I.J. Wireless and Microwave Technologies, **2022, 4, 1-14**
Published Online August 2022 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijwmt.2022.04.01

Cyber-resilient Routing for Internet of Vehicles Networks During Black Hole Attack

Mehnaz Tabassum
Department of Electrical and Computer Engineering, Michigan Technological University, Houghton, MI-49931, USA
E-mail: mtabassu@mtu.edu

Aurenice Oliveira
Department of Electrical and Computer Engineering, Michigan Technological University, Houghton, MI-49931, USA
E-mail: oliveira@mtu.edu

Received: 15 April 2022; Revised: 17 May 2022; Accepted: 25 May 2022; Published: 08 August 2022

Abstract: The ever need for transportation safety, faster and convenient travel, decrease in energy consumption, as well as inter-connectivity has led to the field of intelligent transportation system (ITS). At the core of ITS is the Internet of Vehicles (IoV) combining hardware/sensors, software, and network technologies. Vehicular ad hoc networks (VANETs) create mechanisms to connect IoV main elements, including vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and Vehicle-to-Sensors (V2S). ITS systems heavily rely on its network connecting different parts of its infrastructure and ensuring data exchanges. However, VANET security is one of the primary challenges faced by connected vehicles. In IoV, the network is accessed by a variety device making the system vulnerable to a multitude of malicious attacks, including distributed denial-of-service (DDoS) and black hole attacks. Since critical vehicle systems can be accessed remotely, successful attacks can lead to fatalities. In VANET, any node can function as a router for the other nodes, therefore a malicious node connected to the network may inject spoofed routing tables to the other nodes thereby affecting the operation of the entire network. To overcome this issue, we proposed a security scheme designed to improve routing protocols in the detection of black hole attack. The proposed approach is demonstrated on a Network Simulator (NS3.27) using different network parameters such as average packet loss rate, end-to-end delay, packet delivery ratio (PDR) and network yield. Simulation results demonstrate the proposed method adds 10-15% improvement (on average) in End-to-End Delay, Packet Delivery Rate, Packet Loss Rate and Network Yield as compared with conventional Greedy Parameter Stateless Routing and Path Aware Greedy Parameter Stateless Routing under the black hole attack.

Index Terms: Cyber-resilient, GPSR, Path Aware GPSR, VANET, Internet of Vehicles (IoV), Malicious nodes.

1. Introduction

A vehicular ad hoc network (VANET) provides connectivity to the Internet of vehicles (IoV) main elements, including vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and vehicle-to-sensors (V2S). The development of intelligent transportation systems (ITS) has accelerated the advancement of new technologies to improve transportation safety, traffic management, Internet connectivity, and entertainment applications. One of the biggest benefits of ITS is by significantly improving road safety by providing accurate and fast information of roads and vehicles [1]. In VANET, vehicles are equipped with sensors and software collecting and processing road conditions information, vehicles conditions of mechanical/electrical components, vehicles status (speed, brake, acceleration), and positioning through global positioning system (GPS) receivers. The exchange of beacons allows the network to obtain accurate and up-to-date awareness of the neighbor's vehicles, providing real time information for road safety applications such as collision warning, sudden breaking warning, intersection collision avoidance, and road conditions warning. According to the U.S. National Highway Traffic Safety Administration, 615,000 motor vehicle crashes could be prevented using connected vehicles technology [2]. Also, the percentage of having crashes at or near intersections are more than 50% which is noted by Federal Highway Administration (FHWA) [3]. Network information is broadcasted and accessed remotely by numerous devices. While this architecture allows many benefits, it also makes the network vulnerable to a variety of malicious attacks. Successful malicious attacks can lead to fatalities and chaos. Hence, it is of paramount importance to maximize cybersecurity robustness of networks supporting ITS systems. The key characteristics of VANETs are high mobility, large network size and frequently exchanged information between vehicles (nodes with mobility). Based on

these features, any node transmitting malicious information has the ability to disrupt and compromise the entire network causing car accidents and traffic congestion. Because VANET's infrastructure is distributed, it must maintain all security parameters during data exchange between all the nodes in the network [1, 4]. Internet of vehicles'(IoV) primary objectives include ensuring vehicular traffic safety, high efficiency, assisting drivers in critical situations such as accidents and road congestion as well as safely providing infotainment to road users such as traffic, weather and entertainment. With the development of the Internet of vehicles (IoV), different types of attacks have been disseminated exposing the infrastructure vulnerability to many flaws, resulting numerous security risks that must be resolved before IoV technologies can be implemented safely and effectively. As VANET is a decentralized, fast changing network and with both legitimate and possibly malicious nodes, maintaining network overall security becomes incredibly difficult. A simplified version of a typical VANET architecture including an example of black hole attack in shown in Fig. 1, where car *H* is acting as a malicious node to disrupt the communication between car *A* to any other vehicles, and cars *E* and *G* are the destination nodes. The system is comprised of vehicles equipped with on board units (OBUs) enabling V2V and V2I, and roadside unit (RSU).

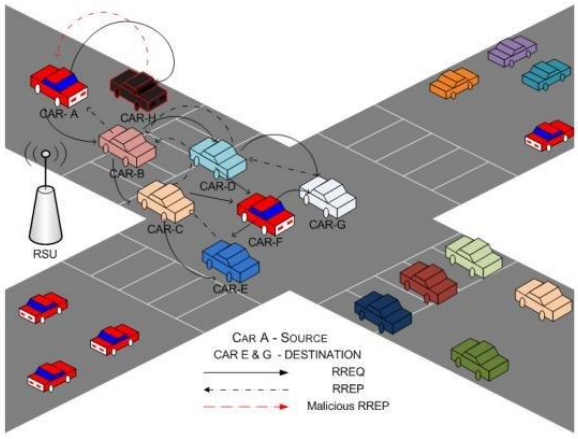


Fig. 1. Black hole attack in VANET [5].

There are several solutions trying to minimize the effects of cybersecurity attacks in VANET, they are discussed in the related work section of this paper. This work briefly explains Black hole attacks in VANET and proposes a solution to overcome network loses as a result of such attacks.

2. Literature Review.

2.1. Parameters of Security in VANET

In this section, we discuss some of VANET's safety features such as authenticity, availability, and confidentiality. These three characteristics cannot be overlooked when it comes to safety [6].

- Authenticity: verifies that the message was delivered by a trusted vehicle. It is very important to verify the sender's authenticity which is the initial security of the message [6].
- Availability: Even if the network is under attack, availability ensures that communication channels and network services are accessible without impacting the network's performance [6].
- Confidentiality: is accomplished by encrypting messages with cryptography techniques. Confidentiality refers to correspondence that is kept secret and safe. When a data is transmitted, only the authenticated recipient should have the power to decode it [6].

