Scientific Research Publishing

Journal of Information Security, 2020, 11, 71-80
http://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

Real Time Vehicular Traffic Simulation for Black Hole Attack in the Greater Detroit Area

Abdulaziz Alshammari[1], Mohamed A. Zohdy[2], Debatosh Debnath[3], George Corser[4]

[1]College of Computer and Information Sciences, IMSIU, Riyadh, KSA
[2]Electrical and Computer Engineering Department, Oakland University, Rochester, MI, USA
[3]Computer Science and Engineering Department, Oakland University, Rochester, MI, USA
[4]Department of Computer Science & Information Systems, Saginaw Valley State University, University Center, MI, USA
Email: aashammariaziz@gmail.com

How to cite this paper: Alshammari, A., Zohdy, M.A., Debnath, D. and Corser, G. (2020) Real Time Vehicular Traffic Simulation for Black Hole Attack in the Greater Detroit Area. *Journal of Information Security*, **11**, 71-80.
https://doi.org/10.4236/jis.2020.111004

Received: January 10, 2019
Accepted: December 20, 2019
Published: December 23, 2019

Abstract

Vehicular Ad-hoc Networks (VANETs) technology has recently emerged, and gaining significant attention from the research because it is promising technologies related to Intelligent Transportation System (ITSs) and smart cities. Wireless vehicular communication is employed to improve traffic safety and to reduce traffic congestion. Each vehicle in the ad-hoc network achieves as a smart mobile node categorized by high mobility and forming of dynamic networks. As a result of the movement of vehicles in a continuous way, VANETs are vulnerable to many security threats so it requisites capable and secure communication. Unfortunately, Ad hoc networks are liable to varied attacks like Block Hole attacks and Grey Hole attacks, Denial of service attacks, etc. Among the most known attacks are the Black Hole attacks while the malicious vehicle is able to intercept the data and drops it without forwarding it to the cars. The main goal of our simulation is to analyze the performance impact of black hole attack in real time vehicular traffic in the Greater Detroit Area using NS-2 and SUMO (Simulation of Urban). The simulation will be with AODV protocol.

Keywords

Black Hole Attacks, Vehicular Ad Hoc Networks, AODV Protocol, Simulation, SUMO, Greater Detroit Area

1. Introduction

VANETs enable communication between vehicles and Road Side Units (RSUs). Each vehicle or an RSU represents a node in VANET. Each vehicle in VANET has a device called On-Board Unit (OBU) to communicate with other vehicles

and RSUs [1]. VANET is a self-organized Vehicular Ad-hoc Network for communication between automobiles and roadside infrastructure. VANETs are vulnerable to many security attacks, malicious intrusion and Black hole is one among these attacks [2]. The increasing connectivity between and within vehicles and V2X has only made malicious attacks more scalable and, in worst case scenarios, capable of disrupting transportation in cities. The black hole attacks are, for present purposes, of particular importance. Capable of going undetected in ad hoc networks and intercepting node communications, black hole attacks represent a major security threat for ad hoc networks in general and VANET in particular AODV (Ad-hoc On-Demand Distance Vector) is one of the routing protocols employed in VANETs to establish routes to destinations through which data packets travel [3] [4]. Security attacks can occur in all types of protocols in VANETs and this paper examines the performance of AODV protocol under Black Hole threat. There are several concerns about the privacy and security of connected automotive and the Intelligent Transport Systems (ITSs) with many attacker models for connected automotive being practiced. Among these problems are cyber security threats on the vehicular communication system where hackers may exploit any potential weaknesses in the system by spoofing and jamming its networks. This would lead to Vehicle-to-Everything (V2X) system being impacted by unreliable signaling, which delays network so as to secure that the message transferred is partial and does not complete its intended commitments. Hacking through the internet is a very scary threat to connected vehicles. Miller and Valasek were clever to control that the Jeep Cherokee intelligence system had cyber security weakness and they compromised its entertainment system, air conditioning system, steering and brakes while the car was occupied with a driver [5]. The paper is organized as follows: Section 2 is the AODV protocol, while explaining Black hole attacks in Section 3. Then in Section 4, relevant related works are discussed. Section 5 describes simulation environments. Section 6 evaluates the analysis of simulation results. Finally, the conclusion is provided in Section 7.

2. AODV

AODV protocol is a routing protocol employed in VANET. It is a reactive routing protocol where the route gets active only when the source node wants to transmit data packets to other nodes which are making on request [6]. AODV protocol supports both unicast and multicast broadcasting. It uses control messages to find route between source and destination nodes. The control messages are Route Request message (RREQ), Route Reply message (RREP), and Route Error Message (RRER) [7] [8].

