Computer Modeling in Engineering & Sciences

Tech Science Press

DOI: 10.32604/cmes.2023.029769

ARTICLE

Mitigating Blackhole and Greyhole Routing Attacks in Vehicular Ad Hoc Networks Using Blockchain Based Smart Contracts

Abdulatif Alabdulatif[1,*], Mada Alharbi[1], Abir Mchergui[2] and Tarek Moulahi[3,4]

[1]Department of Computer Science, College of Computer, Qassim University, Buraydah, 51452, Saudi Arabia

[2]Department of Computer Science, Higher Institute of Management of Gabes, Gabes University, Gabes, 6029, Tunisia

[3]Information Technology, College of Computer, Qassim University, Buraydah, Saudi Arabia

[4]Faculty of Science and Technology of Sidi Bouzid, Kairouan University, Kairouan, 3131, Tunisia

*Corresponding Author: Abdulatif Alabdulatif. Email: ab.alabdulatif@qu.edu.sa

Received: 08 March 2023 Accepted: 07 July 2023 Published: 17 November 2023

ABSTRACT

The rapid increase in vehicle traffic volume in modern societies has raised the need to develop innovative solutions to reduce traffic congestion and enhance traffic management efficiency. Revolutionary advanced technology, such as Intelligent Transportation Systems (ITS), enables improved traffic management, helps eliminate congestion, and supports a safer environment. ITS provides real-time information on vehicle traffic and transportation systems that can improve decision-making for road users. However, ITS suffers from routing issues at the network layer when utilising Vehicular Ad Hoc Networks (VANETs). This is because each vehicle plays the role of a router in this network, which leads to a complex vehicle communication network, causing issues such as repeated link breakages between vehicles resulting from the mobility of the network and rapid topological variation. This may lead to loss or delay in packet transmissions; this weakness can be exploited in routing attacks, such as black-hole and gray-hole attacks, that threaten the availability of ITS services. In this paper, a Blockchain-based smart contracts model is proposed to offer convenient and comprehensive security mechanisms, enhancing the trustworthiness between vehicles. Self-Classification Blockchain-Based Contracts (SCBC) and Voting-Classification Blockchain-Based Contracts (VCBC) are utilised in the proposed protocol. The results show that VCBC succeeds in attaining better results in PDR and TP performance even in the presence of Blackhole and Grayhole attacks.

KEYWORDS

Blockchain; data privacy; machine learning; routing attacks; smart contract; VANET

1 Introduction

The increase in population is directly proportional to traffic jams and accidents globally. Approximately one million people lose their lives in road crashes each year. As life grows and develops, a solution proportionate to modern technical progress becomes a significant necessity. The Intelligent Transportation System (ITS) addresses the need for a safe transportation network with an intelligent collaboration system to provide many safety requirements seamlessly. The main catalyst for this

network is to save human lives and enhance traffic efficiency. ITS is a construction of different technologies to improve vehicular communication to provide secured and well-organized transportation systems. Further, the Vehicular Ad Hoc Networks (VANET) are considered the most prominent approach of the ITS [1–3].

In VANET, the network is designed in an ad hoc manner in which different connecting devices and moving vehicles communicate wirelessly without preexisting communication infrastructure. Therefore, the lack of centralized management in VANET gives the vehicles the responsibility to play the role of a router forwarding traffic information from a source to a destination [4]. The vehicles use this information to become aware of the circumstances ahead or to collaborate with other vehicles to ensure safe operation. In the routing process, nodes work as a bridge between the sender and the receiver node to carry data between nodes that cannot reach each other directly. However, the links between nodes connect and disconnect quickly and frequently because of the extremely dynamic topology and the high mobility of nodes. Further, the use of wireless links to connect vehicles makes traffic information vulnerable to viewing or modification by unauthorized users. Therefore, protecting the accessibility of traffic information in VANET from misleading attacks such as black-hole and gray-hole attacks, is considered a major challenge of the routing process [5].

The black-hole attack is considered one of the most widespread active attacks that degrade the reliability of the network. These attacks occur when all incoming packets are dropped via the malicious node, as shown in Fig. 1. A black-hole node attempts to deceive every node in the network that wants to communicate with other nodes by pretending that it always has the shortest path to the destination node. Conversely, in gray-hole breaches, the attacker has unpredictable behaviour, so the probability of passing or dropping the packet by malicious nodes is 0.5, as shown in Fig. 2.

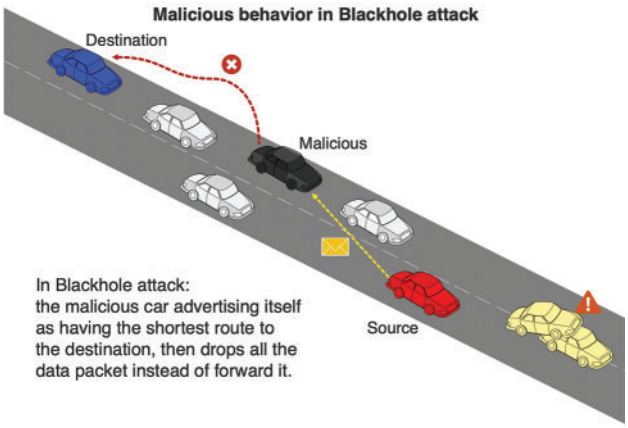

Figure 1: Malicious behavior in the black-hole attack: The malicious car advertising itself as having the shortest path to the destination

This work sheds light on the possibility of mitigating the previous types of attacks through a proposed secure ITS model based on blockchain technology. This model provides the required security mechanisms to protect ITS systems against critical security issues. The concept behind blockchain technology is that processes are not completed by one, but by many nodes simultaneously. Also, each node in the network has a complete image of the updated blockchain network, which makes changing the blockchain database history impossible. These characteristics make the blockchain technique a platform that facilitates the trustworthy exchange of data between independent parties.

The main contribution of this paper is to design and build a secure protocol that allows vehicles to communicate and cooperate with awareness and trust in ITS. Therefore, the vehicles can independently discover routes to their destination. The main contributions of this research are: Prevent black hole and gray hole attacks in ITS by using blockchain technology. Increase the security level in ITS by increasing the awareness of vehicles in VANET. Build an accurate and auto-execution system by utilizing smart contacts.

