Intelligent Transport System based Blockchain to Preventing Routing Attacks

Mada Alharbi[1] and Abdulatif Alabdulatif[2*]

[1] Graduate Student, Department of Computer Science, College of Computer, Qassim University, Buraydah, Saudi Arabia. 391215490@qu.edu.sa, Orcid: https://orcid.org/0009-0008-0561-2838

[2*]Assistant Professor, Department of Computer Science, College of Computer, Qassim University, Buraydah, Saudi Arabia. ab.alabdulatif@qu.edu.sa, Orcid: https://orcid.org/0000-0003-0646-5872

Received: December 22, 2022; Accepted: January 26, 2023; Published: March 30, 2023

Abstract

In the era of smart cities, Intelligent Transportation System (ITS) are necessary towards the success of smart cars in the modern societies. ITS rely on Vehicular Ad-hoc Networks (VANETs), which enable communication between cars to relay safety messages exchange. However, VANETs can be exposed to the issue of decentralization and high mobility of cars. Therefore, VANETs are vulnerable to a variety of attacks such as black-hole and grey-hole attacks. These attacks have a significantly dangerous influence on the availability of ITS, causing traffic disruption. In this paper, a blockchain-based model is proposed to provide a convenient and secure solution for ITS. Furthermore, it enables decentralized cooperation between cars and mutual trust is created using smart contracts. The experimental evaluation shows that the PDR rates of the proposed protocols achieve good results compared to previous routing protocols. However, the VCBC method gives a high rate of PDR than SCBC reaching 70% because of the high awareness of the sender car.

Keywords: Intelligent Transportation System, Vehicular Ad-hoc Network, Black-hole, Grey-hole, Blockchain, Smart Cities, Smart Contracts, Detection Method.

1 Introduction

Intelligent traffic management is an essential for the development of smart cities that utilizing an intelligent collaboration system to provide seamless traffic. In smart cities, Intelligent Transportation System (ITS) uses advanced communication technologies to link people with vehicles and facilities for secure and efficient transportation. ITS is composed of several technologies, such as Artificial Intelligence (AI) and the Internet of Things (IoT), that work together to improve vehicular communication and provide safe and well-organized transportation systems. Furthermore, ITS cooperating with Vehicular Ad-hoc Networks (VANETs) to improve the management of transportation systems, which considered essential for an ITS (Gillani et al., 2013). VANET is designed to improve traffic flow by enabling inter-vehicle communication and the transmission of real-time information about traffic congestion and road conditions (Abbasi et al., 2018). Moreover, VANET is a backbone of smart cities and ITS (Gómez-Arevalillo & Papadimitratos, 2017). It is an important part of the ITS since it enables and integrates numerous technologies and communications (Yang et al., 2019). ITS can link

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), volume: 14, number: 1 (March), pp. 126-143. DOI: *10.58346/JOWUA.2023.I1.011*

*Corresponding author: Assistant Professor, Department of Computer Science, College of Computer, Qassim University, Buraydah, Saudi Arabia.

smart vehicles, whether they are fully autonomous or semi-autonomous with driver-assistance technology.

While VANET enables vehicles to interact together connected directly by wireless links without the assistance of existing infrastructure or any other fixed network station, ITS is an autonomous system provide general web service access, facilitate the interchange of traffic information, and allow cooperative autonomy among entities. VANET is an ad-hoc network that allows wireless communications among its nodes. Therefore, cars in VANET have a responsibility of being a router to relaying traffic packages from a source to a destination (Lachdhaf et al., 2018). In this case, the vehicles act as a bridge between the sender and the receiver to relay data between them that are not able to communicate each other directly. However, due to the dynamic topology in VANET and the high mobility of nodes, links between nodes connect and disconnect in quick and frequent manner. As consequence of using wireless connections, the traffic information vulnerable to being accessed or altered by unauthorized nodes. Therefore, the lack of trust between the cars raises the risk of routing failures. Furthermore, there is probability of joining in relay process by unauthorized nodes if they pretend as legal nodes. Black-hole and grey-hole attacks are the most widespread active attacks that can threaten the reliability of the network. The black-hole attack occurs when every packet that passed through the malicious car are dropped. A black-hole attacker tries to trick every car in the network that wants to communicate with other cars by advertising itself as it has the shortest path to the destination car. On the contrary, a grey-hole attacker has unpredictable behavior about relaying the packet either participating in relay it or dropping it, so the probability of passing or dropping the packet by a grey-hole car is 50% (Ramezan, & Leung, 2018). Therefore, it is necessary to develop strong protocols that prevent malicious nodes from being chosen as relay nodes to provide a secure communication system. The efficient protocols must meet the network's security standards to prevent the VANET from being compromised by malicious vehicles that propagate false information or prevent critical communications from being delivered precisely in real-time. This work provides an insight into the potential of mitigating black-hole and grey-hole attacks through a secure ITS model based on blockchain technology.

This work provide insight into the potential of mitigating black-hole and grey-hole attacks through a secure ITS model based on blockchain technology. The proposed model provides a robust security mechanism against routing attacks that threaten ITS systems. In this work, the blockchain technology has examined to offer a secure routing throughout an immutable distributed ledger in Peer-to-Peer (P2P) networks. In blockchain, blocks are connected using hash pointers, so each hash links to the previous hash to create a chained ledger structure that prevents data tampering and enables data to be tracked back to its source. The data is stored in the distributed ledger in a transparent and decentralized manner and each node participate in this network has a copy of this ledger, which makes changing the ledger history is impossible. These advantages make the blockchain a suitable platform for a secure routing to enhance the trustworthiness between cars in VANET. Further, the smart contract approach enforces each contractual party to completely commit to the terms; otherwise, the process is terminated. So, if a car needs a path to reach another car with an indirect connection, it makes a smart contract via the blockchain with its terms. Consequently, this protocol makes it possible for cars in an ITS to cooperate and trust each other during routing process.

The remainder of the paper is organized as follows: Section 2 introduces a background of VANET and the utilized technology. Section 3 reviews some related works with traditional and blockchain based methods in routing approaches. Section 4 presents and the proposed blockchain-based routing protocol. Section 5 shows the experimental analysis and Section 6 concludes the paper.

2 Background

2.1. VANET Architecture

In ITS, it is planned that every region, vehicle, driver, infrastructure, and even pedestrian would be linked to the vehicular system. This connection will make them aware of local or statewide occurrences and will update the transportation system in real-time. Therefore, ITS will offer and exploit real-time and non-real-time information for safety and efficiency (Hartenstein & Laberteaux, 2010). Consequently, smart vehicles are designed to collect large amounts of data via the electronic control systems embedded within them. This data has been stored onboard by the vehicles but has been processed by only the manufacturers. Data collected by the vehicles can be utilized for various purposes such identify and quickly locating the available parking spaces, safety, or reducing traffic congestion. Figure 1 shows the general components of the basic system model in VANET, which are:

- **On-Board Unit (OBU):** Each vehicle inside the network is equipped with an OBU that connects with roadside units (RSUs) and other OBUs. It includes processors, sensors, storage devices, and systems. The gathered information by sensors is converted into messages and then wirelessly transferred to the nearby vehicle.
- **Roadside Unit (RSU)** The roadside units are non-moving devices that are placed at stationary positions along the roadway. They are equipped with transmission devices that facilitate Dedicated Short-Range Communications (DSRC) and infrastructure communication. RSU offers real-time services like internet access, navigation, and closely monitoring of traffic conditions and accident scenarios. In addition, extend the transmission range of VANETs by relaying messages to further RSUs and OBUs.
- **Trusted Authority (TA)** The trusted authority supervises and manages the whole network as administrator. It established a connection with RSUs through a wired channel. In addition, it is responsible for broadcasting and creating the system's periodic network updates. Further, it authenticates vehicles and eliminates those that exhibit harmful behavior or send fraudulent messages. Consequently, in comparison to OBU and RSU, TA has a large storage capacity and a great computational power.

