ISSN 2277-3061
Volume 16 Number 1
INTERNATIONAL JOURNAL OF COMPUTERS & TECHNOLOGY

Enhanced AODV Protocol for Detection and Prevention of Blackhole Attack in Mobile Ad Hoc Network

Sherin Hijazi[1], Mahmoud Moshref[2], Saleh Al-Sharaeh[3]
1st The University of Jordan, Amman, Jordan, sherinhijazi@yahoo.com
2nd The University of Jordan, Amman, Jordan, Moshref2008@gmail.com
3rd The University of Jordan, Amman, Jordan, ssharaeh@ju.edu.jo

ABSTRACT

Mobile Ad-hoc Network (MANET) is a kind of wireless network that has the most challenging network infrastructure. It is formed using the mobile nodes without any centralized administration from the security perspective and is a self-configuring fastest emerging wireless technology, each node on the MANET will act like a router which forwards the packets. Dynamic nature of this network makes routing protocols to play a prominent role in setting up efficient route among a pair of nodes. Dynamic Source Routing (DSR) and Ad-hoc On-Demand Distance Vector (ADOV) is a reactive MANET routing protocols. Most of the attacks on MANETs are routing protocol attacks. Attacks on routing protocols, especially internal attacks will cause the damage to MANETs. Sinkhole and black hole attacks are a type of internal attack which is affected by attempting to draw all network traffic to malicious nodes that fake routing update and degrade the performance of the network. The black hole nodes should be detected from the network as early as possible via detection mechanism and should also guarantee the higher detection rate and less cross-over error rate. In this paper, we studied the characteristics of black hole attack and how it will affect the performance of the distance vector routing on demand routing protocol such as (ADOV) protocol, which recognizes the presence of black hole node from packet flow information between nodes and isolates it from the network via applying AODV protocol that one of popular routing protocol. We have evaluated the performance of the system using widely used simulator NS2, results prove the effectiveness of our prevention and detection method.

Indexing terms/Keywords

AODV, DSR, Black hole attack, MANET, NS2.

Academic Discipline And Sub-Discipline

Computer Science.

SUBJECT CLASSIFICATION

Networks.

TYPE (METHOD/APPROACH)

Wireless Network

1. Introduction

Mobile Ad hoc networks (MANET) are the collection of autonomous nodes; each node determines the topology of the network. They can communicate to each other via some wireless network (or radio links). Two nodes can communicate directly to forward messages from the source node to neighbors till the messages reach the destination nodes so the nodes act as both host and router at the constant time, but if these nodes are beyond the network range then they need some intermediate nodes to deliver the packet to the designated node. Since the transmission between two nodes should rely on nodes, several routing protocols [11, 7, 12, and 20] have been proposed for ad hoc networks in order to establish an accurate and efficient route between the pair of nodes.

MANETs are more vulnerable to network attacks as it gains and loss many nodes simultaneously, and these nodes are pushed into the resource constraints such as bandwidth, storage, and energy capacity. Attacks on MANETs can be categorized into two major groups: internal and external [13].

An internal attack is originated from a compromised node of the same network. They drop, fabricate, alter, or misroute data packets. The external attack is not participating in the routing process but disrupt network operations like flooding, DOS, or cut-off nodes from network [3].

Sinkhole and blackhole attack is an internal attack where an adversary node misleads routing packets not to select the appropriate path between source and destination. And it diverts all routing packets to itself in order to extract network traffic information and may perform selective forwarding [2, 5, 6]. Black hole attacks are the most popular examples of sinkhole attack. A blackhole attack is an active denial of service attack in which a malicious node can attract all packets by falsely claiming a fresh route to the destination and then absorb them without forwarding them to the destination [23].

Dynamic source routing protocol DSR is a reactive protocol of MANET. It involves two phase: route discovery phase and the route maintenance phase. During the routing discovery, the sinkhole attack is carried out when the sinkhole node propagates a bogus message to advertise the shortest path to the destination node. AODV routing protocol is

compensation or improvement protocol form DSR and DSDV protocols it borrows the routing mechanism and routes discovery from DSR [10].

This paper proposes a secure routing protocol to defend against the attack. The rest of the paper is organized as follows. Section 2 describes routing protocol and malicious attack- an overview. Section 3 contains the related works. Section 4 describes the methodology. Section 5 has the experimental and results in the evaluation. Section 6 concludes the results and presents the future works.

2. An-Overview

We will give an overview of routing protocol and Malicious attack. To show some of it is characteristics.

2.1 Dynamic source routing (DSR)

Dynamic source routing (DSR) is an on-demand/ reactive routing protocol of MANET where the nodes on the network utilize the source routing mechanism [10]. It involves two main phases one is routed discovery phase and the other is route maintenance phase [15] and DSR works in two phases: route discovery and route mechanism [1]. It doesn't send periodic beacons for route maintenance. It uses route cache instead of routing tables [1]. The source node adds the routes that have to be taken by each packet after the route discovery. This route information is stored in a cache memory of the nodes. To discover a route, the source node that needs to send the packet to the destination node floods a Route Request (RREQ) message. The RREQ has sender's address, destination address and a unique sequence ID determined by the sender. Whenever the RREQ reaches a neighboring node they will check their cache memory for a route to the destination. If there is a route to the destination or if this node is the target (destination) node they will append their ID and send Route Reply (RREP) message back to the source node in the reverse path followed by the RREQ. If the node is not the destination node, then it will append its ID in the RREQ and forwards this to its neighboring nodes. After this route discovery process, the source will append the whole path in the other packets and will send it to the destination [10] [15]. The dynamic source routing protocol does not have any detection mechanisms to find out the presence of malicious nodes in the network [15].