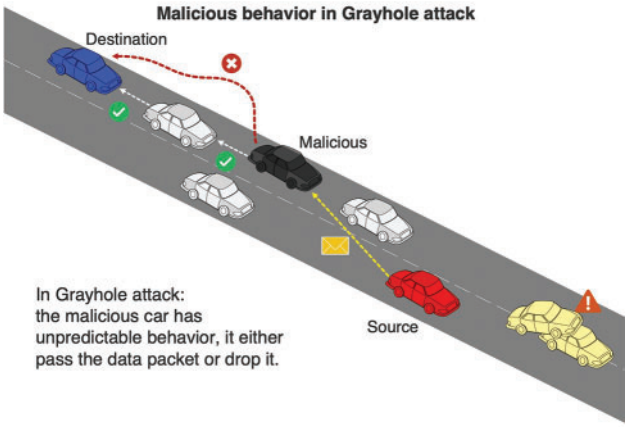

Figure 2: Malicious behavior in the gray-hole attack: The malicious car has unpredictable behavior

The proposed solution generates a blockchain-based model in which the trustworthiness of connections between nodes is guaranteed by placing their transactions in a public ledger, providing ground truth for further verification processes. Further, the proposed protocol utilizes smart contracts to discover the right route to a destination in a decentralized manner without the need for certificate authority. Hence, the route from a source to a specific destination can be guaranteed by intermediary nodes. This protocol enables vehicles in ITS to trust one another and cooperate during data communication.

The remainder of the paper is organized as follows: In Section 3, we review some related works with traditional and blockchain-based methods in routing approaches. In Section 4, we introduce and detail our proposed smart contract-based routing solution. In Section 5, we present the experimental evaluation of our contribution. In Section 6, we analyzed and interpret the obtained results and in Section 7, we conclude the paper.

2 Background

2.1 VANET Overview

VANET technology has become a popular area of study because it is a promising technology to improve vehicles communications in ITS [6]. The improvement of VANET technology in ITSs enables vehicular communications via Vehicle-to-Vehicle (V2V) communications. In VANET, the vehicle uses V2V communication to send and receive messages about traffic situations with nearby vehicles. Vehicles can use these messages to avoid accidents and drive to other safer roads. However, messages sent over an open wireless channel may put it at risk of being eavesdropped, modified, repeated, or deleted by an attacker.

2.1.1 Components of VANET

- **On-Board Unit (OBU):** Each vehicle inside the network is equipped with an OBU that connects with roadside units (RSUs) and other OBUs to enable wireless communication to the nearby vehicle.
- **Road Side Unit (RSU):** They are non-moving devices that are placed at stationary positions along the roadway. They offers real-time services like internet access and provide an extended communication range by relaying messages to further RSUs and OBUs.
- **Trusted Authority (TA):** The trusted authority supervises and manages the whole network by authenticating vehicles and eliminating those that exhibit harmful behavior or send fraudulent messages.

2.1.2 VANET Security Requirements

There are five security requirements that should be fulfilled to ensure a secure VANET, which are:

- **Availability:** It ensures that the components of the network remain available under any threat.
- **Confidentiality:** It ensures that the message reaches its destination in its original format.
- **Authentication:** It prevents unauthorized members from engaging in the network.
- **Data integrity:** It ensures that no changes are made to the messages while they are transmitted over the network.
- **Non-repudiation:** It ensures that the message is owned by the sender.

2.2 Blockchain Overview

Blockchain is emerged as a solution for VANETs because of its major characteristics such as decentralization, collaborative maintenance, redundant storage, and tamper-proof functionality. It incorporates the following techniques to produce trustworthy and secure systems:

- **The distributed ledger:** It contains all the transactions on the blockchain. Each node in the blockchain has a copy of the complete ledger which makes tampering with ledger information impossible.
- **Asymmetric encryption:** It is an authorization verification technology that uses different encryption keys.
- **Smart contract:** It consists of predefined code performed automatically by a blockchain miner, then confirmed by the consensus mechanism on the blockchain network.
- **The consensus mechanism:** It is a mechanism of rewarding nodes to participate in the block validation process.

3 Related Work

ITS is a cooperative system composed of vehicle nodes and different heterogeneous devices. In ITS, nodes can randomly move and communicate with one another directly or indirectly via wireless connections without any fixed infrastructure. Currently, securing vehicle communications in ITS is one of the biggest challenges faced by researchers. To introduce trust into ITS under several critical conditions, system designers should consider various aspects (e.g., node heterogeneity, rapid changes in network topology, and the lack of predefined trust relationships [7]). Therefore, to ensure safe routing

within the network, many researchers have introduced an authentication mechanism [8]. However, researchers have different perspectives on how they can avoid malicious nodes during the routing process. This section is divided into two parts. The first section reviews the traditional trusted routing approaches for improving routing security and reliability. The second section introduces the relevant research approaches to routing schemes using blockchain technology.

3.1 Traditional Trusted Routing Approaches

Generally, two types of routing protocols are widely utilized: Ad-Hoc On-Demand Distance Vector (AODV) and optimized link state routing (OLSR). AODV [9] is a reactive routing protocol, which means the routing request is sent on-demand. In AODV, when a vehicle wants to communicate with another, it broadcasts a route request and expects a response from the destination. OLSR is a proactive routing protocol based on updating routing information continuously to obtain a complete overview of network topology [10]. According to Sirisala et al. [11], the trustworthiness of the routing nodes is evaluated by a quality of service (QoS) routing algorithm. QoS trust of a node is calculated based on its multiple quality parameters, such as route request, route reply, route error and data packet. The QoS trust of the routing node is calculated by the transitive rule (e.g., A trusts B and B trusts C, then A trusts C). Chadha et al. [12] and Jain et al. [13] developed a different approach that assumes the first received route reply is usually from a black-hole node and the subsequent route reply messages are safe. Alternatively, Upadhyaya et al. [14] used the AODV protocol to implement three approaches for black-hole detection. The first approach is based on the awareness of neighbours each neighbour observes the trusted values of the others. Another approach is based on the identification of higher sequence numbers; if a source node receives a reply packet with the largest sequence numbers, this node will be considered malicious. The third approach depends on the packet drop rate calculated by the roadside unit (RSU), in which RSUs manage the list of trusted nodes and non-trusted nodes. Therefore, if the packet drop rate exceeds the threshold value, there is a black hole attack. Their first approach, based on the "reputation system" is commonly used by researchers. It evaluates the reputation of other nodes by the historical behaviours of the routing nodes. However, the reputation table may be tampered with, which means absolute integrity is difficult to guarantee.