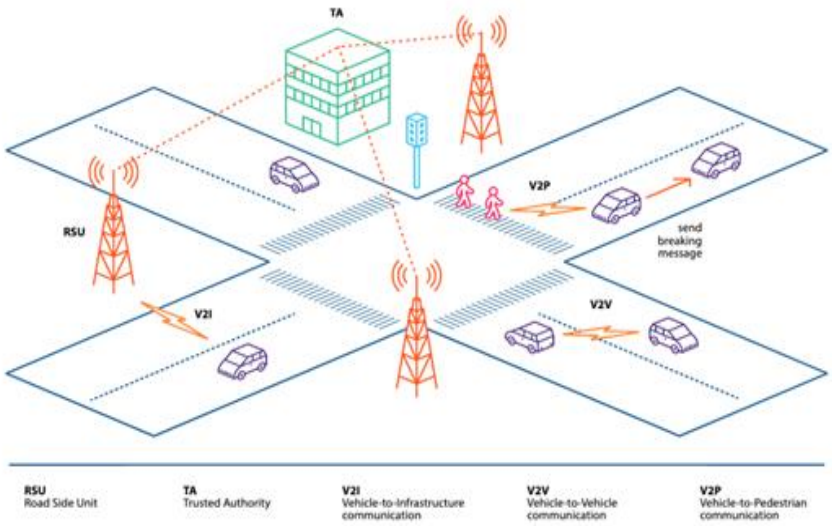

Figure 1: An Overview of the Proposed Architecture Components in VANET

2.2. Communication in VANET

ITS focuses on providing secure vehicular communication by utilizing VANET. Vehicle to Everything (V2X) communication plays a crucial role in ITS to enhance traffic safety and efficiency by providing real-time and accurate information such as collision warning, traffic congestion warning, road bottleneck information, emergencies, and other transportation services (Cheng et al., 2017). In V2X communication, the information can be exchanged between Vehicle to Vehicle (V2V), Vehicle to Infrastructure (V2I), and vehicle to pedestrians (V2P). In V2V, vehicles may share vital information such as traffic conditions, emergency braking, and accident detection with each other. While V2I is used to transfer data between network infrastructures and vehicles. In V2I communication, the vehicle established a connection with RSUs to share data with other networks, such as the Internet. Consequently, V2I needs a greater bandwidth for transmission than V2V (Kaushik, 2013).

2.2.1 VANET Characteristics

The VANET consists of moving vehicles that are connected to form a peer-to-peer infrastructure-less network. It is reliable, highly dynamic, and offers multiple services. Although VANET is an ad-hoc network and closely related to Mobile Ad-hoc Network (MANET), the vehicular networks show unique characteristics compared to MANET and other ad-hoc networks. These characteristics are essential for the security and privacy of VANETs (Dhamgaye & Chavhan, 2013), which are:

- **High Mobility:** Compared to MANETs, VANETs have high mobility. Consequently, vehicles moving at high speeds may delay V2V communication.
- **Dynamic Network Topology:** Because of the high mobility of vehicles, the topology of VANETs rapidly changes. As a result, VANETs become more vulnerable to attacks, and it becomes more difficult to identify malicious vehicles.
- **Computing and Storage:** Processing, calculating, storing, and transmitting a huge volume of data transmitted between vehicles and infrastructures is crucial and challenging in VANETs.
- **Time Critical:** VANET nodes share information in real time, therefore any choice or action must be done immediately after receiving the information.
- **Volatility:** It is difficult to ensure security in VANETs since the connections between vehicles may be lost or stay active after a few wireless hops (Lu et al., 2019).

2.2.2 VANET Security Requirements

The interaction between vehicles is temporary because vehicles frequently change their neighborhood. Moreover, V2V communication enables information exchange between vehicles without an infrastructure. In V2V, vehicles in VANET should accurately inform the traffic conditions in real-time, which makes VANET more sensitive to breach attacks. Additionally, vehicles need to trust the data relayed by other vehicles. However, the authentication process of vehicles requires revealing the identity of vehicles. Therefore, drivers are vulnerable to privacy breaches because of revealing their identities.

Furthermore, the lack of vehicle authentication to protect privacy may result in the transmission of harmful messages (Talat et al., 2019). To ensure non-repudiation, the vehicle's identification may be revealed if required by law via the use of conditional privacy. The inability to fulfill the requirements of VANET security services make this network vulnerable to threat or attacks. These requirements are divided into five primary domains (Raya & Hubaux, 2007): availability, confidentiality, authenticity, data integrity, and non-repudiation. Figure 2 show VANET security services and their threats and attacks.

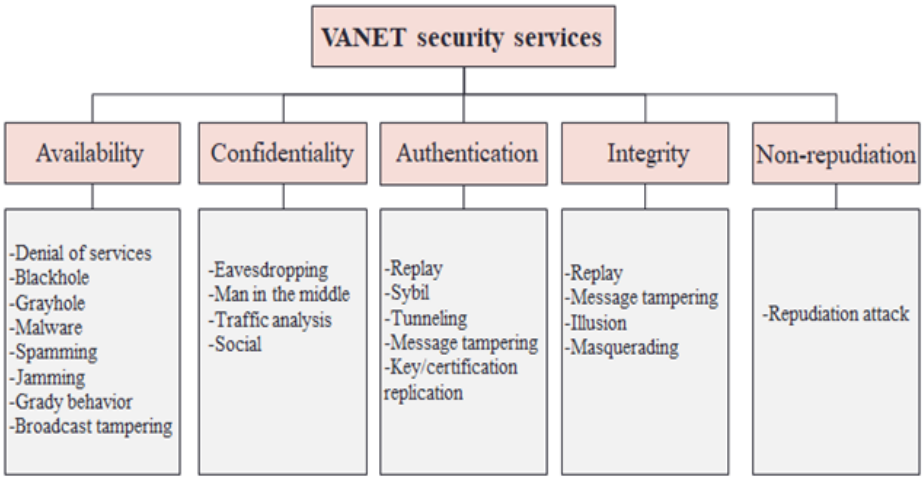

Figure 2: VANET Security Services and their Threats and Attacks

- **Availability:** It is critical in VANET security services because it is closely related to all safety applications. It ensures that the components of the network remain available under any threat (Qian & Moayeri, 2008).
- **Confidentiality:** It ensures that the safety message or relayed information reaches its destination in its original format. Only authorized members have access to view or read the message's contents, which are protected by certificates and shared public keys.
- **Authentication:** It plays a crucial role in VANETs because it prevents unauthorized members from engaging in the network.
- **Data Integrity:** It ensures that no changes or updates are made to the messages while they are transmitted over the network. In VANET, that can be ensured by the cryptography revocation process and the public key infrastructure (Kerrache et al., 2016).
- **Non-Repudiation:** It ensures that the message is owned by the sender. This attribute is essential due to the possibility of sending malicious messages via the network.

