Journal of Theoretical and Applied Information Technology
15th May 2021. Vol.99. No 9

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

A COMPARATIVE STUDY FOR THE WORM WHOLE ATTACK EFFECT ON MANET

[1*]MAHA ABDELHAQ, [2]RAED ALSAQOUR, [1]FAY ALSUBAIE, [1]GHADA ALESSA, [1]LUJAIN ALGHAMDI, [1]HANA ALTUKHAIM, [1]LAMA ALSHAMMARI, [1]ALAA ALSALEEM

[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 Ad hoc network (MANET) is a wireless network that has the ability to reconfigure itself without any centralized infrastructure. This type of network is not in a fixed composition and form, but instead, it forms itself and allows for other nodes to join in automatically. Since it has a flexible and dynamic nature, that makes it vulnerable to attacks which could be attached to the network very easily. As a result, the attacker would later serve as a sender or receiver for faked packets. One of the most dangerous attacks of this network is wormhole attack. With wormhole attack, packets of data are transferred from one node to another harmful node inside or outside the network. Therefore, we aim in this paper to study the effect of a wormhole attack on two routing protocols, namely Ad hoc On-Demand Distance Vector (AODV) and Dynamic Source Routing (DSR). The comparison will be held in terms of two main network performance metrics: throughput and end-to-end delay. Network Simulator-2 (NS-2) will be used to conduct the simulation experiments in this paper and calculate the results. This research gives a new contribution to the area of network attacks. It provides a new Worm Hole Attack Model (WHAM), which will be applied to MANET routing using NS-2 WHAM has been applied to the protocols mentioned above to test their resistance and stability under the attack.

Keywords: *Mobile ad hoc network; Routing Protocols; AODV; DSR; Wormhole Attack*

1. INTRODUCTION

Mobile Ad hoc Network (MANET) is built to create a network anywhere and wherever there is no fixed infrastructure, in order to enable the mobility of the user on the network. In other words, MANET is a group of mobile nodes that communicate and interact in a distributed manner with each other through wireless connections. in order to provide the necessary network functionality. There is no centralized structure, so the node itself does the routing. MANET can be used in areas such as military fields, sensor networks, disaster rescue operations, and conferences. Regardless of geographical location, this type of network provides the information as well as services due to their self-reconfiguration nature.

In MANET, there are three types of protocols which are, reactive, proactive, and hybrid routing protocols. This research aims to study two types of routing protocols, namely Ad hoc On-Demand Distance Vector (AODV) and Dynamic Source Routing (DSR), under the impact of wormhole attack. As far as we know, no researcher has presented such a study until now. This research gives a new contribution to the area of network security. It provides a new Wormhole Attack Model (WHAM), which has been applied in MANET routing using network simulator-2 (NS-2). WHAM has been applied to the protocols mentioned above to test their resistance and stability under the attack.

The body of the article has the following structure: Section 2 includes our background and related work. Section 3 presents the wormhole attack. In section 4, we explain AODV and DSR vulnerability to wormhole attack. In section 5, we explain the simulation environment and settings. Section 6 presents the results and discussion. Finally, the conclusions and possible guidelines for further work are presented in Section 7.

2. BACKGROUND AND RELATED WORK

2.1 Mobile Ad-Hoc Network

MANET is designed to be used in a specific field, made up of a group of nodes connected wirelessly. It is an infrastructure-less network which has an ability to configure itself without any human intervention. Any node in the network is concurrently a router as well as a host. Nodes can be transferred easily as network topology differs randomly [1, 2].

The development of communications and the expansion of network areas has led to an increase in MANET network applications such as military fields, wildlife monitoring, medical applications, earthquakes and disaster areas applications [2, 3].

2.2 Ad Hoc On-Demand Distance Vector

This paperwork uses AODV routing protocol. AODV is a dynamic routing protocol. It has been extensively studied and developed for many years, demonstrating its robustness and advantages.

The key advantages of the AODV protocol are that, relative to other MANET routing protocols, the delay in communication configuration with the destination is smaller. Secondly, in contrast with other ad hoc routing protocols, AODV avoids congested routes. Third, the fast ad hoc topological reconfigurations that can influence the other protocols of routing can be managed [1, 4].

In the route discovery loop of the AODV routing protocol in MANET, the source broadcasts RREQ to the neighbors, as seen in Figure 1. Regarding RREQ, we know that it contains the IP addresses of the recipient, the broadcast ID, and the sequence number of the destination. Every intermediate node receives the RREQ packet does two separate processes: first, It checks whether the RREQ packet has already been sent by the same address as originator of the RREQ, based on this checking it then either discards or accepts the RREQ packet. Flooding attacks can be avoided by providing this degree of verification. Second, the intermediate node tests the destination sequence number contained in its routing table if the RREQ packet is approved. It uni-casts the RREP packet to the source node if it is greater than or equal to the one contained in the RREQ packet. If no intermediate node has a sufficiently new (fresh destination sequence number) path to the destination node, the RREQ packet can retain its navigation until it reaches the destination node itself, unlocking the RREP packet to the source node, as seen in Figure 1 [5].