3.2 Blockchain-Based Routing Approaches

Blockchain is a potential solution for trust management. It has proven its efficiency in various fields, including wireless networks and the Internet of Things [15]. Practically, the decentralized nature of blockchain technology is one of its advantages; this quality manages infrastructure-less environments in ITS. Moreover, because of the traceable and tamper-proof characteristics of the blockchain technique, many researchers combine it with routing algorithms to improve the trustworthiness between routing nodes. Careem et al. [16] improved the AODV routing protocol and increased the reliability of packet delivery by enhancing the trustworthiness and reputation of the participating nodes. They used a fraction of nodes to monitor the actions of other nodes, then classified the actions as "good" or "bad". These transactions are aggregated to generate one block by the consensus mechanism in the blockchain technique. Blockchain provides an immutable record of nodes' behaviours. Also, the increasing number of validators in the fraction ensures credibility. Lwin et al. [17] exploited the advantage of blockchain to build a distributed trust framework for the routing nodes with lightweight consensus. In this research, the overhead and repetition of the OLSR routing protocol are reduced because of the distributed and scalable trust between the routing nodes.

de la Rocha Gómez-Arevalillo et al. [18] proposed a trusted public key management framework secure blockchain trust management. Their approach replaces the traditional public key infrastructure

with a blockchain protocol, removing the dependence on central authentication and providing a decentralized routing system. However, the gaps in the previous schemes can be addressed with the use of smart contract concepts in the blockchain technique. Ramezan et al. [5] proposed a blockchain-based contractual routing protocol for routing networks with untrusted nodes. It utilizes the smart contract approach to help routing nodes find a trusted route to destination nodes. The main goal is that the source node confirms the arrival of the routing for each hop on the smart contract and records the malicious routing nodes as misbehaving nodes. Thus, the subsequent packets will never pass through a known malicious node.

4 Proposed System

In VANET, the relayed message moves from one car to another in a sequential manner without needing centralized management. The rapid change in VANET topology makes the bridge between cars broken many times which reflects on the difficulty of getting the best results in research. In this work, the scenario of the test network proposed in a highway where the test vehicles forward in one direction due to the stability of topology on highways, unlike the topology inside the cities. In the scenario described in Fig. 3, when an accident happens on the highway the previous car to the crushed car tries to send an alert to its previous car. Furthermore, the message will relay until reaches a specific car.

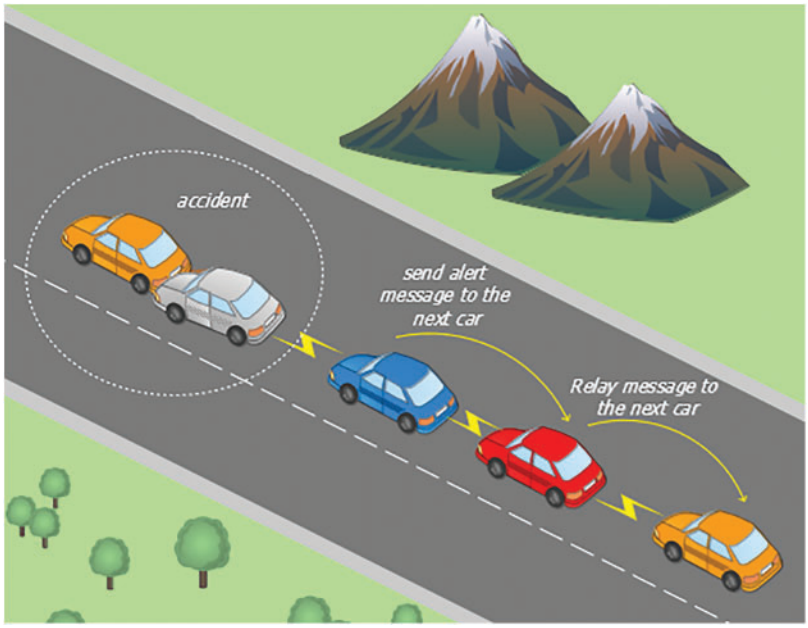

Figure 3: The proposed scenario is to test the network on the highway where the test vehicles forward in one direction

4.1 System Model

While the vehicles in VANET play the role of a router to relay a packet, the integrity and availability of exchanged information can be vulnerable to various security attacks. The proposed protocol aims to enhance the security of VANET by using blockchain technology where all transactions are

processed and stored in an immutable database. A smart-contract approach is applied to ensure that each party has to be committed to pre-defined terms; otherwise, the process will be cancelled.

This proposal protocol depends on the idea of Ad Hoc On demand Distance Vector (AODV) routing protocol with requisite modifications for the smart-contract approach adaption. AODV is a reactive protocol which means the routes are created only when needed. Route discovery in AODV based on the query and reply cycles. To require a route to another node, the source node broadcasts a routing request message (RREQ). The adjacent node to the source responds to RREQ and then sends RREP if it was the same as the destination's address. Otherwise, checking the routing table, if it finds a path to the destination send an RREP to the source or continue to relay RREQ [19]. In AODV, the route information is stored in route tables of all intermediate nodes along the route.

In this proposal protocol, if a vehicle needs a path to reach another vehicle through multi-hop relays, it calls a smart contract via the blockchain with its functions instead of sending RREQ. After this, the source vehicles can determine a route from the list of neighbours to establish a route to the destination for relaying the data packets. Furthermore, the robustness of the blockchain provides a distributed routing information management platform that records all the routing information in the blockchain. The architecture of the developed model consists of both multi-hop vehicular networks along with cooperative blockchain networks as shown in Fig. 4.