2.2.3 VANET Issues and Challenges

The critical issues that might impact security techniques to constructing a secure network are highlighted in (Arif & Rani, 2011), which are:

- **Network Volatility**: Data communication between nodes is temporary. As a result, the link may be established for a short time and then terminated due to vehicle movement.
- **Privacy:** The user's privacy should be protected. Also, the user’s information should be embraced by an authorized member.
- **Time-Sensitive:** Some applications and messages should arrive at their destination with as little delay as possible. Therefore, when designing the routing approach, a minimal transmission latency should be considered.
- **Ad-Hoc Mode:** In VANET, all the vehicles are connected in a wireless fashion. So it is necessary to create trust between vehicles.

Due to the lack of centralized management in ad-hoc networks, vehicles in VANET have extra responsibilities in the routing process. Hence, each vehicle that participates in the network also manages and controls the communication on that network. The links between vehicles frequently connect and

disconnect, which makes the routing process challenging due to characteristics of VANET discussed above, such as the high mobility of nodes and dynamic network topology. AODV protocol is the most reactive routing protocol frequently used in VANET (Rehman et al., 2017). But it is not designed to tackle security threats. So, it is prone to black-hole attack, grey-hole attack, sybil attack, wormhole attack. Recently, researchers have been identified more sophisticated attacks in VANET. Therefore, to overcome these attacks, some researchers proposed routing protocols and some enhanced existing protocols. However, it is still an interesting area for security research.

2.2.4 Routing Attacks in VANET

The dynamic topology and the repeated link breakage between vehicles due to their frequent movement raises the issue of maintaining a route for any vehicle in VANET. Furthermore, VANET is vulnerable to attack in the routing phase due to the decentralization, which makes vehicles work as routers. This attack has the potential to disable the whole network by interrupting all communication. Therefore, protecting security in the network layer is a necessary to protecting the whole network's security. Table 1 identifies common routing attacks stated in the network layer of VANET.

Table 1: The Description of Some Routing Attacks in VANET (Sleem et al., 2020)

Attack	Description
Denial of Service	It is one of the most harmful attacks in terms of availability. Its goal is to prevent users from accessing network services.
Sybil	The attacker in a Sybil attack can have several identities therefore, it is difficult to know whether the information received is from an authorized node or a malicious node.
Black-hole	In black-hole attack, malicious node either drop packets instead of forwarding them or reject participating in relaying process. Data loss can lead to denial-of-service attacks or man-in-the-middle attacks.
Grey-hole	It is a form of black-hole attack that relies on the idea of selective forwarding. Where the malicious nodes choose which packets to forward and which to drop. As a result of its suspicious behavior, the network's packet delivery ratio may degrade
Wormhole	It happens between two far malicious nodes in the network causing create non-existing roads.
Masquerading	The attacker in a masquerading attack poses as a reliable node to get a valid identity, by creating a black-hole or sending fake messages.
Replay	The attacker broadcasts a previously sent message to confuse the node and prevent it from determining the sender's identity.
Man in the middle	In this attack, the attacker takes place among communicating nodes then eavesdrop on their communication and injects the false information or modifies the exchanged messages between them.

Several routing protocols designed for VANETs have similar features, including self-management networks, self-organization, and a limited communication range. The main contribution of the routing protocols is to provide secure communication between vehicles. Routing protocols are classified into two types: The first type is proactive routing protocols, in which nodes send frequent messages to update their routing tables. The second type is reactive routing protocols, where the routes are created on-demand. The most common applications of routing protocol are OLSR for proactive routing protocol and AODV for reactive routing protocol (Rastogi et al., 2007). Common attacks on the network layer in VANET exploit vulnerabilities in routing protocols. In AODV, the attacker takes advantage of the concept of offering a route and then presents itself as having the shortest distance path to the target, despite the route being fake. The black-hole attack is an example where the malicious node uses AODV protocol for advertising itself as having the best route to a destination to intercept the packets. Therefore, the attacker gets the packets and never forwards them.

In VANET, the attacks on routing protocols are classified into active and passive attacks. In the active attack, the attacker interrupts the protocol's operations by attracting all packets to affect services' availability or disable the network. In the passive attack, the attacker does not interrupt the protocol's operation, but he tries to be eavesdropping the traffic. Therefore, it is challenging to defend against these attacks since they are difficult to detect. In this work, we focused on two types of attacks: the active attack (black-hole), and the passive attack (grey-hole). It is a challenge to discovering attack such as grey-hole due to its unpredictable behavior unlike black-hole. In the following, the explanation of the behavior of each attack:

- **Black-Hole Attack**

This type of attack targets the availability in VANET. In the black-hole attack, the malicious node participates in relaying process as a registered VANET user and pretends to contribute to the communicating operation. Nevertheless, it declines to contribute to the relaying process by disrupting the routing table and preventing the critical message from reaching its recipients (Mejri et al., 2014; Al-kahtani, 2012).

- **Grey-Hole Attack**

In the grey-hole attack, malicious nodes may drop or relay packets selectively. This makes it is difficult to predict the malicious behavior in a grey-hole attack.

When a source node demands a route due to AODV routing, it broadcasts an RREQ to its neighboring nodes. RREQs are disseminated throughout the network until the node with the optimal path to the destination is reached. As a response to RREQ, an RREP is sent back to the source. In the black-hole attack, a malicious node presents itself as having the shortest path to the destination. Then, once the source picks this route for usage, the malicious node rejects any data packets it receives instead of relaying to the next hop in the route to prevent communication between nodes.

Figure 3 shows the mechanism of the AODV routing protocol in case of no attacks in the network. A malicious node in a black-hole attack fraudulently responds to any RREQ it receives by advertising itself as having the shortest route possible or direct path to the destination. Therefore, when the malicious node starts to receive traffic messages to relay, it drops them. Figure 4 shows the impact of the black-hole attack on the availability of services in the VANET communication.