In VANET network, when a vehicle wants to send data packets to another vehicle but does not know the path to a destination, it generates a RREQ message and sends it across the network. Vehicles that receive this RREQ message check their routing table to know if they have a destination route. If they find a fresh route, they reply back with a unicast RREP packet to the source vehicle. The

freshness of a route is indicated by a high sequence number in AODV protocol. The RREP message replies back by incrementing the sequence number in the original RREQ packet. If they do not find a route, they rebroadcast the RREQ message to the source vehicle. The source starts to send data packets to the destination node as soon as it receives the RREP message from it. When a path could not be set to the destination node, the neighboring nodes send a RRER packet to the source [9] [10].

3. Black Hole Attacks

Black holes attack in VANETs is a denial-of-service attack by a node or a router. It either refuses to participate in the network or drops the data packets instead of transmitting them. Since the attack is carried out by internal malicious nodes inside the network, this is an insider type of attack. There may be a single black hole or a collaborative black hole when some malicious nodes collaborate to behave as the normal route. This type of attack happens in all types of routing protocols. This attack reduces the performance of VANETs [11].

Traffic is redirected in the black hole area in VANET. Data packets are directed to the malicious vehicle with the promise of having the shortest route. In AODV protocol, the attacker takes advantage of the AODV property of having the highest sequence number for a new route. A malicious node introduces itself as having the shortest route to the destination and cheats the AODV protocol. A malicious node waits for neighboring nodes to send RREQ request. When it receives a RREQ message, it does not check the routing table, but sends a false RREP message immediately. Therefore, getting the route to destination, and settles with a high sequence number in the source node, before other nodes reply back. Requesting nodes assume that route discovery process is finished and start to send packets to this malicious node. The malicious node does not own a route to further forward the data packets and loss all the received packets [12].

Figure 1 shows the schematic diagram of a black hole attack. Vehicle A wants to send data packets to Vehicle J, but does not know the route to node F. Node A initiates a route discovery process by sending RREQ messages to other neighborhood nodes. Malicious node D intercepts the message, claims that it has an active route to F, and pretends that it is the next node from A to reach F. Equations.

4. Related Works

Security is, undoubtedly, one most important issue in ad hoc networks. To address black hole attacks, a growing body of works offers innovative solutions. We will focus on the simulation studies because VANET does not have data but, most of researchers in this field have evaluated the performance of AODV in Vehicular ad hoc by simulation. Grimaldo and Martí [13] evaluated the performance impact of black hole attacks on Vehicular ad hoc networks in real traffic scenarios in Panama City. They analyzed four protocols which are AODV, OLSR, DSR and DSDV by using NS3 and SUMO. More research done by Ahmed *et al.* [14] analyzed the impact of Blackhole attack on the VANET's reactive and

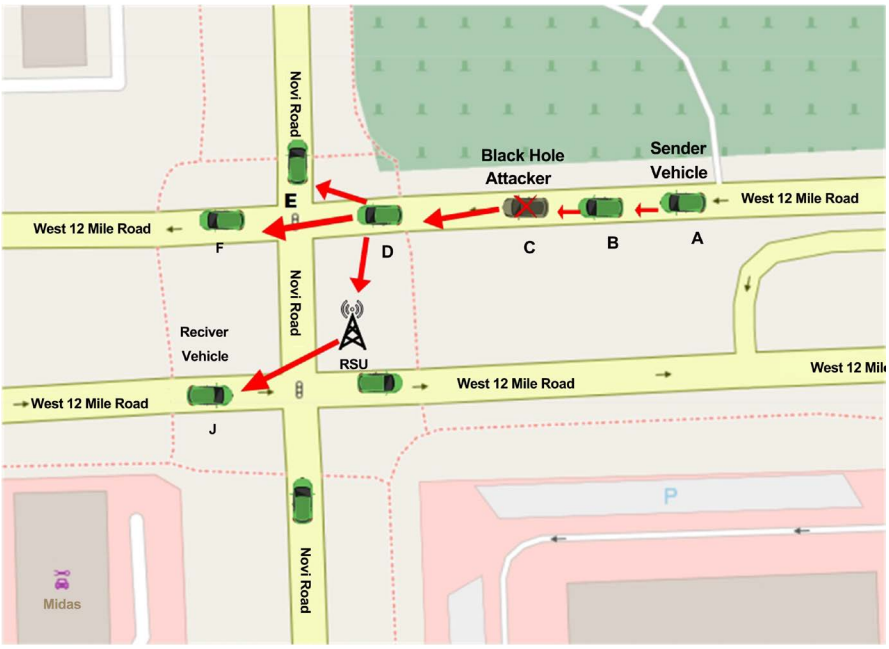

Figure 1. Black hole attack simulation scenario.

proactive routing protocols including AODV, DSR, OLSR, and TORA. They used OPNET modeler 14.5. The results of their simulation display that the impact of Black hole attack on AODV is more than other protocols.