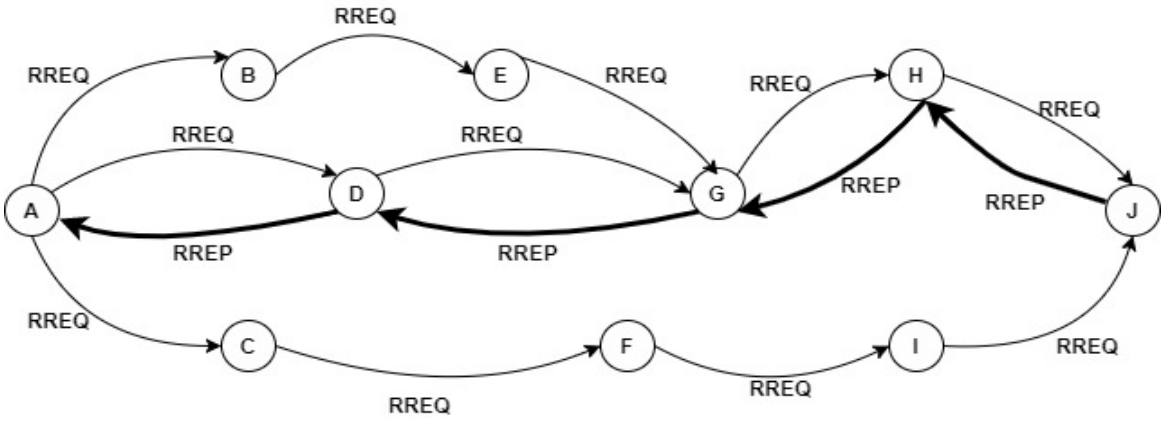

Figure 1: AODV

2.3 Dynamic Source Routing

DSR is a routing protocol that comes within the category of reactive routing protocols. It can detect or track the way from the source to the destination only when needed. A procedure called the Rout Discovery Method is used by DSR to detect the route from the source node to the destination node. [6].

The route discovery and route maintenance steps involve three types of messages:

1. RREQ packet: it is broadcasted from source node to destination node that contains packet ID, destination address, and own address.
2. RREP packet: When the destination receives from the source node a RREQ packet. It generates a new packet of RREP and forwards it to the source.
3. RERR packet: during the packet delivery, the RERR check to see if the path of the node has changed, then the node will not be able to send

the packet, so it will send the RERR packet to the source of the packet [7].

The DSR Protocol transmits the path to its neighbors but does not flood it. It just tracks the path by measuring the cumulative distance between the source node and the destination node or calculating the number of nodes present. [8].

As shown Figure 2 for example, we have a network containing 7 nodes, the source node is the node number (N1), and the destination node is the node number (N7)

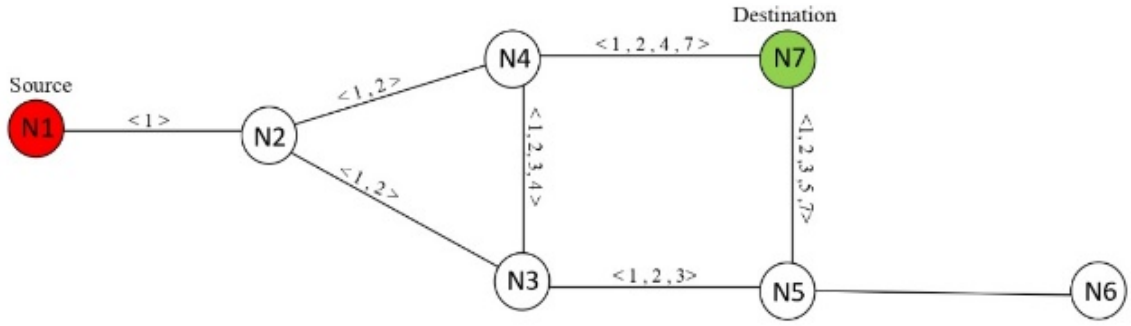

Figure 2: The Route Discovery and Route Maintenance

Step 1: You will be starting from the node number N1 and broadcast the information about it to its neighbors. In this case the route info is <1> because it has a link (one-to-one) between node number N1 and number N2.

Step 2: Broadcast previous route information to neighbors of node N2 to nodes number N3 and N4. And the new route will remain same <1,2> in all the cases.

Step 3: In node number N3 the previous route <1,2> is broadcasted to next neighboring nodes. New route till node N5 will be <1,2,3>and same process can be done for other nodes.

Step 4: Broadcast the new routes <1,2,3,5>, <1,2,4> to nodes N6 and N7, respectively.

Step 5: all the previous steps are repeated until the source node reaches the destination node via all routes. Three possible routes are generated:

- Route 1: <1,2,3,4,7>
- Route 2: <1,2,3,6,7>
- Route 3: <1,2,4,7>

DSR choose the shortest route which is route 3 as shown in Figure 3.