2.2. Different Types of Attacks in VANET

There are number of attacks that can impact the whole system or adversely affect the system's execution. These attacks can be classified into different categories [7,8]: impersonation, denial of service (DoS), routing (e.g., worm hole, black hole, and gray hole), sybil, timing. In this paper, we investigate how to improve the network performance subject to black hole attack which we describe as follow:

2.3. Black Hole Attack

A black hole attack, also known as a packet-drop attack, occurs when a malicious node in a routed network intends to direct any or all network traffic towards itself but refuses to act as a relay. The attack entails connecting a relatively new contact node that wishes to send packets over the network. This malicious node declares that it has the shortest path from sender to the information receiver node to accomplish this transmission [9]. The sender makes requests for

information to be sent and waits for the response to determine which path is the best. Unsecured nodes (without cybersecurity protection) attacked by malicious nodes will behave as if they are obtaining the correct paths to forward packets. This is because malicious nodes may lead the way thought to have the correct path to a series of packages. Therefore, undoubtedly all the data packets will be lost [10]. To make matters worse, the malicious nodes between the source and the destination nodes can also prevent source/destination pair from maintaining a connection, which also results in dropping of packets [11]. This type of attack is frequent but not easily detectable since a malicious node can eventually also act as a regular node. Black hole attack is a significant security problem in VANETs, however, identifying a black hole attack is difficult since packets are dropped on compressed networks like VANETs on a regular basis. Moreover, numerous factors such as channel congestion can impact the extent of lost packets. Therefore, detecting and mitigating this attack result in significant improvements in VANET routing [10,11].

2.4. Investigated Routing Protocols

The protocol we investigated and chose as benchmark algorithms is the Geographic Perimeter Stateless Routing (GPSR), which is one the most widely used location-based [12] stateless routing schemes as well as highly effective in dynamic networks [13]. We also investigated the performance of a novel routing protocol known as Path Aware GPSR (PA-GPSR) [14]. GPSR forwards data packets from the source to destination node with the help of two forwarding schemes: greedy forwarding and recovery mode (perimeter forwarding). Greedy forwarding strategy makes it possible to send a packet to the destination by locating the closest neighboring node to destination and transmit the packet one hop at a time shown in Fig. 2. When greedy forwarding is not possible the perimeter forwarding mode is applied. In this mode the packets are transmitted based on the right-hand rule, which is more time and bandwidth costly. Every node knows the routing strategy by checking the packet header fields where it is indicated whether the packet is in greedy mode or in perimeter mode. The default forwarding method is greedy forwarding and perimeter forwarding will only be activated when greedy forwarding becomes inefficient [13].

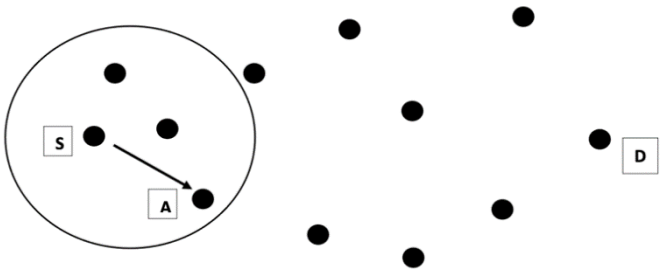


Fig. 2. Greedy Forwarding Strategy in GPSR.

An example of the routing strategy is presented in Fig. 3. In this example, node *S* wants to forward data packets to its intended destination, node *D*. The GPSR protocol assumes every node to be equipped with GPS device to acquire its position coordinates. Nodes periodically broadcast their own IP with the position information through beacon messages. The nodes within the communication range of each other can have the position information of other nodes along with the IP. The black dotted circle shown around the nodes indicate their communication range. Node *S* first checks its surroundings for greedy choice to forward the packet. However, there is no node within the communication range of *S* that is closer to destination *D* than *S* itself. Hence node *S* is considered to be a local maximum in its geographic proximity to destination, which causes node *S* to switch to perimeter forwarding. Node *S* forwards the packet to node *B* based on right hand rule. The latter method helps to recover from local maximum. Node *B* also checks its surroundings and finds itself to be the closer node and keeps on forwarding the packets via perimeter forwarding. The process continues till the packet reaches node *G* via *B,C,E,F_recovery.* Node *G* then finds itself to be closer than node *S*. Therefore, it turns back to greedy forwarding and forwards the packets to the closer node *H.* The process continues till the packet reaches the destination *D.*

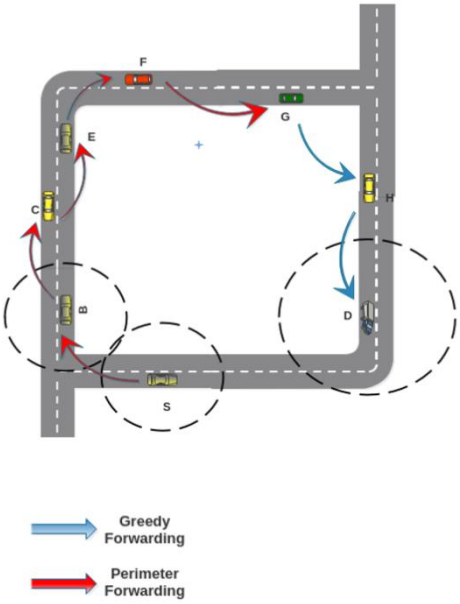


Fig. 3. GPSR forwarding example.

The Path Aware GPSR strategy (PA-GPSR) is a vehicle-to-vehicle (V2V) position-based routing protocol scheme (currently designed only to urban scenarios) that aims to reduce the drawbacks of GPSR using a particular form of greedy and recovery forwarding. PA-GPSR routing protocol's goal is to improve the greedy and recovery forwarding strategies of the GPSR by introducing two extensions of the Neighbors' Table (NT) called Deny Table (DT) and Recently Sent Table (RST). The DT and RST will be used by the packet forwarding decision policy. Another contribution of this work is the replacement of the right-hand rule in recovery mode by a new recovery algorithm that duplicates the packet and sends it using both the right-hand rule and the left-hand rule [14].

2.5. Black-Hole Attack in GPSR and PA-GPSR

In black hole attack, malicious nodes [15] utilize the network routing protocol to indicate they have the shortest route to the destination node of the message they want to intercept [16,17]. Regardless of whether it has tested its routing table, this aggressive malicious node advertises the availability of new paths [8]. As a result, the attacker node will still be available to respond to the route request, intercepting and retaining the data packet. The requesting node will receive the attacker nodes' reply even before actual node responds, resulting in the creation of a malicious and manipulated path. If this route has been developed, the requesting node must determine whether to discard all packets or forward them to the unknown address. The process by which a malicious node is integrated into data routes can differ by various reasons [8]. If the malicious node is located in such a place where the perimeter forwarding method is required, it will pretend to have an updated but fake routing table which consists of Neighbors' table (NT) for GPSR and Deny Table (DT) and Recently Sent Table (RST) for PA-GPSR Routing protocol. The black hole problem in GPSR or PA-GPSR is illustrated in Fig. 4, where node *A* wishes to transmit data packets to node *C* and begin the route discovery process.

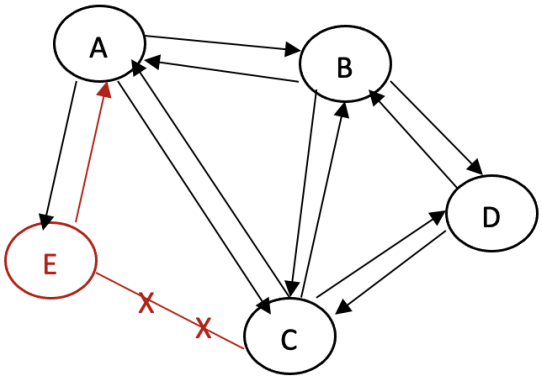


Fig. 4. Black Hole Attack Problem.