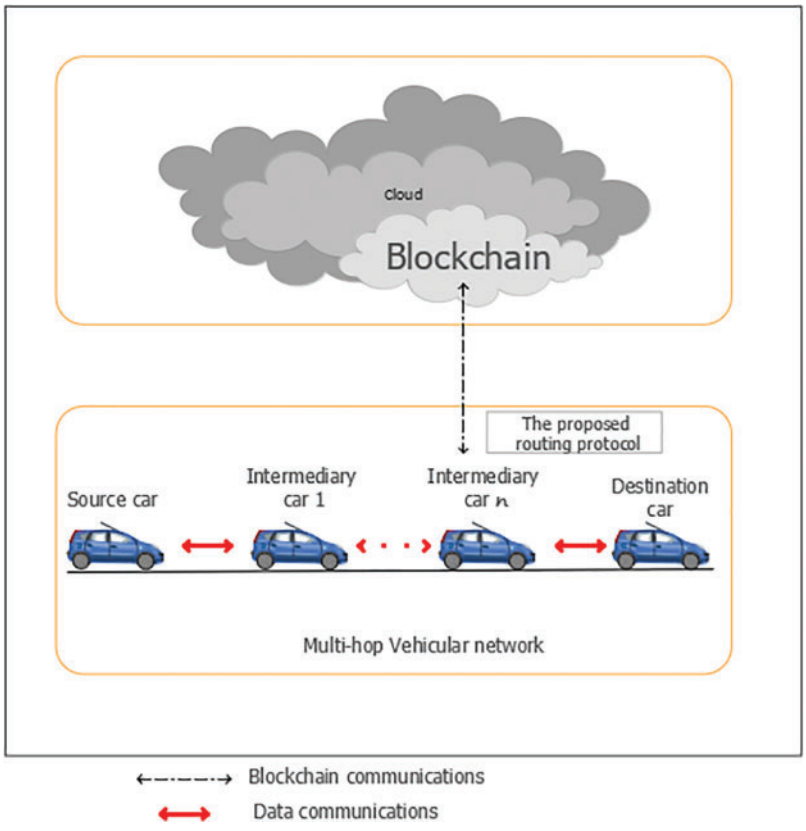

Figure 4: Setup for a decentralized communications network for the vehicular network

4.2 Multi-Hop Vehicular Network

VANET is a subform of Ad Hoc Networks that have no infrastructure and the communicating entities are vehicles. VANET depends on Peer-to-Peer (P2P) communication or multi-hop communication. Therefore, when a node tries to send data packets to other nodes which are out of its communication range, the packet can be forwarded via one or more intermediate nodes which are called "Multi-hop nodes".

A multi-hop vehicular network consists of a set of source cars, intermediary cars and destination cars. Furthermore, it does not provide central management for registration, authentication, or authorization. In case a source car requires to send data to a destination car, it establishes request access to send data to the destination. The car with no direct connection to the destination needs another car to relay its packets. The car that relays the source traffic to the destination is called an intermediary car as shown in Fig. 5.

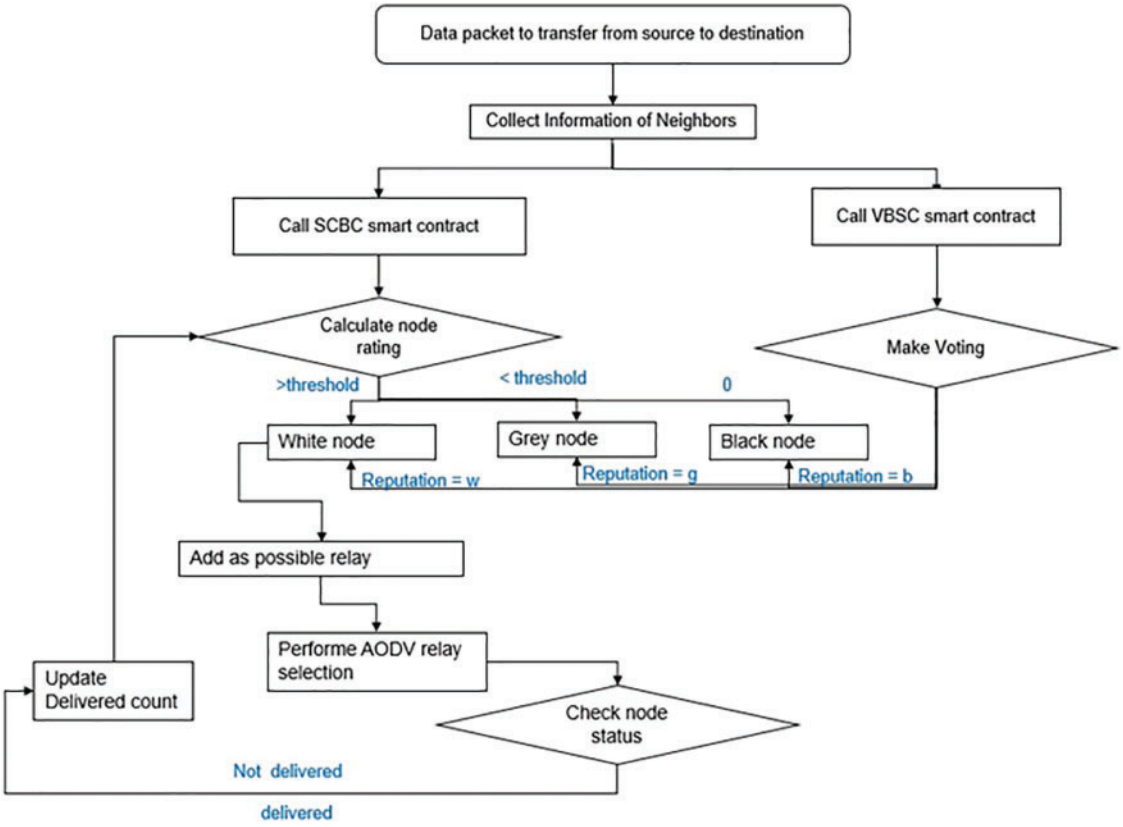

Figure 5: The state machine diagram of the proposed protocol: After collecting information of neighbors, one of the SCBC and VBSC smart contracts is called and the relay node is selected respectively based on calculated rating or reputation. Finally the AODV protocol is applied and the node sate is updated

4.3 The Proposed Routing Protocol Based Smart Contract

The conventional routing protocols consist of two phases; one for the route establishment and another for the route maintenance. In the route establishment phase, the source car sends a Route

Request (RREQ) message to find a route to the destination. When the RREQ packet is received by an intermediary or destination car they can respond by sending a Route Reply (RREP) message to the source car.

