THE EFFECTIVENESS OF MOBILE AD HOC ROUTING PROTOCOLS UNDER A GRAY HOLE ATTACK

Ahmed Redha Mahlous

Prince Sultan University, Riyadh, KSA
e-mail: armahlous@psu.edu.sa
Kingdom Saudi Arabia

Abstract: Mobile Ad Hoc Networks (MANETs) are an interconnected system of wireless nodes without any central administration, making them more vulnerable to attacks than their wired counterparts. One such attack is the "gray hole" attack, which affects the integrity of the MANET. In this paper we analyse the effectiveness of three MANET protocols: CGSR, TORA, and ZHLS under a gray-hole attack. Using the NS2.35 simulator, we study the impact of gray-hole attacks on the aforementioned protocols in terms of performance metrics such as packet delivery ratio, jitter and throughput. The results showed that ZHLS is more robust under a gray hole attack than its counterparts CGSR and TORA.

Key words: Mobile Communications, Attacks, Simulation, Performance metrics, Routing protocols.

1. INTRODUCTION

Mobile Ad Hoc Networks (MANETs) are an evolving type of wireless network, in which mobile nodes communicate on an extemporal or ad hoc basis. They communicate between each other at peer level without the need for a centralized or fixed infrastructure. These attributes enable MANETs to provide many benefits in virtually any harsh environment where a fixed network infrastructure is impractical or impossible [1].

In this open and hostile environment, MANETs nodes are wide-open to different types of security attacks. One of these attacks is the gray hole attack, in which a malicious attacker's bogus node responds to the request that another node sent to its neighbours in search of a route to a given destination, with a fake reply pretending to have the best route to that destination. Then, it receives all the data packets supposedly to be forwarded to the destination and drops them, hence greatly affecting the performance of the network due to the large number of packets lost. In this paper, we undergo a simulation study to analyse the effectiveness of three MANET routing protocols: CGSR [2], TORA [3], and ZHLS [4] under a gray hole attack.

The rest of the paper is structured as follows. In Section 2 we present related works, and in Section 3 we describe the MANET routing protocols. In Section 4 we discuss attacks

against MANETs and in Section 5 we present the simulation scenarios and results. Section 6 concludes the paper.

2. RELATED WORKS

Many researches studied the mitigation of a black and gray hole attack in MANETs routing protocols [5-11]. In our paper, we examined those that studied the performance of MANET routing protocols under black and gray hole attacks. As it can be seen in Table 1, most of them so far have been dedicated to black hole attacks and only a few of them have looked at gray hole attacks. Even for those that studied gray hole attacks, none of them looked at the performance of CGSR, TORA, and ZHL under this type of attack. The aim of our paper is to fill this gap and provide the research community with a paper that carefully evaluates the performance of these three protocols, each of which comes from a distinct family of MANET routing protocols: "proactive", "reactive", and "hybrid", as defined in the next section.

Table1. Black/Gray hole attacks researches

Reference	***Protocols used for performance comparison***	***Type of attack***	***Combined all three MANETS family routing protocols (Yes/NO)***
[12]	LEACH	Black /Gray	NO
[13]	AODV, DSDV	Black	NO
[14,15]	AODV, OLSR	Black	NO
[16-27]	AODV	Black	NO
[28]	AODV	Gray	NO
[29]	AODV, DOA	Black	NO
[30,31]	AODV	Black/Gray	NO
[32]	AODV, TSDRP	Black	NO
[33]	SAODV	Gray	NO
[34]	AODV, TAODV	Black	NO
[35]	DSR	Black	NO
[36]	OLSR	Gray	NO
[37]	AODV, DSR	Black, Worm	NO
[38,39]	AODV, DSR	Black	NO
[40-41]	AODV, DSDV, ZRP	Black	YES
[42,43]	AODV, DSDV, DSR	Black	NO
[44]	FSR, LAR, ZRP	Black	YES

3. ROUTING PROTOCOLS IN MANET

Routing protocols in MANETs can be categorized into three main types: On-Demand (reactive), Table-driven (proactive), and Hybrid (Fig. 1) [45].