If node *E* is a malicious node, it will pretend to have an active path to the destination point as soon as packets arrive. Then, it will send the reply to node *A* first, before sending it to any other node. As a result, node *A* will believe this is the appropriate path, and active route exploration will be successful. Node *A* will disregard all other responses and begin sending data packets to node *E*. Consequently, many of the data packets would be lost in this process.

3. Related Work

There have been several studies comparing the performances of different routing protocols. Some of them were concerned with the network capacity of VANETs, while others emphasized the performance and safety of routing protocols under different attacks such as black hole attacks, worm hole attacks, flooding attacks, among others.

Kumar et al. [4] presented a reliable AODV routing protocol which has been developed for the detection and remediation of black hole attacks in VANET. The proposed approach is essentially a revised version of the standard AODV routing protocol, with improved RREQ and RREP packet formats. To ensure confidentiality, the source and destination nodes are validated using a cryptography function-based encryption and decryption. Simulations of different comparative analyses were used to illustrate the feasibility of the proposed solution. In our proposed work, instead of AODV routing protocol, we have chosen GPSR routing protocols. GPSR is well known to perform better than AODV by using the geographic position of the nodes to make the routing decisions. Every node knows its own geographical location using global positioning systems (GPS) making this routing more suitable for modern vehicular networks than AODV.

Ahmed et al. [18] demonstrated a method for detecting and preventing black hole attack by malicious nodes. In this study, the TOPSIS method was used to pick the most trustworthy node for smart routing. A simulation model in NS-2 simulator was used to test the method. According to the simulation results, the proposed method can effectively avoid malicious attacks while providing a low overhead. In addition to propose a different cyber security scheme, we are using NS-3 simulator instead of NS-2. NS-3 has improved features as compared to NS-2 and it is more suitable for VANET simulations. Unlike NS-2, in NS-3 each packet contains a byte buffer, a set of byte tags, a set of packet tags, and metadata. NS-3 stores all tags in a single byte buffer. Because NS-3 has small packet tags and buffer while simulating, our simulations are more efficient by avoiding unnecessary overhead.

Lyu et al. [19] proposed a Trust-based Greedy Forwarding Routing (TGF) in a dynamic 3D VANET environment considering the effect of geographic location and the number of communications between nodes while establishing a safer path than 2D VANETs. In 3D networks, transmission loss can be considered more effectively than 2D environment. This modified protocol improves the throughput approximately by 18 percent and reduces the packet loss rate approximately by 24 percent compared to the standard GPSR. The simulation results demonstrated that TGF is more suitable for black hole Attacks with 3D scenarios than standard GPSR. In our study, we evaluate the performance of our proposed cybersecurity scheme by modifying the conventional GPSR and PA-GPSR under black hole attack. By comparison with the results in paper [19], our results show better performance in average packet loss rates, end to end delays, network yield and PDR.

Fiade et al. [20] compared the effects of black hole attack and flooding attack on a battery energy efficient AODV. Their results showed higher throughput and lowest packet loss rate in the case of black hole attacks compared to standard AODV. The simulation results for flooding attacks in the modified AODV also shows better remaining battery energy and end to end delays than AODV protocol with black hole attacks. Even though, energy consumption is an issue in many MANET and sensor networks, this is not a real challenge for VANET since the vehicles when running usually don't have energy/battery consumption problem. In our study we focused on the packet transmission parameters to measure the performance of the modified routing protocols.

In Shajin et al. [21], the trust value for a secure node represents the location information and the routing information. For an efficient communication between sender and destination node, their modified routing protocol TSGRP (Trusted Secure Geographic Routing Protocol) evaluates the trust value for each node, computes the trust value to match all the routing requirements and updates the trust value after transmission.

TSGRP establishes a secure communication channel between the sender and the destination node based on trust. Following the transmission of route-request and route-reply packets, the evaluated direct trust value is used to evaluate the direct trust value of each node, and a secure path is formed between the sender and destination node. We have adopted a similar routing scenario in our study but instead of MANET, we have focused on VANET.

4. Methodology

As previously discussed, VANET data is broadcasted and accessed remotely by numerous devices. While this architecture allows many benefits, it also makes the network vulnerable to a variety of malicious attacks potentially leading to catastrophic consequences. VANET routing protocols such as GPSR and PA-GPSR (an improved version of GPSR Protocol [14]. are not capable of detecting black hole attack, the modified protocols with cyber-resilient scheme we are proposing is based on authentication techniques to check the validity of nodes. The new cyber-resilient protocols only forward data packet after confirming nodes authenticity. This reduces the probability of cyber-attacks and

improves overall network performance. In this paper, we also compare the network performance when subjected to different numbers of malicious nodes. Simulation results demonstrate that the proposed scheme can improve the network performance by 15-20%.

4.1. Proposed Algorithm

In black hole attacks, malicious nodes act as destination nodes or declare having the shortest path to the destination node. Thus, before sending data packets, hop counts for every transmission is calculated for both standard GPSR and PA-GPSR routing protocols. Following that, we calculate the average hop counts for the transmissions with different numbers of nodes.

Once the average transmission hop count is obtained, threshold values are set for comparison. When the cyber-resilient protocols are used, instead of the traditional ones, if a destination node receives the data packet with a lesser hop count than the threshold route, the packets will be dropped since the shorter path will be considered a faulty path.

Calculating and analyzing the threshold packet transmission time is the approach used to evaluate the performance of our proposed scheme. The proposed scheme Pseudo Algorithm is as follow:

Trusted_route()
for each (N_n)
if $((R_{seq}(i) \gg (R_{seq}(j))$
then
$R_{seq}(j) = M_{seq}(n);$
Update_Trusted_Route()
$T_{seq} \leftarrow R_{seq}(i);$
Update_Non_Trusted_Route()
$N\_T_{seq} \leftarrow R_{seq}(j);$
endif
if (Greedy_mode==true)
then
Distance (n,D)<=Dist(R,D)
then
d(n)=Distance (n, D);
n(i)= $N_n()$
if $(S_t == true \;\&\&\; is\_\min\_distance\_to\_D)$
then
Forward_Packet();
endif
endif
Go_to_Parameter_mode
if (Parameter_mode==true)

then
D_{ad} *=data_packet_destination_node();*
P_{ad} *=data_packet_previous_node();*
$Dt_p(P_{ad}, D_{ad})$
Forward_Packet();
else
Discard_Packet();
endif
endif

Here,
N_n*= Neighboring Node*
R_{seq}*= Routing Sequence*
M_{seq}*=Malicious Routing Sequence*
T_{seq}*= Trusted Sequence*

4.2. Simulation Setup

To validate and evaluate our proposed scheme, we used network simulator 3 *(NS-3 V 3.27)* and Simulation of Urban Mobility (SUMO) [22]. We evaluated the performance of GPSR and PA-GPSR during blackhole attack as well

as the proposed cyber-resilient versions of GPSR and PA-GPSR with the implementation of the proposed cyber security schemes. The following considerations are made in order to ensure some realism in our simulation:

- The Network Traffic Model: We set the Beacon interval to be 1 second and the channel data rate to be 3 Mbps. Constant Bit Rate (CBR) data traffic was considered for each source-destination pair of nodes generating packets of 512 bytes fixed size. To assess the impact of existing network traffic, we varied the number of malicious nodes for each scenario from 5 to 20. For each set of simulations, we chose random source-destination pairs. In this way we randomly selected 5 pairs to perform the tests for 20 CBR connections and used the same pairs for all sets of simulation runs. For our study, we also assumed UDP as the transport layer protocol.
- Vehicle Traffic Model: We used SUMO framework on Manhattan grid with an area of 1100 m^2 with 9 intersections and 12 two-way streets, as shown in Fig. 5. The vehicles were placed initially by a random distribution and the movement of vehicles on the roads was restricted along the street based on the car-following model with speed not exceeding 15 m/s. We used 50, 70, 90 and 110 nodes to represent a sparse network.
- Simulation Environment: Each simulation was run for a total of 200 seconds. For all the results, we have run the simulation on an average of 30 times with a confidence interval of 95%.
- Communication Model: The IEEE 802.11p standard was used to model the MAC layer.

