I.J.Modern Education and Computer Science, **2013, 10, 19-26**
Published Online November 2013 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijmecs.2013.10.03

Simulation and Analysis of AODV and DSR Routing Protocol under Black Hole Attack

Amin Mohebi
Faculty of Computing and Technology, Asia Pacific University of Technology and Innovation, Kuala Lumpur
amin_524@me.com

Ehsan Kamal
Faculty of Computer Science, Islamic Azad University of Hamadan, Iran
Ehsankamal86@gmail.com

Prof.Dr.Simon.Scott
Faculty of Computing and Technology, Asia Pacific University of Technology and Innovation, Kuala Lumpur
Simon@apu.edu.my

Abstract— In this paper, two routing protocols (AODV and DSR) are simulated under regular operation, single and cooperative black hole attack. This work has been performed by simulator to show consequence of black hole attacks in MANET by using various graphs which are used to collect data in term of several metrics. One common method to perform most of researches in the MANET security field is to simulate and analyze the routing protocols in various scenarios. This work has been based on the implementation and experiments in the OPNET modeler version 14.5. Finally the results have been computed and compared to stumble on which protocol is least affected by these attacks.

Index Terms— Mobile Ad hoc Network (MANET); Black hole attack; Cooperative Black hole attack; Ad-hoc On-demand Distance Vector (AODV**)**

I. INTRODUCTION

Information Technology (IT) is growing day-by-day however the network environments have become more and more complex to be used in industries. The Mobile Ad hoc Networks (MANETs) are indeed a part of this technological revolution. MANETs are a group of nodes that have communication with each other without any fixed infrastructure or centralized network authority, which communicate by transmitting data packets to another node or on behalf of another node. There is no limitation for connectivity and mobility and every node acts as a router for the other nodes [1]. However, acting the mobile nodes as router has benefits such as limitless connectivity and mobility but it makes MANET hard to be secured against attacks. Hence, having a secure MANET can be a challenging and vital issue due to various attacks that could be launched in this type of network. Mobile Ad hoc Networks suffer from various security attacks (i.e. Denial of Service (Dos), flooding attack, impersonation attack, selfish node misbehaving, routing table overflow attack, wormhole attack, black hole attack) which are due to no fixed infrastructure, network manager and centralized authority that make MANET vulnerable against these attacks [2]. Despite of the attacks mentioned above, there are various attacks that involve multiple nodes, which act in a cooperation and have received little attention. . The problems in single black hole attack have been solved, but a little attention has been paid to cooperative black hole attacks that act in a group**.** Hence**,** the main focus of this research is to analysis the behavior of cooperative black hole attacks and enhancing AODV routing protocol to prevent against the cooperative black hole attacks. Such a study is important due to packets that are dropped by cooperative black hole nodes in MANET. The research approach adopted in this paper includes a wide review of relevant literature on black hole attacks in MANET, coupled with the collection and analysis of data obtained of OPNET simulator, and in order to get results some different scenarios were simulated

II. RELATED WORKS

Deng [2] used On-Demand Distance Vector (AODV) and proposed a solution for black holes attacks. This solution related to when an intermediate node applies for RREQ, the RREP packet should be included information about the next hop to destination. Next, the source node sends a further request (FREQ) to next hop of replied node to know about replied node and route to the destination. This approach may help to identify the reliability of the replied node if the next hop is trusted. Sun Guan and Chen [3] used On-Demand Distance Vector (AODV) as their routing protocol. The detection scheme utilized neighborhood-based technique to discover the black hole attacks and represent a routing recovery protocol to create a reliable route to the destination. They designed a method with two parts to encounter with black hole attack. Al-Shurman M, Yoo S-

