PERFORMANCE ANALYSIS OF ROUTING PROTOCOLS IN MANET UNDER MALICIOUS ATTACKS

Dr. Gorine[1] and Rabia Saleh

[1]School of Business and Technology, Gloucestershire University, Cheltenham, England

ABSTRACT

MANETs routing protocols are vulnerable to various types of security attacks such as selfish nodes, grey-hole and black-hole attacks. These routing protocols are unprotected and subsequently result in various kinds of malicious mobile nodes being injected into the networks. In this paper, three types of attacks such as selfish, grey-hole and black-hole attacks have been applied to two important MANET routing protocols; Ad-hoc On demand Distance Vector (OADV) and Dynamic Source Routing (DSR) in order to analyse and compare the impact of these attacks on the network performance based on throughput, average delay, packet loss and consumption of energy.

KEYWORDS

Mobile Ad-Hoc Networks, DSR, AODV, Routing Protocols, Wireless Network Security, Malicious Node, Network Performance

1. INTRODUCTION

Mobile ad-hoc networks are composed of a number of wireless mobile devices called nodes as shown in figure 1. These networks have no fixed infrastructure and no central administration. MANETs are characterised by resource constraints, dynamic topology, and openness to wireless media. However, wireless networks have a number of vulnerabilities, which may be exploited by hackers to gain access to the network to steal or tamper with data [4, 11].

In this paper, the performance of two MANET's routing protocols; Ad-hoc On demand Distance Vector (AODV) and Dynamic Source Routing (DSR) have been analysed under malicious attacks [10].

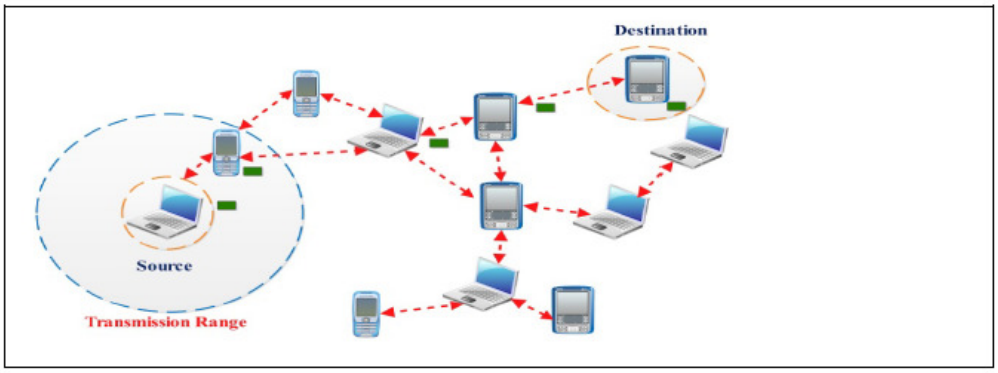

Figure 1. MANET architecture

DOI: 10.5121/ijnsa.2019.11201

2. RELATED WORK

Mobile Ad Hoc Networks routing protocols have been the subject of intense research in the past 20 years. Many researchers have been studying the performance of a single protocol under several attacks, but attempts are carried out on performance analysis of routing protocols under malicious attacks.

In [15], the authors evaluated the performance of AODV routing under black-hole, grey-hole, selfish and flooding attacks. Their finding is that black-hole and flooding attacks have a severe impact on the AODV performance compared to selfish and grey-hole attacks.

In 2016, the authors [16], also focused on the impact of the black hole, flooding and rushing attacks against AODV. They compared the performance of AODV under attacks with the original AODV in terms of Packet Delivery Ratio, Average End to End Delay and Average Throughput. They concluded that the performance of AODV degrades under the attacks. Their finding is that black hole attack has a higher significant effect on the network performance than flooding and rushing attacks.

In [17], the authors conducted a comparative study between AODV and DSR routing protocols, but under wormhole attacks only. Their simulation results show that DSR performs better than AODV under wormhole attacks in MANET. They concluded that the high performance of DSR is due to the alternative data delivery path provided by DSR.

However, in our research paper, a comparative study between AODV and DSR routing protocols subject to several attacks including back-hole, grey-hole and selfish node attacks.

3. SECURITY GOALS

The majority of previous security studies define five major security goals which are required for attacks' prevention [7].

Like all wireless networks, MANETs need is to achieve the security goals, such as confidentiality, authentication, integrity, availability, and data freshness.