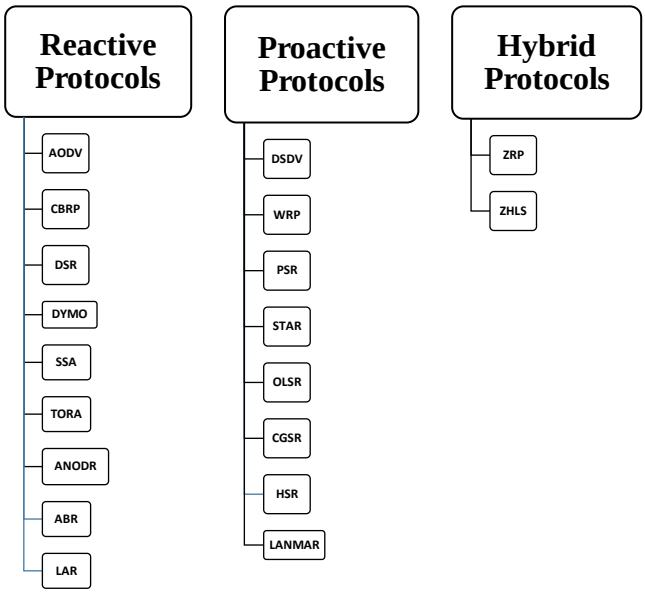

Fig. 1. MANETs Routing Protocols

3.1. Proactive routing protocols (table-driven routing protocol)

In this type of routing protocol, each node in the network tries to keep a table that contains fresh and updated network routes. Any changes in the topology are propagated to all nodes through the exchange of information among nodes. Thus, all nodes have a reliable routing table. If any node wants to forward messages, it just searches for a path to the destination in its routing table. If no such path is found, it sends a request message to all of its neighbours asking for a path to the destination. However, some disadvantages are associated with this type or protocol such as the increase in bandwidth overhead due to the periodic exchange of information, and the fact that many redundant paths to the same destination are stored in the routing table [46].

3.2. Reactive routing protocols (on-demand routing protocol)

In this type of protocol, the routes to destination nodes are established only when required and not known to the sending node. As shown in Fig. 2, this sending node broadcasts a route request message to its neighbours in order to discover a routing path to the destination. Upon receiving the message, any node will compare the destination IP with its own IP address to verify whether it is the concerned destination or not. In the case of it being the destination, the node will reply with a route reply (RREP) packet. If it is not, it will search for a destination in its routing table. If no route is found, it broadcasts the RREQ

packet to its neighbours' nodes. If there is a route in its routing table, the node compares the RREQ packet sequence number with the destination sequence number in the routing table in order to verify whether the route is updated or not. A route is considered as updated if it has a higher sequence number than the one that comes with RREQ packet.

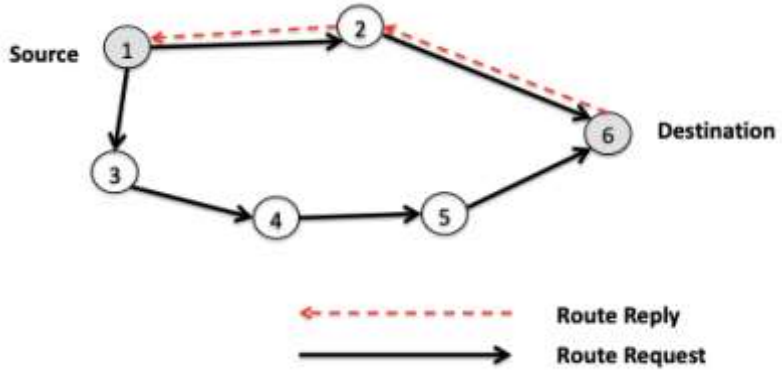

Fig. 2. Route Request and Route Reply

If the intermediate node has a fresh route to the destination, it uses the opposite route to send a unicast RREP packet to the source node. If not, it further sends the RREQ packet to its neighbours. Once the source node receives this RREP packet, it starts sending messages through this route, which is kept in its routing table until it is no longer needed.

3.3. Hybrid routing protocol

Hybrid routing protocols are a combination of proactive and reactive routing protocols. They use the route discovery mechanism of reactive protocols and the table maintenance mechanism of proactive protocols so as to avoid latency and overhead problems in the network. Thus, their design aims to provide better results by utilizing the benefits of both proactive and reactive protocols.

4. ATTACKS IN MANET

4.1. Black Hole Attack

Attacks against MANETs can be categorized into targeting one of the following three layers: Physical, MAC, or Network. At the network layer, the objective of the attack is commonly to not forward the received packets or changes their contents, such as the sequence number and hop count.

A malicious node exploits the route discovery process in the reactive routing protocols. Upon intercepting the RREQ packet, it will immediately reply with a false RREP packet, which holds a modified, higher sequence number, misleading the other nodes by claiming that it has the best route to the destination. The source node ignores all RREPs received from other nodes, and starts sending messages over the malicious nodes, mistakenly thinking that

it has the right path to the destination. Unfortunately, upon receiving packets from the source node, the malicious node will dump and discard them. As mentioned earlier, this type of attack is called a "black hole" attack as it swallows all data packets and severely affects the packet delivery ratio (PDR). This is illustrated in Fig 3 where nodes 1 and 6 represent the source and destination nodes, respectively. Node 3 is the malicious node that replies with a fake RREP to the RREQ initiated by node 1. The latter will wrongly think that node 3 has the best path to the destination (node 6) and will start sending data packets to it. Node 3 will then drop all of the received data packets, effectively creating a hole in the network.