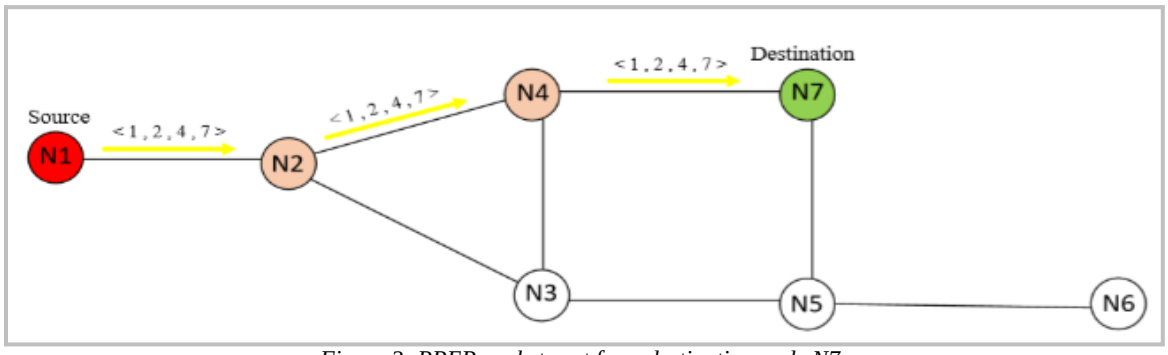

Figure 3: RREP packet sent from destination node N7

2.4 Related work

In [9], the authors conducted a study of both AODV and DSR protocol and the experiment was applied to wormhole attacks. The results of the study showed that Protocol DSR has a significant advantage over Protocol AODV, due to the fact that Protocol DSR provides an alternative path when delivering data.

In [10], The authors concentrated on the effect of the black hole, flooding attacks and rushing attacks against AODV. They provided a number of

similarities with the initial AODV in package delivery pace, the average end-to-end latency and the average network throughput on the efficiency of AODV under attacks. They concluded that a black hole attack had the most impact on the network and its performance.

In [11], the authors set a clear view of the performance of each of the protocols AODV, DSR, DSDV, RAODV, AOMDV, and TORA protocols, after a comparison between them, and the results showed that TORA under normal conditions has worked better than TORA under DDoS attack. Similarly, in other hand the AODV performed way better under normal conditions.

In [12], detailed study about the cooperative black hole attack is done. When black holes attack in a group they decrease the throughput value and increase the delay. This paper focuses on one such attack known as "Black hole attack" and AODV is the routing protocol used here in MANET.

In [13], the authors study and analyze the performance of AODV in MANET. The selfish node is introduced in the network to analyses the selfish node attack. Network parameters are evaluated and compared using simulation tool. The selfish node does not send the packets of other nodes and decreases the performance of the network, and the author compares between Packet Delivery Ratio and End-to-End delay with and without the existence of the selfish node in the network.

Based on the summarized related work, as shown in Table 1, we introduced a comparative study of the three chosen routing protocols, which are: DSR and AODV under the impact of RCA. To the best of our knowledge, no researcher has introduced a new model for RCA on AODV and DSR to study their resistance against the attack.

Table 1: Related works comparison; PDR: Packet Delivery Ratio, E2E delay: End to End delay

Authors	Research topic	Year	Simulator	Performance metrics
Our work	Study the effect of wormhole attack in AODV and DSR routing protocols	2021	NS-2	Throughput, E2E delay
[13]	Study of impact of selfishness node on AODV	2017	GloMoSim	PDR, E2E delay
[9]	Study the performance analysis of AODV and DSR routing protocols under wormhole attack	2016	QualNet 5.0.2	Throughput, E2E delay
[10]	Study the Performance analysis of AODV routing protocol under blackhole, flooding attacks and rushing attacks	2016	NS-2	Throughput, E2E delay
[12]	Collaborative blackhole attack resolution simulation-based analysis using a cross-checking algorithm.	2015	NS-2	Throughput, E2E delay
[11]	Study the performance analysis of AODV and TORA under DDoS.	2014	NS-2	Throughput, E2E delay, PDR, Network load

3. WORMHOLE ATTACK

This attack is the destruction of a single path in MANET and is one of the most common security problems in this type of network. It is also considered a type of tunnel attack where a specific malicious node receives a specific package and then transfers it to other places in the network and then returns it to the network, which is shown in the figure below, Figure 4.

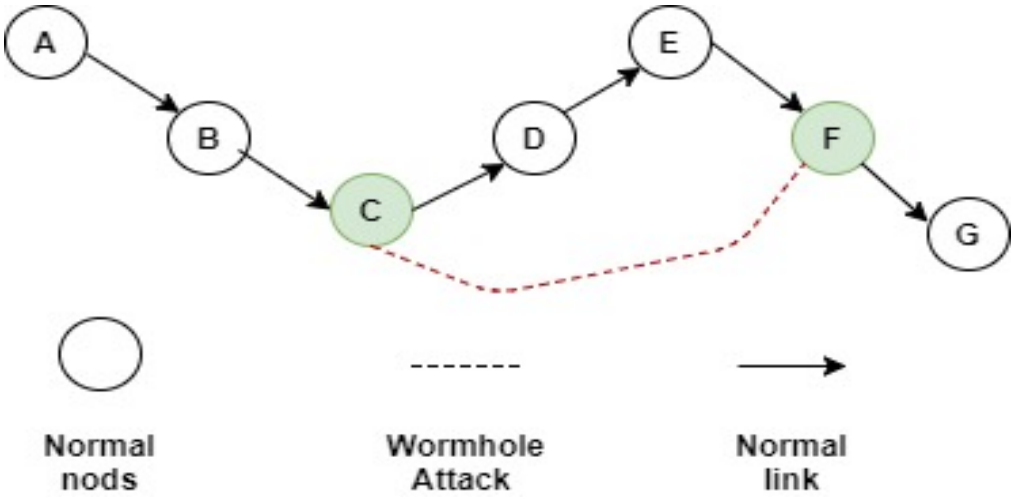

Figure 4: Wormhole Attack

Wormhole attacks cause a significant decline in network operation and performance and threaten entire network security.