M, Park S [4] used two techniques to avoid the black hole attack in mobile ad hoc networks. The first technique would find at least two routes from the source to the destination node. The second technique is related to number of unique sequence used. The authors simulated the proposed approach by NS2 and they confirmed that these techniques have less numbers of RREQ and RREP in comparison with current AODV.A study has been conducted by Latha Tamilselvan [5] who proposed a solution to enhance the original AODV protocol. This concept was designed by setting timer in the RimerExpiredTable to collect the other request from other nodes when receiving the first request. The packet's sequence number and the received time will be stored in a Collect Route Reply Table (CRRT), calculating the timeout value based on the arriving time of the first route request then it judges the validation of the route based on the threshold value. The author simulated this solution by (GloMoSim) and results indicate that packet delivery ratio was improved with low delay and overhead. Tsou ,Chang , Lin , Chao and Chen [6] presented a novel approach entitled Bait DSR (BDSR) scheme to defend the collaborative black hole attacks. This approach has been composed of both proactive and reactive method to create a hybrid routing protocol. The basis routing protocol utilized is the Dynamic Source Routing on-demand routing. In this approach, firstly the source node sends bait RREQ packet. A similar technique that was used in DSR is used here to prevent the traffic jam problem which will be generated by bait RREQ. These sent bait RREQs could easily detect malicious nodes and defend against black hole attacks. RREPs additional field is able to keep the identity of malicious nodes. Therefore, the source node could simply discover the situation of malicious nodes and Remove all the RREPs coming from that location. The authors discovered that this approach has higher PDR in compare with existing DSR and the communication overhead was improved when compared with DSR routing protocol. Finally, Rutvij, Sankita and Deves h [7] investigated on some of the existing approaches for black hole and gray hole attack and presented a novel solution against these attacks which is able to find effectively short and secure routes to destination. Their theoretical analysis illustrated that this approach properly can increase packet delivery ratio (PDR) with negligible difference in routing overhead. The authors believed that this algorithm could be used for the other reactive protocol and finds and eliminates malicious nodes within the route finding phase. Nodes receiving RREP confirm the truth of routing information; source node broadcasts a list of malicious nodes when sending RREQ. Nodes update route tables when they get any information of malicious nodes from received routing packets. No additional control packet can be mentioned as benefit of this algorithm and there is minor difference in routing overhead which is the ratio of the number of routing related transmissions to the number of data related transmissions. Additionally, the malicious nodes would be isolated and packet delivery ratio (PDR) will greatly be improved.

III. PROTOCOL USED IN MANETS

Mobile ad-hoc Network normally is based on TCP/IP structure to offer the means of communication between communicating work stations which are mobile nodes by limited sources. Hence, the old-fashioned TCP/IP model shall be modified to provide efficient functionality that has been made the routing protocols as key research area for investigators and challenging task as well. There are various routing protocols in MANET which are categorized in term of functionality as follow:

A. **Proactive protocols:** act different when compared to reactive protocols. Basically, Proactive routing protocols maintain the updated topology of the network. Every node knows the other nodes in the network in advance. As their name implies, these protocols are deployed when they are required. AODV is a routing protocol that has been chosen to be investigated in detail. This protocol is designed for MANETs and it is employing the on-demand routing method to establish the routes between nodes. The main benefit of this protocol is establishment of desired route to destination when the source node requires and it keeps the routes as long as they are needed. Another benefit of AODV is having proper quality to support broadcast, multicast and unicast routing with scalable characteristic and self-starting. AODV let mobile nodes to forward the packets through their neighbors (which maybe do not have direct communication to the destination) until the destination node receive the data packets. This protocol is able to find the shortest and loop free routes to transmit data packets. Also, AODV can create a new route in case of link downs or changes in route. DSR is another routing protocol that has been chosen for this work. This protocol manages the waste of bandwidth by removing the requirement of periodic table updating. DSR establish a route to destination for source node, hence there is no need to transmit periodic 'HELLO' message by a node to notify its neighbors about his presence [8]. The main point of this protocol is that intermediate nodes of MANET do not require to maintain route information which makes less load in the network and the path is simply defined in data packets of source node.

B. **Reactive protocols:** that known as On Demand Reactive protocols which never initiate route discovery, unless they are requested by a source node. In other word, these protocols setup routes when demanded.

C. **Hybrid protocol** is created by exploiting the benefits of both reactive and proactive protocols which could be used to achieve better results. In this protocol the network will be divided into two zones. One protocol can be used within zone and the other one between zones [9].

IV.ROLE OF ATTACKS IN MANETS

This kind of network (MANET) could be attacked in the various ways. Hence, before investigating the other sections, the attacks should be classified in the context of MANET. The attacks could be classified base on the source of attacks (Internal or External), behavior of the attacks (Passive or Active attack) and routing (i.e. special attacks).

A. Passive vs. Active attack

Passive attacks are aimed by an attacker to steal important information in the entire network. Eavesdropping attacks and traffic analysis attacks are two common types of passive attack [10] Active attacks modify the data with the aim of obstruction of the operations in the targeted network.

B. Internal vs. External attack

As the name implies, the attacker stays on the outside of the network and aims to block the authorized access to functions in the network (i.e. http traffic) or even produces network congestion to disrupt the entire network. If the network is correctly configured, the external attack could be difficult to be lunched. While, the internal attacks are much tougher to defend against which want to have normal access to the network as well as participate in the normal activities of the network.