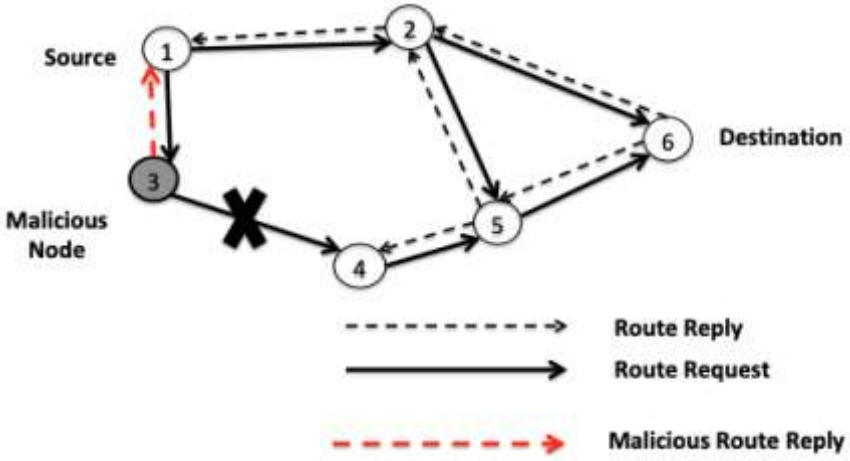

Fig. 3. Single Black Hole Attack

4.2. Gray Hole attack

This type of attack is considered as an extension to the black hole attack [47-49]. In this type of attack, the malicious gray hole node forwards routing and control packets, while selectively dropping data packets after sending false routing information in the reply packet. Through partial forwarding, the malicious node aims to fool the source node into thinking that it is a genuine node. The gray hole node maliciously participates in the route discovery process and updates the source node as having the shortest path to the destination. Then, when it receives packets from the source it drops them on random basis.

5. SIMULATIONS SCENARIOS AND RESULTS

The aim of this paper is to evaluate the performance of three MANETs protocols: CGSR, TORA, and ZHLS under a gray hole attack. For this we use NS2.35 simulator [50] and a modified version of CGSR, TORA, and ZHLS containing a gray hole attack (grayholeCGSR, grayholeTORA and grayholeZHLS). Simulation parameters are set as shown in Table 2. We used a Random Waypoint Model (RWP) as the mobility model of each node. Each node chooses a random destination within the simulation area.

Table 2. Simulation Parameters

Parameter	***Value***
Routing Protocols	*CGSR, TORA, and ZHLS*
MAC layer	*IEEE 802.11*
Simulation area	*1000 * 1000 (m)*
Simulation Time	*300 (s)*
Data packet Size	*512 bytes*
Traffic Sources	*Constant Bit Rate (CBR)*
Number of connection	*20*
Number of gray hole nodes	*1*
Antenna type	*Antenna/Omni Antenna*
Pause Time	*10(m/s)*
Max Speed	*0-20 (m/s)*
Simulator's version	*2-35*

To analyse and evaluate the effectiveness of CGSR, TORA, and ZHLS under a gray hole attack, the following metrics were used: Packet Delivery Ratio, Average End-to-End Delay, and Throughput.

5.1. Simulation Metrics

Packet Delivery Ratio (PDR): The ratio of the received packets and the number of packets originated from the sources. It describes the packet loss rate; the higher the PDR the better the performance.

$$PDR = \frac{\sum Packets\ received\ by\ destination}{\sum Packets\ sent\ by\ sources}\ X\ 100$$

Average End-to-End Delay (Avg.EED): It is the average delay between the sending of the data packet by the CBR source and its receipt at the corresponding CBR receiver.

$$Avg.EED = \frac{1}{N}\sum_{n=1}^{N}(TR_n - TS_n)$$

TR_n= Time at which data packet n was received.
TS_n= Time at which data packet n was sent.
N= Total number of data packets received.

Throughput: The total number of packets delivered to individual destinations over time.

$$\text{Throughput} = \frac{\sum Number\ of\ packets\ received\ by\ destination}{Time}$$

5.2. Simulation Results

In the simulation we undergo two scenarios. First we varied the number of nodes used in the network, second, we varied the node speed.

In the first scenario, the number of nodes in the network was gradually varied from 20 to 40, 60, 80 and finally 100. The following results show the effect of this variation under one malicious node performing a gray hole attack.

In terms of packet delivery ratio, as it can be seen in Fig. 4, ZHLS performs better than TORA and CGSR in terms of the number of packets delivered to the destination under a gray hole attack. This can be justified by it being a hybrid protocol, since ZHLS benefits from the combination of features from both reactive and proactive routing protocols. It uses the reactive routing protocol method in the route discovery process, while using the proactive one during the table maintenance process, consequently circumventing long latency in the network and yielding a higher packet delivery ratio. On the other hand, CGSR induces a lot of overhead due to the increase in the number of nodes because it maintains a route for all of the available nodes in the network, which at certain point, the queue at node level start dropping packets due to the increase of processing time. As the number of nodes increases in the network, TORA exhibits a higher drop in packet delivery,