In the proposed protocol, each source car calls the smart contract to request the best next-hop relay avoiding malicious nodes. The proposed protocol is implemented using smart contracts within the blockchain. The cars request that the functions within the smart contract follow the proposed protocol. Thus, the transmission of control messages in existing routing protocols is replaced by smart contract function calls in the proposed protocol. Fig. 5 describes the state machine of the proposed protocol. In the protocol, the differentiation between nodes' status occurs when cars call some functions inside smart contracts. The processes of the proposed protocol can be defined as follows:

1. **Route request:** When a source car tries to send a packet to a destination car, it calls the smart contract through the blockchain network and using the information about its surrounding neighbours.
2. **Route response:** The smart contract performs a classification of all neighbours to avoid malicious cars. Two different types of classification are possible according to the prior common awareness about the considered neighbours in the network. Self-classification (SCBC) is performed in the case there is no prior knowledge about the degree of trust that can be assigned to the surrounding neighbours by a minimum subset of nodes in the network. However, in the other case; when a minimum awareness about the neighbours is available, a vote-based classification smart contract can be applied (VCBC).
3. **Classification of nodes:** By default, each intermediary car chosen by the source as having the best route to the destination is named a white car. A white car is a status for a car that behaves well in the relaying process; it means that it has a rate of successfully delivered relays beyond a threshold value. However, black cars and gray cars are classified as malicious due to their behaviour in the relaying process. A black car drops all packets, it received from the source car. Unlike a black car, a gray car has unpredictable behaviour in relaying the packet, it either drops it or makes it through. To differentiate between malicious types, the packet delivery ratio (PDR) and the threshold rate should be considered.

4.4 Self-Classification Blockchain Based Contract (SCBC)

In a self-classification-based contract, the source car does not have any knowledge about the status of its neighbours. The classification is then, performed only according to the ratio of the number of delivered relays to the total number of assigned relays. The value of this ratio is called rating in the updateNode function. If the node does not deliver any relay (rating = 0) then it is certainly a blackhole, however, if the rating value is under a predefined threshold, then the node is likely to be a greyhole node. Only nodes with a rating value superior to the threshold will be classified as white nodes and can be added as a potential relay for the AODV routing protocol. The overall SCBC protocol is detailed in Algorithm 1.

Algorithm 1: SCBC

```
Input: List of neighbors        ▷ N [n (nodeName, relayTime, deliveredCount, notDeliveredCount)]
Output: nodeStatus
foreach node n in N do
  R.push(Relay(nodeName, relayTime, "waiting"))        ▷ new relay
times ← deliveredCount + notDeliveredCount        ▷ counting times
```

(Continued)

Algorithm 1 (continued)

6: status ← updateRelay()
7: deliveredCount ← updateRelay (deliveredCount, status). deliveredCount
8: nodeStatus ← updateNode(deliveredCount, times)
9: **end for each**
10: **return** nodeStatus

Algorithm 2 shows how to update the status of the relay, i.e., if after a certain time, it has happened or not. Algorithm 3 shows how to update the node status. Node s is initially white. Next, depending on its performance and relay ratio, it can be considered grey or white.

Algorithm 2: Update relay

1: **function** updateRelay(status)
2: time ← block.timestamp
3: **if** (R. relayTime > time and R.relayTime <= (time + τ))
4: status ← "delivered"
5: **else**
6: status ← "not delivered"
7: **end if**
8: R.status ← status
9: **if** (status = "delivered")
10: deliveredCount ++
11: **else**
12: notDeliveredCount ++
13: **end if**
14: **end function**

Algorithm 3: Update node status

1: **function** updateNode (deliveredCount, times)
2: threshold τ
3: rate $= \dfrac{deliveredCount \times 100}{deliveredCount + notDeliveredCount}$
4: **if** (rating = 0)
5: nodeStatus = "black"
6: **else**
7: **if** (rating > τ)
8: nodeStatus ← white
9: **else**
10: nodeStatus ← grey
11: **end if**
12: **end if**
13: **end function**

4.5 Voting-Classification Blockchain Based Contract

Unlike SCBC, in VCBC, a voting dataset is available to provide the source car with preliminary knowledge about the reputation of each one of its neighbours. The overall reputation can be calculated

(using the makeVoting function according to elementary stored reputation values according to each node in the network). So, this voting function allows the first selection of a subset of the highly reputed nodes (the mean reputation value is equal to w). Then, a second phase of the classification is performed similarly to the SCBC based on the ratio of the delivered relays. This procedure is described by the Algorithm 5. Algorithm 4 defines the status of a node by voting.

Algorithm 4: Make voting

```
foreach node n in N do
r ← getReputationFromNeighbors()
  if r= "grey" or r= "black"
  retrieve n from N
    end if
  end for each
return N
end function
```

Algorithm 5: VCBC

```
Input: List of neighbors  ▷ N [n (nodeName, relayTime, deliveredCount, notDeliveredCount)]
Ouput: nodeStatus
N1 ← makeVoting(N)
foreach node n in N1 do
  R.push(Relay(nodeName, relayTime, "waiting"))        ▷ new relay
times ← deliveredCount + notDeliveredCount          ▷ counting times
status ← updateRelay()
deliveredCount ← updateRelay (deliveredCount, status). deliveredCount
nodeStatus ← updateNode(deliveredCount, times)
  end for each
return nodeStatus
```

5 Experimental Evaluation

In this section, we evaluate our proposed model that contains two methods which are: SCBC and VCBC. The performance of both methods is assessed in a completely decentralized management network. Moreover, we adopt a network scenario with blackhole and gray hole attack examples. Thus, we study the impact of these attacks on SCBC and VCBC methods. Furthermore, to provide a proof of concept of our proposed protocol, we obtained the results by using Remix IDE, which allows deploying smart contracts in the browser using Ethereum Blockchain and solidity language The evaluation process was based on several metrics which are: Packet Delivery Ratio (PDR), Throughput (TP) and Routing Overhead (RO). In addition, we involved the evaluation process by measuring the accuracy ratio for SCBC and VCBC and compared our results with BCR protocol in [5].