2.2 AODV Routing Protocol

It is compensation or improvement protocol form DSR and DSDV protocols it borrows the routing mechanism and routes discovery form DSR [11]. The main advantage for AODV over DSR is the source route does not need to be included in each packet. So this will give less overhead than DSR. So in our research, we go to use AODV to simulate ad hoc Mobile network (MANET), for this reason. The routing messages do not contain information about the whole route path, but only about the source and the destination [22]. In AODV when source node needs to send the packet to the destination node, it broadcast its request (RREQ) to its neighbors. Then each node that found in neighbors do reverse route toward the source node to tell it about the fresh route to the destination when the destination receives RREQ, it relies on (RREP).

2.3 Sinkhole Attach

Sinkhole attack is a type of internal attack is affected by attempting to draw all network traffic to malicious nodes that fake routing update and degrade the performance of the network. The idea of the attacker in this attack is to attract all the network traffic towards itself [4]. The attacker executes this attack by making the neighboring nodes believe that the shortest path to the destination is through it. One of the impacts of sinkhole attack is that it can be used to launch other attacks like selective forwarding attack, acknowledge spoofing attack and drops or altered routing information. It can also use to send bogus information to the base station. It increases network overhead, decreases network's life time by boosting energy consumption; finally, destroy the network [14].

In DSR protocol, Sinkhole attack affects the performance of the DSR routing by using the flaws like sequence number. The sinkhole node modifies the sequence number [10].

2.4 Black hole Attack

The most popular examples of sinkhole attack are black hole attack. A black hole attack is an active denial of service attack in which a malicious node can attract all packets by falsely claiming a fresh route to the destination and then absorb them without forwarding them to the destination [23].

When a source node broadcasts the RREQ message for any destination, the black le node-replay with RREP that includes the highest sequence number and this message is perceived as if it is coming from the destination or from a node which has a fresh enough route to the destination. The source assumes that the destination is behind the black hole and discards the other RREP packets coming from other nodes. The source then starts to send out its data packets to the black hole trusting that these packets will reach the destination [24]. A black hole attack (or sinkhole attack) also leads to denial of service in wireless mesh networks. It also exploits the route discovery mechanism of on-demand routing protocols. Almost all the traffic within the neighborhood of the malicious node will be directed towards the malicious node, which may drop all the packets, resulting in the denial of service [25].

3. Related Work

Different solutions which were used to detect and identified sinkhole and blackhole attack were suggested by different researchers, H. Deng, W. Li, and D. P. Agrawal, each source requires next hop information of each node of source route to verifies the truthfulness of the route [6].

S. Lee, B. Han, and M. Shin Requires each node send route Confirmation REQuest (CREQ) to next hop node. Next node checks the route cache, confirms the route and remote destination and sends a reply to the source. The same procedure was followed by all intermediate nodes in the source to destination path [18].

S. Marti, T. J. Giuli, K. Lai, and M. Baker, and Watchdog proposed the scheme to detects and mitigates malicious node attack to improve the performance of a network. [19]. S. Buchegger and J.-Y Le Boudec, suggests CONFIDANT method consists of four modules Monitor, Reputation System, Trust Manager, and Path Manager, all four modules work together and removes malicious node [17].

Tseng and Culpepper proposed two sinkhole detection indicators for MANETs which use the DSR protocol [21]. Marching and Datta proposed a collaborative technique which uses a monitor [9]. Kim et al proposed the cooperative method. This method uses three kinds of packets for isolating sinkhole nodes node for the detection of the malicious nodes [8]. Shim et al. proposed Cluster analysis method for sinkhole detection. [16].

4. Methodology

The methodology of this project is divided into three steps:

First step: reviews related work and gathering information from different papers.

Second step: analyze the requirement project needing to design experimental via the NS2 simulator.

Third step: implement and apply the design solution and outs the results.

Figure 1 shows the entire steps that make up the methodology that is used in this research for experimental and result evaluation. The overall framework consists of five main steps which are, prepare requirements, requirements preprocessing and experimentation, and enhance AODV by caching mechanism and result and evaluation.

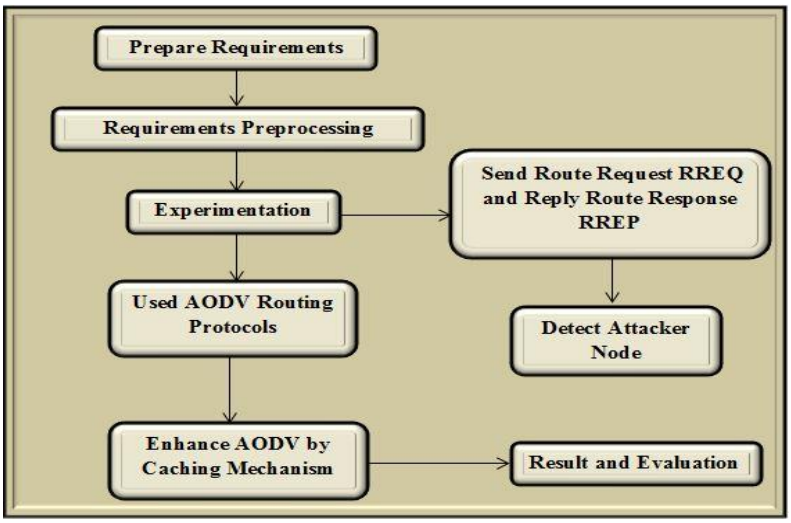

Fig. 1 Methodology Overall.

5. Experimental and Result Evaluation

Implement AODV protocol which it is one of the most popular routing protocol like DSR protocol used NS2 simulator via two scenarios under test (AODV protocol without malicious attack – a black hole attack, AODV protocol with malicious attack) by used intrusion detection and prevention mechanism. We used NS2 simulator toolkit to prepare experimentation to as enhanced AODV protocol for detection and prevention of black hole attack in mobile ad hoc networks. The experiments are conducted on different measurement are throughput, packet delay, and packet loss to find out the best accurate results.