C. Routing attacks

Usually, there are four different kinds of MANET routing protocol attacks which are divided into several types as following:

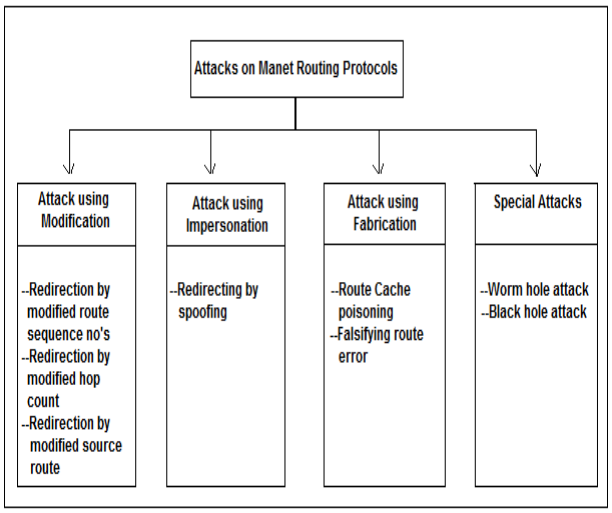

Figure 1: Attacks on MANET routing protocols

D. Attacks using Modification

In this kind of attacks, the attacker modifies the messages in the protocol fields and passes them between nodes and it causes traffic subversion and traffic redirection.

E. Attacks using Impersonation

This kind of attack is used to violate authenticity and confidentiality of a network. Normally, the attacker is a malicious node which impersonates the address of the other user node in order to change the network topology.

F. Attacks using Fabrication

In this type of attacks, where an attacker uses a malicious node to inject wrong messages or fake routing packets in order to disrupt the routing process.

G. Special Attacks

There are various types of attacks which are only occurred against routing protocols such DSR and AODV. The worm hole, gray hole and black hole attack are the common types of special attacks

- *Worm hole Attack*

One of the severe types of special attacks is worm hole attack which attackers use of two malicious nodes in MANET in order to forward the packets over a private tunnel. This tunnel is aimed to record the traffic data and channels them to another place in the network. This type of attack is known as invisible attacks due to attackers are hidden at higher layers.

- *Gray hole attack*

In gray hole attack an attacker misleads the network to forward the desired packets through the network. When the attacker receives the packets from neighbor nodes, then it drops the packets without delivering to the destination node. In this type of attack the attackers act normally in the beginning of the attack and they send true RREP to the nodes that sent RREQ. When they receive the packets, they drop the packets and Denial of Service (DoS) will be launched.

- *Black hole attack*

Black hole attacks have been known as the most important concern of security experts in MANET and the main aim of this work is black hole attack. The attackers use of one or more malicious nodes which advertise themselves in the network by setting a zero metric to all the destinations that causes all the nodes toward the data packets to these malicious nodes. The AODV and DSR are vulnerable against black hole attacks due to having network centric property, where all the nodes have to share their routing tables for each other.

V. THE OVERVIEW OF SELECTED ATTACKS

As explained in previous sections, MANETs offer unique benefits, but they are encountered with unique challenges as well, such as the dynamic topology, bandwidth constraint, media interference, etc. Hence, the security of MANET has been considered as main concern among security experts especially in routing protocols. In previous section a brief classification of attacks was described. The main aim of this paper is to investigate on the black hole attack with respect to routing protocols therefore the author compared routing attacks in following table to show the importance of this kind of attack in term of following properties.

1-**Type of attacker**: Internal attacker or external attacker.
2-**Required knowledge**: The amount of knowledge that attackers require to know about network to successfully perform the attack.
3-**Cost:** The amount of resources and time that attackers need to run an attack.
4-**Detectability:** The level of detectable of an attack on the network layer or routing protocols.

TABLE 1. Comparison of attacks

Attack	Required Knowledge	Cost	Detectability
Black-hole Single Cooperative	 Low Low	 Low Low	 High Low
Worm hole	High	High	Low
Gray hole	Medium	Medium	Low

As it is shown in the table 1, black-hole attacks are preferred by most of attackers who have intention to forge the entire network communication with minimum cost and amount of knowledge about MANET because the black hole attack needs to minimum cost and required knowledge when compared with other attacks. According to the table 1, the level of detectability of single black hole attack is certainly higher than other attacks but there is a more complex form of Black-hole attack that is called Cooperative Black-hole attack which has been considered to be hard to be defended. Therefore, the black hole could be the most important attack that shall be studied to achieve a secure MANET and this study will be carried on in this area. The next section aims to defined Black-hole attack in detail.