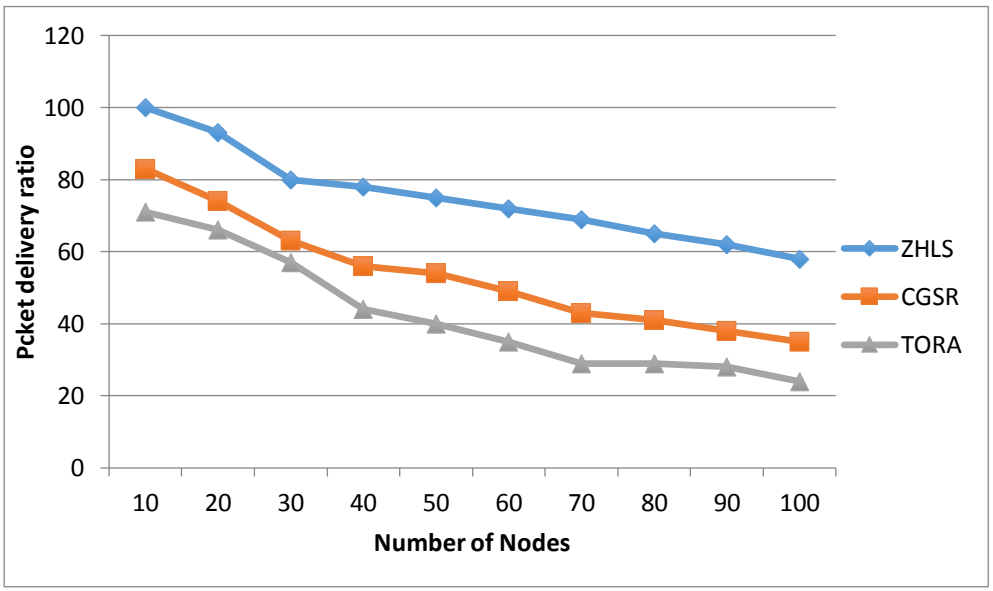

Fig. 4. Packet Delivery Ratio

For the average end-to-end delay, we can see from Fig. 5 that ZHLS has a lower delay than TORA and CGSR. This is due to the same reasons stated above (being a hybrid protocol). CGSR exhibits an increase in the delay when the number of nodes is increased. This escalation is due to the increase in data sessions, leading to the poor results shown. TORA has variable delay with respect to node density but better than that of CGSR due to the caching of routes.

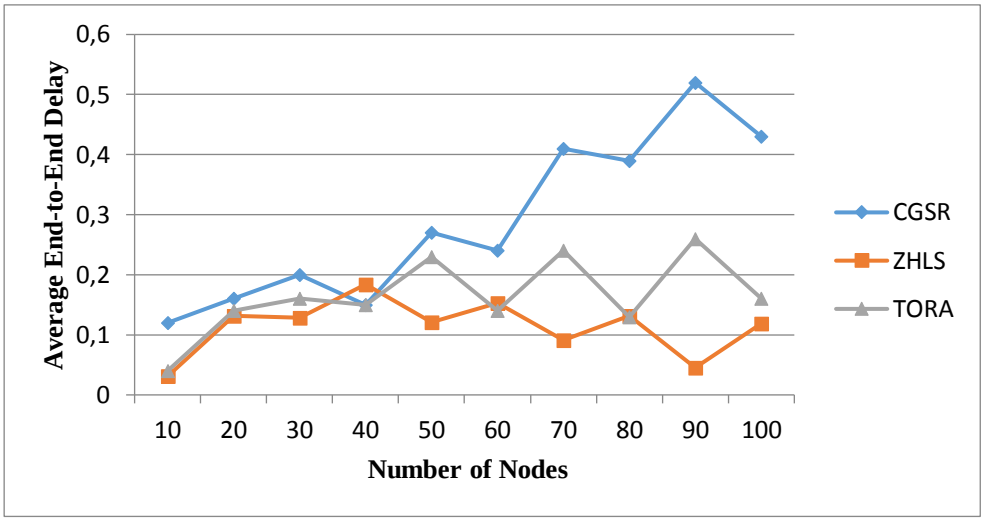

Fig. 5. Average End-to-End Delay

For the throughput, as shown in Fig. 6., ZHLS and CGSR as expected have a better throughput than that of TORA because they have a higher packet delivery ratio. TORA's poor results are due to the loss of packets that are sent before the network has converged.