The concept of the attack will be clear through the following example. Initially, we will assume that we have two networks one named A and the other is B, we consider that one of these two networks will start as a malicious node, and each of these nodes is linked through a connected link between them, so node X in A and node Y in B are two neighbours if they make a private direct connection between each other, see Figure 5. This type of attack is considered one of the most sophisticated types of attacks in MANET, if the attackers are connected to the normal link and not to the wormhole in this case the attacker has a flexible environment so that he can direct the wrong direction.

- The wormhole link is referred to as the tunnel that is formed between the attackers.
- The tunnel is either a wire connection or links in which the frequency is very high [21].

The working principles of the wormhole attack are seen in Figure 5 below, and the same line is used for sending and receiving packets during transmission between X and Y.

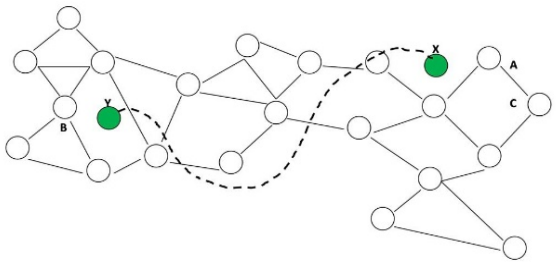

Figure 5: Wormhole Attack

4. AODV AND DSR VULNERABILITY TO WORMHOLE ATTACK

In a wormhole Attack, the attacker finds a strong strategic location in the network using the shortest path between nodes. Attacker advertises the path that found to let the rest of nodes knows about the shortest path to broadcast the data. Once the nodes created a direct link from each other, the attacker will receive the packets from one specific location in the network and encapsulate these packets using the tunnel to receive by another location in the same network, and then the packet will be forwarded from that location. This is the way to attack routing protocols of networks. This type of attack is very dangerous, even when the network provides confidentiality and security.

AODV and DSR are very vulnerable to wormhole attack. The attacker may send RREQ packets directly to the destination node by using wormhole through the network. If the neighbours of the destination node received the request, they will forward it and discard all other RREQ packets from the normal node. For routes that have more than one hop, the attacker can easily make a packet sent bypass through the wormhole link and arrive fast which is shown in Figure 6(a). The attacker can also send the packet bit by bit to decrease the delay time, which is shown in Figure 6(b) [21].

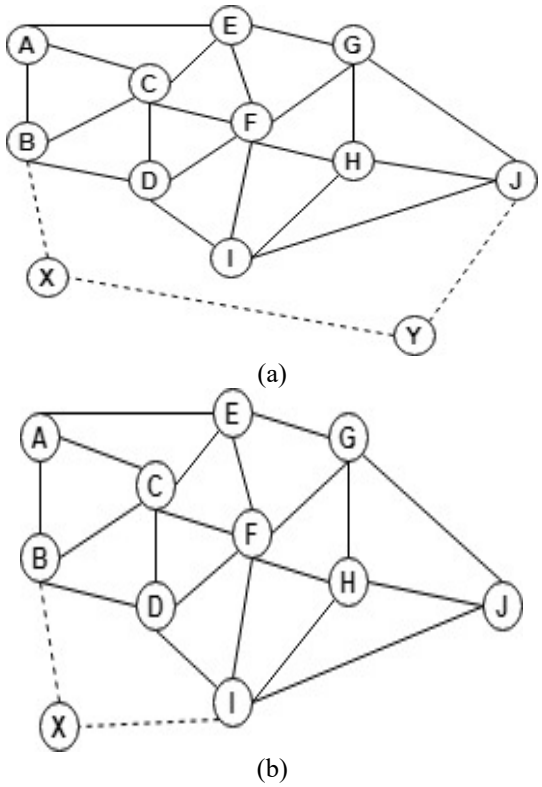

Figure 6: Wormhole Attack in AODV and DSR

5. SIMULATION ENVIRONMENT AND SETTINGS

In Figure 7, The proposed wormhole attack model (WHAM) architecture is applied on the two chosen routing protocols namely, AODV and DSR. When IP protocol requests a route, the routing protocol starts to discover paths in this instance, WHAM starts wormhole attack on MANET.