5.1 Experiments Settings

The test of the proposed approaches is performed in a highway scenario where the test vehicles forward data in one direction. We conduct the simulations experiments for the network topology with 7 cars, as shown in Fig. 6 where the source car has three possible paths to reach the destination. In this section, we assess the performance of SCBC and VCBC methods in the presence of blackhole and

greyhole attacks. In a blackhole attack, the malicious car present as a candidate node for the relay is offering wrong routes to drop the sender's packets and disruption. In greyhole attacks, the malicious car confused its neighbours whether it is malicious or not because it may forward or drop data packets.

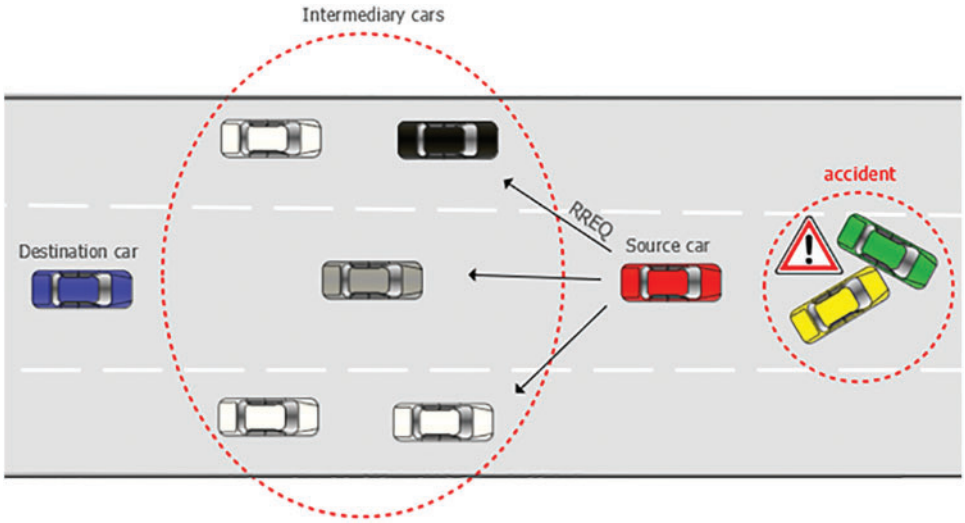

Figure 6: The network topology for the simulation process. A red car is the source car, a blue car is the destination car, black and gray cars are malicious cars

5.2 Evaluation Criteria

As we declared before, the evaluation process was based on several metrics which are: Packet Delivery Ratio (PDR), Throughput (TP) and Routing Overhead (RO) as follows:

$$PDR = \frac{D_{rcv}}{D_{Total}}, \tag{1}$$

where D_{rec} is the number of data packets successfully received by the destination and D_{total} is the total number of data packets sent by the source car.

The throughput (TP) is given by:

$$TP = \frac{D_{rcv}}{D_{sim}}, \tag{2}$$

where T_{sim} is the simulation duration.

The Routing Overhead (RO) is given by:

$$RO = \frac{D_{net} + D_{ctrl}}{D_{net}}, \tag{3}$$

where D_{net} is the total number of passed data packets. We considered 1000 data packets for each smart contract. D_{ctrl} is the total number of control messages; that is, the number of function calls in smart contracts. Each function call in a smart contract is assumed to need a 100-byte control packet.

To check the efficiency of our proposed methods, we measured the accuracy ratio for SCBC and VCBC. We calculate the accuracy ratio by dividing true classified results on all classified results multiplied by 100%. In VCBC, the accuracy converged to 80%, while it converged to 60% in SCBC.

6 Analysis of the Results

The findings of this research provide encouraging results to support the ability of blockchain-based smart contracts in VANET applications. As we noticed, after applying the experiments, SCBC and VCBC achieved the target perfectly. Next, we discuss the experiments and their results in detail. As illustrated in Fig. 6, the sender has three possible paths to deliver data packets to the destination. The routing process in SCBC and VCBC methods follows the approach of the AODV protocol where choosing the relay nodes is based on their hop counts to the destination. Whereas, the strength of SCBC and VCBC methods lies in the ability of the source to increase its awareness about the status of the neighbour after many sending which has a proportional effect on PDR. Our proposed model is designed to give a relay node at least two relay times to judge whether it is Black, Gray or White. In a blackhole attack, the model can classify a car as Black after two undelivered packets. While the model takes a long time to decide if the relay node is Gray due to the unpredictable behaviour of gray hole attack, that is the process of classifying the gray hole based on the rate of undelivered packets to all packets sent by the source.

In SCBC, the source car has no initial view of neighbours' status as shown in Fig. 7. Therefore, it chooses the best path according to the mechanism in AODV then after a while as much as the awareness of the source increases, the value of the PDR is improved after each successful relay.

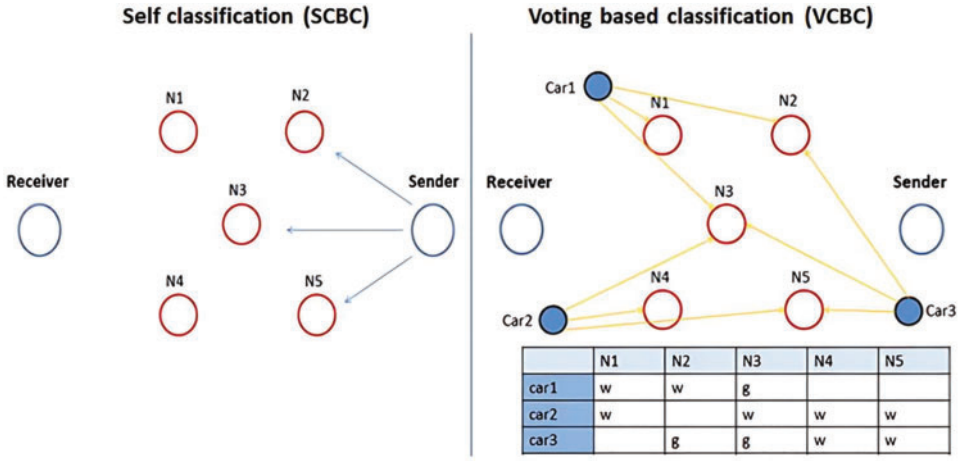

Figure 7: A comparison between SCBC and VCBC shows the initial awareness of the sender, the absence of miner cars in SCBC describes the less awareness of the sender