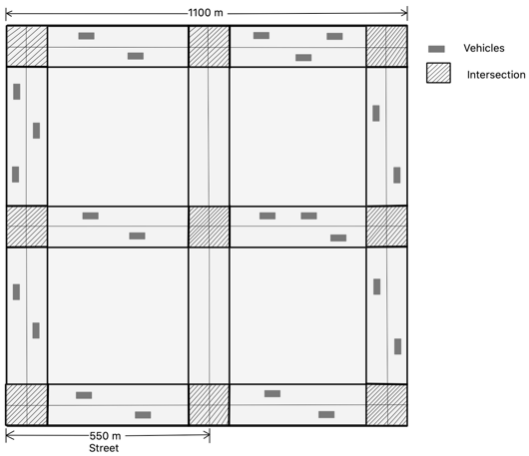


Fig. 5. Simulation scenario with 9 intersections and 12 streets.

- Propagation Model: Two ray ground propagation loss model is used for predicting the path losses between the transmitter and the receiver which considers both direct path and a ground reflection path.
- Assumptions: In addition to the previously described simulation environment, we are making the following assumptions. All the vehicles are equipped with GPS and digital map, and they are not using any fixed infrastructure for communication. All the vehicles have same transmission rate.

4.3. Performance Metrics

- Network Yield: ratio of the total packets received *R* by the destination to the total number of packets which are sent by all the nodes of the network T_{all}. Network yield can be used to measure achieved throughput and transmission cost of the network.

$$Net.yield = \frac{R}{T_{all}} \tag{1}$$

- Packet loss rate: ratio of the total number of lost packets *L* over the total number of packets which are sent of the sources T_{source},

$$Loss\ Tate = \frac{L}{T_{Source}} \times 100 \tag{2}$$

- End-to-end Delay: average value of successfully received packets delay D_n,

$$Delay = \frac{\sum_{n=1}^{N} D_n}{N} \quad (3)$$

- Cumulative End-to-end Delay: Cumulative value of successfully received packets delay D_n,

$$Cumulative\ Delay = \sum_{n=1}^{N} D_n \quad (4)$$

- Packet Delivery Ratio: ratio of the total number of received Packets *R* to the total number of packets sent from the source nodes T_{source},

$$PDR(\%) = \frac{R}{T_{Source}} \quad (5)$$

Table 1. Simulation Parameters.

Parameter	Value	Unit
Simulator	NS-3/SUMO	-
Packet Size	512	byte
Simulation Time	200	s
Simulation Area	1100x1100	m^2
Number of CBR Connections	15	-
Number of Nodes	30, 50, 70, 90, 110	-
Max. Speed	15	m/s
Data Type	CBR	-
Hello Interval	1	s
NT Entry Lifetime	2	s
Transport Protocol	UDP	-
Packet Interval	0.2	s
Mac Protocol	802.11p	-
Channel Data Rate	3	Mbps
Transmission Range	250	m
Propagation Model	Two-ray ground	-
Total Number of Simulation Runs	30	-
Routing Protocol	GPSR, PA-GPSR, Cyber-resilient GPSR, Cyber-resilient PA-GPSR	-

5. Results & Discussion

The average Packet Loss Rate (PLR) in GPSR and PA-GPSR is defined by the ratio of the total lost packets to the total number of packets sent from the source nodes. In Fig. 6 we can observe for all the algorithms (I, II, III, IV) that most of the packets are lost during the attack for lower numbers of nodes (vehicles) and as expected, the packet drops increase with the increasing number of malicious nodes in the network. As the number of nodes increases, the average PLR becomes stable for algorithms I and III. This is because the valid nodes to malicious nodes ratio is higher when there is a larger number of valid nodes in the network. Thus, some of the packets can avoid the faulty paths. On the other hand, in the Cyber-resilient versions (II and IV), as the number of nodes increase the packet loss ratio decreases because the nodes are now using the modified hop count to choose as their routing path. The paths may have more hops, but it will be secure and therefore, the packet loss rate will decrease. However, there are some trade-offs because packets now are not necessarily choosing the shortest route. Some of the correct paths are removed due to the faulty lowest path problem created by the malicious nodes. That is the reasoning why the packet loss rates are high when there are few nodes. As the number of nodes increases, the route becomes more trusted for II and IV rather than I and III. The graphs show that the higher number of nodes (70, 90, 110) have about 25-30% improvement in the cyber-resilient GPSR (II) and PA-GPSR (IV) compared to GPSR(I) and PA-GPSR(III), respectively, during the attack. The results in PA-GPSR (IV) are almost 6-10 % better than the GPSR (II) routing protocol because of the packet loop control and the fact that PA-GPSR can duplicate each packet in the network to send it in both right and left route. But overall, the modified algorithms (II and IV) are still facing a larger packet loss rate than the standard GPSR(I) and PA-GPSR(III)

because every packet in the network has a time limit to stay in the network. In some cases, the routes are longer, and the simulation time is limited, resulting in packets getting dropped because they don't have enough time to reach the destination.