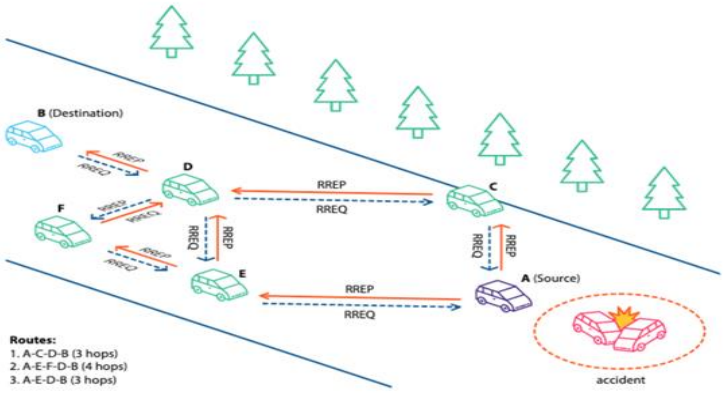

Figure 3: The Mechanism of the AODV Routing Protocol in Case of No Attacks in the Network. RREP Messages Replayed Back as a Response to the Source after an RREQ Reached the Destination

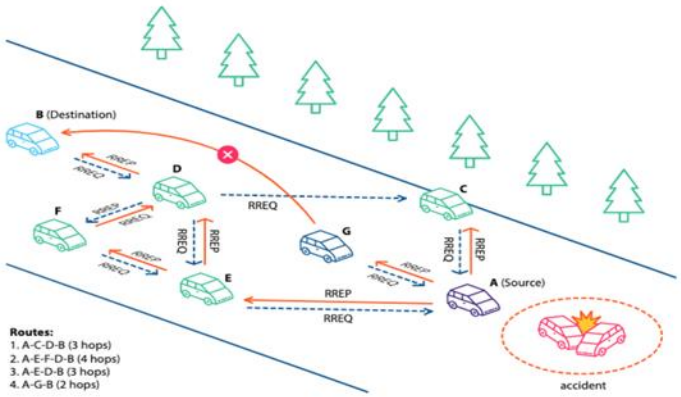

Figure 4: The Impact of the Black-hole Attack on the Routing Process in VANET. The Malicious Car Creates an RREP to Pretend as it has a Direct Route to the Destination

3 Related work

3.1. Traditional Trusted Routing Approaches for Black-hole and Grey-Hole Attacks

Several studies have focused on the black-hole attack in VANETs. The routing process in ad-hoc networks is at risk from black-hole attacks, which are not just restricted to the field of vehicular networking. In (Al-kahtani, 2012), the combination of trust tables and greedy geographic routing protocol improved node reliability. However, their approach is only appropriate for networks with low densities and straight-line traffic. Based on an intelligent Intrusion Detection System, researchers in (Alheeti et al., 2015) have developed a VANET black-hole detection method (IDS). This system can also be used to identify different black-hole attacks. However, it requires more computational resources and takes more time. In (Khamayseh et al., 2011), the authors suggested a system in which a trust table is used to store the trusted nodes. In their system, the RREP in the routing protocol is overloaded with the trusted value of the replying node. As a result, if a trusted node propagates the RREP, the source node sends out the packet. However, if other malicious nodes are present during the routing process, this system may fail to detect the black-hole node. In (Marti et al., 2000), they utilize an IDS where each node is connected to an IDS. Therefore, the whole network structure is monitored by this system. In order to defend against grey-hole attacks, the authors in (Schweitzer et al., 2016) have created a technique known as IMP, which is based on the enhancement of Denial Contradictions with Fictitious Node Mechanism (DCFM). Their mechanism improves routing decisions by employing two DCFM contradiction rules. Due to the attacker's behavior as a multi-point relay node (MPR), other nodes will make routing decisions based on the outcomes of current rules. The advantage of this method is that it reduces grey-hole attacks by up to 51% when compared to previously dropped packets. The research in (Rafique et al., 2016) is the other solution based on trust values when every node monitors a trust table beside to the routing table. Based on observations of forwarded or dropped packets, each node records the trust value of its neighbor node. In this study, the authors create a trust manager that is control of sending and receiving trust tables to and from RSUs. However, due to central trust management, the system fails in the extended network, resulting in communication delays. Furthermore, if the trust manager is compromised by a broadcast tampering attack, the entire network will be vulnerable to a single point of failure. Therefore as result, it may discard packets without forwarding or modifying the original message. Some solutions are based on the rewards approach, for example, the authors of (Zhong

et al., 2003) proposed a mechanism for rewarding each cooperating node for successfully routing data packets. To send a proof message using this mechanism, nodes must connect to a central administration system (such as a bank). The proof message verifies that the data packet was sent successfully. Furthermore, it also involves the node identities and digital signatures required to obtain bank rewards. However, this method is vulnerable to attacks, such as trying to forge a proof message to get rewards. As we have seen, the most of the proposed methods enhance the attack detection scheme. However, they had drawbacks such as scalability in (Almutairi et al., 2014) a problem of limited computing power in (Alheeti et al., 2015), and some like (Khamayseh et al., 2014) applied a decentralized trust management approach, which is not applicable in a large network. The transmission of multiple neighbor node trust scores to central trust management may result in network congestion and communication delays. As a consequence, this becomes critical in emergency situations. In the case of a broadcast tampering attack, the trust score procedure will fail if the intermediary nodes or the trust manager modify the original message or discard packets.

3.2. Blockchain-Based Routing Approaches for Black-hole and Grey-Hole Attacks

The necessity for a more reliable trust management system has motivated academics to investigate "blockchain," a revolutionary decentralized distributed technology that ensures trust in untrustworthy environments. Some researchers are concerned about misbehavior attacks that threaten the proper routing process, as in (David et al., 2018), the authors develop routing protocols using public ledger approaches and the node's reputation. The authors of (Yang et al., 2018) presented a learning scheme based on blockchain technology and trust. They use blockchain to prevent tampering with routing information. In addition, reinforcement learning is being integrated with blockchain to improve the routing process. Instead of the Proof of Work (POW) algorithm, they are using Proof of Authority (POA) to optimize resource consumption during the consensus stage. The authors of (Guehguih & Lu, 2019) propose a blockchain-based authentication and management technique for distributed data in VANETs. To meet their goals, they combined a private and public blockchain. After the vehicle enters the VANET via the private blockchain, the Trusted Authority (TA) on that private blockchain is in charge of verifying it. On the other hand, the public blockchain is in charge of guaranteeing message security during distribution across the network. However, this technique has significant computing and transmission overhead. The authors of Liu et al., 2019created a Confidentiality-Preserving Conditional Announcement System and a Blockchain-Based Trust Management Architecture for the Vehicular Network (BTCPS). Both the POW consensus method and the realistic Byzantine fault tolerance algorithm are used in this research. They presented a trust management architecture based on blockchain to ensure message synchronization and trustworthiness. They also suggested a technique to protect vehicle's privacy during relaying messages. The reliability of the communication is assessed using reputation values stored on the blockchain.