5.1 Implementation

The experimental is done by NS2 simulator, which is a Network tool. In order to get accurate results from the simulations, we used UDP protocol. We did our research in three scenarios, first, we used AODV without any hacking or malicious in MANET. Then we implemented MANET with a blackhole attack. Finally, we implemented MANET under intrusion detection and prevention solution using RREP Caching Mechanism [24].

5.2 Implementation Plan

- Twenty nodes were used to form the MANET. Each of which is all mobile nodes.
- Detect the location of all nodes. Select source and destination.

- Then, the source node will send the route request RREQ to all nearest node to reach the Destination and the destination will send the route response RREP to all nearest node to reach the Source.
- During the RREQ and RREP, the attacker node will get the data, but will not transfer it to the next node.
- Find the path between the source and destination.
- We use to select the secure path between the source and destination using an idsAOVD protocol which is using RREP Caching Mechanism.
- Finally, the packets will be transmitted.

We generated Xgraph for Number of Packet in bits vs. routing time which gives us throughput, Xgraph for Number of lost packets vs. time, and Last packet time vs. A number of packets to find delay.

5.3 Requirement and Resources

Table 1 shows software requirements. In Table 2 we represent parameters that we used in the ns2 simulator. Then in Table 3, we illustrate measurements that we find.

Table 1: Software Requirements

Software Equipment	***Type***
Simulator	Ns2.35
Operating System	Ubuntu12.04
Programming Language	TCL, c++, and AWK script

Table 2: Parameters are used

Parameter	***Value***
SIMULATOR	Network Simulator 2
SIMULATION OF NODES	20
INTERFACE TYPE	Phy/WirelessPhy
CHANNEL	Wireless Channel
MAC TYPE	Mac/802_11
QUEUE TYPE	Queue/DropTail/PriQueue
Converge area	750 ×750 m
Mobility model	Random waypoint model
Transmutation and Traffic	UDP –CBR
UDP packet	512 byte

Table 3: Measurements are used

No.	*Measurement*
1.	Throughput
2.	Packet delay
3.	Packet loss

5.4 Results and Analysis

In the first scenario, the previous parameters with normal AODV protocol were used. We started our experiment using AODV routing protocol then initialized 20 nodes, given each node the mobility, create the connections between each two nodes using CBR application over UDP connection, and then implement the result in Xgraph. Figure 2 shows the scenario execution.

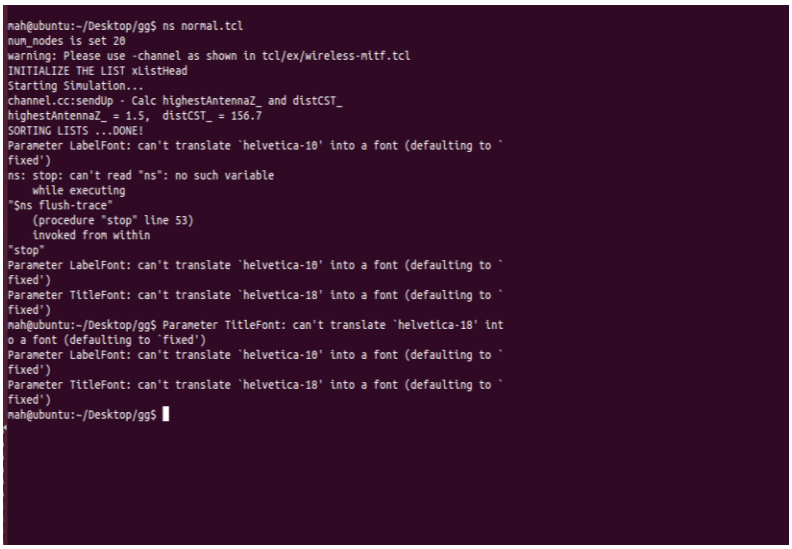

Fig. 2 The scenario execution.

Figure 3 shows the name file for the previous scenario we have 20 circles which implement the mobile nodes. The source node in blue color and the destination node in green color. We can see how nodes are moved and some packets are dropped because we used UDP protocol which is unreliable.

The next three figures will show the results after the first scenario simulation. Figure 4 illustrates the average network throughput in Xgraph using transfer size vs. time. As we see average throughput gives the high result because there is a normal situation.

Figure 5 illustrates the lost packets vs. time. The number of packets lost at the beginning of the simulation is less than the number of packets which are delivered at the end.

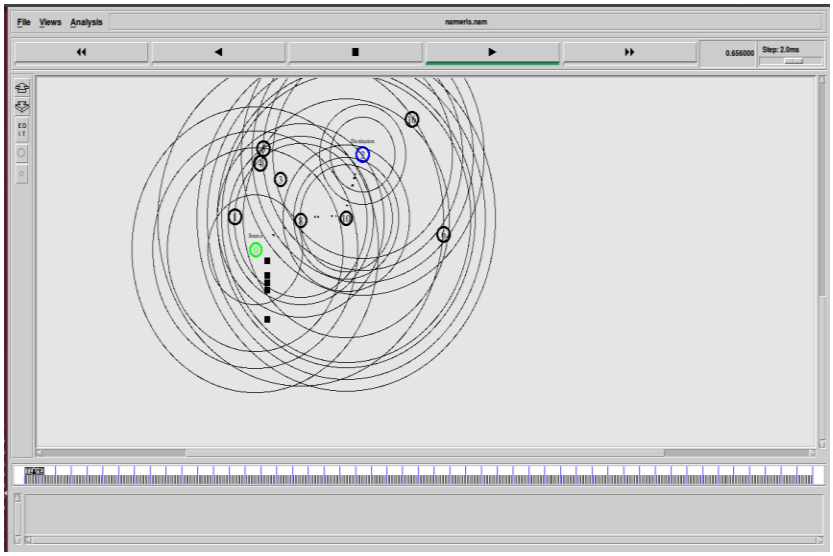

Fig. 3 The nam file for AODV.