3.1. DATA CONFIDENTIALITY

Routing and packet forwarding information must remain confidential. To keep the confidentiality, it is required to ensure to disclose data packets to authorized nodes only. Data encryption is a common method of ensuring confidentiality

3.2. DATA AUTHENTICATION

Authentication ensures that data packets or communications between nodes are accessible by only authorised nodes. Without authentication, a malicious node can masquerade as a trusted node in MANET and can have a negative impact on data transmission between nodes.

3.3. DATA INTEGRITY

Integrity ensures that data must not be changed in transit, and steps must be taken to ensure that data cannot be altered by unauthorized nodes.

For example, a malicious node may add some packets or modify data within a packet before forwarding the corrupt data to its neighbour.

3.4. DATA AVAILABILITY

Availability ensures that services provided by nodes should be available to their users even under attacks, such as energy starvation, denial of service and a misbehaving node.

3.5. DATA FRESHNESS

Even if confidentiality and data integrity have been achieved it is imperative to ensure that no old data have been replayed. This requirement of fresh data is important when dealing with shared-keys which need to be changed over time.

4. ROUTING PROTOCOLS IN MANET

Protocols are defined as the set of rules which are used by network devices to communicate between them. Due to mobility nature of nodes of MANET and the dynamic network topology, an effective routing protocol is needed to manage the communication between the nodes within the network.

Routing protocols in MANET's routing protocols are divided into two groups; proactive and reactive routing protocols [1].

In this paper, the performance of two MANET's routing protocols; Ad-hoc on demand Distance Vector (OADV) and Dynamic Source Routing (DSR) have been analysed under normal operation

4.1. AD-HOC ON DEMAND DISTANCE VECTOR ROUTING (AODV)

Ad hoc On-Demand Distance Vector (AODV) is a routing protocol for mobile ad hoc networks (MANETs) and other wireless ad hoc networks with a large number of mobile nodes [14]. The protocol's algorithm creates a route between two nodes only when the route is requested by the source node. This route will remain active as long as the source node has data packets to send to the destination node. However the route will be dropped as soon as the source stops sending data packets.

AODV uses optimisation; this will reduce the overhead in the network. Optimisation in AODV, being the "time-to-live" field will limit propagation in route requests when they are sent. The time-to-live field can fluctuate if there is no route reply.

4.2. DYNAMIC SOURCE ROUTING (DSR)

DSR is a fully reactive routing protocol [17]. It is a source routing protocol meaning that a packet carried in the network contains an ordered list of all nodes through which the packet must be routed.

The DSR protocol is composed of two mechanisms that work together to allow the discovery and maintenance of source routes in the ad hoc network as shown in figure 2:

- Route Discovery is the mechanism by which a node S wishing to send a packet to a destination node D obtains a source route to D. Route Discovery is used only when S attempts to send a packet to D and does not already know a route to D.

- Route Maintenance is the mechanism by which node S is able to detect, while using a source route to D, if the network topology has changed such that it can no longer use its route to D because a link along the route no longer works. When Route Maintenance indicates a source route is broken, S can attempt to use any other route it happens to know to D, or can invoke Route Discovery again to find a new route. Route Maintenance is used only when S is actually sending packets to D.

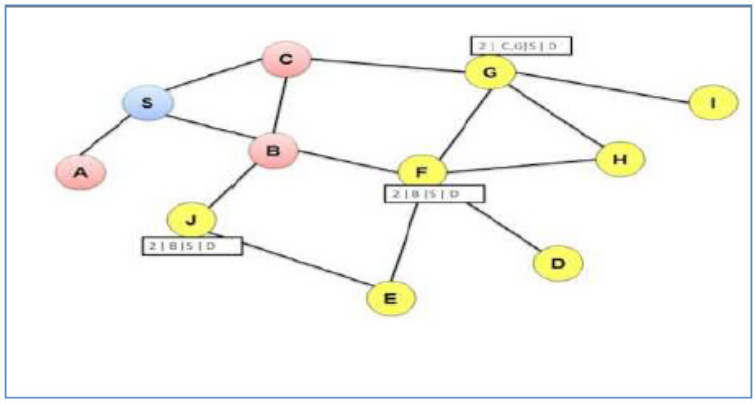

Figure 2. DSR protocol diagram

5. SECURITY THREATS IN MANET

Due to the lack of infrastructure and the dynamic nature of MANET, they are more likely to be open to attacks [2], which may disturb the relationship of trust between nodes. These MANETs' characteristics allow attackers to readily target the network and jeopardise its resources by jamming and disturbing the communication between trusted nodes.