A secure trust-based blockchain architecture was presented by the developers of (Khan et al., 2019) to enhance security and privacy. The suggested approach uses blockchain technology's hashing algorithms and timestamps to keep transmitted messages up to date. Since timestamps document the precise moment at which a message was delivered and hashing protects against the message being altered by malicious nodes in the network, these techniques give defense against attacks that change or fabricate messages. This solution provide protection against manipulated messages attacks by malicious nodes in the network. Furthermore, they perform a message evaluation and trustworthiness approach to ensure trust among cars when exchanging information in the VANET. As a result, any car that transmits misleading signals to other vehicles on the network would receive negative values, lowering its trustworthiness. Vehicles with a trust value below the threshold will not have access to the network, and

their certificates will be revoked. In (Yang et al., 2018), a decentralized trust management scheme in vehicular networks using blockchain technology has been proposed. In this method, the maintenance of the blockchain performs at the RSU level and the validation of transactions done by integrating the PoW and PoS consensus mechanisms. The cars perform self-evaluations and send the findings to RSUs, which further compute the trust value of the cars and compile the information into a "block." RSUs working collaboratively to help in updating trusted blockchain by adding new "blocks". Each RSU maintains a trust blockchain that is continuously updated. RSUs, however, run the danger of becoming a target of attackers if they are overused. In (Tobin et al., 2018), the authors suggested an anonymous reputation system based on the blockchain to managing VANET reliability. They design a trust model that is based on the reputation of the relay node to increase the reliability of transmitted messages. Therefore, evaluation of vehicles reputation are relying on their broadcasted messages which are stored on a blockchain. Similarly, in (Careem et al., 2020), a blockchain-based decentralized trust management system in VANETs has been proposed using the Bayesian inference model to assess the reliability of received messages. Each vehicle can enquire about the status of its neighbors since the trusted values are stored in RSUs using blockchain. Moreover, a solution against black-hole attacks in VANETs has been suggested (Tobin et al., 2018). The system is designed to detect black-hole nodes using backtracking approach.

If the suspect node is shown to be operating maliciously, both the sender and recipient nodes can temporarily block it while protecting its blockchain data. However, their solution has been simulated in the network with a single malicious node. The authors of (Ramezan & Leung, 2018) have created blockchain-based contractual routing protocols for a network of suspicious nodes. To create a secure network, restrictions are placed between untrusted nodes using the smart contract. The source node verifies each hop routed to the smart contract, and malicious nodes are placed in a list. The packets are supposed not to pass through the blocked malicious node in this system. However, there is an issue if the malicious node pretend as it deliver the packets. All previous research have been reviewed, and it is noticeable that there are serious challenges that need to be fixed. Further investigation and testing are necessary to defeat black-hole and grey-hole attacks. Although there are many different security solutions for black-hole attacks already offered, many of them have significant disadvantages. A few of them build their proposals with the unrealistic assumption that there is only one malicious node. Additionally, some studies face a limitation when dealing with the Internet of Things (IoT) because of the high cost of computation and storage. Furthermore, some are vulnerable to a single point of failure when dealing with centralized management. Although prior researches has focused on enhancing security in VANET through utilizing blockchain, there are limitations to employing blockchain-based smart contracts to increase availability in VANET and protect routing processes against misbehavior attacks such as black-hole and grey-hole. As consequence, it is critical to implement up-to-date technology that tackles security issues associated with the routing process between vehicles in ITS.

4 Proposed Secure Blockchain-enabled Routing Protocol

Due to the decentralization in VANET, the cars acting as a routers in order to forwarding messages in the network. However, the high mobility of cars causes a rapid change in the network topology which makes issues facing researchers in getting accurate results. Therefore, because the topology on highways is more stable than that inside cities, the scenario of the test network in this work is proposed in a highway where the cars forward in a one direction. In the case of an accident, as shown in figure 3, the next car to the crushed car is trying to warn its previous cars. The warning message will keep forwarded until it reaches the destination.

4.1. Routing Process based Smart Contract Adaption

The proposed protocol depends on the idea of AODV routing protocol with some modifications for the smart-contract approach adaption. There are no pre-established routes in AODV, which implies that new routes are only built when they are needed. Route discovery mechanism in AODV based on query and reply cycles. Consequently, when a source node needs a route, it sends an RREQ to its neighboring nodes. RREQs are broadcasted through the network until the node with a direct route to the destination is reached. As a response to RREQ, RREP is transmitted back to the source. The route information is stored in route tables of all intermediate nodes along the route. So, if the adjacent node to the source does not have a direct path to the destination, it will forward an RREQ to its adjacent nodes again. This protocol is applicable due to the architecture of cooperative multi-hop networks such as VANET. In the developed proposed protocol, if a vehicle needs a path to a specific vehicle with an indirect connection, it makes a smart contract via the blockchain with its terms overloaded with the destination's address. Broadcasting smart contracts follow the mechanism of broadcasting RREQ in AODV. Therefore, this contract will be broadcasted from the source vehicle to all the nearest vehicles with a direct connection. Later, the source vehicle can determine an appropriate route from the received list of offers to establish a route to the destination and broadcast the data packets. The robustness of the proposed protocol lies in its use of the blockchain, which offers a distributed routing data management system by storing all routing data on the blockchain. The architecture of the developed model consists of both multi-hop vehicular networks along with cooperative Blockchain network as shown in Figure 5.

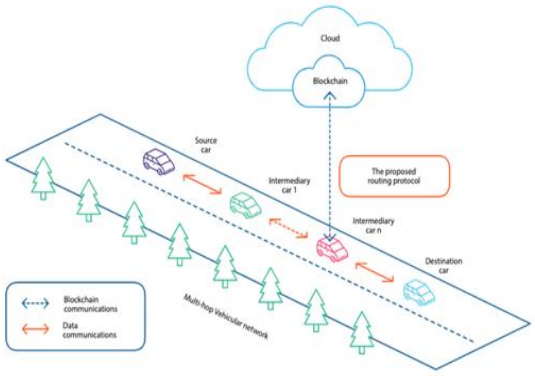

Figure 5: Decentralized Communications Network for Vehicular Network

4.2. System Design

The source, intermediary, and destination cars are integrated to made the multi-hop vehicular network. To relaying a packet in this network, the source car will initiate a request access to the destination. If there is no direct route to the destination, the packet will be picked up by an intermediary car and forwarded. The routing process in the conventional routing protocols is classified into two phases which are the establishment and the maintenance of the route. In the establishment phase, the source car sends a Route Request (RREQ) to the destination car to get the route offers then it will choose the best offer. When a destination or an intermediary car picks up the a Route Request (RREQ), it can response by a Route Reply (RREP) to the source. In this work, the proposed protocol designed to utilized the smart contract functions, where the Smart contract function invocations are used instead of control messages. Thus, the source can made the secure next hop relay by create a smart contract to mitigate unauthorized nodes. The processes of the proposed protocol are shown in Table 4.

Table 4: The Description of the Proposed Protocol Processes

Process	Description
Request	Invocation of the smart contract functions on the blockchain to access to a destination car.
Classify	Initially, each car is classified as a white car on the route that the sender car chooses to access the destination. This means the white car achieves a high delivered rate. However, if case a car is classified as a black and grey car, it means the car is a malicious car because they have a bad relaying performance. A car is classified as a black car in case it drops all packets that trying to pass through. A car is classified as a grey car in case it has unpredictable behavior.
Route	There are two routing approaches, including self-classification and vote-based classification. The former is applied when the sender has no prior knowledge about the status of its neighbors. The latter is applied when the sender has a minimum awareness about the trust value of its neighbors.