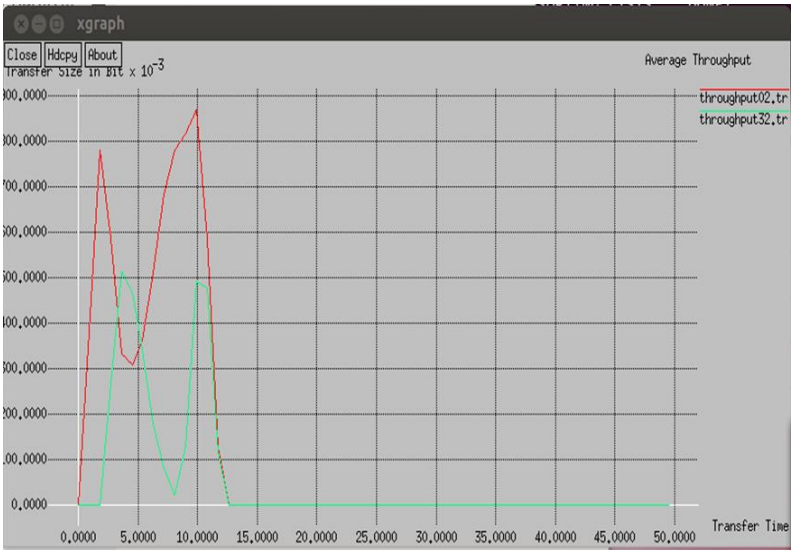

Fig. 4 Normal Graph Model with Average Network Throughput.

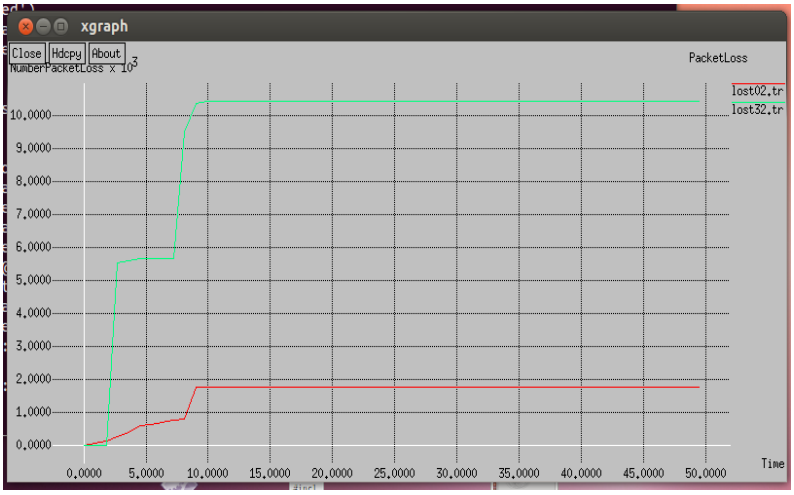

Fig. 5 Packets Loss in Normal Scenario.

Figure 6 shows the packets delay. We used last Packet transfer vs. Number of packets. Because of the using of AODV without any addition or hacking problems, the delay will be decreased.

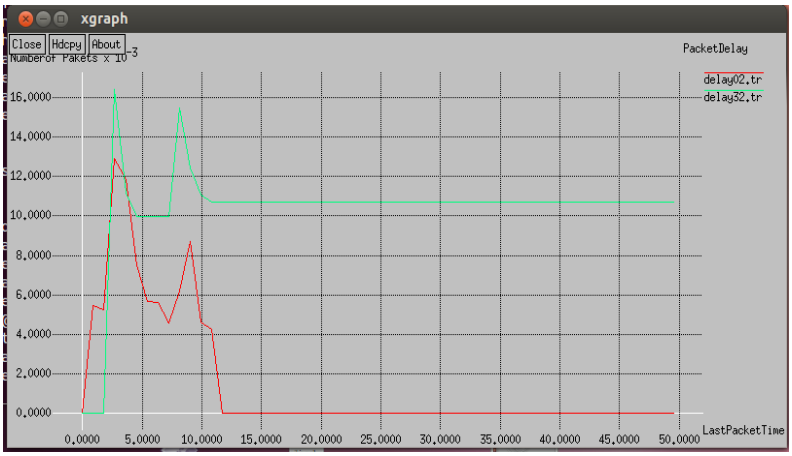

Fig. 6 Packet Delay in Normal Scenario.

Form this scenario we can say MANET here works without any problems in the normal situation. There are no attack conditions.

But in scenario 2 we implemented node 0 as a blackhole node to make an attack in the network by showing a faked shortest bath for other nodes. We simulated these scenarios as in normal situation. But here we used hacked routing protocol in black hole node 0 calls it black hole AODV. So we did some changes in ns2.35 AODV protocol to get this new protocol.

Figure 7 shows the changes in the code for blackhole attack, we add new protocol and call it blackhole AODV. Figure 8 implements nam file for scenario 2. It shows a large amount of Packet lost or drooping when the attacker hacking the Adhoc network, we can see the blackhole node implemented in red color absorb the packets which are come from source implemented in green color without delivering it to destination implemented in blue color.

Figure 9 illustrates the average throughput which is less than normal as it decreases in this scenario. Because sending and receiving mechanism under blackhole attack.

As we see in figure 10, packet loss increases within the time. This refers to some of the packets absorb in the blackhole node without reaching the destination.