Fig. 8 shows the PDR of SCBC in the case of two malicious cars in the network. In SCBC, due to the less awareness level of the source about the status of its neighbour before starting the relay process, we notice higher volatility in PDR results. As shown in this figure, the PDR is almost around 0 in the first and second columns which means that the first and second packets sent by the source were not delivered as a consequence of the existing blackhole in the first path. Therefore, the source classified this node as Black and blocks them from later relays. Whereas, in the third sending PDR increased when Greyhole in the second path delivered the packet successfully to the destination. However, in the fourth transmission the PDR decreased when the Greyhole attacker decides to drop the packet, and the same in the fifth round. Because the rate of delivered packets to the total packets received by the greyhole equals 1:3, the source classified this car as Gray. So, it is clear in this figure the volatility in the first columns when the PDR was up to 33.3% after the third sending, then decreased by 13.3% after the fifth sending. This is because of the confusion caused by the greyhole in relaying process, which means trouble in the awareness level of the source. Then, we notice that PDR re-increases another

time starting from the sixth sending where the source chooses a new relay node from the third path when there are no malicious cars. Therefore, the continuously increasing results in PDR starting from the sixth column represent the increasing awareness level of the source. Thus, even with the volatility in results, the awareness level of the source about a relay node should be increased after at least two transmissions.

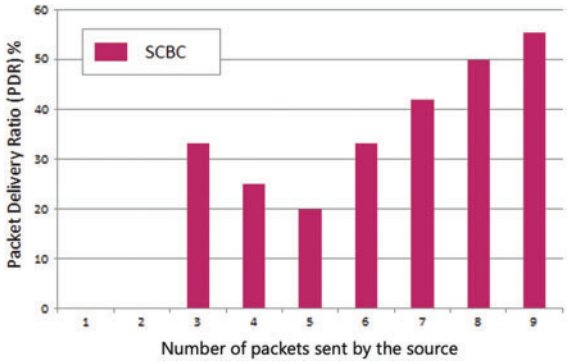

Figure 8: PDR results of SCBC in each relay process with two malicious cars in the network. High volatility in results explains the less awareness level of the source, the constant increase of PDR from the sixth sending represents the high awareness level of the source

In VCBC, the source takes into account the miners' evaluations for the neighbouring cars that are stored in blockchain Fig. 7. Therefore, unlike SCBC, the source in VCBC started the relay process with a high awareness level. Moreover, it will update its reputation table after each sending and reclassify the status of neighbours if needed. Fig. 9 shows the PDR of VCBC in the case of two malicious cars in the network. In the first and second transmissions, the packets fail to be delivered due to the wrong miners' evaluation of the black car. Afterward, the source classifies this car as Black and then tries to send new packets through White cars according to the miner's evaluation and so on. Therefore, we can see the early increase of PDR from the third transmission in Fig. 9. The comparison in Fig. 10 shows the early positive results of PDR achieved by VCBC, unlike SCBC. As we notice, the less volatility in VCBC results because of the high awareness level of the source.

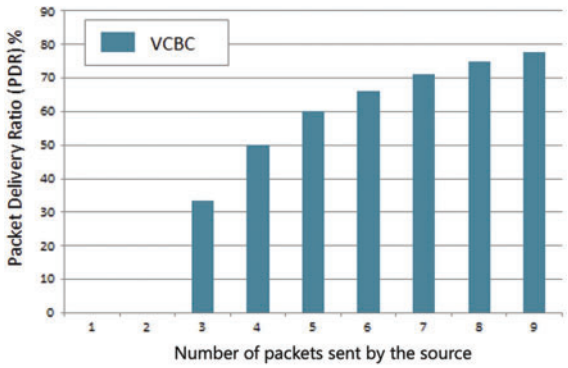

Figure 9: PDR results of VCBC in each relay process with two malicious cars in the network, less volatility in results explains the high awareness level of the source due to voting classification. The failure in the first and second sending was because of the incorrect reputation value assigned to the relaying car

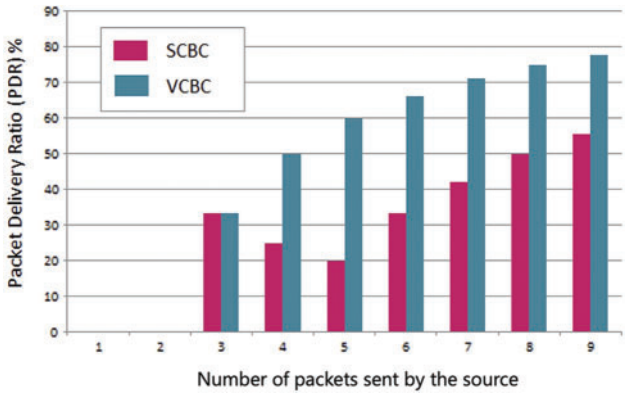

Figure 10: Comparison of PDR results between SCBC and VCBC in each relay process with two malicious cars in the network. The less volatility in VCBC results compared to SCBC, because of the high awareness level of the source. As shown, the PDR of VCBC started improving after the third sending as a consequence of the reliable car being selected through a voting classification

In Fig. 11, we make a comparison of our proposed protocol of SCBC and VCBC with BCR protocol in [5]. In BCR, the average rate of PDR is equal to 35% in the case of existing two malicious nodes in the network. In contrast, the PDR in SCBC and VCBC have a chance to improve when the awareness of the sender improves too and blocks malicious cars from participating in the relaying process.

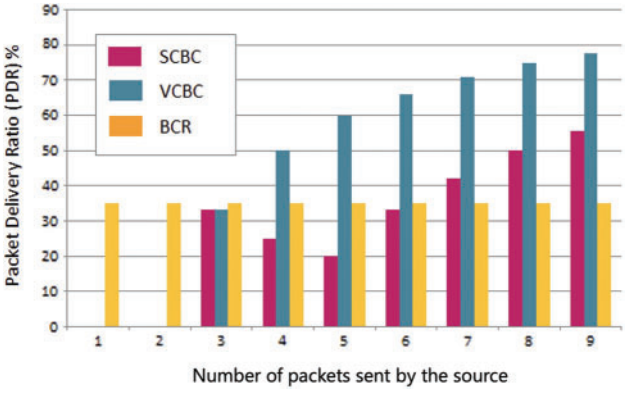

Figure 11: A comparison of PDR results of SCBC and VCBC with the previous protocol BCR in each relay process with two malicious cars in the network. As shown, both SCBC and VCBC have a variable PDR ratio and they have the ability to improve, however, BCR protocol has a stable PDR ratio

Table 1 presents a comparison of our proposed SCBC and VCBC with BCR routing protocols based on PDR, TP and RO performance. In Table 1, we can see the PDR rate of VCBC reaching 78%. Also, the TP performance of VCBC exceeded 1 kbps, while in SCBC and BCR it does not reach 0.5 kbps. Regarding the RO performance, in SCBC and VCBC it is higher than BCR as a consequence of more frequent exchanged messages to discover the most malicious nodes in that network and block them.