4.3. Reputation

The idea of reputation-based routing is the capacity to observe a node's behavior, then acquire and hold information about that node to assess the reputation process in a completely distributed way throughout trustless node. In (Careem et al., 2020), the authors monitored the transmission of wireless packets between nodes by establishing transactions that record the behaviors as good or bad and then using the blockchain to keep track of them. Thus, all nodes validate these actions by using a PoW or PoS methods. In the developed protocol, the reputation approach has been used in two different ways as follow:

- **Self Based Reputation:** In this method, the vehicle depends on itself to discover the best route even there is a malicious vehicle in this route because it does not have prior knowledge about the vesicle's status. Therefore, this will cause a high error rate. However, after many routings, the success rate will be improved.
- **Voting Based Reputation:** This method depends on others feedback and their observations about a specific vehicle's behavior. Therefore, the detection rate will be high and by this method, the malicious node whether it is a black-hole or grey-hole can be avoided.

4.4. Self-Classification Blockchain based Contract

In this method, the source car does not aware about the status of its neighbors. Therefore, the classification here depends on the Packet Delivery Ratio (PDR) which is the ratio of the number of successes delivered packets to the total number of sending packets. This ratio is referred to as rating in the update Node function. The car classified as black-hole if it is does relay any packet (rating=0), however, if the car delivers some packets and drop another and its rating does not exceed a predefined threshold, then the car classified as a grey-hole. Cars that achieve a high rating results over than the threshold will be classified as white cars and recorded as an authenticated node for later relaying in the AODV routing protocol. Initially, each node classified as white, then, after the update Node function invocation it can be considered as black, grey or white node.

4.5. Voting-Classification Blockchain based Contract

In contrast to self-classification blockchain based contract, in the source car in voting-classification Blockchain based contract gets knowledge about the degree of trust of its neighbors through a voting dataset. The complete dataset of reputation can be obtained (through the make Voting function) based on the trust values that assigned to each node in the network. Therefore, this function enables the source car in selecting trusted nodes whose reputation values are white. However, if some nodes fail to relay, the classification will follow the self-classification blockchain based contract procedure, which is based on PDR.

5 Experimental Analysis

In this section, we introduce an evaluation of the proposed protocol that contains two methods which are: self-classification blockchain based contract and voting-classification Blockchain based contract. The assessment of their performance is applied in a completely decentralized management network. Moreover, we simulate a network scenario under threaten of black-hole and grey-hole attacks to examine the effect of these attacks on SCBC and VCBC methods. To investigate the ability of applying our proposed protocol, we use Ethereum platform which is a public blockchain that provide a runtime environment for writing smart contracts. We achieved the results by using solidity language in Remix IDE on, which allows writing solidity-based smart contracts directly from the browser. The main metrics that our evaluation process based on are: Packet Delivery Ratio (PDR), Throughput (TP) and Routing Overhead (RO). In addition, the results of self-classification blockchain based contract and voting-classification Blockchain based contract methods are compared with BCR protocol in (Ramezan & Leung, 2018).

5.1. Experiment Setup

The scenario of the test network in this work proposed in a highway where the test cars forward in one direction due to the stability of topology on highways unlike the topology inside the cities. when an accident happens on the highway the previous car to the crushed car tries to send an alert to its previous car and the message will relay until reaches a specific car. To analyze the network topology, we use simulations and quantitative experiments for the network topology with 7 cars. The findings of the experiment based on the assumption that the source car may reach the destination through three possible routes as shown in Figure. Therefore, we analyze the effectiveness of the self-classification blockchain based contract (SCBC) and voting-classification Blockchain based contract (VCBC) algorithms against black-hole and grey-hole attacks. In a black-hole attack, the malicious car acts as a relay candidate that offers incorrect routes to discard sender packets and cause disruption. While in grey-hole attacks, the malicious car confused its neighbors whether it is malicious or not because it may forward or drop data packets. As we declared before, the evaluation process was based on several metrics which are: Packet Delivery Ratio (PDR), Throughput (TP) and Routing Overhead (RO).

5.2. Results Analysis

The outcome of this research shows the positive results to support the applying of blockchain-based smart contracts in VANET applications. Through the experiments, we noticed that SCBC and VCBC methods achieved the expected target perfectly. In this section, we introduce a detailed discussion of the experiment and their results. For the simulation, we suppose that the sender has three possible routes for relaying packets to the destination. The routing mechanism in SCBC and VCBC methods follows the AODV protocol approach, in which relay nodes are chosen depending on their hop counts to the destination. Whereas the ability of the source to increase its awareness about its neighbor's status after many sending shows the strength of SCBC and VCBC methods. In this work, to judge whether a relay node is black, grey, or white, we built our proposed model to allow at least two relay time. The model can classify a car as black in a black-hole attack after two unsuccessful deliveries. Unlike black-hole, discovering grey-hole attack takes a long time due to unpredictable behavior of its attacker. Therefore, if the rate of delivered packets to all packets sent by the source through a specific car is under a predefined threshold, this car classifies as grey. In SCBC, the awareness of the source improves as PDR increases after each successful relay.

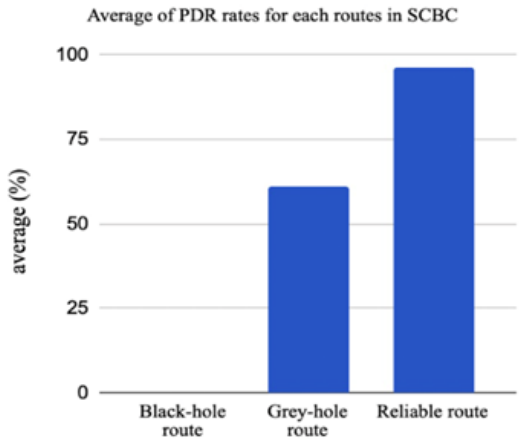

Figure 6: PDR Results of SCBC Method for Each Route in the Network. First Route Contains Black-hole car. Second Route Contains Grey-hole Car. While Third Route is Supposed to be Reliable

We examine our model in a virtual network with the assumption of existing two malicious cars. We suppose that first route contains black car that represents black-hole attack, second route contains grey car that represents grey-hole attack, and third route represent secure route. Figure 6 shows the PDR of SCBC for each route in the network. The source in SCBC method does not aware about the status of its neighbors which may lead to select a route with black-hole or grey-hole node. In this relying, the PDR for the route that contains black-hole node is zero that means no packets are delivered, then the car that receive these packets is blocked and denoted as black. In route of grey-hole node, the PDR is up to zero but under the predefined threshold which means some packets is delivered and others is not. Therefore, this node is denoted as grey, and this route is blocked. The PDR in the third route achieves values above the predefined threshold of 50%.