In mobile ad-hoc networks, attacks can be classified as active and passive attacks [3]. In passive attacks, attackers only listen to the traffic for information without disturbing the normal routing process, which compromises confidentiality such as snooping, eavesdropping, traffic analysis and monitoring. Whereas active attacks destroy, steal or modify useful information as well as damaging network operations, such as wormhole, black hole, grey hole, information disclosure, routing attacks and selfish attacks.

In this paper, three types of attacks have been investigated; these are grey-hole attacks, black-hole attacks and selfish node attacks.

5.1. SELFISH NODES ATTACKS

A selfish node is a type of routing protocol attack at the Data link layer, in which a malicious node deviates from the original routing and forwarding of packets.

Due to the limitation of resources wireless networks, selfish nodes seek to conserve their own resources by refusing to forward packets to other nodes [5]. There are two types of selfish nodes:

• The first type shares the routing table but drops packets instead of forwarding them to their destinations.
• The second type do not share their routing tables, with their neighbours. For example, in DSR routing protocol, a selfish node may decide to drop all RREQ packets received or not forwarding a route reply RREP packet to its destination.

5.2. BLACK HOLE ATTACKS

Black-hole attacks happen at the Network layer [6], in which a malicious node declares to other nodes that it has the shortest route to their destination node. The malicious node will drop all data packets or implement man-in-the-middle attack. For example in figure 3, the malicious node number (3) sends fake routing information by advertising that it has the shortest path to the destination node (4). When the node (1) wants to send a packet data to the node (4), it will initiate route discovery. The malicious node (3) intercepts the RREQ packet and sends a reply RREP to the sender node (1). If the reply from the malicious node (3) reaches the source first, then the sender node (1) disregards all other RREP messages and start sending packets through node (3). Therefore, all packets are lost or consumed at the malicious node.

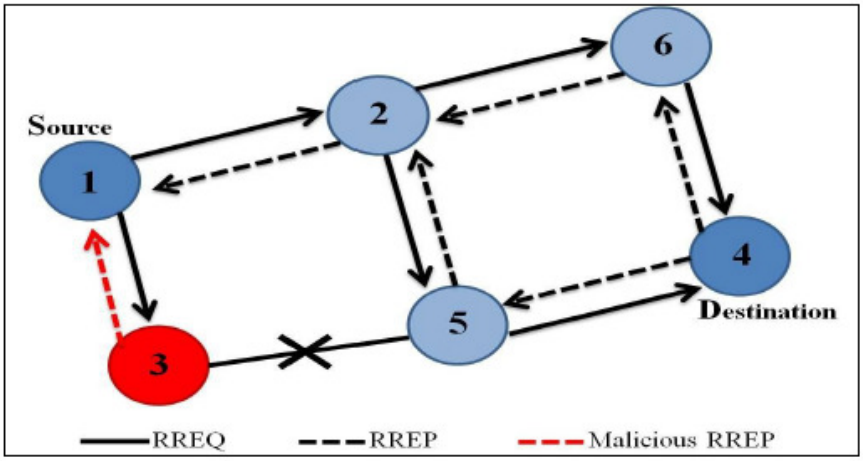

Figure 3. Black hole attack

5.3. GREY HOLE ATTACKS

The grey-hole attack takes place at the network layer and can be used as a slow poison in the network side [12].

A grey-hole attack happens when a malicious node advertises itself as having a valid route to the destination node with the intention of intercepting data packet. However instead of forwarding the data packet, the malicious node (i.e. the grey-hole) may exhibit its malicious behaviour in one of three ways:

- Drops packets sent by specific nodes while forwarding packets sent by the other nodes.
- The malicious node drops all packets received within a specific period of time and forward packets later.
- The grey-hole drops the intercepted packets randomly and forward other packets.
- The grey-hole attack is more difficult to detect than the black hole attack in which the malicious node drops all the packets received.

6. METHODOLOGY

Three types of research methods are used for evaluating the performance of wireless networks: physical measurement, analytical methods and network simulation.

In this research paper, a network simulator called ns2 is selected as it is currently the best-known network simulation package for research into wireless networks [8,13]. ns-2 is written in C++, which uses MIT's Object Tool Command Language (OTcl) as the command and configuration interface.

The simulator is invoked via the ns interpreter and the OTcl scripts defined the simulation rules. ns-2 provides substantial support for the simulation of TCP/ UDP, routing, multicast protocols over both wired and wireless, local and satellite network.

Currently ns-2 development is supported by the Defence Advanced Research Projects Agency (DARPA).

7. IMPLEMENTATION

In this research paper, NS2 (v2.34) is used as the network simulator [9] and was run under Ubuntu v14.04 operating system.

