survey on recent advances in vehicular network security, trust, and privacy. *IEEE Trans.Intell.Transp.Syst.***2019**,*20*,760–776

[10] P.Chinnasamy, P.Deepalakshmi, V. Praveena, K.Rajakumari, P.Hamsagayathri, (2019) “Blockchain Technology: A Step Towards Sustainable Development” International Journal of Innovative Technology and Exploring Engineering (IJITEE), Volume-9 Issue-2S2

[11] Chinnasamy, P., Vinothini, C., Arun Kumar, S., Allwyn Sundarraj, A., Annlin Jeba, S.V., Praveena, V. (2021). Blockchain Technology in Smart-Cities. In: Panda, S.K., Jena, A.K., Swain, S.K., Satapathy, S.C. (eds) Blockchain Technology: Applications and Challenges. Intelligent Systems Reference Library, vol 203. Springer, Cham. https://doi.org/10.1007/978-3-030-69395-4_11

[12] Ahmed, S. Abdullah, S. Iftikhar, I. Ahmad, S. Ajmal and Q. Hussain, "A Novel Blockchain Based Secured and QoS Aware IoT Vehicular Network in Edge Cloud Computing," in *IEEE Access*, vol. 10, pp. 77707-77722, 2022, doi: 10.1109/ACCESS.2022.3192111.

[13] Li Zhang & Jianbo Xu (2022) Blockchain-based anonymous authentication for traffic reporting in VANETs, Connection Science, 34:1, 1038-1065, DOI:10.1080/09540091.2022.2026888

[14] F. Li, Z. Guo, C. Zhang, W. Li and Y. Wang, "ATM: An Active-Detection Trust Mechanism for VANETs Based on Blockchain," in *IEEE Transactions on Vehicular Technology*, vol. 70, no. 5, pp. 4011-4021, May 2021, doi: 10.1109/TVT.2021.3050007.

[15] M. Ahmed *et al*., "A Blockchain-Based Emergency Message Transmission Protocol for Cooperative VANET," in *IEEE Transactions on Intelligent Transportation Systems*, doi: 10.1109/TITS.2021.3115245.

[16] S. Son, J. Lee, Y. Park, Y. Park and A. K. Das, "Design of Blockchain-Based Lightweight V2I Handover Authentication Protocol for VANET," in *IEEE Transactions on Network Science and Engineering*, vol. 9, no. 3, pp. 1346-1358, 1 May-June 2022, doi: 10.1109/TNSE.2022.3142287.

[17] L. -Y. Yeh, N. -X. Shen and R. -H. Hwang, "Blockchain-Based Privacy-Preserving and Sustainable Data Query Service Over 5G-VANETs," in *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 9, pp. 15909-15921, Sept. 2022, doi: 10.1109/TITS.2022.3146322.

[18] KR, U. R. Advanced Vehicular Ad-Hoc Network (VANET) technology using Blockchain. International Journal for Research in Applied Science and Engineering Technology, 10(6), 4873–4880. https://doi.org/10.22214/IJRASET.2022.45086

[19] Jian Wang, Yongxin Liu, Shuteng Niu, Houbing Song, Lightweight blockchain assisted secure routing of swarm UAS networking, Computer Communications, Volume 165, 2021, Pages 131-140, https://doi.org/10.1016/j.comcom.2020.11.008.

[20] Xia Feng, Qichen Shi, Qingqing Xie, Lu Liu, An Efficient Privacy-preserving Authentication Model based on blockchain for VANETs, Journal of Systems Architecture, Volume 117, 2021, 102158, https://doi.org/10.1016/j.sysarc.2021.102158.

[21] Youssef Inedjaren, Mohamed Maachaoui, Besma Zeddini, Jean-Pierre Barbot, Blockchain-based distributed management system for trust in VANET, Vehicular Communications, Volume 30, 2021, 100350, https://doi.org/10.1016/j.vehcom.2021.100350.