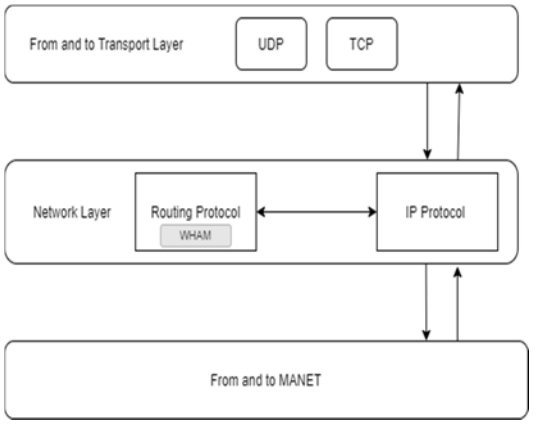

Figure 7: WHAM Architecture

6.1 Simulation WHAM system components

OTcl is an extension to Tcl/Tk for object-oriented programming. NS-2 uses OTcL for the simulation programmer to build up the network objects in the memory. NS-2 uses the last style, where the configuration file is an OTcl file called "OTcl simulation Script". As shown in Figure 8, below, this script contains a Performance Parameters, which contain Number of Attackers and Radio Range. For Network simulation the work will be on the two routing protocols which are AODV and DSR. In NS-2 simulation result stored in Trace file, which gives Network Animator (NAM) is an animation tool based on Tcl/TK for showing traces of network emulation and traces of real-world packets. AWK Scripts for NS-2 to process data from Trace Files. Moreover, the performance metrics that are considered in our work are Throughput and End-to-end delay. Finally, the output is displayed as graphs using Microsoft Excel 2013.

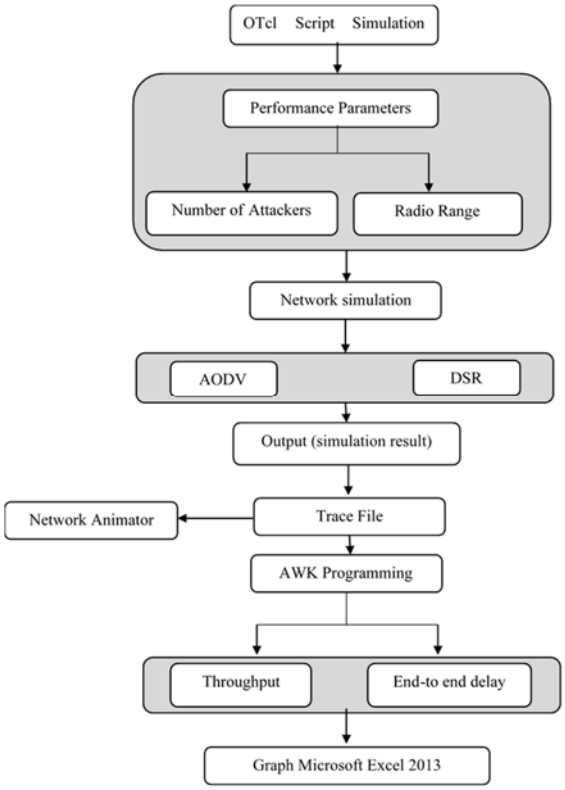

Figure 8: Simulation System Components

6.2 Simulation parameters

To determine the effect of wormhole attack, the research scenario was designed using NS-2 and

obtaining the simulation results experiments. The experiments were carried out by varying one aspect, the number of attackers (2, 4, 6 and 8), positioning the attackers near the target, which helps to understand the impact of wormhole attack. The CBR communication begins with a traffic load of 2 packets/s from 1.0s to the end of the simulation. The packet size is 1000 bytes and the attacker starts the simulation at 30s until the end. The mobility model and radio propagation model used are, random waypoint and two-ray ground reflection models, respectively.

1. Random Waypoint Model (RWP)

RWP is a paradigm of mobility widely used in mobile wireless network efficiency analysis [22]. This elementary model works by describing the movement pattern of independent nodes. The mobile nodes move in random free way without restrictions. To put it another way, the direction, destination and speed are all chosen randomly and independently of other nodes. The (RWP) can produce many mobility scenarios in NS-2 utilizing tools such as setdest (Mobility generation tool).

2. Two-Ray Ground Reflection Model

It is a radio propagation model that anticipates the path losses as they are in LOS between a transmitting antenna and a receiving antenna (line of sight). The two antennas each have different heights and are implemented in NS-2. The obtained signal consists of two elements, the LOS component and the multipath component generated primarily by a single wave mirrored on the field. The line-of-sight direction (LoS) between the receiver and the transmitter. If the influence of reflections from the earth's surface needs to be used in the modelling, the expression for the obtained power becomes complex [23]. The Table 2 below illustrates the node options that we used in our experiment.

Table 2: Simulation settings

Parameter	Value
Network area	1000m × 1000m
Number of nodes	20
Nodes speed	0 – 7 m/s
Bandwidth	11 mbps
Traffic Packet size	512 bytes
Packet rate	2 packets per second
Traffic type	CBR

6.3 Performance metrics

In this paper, each resultant value is collected from the average of 5 runs for the experiment in NS-2. For each routing protocol two-performance metrics has been observed which are: end-to-end delay and throughput.

