Journal of Theoretical and Applied Information Technology
15th March 2021. Vol.99. No 5

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

THE INFLUENCE OF BLACK HOLE ATTACK IN ROUTING EFFICIENCY IN MANET

[1*]MAHA ABDELHAQ, [2]RAED ALSAQOUR, [1]HANEEN AL-ABDULLATIF, [1]WALAA AL-TAMIMI, [1]REHAM AL-ANAZI, [1]MAISA AL-SIBAIE, [1]AMAL AL-ZAHAMI, [1]SHEUIHINAH AL-OTAIBI

[1]Department of Information Technology, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, 84428 Riyadh, Saudi Arabia.

[2]Department of Information Technology, College of Computing and Informatics, Saudi Electronic University, 93499 Riyadh, Saudi Arabia.

E-mail: [1]msabdelhaq@pnu.edu.sa (Corresponding Author), [2]raed.ftsm@gmail.com

ABSTRACT

Mobile Adhoc Network (MANET) is a combination of mobile nodes in a non-infrastructure network in which nodes communicate continuously without a centralized network manager. MANET nodes act as routers and are dependent on one another to keep the network connected. Due to the nature of the MANET network, it is vulnerable to different types of attacks including Blackhole, Denial of Service, and Rushing. Blackhole attack is a harmful active attack on MANET (also called Selfish node attack). In this paper, we present a comparative study on blackhole attack resistance utilizing three types of routing protocols. The three protocols are Ad hoc On-Demand Distance Vector (AODV), Zone Routing Protocol (ZRP) and Optimized Link State Routing Protocol (OLSR). This paper's main contribution is to introduce a new model for blackhole simulation of attacks in Network Simulator Version 2 (NS2). In terms of throughput and end-to-end delay, the efficiency of the three routing protocols will be tested under the direct influence of blackhole attacks.

Keywords: *MANET, Routing protocol, Blackhole attack, AODV, ZRP, OLSR*

1. INTRODUCTION

The Mobile Ad Hoc Network (MANET) is a group of mobile nodes that automatically create a temporary wireless network without infrastructure. [1, 2]. The network is suitable for different applications, such as emergency relief and military operations [3]. Within MANET, a few nodes can communicate through a single wireless connection or a series of wireless connections involving multiple intermediate nodes in several ways. For this purpose, an efficient MANET routing protocol must accommodate several different types of limitations, such as low battery energy [4], low bandwidth [5], high error rates [6], and time-variate channels, which are fundamentally applicable to the nodes and wireless connections [7, 8]. Therefore, the frequent changes in topology generated by mobility nodes must be handled. Implementing an accurate and stable routing protocol thus constitutes one of the MANET issues [9]. The lack of infrastructure and dynamic topology are critical issues for MANET, which are heavily influenced by multiple types of attack, for instance, the blackhole intrusion effect of malicious nodes [10-13].

In this article, we present a new model by extensively evaluating the impact of blackhole attacks on the MANET performance of the routing protocols: Ad hoc On-Demand Distance Vector (AODV), Zone Routing Protocol (ZRP) and simulator Optimised Link State Routing Protocol (OLSR). We also test the efficiency of the simulation model with network throughput and average delay metrics. The study is very relevant to choose from the three protocols the most resistance routing protocols to prevent and track the blackhole attack effect of the routing MANET. To the best of our knowledge, no researcher has introduced such study until now.

The remainder of the article is arranged accordingly. In Section 2, we provide background and related work. Section 3 presents the simulation settings. In section 4, we explain the findings and discussions. Finally, in Section 5, the findings and future recommendations for further work are discussed.

2. BACKGROUND AND RELATED WORK

2.1 Mobile Ad-Hoc Network (MANET)

Mobile nodes in MANET are movable (dynamic) forming a temporary network [14, 15]. If the source and destination nodes are distant from each other (outside direct transmission range), they communicate using a sequence of intermediate nodes, which co-operate to forward the traffic to the destination. MANET is easy to set up in short intervals. This can be useful in natural disasters and wars. Furthermore, MANET has several beneficial advantages such as low budget and effortless installation due to the absence of infrastructure and wires, also for the same reason it has an easy deployment and configuration [16, 17].

2.2 Ad hoc On-Demand Distance Vector Routing (AODV) protocol

AODV is a reactive protocol where a network builds routes at the beginning of the connection [14, 15]. Especially for MANET, AODV was developed. It gets solely on-demand routes that transform it into a very beneficial and needed MANET algorithm. To identify and manage routes, AODV carries out two distinct operations: route discovery and maintenance. AODV uses two signals to monitor the path discovery and route maintenance process. Control messaging used by AODV include: Route Request (RREQ), Route Reply (RREP) and Route Error (RERR).