VI. Black hole Attack on AODV Routing Protocol

The black hole attack includes malicious nodes that forge the nodes to drop the data packets. When a source node wishes to communicate with the other nodes or transmits the data packets to the destination, it sends a RREQ to its neighbors to know the true path to the destination. If there is one or more malicious node (black hole node), it receives the RREQ then sends a fake RREP to sender which shows malicious node already has a true path to the destination and this RREP message includes false routing information and fake higher sequence number that shows it is a fresh path. When the sender of RREQ receives the RREP, it assumes the malicious node as true node then it transmits the data packets within the route that specified by black hole node. Black hole nodes receive the data packets without sending the packets to the destination or the other nodes. By creating routing loops, network congestion and channel contention, attackers degrades the network performance. This kind of attack is illustrated in the figure 2. The source node transmits RREQ packets to its neighbor nodes “B” and “D” to discover fresh route to the destination “F”. The black hole node ”M” immediately respond to the source node without checking its routing table to say it has a fresh path to the intended destination which is done by sending a fake RREP to the source node “A”. The source node “A” considers that the route discovery has been done then rejects other RREP message from other nodes. Then, the attacker will drop the received packets without sending to the destination “F”.

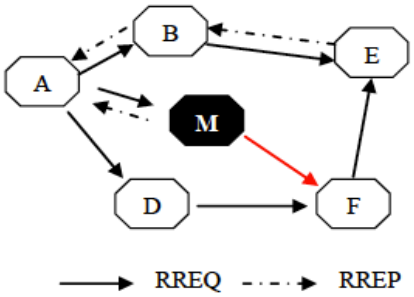

Figure 2: Single black hole attack

However, in case of multiple black hole nodes which act in coordination the level of detectability is low. In this form of black hole attack, multiple black hole nodes are cooperating with each other to attack the intended node or network. For example, as shown in figure 3, the black hole node “B” is cooperating with black hole node “B2” which is its teammate as the next hop.

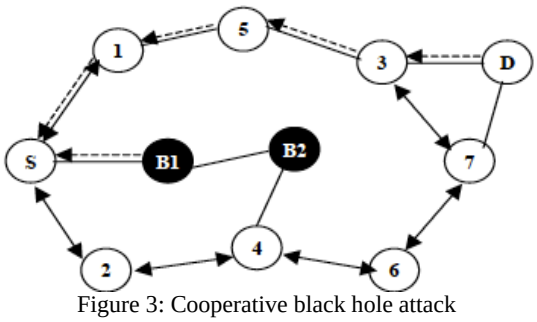

Figure 3: Cooperative black hole attack

Black hole attack in AODV protocol can be performed in two ways [11]. Black hole attacks caused by RREP and by RREQ as discussed in table 2.

TABLE2. Two ways of Black hole attack

Caused by RREQ	Caused by RREP
Set the initial IP address in RREQ to the IP address of source node	Set the initial IP address in RREP to the IP address of source node
Set the destination IP address in RREQ to the IP address of destination node	Set the destination IP address in RREP to the IP address of destination node
Set the destination IP address of IP header to broadcast address	Set the destination IP address of IP header to the IP address of node that RREQ has received
Set the source IP address of IP header to its own IP address and put high sequence number and low hop count in the RREQ field	Set the source IP address of IP header to its own IP address

VII. Simulation Environmen

In this paper, two routing protocols (AODV and DSR) are simulated under regular operation and cooperative black hole attack. This work has been performed by simulator to show consequence of black hole attacks in MANET by using various graphs which are used to collect data in term of several metrics There are several network simulators software which are available to perform such projects, such as NS-2, OPNET , GLOMOSIM , etc. This research has been based on the implementation and experiments in the OPNET modeler version 14.5. This is because, OPNET is considered as one of the leading environments for network modeling. It offers huge number of built-in industry standard network devices protocols and application. Moreover, it helps to programmers to modify the network elements and compare with each other.

A. Performance Metrics

Various statistics and performances metrics can be used to evaluate the proposed routing protocols with and without black hole attacks. These matrices are important to show the performance analysis of network. This section is aimed to explain the essential metrics that are used in this dissertation.

- Network throughput

A network throughput is the average rate at which message is successfully carried between source node and destination node. It is also referred to as the ratio of the amount of data received from its sender to the time the last packet reaches its destination [12]. Bits per second (bps), packets per second or packet per time slot can be considered to measure the throughput but OPNET deploys bits per second to measure the throughput. A MANET network needs to ideal throughput which should be at high level. The main factors that affect on the throughput are bandwidth, limited energy, change in topology and untrusted communication.