Afdal *et al.* [15] examine and analyze the influence of the black hole attack on the AODV and AOMDV routing protocols performance in vehicular ad hoc networks. They found that both AODV and AOMDV are vulnerable to black hole attacks in VANET. Results showed that AOMDV network performance is better than AODV because AOMDV routing uses multipaths but, AODV provides unipath routing.

Gurung and Chauhan [16] simulated two types of attacks: (GAODV) and (SGAODV). GAODV is a series number founded gray hole attack protocol while SGAODV is a smart gray attack due to examining AODV, IDS-AODV and MBDP-AODV by using NS-2. The result showed that impact of gray hole attack on AODV is low as compared with the impact of series number founded gray-hole attack on AODV protocol is lower than its impact of sequence of number on AODV. Moudni *et al.* [17] analyzed black hole flooding and rushing attacks AODV. Deshmukh *et al.* [18] used NS-2 to simulate ADOV and DSR performance under Black hole attack. However, Kaushik and Dureja [19] proposed a solution to modify the AODV routing protocol in such a way that it can block the cooperative Black Hole attack.

5. Simulation Environments

We analyze the vulnerability of black hole attack against AODC routing protocol performance by using SUMO and NS2 simulator. We measured the performance of AODV under Black hole attacks in The Greater Detroit Area mobility model

as shown in Figure 1. We created a real map mobility traces from OpenStreetMap [20]. After taking the map from OpenStreetMap, we converted an osm map to xml file to read all information from it. Then we created the new file from the xml file with 100 vehicles and save it as cfg extension file. We got the real world map from manipulating the map.

In the simulation scenario, the total vehicles involved 100 vehicle nodes that moving randomly on the extracted map (1 Mile × 1 Mile) and the speed of cars is based on the roads speed limit. We supposed the maximal transmission range is 250 m and it is able to a message in the size of 512 bytes. As we mentioned before that we apply the analysis on AODV routing protocol. The traffic sending rate is 10 packets per second as shown in Table 1. We add two black holes nodes, Vehicle number 25 and 53 are black hole nodes. Figure 3 shows a section part of Figure 2 but concentrated to make vehicles visible. When run SUMO and choose the real-world mode, we can see the vehicle moving in the roads. We have faced an issue that we did with the big area so it's hard to see the vehicle but we maximum it in order to see how the simulation working. Figure 3 shows how cars are moving in the real world map.

The general structure of the simulation model is shown in Figure 4.

6. Simulation Analysis

We analyze the performance of AODV routing protocol under Black hole attack on the Vehicular ad hoc networks in real traffic area. Black hole attack is considered a type of Denial-of-Service attack (DoS), so we examine the packet delivery ration, throughput and packet loss. From the result is obvious that black hole nodes impact on the vehicular networks.

a) *Packet Delivery Ratio*

The Packet delivery ratio calculate the number of packets arrived the destination against those packets that have sent by the source [17], and the best case when all packets get and deliver to the final destination. Figure 5 shows the PDR result.

Table 1. Simulation parameters.

Parameters	Values
Simulator	NS-2
Simulation Area (MI × MI)	1 × 1
Simulation Time	200 sec
Movement Model	Greater Detroit Area
Communication Protocol	802.11p
Routing Protocols	AODV
Number of Vehicles	100
Packet Size (Byte)	512
Traffic Type	Constant Bit Rate (CBR)

Figure 2. Extracted map from OpenStreetMap for greater Detroit area.