The discovery of the route would rely on the RREQ and RREP. In routing table entries, the path information for the intermediate nodes is stored. The discovery process is shown in Figure. 1. In Figure. 1, the route discovery source is initiated by sending the RREQ message. In Figure. 2, as the RREQ is obtained by the destination or mid-node, the RREP will be sent to the source node and the hop-count and destination node sequence number is applied to the routing table. Afterward, the RREP message is unicasted to the source node. The route is configured when an RREP is sent to the source node. The message includes the full route to the destination and is stored with next-hop addresses. Maintenance of routes depends, however, on the RERR communication and can handle the dynamic MANET network topology. The RERR message also controls the routes by transmitting a warning of a link failure to the other nodes.

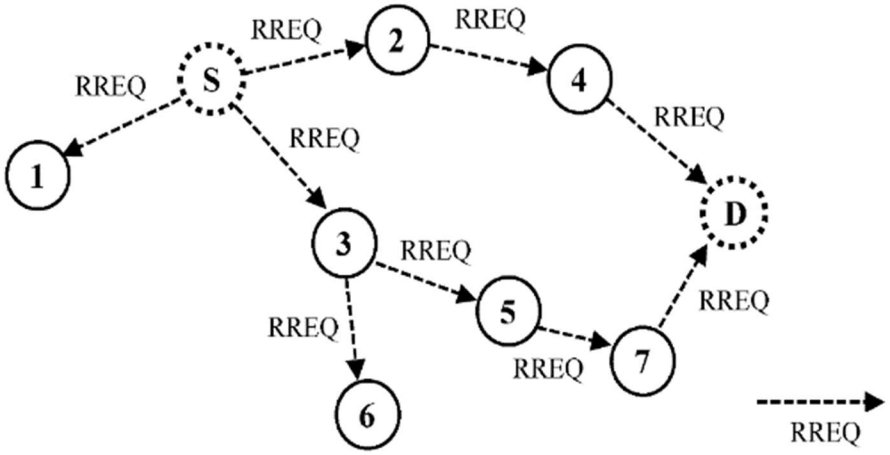

Figure 1: AODV broadcasts RREQ packet

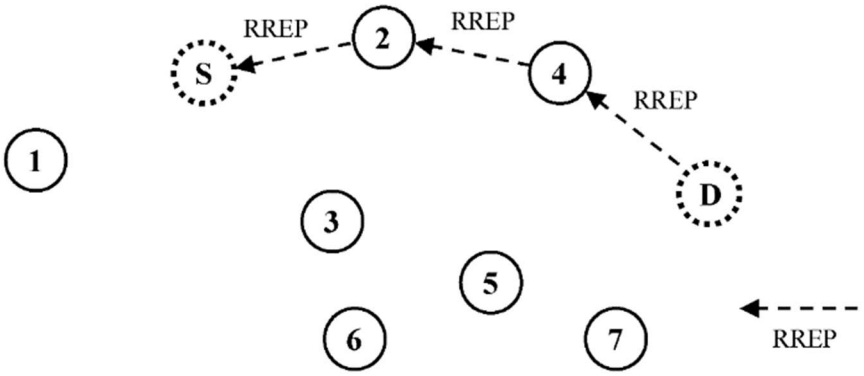

Figure 2: AODV replies RREP packet

2.3 Optimized Link State Routing Protocol (OLSR)

OLSR is an ad hoc wireless network protocol proactive routing [16, 17]. The protocol adopts the reliability of a link algorithm and has the benefits of having accessible routes as soon as possible, because of its proactive design. OLSR is a traditional, mobile ad hoc network optimization link-state protocol. OLSR is fully distributed and does not depend on any single corporation. Reliable control message communication is not required by the protocol. Every node regularly sends control messages so that some of the messages can be relatively lost. These disruptions are often triggered by collisions or other communication problems in radio networks.

The OLSR protocol typically utilizes two forms of forwarding messages, Hello and Topology Control (TC). Message Hello is a message to pick a neighbor sensing and a multipoint relay (MPR). Each node in the network selects a group of nodes that relay messages in its symmetrical 1-hop neighborhood. The MPR set is a set of selected neighbor nodes. Each node generates regular HELLO messages in OLSR. The Hello message to a node includes its own address and its neighbors. By exchanging Hello messages, each node will learn a complete topology of up to two hops. The Hello messages are localized and not transmitted to other nodes via local neighboring nodes. The TC message is the message used to specify the route. OLSR also advertises TC messages at each MPR node. A TC address includes the MPR selector set for senders. In OLSR, the responsibility for forwarding TC messages lies with only MPR nodes. Once all MPR nodes receive TC messages, each node is able to learn the network's partial topology and establish a route to each node inside the network. A collection of MPR nodes can be selected for each node to relay its routing messages. A node in OLSR selects its MPR set which can be reached in two hops by all its neighbors. The minimal set is chosen as MPR when several choices are made.[18].

Figure. 3 demonstrates a message transmitting the node in the middle, with neighbors and 2-hop neighbors. In (a) all nodes retransmit the transmission, whereas in (b) only the main node MPRs retransmit the transmission.