The network consists of 50 wireless nodes spread randomly in a terrain area of 700m x 1000m with simulated waypoint mobility model time of 100, 300, 500, 700 and 900 seconds. The simulation used the random, which has become a "benchmark" model for evaluating the routing protocols of MANET.

The aim of the simulation is to evaluate the network performance by measuring the following parameters: throughput, average delay, packet loss and energy per byte.

These parameters are defined as follow:

- Throughput: The total number of packets successfully received by the destination node.
- Packet Loss: The number of packets dropped during the simulation.
- Average delay: The average time taken by data packets to travel between the source and destination nodes.
- Energy per byte: The amount of energy consumed by nodes to transmit and receive the number of data packets.

In this experiment, the performance of two protocols namely; Dynamic Source Routing (DSR) and Ad-Hoc on Demand Distance Vector (AODV) are evaluated in two separate scenarios. The first one when the network is operating under normal conditions (i.e. without attacks or malicious nodes) and the second scenario, the network is operating under attacks (i.e. with some malicious nodes). The simulation is repeated ten times split equally between AODV and DSR protocols with different time scale (100, 300, 500, 700 and 900).

8. RESULTS OF SIMULATION OF MANET UNDER ATTACKS

In this part of the experiment, the network is simulated under attack by several malicious nodes including black-hole attack, selfish node attack and grey-hole attack under both AODV and DSR protocols.

The selfish nodes are implemented to drop just route request and route reply, because if a node is not involved in route discovery, it will not be used in forwarding data packets. However, black hole nodes are implemented to drop data packets, forward routing requests and reply packets, because the attack affect routing operation. By contrast, the grey-hole attack is similar to the

black hole attack with inconsistent behaviour, as it will drop selective data packets and forward others.

8.1. SELFISH NODES ATTACKS

❖ **THROUGHPUT OF THE PROTOCOLS UNDER SELFISH NODES:**

In Figure 4 the graph shows the throughput in the protocols with selfish nodes, in which their percentages vary from 10% to 50%. It is clear that AODV is much better than DSR to deliver packets successfully in this kind of attack.

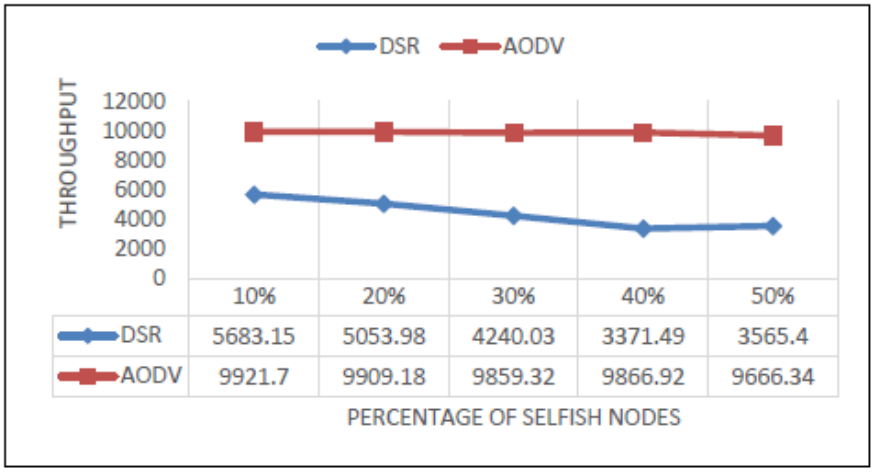

Figure 4. Throughput of the protocols with selfish nodes

❖ **AVERAGE DELAY OF THE PROTOCOLS UNDER SELFISH NODES**

As can be seen from Figure 5, average delay of DSR is higher than AODV. Because DSR is an On-Demand source routing protocol, this can be considered as the major reason for DSR delay. A route is discovered only when needed and also, the mechanism for route discovery happens each time as well as, several paths to the destination is discovered. Consequently, DSR has higher delay. On the other hand, AODV has just one path for each destination in its routing table, which is updated permanently based on a sequence number. Thus, that leads to a slight end to end delay. Also, AODV was not impacted very much with increase in the percentage of selfish nodes, unlike DSR, which was impacted when selfish nodes increased.