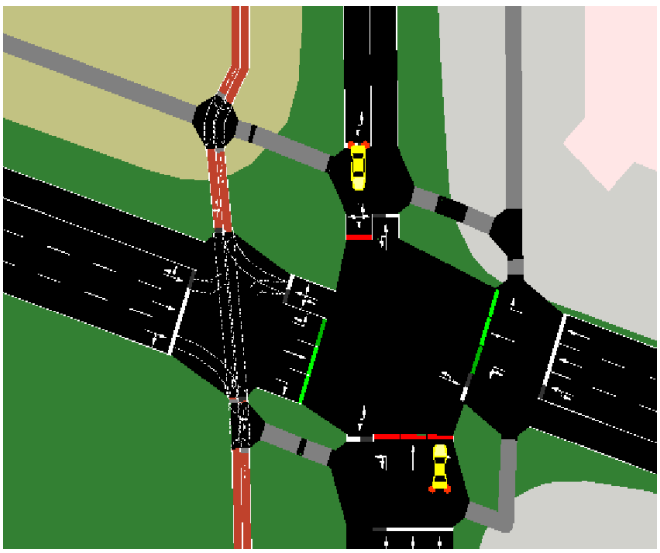

Figure 3. A section of Figure 2.

b) *Throughput*

Throughput is the ratio of whole number of packets received to total number of packets that send by the source [17]. The throughput is shown in Figure 6.

c) *End to End Delay*

We calculate the End to End is by time takes for a packet to deliver from the source node to the destination node [17]. This metric covers the data packets actually received. Figure 7 shows the end to end delay.

7. Conclusion

Nowadays the number of mobility has increased exponentially, and implanting Vehicular ad hoc technology will face many security threats, whether in communication between vehicle or V2X. Black hole attacks are one of these

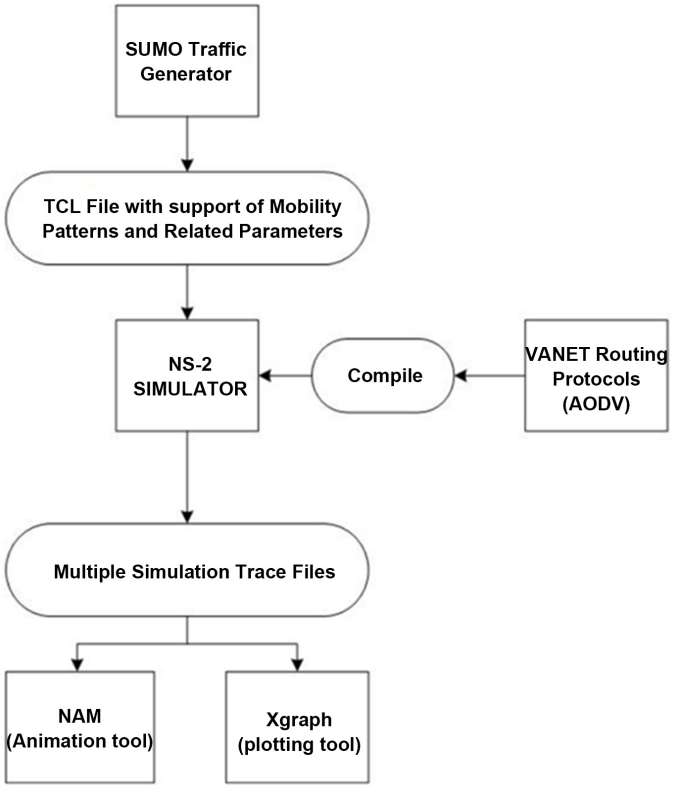

Figure 4. Model of simulation.

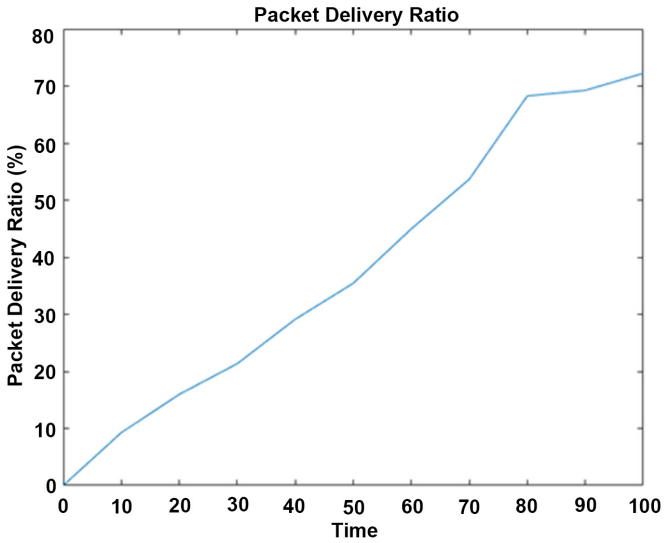

Figure 5. Packet delivery ratio.