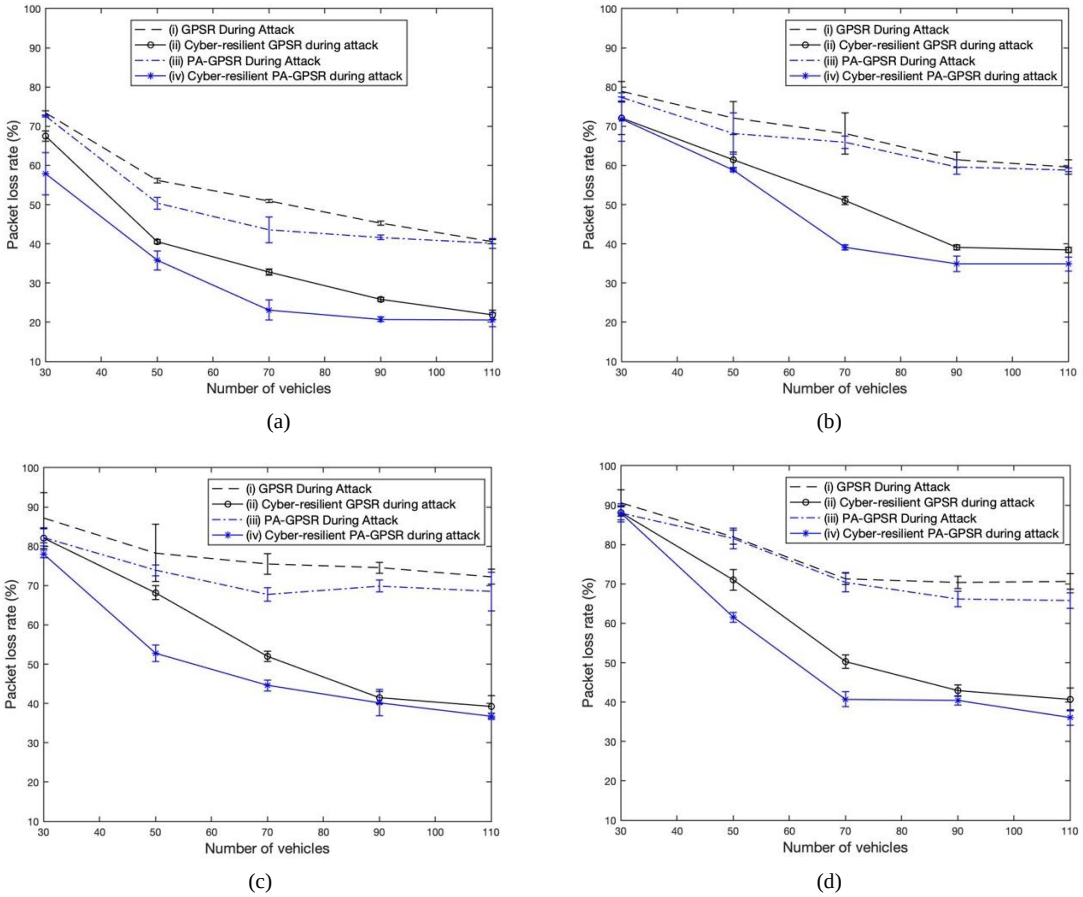


Fig. 6. Average Packet loss rate for varying number of vehicles in GPSR and PA-GPSR in GPSR, PA-GPSR, cyber-resilient GPSR and PA-GPSR during attack (considering 20 CBR connections). (a) 1 Malicious Node, (b) 5 Malicious Nodes, (c) 10 Malicious nodes, (d) 20 Malicious nodes.

The average end-to-end delay is the average transmission time of all successfully received packets. The black hole attack is a type of attack where the malicious node pretends to have the shortest and the fastest way to the destination. In Fig. 7, each set of results represent the average end-to-end delays for GPSR and PA-GPSR routing protocol during attack and the cyber-resilient routing protocols during attack for different numbers of malicious nodes. For different number of malicious nodes, the average end-to-end delay during the attack (I and III) shows similar behavior because almost all the packets are affected by the malicious nodes. The cyber-resilient version of GPSR during black hole attack is based on a threshold hop count and the average end-to-end delay is calculated as the time the packet takes to reach the destination from the source following the correct hop counts. This scheme works better for algorithms II and IV when there are more nodes (vehicles) in the network. That is the reason why we observe lower end-to-end delays when the node numbers increase. Average end-to-end delay is calculated only if there is a successful transmission when a packet is received at the destination node. Thus, the results for the cyber-resilient GPSR (II) have a low average end-to-end delay because packets with higher delays are dropped from the network. The results using PA-GPSR (IV), on the other hand, have higher average delays because there were less packets dropped. It may look like cyber-resilient PA-GPSR (IV) has higher end-to-end delays, but the successful transmission rate was higher implying in higher cumulative delays. For this reason, the percentage of improvement for average end-to-end delays are also described in Fig. 7 (cumulative end-to-end delays).

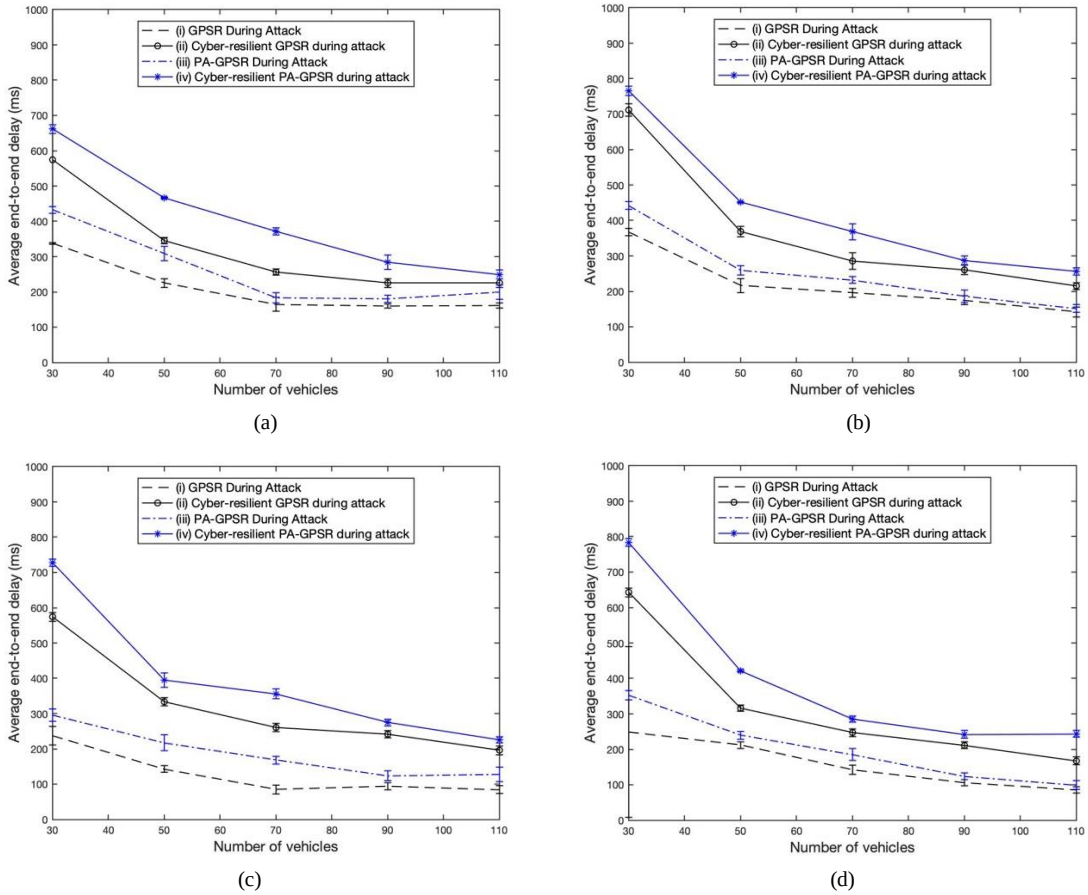
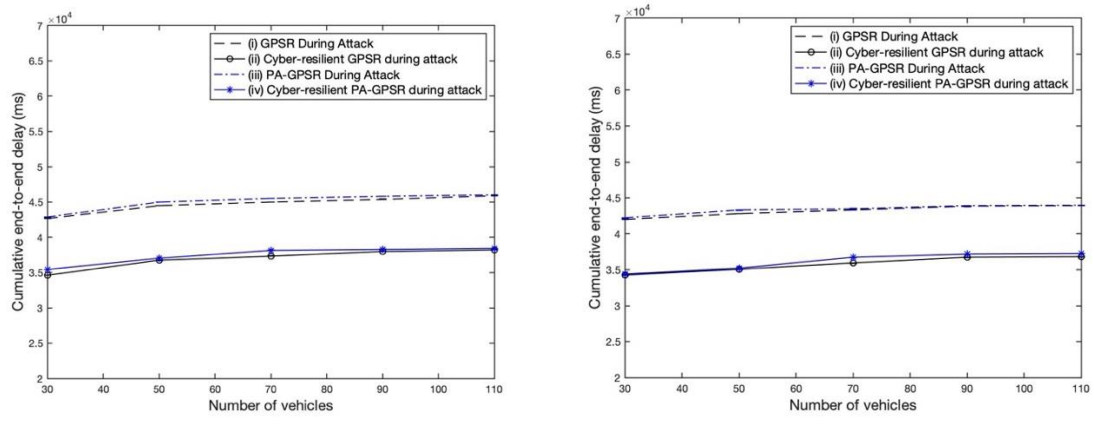
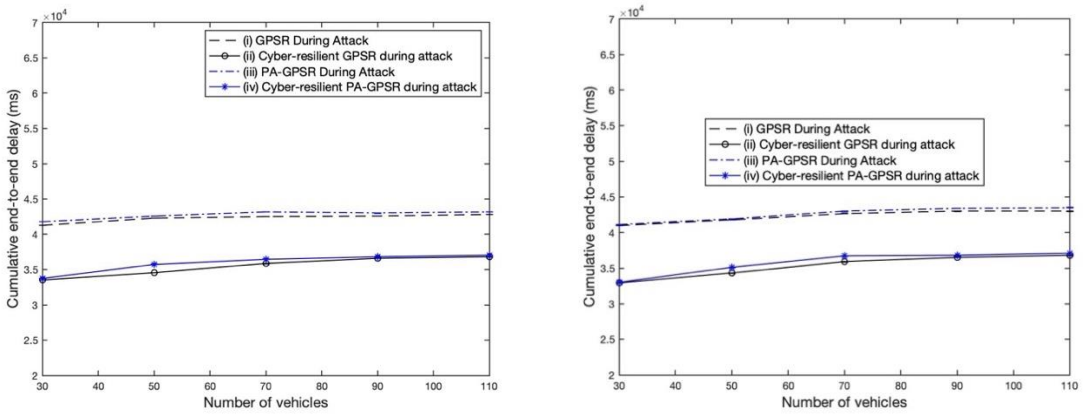


