Computer Systems
Science and Engineering

Tech Science Press

DOI: 10.32604/csse.2024.055128

ARTICLE

A Secure Blockchain-Based Vehicular Collision Avoidance Protocol: Detecting and Preventing Blackhole Attacks

Mosab Manaseer[1] **and Maram Bani Younes**[2,*]

[1]Software Engineering, Philadelphia University, Amman, 19392, Jordan

[2]Cybersecurity and Information Security, Philadelphia University, Amman, 19392, Jordan

*Corresponding Author: Maram Bani Younes. Email: mbani047@uottawa.ca

Received: 18 June 2024 Accepted: 05 October 2024 Published: 22 November 2024

ABSTRACT

This work aims to examine the vulnerabilities and threats in the applications of intelligent transport systems, especially collision avoidance protocols. It focuses on achieving the availability of network communication among traveling vehicles. Finally, it aims to find a secure solution to prevent blackhole attacks on vehicular network communications. The proposed solution relies on authenticating vehicles by joining a blockchain network. This technology provides identification information and receives cryptography keys. Moreover, the *ad hoc* on-demand distance vector (AODV) protocol is used for route discovery and ensuring reliable node communication. The system activates an adaptive mode for monitoring communications and continually adjusts trust scores based on packet delivery performance. From the experimental study, we can infer that the proposed protocol has successfully detected and prevented blackhole attacks for different numbers of simulated vehicles and at different traveling speeds. This reduces accident rates by 60% and increases the packet delivery ratio and the throughput of the connecting network by 40% and 20%, respectively. However, extra overheads in delay and memory are required to create and initialize the blockchain network.

KEYWORDS

Vehicular networks; blockchain; collision avoidance; protocol design; security mechanisms

1 Introduction

Vehicular *ad hoc* networks (VANETs) provide a platform that connects vehicles equipped with wireless transceivers to operate remotely and interact with infrastructure units on the road. This technology is closely related to the traffic department through direct short-range communication (DSRC). The development of VANETs has facilitated numerous applications to enhance traffic safety, efficiency, and infotainment. Among these applications, safety is the most essential, where several collision avoidance protocols have been developed to reduce and prevent accidents and hazardous scenarios. The direct communication links in VANETs connect vehicles equipped with wireless transceivers and infrastructure units. Vehicles can communicate directly with other vehicles within their transmission range (V2V) and with pedestrians, infrastructure, or any entity equipped with wireless transceivers (V2X). This connectivity helps maintain awareness of surrounding traffic and road conditions, thereby supporting the implementation of various safety, efficiency, and infotainment applications over the road network.

However, VANETs' reliance on wireless communication renders them vulnerable to numerous security threats. Ensuring the security and privacy of intelligent transportation systems poses significant technical challenges. Attacks on vehicular network communication links can threaten the safety of citizens, passengers, and vehicles, depending on the specific application in use. The CIA Triad—confidentiality, integrity, and availability—summarizes the general security goals. While cryptographic principles can address most of these requirements, ensuring availability often necessitates additional measures. In this study, we focus on enhancing the availability aspect of security within the vehicular network environment, particularly for collision avoidance protocols. Denial of Service (DoS) attacks include blackhole and jamming attacks that flood the connecting network [1]. In the VANET environment, the most frequent threats to vehicle-to-anything (V2X) connections are DoS and distributed DoS (DDoS) attacks [1]. They significantly overload the communication channels between the Road Side Units (RSUs) and On-Board Units (OBUs) with many unhandled requests, causing a network outage. These attacks have more serious consequences on collision avoidance protocols. They may increase injuries and threaten the safety conditions of drivers, passengers, and pedestrians.

In this work, the primary goal of the proposed protocol is to ensure a high packet delivery ratio, crucial for maintaining network reliability. DoS attacks can disrupt or overwhelm the network, leading to traffic congestion and degraded application performance. The primary aim of such attacks is to deny legitimate users access to network services and resources. To face these threats, we propose a secure protocol that addresses potential attacks on the availability of the VANETs. This protocol has utilized blockchain technology to secure the communications of VANETs and prevent DoS attacks. The proposed protocol has succeeded in increasing the security conditions over the road network for collision avoidance protocols. Thus, it leads to a decrease in the accident rate among traveling vehicles and an increase in the delivery ratio and the throughput metrics of the connecting network.

The remainder of this paper is organized as follows: Section 2 investigates previous studies that address and hand DoS attacks in VANETs. Section 3 presents the main components, connections, and applications of vehicular network technology. Section 4 elaborates on DoS attacks and provides a scenario within the vehicular network environment. Section 5 presents the secure protocol for detecting and preventing DoS attacks in vehicular networks, focusing on collision avoidance protocols. Section 6 evaluates the performance of the proposed protocol. Finally, Section 7 concludes the entire paper and suggests future research directions.

2 Related Work

In the literature, several techniques and mechanisms have been proposed to detect and prevent DoS attacks in VANETs [2–6]. Some previous studies have focused on detecting the attacks [2,3] while others provide solutions to avoid and prevent this type of attack [4–6]. Counting transmitted messages and traffic analysis are early and direct mechanisms that have been used to detect the Dos attacks. Dey et al. [2] have created an effective framework for detecting and localizing DoS attacks. This framework is developed mainly for Long Term Evolution (LTE)-based vehicular networks. The main consideration of this framework is the data packet counter values and average packet delivery ratio. Detecting any node (i.e., vehicle) that transmits a sizeable irresponsible number of packets and noticing a low percentage of packet delivery ratio indicates a DoS attack on the network. Dong et al. [3] have also developed a tracking control approach for network-based nonlinear Unbiased Minimum Variance estimators called UMV systems vulnerable to DoS attacks. The proposed detection approach is based on tracking outputs derived as linear matrix inequalities, after which the controllers are designed to withstand DoS attacks.

On the other hand, advanced technologies, such as Machine Learning (ML) and blockchain, have been used to detect DoS attacks [5,6]. Verma et al. [5] have utilized the BayesNet technique to test its effectiveness on various datasets (i.e., the CIC-DDoS-2019 and the simulation-based datasets). They analyze the results and validate their application for defending against new network security threats. The BayesNet algorithm has been used to identify the various types of DoS. The accuracy of detecting existing attacks is more significant than 90%. Moreover, Ayaz et al. [6] have examined the physical layer characteristics of a full-duplex non-orthogonal multiple access called (FD-NOMA)-based vehicular network. That is analyzing a blockchain-based vehicular network employing FDNOMA to verify block addition dependability. The proposed network's security and privacy are examined from the physical layer perspectives of Signal Interference and Noise Ratio (SINR) and secrecy rate. The success transmission percentage is assessed in the presence of jamming and eavesdropping attacks. This study has suggested combining blockchain technology and Physical Layer Security (CPLS) to guarantee security and privacy. Comparing PLS simulation results to a blockchain system without PLS reveals increased sound output. In the face of many eavesdroppers and interference nodes, they nonetheless achieve the minimum permitted data rate.

Furthermore, some research studies have considered the authentication mechanisms to prevent the DoS attack. When all vehicles on the network are authenticated and their behaviors are monitored, none is supposed to initiate a DoS attack. Sun et al. [4] proposed a mutual authentication framework with the DoS attack resistance mechanism (MADAR). This framework is divided into two categories: Vehicle to Road Side Unit (V2R) and Vehicle to Vehicle (V2V) authentications. It combines ID-based signatures and should register to real-time analytics (RTA) before applying the authentication. Ahmed et al. [7] analyzed various approaches to privacy and security issues. The DoS attacks were defeated using signature and commitment-based authentication. Besides, for obfuscation attacks, they recommended an efficient blowfish crypto-system to create safe routes in VANETs that change the transmission channel and use different frequency hopping technology.

Another recent study has considered the secure messages exchanged between vehicles. Shrestha et al. [8] introduced a blockchain system designed to augment security in VANETs. The study suggests a new method for preventing the dissemination of false data from malicious sources, which involves implementing a particular blockchain system in each country. This blockchain technology maintains a distributed ledger that records the integrity of nodes and messages. It enables a secure and dependable exchange of messages among vehicles. The primary achievement involves the creation of a resilient public blockchain designed explicitly for VANETs, which significantly enhances communication security and trust. The study presents a security solution for VANETs that utilizes blockchain technology. Its main goal is to detect the spread of false information by malicious vehicles. This system utilizes revolutionary blockchain technology tailored to a particular country and region. It is designed to record and verify the integrity of sender vehicles and transmitted packets, providing safe communication between vehicles. The primary achievement of the study is the creation of a specialized public blockchain designed for VANETs to improve communication security and trust. This strategy signifies a notable progression in secure vehicle communication, providing a dependable method for managing information in a scattered and possibly susceptible network environment.

Furthermore, Sachin et al. [9] presented a decentralized approach that calculates trust scores for vehicles in the environment of VANETs. The system has a two-tier detection mechanism to accurately identify and prevent vehicles that are deemed malicious, including those that engage in blackhole attacks. At the initial level, adjacent nodes independently compute trust; however, at the subsequent level, RSUs employ a blockchain framework to authenticate and consolidate these trust ratings. This study showcases the efficacy of this strategy in increasing the performance of VANETs by bolstering security and reliability in network communications. This study addresses key challenges in VANETs, such as the rapid dissemination of accurate information and the prevention of false data spread, marking a significant advancement in vehicular communication networks.

Very few studies have tried to handle security requirements in the safety application protocols [9–12]. However, none of them have investigated the effects of securing these protocols compared to the insecure versions. Table 1 illustrates the previous detection and prevention of DoS attacks in VANETs. The main objective, the technique used, its benefits, and the limitations of each mechanism are presented in this table. As a consequence of previous studies, this paper aims to use blockchain technology, the most recent and effective mechanism, to detect and prevent blackhole attacks on the vehicular environment. All previous studies have developed availability solutions for general application in VANETs. However, this paper particularly investigates and handles the attacks on availability in the collision avoidance protocol. The importance and danger this type of protocol poses causing disasters on the road and loss of human lives. Then, handling this protocol's vulnerabilities directly enhances the safety conditions on the road networks and safe lives.