In the last figure, 11 represent the delay under blackhole attack increases because a large number of packet loss as the blackhole node absorb it.

Fig. 7 The code for the blackhole attack.

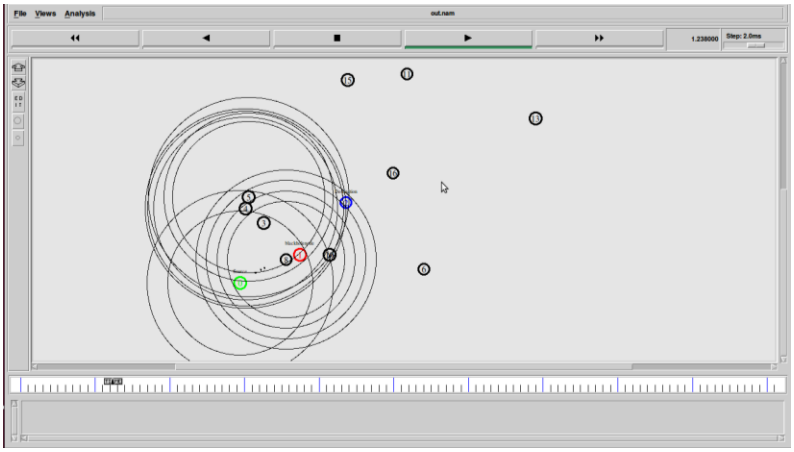

Fig. 8 nam file under Blackhole attack.

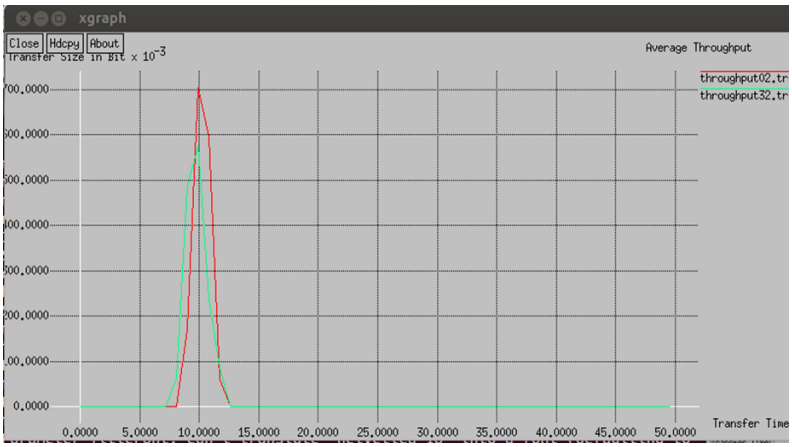

Fig. 9 Average Throughput under Blackhole attack

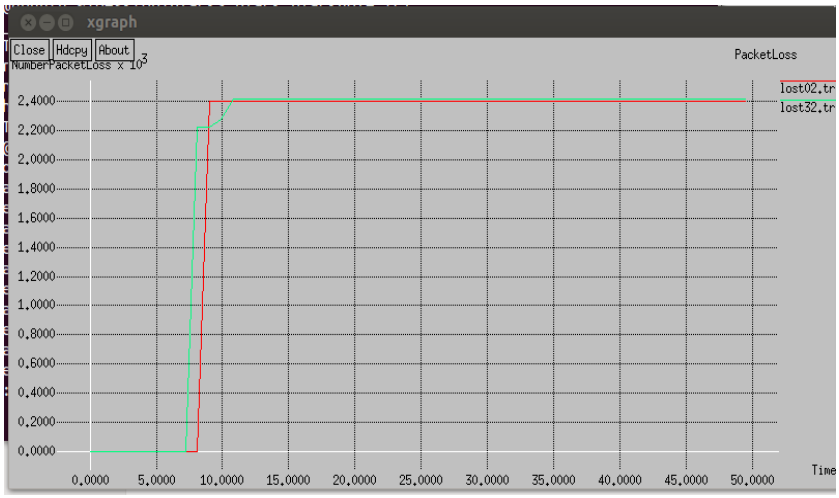

Fig. 10 Packet loss Under Blackhole Attack

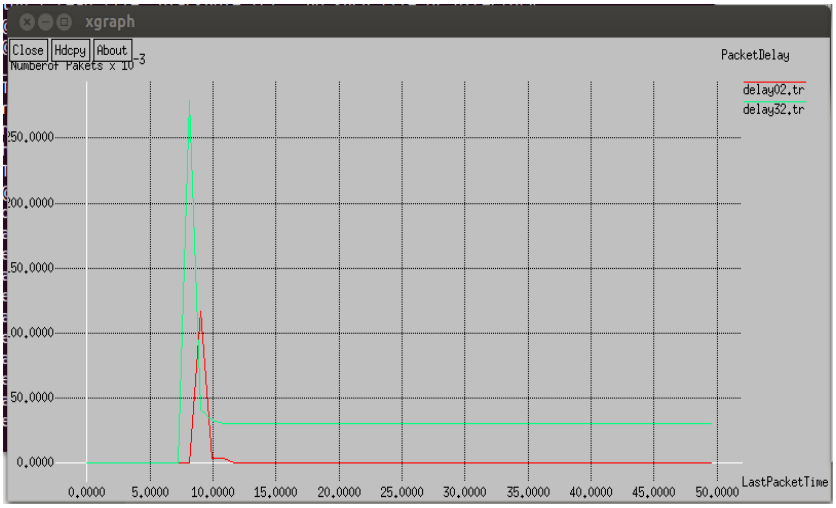

Fig. 11 Delay Under Blockhole Attack.

In scenario 3 we changed and enhanced AODV routing protocol to detect and prevent intrusion and the malicious node which causes attacks and hacking the network so we used a chacing mechanism. We displayed this in idsAODV, ids stands for (intrusion detection Solution).