threats and it represents a dangerous security threat for VANET. This attack occurs due to the lack of protocols in VANET. ADOV is one of these protocols and it is vulnerable for many attacks. In this paper, we have analyzed the impact of Black hole attack on AODV protocol in the Greater Detroit Area by using SUMO and NS2. Based on Packet Delivery Ratio, Throughput and End to End Delay charts, we can see obviously how black hole attacks effect on communication between

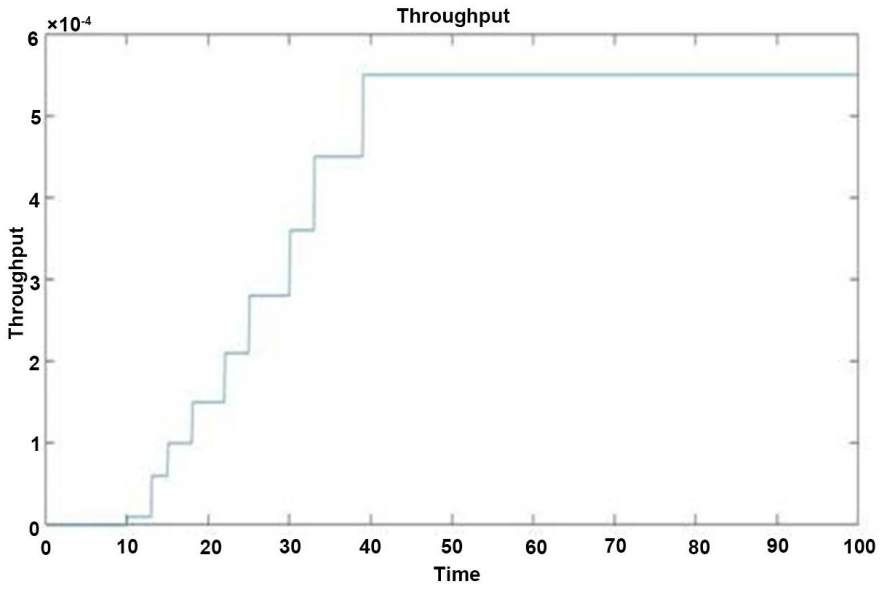

Figure 6. Throughput.

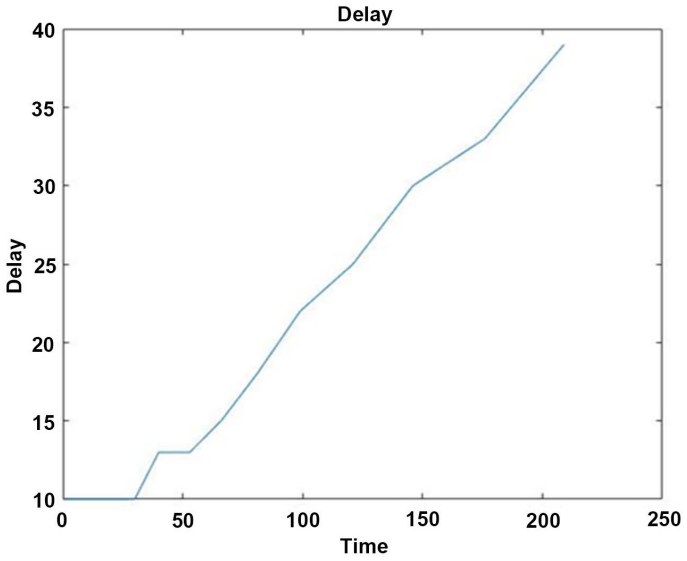

Figure 7. End to end delay.

vehicles. From the results of our analyzed study, we got that Packet Delivery Ration, Throughput, and End to End Delay with AODV protocol in Black hole attacks caused a real issue in Vehicular ad-hoc networks performance.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Zaidi, K. and Rajarajan, M. (2015) Vehicular Internet: Security & Privacy Challenges and Opportunities. *Future Internet*, **7**, 257-275.

https://doi.org/10.3390/fi7030257

[2] Alshammari, A., Zohdy, M.A., Debnath, D. and Corser, G. (2018) Classification Approach for Intrusion Detection in Vehicle Systems. *Wireless Engineering and Technology*, **9**, 79-94. https://doi.org/10.4236/wet.2018.94007

[3] Kaur, T. and Verma, A.K. (2012) Simulation and Analysis of AODV Routing Protocol in VANET. *International Journal of Soft Computing and Engineering*, **2**, 293-301.