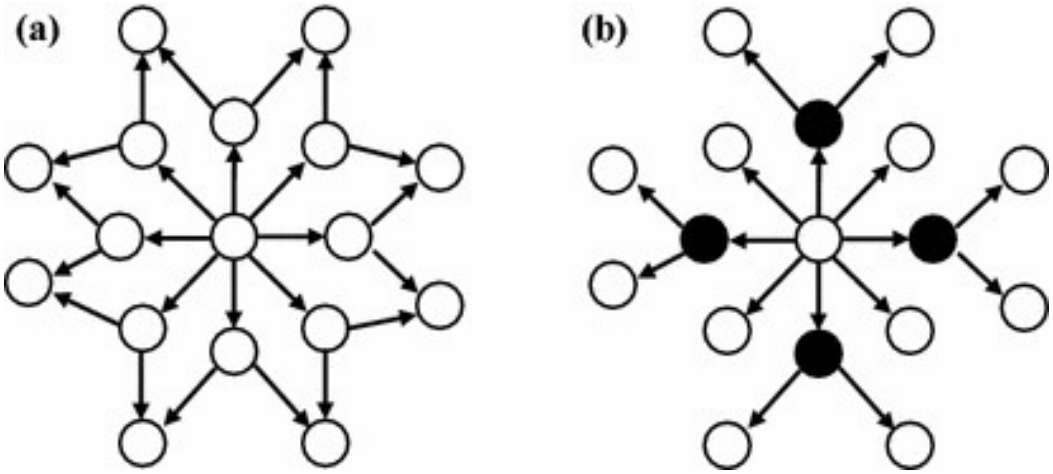

Figure 3: (a) Pure flooding. (b) MPR flooding [19]

2.4 Zone Routing Protocol (ZRP)

The Zone Routing Protocol (ZRP) is a hybrid protocol that incorporates and combines reactive and adaptive protocol capabilities to improve the performance of routing [20-22]. The network is separated into zones as shown in Figure. 4, and uses Two different zones of different protocols, i.e. Within this zone one protocol is used and the other protocol is used within it. ZRP uses a proactive mechanism to set up routes within the neighborhood of the node and use reactive protocols to inter-neighborhood communications. Regional areas are called zones and for the same reason, the protocol has been named as the zone routing protocol. Every zone can have different sizes, and within each node, there may be several overlapping zones. A zone's nodes are broken down into outer nodes and inner nodes. Peripheral nodes are nodes with a minimum diameter exactly equal to that of the radius of the central node region. There are nodes with less than the zone radius of the minimum length. [23].

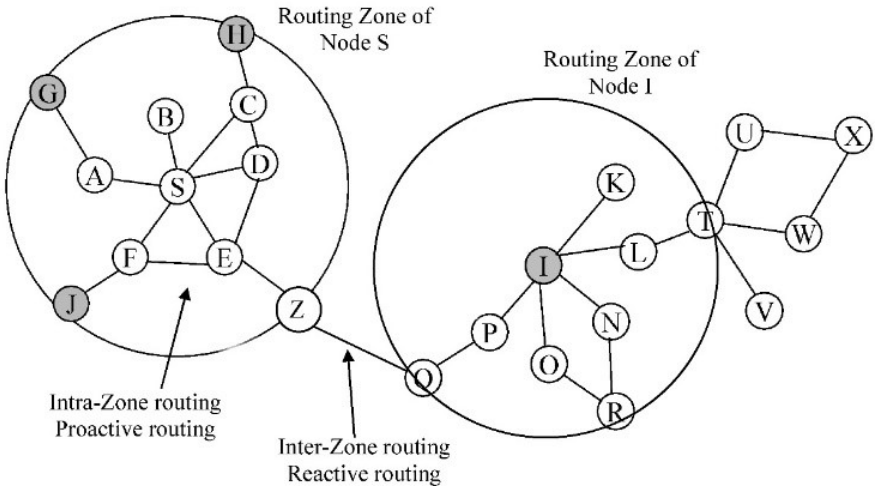

Figure 4: Zone Routing Protocol

2.5 Blackhole Attack

There can be many attacks in different layers of the network, but we have been focusing in our paper on a blackhole attack as a layered threat [24-26]. The basic idea behind the blackhole attack on the network layer, as shown in Figure. 5, is to inject oneself into the active pathway from source to destination [27]. As RREQ packets are sent, the

blackhole attack claims to provide the optimum path to the destination node and to return the RREP with the maximum target sequence number and the minimum hop count length to the source node.