Table 1: Detecting and preventing DoS attack in VANETs

Related work	Main objective	Technique	Benefits	Limitations
Dey et al. [2]	Detection	ML-based techniques to detect DoS attack	Comparison dataset and Decision Tree (DT) improved accuracy	Higher attacks lead to lower accuracy
Dong et al. [3]	Detection	Takagi–Sugeno (T–S) fuzzy approach	T-S fuzzy-based security control provides improved performance, safety, and reliability	T-S fuzzy-based approach can be useful only in certain applications
Sun et al. [4]	Prevention	MADAR is an authentication framework with a DoS-attack resistant mechanism	Secure authentication with minimal computational and transmission costs	Add computational overhead to the VANET and delay message transmission
Verma et al. [5]	Prevention	CIC-DDoS2019 dataset	BayesNet classifier can detect DDoS attacks	Not scalable, high delay, and low system performance
Ayaz et al. [6]	Prevention	V2X is a vehicle-to-everything (V2X) system based on FD-NOMA	V2X based on 5G is recommended for PLS and blockchain integration	High required bandwidth

(Continued)

Table 1 (continued)

Related work	Main objective	Technique	Benefits	Limitations
Shrestha et al. [8]	Prevention	Blockchain technology	Reliable vehicular communication	Delay of block generation by offloading the high computational
Sachin et al. [9]	Detection & Prevention	*Ad hoc* on-demand distance vector (AODV) and blockchain	Enhancing network reliability, and deterring malicious activities	Scalability issues, practical implementation challenges

3 The Vehicular Network Technology and Its Applications

VANETs have been developed to enable vehicles to communicate over road networks [13,14]. VANETs have been used to develop safe and efficient driving protocols that assist drivers and control autonomous vehicles during their trips [14–16]. The two main types of entities of VANETs are RSUs and OBUs. OBUs are mounted in vehicles to enable the periodic exchange of safety information for a safe and comfortable driving environment [16]. In contrast, RSUs are typically installed on roads' sides to support vehicle information exchange [14]. RSUs represent the infrastructure of the network that may connect it to other supporting networks (i.e., the internet or satellites) [15,16]. Three different communication channels are used in the VANET: vehicle-to-infrastructure (V2I) or vehicle-to-RSU, vehicle-to-vehicle (V2V), and V2X on the network, such as pedestrians or other existing objects. Several applications have been developed using VANET technology. These applications are classified into three main categories [17]: safety, traffic efficiency, and infotainment applications.

1. *Safety-Related Application*: These applications are used to promote road safety.
   • *Collision avoidance*: The collision can be avoided if the driver or vehicle receives the warning appropriately [13,15,17,18]. More intelligent protocols are developed to assist drivers and control autonomous vehicles in these scenarios. Fig. 1 illustrates an example of a collision avoidance protocol that uses the technology of VANETs to alert vehicles regarding an existing accident at a road intersection. The collision avoidance protocol in this scenario aims to alert all surrounding vehicles regarding the accident. Thus, it reduces the rate of chain accidents that could occur due to the drivers' ignorance about the existing accident. This should allow them to take actions that avoid chain accidents there [19], such as reducing speed or changing the route towards the targeted destination, etc.
   • *Cooperative driving:* These applications focus on alerting drivers regarding the surrounding traffic conditions. Drivers may receive messages to assist them in critical scenarios such as lane changes [19], curve speed warnings [15], and other traffic-related warnings [16,19,20]. Fig. 2 illustrates an example of a cooperative driving protocol that uses the technology of VANETs to alert vehicles regarding a vehicle that changes lanes and speed warning on the road. Upon receiving these messages and recommendations, drivers collaborate for safe and smooth trips.
2. *Traffic Efficiency Control Applications:* This includes the applications that target to enhance smooth mobility on the road network and reduce fuel consumption and gas emissions.

- *Congestion avoidance applications:* These applications assist vehicles in traveling from a source to a destination without getting stuck in traffic congestion [19,21,22].
- *Efficient-based applications:* These applications aim to reduce the fuel consumption and gas emission of traveling vehicles [21,22].

3. *Infotainment Applications:* Along with safety, these applications also give users comfort [22]. These can also be divided into the following categories:
   - *Peer-to-peer application:* The application offers features like music and video sharing among networked vehicles [21]. Vehicles can exchange entertainment-related information, such as videos and audio [19,21].
   - *Internet connectivity:* People of today want to be connected to the internet constantly. As a result, VANETs offer users uninterrupted, continuous access to the internet [21,22].

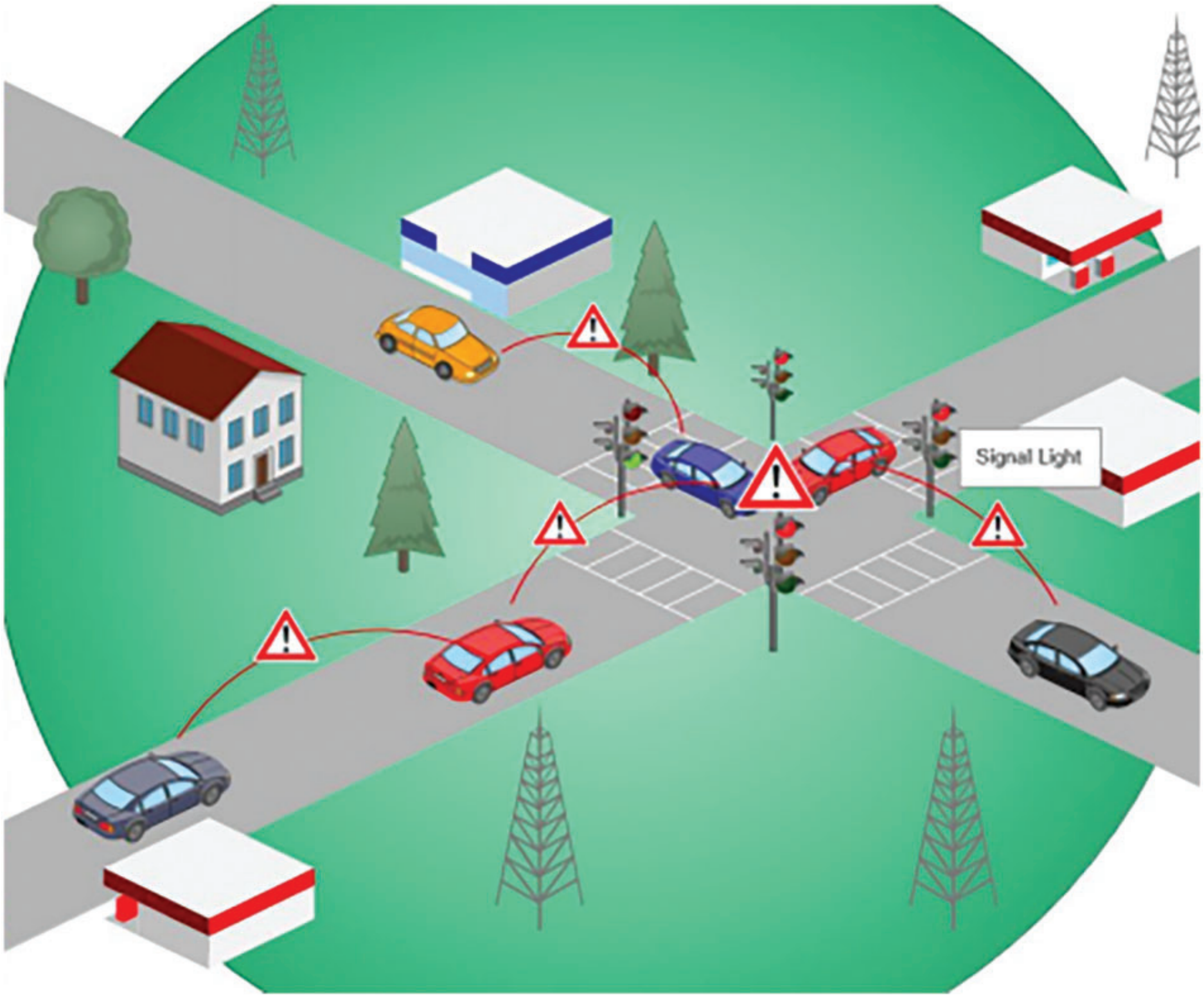


Figure 1: Collision avoidance

Figure 2: Cooperative driving

4 Denial of Service Attacks in Vehicular Networks

DoS and DDoS attacks in VANETs can originate from unauthorized nodes sending fake or spoofed packets [1]. Another common DoS attack involves nodes absorbing packets to disrupt regular communications [7]. These attacks can be both internal and external [18,23]. Fake request packets may also be sent to consume bandwidth, preventing legitimate use of the network [24]. VANETs are vulnerable to network assaults similar to other computer networks. Attackers locate vulnerabilities, such as remotely controllable nodes or those that accept fake messages, and exploit them using malware, Trojans, or other attack mechanisms [2]. Sometimes, exploited nodes unknowingly participate in attacks, spreading malicious messages or code as “slaves” or “zombies” [3]. The impact of these attacks increases when multiple nodes are compromised, leading to overwhelming fictional traffic targeting the network or specific nodes [18,25].

DoS attacks exclusively deplete a particular node’s resources. This node could be a vehicle or infrastructure part (i.e., RSU). Since a lot of data is being sent, connections between vehicles or infrastructure units and vehicles are blocked. The DoS attacks are represented in three main categories on VANETs: Flooding, jamming, and blackhole. This gives the impression that they were corrupted or destroyed during transmission. Communication between vehicles and infrastructure may be disrupted, resulting in traffic jams, accidents, and delays [26]. In this work, we focus on the effects of blackhole attacks, mainly their impacts on collision avoidance protocols developed using the technology of VANETs.