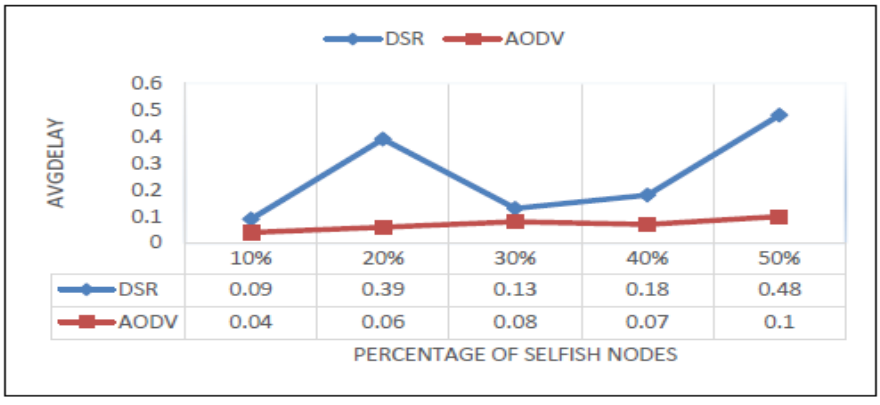

Figure 5. Average delay of the protocols with selfish nodes

❖ PACKET LOSS OF THE PROTOCOLS UNDER SELFISH NODES:

From line graph in Figure 6, it is obvious that DSR was affected excessively by the selfish nodes, despite DSR being better in normal protocols. While AODV as a standard protocol does not have better performance than DSR, in the case of selfish nodes it is better in performance than DSR.

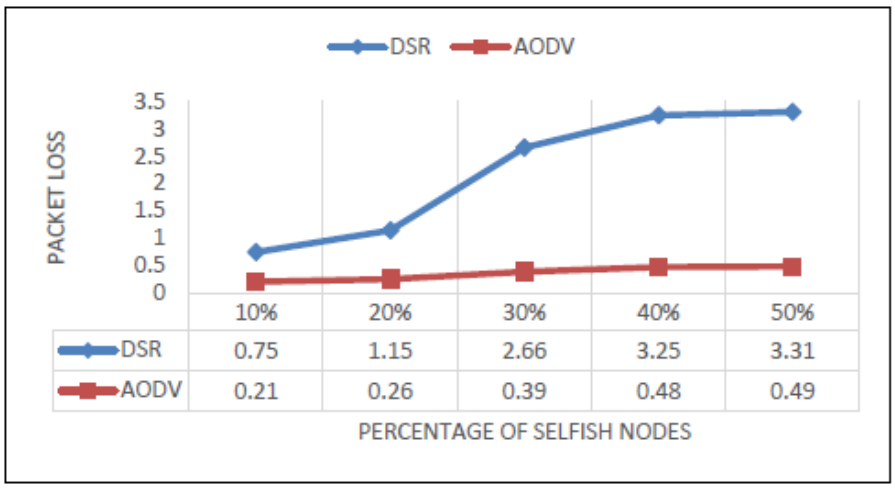

Figure 6. Packet loss of the protocols with selfish nodes

❖ ENERGY PER BYTE OF THE PROTOCOLS WITH SELFISH NODES

Figure 7 illustrates the energy per byte which is consumed during participation in routing activities under different percentages of selfish nodes. It is clear that AODV was nearly the same even when the percentage of selfish nodes reached 40%, while DSR was affected by the attack and consequently, it consumed high amounts of energy when the attacks increased. Thus, AOD outperforms DSR in terms of consuming energy.

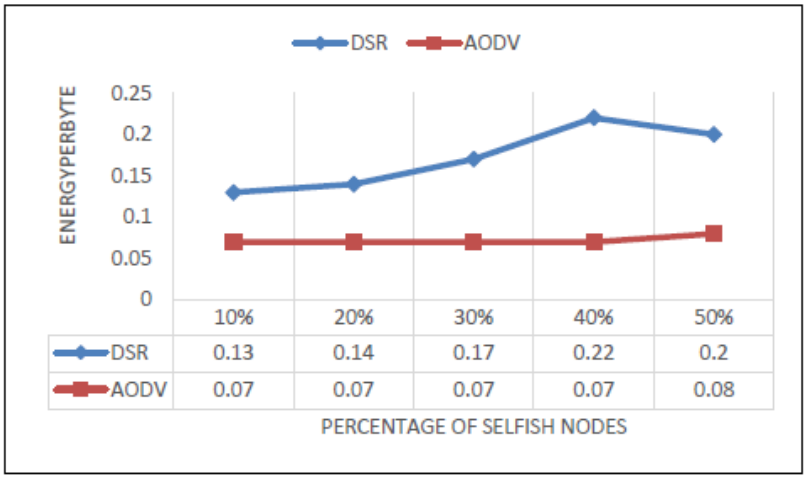

Figure 7. Energy per byte of the protocols with selfish nodes

8.2 BLACK HOLE ATTACKS RESULTS

❖ THROUGHPUT OF THE PROTOCOLS UNDER BLACK HOLE ATTACK:

Figure 8 illustrates throughput of both protocols under different percentages of black hole nodes, and it is clear that both protocols are affected by increasing the percentage of the black hole attack. However, it is obvious that DSR outperforms AODV when the percentage of attack nodes has increased. This performance can be justified because of the different nature of DSR and AODV networks and their different techniques to achieve routing activities, such as the packet salvage of the DSR protocol in NS2.