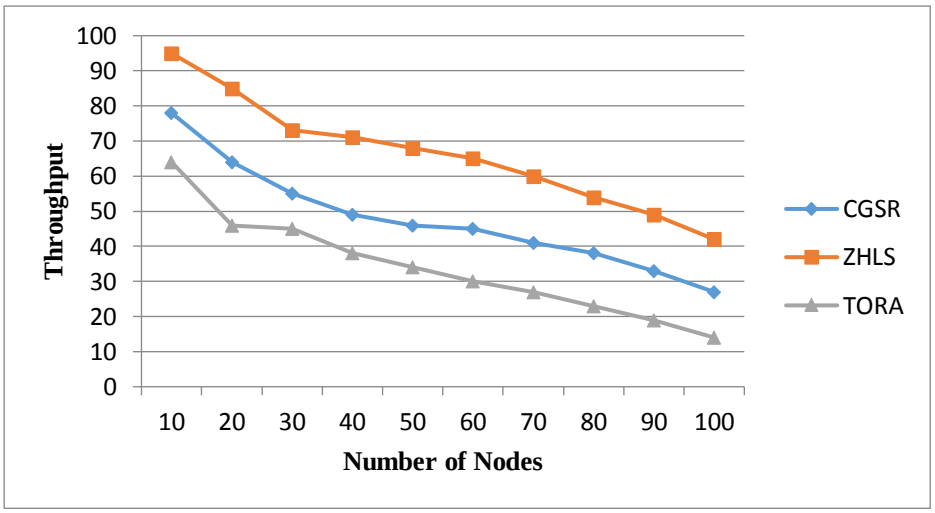

Fig. 6. Throughput

In the second scenario, we analyse the effect of node mobility. The total number of nodes was kept constant at 30 while the mobility of the nodes was varied from 20/ms to 80/ms. As can be seen from Fig. 7 and Fig. 8, when the speed is increased, the packet delivery ratio (Fig. 7) and throughput (Fig. 8) both decrease for the three protocols. This is also due to the effect of the gray hole attack. The frequent updates in source-to-destination paths causes nodes to lose the correct path to any given destination, hence contributing to

packet loss. As for end-to-end delay, Fig. 9 shows that it decreases and this is due to the malicious node responding rapidly to the request originating from the source node, pretending to have a good path to the destination but without actually checking its routing table, hence resulting in faster route discovery times. We also see that ZHLS keeps its lead and performs better than CGSR and TORA in terms of the aforementioned metrics, and this can be justified by the fact that it is a hybrid protocol with the benefits of both proactive and reactive protocols.