Possible Blackhole Attacks and Collision Avoidance Protocols

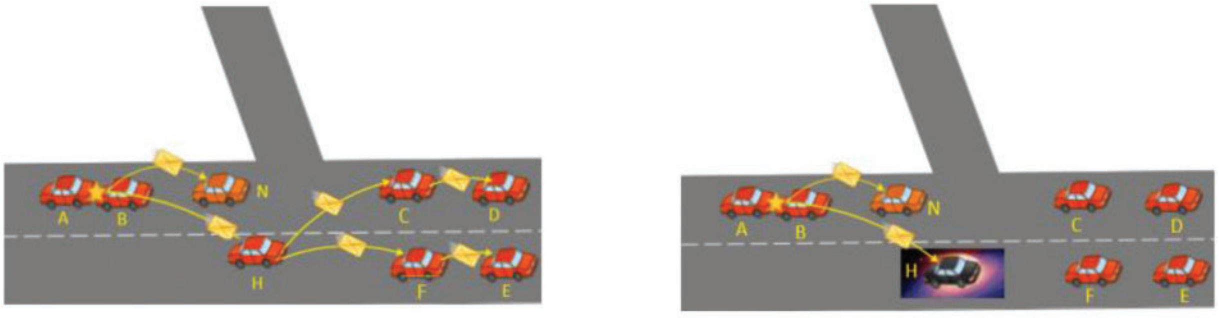
First, as we early discuss collision avoidance protocols aim to prevent vehicle collisions and mitigate their effects. When objects are detected nearby, the system sends alerts and takes action to prevent collisions. Sensors such as radar, lidar (light detection and ranging), and cameras gather data about the vehicle’s surroundings, including pedestrians, other vehicles, and obstructions. Regular “hello” messages among vehicles keep them aware of the traffic situation. The collision avoidance protocol typically involves:

- *Object detection*: Sensors or VANET’s periodic messages identify surrounding objects, including pedestrians, other vehicles, obstructions, or existing accidents.
- *Object tracking*: The system continuously monitors and predicts the movement and future position of detected objects.
- *Risk assessment*: The system evaluates the likelihood of a collision based on the location, speed, and trajectory of surrounding objects.

- *Decision making*: The system determines the best course of action to avoid a collision and minimize its effects.
- *Evasive action:* Actions such as alerting the driver, braking, or changing lanes are taken to prevent an accident. Additionally, the system notifies nearby and distant vehicles of existing accidents to avoid chain collisions.

The blackhole attacks in VANETs is similar to those in traditional computer networks. A malicious node fraudulently claims the shortest path to all destination nodes, attracting all traffic to route through it. In VANETs, the impact is more severe due to direct effects on mobility and road safety, especially in safety-critical applications like collision avoidance or emergency response systems. Vehicles equipped with wireless transceivers act as network nodes, communicating traffic, road conditions, and safety risks. In a "VANET blackhole attack," a malicious vehicle claims to have the shortest path to all destinations, and processes, and then discards or drops all traffic, resulting in a DoS attack. This can prevent the transmission of critical safety messages, leading to accidents or severe traffic jams and restricting network mobility. The loss or delay of communication in these applications may cause fatal accidents.

Fig. 3 illustrates the impact of a blackhole attack on a collision avoidance protocol. When Vehicle A collides with Vehicle B, alert messages are broadcast to notify surrounding vehicles about the accident, including its location, the number of blocked lanes, and involved vehicles. These messages reach all neighboring vehicles within the transmission range of the vehicles involved, such as Vehicle N and Vehicle H. However, vehicles outside the transmission range of the vehicles involved in the accident, like Vehicle C, Vehicle D, and Vehicle E, will not receive direct alert messages. An intermediate vehicle or infrastructure can be selected to forward the alert messages to them. Receiver vehicles then determine their relative locations to the accident and take early evasive actions, such as reducing speed, stopping, changing lanes, etc. Fig. 3a shows the standard scenario for forwarding alert messages to distant vehicles. Vehicle H forwards the alert messages to vehicles outside of the accident transmission range in this scenario.



(a) Alert message forwarding scenario

(b) Blackhole attack scenario

Figure 3: Alert messages of collision avoidance

Fig. 3b illustrates the attack scenario, where the intermediate node that is used to forward alert messages absorbs the message. This blackhole attack can compromise the entire system. The forwarding node is responsible for re-sending alert messages to vehicles heading towards the accident. In a black hole scenario, the elected forwarding node is compromised and absorbs all messages without forwarding them. In Fig. 3b, Vehicle H acts as the blackhole node, absorbing all alert messages and preventing them from reaching Vehicle C, Vehicle D, or Vehicle E. As a result, these vehicles do not take evasive actions and may collide with the accident, leading to a chain accident and exacerbating the incident, increasing costs and damages.

5 The Secure Proposed Protocol

This section shows how to apply and connect blockchain technology to the environment of VANETs. After that, the AODV protocol and the trust score evaluation of each node is explained accordingly. We aim to merge the latter protocol (AODV) with blockchain technology to obtain trust score values for each node to join blocks of the blockchain architecture. Finally, a blockchain-based secure protocol is proposed to prevent the DoS attack and specifically detect and prevent the blackhole attack.

5.1 Vehicular Blockchain-Based Model for Collision Avoidance Protocol

This section mainly presents the primary contents and the structured architecture of the collision avoidance protocol. Blockchain technology is implemented to enhance the security and reliability of vehicular communications within VANETs. The protocol utilizes a private blockchain framework, which requires pre-authorization for nodes (vehicles) to participate. This blockchain is initiated with a genesis block, containing essential elements such as the previous block hash (set to "0"), an empty list of prohibited nodes, and placeholders for timestamp and highest destination sequence numbers.

Fig. 4 graphically illustrates the architecture of the secure collision avoidance protocol. As we can see from the figure, a new block is created upon an accident occurrence on the road network. Any other event such as new vehicle appearance, traffic speed changes or obstacle appearance should lead into creating a new block in the block-chain architecture. The details of each new block are illustrated on the top layer of the architecture in Fig. 4, and more details are presented in the rest of this section regarding the contents of each block. This architecture draws inspiration from the work of Sachin et al. [9]. It represents the key components and processes of the vehicular blockchain-based model for collision avoidance protocol graphically.

5.1.1 Initialization and Identity Management

When a vehicle joins the blockchain network, it provides basic information such as speed, location, and Electronic License Plate (ELP) number. The blockchain assigns a unique pseudo-identity (ID) to each vehicle and generates public (PK) and secret (SK) keys using the Elliptic-Curve Diffie-Hellman (ECDH) protocol. These keys are used to encrypt/decrepit its messages and securely communicate alert collision messages.

5.1.2 Trust Score Assignment

Each vehicle is assigned an initial trust score of "0.5" upon joining the network. This score is crucial for distinguishing between reliable and unreliable vehicles. The trust score varies based on factors such as time and the performance of alert collision packets. This value is important to allow vehicles to communicate on a secure network. Vehicles with trust scores below a predetermined threshold are added to a blacklist, marking them as unapproved for network communication.

5.1.3 Block Creation and Consensus

Blocks are created based on actions and events that happen among traveling vehicles on the network. For example, when an accident occurs, a new block is created with detailed information about the collision event and added to the blockchain. Subsequent blocks contain alert messages sent to other vehicles on the network. Each block's header includes the previous block's hash, timestamp, and the Merkle root of the transactions. The body contains vehicle credentials (ID, PK, SK), trust scores, a registry of blacklisted nodes, and collision alert messages.

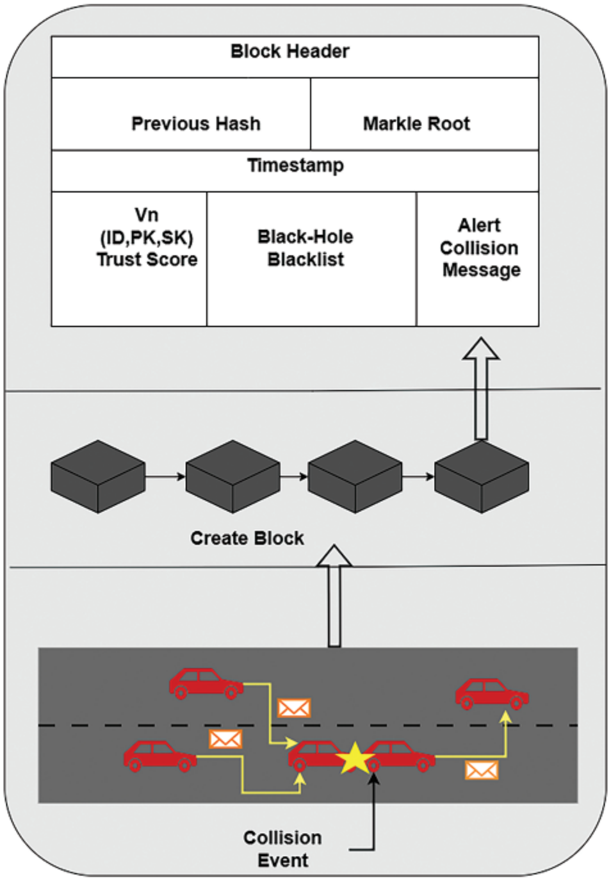


Figure 4: The architecture of blockchain-based collision avoidance protocol

Moreover, the Practical Byzantine Fault Tolerance (PBFT) protocol is the consensus mechanism implemented in this protocol [27]. Nodes validate alert messages to ensure their legitimacy and consistency. Once validated, the network agrees to append the messages to their version of the blockchain, maintaining uniformity and authenticity.

5.1.4 Security and Integrity

Blockchain ensures the immutability of the data recorded, making it suitable for documenting crucial events and messages in VANETs. The Merkle root is a cryptographic hash of all transactions in a block, ensuring data integrity by validating the contents of the block. This mechanism prevents tampering and ensures that all nodes in the network agree on the state of the blockchain.