Figure 12 shows num file after using idsAODV, this figure shows that although we have blackhole node in red color but packets can deliver from the source to destination. Figure 13, figure 14 and figure 15, respectively illustrate that average throughput increase, packet loss decrease, and delay decrease too.

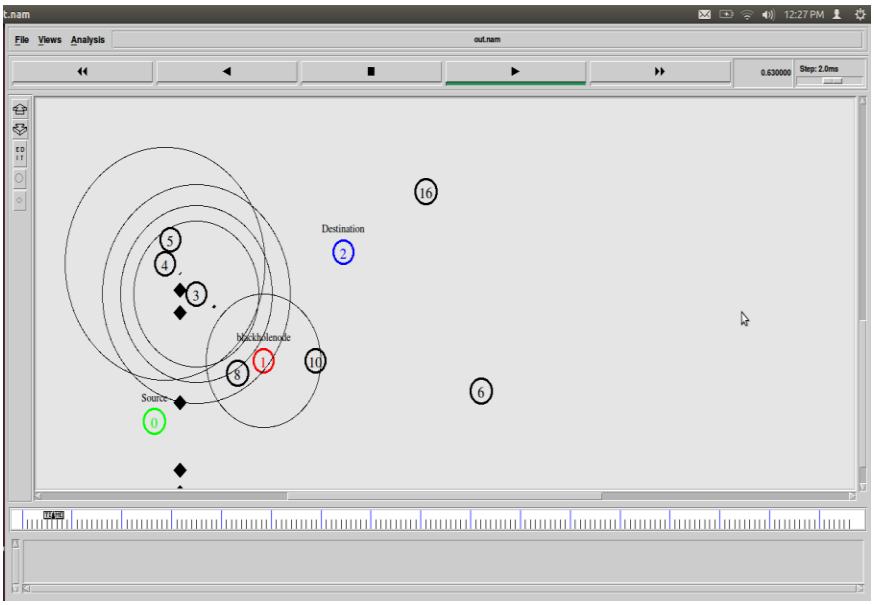

Fig. 12 Num file idsAODV.

In the next three figures we used and add now protocol to ns2.35, this process needs to add some files to the simulator and update our program.

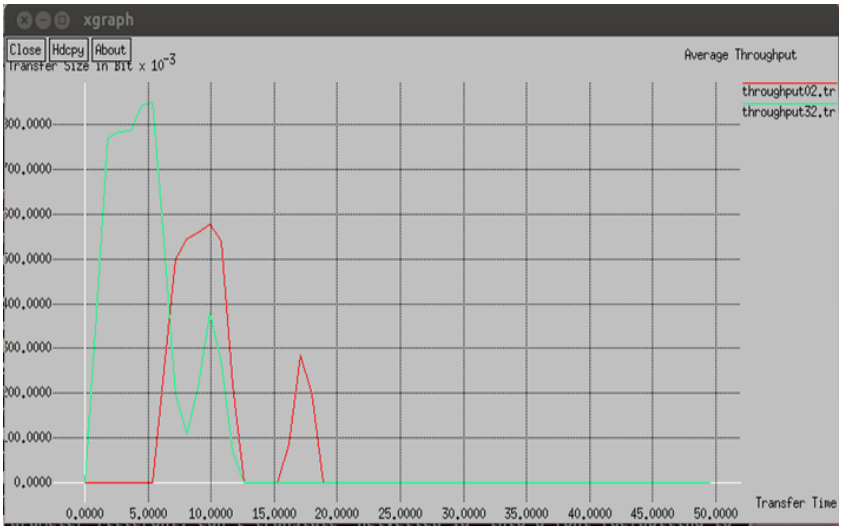

Fig. 13 Average Throughput with idsAODV.

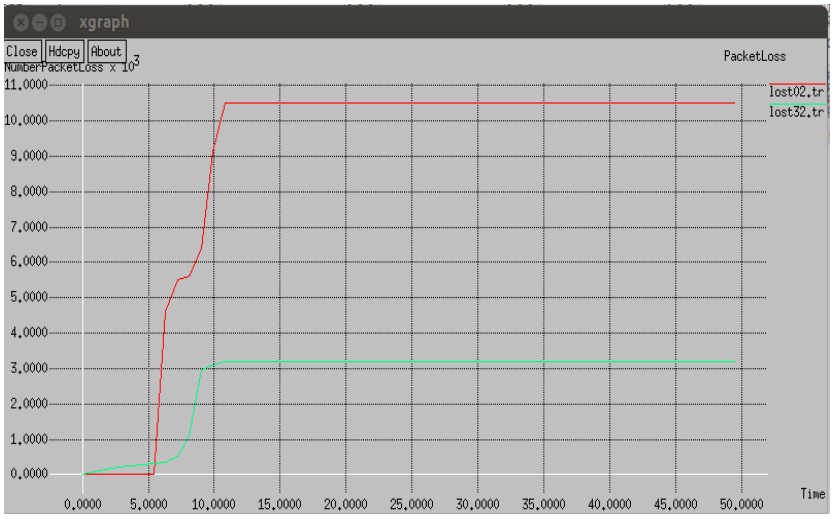

Fig. 14 Packet loss with using idsAODV.