- End-to-End delay

End-to-end delay is the average time that starts in the first node by generating the packets till the arriving the packets in destination node which shown in seconds. This delay includes the overall delay in the networks (i.e. buffer queues, transmission time and so on). In MANET networks, this metric could be accrued due to link downs and/or the weakness of the signal between nodes. This delay will be reduced when a reliable routing protocol is set up in the network. This is because, the routing protocol establishes a true route and every node knows the route to its destination so, the number of packets is reduced.

- Network load

Network load is a major parameter with large effect on networks protocols that referred to the overall load that is impacted by the whole higher layer in all WLAN nodes in the network. Generally, Network load is based on the results of buffer availability, exploited bandwidth and processing time at intermediate nodes. Network delay produces a load in the network and hence there will be more delay in starting time because of establishing connection for MANET nodes which results a peak load and it will be reduced when connection establishment is done.

B. Assumption

The mobility of 10 m/s is considered for all the nodes. This simulation was done in 1000 x 1000 meters. All the scenarios were run for 600 seconds. Packet Inter- Arrival Time (sec) is considered as exponential (1) and packet size (bits) is exponential (1024). 11 Mbps is taken for each mobile node as data rate. A constant speed of 10 m/s was allocated as Random way point mobility with pause time of constant 100 seconds. This pause time is taken after data reaches the destination only. The main goal was to find out the better protocol against attacks in case of black hole attack. AODV and DSR routing protocol which are reactive protocols respectively are selected. In both protocols, malicious nodes buffer is lowered to a level which increase packet drop. Table 3 depicts the mentioned parameters.

TABLE 3. Documentation of assumptions

Examined protocols	AODV and DSR
Simulation time	600 seconds
Simulation area (m x m)	1000x1000
Number of Nodes	8-16-32-64
Performance Parameter	
Pause time	100
Mobility (m/s)	10(m/s)
Packet Inter-Arrival Time (s)	Exponential (1)
Packet size (bits)	Exponential (1024)
Transmit Power (W)	0.005
Date Rate (Mbps)	11 Mbps
Mobility Model	Random waypoint

VIII. Results & Discussions

This scenario aims to show the performance of AODV and DSR, when there are different numbers of mobile nodes and black hole nodes. The main benefit of this scenario is to understand MANET performance when the number of mobile nodes and black hole nodes are changed.

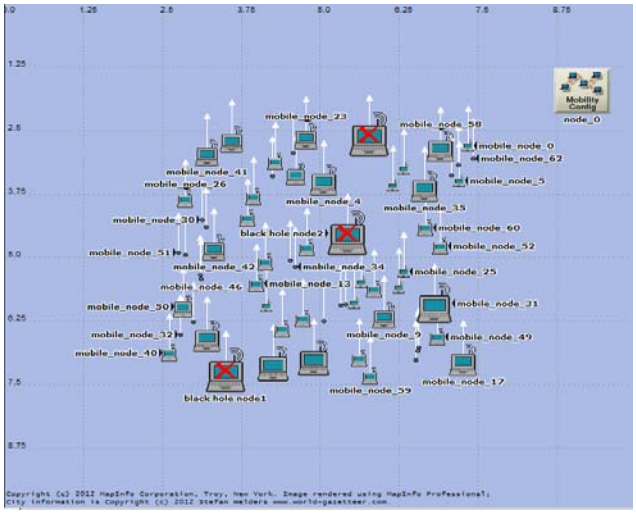

Figure 4: MANET model layout with different mobile nodes

A. *Throughput*

This section aims to show the throughput of both protocols when they are under different numbers of black hole nodes. Figure 5 illustrates the case of 8 nodes where that DSR outperforms AODV in all the numbers of black hole nodes. In the figure 6, the case of 16 nodes is observed. AODV and DSR act approximately like each other where there is no attack or only single attack. However, when the number of black hole nodes is increased, DSR again outperforms AODV.