5.2 Detecting DoS Attack Using Trust-Based AODV Protocol

In the proposed protocol, every vehicle should keep a routing table for its known neighbor destinations to be able to communicate with them. The route is updated for each destination using route request (RREQ) and route reply (RREP) messages among vehicles. These messages are sent by executing the verified AODV routing protocol. In the AODV protocol nodes keep updating the routing table, the source node first sends RREQ messages to destinations [28]. If a malicious node receives and drops the message (i.e., a blackhole attacker), RREP is sent to the requester vehicle only from the intermediate node (i.e., attacker) [28]. Fig. 5 presents an illustrative example, as shown in Fig. 5, the source (i.e., Node 1) disseminates RREQ packets to the network nodes to discover the available routes to its neighboring nodes. Nodes 2, 3, 4, 6, 7, and 8 forward the received RREQ packets to Node 5 (i.e., destination), while Node 9 (i.e., blackhole) drops the RREQ packet and does not forward it to Node 5. Two different routes are discovered between Nodes 1 and 5 in this figure.

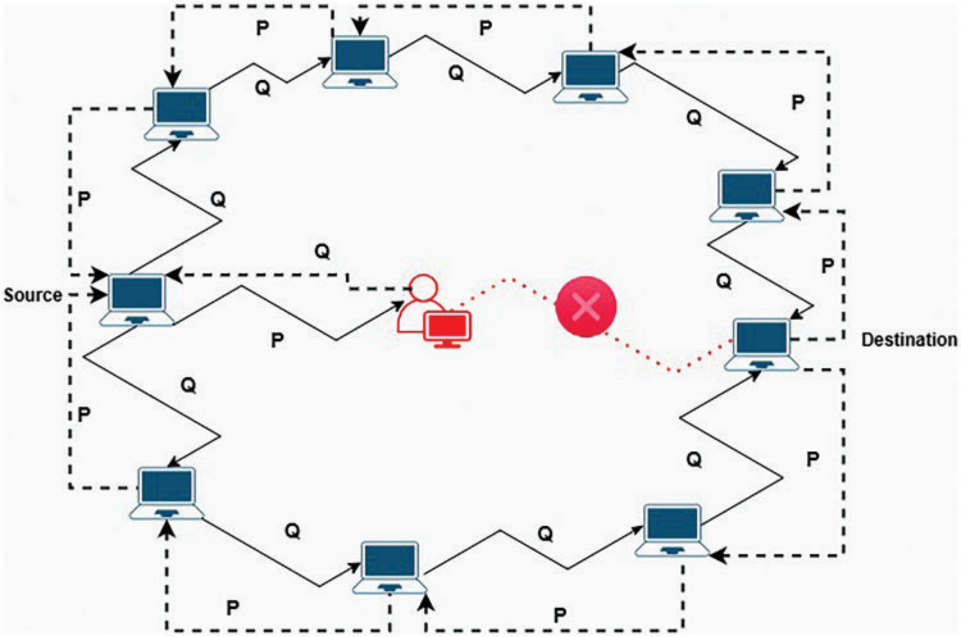
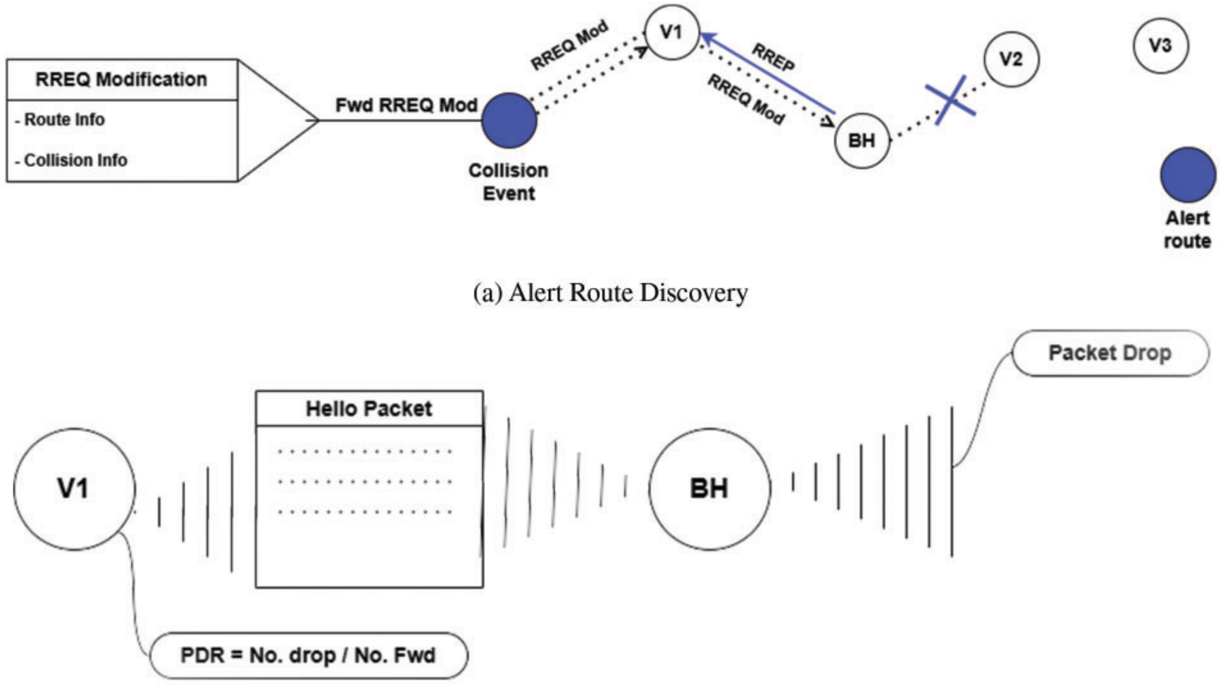


Figure 5: Malicious node in AODV routing protocol

When executing the AODV protocol for each node, upon receiving the RREQ, the receiver node transmits the RREP packet back to the source. This is when the node is the end destination or an intermediate node with a known route to the destination. The hop count in each node is increased by one when it gets an RREQ message [8]. The Destination Sequence Number (DSN) is associated with each route used to determine the validation time of the recommended route [29].

As shown in Fig. 6a, our method uses the AODV protocol to find routes. It adds collision alert messages to the collision avoidance protocol framework. The collision avoidance protocol uses the AODV protocol to establish a connection and send a collision alert message to ($AlertRout$), which designed a new pathway through which we aim to disseminate warning messages in critical scenarios. This ensures that all vehicles at a considerable distance from the accident site are adequately informed and receive the collision alert. This communication channel is essential for the proactive dissemination of information, facilitating heightened situational awareness and timely appropriate responses to mitigate the potential impact of the accident. In this work, the content of the $RREQ$ message is modified to align with the proposed approach. After the collision, a route request ($RREQ$) is initiated, a collision field is created, collision-related information is added, and the message is included in the $RREQ_{\text{modif action}}$ packet. Through the PBFT protocol, the nodes collectively confirm the veracity of each message they receive. The packet is systematically propagated along a predetermined trajectory to facilitate the transmission of the alert message directly to the specified alert path. Suppose the $RREQ_{\text{modif action}}$ packet reaches a blackhole node. In that case, this node drops the $RREQ_{\text{modif action}}$, sends the $RREP$ packet with the highest DSN to neighboring nodes, and calculates the trust score for this node. Fig. 6b shows how the "Hello" packet can fall in a blockhole attack.



(a) Alert Route Discovery

(b) Hello Packet in Blackhole Attack

Figure 6: Alert route discovery in AODV modification and hello packet

Moreover, this study uses a decentralized trust score system that evaluates the reliability of automobile nodes. It computes the trust score by assigning each vehicle a default trust score during network entry, set to 0.5. Trust scores are variable and subject to change based on factors like time and packet performance. As depicted in Fig. 6, the packet delivery ratio (PDR) is quantified as the proportion of successfully delivered messages. According to the AODV protocol, the confidence metric decreases if the forwarding rate exceeds the delivery rate. Thus, the trust score is reduced to 0.0 when the blackhole node drops the packet. Subsequently, the node is designated as a blackhole entity following a consensus reached through the PBFT protocol.

Each block maintains in the first fields of its body a list of the neighboring vehicles containing the identity, public key, and secret key and the trust score (i.e., 0.5) of the vehicles there (i.e., ID, PK, SK, trust score value). A blacklist of nodes that have created blackhole attacks is maintained to monitor nodes that display suspicious behavior or possess low trust scores (i.e., 0.0), as explained in Section 5.2. Malicious nodes purposefully make this list unchangeable, and the blockchain promptly distributes it to all nodes. The trust score threshold allows nodes to update this table. If the trust score of a node drops below this threshold of 0.5, it will be added to the blacklist. The reliability and credibility of neighboring nodes are assessed by calculating their trust scores.

5.3 Secure Collision Avoidance Protocol Using Blockchain

This section presents the systematic procedure of the proposed protocol for secure collision avoidance. This protocol utilizes the blockchain framework to secure VANETs Communications proposed by Shrestha et al. [8]. The trust score computation is inspired by Sachin et al. [9], which used the AODV protocol for this purpose. Fig. 7 systematically illustrates the steps of the proposed protocol. More details regarding the proposed protocol are presented in the rest of this section.