Fig 7. Average end-to-end delay for varying number of vehicles in GPSR and PA-GPSR in GPSR, PA-GPSR, cyber-resilient GPSR and PA-GPSR during attack (considering 20 CBR connections). (a) 1 Malicious Node, (b) 5 Malicious Nodes, (c) 10 Malicious nodes, (d) 20 Malicious nodes.

The cumulative end-to-end delay is another metric to represent the end-to-end delay. The results shown in Fig. 8 demonstrate that the cyber-resilient protocols (II and IV) are actually taking less time to send the packets from sender to receiver (or source to destination). As mentioned before, average end-to-end delays are calculated by the number of packets that are successfully transferred through the correct path. Cumulative end-to-end delays, on the other hand, represent the total time the packets are taking in all the algorithms (I, II, III and IV) to be transmitted from source to destination. Hence, for all the results presented in Fig. 7, when under attack, the cyber-resilient GPSR (II) and PA-GPSR (IV) take less time to reach the destination while GPSR (I) and PA-GPSR (III) take much more time to reach the destination because the paths are not optimal all the time. The results show that cyber-resilient GPSR (II) and PA-GPSR (IV) require about 16% less time to send the packets from sender to destination as compared to GPSR (I) and PA-GPSR (III) during the attack.

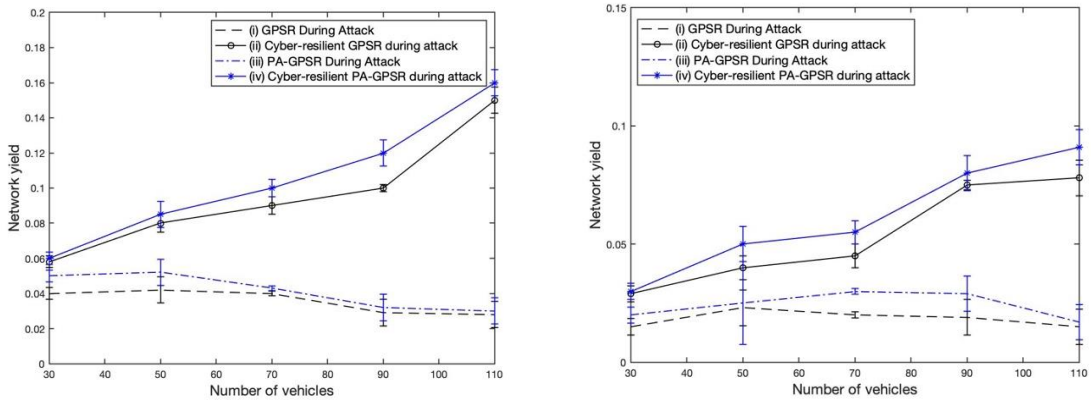




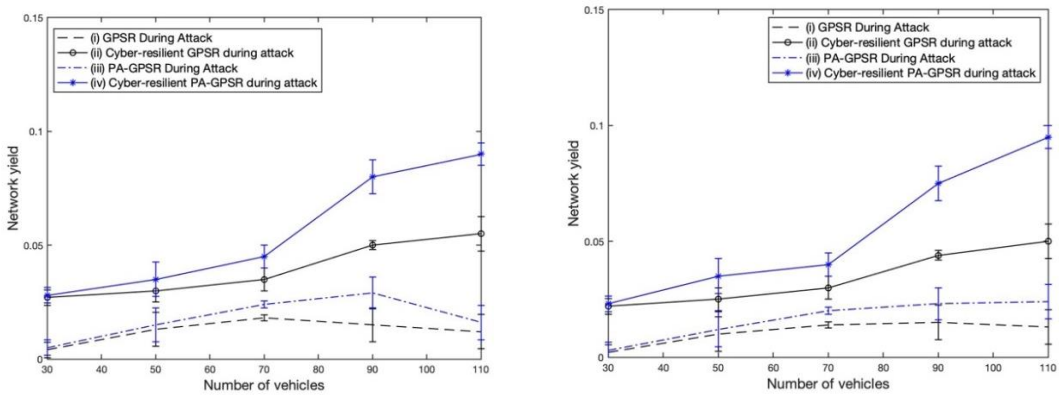
(c) (d)

Fig. 8. Cumulative end-to-end delay for varying number of vehicles in GPSR and PA-GPSR in GPSR, PA-GPSR, cyber-resilient GPSR and PA-GPSR during attack (considering 20 CBR connections). (a) 1 Malicious Node, (b) 5 Malicious Nodes, (c) 10 Malicious nodes, (d) 20 Malicious nodes.