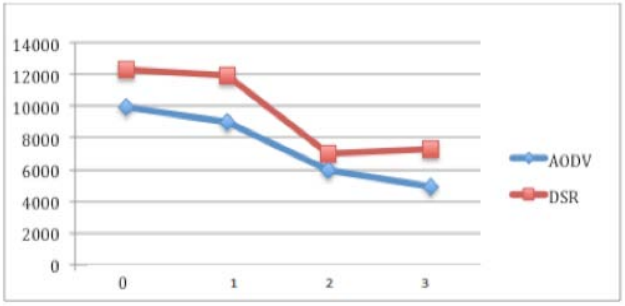

Figure 5: Throughput of 8 nodes

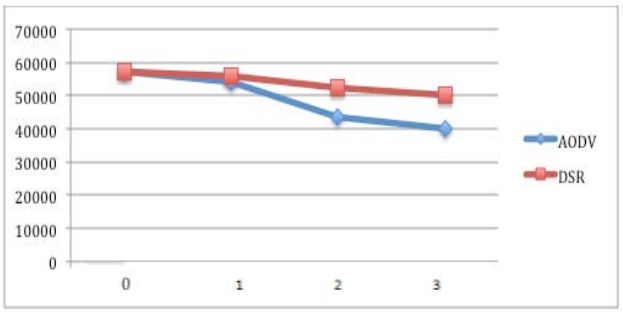

Figure 6: Throughput of 16 nodes

Figure 7 and 8 show the throughput for case of 32 and 64 nodes. In both case when there is no attack, AODV performs the best and its performance is improved by increasing the number of nodes as compare to previous scenarios. When the number of black hole nodes is increased, the performance of both protocols was reduced but AODV still performs better than DSR.

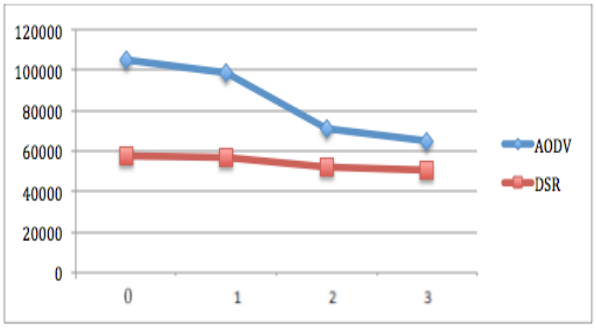

Figure 7: Throughput of 32 nodes

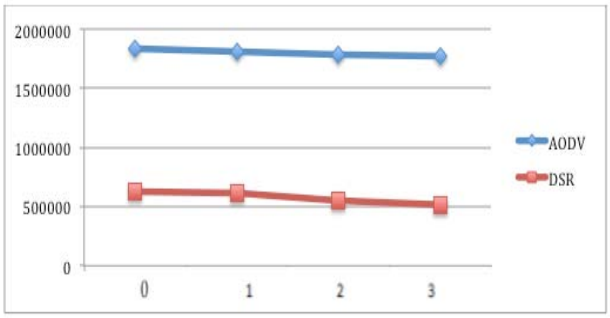

Figure 8: Throughput of 64 nodes

B. *Network load*

This section shows the network load of both protocols when they are under different numbers of black hole nodes. Figure 9 depicts the case of 8 nodes where that DSR performs far better than AODV in all the numbers of black hole nodes. In the figure 10, the case of 16 nodes is shown. AODV and DSR perform approximately like each other however DSR performs little better than AODV, when the number of black hole nodes is increased. In overall, it is observed that the performance of DSR is decreased when the network moves from 8 nodes to 16 nodes.

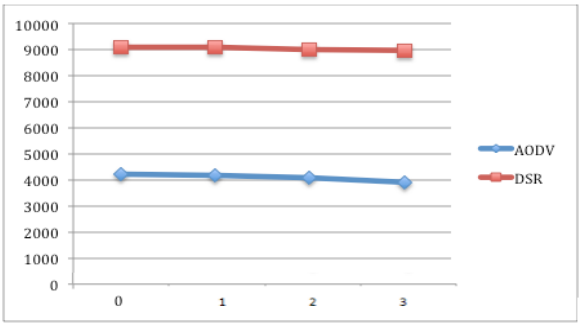

Figure 9: Network load of 8 nodes

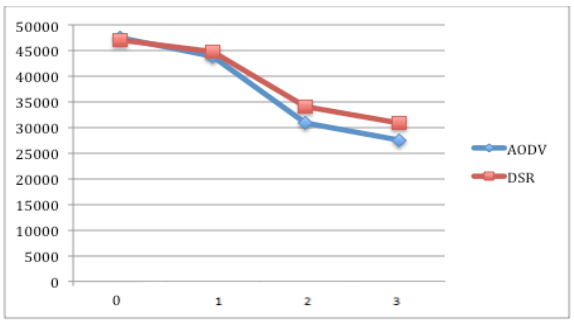

Figure 10: Network load of 16 nodes

Figure 11 and 12 indicate the network load for case of 32 and 64 nodes. In both case, AODV performs the best and its performance is improved by increasing the number of nodes as compare to previous scenarios. It is also observed that when the number of black hole nodes increase, the performance of both protocols is reduced but AODV outperforms DSR.