End-to-end delay: The time that a data packet takes to reach the destination. This involves any potential delays incurred during path discovery latency by buffering. The average of duration for the destination is recorded in each experiment. 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 amount of successfully transmitted data packets across the network, i is the specific packet ID, Ri is the time to receive a unique ID packet i and Si is the time it takes to deliver a unique ID packet i.

Throughput: it is the total number of delivered packets for the total duration of the simulation. It represents the average of the throughput values for destinations in each experimental result.

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

6.4 Experimental Cases

Case-I studies the effects of varying the number of attackers on throughput, end-to-end delay, and energy consumption on all studied protocols in MANET as shown in Figure 9, where the source node (1) and the attackers are located near-destination node (17).

Case-II studies the effects of varying the radio range on throughput, end-to-end delay, and energy consumption on all studied protocols in MANET as shown in Figure 10, where the source node (1) and the attackers are located near-destination node (17) and we select constant number of attackers which is 4 attackers.

Journal of Theoretical and Applied Information Technology
15th May 2021. Vol.99. No 9

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

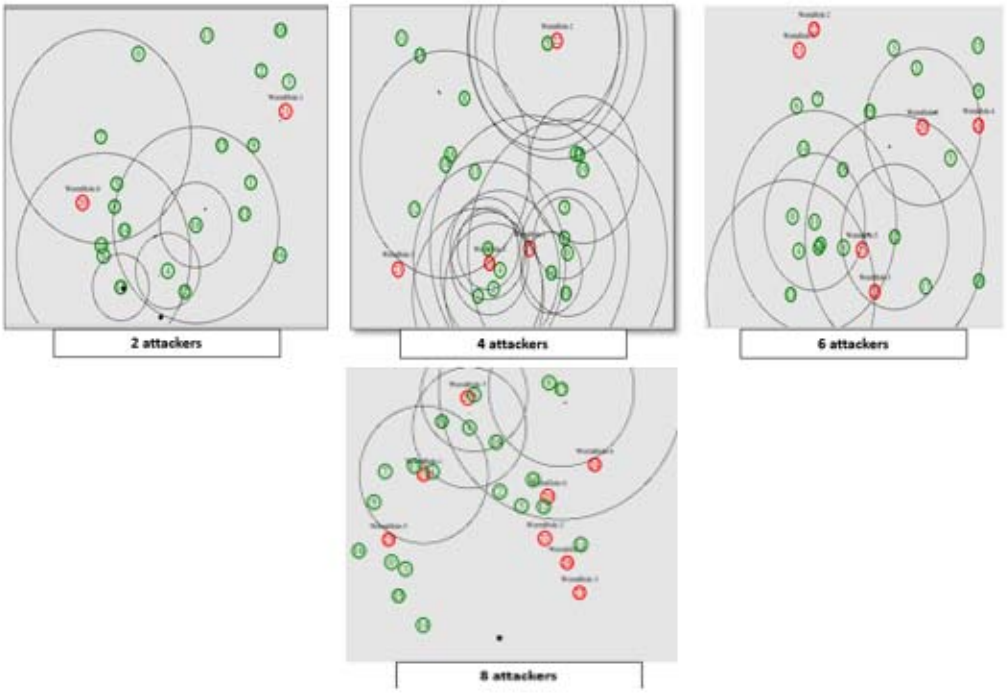

Figure 9: Case I; varying the number of attacks.

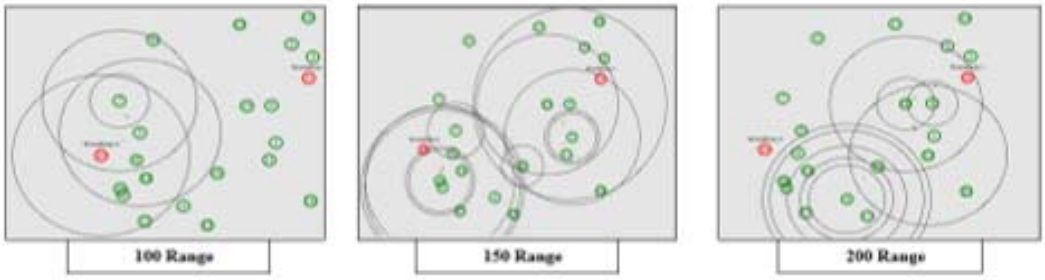

Figure 10: Case I; varying the radio ranges.

6. RESULTS AND DISCUSSION

The result of calculating the Average Throughput for AODV and DSR when we change the number of worm attack nodes, we have seen that the AODV have higher average throughput values when compared with the DSR protocol. While, the DSR has lower average throughput values. Figure 11 below show the comparison between AODV and DSR. AODV protocol has the line with red color and DSR has the line with blue color.