The Network Yield (NY) is the ratio of the total packets received at the destination over to the total number of packets sent by all the nodes of the Network. It measures both the transmission cost as well as achieved throughput in the network. During attacks, the NY results for GPSR (I) and PA-GPSR (III) are relatively low and don't significantly change for different numbers of malicious nodes and for various numbers of valid nodes. Note that for both GPSR (I) and PA-GPSR (III) during attacks, the hop counts are low but as in most of the cases, most of the packets are lost. Thus, these transmissions are not counted as successful ones. However, in the cyber-resilient versions of the routing protocol, the network yield increases with the increased number of vehicles in PA-GPSR (IV) compared to GPSR (II). For the cyber resilient versions, the successful hop counts for each transmission are not the lowest hop counts because there is a threshold for hop counts, but on average the hop counts are lesser than the GPSR(I) and PAGPSR (III) for the successful transmission cases when they are under attack. As shown in Fig. 9, PA-GPSR algorithms (II and IV) have higher network yield in comparison with GPSR (I and III) for all set of pairs of source-destination. Two possible reasons for this behavior are: i) the right-hand rule is the best path option to reach the destination, and ii) there is no situation where the Deny Table (DT) (Silva et al., 2019) is useful to reduce the number of hops. In this case, the greedy forwarding of the PA-GPSR acts exactly as GPSR greedy forwarding. Therefore, since PA-GPSR uses packet duplication in recovery mode (even reaching the destination with the same number of hops and same packet delivery ratio), the network yield of PA-GPSR tends to be 10 % higher than GPSR. Fig. 9 also shows that during the attacks, the higher number of nodes have about 5-8% (for 70 nodes) and 20-30% (for 90 and 110 nodes) better network yield in the cyber-resilient GPSR (II) and PA-GPSR (IV) as compared to GPSR (I) and PA-GPSR (III).



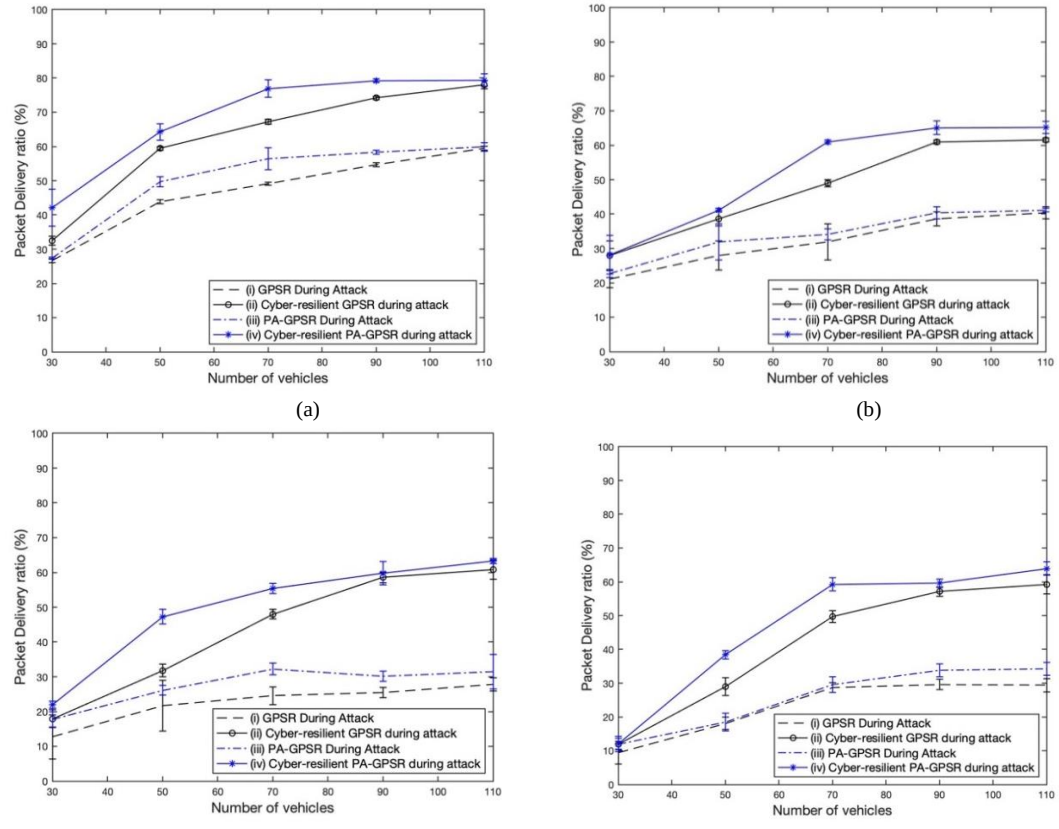
(a) (b)



(c) (d)

Fig. 9. Average Network Yield for varying number of vehicles in GPSR, PA-GPSR, cyber-resilient GPSR and PA-GPSR during attack considering 20 CBR connections. (a) 1 Malicious Node, (b) 5 Malicious Nodes, (c) 10 Malicious nodes, (d) 20 Malicious nodes.

The Packet Delivery Ratio (PDR) in GPSR and PA-GPSR is defined by the ratio of the total number of received packets to the total number of packets sent from the source nodes. Fig. 10 shows that a small number of packets are delivered during the attack and PDR increases by the increase of malicious and valid nodes in the network. As the number of nodes increases, the PDR becomes constant because of the malicious nodes are creating false routing sequences and the packets are following these routes. In the cyber-resilient versions, the packet delivery ratio increases because the packets are not choosing the shortest route (faulty lowest path created by malicious nodes) and consequently been dropped. As the number of nodes (vehicles) increases, the route becomes more trusted compared to the attack scenarios. That is the why PDR is lower with few nodes. The results in Fig. 10 show that the higher number of nodes (70, 90, 110) have about 25-30% better PDR in the cyber-resilient GPSR (II) and PA-GPSR (IV) as compared to GPSR (I) and PA-GPSR (III) during the attacks. The results in PA-GPSR (IV) are 6-10% better than the GPSR (II) because PA-GPSR has packet loop control and can duplicate each packet in the network to send it in both right and left route.



(a) (b)

(c) (d)

Fig. 10. Packet Delivery Ratio for varying number of vehicles in GPSR, PA-GPSR, cyber-resilient GPSR and PA-GPSR during attack (considering 20 CBR connections). (a) 1 Malicious Node, (b) 5 Malicious Nodes, (c) 10 Malicious nodes, (d) 20 Malicious nodes.

The cyber-resilient algorithm for PAGPSR (IV) has an increase of packet delivery rate because every packet in the network has a time limit to stay in the network. If any packet is searching the correct routing path for a long period of time it will be automatically dropped because the simulation runs for a limited time. Since PA-GPSR chooses routing path based on both right- and left-hand method in recovery mode, the probability of the cyber-resilient PA-GPSR (IV) protocol to find the routing path is higher than the cyber-resilient GPSR (II) protocol.