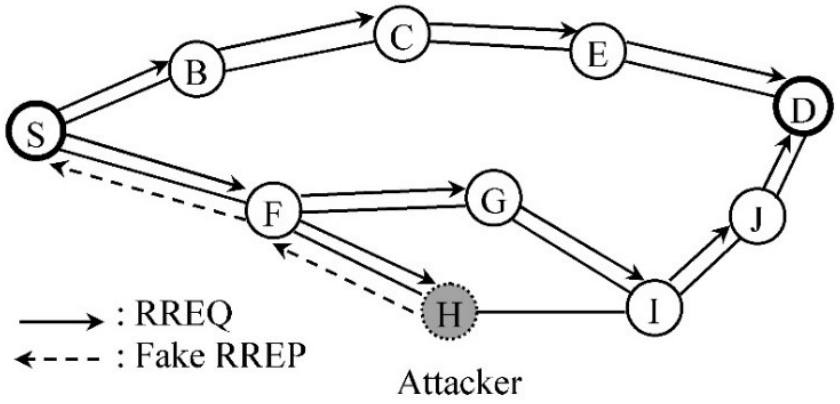

Figure 5: Blackhole attack

2.6 Related Work

In [28], the authors provided a comparative performance analysis of AODV routing protocols and Dynamic Source Routing (DSR), using different speeds in MANET's wormhole attack. The analysis is performed using a network emulator QualNet 5.0.2. Results showed that the presence of a wormhole attack affects the performance and the average time between the source and destination of the AODV and DSR routing protocol in the mobile ad-hoc network. The results showed that in terms of throughput and average end-to-end latency, the existence of a wormhole attack affects the efficiency of the ad hoc mobile network AODV and DSR routing protocol.

In [29], the authors proposed an AODV routing protocol simulation-based RCA impact study on the MANET performance. The findings of this research open the door to a program for intrusion detection that mitigates and avoids horrible RCA consequences on MANET.

In [30], the AODV and TORA protocols' performance was compared by the authors based on load, packet loss, time, throughput and the delivery ratio of the packet. The TORA simulation results showed that TORA worked much better than AODV with a Distributed Denial-of-Service (DDoS) attack [31]. Likewise, AODV performed much better in normal conditions.

In [32], the authors studied and analyzed the performance of blackhole, gray hole, selfish and flooding routing protocols for both AODV and Secure Ad hoc On-Demand Distance Vector (SAODV). The findings have concluded that the attacks of blackhole and flooding had a dramatic impact on network performance. Because a fake RREP is introduced by the blackhole attack. In the presence of blackhole, graywhole and selfish attacks, on the other hand, SAODV's performance is better than AODV because SAODV does not forward the routing packets without ensuring authenticity and integrity.

In [33], the four well-known protocols OLSR, DSDV, AODV and DSR were performed on detailed performance analysis. It has been found that each protocol has its advantages and disadvantages under regular network operations (without attack) and no better protocol is possible to identify. Nonetheless, without taking the security issues account, all the routing protocols considered were designed. Some protocols that performed better without attack scenarios often fail to deliver the same output during attacks. It highlights the need to discuss safety aspects during the implementation of a MANET routing protocol. In addition, a general security mechanism is required that can be used by protocols to reduce the impact of malicious nodes by removing them from the routing path [34].

3. SIMULATION ENVIRONMENT AND SETTINGS

We use the ns-2.35 simulator to conduct our experiments, ns2 has many tools to help researchers

in performing their work. In our experiments, we use a "setdest" CMU method to create many nodes and their movements; the tool uses a random waypoint model. The number of nodes is 20 nodes, with a flat grid x-800, y-800, and the simulation time is 100 seconds. The nodes that chosen to be malicious blackhole attackers start their attacks at the beginning of the simulator, we create Constant Bit Rate (CBR), it starts at the beginning of the simulator until the simulator ends the following illustrates the CBR options. Table 1 lists the simulation parameters and their values.

Table 1: Simulation Parameters

Parameter	Value	Unit
Simulator	NS-2 (Version 2.35)	-
Simulation time	100	s
Number of nodes	20	nodes
Pause time	2	s
Node speed	0-5	m/s
Simulation Area	800 X 800	m2
Routing Protocols	AODV, OLSR, ZRP	-
Mobility Model	Random Way Point	-
Source Type	CBR	-
Mobility Model	Random Way Point	-
Source Type	CBR	-
Packet size	512	bytes
Packet rate		
Maximum packets	1000	packet
Number of attackers	1-4	-
Packet rate	10 packet/s	-
Channel type	Channel/Wireless channel	-
Radio-propagation model	Propagation/Two ray round wave	-
Network interface type	Phy/WirelessPhy	-
MAC Type	Mac /802.11	-
Interface queue Type	Queue/Drop Tail	-
Al Type	LL	-
Antenna	Antenna/Omni Antenna	-

Figure. 6 shows the topology for modelling networks used in simulation experiments. The source node is node number (1), the destination node is node number (7), and node number (5) is the attacker.