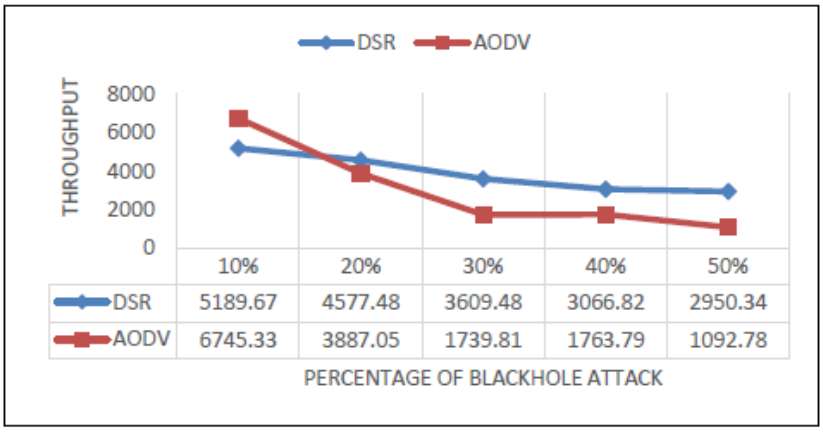

Figure 8. Throughput of the protocols with black hole attack

❖ AVERAGE DELAY OF THE PROTOCOLS UNDER BLACK HOLE ATTACK:

In Figure 9, the line graph shows the average delay of both protocols under black hole nodes. Both protocols have approximately the same nature in terms of performance when assessing the average delay metric as the average delay fluctuated over the time of the simulation. However, AODV suffered less delay than DSR in all the percentages of attacks, for the reasons discussed in the previous section.

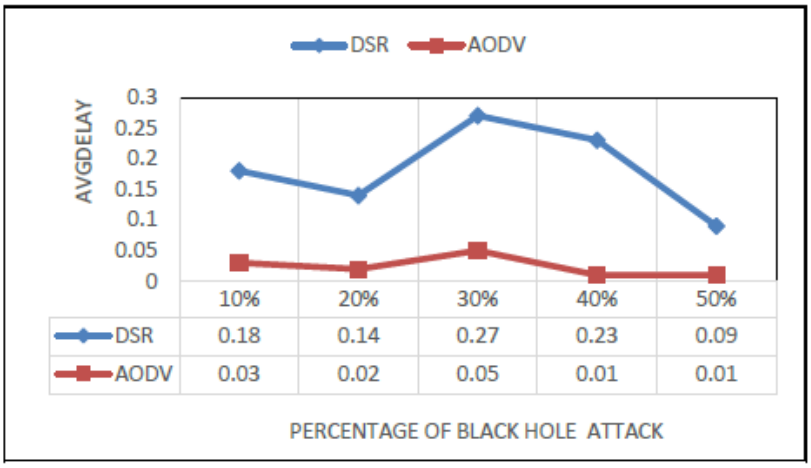

Figure 9. Average delay of the protocols with black hole attack

❖ **PACKET LOSS OF THE PROTOCOLS UNDER BLACK HOLE ATTACK:**

From Figure 10 below, it can be observed that packet loss for both protocols under black hole nodes increases when the percentage of the attack is increased. Also, as discussed earlier in the simulation of the normal protocols section, the DSR protocol has better performance than the AODV protocol for the same reasons discussed in the normal protocol.