[22] Ying, B.; Nayak, A. Anonymous and lightweight authentication for secure vehicular networks. IEEE Trans. Veh. Technol. 2017, 66, 10626–10636

[23] Wazid, M.; Das, A.K.; Kumar, N.; Odelu, V.; Reddy, A.G.; Park, K.; Park, Y. Design of lightweight authentication and key agreement protocol for vehicular ad hoc networks. IEEE Access 2017, 5, 14966–14980

[24] Rajput, U.; Abbas, F.; Eun, H.; Oh, H. A hybrid approach for efficient privacy-preserving authentication in VANET. IEEE Access 2017, 5, 12014–12030

[25] Tangade, S.; Manvi, S.S. Scalable and privacy-preserving authentication protocol for secure vehicular communications. In Proceedings of the 2016 IEEE International Conference on Advanced Networks and Telecommunications Systems, Bangalore, India, 6–9 November 2016

[26] Khattab M Ali Alheeti, Anna Gruebler, Klaus D McDonald-Maier, An intru-sion detection system against black hole attacks on the communicationnetwork of self-driving cars, in: 2015 Sixth International Conference onEmerging Security Technologies (EST), IEEE, 2015, pp. 86–91.

[27] Hanin Almutairi, Samia Chelloug, Hanan Alqarni, Raghda Aljaber, Alyah Alshehri, Dima Alotaish, A new black hole detection scheme for VANETs, in: Proceedings of the 6th International Conference on Management of Emergent Digital EcoSystems, 2014, pp. 133–138.

[28] http://www.openstreetmap.org last accessed on 19.09.2022.

[29] Michael Behrisch, Laura Bieker, Jakob Erdmann, Daniel Krajzewicz, SUMO–Simulation of urban mobility: an overview, in: Proceedings of SIMUL 2011,the Third International Conference on Advances in System Simulation,ThinkMind, 2011.

[30] https://oyente.tech/ last accessed on 27.09.2022.

[31] Joshi GP, Perumal E, Shankar K, Tariq U, Ahmad T, Ibrahim A. Toward Blockchain-Enabled Privacy-Preserving Data Transmission in Cluster-Based Vehicular Networks. *Electronics*. 2020; 9(9):1358. https://doi.org/10.3390/electronics9091358

[32] R. Bhavadharini and S. Karthik, "Blockchain enabled metaheuristic cluster based routing model for wireless networks," Computer Systems Science and Engineering, vol. 44, no.2, pp. 1233–1250, 2023.

[33] Asmaa M.Morsi,, Tamer M. Barakat and Ahmed Ali Nashaat : An Efficient and Secure Malicious Node Detection Model For Wireless Sensor Networks.InternationalJournal of Computer Networks & Communications (IJCNC) Vol.12, No.1, January 2020

[34] Hariharasudhan, V., and P. Vetrivelan. "VANETs Based Traffic Signals Controlling With Enhanced Security Module (ESM) In Smart Cities." Indian Journal of Computer Science and Engineering (IJCSE) Vol. 13 No. 4 Jul-Aug 2022, DOI,10.21817/indjcse/2022/v13i4/221304129

AUTHORS

Hariharasudhan V received a bachelor's degree inElectronics and Instrumentation Engineering from Bharathiar University, Coimbatore, and a Master's degree at Embedded Systems and Technology from SRM University, Chennai. Currently, he is working as a Principal Engineering Manager in Johnson Controls, Pune. He has 23 years of rich experience in end-to-end product design & development of embedded system controls the automotive domain & Building Automation Technology. His research interests are Wireless sensor networking, VANETs mobility, Embedded Controls, Cloud computing, Data Science, and IoT.

Dr.Vetrivelan P completed a Bachelor of Engineering from the University of a Master, Chennai, and both Master of Engineering in Embedded Systems Technologies and a Doctor of Philosophy in Information and Communication Engineering from Anna University, Chennai. He is working as a Professor in the School of Electronics Engineering & Assistant Controller of Examinations (ACOE) at Vellore Institute of Technology (VIT), Chennai, India. He has 18.6 years of teaching experience altogether in CSE and ECE Departments in both private Engineering Colleges in Chennai and Private Engineering Universities in Chennai, respectively. His research interests include Wireless Networks, Adhoc and Sensor Networks, VANETs, Embedded Systems, and the Internet of Things (IoT) with Machine Learning.