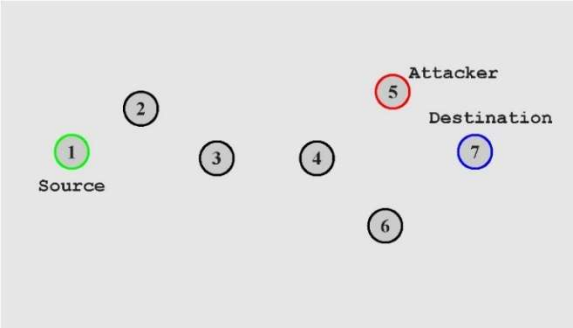

Figure 6: Network simulation topology

In this article, we examine the effect of the blackhole attack on the ad hoc routing protocols, including throughput and end-to-end delay measurements.

3.1 End-to-End (E2E) delay

The E2E delay refers to the average time consumed in one millisecond to transfer a data packet successfully from source to destination across your network [35]. It includes any delay, such as latency of route discovery buffering, media-control retransmission delay (MAC), lining at the queue of the interface, propagation delay and the time of transmission. The delay of E2E is calculated as follows:

$$E2E\ delay = \frac{\sum_{i=1}^{n}(R_i - S_i)}{n} \quad (1)$$

where n is the number of data packets transmitted successfully across the network, i is the unique packet ID, *Ri* is the time to receive a packet with unique ID i, and *Si* is the time it takes to send a packet with a unique ID i.

3.2 Throughput

The throughput metric is the average of efficient data packets received during the entire simulation period. This measures the efficiency and effectiveness of the routing protocol when processing data packets from the destinations [36]. Throughput estimated per second in kilobits (kbps). For measure the throughput the following formula is used:

$$Throughput = \sum \frac{Total\ bytes\ received}{Stop\ time - Start\ time} \quad (2)$$

4. RESULTS AND DISCUSSION

ZRP protocol is a hybrid protocol and has the advantages of the two approaches. As shown in

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Figures 7-10, the ZRP protocol has the highest throughput compared with AODV and OLSR protocols. It is less sensitive than other protocols against blackhole attacks. On the other hand, ZRP has the highest end-to-end delay according to its complexity, as shown in. OLSR is more sensitive than ZRP against blackhole attack, and its throughput is less than that corresponding to ZRP protocol, OLSR is precative routing approach, its throughput is more than AODV, and also it has the smallest end-to-end delay. AODV protocol has the worst throughput but stills has fewer delay values from the ZRP protocol.

AODV protocol is very sensitive to blockhole attacks. A malicious node does not have to be in the direction from source to destination, a malicious node can easily change all network topology and metrics and enforce all sender nodes to direct them traffics into this malicious node, which drops all data and causes network down. In OLSR, the sender node, if it has a malicious neighbor, the probability of redirect traffic to this malicious is very high according to hello messages. Also, if a malicious occupies a strategy place as connected two zones will cut-off traffics between these two zones. ZRP is less sensitive to the blackhole attack. The problem when a malicious node occupies a strategy place between two zones as in OLSR, the traffic between these two zones will be dropping. Also, if a sender node has one node in its range and this node is malicious, the sender will send across the malicious and all its data will be dropped, and it will get no notifications about that.