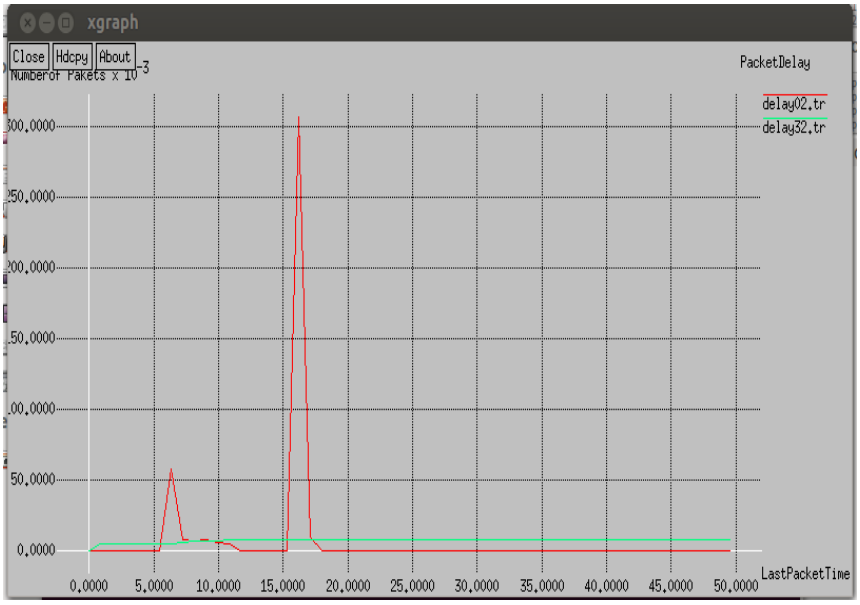

Fig. 15 Packet Delay with using idsAODV

A comparison between these three protocols or mechanisms through using average throughput is shown in figure 16. From this figure, we can see throughput increase and decrease for three protocols or scenarios. But the average throughput for each protocol. Illustrate it in Table 4. Which represent that an intrusion detection solution idsAODV come in between more than blackhole AODV, and less than normal AODV.

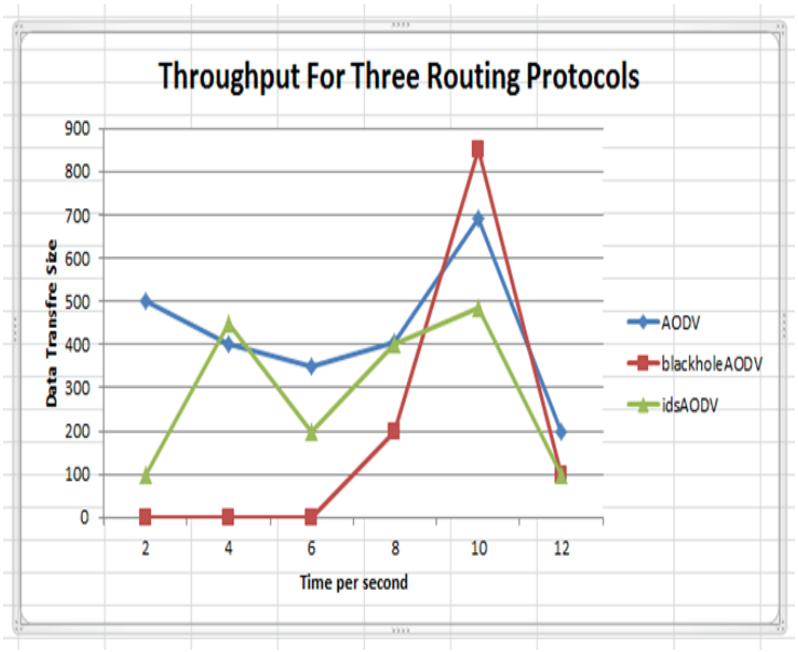

Fig. 16 Throughput Vs Time per second.

Table 4: Average Throughput for protocols

Protocol	*Average Throughput*
AODV	424
blackholeAODV	192
idsAODV	289

6. Conclusions and Future Works

In this research, we studied the enhanced AODV protocol for routing in MANETs to detect and prevent of black hole attack via NS2 simulator by overview the DSR protocol, AODV protocol, sinkhole attack and black hole attack.

Then we do the comparison among two scenarios with enhanced AODV protocol by used cache mechanism to find out the best accurate result of the new route and thus efficiently detects the black hole behavior of the nodes and isolates them quickly. In terms of measurement evaluation, results show that enhanced AODV protocol achieves the highest accuracy and best performance evaluation results than blackholeAODV, but it gives less accuracy and bad performance evaluation than normal AODV.

As a future work, we aim to update a new protocol called “idsAODV” protocol to find out the best accurate and performance results for detect and prevent attack more than current AODV routing protocol.

References

[1] Charu Sharma, Jaspreet Kaur, "Simulative Analysis of AODV Routing Protocol Of MANET Using OPNET Modeler 14.0”, International Research Journal of Engineering and Technology (IRJET), Volume: 02 Issue: 03 | June-2015.

[2] C. Karlof, and D. Wagner, "Secure routing in sensor networks: attacks and countermeasures", Proceedings of the 1st IEEE Workshop on Sensor Network protocols and Applications, pp. 1-15, May 2003.

[3] DEVI. P, KANNAMMAL. A, “A PRAGMATIC APPROACH TO SECURE DSR PROTOCOL FROM SINKHOLE ATTACK IN AD HOC ENVIRONMENT", Journal of Theoretical and Applied Information Technology, 31st August 2014. Vol. 66 No.3

[4] Harshavardhan Kayarkar, "A Survey on Security Issues in Ad Hoc Routing Protocols and their Mitigation Techniques", International Journal of Advanced Networking and Application, Vol. 03, Issue 05, pp. 1338-1351, March-April, 2012.

[5] H. C. Tseng, B. J. Culpepper, "Sinkhole intrusion in mobile ad hoc networks: The problem and some detection indicators", Computers & Security, vol.24, 561-570, 2005.

[6] H. Deng, W. Li, and D. P. Agrawal, "Routing security in wireless ad hoc networks", IEEE Communications Magazine vol. 40 no. 10, pp. 70-75, Oct. 2002.