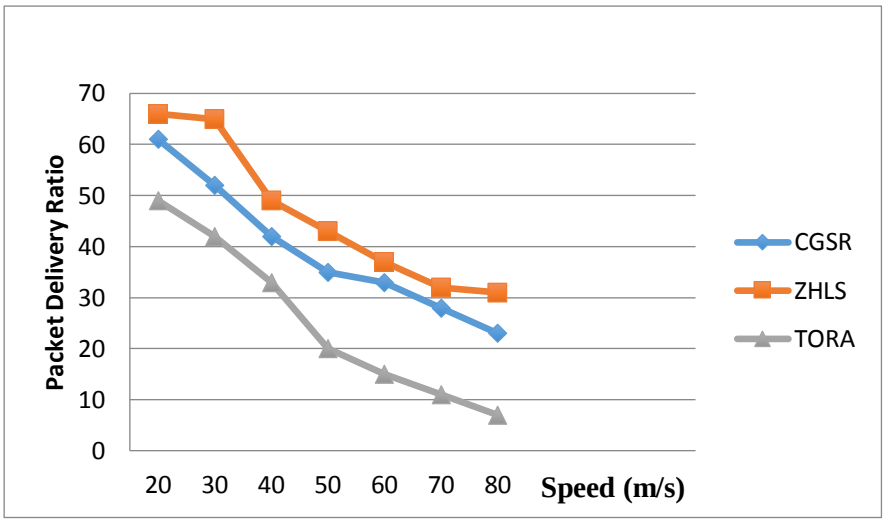

Fig. 7. Packet Delivery Ratio

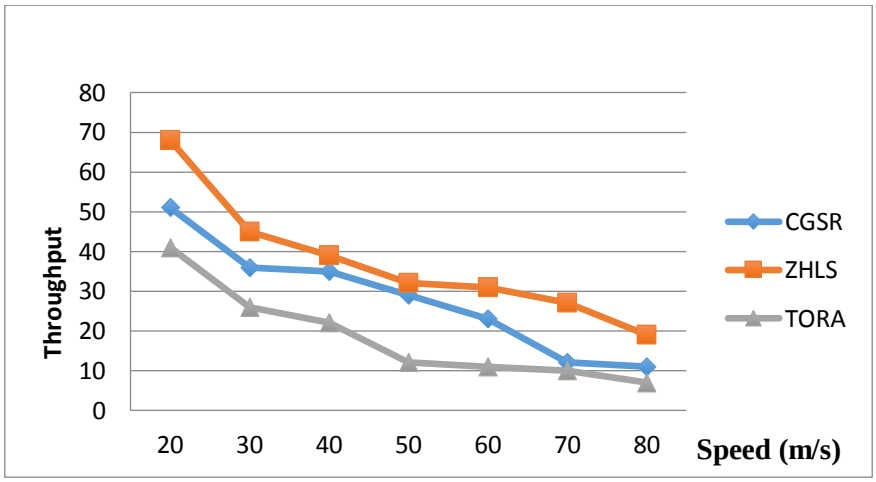

Fig. 8. Throughput

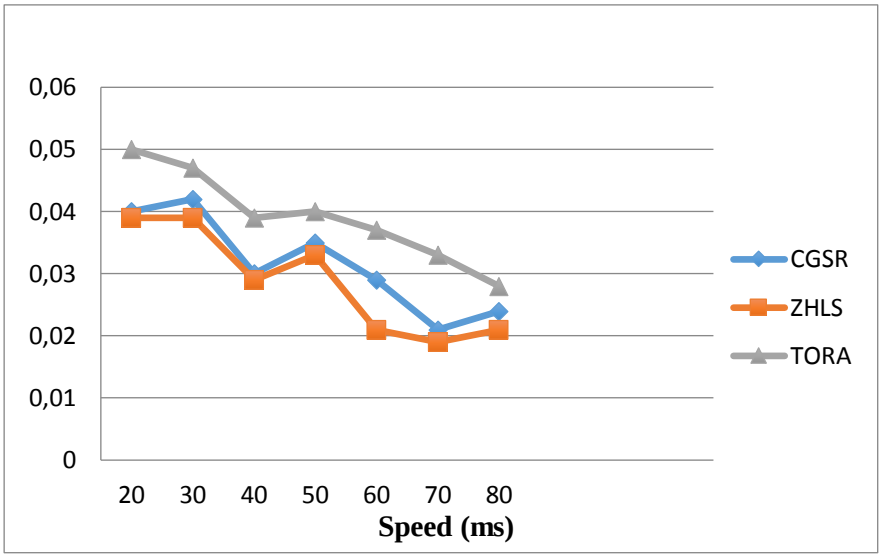

Fig. 9. End-to-End Delay

6. CONCLUSION

In this paper we studied the effectiveness of three MANET protocols: ZHLS, CGSR, and TORA under a gray hole attack. Using simulation, we compared their efficiencies on the basis of some QoS metrics, namely packet delivery ratio, average end-to-end delay, and throughput. We varied the network's size by increasing the number of nodes and we noticed the following results: for a small, medium, and large network size, ZHLS is more robust under a gray hole attack than its counterparts CGSR and TORA. CGSR works fine and provides better results for packet delivery ratio than TORA, but loses its lead in the end-to-end delay measurements. The same remarks can be made about varying the mobility speed. As a conclusion, we can say that for a dense mobile ad hoc network under a single gray hole attack, ZHLS is the preferred routing protocol even under high node mobility. As a future work, we intend to study the performance of these routing protocols with the presence of many malicious nodes and provide a solution to mitigate this type of attack.

REFERENCES

[1] https://www.cisco.com/c/en/us/products/ios-nx-os-software/mobile-ad-hoc-networking/index.html

[2] J. Broch, D.A. Maltz, D. B. Johnson, Y-C. Hu, J. Jetcheva, A performance comparison of Multi-hop wireless ad-hoc networking routing protocols, *in the proceedings of the 4th International Conference on Mobile Computing and Networking (ACM MOBICOM '98)*, October 1998, pp. 85- 97.

[3] Vincent D. Park, M. Scott Corson, A Highly Adaptive Distributed Routing Algorithm for Mobile Wireless Networks, *INFOCOM '97 Proceedings of the INFOCOM '97. Sixteenth Annual*

Joint Conference of the IEEE Computer and Communications Societies. Driving the Information Revolution, April 09-11, 1997, pp. 1405.

[4] C.S.R Murthy and B.S. Manoj, Ad Hoc Wireless Networks and protocol Architectures, *Pub.Pearson Education*, 2005, pp. 342.

[5] Pandi Selvam Raman, A Study of Black Hole Attack and its Recent Prevention Techniques in MANET, *International Journal of Computer Applications (0975 – 8887)*, **8** (Vol. 162), March 2017.

[6] Christeena Joseph, P. C. Kishoreraja, Radhika Baskar and M. Reji, Performance Evaluation of MANETS under Black Hole Attack for Different Network Scenarios, *Indian Journal of Science and Technology*, (Vol. 8), November 2015, 29, DOI: 10.17485/ijst/2015/v8i29/84653, ISSN (Online): 0974-5645.

[7] Mangesh Ghonge , S. U. Nimbhorkar, Simulation of AODV under Blackhole Attack in MANET, *International Journal of Advanced Research in Computer Science and Software Engineering*, **2** (Vol. 2), February 2012, ISSN: 2277 128X.

[8] Ei Ei Khin and Thandar Phyu, Impact of Black Hole Attack on AODV Routing Protocol, *International Journal of Information Technology, Modeling and Computing (IJITMC)*, **2** (Vol. 2), May 2014.

[9] Hicham Zougagh, Ahmed Toumanari, Rachid Latif, Noureddine. Idboufker, Youssef. Elmourabit, A Performance Comparison of Routing Protocols for Ad Hoc Networks, *Int. Journal of Engineering Research and Applications*, **9** (Vol. 4), September 2014, pp.124-131.

[10] Mandeep Kaur Gulati and Krishan Kumar, Performance Comparison of Mobile Ad Hoc Network Routing Protocols, *International Journal of Computer Networks & Communications (IJCNC)*, **2** (Vol.6), March 2014.

[11] Shahabi, S., Ghazvini, M. & Bakhtiarian, M., A modified algorithm to improve security and performance of AODV protocol against black hole attack, *Wireless Network*, 2016, (Vol. 22), 1505-1511, https://doi.org/10.1007/s11276-015-1032-y

[12] Meenakshi Tripathi,M.S.Gaur,V.Laxmi , Comparing the Impact of Black Hole and Gray Hole Attack on LEACH in WSN, *The 8th International Symposium on Intelligent Systems Techniques for Ad Hoc and Wireless Sensor Networks (IST-AWSN), Procedia Computer, Science*, (Vol. 19), 2013, pp. 1101 – 1107,

[13] A. A. Chavan , Prof. D. S. Kurule, Prof. P. U. Dere, Performance Analysis of AODV and DSDV Routing Protocol in MANET and Modifications in AODV against Black Hole Attack, *7th International Conference on Communication, Computing and Virtualization 2016*, Procedia Computer Science (Vol.79), 2016, pp. 835 – 844.