6. Conclusions

Blackhole attack is one of many challenging security issues in VANETs. Detection and remediation of cybersecurity attacks is a critical network task to prevent the network from collapsing. In a black hole attack, malicious nodes direct network traffic towards itself but refuses to act as a relay, thus creating faulty routes. The black hole attack is dangerous enough to have a significant influence on VANET. Malicious nodes' access to the network should be constrained for secure data transmission. Given the sensitive nature of VANET, a strong security mechanism for message routing is also necessary. The proposed cyber-resilient GPSR and PA-GPSR routing algorithms successfully detect malicious nodes and provide resources for the network to avoid the paths comprised of the faulty nodes. Simulation results show that the cyber resilient GPSR and PA-GPSR improve the network parameters (average packet loss rate, PDR, Network yield, and end-to-end delay) we investigated, providing a robust performance. Although the identification of the black hole attack is somehow complex due to VANET characteristics (e.g., scalability, poor connectivity), the proposed strategy was successful in disconnecting the paths created by malicious nodes in the network.

Acknowledgment

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

References

[1] Goyal, Amit Kumar, Gaurav Agarwal, and Arun Kumar Tripathi. "Network Architectures, Challenges, Security Attacks, Research Domains and Research Methodologies in VANET: A Survey." *International Journal of Computer Network & Information Security* 11, no. 10 (2019).

[2] NHTSA, "Vehicle-to-Vehicle Communication Report", United States Department of Transportation, 2018.

[3] Congress, S.S.C., Puppala, A.J., Banerjee, A. and Patil, U.D., "Identifying hazardous obstructions within an intersection using unmanned aerial data analysis", *International Journal of Transportation Science and Technology*, *10*(1), pp.34-48, 2021.

[4] Kumar, A., Varadarajan, V., Kumar, A., Dadheech, P., Choudhary, S.S., Kumar, V.A., Panigrahi, B.K. and Veluvolu, K.C., "Black hole attack detection in vehicular ad-hoc network using secure AODV routing algorithm", *Microprocessors and Microsystems*, *80*, p.103352, 2021.

[5] Upadhyaya, A.N. and Shah, J.S., "Blackhole Attack and its effect on VANET", 2017.

[6] Zaidi, T. and Faisal, S., 2018, "An overview: Various attacks in VANET", *4th International Conference on Computing Communication and Automation (ICCCA)* (pp. 1-6). IEEE, December 2018.

[7] Pokar, T., Patel, S. and Shah, R., "An Efficient Approach of DSR Protocol to Detect and Prevent Black Hole Attack For VANET", International Journal of Research and Analytical Reviws (IJRAR), 2019.

[8] Bibhu, V., Roshan, K., Singh, K.B. and Singh, D.K., "Performance Analysis of Black Hole Attack in Vanet", *International Journal of Computer Network & Information Security*, *4*(11), 2012.

[9] Yassein, M.B., Hmeidi, I., Khamayseh, Y., Al-Rousan, M. and Arrabi, D., "Black Hole Attack Security Issues, Challenges & Solution in MANET", *CS & IT Conference Proceedings* (Vol. 8, No. 18). CS & IT Conference Proceedings, December 2018.

[10] Yasin, A. and Abu Zant, M., "Detecting and isolating black-hole attacks in MANET using timer based baited technique", *Wireless Communications and Mobile Computing*, *2018*.

[11] Stępień, K. and Poniszewska-Marańda, A., "November. Security methods against Black Hole attacks in Vehicular Ad-Hoc Network", *2020 IEEE 19th International Symposium on Network Computing and Applications (NCA)* (pp. 1-4). IEEE, 2020.

[12] Dhiman, Vikram, Ikjot Saini, P. Manoj, M. Kumar, and P. Manoj. "A Comprehensive Survey of Location Based Routing in Vehicular Networks." *International Journal of Wireless and Microwave Technology* 1: 40-48, 2017.

[13] Karp, B. and Kung, H.T., "GPSR: Greedy perimeter stateless routing for wireless networks", *Proceedings of the 6th annual international conference on Mobile computing and networking* (pp. 243-254), August 2000.

[14] Silva, A., Reza, N. and Oliveira, A., "Improvement and performance evaluation of GPSR based routing techniques for vehicular ad hoc networks", *IEEE Access*, *7*, pp.21722-21733, 2019.

[15] Selvi, M., and B. Ramakrishnan. "Secured Message Broadcasting in VANET using Blowfish Algorithm with Oppositional Deer Hunting Optimization." *International Journal of Computer Network & Information Security* 13, no. 2, 2021.

[16] Ahmad, Shahnawaz. "Alleviating Malicious Insider Attacks in MANET using a Multipath On-demand Security Mechanism." *International Journal of Computer Network & Information Security* 10, no. 6, 2018.

[17] Houssaini, Z.S., Zaimi, I., Oumsis, M. and Ouatik, S.E.A., "Comparative study of routing protocols performance for vehicular ad-hoc networks", *International Journal of Applied Engineering Research*, *12*(13), pp.3867-3878, 2017.

[18] Ahmed, A.K., Abdulwahed, M.N. and Farzaneh, B., "A distributed trust mechanism for malicious behaviors in VANETs", *Indonesian Journal of Electrical Engineering and Computer Science*, *19*(3), pp.1147-1155, 2020.
[19] Lyu, J., Chen, C. and Tian, H., "Secure Routing Based on Geographic Location for Resisting Blackhole Attack In Three-dimensional VANETs", *2020 IEEE/CIC International Conference on Communications in China (ICCC)* (pp. 1168-1173). IEEE, August 2020.
[20] Fiade, A., Triadi, A.Y., Sulhi, A., Masruroh, S.U., Handayani, V. and Suseno, H.B., "Performance Analysis of Black Hole Attack and Flooding Attack AODV Routing Protocol on VANET (Vehicular Ad-Hoc Network)", *2020 8th International Conference on Cyber and IT Service Management (CITSM)* (pp. 1-5). IEEE, October, 2020.
[21] Shajin, F.H. and Rajesh, P., "Trusted secure geographic routing protocol: outsider attack detection in mobile ad hoc networks by adopting trusted secure geographic routing protocol", *International Journal of Pervasive Computing and Communications*, 2020.
[22] Krajzewicz, D., Erdmann, J., Behrisch, M. and Bieker, L., "Recent development and applications of SUMO-Simulation of Urban Mobility", *International journal on advances in systems and measurements*, *5*(3&4), 2012.

Authors' Profiles

Mehnaz Tabassum received her B.Sc. degree in Applied Physics, Electronics and Communication Engineering, and the M.Sc. degree in Electrical and Electronic Engineering from University of Dhaka, Bangladesh, in 2014 and 2016, respectively. She is currently pursuing her Ph.D. degree in Electrical and Computer Engineering from Michigan Technological University, Houghton, MI, USA. Her research interest is Vehicular Communication, Vehicular Networking, Signal Processing and Wireless Communication.

Aurenice Oliveira holds a Ph.D. degree in electrical engineering from the University of Maryland Balt. Co., USA. She is currently an Associate Professor with the Department of Electrical and Computer Engineering, Michigan Technological University. Oliveira's research interests include connected and autonomous vehicles communications, hybrid communications and networking, digital signal processing, RF/wireless communications, and engineering education. She is a senior member of Institute of Electrical and Electronics Engineers (IEEE), IEEE-VTS Society, Society of Automotive Engineers (SAE), and member of American Society of Engineering Education (ASEE).

How to cite this paper: Mehnaz Tabassum, Aurenice Oliveira, "Cyber-resilient Routing for Internet of Vehicles Networks During Black Hole Attack", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.12, No.4, pp. 1-14, 2022. DOI:10.5815/ijwmt.2022.04.01