[7] Johnson DB, Maltz DA, Hu YC.The dynamic source routing protocol for the mobile ad-hoc network (DSR), IETF internet-draft (work in progress); July 2004.

[8] Kim, G., Han, Y. and Kim, S. (2010) 'A cooperative sinkhole detection method for mobile ad hoc networks', AEU – International Journal of Electronics and Communications, Vol. 64, No. 5, pp.390–397, Elsevier

[9] Marchang, N., and Datta, R. (2008) 'Collaborative techniques for intrusion detection in mobile ad-hoc networks', Ad Hoc Networks, Vol. 6, No. 4, pp.508–523, Elsevier.

[10] Mohammed Ashfaq Hussain, Dr. A. Francis Saviour Devaraj, "Upshot of Sinkhole Attack in DSR Routing Protocol Based MANET", International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 3, Issue 2, March -April 2013, pp.1737-1741.

[11] Perkins CE, Royer EM, Das SR. Ad-hoc on-demand distance vector (AODV) routing, IETF internet draft. MANET Working Group

[12] P.G. Argyroudis and D. O'Mahony, "Secure Routing for mobile ad hoc networks", IEEE Communications Surveys & Tutorials, third quarter 2005, Vol. 7, no3, 2005 258 Authorized licensed use limited to University of Allahabad.

[13] P. Papadimitratos and Z. Haas, "Securing the Internet routing infrastructure", IEEE Communications Magazine, vol. 40, no. 10, pp 60-68, Oct 2002.

[14] Rajeshwar L. Balla, Venugopal Kotoju, "Sinkhole Attack detection and prevention in MANET & Improving the performance of AODV Protocol", COMPUSOFT, An international journal of advanced computer technology, 2 (7), July-2013 (Volume-II, Issue-VII).

[15] R.Bhairavi, A.Santhiya," Intelligent Scheme for Defending Against Black-Hole Attacks by Malicious Nodes in Dynamic Source Routing Protocol", International Journal of Modern Electronics and Communication Engineering (IJMECE) ISSN: 2321-2152 Volume No.-4, Issue No.-2, March 2016.

[16] Shim, W., Kim, G. and Kim, S. (2010) 'A distributed sinkhole detection method using cluster analysis', Expert Systems with Applications, Vol. 37, No. 12, pp.8486–8491, Elsevier.

[17] S. Buchegger and J.-Y. Le Boudec, "Performance Analysis of the CONFIDANT Protocol: Cooperation of Nodes, Fairness in Dynamic Ad-Hoc Networks," Proceedings of MobiHoc, June 2002.

[18] S. Lee, B. Han, and M. Shin, "Robust routing in wireless ad hoc networks," Proceedings of 31st ICPP Workshops, pp. 73–78, Aug. 2002

[19] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," Proceeding of 6th Annual International Conference on Mobile Computing and Network, Boston, MA, pp. 255–265, 2000

[20] Tirthraj Rai1 & Ashish Jain2, "Secure Routing in Mobile Ad hoc Network", International Journal of Computer Science & Communication Vol. 1, No. 1, January-June 2010, pp. 125-127

[21] Tseng, H.C., and Culpepper, B.J. (2005) 'Sinkhole intrusion in mobile ad hoc networks: the problem and some detection indicators', Computers & Security, Vol. 24, No. 7, pp.561–570, Elsevier.

[22] Manel Guerrero Zapata, N. Asokan. "Securing Ad hoc Routing Protocols".

[23] Nisha Puri, Simranjit Kaur, Sandeep Kumar Arora. "Performance Analysis of Mobile Ad Hoc Network in the Presence of Sink Hole attack". International Journal of Scientific Engineering and Research (IJSER). Volume 1 Issue 3, November 2013.

[24] Semih Dokurer, Y. M. Erten, Can Erkin Acar, " Performance analysis of ad-hoc networks under black hole attacks". Department of Computer Engineering, Southeastcon Journal. 2007.

[25] Monika, Denial of Service Attacks in Wireless Mesh Networks, Monika /(IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 3 (3), 2012,4516-4522.

Author's biography

Sherin Hijazi Sherin obtained her Bc in Management Information Systems from An-Najah University in 2005, then she completed her study in the master of Information Technology and Computer Science from Al Yarmouk University in 2012.She has 10 years' experiences in computer information system and programming. She worked in Palestine Technical University, Tulkarem, Palestine as a lecturer, between 2007 until now. Now she is a Ph.D. student in The University of Jordan. She interests in network security, Data Base, and algorithms.

Mahmoud Moshref obtained his Bc in computer Science from An-Najah University in 2003, then he completed his study in a master of computing from birzeit University in 2012. he worked at Palestine Technical University, Tulkarem, Palestine as a part-time lecturer. Now he is a Ph.D. student in The University of Jordan. He interests in networks, network security, and an internet of things, and RFID system fields.

Saleh Al-Sharaeh Ph. D in Computer Engineering. Area of specialization: Parallel and Distributed Computing. Bell Labs Silver Award for contribution to the development of wireless features for PHS development. Bell Labs appreciations award for the CAMEL feature development. A key figure in the foundation of Lucent China in Qingdao. A co-founder and the Dean of Faculty of Information Technology and Systems and the Faculty of Business and Finance in Aqaba, Jordan. Served as a member of various academic committees related to the development of Ph.D., MS, BSc Programs in computer science and Engineering curriculum, the Quality Assurance Committee, under the auspices of the Ministry of Higher Education of Jordan. Worked with Al-Faisal group in developing different programs for teaching training of the Ministry of Education staff in applying various software packages for the betterment of the traditional and eLearning More than forty-five published research papers/articles in different areas of Wireless Networking, Wireless Sensor Networks, Mobile Computing, Distributed Computing, Space Physics, and Protocol Routing Engineering.