In contrary to SCBC method, the source in VCBC method takes knowledge about its neighbors from voting dataset to make a decision. Therefore, the probability of select a maliciously route is too low. However, if there is node has incorrect reputation value, the sender will discover that after many sendings by the same approach in SCBC method. For the VCBC senario, we suppose that black car recorded by miners in voting dataset as white. Unfortunately, the sender may choose this route as the shortest route to the destination without realizing it is malicious. Therefore, the voting dataset will be updated after many sendings and the status of black car will be correctly classified and the first route will be blocked. The source already aware about the grey car in the second route, so it will try a third route which is reliable. As consequence, the PDR of the third route gives positive results above the predefined threshold. The VCBC method takes less tries than the SCBC method to identify a trustworthy route.

To examine our results, we make a comparison of the proposed protocols (SCBC and VCBC) with BCR protocol in (Ramezan & Leung, 2018) based on PDR, TP, and RO performance. As shown in Figure 7, the average rate of PDR in BCR protocol is 35% in the presence of two malicious nodes in the network. In contrast, SCBC and VCBC achieve high PDR results and could increase as sender awareness increases. In Figure 8, the comparison between the protocols for the TP performance shows that VCBC gives high results exceed 0.5 kbps. However, high RO ratio in SCBC and VCBC compering to BCR protocol explains the sender efforts to find a trusted car to make a relay via frequent exchanged message. As shown in Figure 9, because of less awareness of the sender, RO in SCBC higher than RO in VCBC.

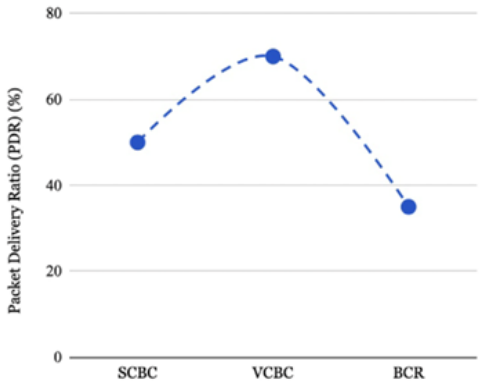

Figure 7: Comparison of SCBC and VCBC with BCR Protocol based on PDR Performance. As Shown, SCBC and VCBC Achieve High PDR Results and have the Ability to Increase as Sender Awareness Increases

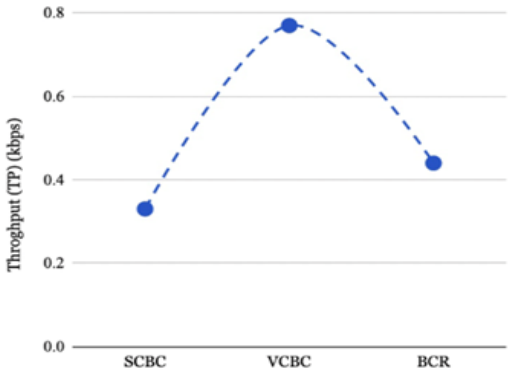

Figure 8: Comparison of SCBC and VCBC with BCR Protocol based on TP Performance. As Shown, VCBC gives High Results Exceed 0.5 kbps

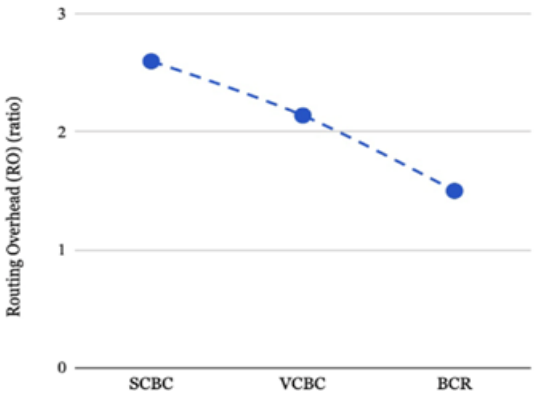

Figure 9: Comparison of SCBC and VCBC with BCR Protocol based on RO Performance. As Shown, RO is Higher in SCBC and VCBC than in BCR which Explains the Sender Efforts to Find a Trusted Car to make a Relay Via Frequent Exchanged Message

6 Conclusion

VANET security can be compromised due to the openness of communication where untrusted nodes can participate in the relaying process such as black-hole or grey-hole. In this research, we have proposed smart contract protocols based on blockchain for a secure routing in VANET. The proposed protocol contains two methods which are: SCBC and VCBC. The SCBC applied when the source car does not aware about the neighbor's status. While the VCBC applied when the source car has previous voting values for the cars in its network domain. Thus, due to the high awareness level of the source car in VCBC about the status of its neighbors, the PDR rate of VCBC gives high positive results. Whereas, in the SCBC, the source car's efforts to find the trusted car which result in an increase in the routing overhead. To assess our protocol, we make a comparison between the protocol methods: SCBC and VCBC with a previous routing protocol BCR. Compared to SCBC and BCR, we find that the VCBC achieves early high PDR rates that reach 70%. Further, the TP performance of VCBC is higher than SCBC and BCR. Therefore, even in the presence of black-hole and grey-hole attacks, our findings showed that the VCBC approach achieves positive results in PDR and TP performance. These positive results can be applied to other ad-hoc networks.

7 Acknowledgement

The authors gratefully acknowledge Qassim University, represented by the Deanship of Scientific Research, on the financial support for this research under the number (COC-2022-1-3-J- 31431) during the academic year 1444 AH / 2022 AD.

References

[1] Abbasi, I.A., & Shahid Khan, A. (2018). A review of vehicle to vehicle communication protocols for VANETs in the urban environment. *future internet*, *10*(2), 1-15.

[2] Alheeti, K.M.A., Gruebler, A., & McDonald-Maier, K.D. (2015). An intrusion detection system against malicious attacks on the communication network of driverless cars. *In 12th Annual IEEE Consumer Communications and Networking Conference (CCNC)*, 916-921.

[3] Al-Kahtani, M.S. (2012). Survey on security attacks in vehicular ad hoc networks (VANETs). *In IEEE 6th international conference on signal processing and communication systems*, 1-9.

[4] Almutairi, H., Chelloug, S., Alqarni, H., Aljaber, R., Alshehri, A., & Alotaish, D. (2014). A new black hole detection scheme for VANETs. *In Proceedings of the 6th International Conference on Management of Emergent Digital Eco Systems*, 133-138.

[5] Arif, M., & Rani, T. (2011). Enhanced ant colony-based routing in MANETs. In *Proceedings of 5th IEEE International Conference on Advanced Computing & Communication Technologies, Panipat, India*, 48-54.

[6] Careem, M.A.A., & Dutta, A. (2020). Reputation based Routing in MANET using Blockchain. *In IEEE International Conference on Communication Systems & Networks (COMSNETS)*, 1-6.

[7] Cheng, X., Chen, C., Zhang, W., & Yang, Y. (2017). 5G-enabled cooperative intelligent vehicular (5GenCIV) framework: When Benz meets Marconi. *IEEE Intelligent Systems*, *32*(3), 53-59.

[8] Colace, F., De Santo, M., Lombardi, M., Mosca, R., & Santaniello, D. (2020). A Multilayer Approach for Recommending Contextual Learning Paths. *Journal of Internet Services and Information Security*, *10*(2), 91-102.

[9] David, B., Dowsley, R., & Larangeira, M. (2018). MARS: Monetized ad-hoc routing system (a position paper). *In Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems*, 82-86.