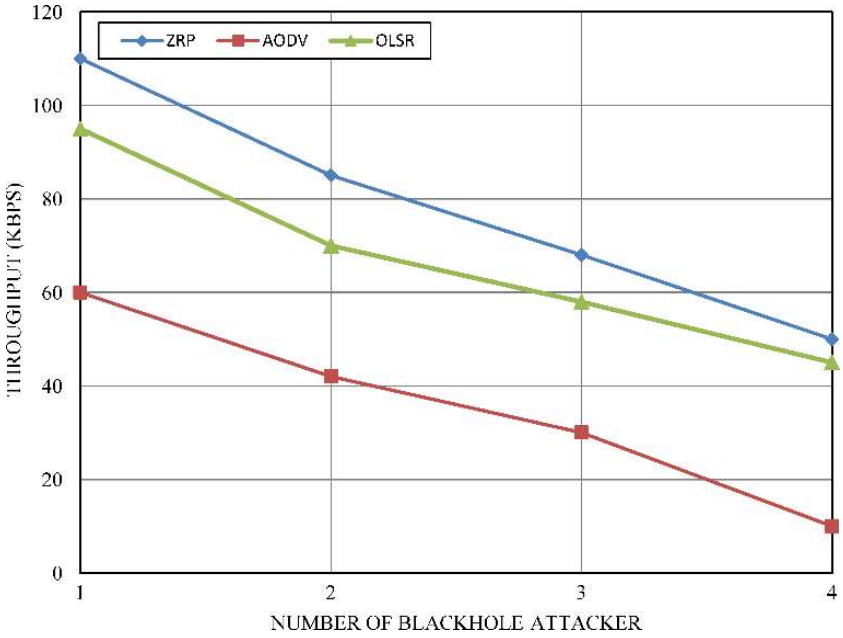

Figure 7: Throughput against the number of attackers

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

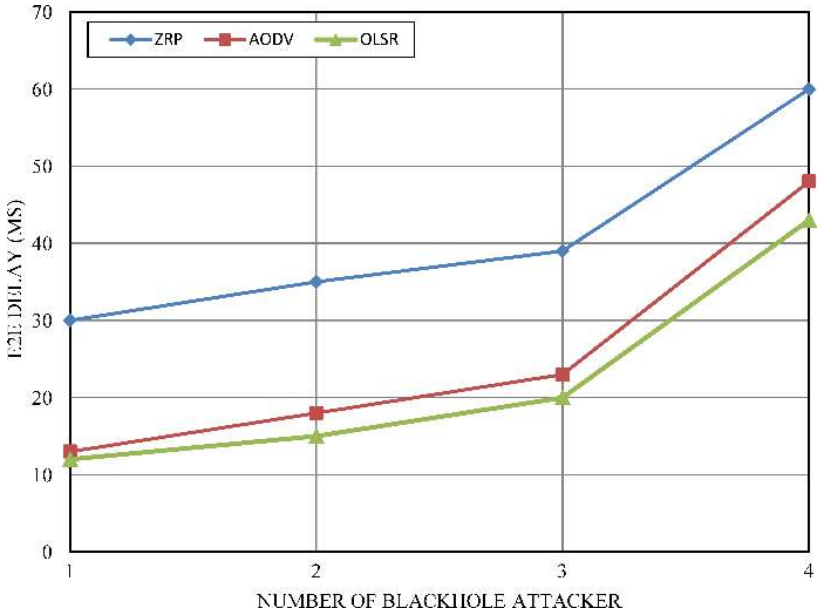

Figure 8: E2E delay against the number of attackers

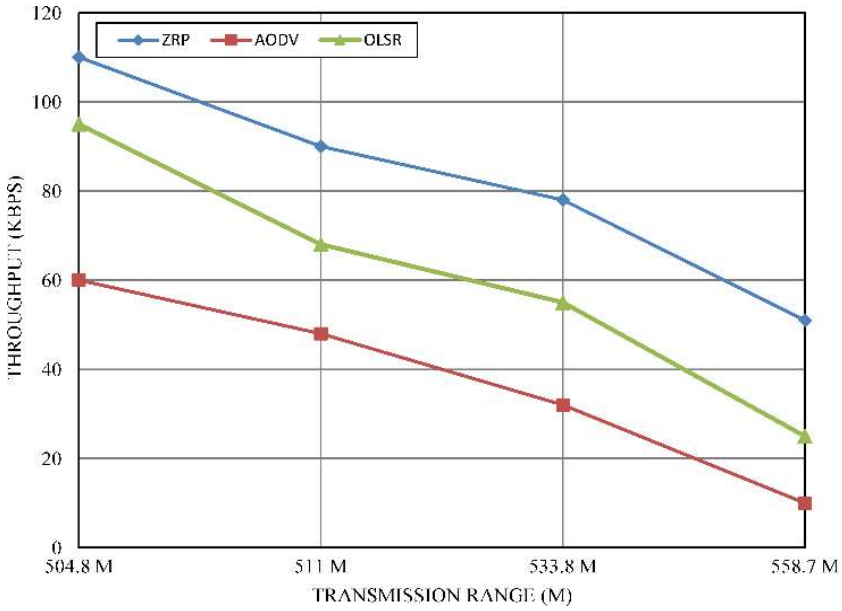

Figure 9: Throughput against the transmission

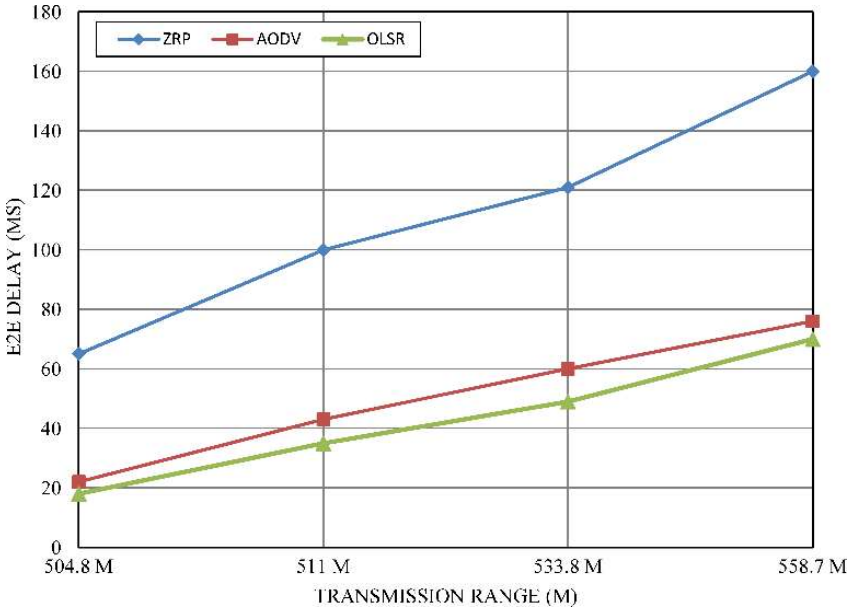

Figure 10: E2E delay against the transmission

5. CONCLUSIONS AND FUTURE WORK

In this paper, we have introduced the new blackhole attack simulation model applied on AODV, ZRP and OLSR. we also made a comprehensive analysis and comparison study between these routing protocols to show which protocol more resistance against blackhole attack. The Performance of all protocols was carried out by increasing the number of attacks with different radio ranges. The overall analysis of routing protocols has been showing that the ZRP protocol has the highest throughput against AODV and OLSR protocols. Although ZRP has the highest end-to-end delay according to its complexity in return, it was more resistant to blackhole attack compered to AODV and OLSR. To sum up, the AODV protocol has the worst throughput but on the other hand, it has fewer delay values from the ZRP protocol. OLSR was the most effected protocol against blackhole attack. Corresponding to ZRP, the throughput in OLSR was lesser but it was more than it on AODV.

In future study, we plan to expand our work with certain security algorithms in order to identify and prevent blackhole.

ACKNOWLEDGMENT

This research was funded by the Deanship of Scientific Research at Princess Nourah bint Abdulrahman University through the Fast-track Research Funding Program.

REFERENCES

[1] M. S. Daas and S. Chikhi, "Response surface methodology for performance analysis and modeling of MANET routing protocols," *Int. J. Comput. Netw. Commun.,* vol. 10, pp. 45-61, 2018.

[2] N. Raza, M. U. Aftab, M. Q. Akbar, O. Ashraf, and M. Irfan, "Mobile ad-hoc networks applications and its challenges," *Communications and Network,* vol. 8, pp. 131-136, 2016.

[3] M. Abdelhaq, R. Alsaqour, and S. Abdelhaq, "Securing mobile ad hoc networks using danger theory-based artificial immune algorithm," *PloS one,* vol. 10, p. e0120715, 2015.

[4] J. Deepa and J. Sutha, "A new energy based power aware routing method for MANETs," *Cluster Computing,* vol. 22, pp. 13317-13324, 2019.