[4] Jamali, S.B.S. (2015) A Survey over Black Hole Attack Detection in Mobile ad Hoc Network. *International Journal of Computer Science and Network Security*, **15**, 44.

[5] Miller, C. and Valasek, C. (2015) Remote Exploitation of an Unaltered Passenger Vehicle. Black Hat USA.

[6] Van Glabbeek, R., Höfner, P., Portmann, M. and Tan, W.L. (2016) Modelling and Verifying the AODV Routing Protocol. *Distributed Computing*, **29**, 279-315. https://doi.org/10.1007/s00446-015-0262-7

[7] Kumar, J., Kulkarni, M. and Gupta, D. (2013) Effect of Black Hole Attack on MANET Routing Protocols. *International Journal of Computer Network and Information Security*, **5**, 64. https://doi.org/10.5815/ijcnis.2013.05.08

[8] Singh, H. and Singh, M. (2013) Securing MANETs Routing Protocol under Black Hole Attack. *International Journal of Innovative Research in Computer and Communication Engineering*, **1**, 808-813.

[9] Shahabi, S., Ghazvini, M. and Bakhtiarian, M. (2016) A Modified Algorithm to Improve Security and Performance of AODV Protocol against Black Hole Attack. *Wireless Networks*, **22**, 1505-1511. https://doi.org/10.1007/s11276-015-1032-y

[10] Abdulkader, Z.A., Abdullah, A., Abdullah, M.T. and Zukarnain, Z.A. (2017) LI-AODV: Lifetime Improving AODV Routing for Detecting and Removing Black-Hole Attack from VANET. *Journal of Theoretical & Applied Information Technology*, **95**, 196-209.

[11] Bibhu, V., Kumar, R., Kumar, B.S. and Singh, D.K. (2012) Performance Analysis of Black Hole Attack in VANET. *International Journal of Computer Network and Information Security*, **4**, 47. https://doi.org/10.5815/ijcnis.2012.11.06

[12] Alheeti, K.M.A., Gruebler, A. and McDonald-Maier, K.D. (2015) An Intrusion Detection System against Black Hole Attacks on the Communication Network of Self-Driving Cars. 6*th International Conference on Emerging Security Technologies*, Braunschweig, 3-5 September 2015, 86-91. https://doi.org/10.1109/EST.2015.10

[13] Grimaldo, J. and Martí, R. (2018) Performance Comparison of Routing Protocols in VANETs under Black Hole Attack in Panama City. *International Conference on Electronics, Communications and Computers*, Cholula, 126-132. https://doi.org/10.1109/CONIELECOMP.2018.8327187

[14] Ahmed, E.F., Abouhogail, R.A. and Yahya, A. (2014) Performance Evaluation of Blackhole Attack on Vanet's Routing Protocols. *Science and Engineering Research Support Society*, **8**, 39-54.

[15] Afdhal, A., Muchallil, S., Walidainy, H. and Yuhardian, Q. (2017) Black Hole Attacks Analysis for AODV and AOMDV Routing Performance in VANETs. *International Conference on Electrical Engineering and Informatics*, Banda Aceh, 18-20 October 2017, 29-34. https://doi.org/10.1109/ICELTICS.2017.8253244

[16] Gurung, S. and Chauhan, S. (2019) Performance Analysis of Black-Hole Attack Mitigation Protocols under Gray-Hole Attacks in MANET. *Wireless Networks*, **25**, 975-988.

[17] Moudni, H., Er-rouidi, M., Mouncif, H. and El Hadadi, B. (2016) Performance Analysis of AODV Routing Protocol in MANET under the Influence of Routing Attacks. *International Conference on Electrical and Information Technologies*, Tangiers, 4-7 May 2016, 536-542. https://doi.org/10.1109/EITech.2016.7519658

[18] Deshmukh, S.R., Chatur, P.N. and Bhople, N.B. (2016) AODV-Based Secure Routing against Blackhole Attack in MANET. *IEEE International Conference on Recent Trends in Electronics*, *Information & Communication Technology*, Bangalore, 20-21 May 2016, 1960-1964. https://doi.org/10.1109/RTEICT.2016.7808179

[19] Kaushik, N. and Dureja, A. (2013) Performance Evaluation of Modified AODV against Black Hole Attack in MANET. *European Scientific Journal*, **9**, 182-193.

[20] Open Street Map. https://www.openstreetmap.org