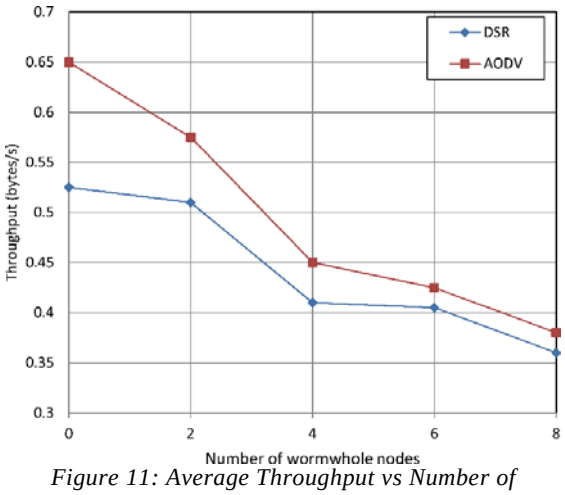

Figure 11: Average Throughput vs Number of Wormhole Nodes

The result of calculating the End-to-End Delay for AODV and DSR when we change the number of worm attack nodes, we have seen that the AODV have lower end-to-end delay values when compared with the DSR protocol. Also, the DSR has higher delay. The figure 12 below show the comparison between AODV & DSR. The AODV protocol has the line with red colour and DSR has the line with blue colour.

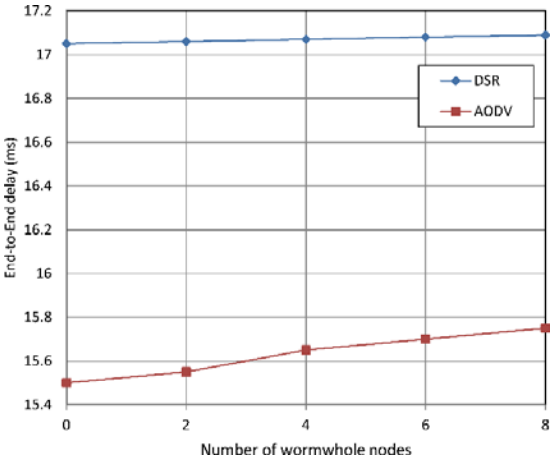

Figure 12: End-To-End Delay vs Number of Wormhole Nodes

The results of experiments show that AODV is better than DSR. AODV has higher performance than DSR, which has high result of throughput and less end-to-end delay from DSR. DSR shows that it collapses to wormhole attacks. The results show that the increasing the radio range on all protocols increase the throughput and increase the end-to-end delay values. The experimental results in figure 13, prove that when the higher radio range the higher throughput. When the radio range increase it enable the network to increase the throughput. The following figure 13 show the throughput when using different radio rang. In which the colored red belongs to AODV and blue belong to DSR.

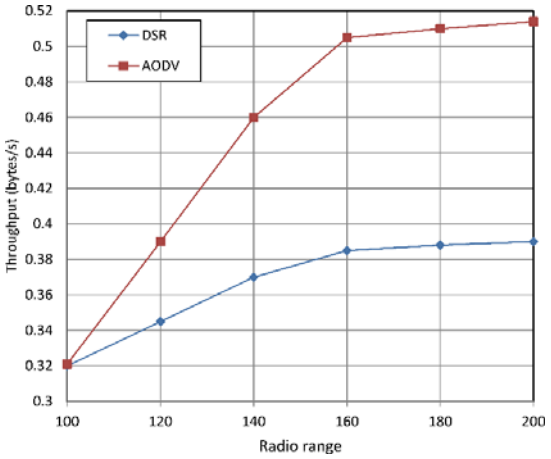

Figure 13: Average Throughput vs Different Radio Range

For the end-to-end delay we found that the AODV have shortest end-to-end delay when compared with the DSR, and DSR have higher end-to-end delay when the range increases. The following figure 14 show the effect of end-to-end delay when the radio range changed and AODV protocol with the red colour and the DSR with blue colour.

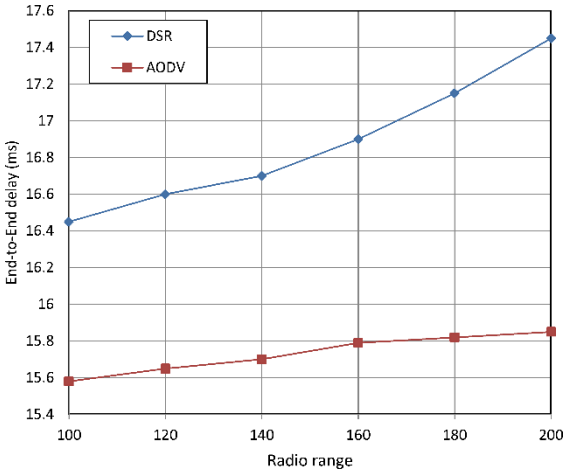

Figure 14: End-To-End Delay vs Different Radio Range

7. CONCLUSIONS AND FUTURE WORK

This paper examined two routing protocols in MANET and introduced a worm hole attack model (WHAM) that creates wormhole nodes in CBR traffic, which was implemented in AODV and DSR routing protocols using NS2. Two network performance metrics were used to compare the two protocols under attack: throughput and end-to-end delay. The results and

their analysis have been presented. As shown in the previous graphs, AODV performed better in terms of throughput and end-to-end delay and shew the most resistant behaviour compared to DSR.

In this study, we did not evaluate the performance of our model using jitter, routing overhead and packet lose ratio network performance metrics. In the future, we will evaluate the performance of these protocols using these performance metrics and we are looking for doing real implementation.