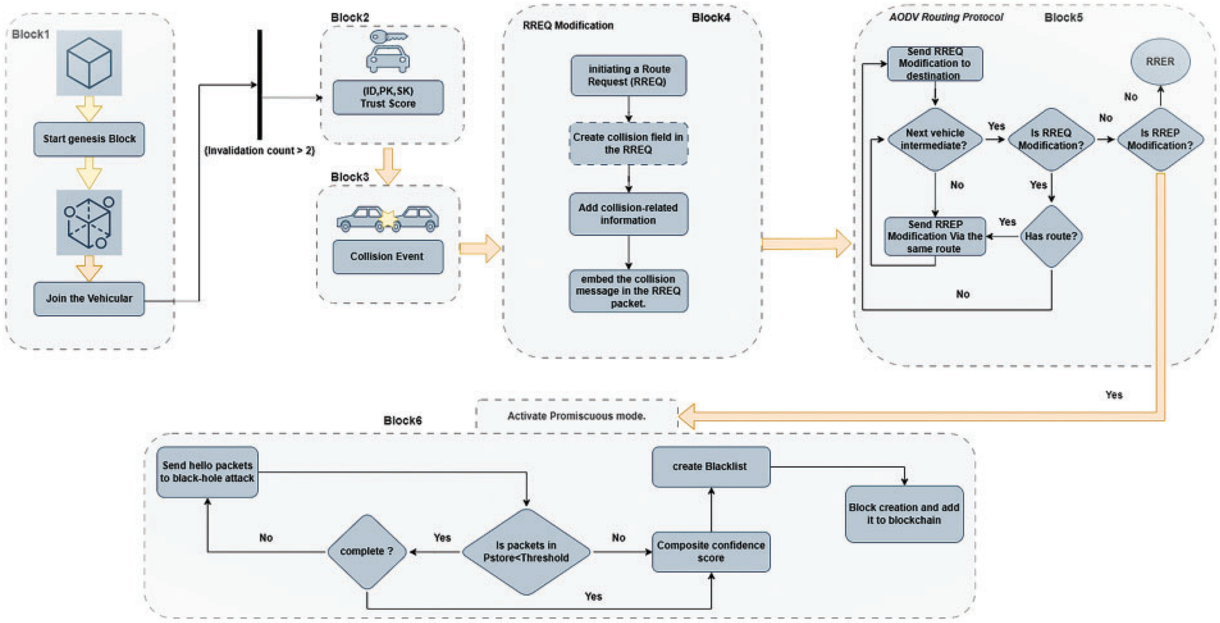

Block1
Start genesis Block
Join the Vehicular
(Invalidation count > 2)
Block2
(ID,PK,SK)
Trust Score
Block3
Collision Event
RREQ Modification
Block4
initiating a Route Request (RREQ)
Create collision field in the RREQ
Add collision-related information
embed the collision message in the RREQ packet.
AODV Routing Protocol
Block5
Send RREQ Modification to destination
RRER
No
Next vehicle intermediate?
Yes
Is RREQ Modification?
No
Is RREP Modification?
No
Yes
Send RREP Modification Via the same route
Yes
Has route?
No
Yes
Activate Promiscuous mode.
Block6
Send hello packets to black-hole attack
create Blacklist
Block creation and add it to blockchain
No
complete ?
Yes
Is packets in Pstore<Threshold
No
Composite confidence score
Yes

Figure 7: Secure protocol design of the proposed blockchain-based collision avoidance protocol

1. *Initialization of the Protocol:*
   When a vehicle initially joins the blockchain, it provides its basic information. This includes the speed, location, and ELP number. Blockchain, in response, assigns a pseudo-identity called ID for that vehicle, which serves as a distinct and unique number for each vehicle on the road network. It also gets public (P_K) and secret (S_K) keys using the ECDH protocol [30]. The vehicle has to use these keys to encrypt alert collision messages and communicate securely with its neighbors. This appears in Blocks 1 and 2 in Fig. 7.
2. *Default Trust Score Assignment:*
   After that, as shown in Block 2 in Fig. 7, each vehicle is assigned a default trust score as an extra initialization step during the network entry process. The initial trust score is automatically set to 0.5. The deliberate selection of a default trust score is a purposeful decision made during the protocol configuration to address the issue of blackhole attacks. It is crucial to distinguish between reliable and unreliable vehicles, particularly for new blockchain network participants. The trust scores are variable and subject to change based on factors such as time and the performance of alert collision packets. Once the packet delivery ratio falls below a predetermined threshold, the trust score is deceased, and the minimum value that can be assigned to the trust score is 0.0. The forwarding node with a trust score less than 0.5 is added

to the blacklist (i.e., blackhole detection). That node transforms into an unapproved node for network communication.

3. *Creation of Genesis Blocks:*
   As previously mentioned, the blockchain is initiated with the genesis block, as shown in Fig. 7 Block 1. This is the fundamental basis upon which all subsequent blocks are built. This block comprises several vital elements, such as a previous block hash value of "0," an empty roster of prohibited nodes, and void transaction lists. Additionally, it includes placeholders for various other data, such as the current timestamp and the highest destination sequence number. Upon initial integration into the network, the vehicle knows the genesis block solely. Subsequently, the blackhole nodes in the blacklisted node table are modified according to the latest communication.
4. *Route Discovery and* $RREQ_{modif\ ication}$:
   In the scenario depicted in Fig. 6, the node labeled as Collision Event serves as the originating node to establish a connection and transmit a collision alert message to the node labeled as *AlertRout*. By employing the AODV protocol, we have modified the *RREQ* content in the AODV protocol to align with our proposed approach in the collision avoidance protocol as shown in Fig. 7 Block 4. The fields added to the *RREQ* packet are:
   (a) A Route Request (RREQ) is initiated after the collision.
   (b) Create a Collision Field in the RREQ.
   (c) Add collision-related information.
   (d) Embed the collision message in the RREQ packet.
   Then, $RREQ_{\mathrm{modif\ ication}}$ packet is distributed throughout the protocol. It contains a newly established route to the intended destination and an alert collision message. Each node in the network actively forwards this request along with alert collision messages until a notification of a newly accessible route is received. In this scenario, the blackhole node (*BH*) intercepts and drops the $RREQ_{\mathrm{modif\ ication}}$ packet, as shown in Fig. 6a. Following this interception, the AODV protocol initiates a Route Reply (RREP) to node *V1*, including the highest DSN. Consequently, the BH node effectively obstructs the transmission of the collision alert message to node *V2*. This interruption prevents the message from reaching its intended recipient (i.e., Alert Route node). When the *RREP* packet is sent from *BH* to *V1*, the node positioned ahead of the sender should verify the authenticity of the sender node. *V1* performs initial verification steps by examining the content of the *RREP* message. This includes the trust score and the *ID*, P_{K}, and S_{K} values. Then, it examines the DSN and the value of the trust score received. Suppose the DNS number in the *RREP* is more than the highest DSN of the system or if the trust score is less than the threshold set by the system. Subsequently, it computes the temporal disparity between the receipt of the *RREP* and the previously acquired $RREQ_{\mathrm{modif\ ication}}$.
5. *Activating Attack Mode:*
   Upon verification of the blackhole attack through the computation of the trust score and DSN value, as delineated in the previous point. Node *V1* activates its attack mode to intercept communications with *BH*. In networking, attack mode refers to a node's ability to eavesdrop on packets transmitted by its neighboring node through passive communication channel monitoring. Afterward, *V1* begins sending a series of "Hello" packets to the detention node labeled *AlertRoute* via node BH, which acts as an intermediary, as illustrated in Fig. 7. The p-store, a data structure, stores all packets containing the message "Hello" from node *V1*. One must employ the packet lookup method for each packet to retrieve specific information. This framework's structure contains important header data for each packet transmitted to node *BH*. The *methodhellopacket* function verifies whether the packet sent to BH matches the

packet stored in the *V1*'s p-store. Therefore, it guarantees the authenticity of the transmission. Once a match is verified, the packet is immediately eliminated from the p-store by executing the delete packet function. Their main purpose is to assist the honest node *V1* in intercepting and monitoring the neighboring node *BH* within its communication range, thus allowing the exchange of network packets. These steps are illustrated in Fig. 7 Block 6.

6. *Calculating the Value of Trust Scores:*
   Upon receiving an *RREP* message from a neighboring node in the network, each recipient node assesses the reliability and credibility of that neighbor. This signifies the preliminary stage of trust score calculation in our proposed protocol. The quantity of packets that node *BH* forwards indicates its trustworthiness. When $RREQ_{\text{modif ication}}$ messages are tampered with, the trust score value decreases until it reaches 0.0. Nevertheless, the total number of packets in the packet stores should not exceed a predetermined threshold during transmission. This threshold is a value dynamically set based on the importance of the message being transmitted through the collision avoidance protocol. For instance, in crucial communication scenarios like collision avoidance protocols, the threshold may be deliberately set at a low level to avoid the accumulation of packets in the queue for a long duration. Fig. 7 Block 6 shows in the setup phase, the maximum threshold value of 5 packets is implemented, representing the highest number of packets stored in the packet store (p-store). This approach is reliable and effective for identifying deceitful nodes trying to send an alert collision message. If the node is not blacklisted, reducing the trust score by a specific percentage in such a situation would still classify it as trustworthy. As a result, this would lead to the incorrect perception of malicious nodes as trustworthy. To deal with this issue, our design promptly decreases the trust score to 0.0 when it detects any instance of a node dropping packets.
7. *Block Creation and Blackhole Blacklisted:*
   After calculating trust scores and creating the blacklist, this data is included in a new block. The block contains information related to blackhole attacks, as shown in Fig. 7 Block 6. Afterward, the newly formed block is submitted for validation by secondary nodes. These nodes conduct comprehensive evaluations to verify the accuracy of the block and subsequently send confirmation messages to the leader node. After receiving consensus from at least two-thirds of the network, the leader node adds the block to the blockchain network. All nodes follow the PBFT protocol to achieve credibility for the alert messages included in the block. This rigorous procedure guarantees the integrity of the blockchain and the credibility of its content, thereby bolstering the security and dependability of the entire protocol.

6 Performance Evaluation

In this section, the performance of the proposed protocol is evaluated to test and investigate its correctness and effectiveness. The experimental study is executed around an assumed accident among a set of traveling vehicles on a long highway road scenario. A malicious vehicle that pretends to be the best forwarder towards far vehicles on the road and then drops all the alert messages has been simulated as a blackhole attack. The performance of the proposed protocol has been tested in three main aspects. First, since we are utilizing blockchain technology, we measure the overhead of the proposed solution in terms of the time and capacity of the formed blocks for different numbers of traveling vehicles. Second, the ability of the proposed protocol to detect the malicious node for different numbers of traveling vehicles and speeds has been experimentally tested. Finally, we measure the effects of avoiding the blackhole attack on the performance of the collision avoidance protocol in reducing the number of vehicles crashed to the existing accident (i.e., the accident rate on the road network), the packet delivery ratio, and the throughput utilization of the connecting network.