[14] Praveen K S, Gururaj H L, Ramesh B, Comparative Analysis of Black Hole Attack in Ad Hoc Network Using AODV and OLSR Protocols, *International Conference on Computational Modeling and Security (CMS 2016)*, Procedia Computer Science (Vol.85), 2016, pp.325 – 330.

[15] Assia Hammamouche, Mawloud Omar, Nabil Djebari, Abdelkamel Tari , Lightweight reputation-based approach against simple and cooperative black-hole attacks for MANET, *Journal of Information Security and Applications*, (Vol.43), 2018, pp.12–20.

[16] Yaser M. Khamayseh, Shadi A. Aljawarneh, Alaa Ebrahim Asaad, Ensuring survivability against Black Hole Attacks in MANETS for preserving energy efficiency, *Sustainable Computing: Informatics and Systems*, (Vol.18), 2018, pp. 90–100.

[17] Christeena Joseph, P. C. Kishoreraja, Radhika Baskar and M. Reji, Performance Evaluation of MANETS under Black Hole Attack for Different Network Scenarios , *Indian Journal of Science and Technology*, **29** (Vol. 8), DOI: 10.17485/ijst/2015/v8i29/84653, November 2015.

[18] Konagala Pavani, Damodaram Avula, Performance evaluation of mobile adhoc network under black hole attack, *International Conference on Software Engineering and Mobile Application Modelling and Development (ICSEMA 2012), Chennai, India*, Dec. 2012, pp. 19-21.

[19] Performance evaluation of AODV routing protocol under Black Hole attack with varying Black hole nodes, *IEEE Students' Conference on Electrical, Electronics and Computer Science, Bhopal*, 2014, pp. 1-6, doi: 10.1109/SCEECS.2014.6804503.

[20] A. Sardana, T. Bedwal, A. Saini and R. Tayal, Black hole attack's effect mobile ad-hoc networks (MANET), *International Conference on Advances in Computer Engineering and Applications, Ghaziabad*, 2015, pp. 966-970.

[21] K. Madhuri, N. K. Viswanath and P. U. Gayatri, Performance evaluation of AODV under Black hole attack in MANET using NS2, *International Conference on ICT in Business Industry & Government (ICTBIG), Indore*, 2016, pp. 1-3.

[22] V. Trivedi and V. Preethi, Depictive Analysis of MANETs under Black Hole Attack," *International Conference on Current Trends in Computer, Electrical, Electronics and Communication (CTCEEC), Mysore*, 2017, pp. 1116-1120.

[23] Ashok Koujalagi, Considerable Detection of Black Hole Attack and Analyzing its Performance on AODV Routing Protocol in MANET, *American Journal of Computer Science and Information Technology, (Mobile Ad Hoc Network),* 2:25 (Vol.6) 2018,

[24] Jamal, T. & Butt, S.A. Malicious node analysis in MANETS, *Int. j. inf. Technol*, 2018. https://doi.org/10.1007/s41870-018-0168-2

[25] Christeena Joseph, P. C. Kishoreraja, Radhika Baskar and M. Reji, Performance Evaluation of MANETS under Black Hole Attack for Different Network Scenarios, *Indian Journal of Science and Technology*, **29** (Vol 8), November 2015.

[26] Mangesh Ghonge, Prof. S. U. Nimbhorkar, Simulation of AODV under Blackhole Attack in MANET, *International Journal of Advanced Research in Computer Science and Software Engineering*, **2** (Vol. 2), February 2012 ISSN: 2277 128X

[27] Shree Om and Mohammad Talib , Wireless Ad-hoc Network under Black-hole Attack, *International Journal of Digital Information and Wireless Communications (IJDIWC)*, **1** (Vol. 3): 591-596

[28] Akshaya, Karthik Pai B H, Performance Analysis and Mitigation of Gray Hole Attack against AODV under Collaborative Environment using MANETs, *International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization)*, **5** (Vol. 4), May 2016.

[29] P. R. Jasmine Jeni, A. Vimala Juliet , R.Parthasarath, A.Messiah Bose , Performance Analysis of DOA and AODV Routing Protocols with Black Hole Attack in MANET, *International Conference on Smart Structures & Systems (JCSSS-2013)*, March 28 - 29, 2013, Chennai, INDIA

[30] Kriti Chadha, Dr. Sushma Jain , Impact of Black Hole and Gray Hole Attack in AODV Protocol, IEEE, *International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2014)*, May 09-11, 2014, Jaipur, India

[31] S. V. Vasantha and A. Damodaram, Bulwark AODV against Black hole and Gray hole attacks in MANET, *IEEE International Conference on Computational Intelligence and Computing Research (ICCIC)*, Madurai, 2015, pp. 1-5.