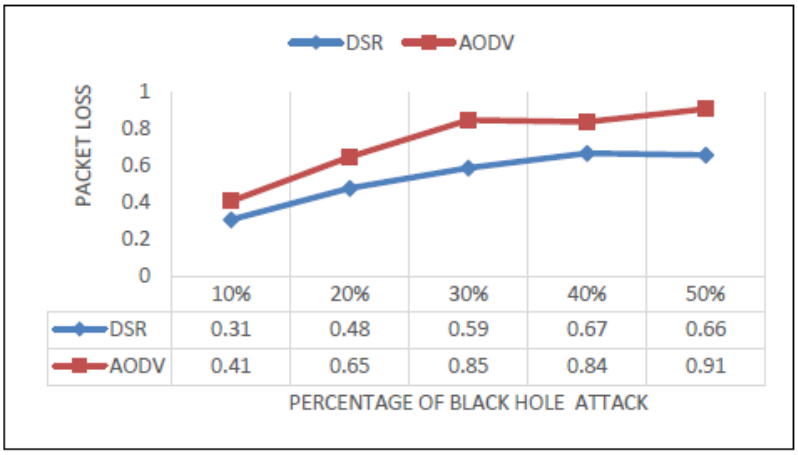

Figure 10. Packet loss of the protocols with black hole attack

❖ **ENERGY PER BYTE OF THE PROTOCOLS UNDER BLACK HOLE ATTACK:**

Figure 11 below shows the energy consumption of the protocols under different percentages of black hole attack. It is clear that DSR shows better performance than AODV, which increased slightly when the black hole nodes increased in the network, while the black hole attack had a very much greater impact on AODV, which increased from 0.11 when the percentage of black hole nodes was 10% to 0.68 when the attack increased to 50%.

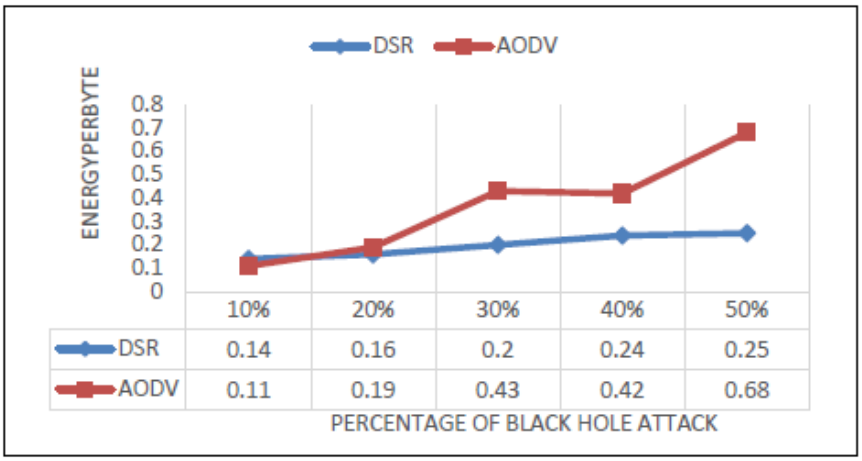

Figure 11. Energy per byte of the protocols with black hole attacks

8.3. GREY HOLE ATTACKS

Grey-hole attack has the same impact as black hole attack on throughput, average delay and energy consumption. However, it has a different effect on dropping packets in the protocols, for

the reason that it is designed to drop fewer packets than the black hole because of its fluctuation in behaviour. Consequently, at instance T1, a grey-hole node behaves normally, while at instance T2 it becomes a malicious node.

❖ **DROPPED PACKETS IN THE PROTOCOLS UNDER GREY HOLE ATTACK:**

As can be seen from the below graph in Figure 12, packet loss is higher in AODV than in DSR. The reason behind this is related to the same discussion as given above regarding selfish and black hole attacks.

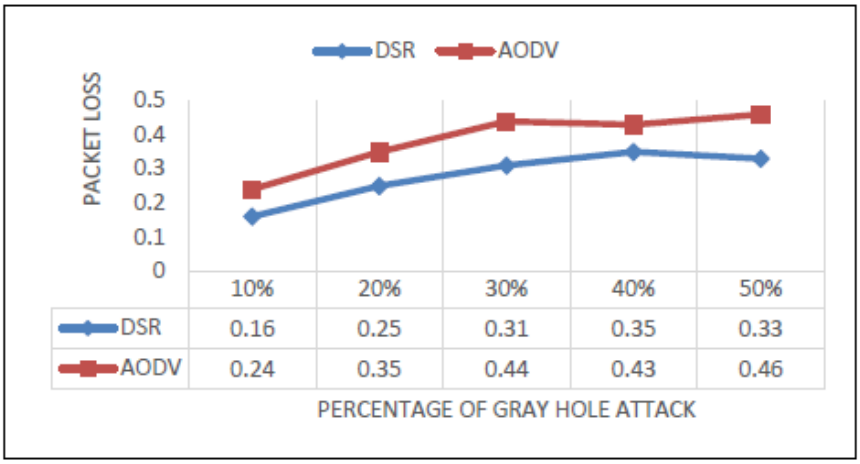

Figure 12. Packet loss of the protocols under grey-hole attack

9. CONCLUSION

Security is an important issue in MANET as hackers are finding new ways to intercept data during their exchange between wireless nodes in order to steal or tamper with it.