We used the network simulator NS2 [31] to implement the communications and transmitted packets among traveling vehicles and the proposed security protocol phases. Moreover, the simulation of the urban mobility tool (SUMO) [32] is used for real-time traffic simulation. Table 2 illustrates the tested experiments' main parameters.

Table 2: Simulation parameter

Parameter	Value
MAC type	IEEE802.11P
Transmission range (m)	1000
Vehicle's speed (m/s)	17, 22, 27, 33, 38
Simulation area (m^2)	30 m × 400 m
Number of vehicles	20, 40, 60, 80, 100
Number of blackholes	1
Simulation time	10,000

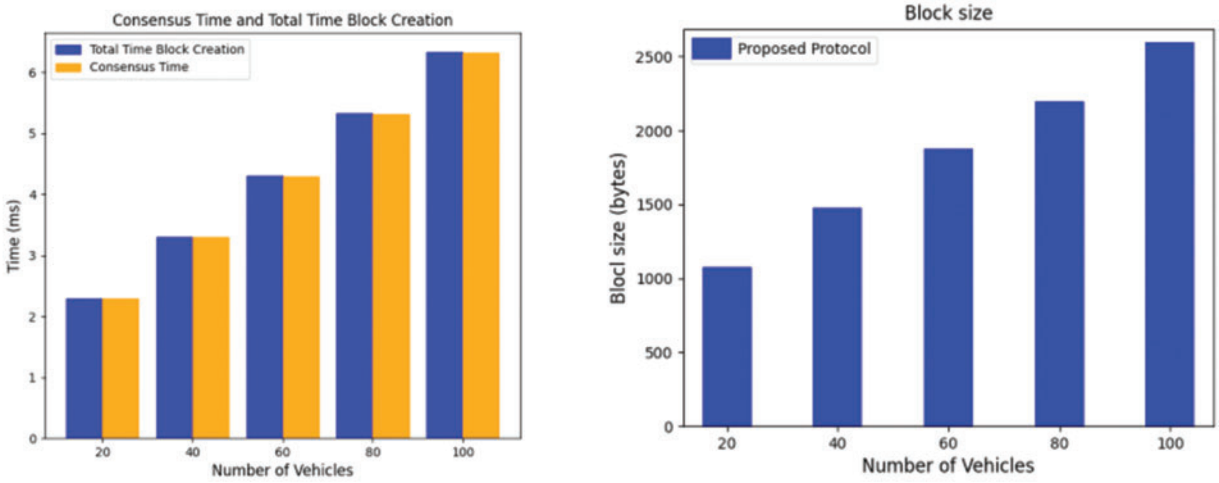
6.1 Blockchain Creation Overhead

Blockchain technology requires time and high storage costs to be created, initialized, and utilized in any investigated environment. In this set of experiments, we measure the delay time of creating blocks and obtain a consensus to achieve trust among the traveling vehicles for any event in the road scenario. Besides, different numbers of traveling vehicles are investigated in these experiments. Then, we investigate the required storage for any created block on the infrastructure. The latter parameter has also been investigated for different numbers of traveling vehicles in the investigated road scenario. These experiments assess the performance of the proposed model by measuring the time it takes for validation to obtain a consensus on transaction states and then create a block that contains a table of blacklisted nodes. We conduct this test using fifteen validated nodes, namely RSUs, to handle various block sizes. These results are considered acceptable due to the utilization of the PBFT consensus protocol which incurs low efficiency and high energy consumption.

Fig. 8a illustrates the required time to obtain consensus on any appeared vehicle or event to participate in the trusted created environment. Moreover, it illustrates the overall time expenses for each block construction. As we can see from the Figure, both the creation and the consensus times of each block are increased by increasing the number of vehicles in the tested experiment. Creating a new block, with a capacity of up to twenty vehicles, takes around two ms. However, the delay time is increased to six ms when the block capacity is increased to one hundred vehicles. On the other hand, Fig. 8b illustrates the block sizes that are initiated for different numbers of vehicles. The storage overhead (S_{Over}) is computed using Eq. (2) [33]. B_{Size} is the average initial block size, typically set at 0.9 KB. B_{rate} represents the ratio between the number of blocks per hour on the block creation interval (i.e., Number of blocks per hour) and the average number of blocks that are added daily (i.e., Block creation interval), as illustrated in Eq. (1) [33]. Finally, Hours represent the number of hours per day (i.e., 24), and Days represent the number of days in a year (i.e., 365).

$$B_{\text{rate}} = \frac{Number\ of\ blocks\ per\ hour}{Block\ creation\ interval} \tag{1}$$

$$S_{\text{Over}} = B_{\text{Size}} \times B_{\text{rate}} \times \text{ Hours } \times \text{ Days} \tag{2}$$



(a) Time of creating blocks and consensus time

(b) The block size

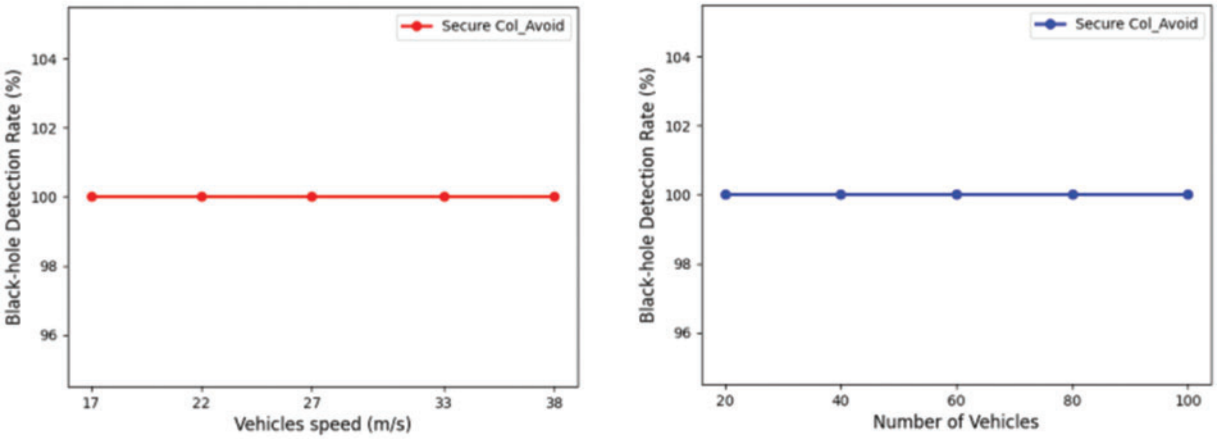
Figure 8: Overheads of creating a blockchain environment for different numbers of vehicles on a road network

Eq. (1) represents block rate (B_{rate}), the ratio of the number of blocks created per hour to the block creation interval. This represents how many blocks are created in one hour (i.e., 60_{block}). The block creation interval is the time it takes to create a new block (i.e., 120 s). Performing calculations using Eqs. (1) and (2) based on the previously provided numbers. The storage overhead is estimated to be around 3942 KB per year, based on a calculation of 0.9 × (60/120) × 24 × 365.

6.2 *Detecting Blackhole Attacks*

Here, we first simulated an attacker vehicle in the tested environment that used a fake identity aiming to get authenticated on the protocol to gather the messages and drop them. Then, we measure the ability of the proposed protocol to detect this vehicle when different numbers of vehicles are traveling on the investigated road scenario and for different traveling speeds. This is mainly to measure the scalability and adaptability of the proposed protocol. The blackhole detection ratio is defined mainly as the ability of the protocol in detecting the simulated blackhole attacker vehicle.

Fig. 9 graphically illustrates the blackhole detection percentages for the simulated scenario. The packet delivery ratio is defined by the ability of the proposed protocol to detect the simulated black hole. As we can see from Fig. 9a, the proposed protocol (i.e., *Secure Col Avoid*) detected the blackhole attack by 100% for different numbers of traveling vehicles. The traffic speed was set at 80 km/h in this set of experiments as a static unaffected parameter. After that, have also investigated the effect of the traffic speed on the blackhole detection ability. As we can see in Fig. 9b, the proposed protocol also succeeds in detecting the blackhole attack by 100% for different simulated traffic speed scenarios. The different tested vehicle speeds in the last set of experiments guarantee the performance for different traffic conditions. This includes considering urban areas and highways where the traffic speed is the main distinguishing factor between these scenarios.