[5] P. Jayalakshmi and R. Saravanan, "Dynamic high bandwidth nodes for routing in MANETs," *International Journal of Internet Technology and Secured Transactions,* vol. 9, pp. 1-11, 2019.

[6] G. Marcel and N. Vetrivelan, "MARMAQS: a new efficient multi-algorithm routing mechanism for acquiring high Quality of Service in MANET," *International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST),* vol. 2, 2016.

[7] A. Taha, R. Alsaqour, M. Uddin, M. Abdelhaq, and T. Saba, "Energy efficient multipath routing protocol for mobile ad-hoc network using the fitness function," *IEEE access,* vol. 5, pp. 10369-10381, 2017.

[8] M. A. Saad, H. J. Alhamdane, S. Ali, M. M. Hashim, and B. Hasan, "Total energy consumption analysis in wireless Mobile ad hoc network with varying mobile nodes," *Indonesian Journal of Electrical Engineering and Computer Science,* vol. 14, 2019.

[9] G. S. Dhillon, "Vulnerabilities & Attacks in Mobile Adhoc Networks (MANET)," *International Journal of Advanced Research in Computer Science,* vol. 8, 2017.

[10] P. Gupta, P. Goel, P. Varshney, and N. Tyagi, "Reliability Factor Based AODV Protocol: Prevention of Black Hole Attack in MANET," in *Smart Innovations in Communication and Computational Sciences*, ed: Springer, 2019, pp. 271-279.

[11] H. Alani, M. Abdelhaq, and R. Alsaqour, "Dynamic routing discovery scheme for high mobility in mobile ad hoc wireless networks," *International Journal of Electrical and Computer Engineering,* vol. 10, p. 3702, 2020.

[12] L. Al Dulaimi, "Black hole attack behavioral analysis general network scalability," *Indonesian Journal of Electrical Engineering and Computer Science,* vol. 13, pp. 677-682, 2019.

[13] T. Jamal and S. A. Butt, "Malicious node analysis in MANETS," *International Journal of Information Technology,* vol. 11, pp. 859-867, 2019.

[14] C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing," in *Proceedings WMCSA'99. Second IEEE Workshop on Mobile Computing Systems and Applications*, 1999, pp. 90-100.

[15] M. T. Sultan and S. M. Zaki, "Evaluation of energy consumption of reactive and proactive routing protocols in MANET," *arXiv preprint arXiv:1706.06322,* 2017.

[16] F. Sammy, "A Performance Comparison of OLSR Routing Protocols for Manet," *i-Manager's Journal on Wireless Communication Networks,* vol. 1, p. 1, 2012.