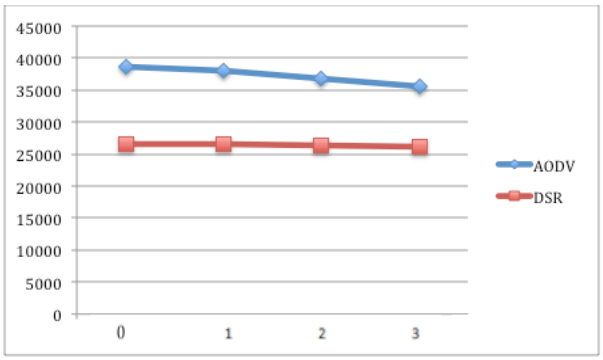

Figure 11: Network load of 32 nodes

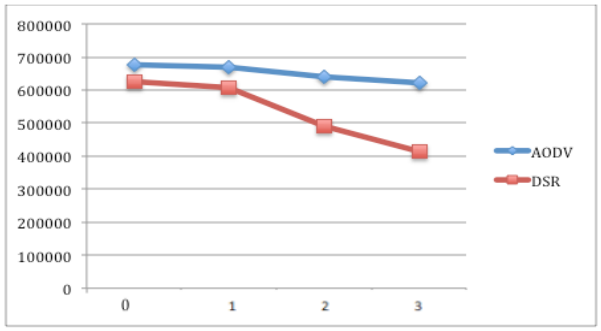

Figure 12: Network load of 64 nodes

C. *Delay*

Figure 13 illustrates the case of 8 nodes where that DSR shows the less delay when compared with AODV. It is also observed that DSR has the less delay, when the number of black hole nodes is increased.

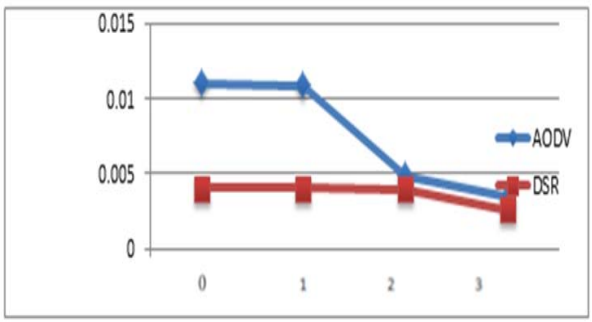

Figure 13: Delay of 8 nodes

In case of 16 nodes (figure 14), delay in AODV is less than DSR, when there is no attack. However, when the number of black hole nodes increase, DSR shows less delay as compare to AODV.

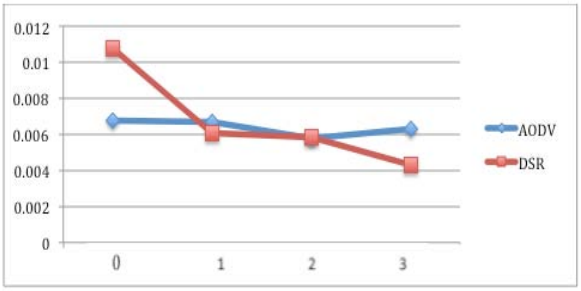

Figure 14: Delay of 16 nodes

Figure 15 and 16 indicate the delay for case of 32 and 64 nodes. In both case when there is no attack, AODV performs the best and its performance is improved by increasing the number of nodes as compare to previous scenarios. When the number of black hole nodes is increased, the delay of both protocols is reduced but AODV still has the less delay when compared with DSR.