(a) Different Number of Vehicles

(b) Different Traffic Speeds

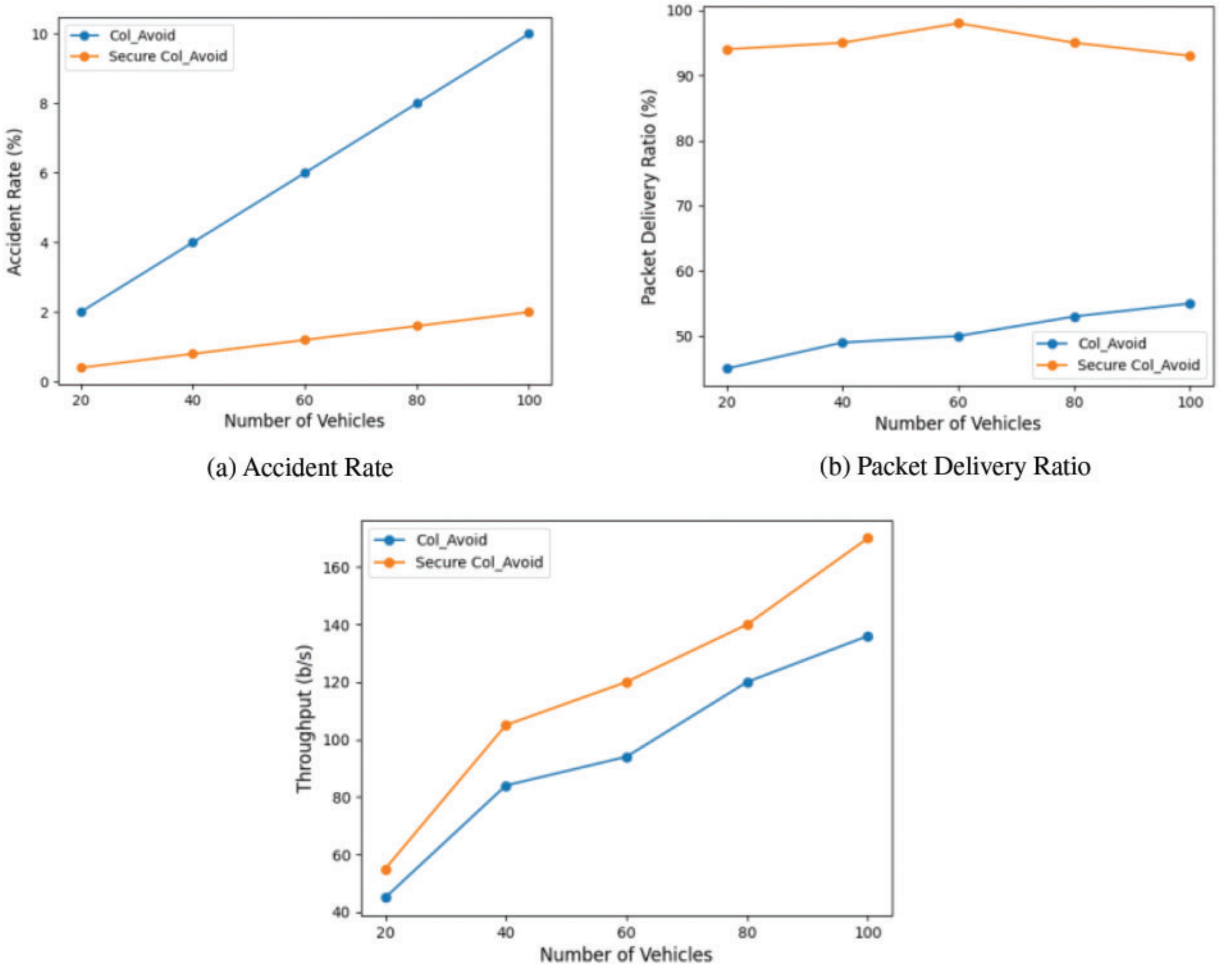
Figure 9: Blackhole detection ratio

6.3 Effects of Avoiding Blackhole Attacks

As discussed and presented in the early sections, the proposed protocol aims to detect and avoid blackhole attacks on the collision avoidance protocol. In this set of experiments, we aim to investigate the benefits and effects of avoiding the blackhole attack on the performance of the collision avoidance protocol. We compare the performance of the typical collision avoidance protocol (i.e., *Col Avoid*) and the proposed protocol, which is a blockchain-based secure version of the collision avoidance protocol (i.e., *Secure Col Avoid*). This comparison considers the accident rate, packet delivery ratio, and network throughput. We have simulated one vehicle that acts as a blackhole attacker. It tricks the surrounding vehicles into forwarding the alert messages through it. Then, it drops the messages instead of forwarding them.

First, Fig. 10a illustrates the accident rate (i.e., percentage of vehicles involved in the occurred accident) of the investigated protocols. In both tested protocols, the accident rate increases by increasing the number of vehicles in the simulated road scenario. As we can infer from the Figure, the proposed protocol (*Secure Col Avoid*) succeeded in reducing the accident rate by 60% compared to the security absent scenario (*Col Avoid*). This is due to the early alerts delivered to the far vehicles through trusted forwarding vehicles in the Secure Col Avoid. These far vehicles have time to respond to the accident's existence and adapt their speed or route accordingly. On the other hand, relying on an un-trusted vehicle (i.e., blackhole) to forward the messages leaves far vehicles unaware from the existing accident and thus leads them to crash into it. Then, the accident rate is increased accordingly.

Second, Fig. 10b illustrates the packet delivery ratio of the investigated protocols. Considering two transition ranges on the road scenario, the packet delivery ratio is less than 50% using the Col Avoid protocol. More than 50% of messages are dropped and not delivered due to the blackhole attack. In this scenario, the packet delivery ratio increases by increasing the number of vehicles on the road because more vehicles exist inside the same transition range. However, using the Secure Col Avoid protocol, the packet delivery ratio is more than 90%. The ratio is decreased here by increasing the number of tested vehicles on the road. This is mainly due to increasing the rate of collision possibility between transmitted messages.



(a) Accident Rate

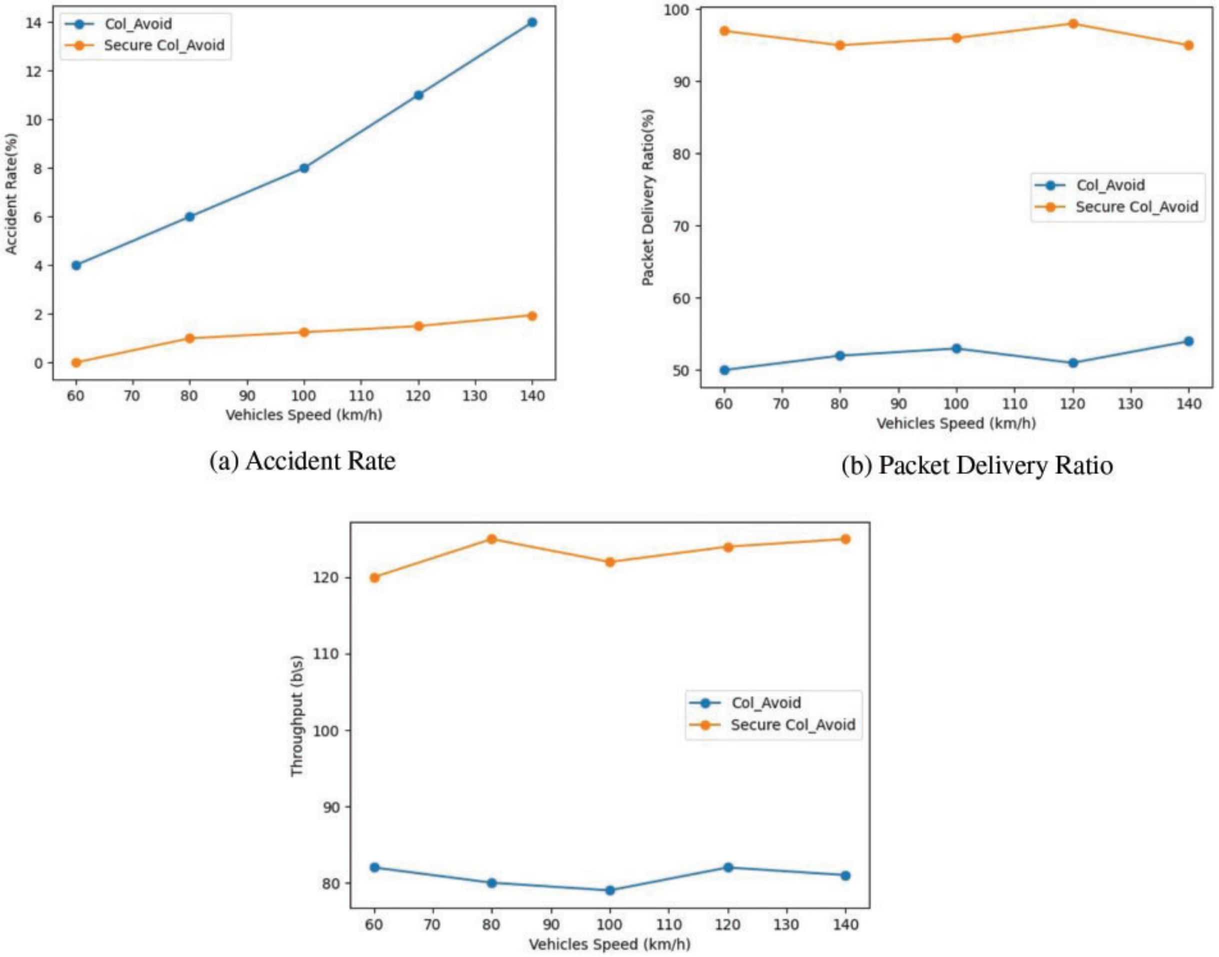
(b) Packet Delivery Ratio

(c) Throughput

Figure 10: Variation of network performance of collision avoidance nodes in the presence and after removing malicious nodes for different numbers of vehicles

Third, Fig. 10c graphically illustrates the network's throughput using Col Avoid and Secure Col Avoid protocols. The throughput metric measures the amount of utilized bandwidth by sending the packets per second. As we can see from the figure, the Secure Col Avoid protocol has increased the throughput utilization of the network by 20% compared to the Col Avoid protocol in the simulated scenario. This is the direct consequence of the blackhole avoidance and true messages forwarding on the network. More bandwidth has been utilized.

On the other hand, the effects of securing the collision avoidance protocol for different traffic speeds are illustrated in Fig. 11. As we see from Fig. 11a, the secure proposed protocol has highly reduced the accident rate, especially for high traffic speeds. Fig. 11b shows the delivery packet ratios among traveling vehicles is increased by 50% regardless of the traveling speed of vehicles. The utilized throughput of the connecting network is also increased by 50% for all tested traveling speeds as well.



(a) Accident Rate

(b) Packet Delivery Ratio

(c) Throughput

Figure 11: Variation of network performance of collision avoidance nodes in the presence and after removing malicious nodes for different traffic speeds

Finally, the security overhead in terms of extra delay and memory is completely considered in Section 6.1. No extra data or time is required by this secure protocol except the required time and memory for creating and storing blocks in the initial phase. Vehicles can reliably and securely communicate after they get authorized by the blockchain establishment.