Table 1: Comparison of SCBC and VCBC with BCR protocol based on PDR, TP and RO performance

Method	PDR (%)	TP (%)	RO (%)
SCBC	56	0.41	2.6
VCBC	78	1.16	2.14
BCR	35	0.44	1.7

7 Conclusion

In this research, we have proposed a smart contract model-based blockchain for secure routing to enhance the trustworthiness between vehicles during relaying data in VANET. The robustness of our proposed model lies in using two versions of the smart contract in the routing process. The first is SCBC where the source car does not have any prior awareness about the neighbour's status. The second is VCBC where the source car depends on the voting of miners stored in the blockchain. Thus, the awareness level of the source car about the reputation of its neighbours in VCBC becomes higher which explains the high rate of PDR performance when compared with SCBC and BCR. Whereas, even in SCBC, the source can increase its awareness after many transmissions which causes an increase in the routing overhead. Our experiments show that the VCBC method achieves good results in terms of PDR and TP performance even in the presence of black hole and gray hole attacks. The conducted experiments show that even in the presence of black hole and gray hole attacks, the VCBC method obtains positive results in terms of PDR by converging to 80% and it is exceeded 1 kbps in TP performance which is more than double that of SCBC and BCR. In general, these encouraging findings can also be applied in other Ad Hoc Networks. Future research should further develop and confirm these initial findings by increasing the sample and performing more experiments to obtain a good evaluation of the model. Therefore, future research might apply machine learning methods to train a large data set.

Acknowledgement: Researchers would like to thank the Deanship of Scientific Research, Qassim University for funding publication of this project.

Funding Statement: Researchers would like to thank the Deanship of Scientific Research, Qassim University for funding publication of this project.

Author Contributions: The authors confirm contribution to the paper as follows: study conception and design: A. Alabdulatif, M. Alharbi; data collection: M. Alharbi, A. Mchergui; analysis and interpretation of results: A. Alabdulatif, A. Mchergui, T. Moulahi; draft manuscript preparation: A. Alabdulatif, M. Alharbi, T. Moulahi. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: Not applicable.

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

References

1. Al-Kahtani, M. S. (2012). Survey on security attacks in vehicular ad hoc networks (VANETs). *2012 6th International Conference on Signal Processing and Communication Systems*, Gold Coast, QLD, Australia, IEEE.
2. Mchergui, A., Moulahi, T., Alaya, B., Nasri, S. (2017). A survey and comparative study of QoS aware broadcasting techniques in VANET. *Telecommunication Systems, 66(2),* 253–281.
3. Hajlaoui, R., Guyennet, H., Moulahi, T. (2016). A survey on heuristic-based routing methods in vehicular ad-hoc network: Technical challenges and future trends. *IEEE Sensors Journal, 16(17),* 6782–6792.
4. 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.
5. Ramezan, G., Leung, C. (2018). A blockchain-based contractual routing protocol for the Internet of Things using smart contracts. *Wireless Communications and Mobile Computing, 2018,* 1–14.
6. Dimitrakopoulos, G., Demestichas, P. (2010). Intelligent transportation systems. *IEEE Vehicular Technology Magazine, 5(1),* 77–84.
7. Plesse, T., Adjih, C., Minet, P., Laouiti, A., Plakoo, A. et al. (2005). OLSR performance measurement in a military mobile ad hoc network. *Ad Hoc Networks, 3(5),* 575–588.
8. Omar, M., Challal, Y., Bouabdallah, A. (2012). Certification-based trust models in mobile ad hoc networks: A survey and taxonomy. *Journal of Network and Computer Applications, 35(1),* 268–286.
9. Das, S., Perkins, C., Royer, E. (2003). Ad Hoc On Demand Distance Vector (AODV) routing. *IETF RFC3561*. https://www.rfc-editor.org/rfc/rfc3561.html
10. Adnane, A., Bidan, C., de Sousa Júnior, R. T. (2013). Trust-based security for the OLSR routing protocol. *Computer Communications, 36(10–11),* 1159–1171.
11. Sirisala, N., Bindu, C. S. (2016). Recommendations based QoS trust aggregation and routing in mobile adhoc networks. *International Journal of Communication Networks and Information Security, 8(3),* 215.
12. Chadha, K., Jain, S. (2014). Impact of black hole and gray hole attack in aodv protocol. *International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2014)*, Jaipur, India, IEEE.
13. Jain, A. K., Tokekar, V. (2015). Mitigating the effects of black hole attacks on aodv routing protocol in mobile ad hoc networks. *2015 International Conference on Pervasive Computing (ICPC)*, Pune, India, IEEE.
14. Upadhyaya, A. N., Shah, J. (2017). Blackhole attack and its effect on vanet. *International Journal of Computer Sciences and Engineering, 5,* 25–32.
15. 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),* 970.
16. Careem, M. A. A., Dutta, A. (2020). Reputation based routing in manet using blockchain. *2020 International Conference on COMmunication Systems & NETworkS (COMSNETS)*, Bengaluru, India, IEEE.
17. Lwin, M. T., Yim, J., Ko, Y. B. (2020). Blockchain-based lightweight trust management in mobile Ad-Hoc Networks. *Sensors, 20(3),* 698.
18. de la Rocha Gómez-Arevalillo, A., Papadimitratos, P. (2017). Blockchain-based public key infrastructure for inter-domain secure routing. *International Workshop on Open Problems in Network Security (iNetSec)*, Lucerne, Switzerland.
19. Talukdar, M. I., Hassan, R., Hossen, M. S., Ahmad, K., Qamar, F. et al. (2021). Performance improvements of AODV by black hole attack detection using IDS and digital signature. *Wireless Communications and Mobile Computing, 2021,* 1–13.