ACKNOWLEDGEMENT

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] A.-S. K. Pathan, *Security of self-organizing networks: MANET, WSN, WMN, VANET*: CRC press, NW, USA, 2016.

[2] S. Mishra, P. Varshney, S. Choudhary, and R. Purohit, "Performance Evolution of Conventional and Swarm based Routing Methods in Mobile Ad-Hoc Networks," in *2019 2nd International Conference on Power Energy, Environment and Intelligent Control (PEEIC)*, 2019, pp. 528-531.

[3] R. Singh, "An Overview of MANET: Characteristics, Applications Attacks and Security Parameters as well as Security Mechanism," *International Research Journal of Engineering and Technology (IRJET),* vol. 5, pp. 1155-1159, 2018.

[4] K. Rajani, P. Aishwarya, and S. Meenakshi, "A review on multicasting routing protocols for mobile ad-hoc wireless networks," in *2016 International Conference on Communication and Signal Processing (ICCSP)*, 2016, pp. 1045-1052.

[5] R. Sadakale, A. Bhosale, and N. Ramesh, "Performance Analysis of Traffic Types in AODV Routing Protocol for VANETs," in *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, 2019, pp. 1-5.

[6] D. Johnson, Y.-c. Hu, and D. Maltz, "The dynamic source routing protocol (DSR) for mobile ad hoc networks for IPv4," RFC 47282007.

[7] N. Jain, A. Rahman, and A. K. Dubey, "Code Aware Dynamic Source Routing for Distributed Sensor Network," in *2013 International Conference on Communication Systems and Network Technologies*, 2013, pp. 272-276.

[8] I.-R. R. P.1546, "Method for point-to-area predictions for terrestrial services in the frequency range 30 MHz to 3 000 MHz," International Telecommunication Union Radiocommunication Sector (ITU-R) P.1546-4, 2009.

[9] 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.

[10] H. Moudni, M. Er-rouidi, H. Mouncif, and B. El Hadadi, "Performance analysis of AODV routing protocol in MANET under the influence of routing attacks," in *2016 International Conference on Electrical and Information Technologies (ICEIT)*, 2016, pp. 536-542.

[11] 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.

[12] G. Gupta and A. Mishra, "Simulation Based Study of Cooperative Black Hole Attack Resolution using Cross-Checking Algorithm," *International Journal on AdHoc Networking Systems (IJANS),* vol. 5, pp. 17-28.

[13] S. Ruj and R. Sachdeva, "Analysis of Selfish Node Attack in AODV Routing Protocol using GLOMOSIM," *International Journal of Engineering Development and Research,* vol. 5, pp. 784-789, 2017.

[14] Y. Bai, Y. Mai, and N. Wang, "Performance comparison and evaluation of the proactive and reactive routing protocols for MANETs," in *2017 Wireless Telecommunications Symposium (WTS)*, Chicago, IL, 2017, pp. 1-5.

[15] T. Issariyakul and E. Hossain, "Introduction to network simulator 2 (NS2)," in *Introduction to network simulator NS2*, 1st ed: Springer, Boston, MA, 2009, pp. 1-18.

[16] R. Singh and T. P. Sharma, "Present Status of Distributed Denial of service (DDoS) attacks in internet world," *International Journal of Mathematical, Engineering and Management Sciences,* vol. 4, pp. 1008-1017, 2019.

[17] P. Oberoi, S. Mittal, and R. K. Gujral, "ADRCN: A framework to detect and mitigate malicious insider attacks in cloud-based

environment on IaaS," *International Journal of Mathematical, Engineering and Management Sciences,* vol. 4, pp. 654-670, 2019.

[18] A. A. Ajibesin, M. M. Kah, A. T. Ishaq, and C. A. Ajibesin, "Performance Analysis of Topology and Destination Based Routing Protocols in Mobile Ad-Hoc Network Using NS2," in *2019 IEEE 13th International Conference on Application of Information and Communication Technologies (AICT)*, 2019, pp. 1-6.

[19] A. Alsumayt, J. Haggerty, and A. Lotfi, "Evaluation of detection method to mitigate DoS attacks in MANETs," in *2018 1st International Conference on Computer Applications & Information Security (ICCAIS)*, 2018, pp. 1-5.

[20] A. Sahoo, A. Shreya, C. S. Dash, I. Priyadarshini, S. Sobhanayak, S. S. Panda, *et al.*, "Performance Evaluation of AODV, DSDV and DSR Routing Protocol For Wireless Adhoc Network," in *2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN)*, 2018, pp. 348-351.

[21] S. Qazi, R. Raad, Y. Mu, and W. Susilo, "Securing DSR against wormhole attacks in multirate ad hoc networks," *Journal of Network and Computer Applications,* vol. 36, pp. 582-592, 2013.

[22] E. Hyytiä and J. Virtamo, "Random waypoint model in n-dimensional space," *Operations Research Letters,* vol. 33, pp. 567-571, 2005.

[23] A. M. Kanthe, D. Simunic, and R. Prasad, "Effects of propagation models on AODV in mobile ad-hoc networks," *Wireless personal communications,* vol. 79, pp. 389-403, 2014.