[32] Nirbhay Chaubey, Akshai Aggarwal, Savita Gandhi, Keyurbhai A Jani, Performance Analysis of TSDRP and AODV Routing Protocol under Black Hole Attacks in MANETs by Varying Network Size, *Fifth International Conference on Advanced Computing & Communication Technologies*, 2015.

[33] A. Lupia and F. De Rango, Energy consumption evaluation of SAODV with trust management scheme under gray-hole attacks, 2015 *Wireless Telecommunications Symposium (WTS)*, New York, NY, 2015, pp. 1-8. doi: 10.1109/WTS.2015.7117288

[34] A. Jain and A. Shrotriya, Investigating the effects of black hole attack in MANET under shadowing model with different traffic conditions, *International Conference on Computer, Communication and Control (IC4), Indore*, 2015, pp. 1-6.

[35] L. Mejaele and E. O. Ochola, Analysing the impact of black hole attack on DSR-based MANET: The hidden network destructor, *Second International Conference on Information Security and Cyber Forensics (InfoSec), Cape Town*, 2015, pp. 140-144.

[36] N. Schweitzer, A. Stulman, R. D. Margalit and A. Shabtai, Contradiction Based Gray-Hole Attack Minimization for Ad-Hoc Networks, *in IEEE Transactions on Mobile Computing*, **8** (Vol. 16), pp. 2174-2183, 1 Aug. 2017.

[37] L. Prashar and R. K. Kapur, Performance analysis of routing protocols under different types of attacks in MANETs, *5th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Noida*, 2016, pp. 405-408.

[38] L. Mejaele and E. Oketch Ochola, Effect of varying node mobility in the analysis of black hole attack on MANET reactive routing protocols, *Information Security for South Africa (ISSA), Johannesburg*, 2016, pp. 62-68.

[39] E. O. Ochola, L. F. Mejaele, M. M. Eloff and J. A. van der Poll, Manet Reactive Routing Protocols Node Mobility Variation Effect in Analysing the Impact of Black Hole Attack, *in SAIEE Africa Research Journal*, **2** (Vol. 108), June 2017, pp. 80-92.

[40] Neeraj Arora, Dr. N.C. Barwar, Performance Analysis of DSDV, AODV and ZRP under Blackhole attack, *International Journal of Engineering Research & Technology (IJERT)*, **4** (Vol. 3), April 2014.

[41] S Muzamil Basha, SR Raj Kumar, G N. Vivekananda, Raghu Veer Matam, Improved Performance Analysis of DSDV, AODV, ZRP Under Black Hole Attack in MANETs, *IJECT*, **4** (Vol. 4), OCT- DEC 2013.

[42] Rozy Rana, Kanwal Preet Singh, Performance Evaluation of Routing Protocols (AODV, DSDV and DSR) with Black Hole Attack, *International Journal of Science and Research (IJSR)*, 2014.

[43] Mandeep Kaur Gulati and Krishan Kumar, Performance Comparison Of Mobile Ad Hoc Network Routing Protocols, *International Journal of Computer Networks & Communications (IJCNC)*, **2** (Vol. 6), March 2014.

[44] Ria Ranjan, Ashish Xavier Das, A.K. Jaiswal, Ashish Allen Roberts, Performance Evaluation of FSR, LAR1 and ZRP Routing Protocols in MANET based on RWP Mobility Model, *International Journal of Computer Applications (0975 – 8887)*, **3** (Vol. 71), May 2013.

[45] Sachin Lalar and Arun Kumar Yadav, Comparative Study of Routing protocols in MANET, *Oriental Journal of Computer Science & Technology*, March 2017, 1 (Vol. 10), pp. 174-179.

[46] Lineo Mejaele, Elisha Oketch Ochola, Effect of Varying Node Mobility in the Analysis of Black Hole Attack on MANET Reactive Routing Protocols, *Information Security for South Africa (ISSA)*, August, 2016.

[47] Hao Yang, Haiyun Luo, Fan Ye, songwu Lu and Lixia Zhang, Security in mobile ad hoc networks: Challenges and solutions, *IEEE Wireless Communications*, (Vol. 11), pp. 38-47.

[48] Hoang Lan Nguyen, Uyen Trang Nguyen, A study of different types of attacks on multicast in mobile ad hoc networks, *Journal of Ad hoc Networks*, (Vol. 6), pp. 32-46.

[49] Hongmei Deng, Wei Li, and Dharma P. Agrawal, Routing Security in Wireless Ad Hoc Networks, *IEEE Communications Magazine*, pp. 70-75.

[50] K. Fall and K. Vardhan, The Network Simulator (ns-2) Available: http://www.isi.edu/nsnam/ns

Information about the author:

Dr. Ahmed Redha Mahlous received his MSc in Computer systems and Internetworking from South Bank University (London, UK) and a PhD degree in Computer Networks from University of Bradford (UK). His area of research includes Network Security, Software Security and QoS. He is currently working as an assistant professor at Prince Sultan University (Riyadh, KSA).

Manuscript received on 20 December 2018