In this research paper, the performance of two protocols namely; DSR and AODV are evaluated by measuring several parameters under different attacks by introducing some malicious nodes within the network.

Based on the simulation results, DSR was affected more by selfish nodes than AODV. However, DSR performed better than AODV under black hole attack. In terms of average delay, under selfish nodes and under black hole attack, AODV has better performance than DSR, which has high average delay in all scenarios.

AODV performed better than DSR under selfish nodes, but under black hole attack, DSR performed better than AODV.

In the case of energy per byte and under selfish nodes, DSR consumed less energy than AODV. However, under black hole attack, DSR consumed more energy than AODV.

In summary, both DSR and AODV protocols have been affected by the attacks and their performance decreased in all terms (i.e end-to-end delay, packet loss, energy consumption and throughput). Therefore, such attacks need to be detected and prevented in MANETs.

REFERENCES

[1] Odeh, A. Abdelfattah, E and Alshowkan, M., (2012) "Performance evaluation of AODV and DSR routing protocols in MANET networks". International Journal of Distributed and Parallel Systems (IJDPS), 13(4), 13-22

[2] Gagandeep, A. & Kumar, P., (2012) "Analysis of Different Security Attacks in MANETs on Protocol Stack" International Journal of Engineering and Advanced Technology (IJEAT), 1(5), pp.269-275.

[3] Chandure, O.V & Gaikwad, V.T.,(2012) "Detection and Prevention of Gray Hole attack in Mobile Ad-Hoc Network using AODV Routing Protocol. " International Journal of Computer Application, 41(5), pp.27-32.

[4] Gorine, H. & M.Ramadan Elmezughi., (2016) "Security Threats on Wireless Sensor Network Protocols," 18th International Conference on Cryptology and Network Security, Kuala Lumpur, 18-19 August 2016.

[5] Soni, G. and Chandrawanshi, K., (2013) "A Novel defence Scheme Against Selfish Node Attack in MANET," International Journal on Computational Science & Applications (IJCSA), 3(3), pp.51-63.

[6] Kaur, H., Bala, M. and Sahni, V., (2013) "Study of Black Hole Attack using different routing protocols in MANETs." International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering (IJAREEIE), 2(7).

[7] Kavitha, T. & Sridharan, D., (2010) "Security vulnerabilities in wireless sensor networks: A survey". Journal of information Assurance and Security, 5(1), pp. 31-44.

[8] Singh, S.K., Singh, M.P. and Singh, D.K.,(2001) "A Survey on Network Security and Attack Defence Mechanism for Wireless Sensor Networks," International Journal of Computer Trends and Technology, May-June Issue.

[9] Haddad , I. F. & Gordon, D., (2002) Network Simulator 2: a Simulation Tool for Linux | Linux Journal. [Online] available at http://www.linuxjournal.com/article/5929 [accessed 12 January 2016]

[10] Kavitha, T. Sridharan, D., (2010) "Security vulnerabilities in wireless sensor networks: A survey". Journal of information Assurance and Security, 5(1), pp. 31-44.

[11] Taneja, S. & Kush, A., (2010) "A Survey of Routing Protocols in Mobile Ad-Hoc Networks". Internbational Journal of Innovation, Management and Technology, Vol.1, No.3.

[12] Tripathi,M., Gaur, M.S and Laxmi, V.(2013) "Comparing the Impact of the Black Hole and Gray Hole Attack on LEACH in WSN" , Procedia Computer Science 19, pp 1101 – 1107

[13] Vasudeva, A. and Sood, M., (2012) "Sybil attack on lowest id clustering algorithm in the mobile ad hoc networks", International Journal of Network Security & Its Applications. 4(5):135–147.

[14] Arunmozhi, S.A. & Venkataramani, Y. (2011) "DDos Attack and Defense Scheme in Wireless Ad Hoc Networks", International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.3

[15] Mohamed A. Abdelshafy, Peter J. B. King, (2014) "AODV Routing Protocol Performance Analysis under MANET Attacks", International Journal for Information Security Research (IJISR), Volume 4, Issue 2.

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

[17] Shahjahan, A. and Parma N.,(2016) "Comparative performance analysis of AODV and DSR routing protocols under wormhole attack in mobile ad hoc network on different node's speeds", International Conference on Computing Communication and Automation (ICCCA).