[10] Dhamgaye, A., & Chavhan, N. (2013). Survey on security challenges in VANET. *International Journal of Computer Science*, *2*(1), 88-96.

[11] Gillani, S., Shahzad, F., Qayyum, A., & Mehmood, R. (2013). A survey on security in vehicular ad hoc networks. *In Communication Technologies for Vehicles: 5th International Workshop, Nets4Cars/Nets4Trains, Villeneuve d'Ascq, France, May 14-15. Proceedings 5*, 59-74. Springer Berlin Heidelberg.

[12] Gómez-Arevalillo, A.D.L.R., & Papadimitratos, P. (2017). Blockchain-based public key infrastructure for inter-domain secure routing. In *International workshop on open problems in network security (iNetSec)*, 20-38.

[13] Guehguih, B., & Lu, H. (2019). Blockchain-based privacy-preserving authentication and message dissemination scheme for vanet. *In Proceedings of 5th International Conference on Systems, Control and Communications*, 16-21.

[14] Hartenstein, H., & Laberteaux, K.P. (2010). VANET: Vehicular Applications and Inter-Networking Technologies.

[15] Kaushik, S.S. (2013). Review of different approaches for privacy scheme in VANETs. *International Journal of Advances in Engineering & Technology*, *5*(2), 356-363.

[16] Kerrache, C.A., Calafate, C.T., Cano, J.C., Lagraa, N., & Manzoni, P. (2016). Trust management for vehicular networks: An adversary-oriented overview. *IEEE Access*, *4*, 9293-9307.

[17] Khamayseh, Y., Bader, A., Mardini, W., & Yasein, M.B. (2011). A new protocol for detecting black hole nodes in ad hoc networks. *International Journal of Communication Networks and Information Security*, *3*(1), 36-47.

[18] Khan, A.S., Balan, K., Javed, Y., Tarmizi, S., & Abdullah, J. (2019). Secure trust-based blockchain architecture to prevent attacks in VANET. *Sensors*, *19*(22), 1-27.

[19] Lachdhaf, S., Mazouzi, M., & Abid, M. (2018). Secured AODV routing protocol for the detection and prevention of black hole attack in VANET. *Advanced Computing: An International Journal (ACIJ)*, *9*(1), 1-14.

[20] Liu, X., Huang, H., Xiao, F., & Ma, Z. (2019). A blockchain-based trust management with conditional privacy-preserving announcement scheme for VANETs. *IEEE Internet of Things Journal*, *7*(5), 4101-4112.

[21] Lu, Z., & Czap, L. (2018). Modelling the tongue movement of Chinese Shaanxi Xi'an dialect speech. *In IEEE 19th International Carpathian Control Conference (ICCC)*, 98-103.

[22] Lu, Z., Qu, G., & Liu, Z. (2018). A survey on recent advances in vehicular network security, trust, and privacy. *IEEE Transactions on Intelligent Transportation Systems*, *20*(2), 760-776.

[23] Marti, S., Giuli, T.J., Lai, K., & Baker, M. (2000). Mitigating routing misbehavior in mobile ad hoc networks. In *Proceedings of the 6th annual international conference on Mobile computing and networking*, 255-265.

[24] Mejri, M.N., Ben-Othman, J., & Hamdi, M. (2014). Survey on VANET security challenges and possible cryptographic solutions. *Vehicular Communications*, *1*(2), 53-66.

[25] Qian, Y., & Moayeri, N. (2008). Design of secure and application-oriented VANETs. *In VTC Spring IEEE Vehicular Technology Conference*, 2794-2799.

[26] Rafique, N., Khan, M.A., Saqib, N.A., Bashir, F., Beard, C., & Li, Z. (2016). Black hole prevention in vanets using trust management and fuzzy logic analyzer. *International Journal of Computer Science and Security*, *14*(9), 1226-1231.

[27] Ramezan, G., & Leung, C. (2018). A blockchain-based contractual routing protocol for the internet of things using smart contracts. *Wireless Communications and Mobile Computing*.

[28] Rastogi, D., Ganu, S., Zhang, Y., Trappe, W., & Graff, C. (2007). A comparative study of AODV and OLSR on the ORBIT testbed. *In MILCOM IEEE Military Communications Conference*, 1-7.

[29] Raya, M., & Hubaux, J.P. (2007). Securing vehicular ad hoc networks. *Journal of computer security*, *15*(1), 39-68.

[30] Rehman, S.U., Khan, M., Zia, T., & Zheng, L. (2013). Vehicular ad-hoc networks (VANETs): an overview and challenges. *Journal of Wireless Networking and communications*, *3*(3), 29-38.
[31] Schweitzer, N., Stulman, A., Margalit, R.D., & Shabtai, A. (2016). Contradiction based gray-hole attack minimization for ad-hoc networks. *IEEE Transactions on Mobile Computing*, *16*(8), 2174-2183.
[32] Sleem, L., Noura, H.N., & Couturier, R. (2020). Towards a secure ITS: Overview, challenges and solutions. *Journal of Information Security and Applications*, *55*.
[33] Talat, H., Nomani, T., Mohsin, M., & Sattar, S. (2019). A survey on location privacy techniques deployed in vehicular networks. *In IEEE 16th International Bhurban conference on applied sciences and technology (IBCAST)*, 604-613.
[34] Tobin, J., Thorpe, C., & Murphy, L. (2017). An approach to mitigate black hole attacks on vehicular wireless networks. *In IEEE 85th vehicular technology conference (VTC Spring)*, 1-7.
[35] Yang, J., He, S., Xu, Y., Chen, L., & Ren, J. (2019). A trusted routing scheme using blockchain and reinforcement learning for wireless sensor networks. *Sensors*, *19*(4), 1-19.
[36] Yang, Z., Yang, K., Lei, L., Zheng, K., & Leung, V.C. (2018). Blockchain-based decentralized trust management in vehicular networks. *IEEE internet of things journal*, *6*(2), 1495-1505.
[37] Zhong, S., Chen, J., & Yang, Y.R. (2003). Sprite: A simple, cheat-proof, credit-based system for mobile ad-hoc networks. *In IEEE INFOCOM 2003. Twenty-second Annual Joint Conference of the IEEE Computer and Communications Societies*, *3*, 1987-1997.

Authors Biography

Mada Alharbi is a graduate student from Qassim University in Saudi Arabia, computer science department. She got her B.Sc. degree in Computer Science from Qassim University, Saudi Arabia in 2015. She completed her M.Sc. degree in Computer Science from Qassim University, Saudi Arabia in 2022. Cryptography is her research interest.

Abdulatif Alabdulatif is an Assistant Professor at the School of Computer Science & IT, Qassim University, Saudi Arabia. He completed his Ph.D. degree in Computer Science from RMIT University, Australia in 2018. He received his B.Sc. degree in Computer Science from Qassim University, Saudi Arabia in 2008 and his M.Sc. degree in Computer Science from RMIT University, Australia in 2013. His research interests include applied cryptography, cloud computing, data mining and remote healthcare.