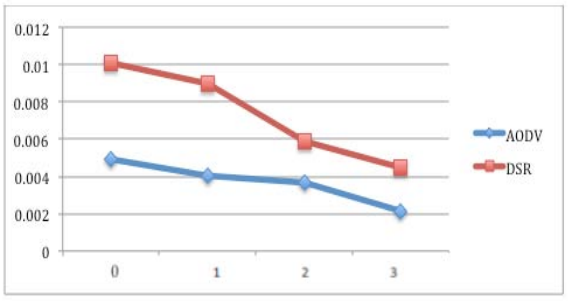

Figure 15: Delay of 32 nodes

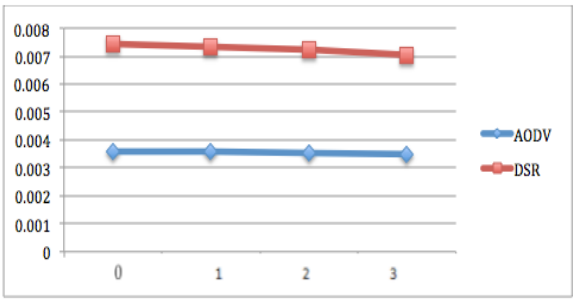

Figure 16: Delay of 64 nodes

IX. Conclusion

In this paper, two routing protocols (DSR and AODV) are evaluated in a simple environment and malicious environment. There are various parameters to evaluate the performance of any routing protocol which described in previous section. Both AODV and DSR routing protocols show good percentage of originated data packets where there is node mobility occur. Both DSR and AODV are on-demand protocols whose basic characteristic is demonstrated in the shape of its overhead. In order to realize the differences in the simulation results and also to compare results, the simulation was done in five scenarios based on different network sizes with/without black hole attack which means first experiment for regular operation of MANET and second experiment for MANET operation under a cooperative black hole attack. The experiments display encouraging results gained from the five scenarios. The MANET under regular operation outperforms the MANET under cooperative black hole attack in terms of throughput and network load in both cases. The results obtained are used to find the impact of the cooperative black hole attack on MANET because the network load and throughput of a good network should be high. On the other hand, the results in term of End-to-End delay show that MANET under cooperative black hole attack had a slight reduce because the black hole nodes claim to have ta quick route to destination by providing a quick RREP to source node which makes these nodes as benign node and it is obvious that the End-to-End delay will be decreased in the entire network. In conclude, DSR routing protocol is not efficient for large networks with many mobile nodes and this protocol shows big variation in malicious environments for huge networks. In such situation AODV routing protocol is ideal because of its hop-by-hop routing.

Reference

[1] Weerasinghe, H. and H. Fu, “Preventing cooperative black hole attacks in mobile ad hoc networks”. Simulation implementation and evaluation. Future Generat. Commun. Netw, 2007, Volume 10, Issue, 6, pp. 362- 367.

[2] Deng H, Li W, Agrawal “Routing Security in Wireless Ad-hoc Networks”. IEEE Communications Magazine, 2002 Volume 103, Issue, 10 pp. 70 – 75.

[3] Bo Sun,Yong Guan,Jian Chen,Udo W.Pooch “Detecting Black-hole Attack in Mobile Ad Hoc Network”. 5th European Personal Mobile Communications Conference, Glasgow, April 2003 Volume 492, Issue, 22-25 pp. 490 – 495.

[4] Mohammad AL-Shurman,Seon-Moo Yoo and Seungiin Park,” Black Hole Attack in Mobile Ad Hoc Networks” ACMSE’04,April 2-3,2004,Huntsville,AL,USA.

[5] Latha Tamilselvan & Sankaranarayanan, V. (2007). Prevention of Blackhole Attack in MANET. The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications (AusWireless 2007) Pages 21-27.

[6] Tsou P-C, Chang J-M, Lin Y-H, Chao H-C, Chen J-L, “ Developing a BDSRScheme to Avoid Black Hole Attack Based on Proactive and ReactiveArchitecture in MANETs”. Paper presented at the 13th InternationalConference on Advanced Communication Technology, Phoenix Park, Korea,Feb. 2011, pp. 13-16 .

[7] Rutvij H. Jhaveri , Sankita J. Patel. (2012). DoS Attacks in Mobile Ad-hoc Networks: A Survey. *2012 Second International Conference on Advanced Computing & Communication Technologies*. 2 (2), p535-540.

[8] Mukija, A, “Reactive Routing Protocols for Mobile Ad Hoc network”. IEEE Network magazine, special issue on networking security, 2001, Volume 14.

[9] K.Netmesiter “Routing protocols In Mobile Ad Hoc Networks: Challenges And Solutions”. IEEE Wireless Communications Magazine, Sponsored byIEEE Communications Society, February 2010,Volume 11, Issue.

[10] Bouam and Z. Othman. “Securing Ad Hoc Networks”. IEEE Network magazine, special issue on networking security, November/December 2003,Volume 13, Issue, 6.

[11] Deborah Estrin, Lewis Girod, Greg Pottie, and Mani Srivastava. Instrumenting the world with wireless sensor networks. In International Conference on Acoustics, Speech, and SignalProcessing, 2001.

[12] N.V Trang and X.Xing “Rate–adaptive Multicast in MANETS” WiMob’2005, Volume 3, Issue, 19 pp. 352-360.

Authors’ Profile

Amin Mohebbi has received MSc degree from Staffordshire University in 2013. He is studying Phd in Computer Science from 2013 in UM University. He is a research scholar in Computer Science Department of UM university in Malaysia. He has published over 5 papers in various International Conferences. His areas of interest are Mobile Ad hoc Networks, Swarm Intelligence and Software Testing.

Dr. P. Simon Scott received the Master ‟ s degree in Computer Science from Cambridge University. He received Ph.D. degree in mathematical science from Bath University. He is currently working as Professor in Department of Computer Science in APU University, Kuala Lumpur, Malaysia He published several papers in National and International Journals. He is active member of various professional bodies. His current research is focused on artificial intelligence.