7 Conclusion and Future Work

The paper proposes a blockchain-based method to reduce the impact of blackhole attacks in the collision avoidance protocol by utilizing the Trusted AODV protocol. Within this study, the vehicular nodes transfer the mining process to the RSUs to accelerate the block creation, which is well-suited for the suggested collision avoidance protocol. We employ promiscuous mode to assign a trust value to neighboring vehicular nodes that reacted dynamically and frequently with RREP messages. We additionally demonstrate the process by which the trust score is combined with approved RSUs, and we assessed the amount of time required for block consumption about PBFT consensus.

The findings demonstrate that integrating a blockchain-based collision-avoidance protocol enhances packet delivery ratio and network throughput. The effectiveness of the collision avoidance technique is enhanced by efficiently eliminating blackhole nodes, resulting in improved message dissemination efficiency. In future studies, we aim to investigate the impact of other attaches on the tested scenarios and adapt the blockchain-based secure protocol to secure them.

Acknowledgement: Philadelphia University, Jordan, which provides us with a peaceful area and equipped labs to implement and test the protocols.

Funding Statement: The authors received no specific funding for this study.

Author Contributions: The authors confirm their contributions to the paper as follows: study conception and design: Mosab Manaseer, Maram Bani Younes; data collection: Mosab Manaseer; analysis and interpretation of results: Mosab Manaseer, Maram Bani Younes; draft manuscript preparation: Mosab Manaseer. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: The data that support the findings of this study are available on request from the corresponding author, Maram Bani Younes.

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] D. Swessi and H. H. Idoudi, "A comparative review of security threats datasets for vehicular networks," presented at Int. Conf. Innov. Intell. Informat., Comput., Technol., IEEE, Sep. 2021, pp. 746–751.

[2] M. R. Dey, M. Patra, and P. Mishra, "Efficient detection and localization of DoS attacks in heterogeneous vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 72, no. 5, pp. 5597–5611, 2023. doi: 10.1109/TVT.2022.3233624.

[3] J. Dong, Z. Ye, D. Zhang, and F. Guo, "T-S fuzzy-based security control of nonlinear unmanned marine vehicle systems with uncertain stochastic DoS attack," *Int. J. Fuzzy Syst.*, vol. 25, no. 1, pp. 289–301, 2023. doi: 10.1007/s40815-022-01311-1.

[4] C. Sun, J. Liu, X. Xu, and J. Ma, "A privacy-preserving mutual authentication resisting DoS attacks in VANETs," *IEEE Access*, vol. 5, pp. 24012–24022, 2017. doi: 10.1109/ACCESS.2017.2768499.

[5] A. Verma and R. Saha, "Analysis of BayesNet classifier for DDoS detection in vehicular networks," presented at Int. Conf. Augment. Intell. Sustain. Syst. (ICAISS), Trichy, India, 2022, pp. 980–987. doi: 10.1109/ICAISS55157.2022.10011115.

[6] F. Ayaz, Z. Sheng, I. W. -H. Ho, D. Tiany, and Z. Ding, "Blockchain-enabled FDNOMA based vehicular network with physical layer security," presented at 95th Veh. Technol. Conf.: (VTC2022-Spring), Helsinki, Finland, 2022, pp. 1–6. doi: 10.1109/VTC2022-Spring54318.2022.9860421.

[7] N. Ahmed, Z. Deng, I. Memon, F. Hassan, K. H. Mohammadani and R. Iqbal, "A survey on location privacy attacks and prevention deployed with IoT in vehicular networks," *Wirel. Commun. Mob. Comput.*, vol. 2022, pp. 1–15, 2022. doi: 10.1155/2022/6503299.

[8] R. Shrestha, R. Bajracharya, A. P. Shrestha, and S. Y. Nam, "A new type of blockchain for secure message exchange in VANET," *Digit. Commun. Netw.*, vol. 6, no. 2, pp. 177–186, 2020. doi: 10.1016/j.dcan.2019.04.003.

[9] K. Sachin and P. K. Verma, "A comparative study of collision avoidance medium access control protocols in internet-of-things," *Int. J. Cloud Comput.*, vol. 13, no. 2, pp. 139–164, 2024. doi: 10.1504/IJCC.2024.137409.

[10] K. Fan, Y. Bi, Y. Yang, K. Zhang, and H. Li, "Secure and efficient lightweight protocol for emergency vehicle avoidance based on cloud," *IEEE Netw.*, vol. 37, no. 4, pp. 314–322, 2023. doi: 10.1109/MNET.002.2300009.

[11] P. Kanani *et al.*, "Improving QoS of DSDV protocol to deliver a successful collision avoidance message in case of an emergency in VANET," *Soft Comput.*, vol. 8, no. 22, pp. 1–11, 2023. doi: 10.1007/s00500-023-08766-w.

[12] K. Sutradhar, "A quantum cryptographic protocol for secure vehicular communication," *IEEE Trans. Intell. Transp. Syst.*, vol. 25, no. 5, pp. 3513–3522, 2024. doi: 10.1109/TITS.2023.3322728.

[13] M. B. Younes and A. Boukerche, "A performance evaluation of a fault-tolerant path recommendation protocol for smart transportation system," *Wirel. Netw.*, vol. 24, no. 2, pp. 345–360, 2018. doi: 10.1007/s11276-016-1335-7.

[14] M. B. Younes and A. Boukerche, "A vehicular network based intelligent lane change assistance protocol for highways," presented at IEEE Int. Conf. Commun. (ICC), May 2017, pp. 1–6.

[15] M. B. Younes, A. Boukerche, "Boukerche a novel traffic characteristics aware and context prediction protocol for intelligent connected vehicles," *IEEE Trans. Veh. Technol.*, vol. 72, no. 8, pp. 9897–9908, 2023. doi: 10.1109/TVT.2023.3259903.

[16] R. Al-Ani, B. Zhou, Q. Shi, T. Baker, and M. Abdlhamed, "Adjusted location privacy scheme for VANET safety applications," Presented at NOMS 2020-2020 IEEE/IFIP Netw. Operat. Manag. Symp., 2020, pp. 1–4.

[17] A. Sinha and S. K. Mishra, "QLA (Queue Limiting Algorithm) for protecting VANET from DOS (Denial of Service)," *Int. J. Comput. Appl.*, vol. 86, no. 8, pp. 14–17, 2014.

[18] M. S. Manaseer and M. B. Younes, "Secure protocols in VANETs: Availability considerations," presented at Int. Conf. Inf. Commun. Syst. (ICICS), Irbid, Jordan, 2023, pp. 1–6. doi: 10.1109/ICICS60529.2023.10330450.

[19] R. Al-Ani, T. Baker, B. Zhou, and Q. Shi, "Privacy and safety improvement of VANET data via a safety-related privacy scheme," *Int. J. Inf. Secur.*, vol. 22, no. 4, pp. 763–778, 2023. doi: 10.1007/s10207-023-00662-6.

[20] D. T. Radhakrishna Karne, "Review on vanet architecture and applications," *Turk. J. Comput. Math. Educ.*, vol. 12, no. 4, pp. 1745–1749, 2021.

[21] S. Majumder, A. Mathur, and A. Y. Javaid, "A study on recent applications of blockchain technology in vehicular ad hoc network (VANET)," in *Natl. Cyber Summit (NCS) Res. Track*, 2020, pp. 293–308.

[22] F. B. Günay, E. Öztürk, T. Avdar, Y. S. Hanay, and A. U. R. Khan, "Vehicular *ad hoc* network (VANET) localization techniques: A survey," *Arch. Comput. Methods Eng.*, vol. 28, pp. 3001–3033, 2021.

[23] E. Aliwa, O. Rana, C. Perera, and P. Burnap, "Cyberattacks and countermeasures for in-vehicle networks," *ACM Comput. Surv.*, vol. 54, no. 1, pp. 1–37, 2021.

[24] H. Hasbullah and I. A. Soomro, "Denial of service (DOS) attack and its possible solutions in VANET," *Int. J. Electron. Commun. Eng.*, vol. 4, no. 5, pp. 813–817, 2010.

[25] T. Zaidi and S. Faisal, "An overview: Various attacks in VANET," presented at 4th Int. Conf. Comput. Commun. Autom. (ICCCA), Dec. 2018, pp. 1–6.

[26] A. Ilavendhan and K. Saruladha, "Comparative analysis of various approaches for DoS attack detection in VANETs," in *Int. Conf. Electr. Sustain. Commun. Syst. (ICESC)*, 2020, pp. 821–825.

[27] M. Castro and B. Liskov, "Practical byzantine fault tolerance and proactive recovery," *ACM Trans. Comput. Syst. (TOCS)*, vol. 20, no. 4, pp. 398–461, 2002.

[28] I. Moumen, N. Rafalia, J. Abouchabaka, and Y. Chatoui, "AODV-based defense mechanism for mitigating blackhole attacks in MANET," *E3S Web Conf.*, vol. 412, 2023, Art. no. 01094.

[29] D. G. Fragkoulis, N. D. Kouvakas, F. N. Koumboulis, and N. I. Georgiou, "Modeling and modular supervisory control for the AODV routing protocol," *AEU-Int. J. Electr. Commun.*, vol. 15, pp. 47–61, 2023.

[30] F. Thachil and K. C. Shet, "A trust-based approach for AODV protocol to mitigate black hole attack in MANET," in *2012 Int. Conf. Comput. Sci.*, Phagwara, India, 2012, pp. 281–285. doi: 10.1109/ICCS.2012.7.

[31] H. Rehmani and Y. Saleem, "Network simulator NS-2," in *Encyclopedia of Information Science and Technology*, 3rd ed. USA: IGI Global, 2015, pp. 6249–6258.

[32] M. Behrisch, L. Bieker, J. Erdmann, and D. Krajzewicz, "SUMO simulation of urban mobility: An overview," in *Third Int. Conf. Adv. Syst. Simul. (SIMUL)*, 2011, pp. 63–68.

[33] S. Kudva, S. Badsha, S. Sengupta, H. La, I. Khalil and M. Atiquzzaman, "A scalable blockchain based trust management in VANET routing protocol," *J. Parallel Distr. Comput.*, vol. 152, no. 9, pp. 144–156, 2023. doi: 10.1016/j.jpdc.2021.02.024.