[17] T. Sanguankotchakorn, S. K. Wijayasekara, and S. Nobuhiko, "Performance of OLSR MANET Adopting Cross-Layer Approach Under CBR and VBR Traffics Environment," *International Journal of Computer Networks & Communications (IJCNC) Vol,* vol. 10, 2018.

[18] P. Jacquet, P. Muhlethaler, T. Clausen, A. Laouiti, A. Qayyum, and L. Viennot, "Optimized link state routing protocol for ad hoc networks," in *Proceedings. IEEE International Multi Topic Conference, 2001. IEEE INMIC 2001. Technology for the 21st Century.*, 2001, pp. 62-68.

[19] H. Moudni, M. Er-rouidi, H. Faouzi, H. Mouncif, and B. El Hadadi, "Enhancing Security in Optimized Link State Routing Protocol for Mobile Ad Hoc Networks," in *International Symposium on Ubiquitous Networking*, 2017, pp. 107-116.

[20] S. Mohseni, R. Hassan, A. Patel, and R. Razali, "Comparative review study of reactive and proactive routing protocols in MANETs," in *4th IEEE International Conference on Digital Ecosystems and Technologies*, 2010, pp. 304-309.

[21] D. Dasarathan and P. N. Kumar, "Multicasting Based Enhanced Proactive Source Routing in MANETS," *International Journal of Computer Networks & Communications (IJCNC) Vol,* vol. 9.

[22] M. Saseekala and P. Kamalakannan, "Resource Optimized Kernel Support Vector for Scalable and Reliable Multipath Multicast Routing in MANET," *Journal of Theoretical & Applied Information Technology,* vol. 96, 2018.

[23] S. Prakash and A. Swaroop, "A brief survey of blackhole detection and avoidance for ZRP protocol in MANETs," in *2016 International Conference on Computing, Communication and Automation (ICCCA)*, 2016, pp. 651-654.

[24] S. Gurung and S. Chauhan, "A survey of black-hole attack mitigation techniques in MANET: merits, drawbacks, and suitability," *Wireless Networks,* vol. 26, pp. 1981-2011, 2020.

[25] S. Gurung and S. Chauhan, "A dynamic threshold based approach for mitigating black-hole attack in MANET," *Wireless Networks,* vol. 24, pp. 2957-2971, 2018.

[26] C. Panos, C. Ntantogian, S. Malliaros, and C. Xenakis, "Analyzing, quantifying, and detecting the blackhole attack in infrastructure-less networks," *Computer Networks,* vol. 113, pp. 94-110, 2017.

[27] O. Singh, J. Singh, and R. Singh, "MRWDP: Multipoint Relays based Watch Dog Monitoring and Prevention For Blackhole Attack in Mobile Adhoc Networks," *Journal*

of Theoretical & Applied Information Technology, vol. 95, 2017.

[28] S. Ali and P. Nand, "Comparative performance analysis of AODV and DSR routing protocols under wormhole attack in mobile ad hoc network on different node's speeds," in *2016 International Conference on Computing, Communication and Automation (ICCCA)*, 2016, pp. 641-644.

[29] M. S. Abdelhaq, R. A. Alsaqour, M. Al-Hubaishi, T. Alahdal, and M. Uddin, "The Impact of Resource Consumption Attack on Mobile Ad-hoc Network Routing," *IJ Network Security,* vol. 16, pp. 376-381, 2014.

[30] S. Garg, "Performance analysis of AODV and TORA under DDoS attack in MANETs," *IJSR International journal of science and research,* vol. 3, pp. 297-304, 2014.

[31] M. Abdelhaq, R. Alsaqour, M. Alaskar, F. Alotaibi, R. Almutlaq, B. Alghamdi*, et al.*, "The resistance of routing protocols against DDOS attack in MANET," *International Journal of Electrical & Computer Engineering (2088-8708),* vol. 10, 2020.

[32] M. A. Abdelshafy and P. J. King, "AODV and SAODV under attack: Performance comparison," in *International Conference on Ad-Hoc Networks and Wireless*, 2014, pp. 318-331.

[33] M. S. Khan, Q. K. Jadoon, and M. I. Khan, "A comparative performance analysis of MANET routing protocols under security attacks," in *Mobile and Wireless Technology 2015*, ed: Springer, 2015, pp. 137-145.

[34] M. Anupama and B. Sathyanarayana, "An Optimal Key Management Technique for Secure Data Transmission in MANET," *Journal of Theoretical & Applied Information Technology,* vol. 95, 2017.

[35] D. Gao, H. Lin, Y. Liu, and A. Jiang, "Minimizing End-to-End Delay Routing Protocol for Rechargeable Wireless Sensor Networks," *Adhoc & Sensor Wireless Networks,* vol. 34, 2016.

[36] N. Muthukumaran, "Analyzing throughput of MANET with reduced packet loss," *Wireless Personal Communications,* vol. 97, pp. 565-578, 2017.