ISSN 2047-3338

Comparative Study of AODV and OLSR Protocols in MANET Network under the Impact of Black Hole Attack

Karim Shamekh[1] and Essam Elden Elfakharany[2]

[1]Computer Science Department, High Technology Institute, 10th of Ramadan, Egypt
[2]Arab Academy for Science, Technology and Maritime, Cairo, Egypt
[1]Karim_Shamekh@hotmail.com, [2]essam.fakharany@gmail.com

***Abstract*— Wireless Networks are raising fast today, as users wants to have wireless network anywhere they are located. Mobile Ad-Hoc Networks also named as MANETs became one of the most well-liked wireless networks because it is easy to be deployed and due to its dynamic nature. Existence of MANETs created a new set of demands to be implemented and to provide efficient better end-to-end delay communication. MANET is a collection of mobile nodes that dynamically form a temporary network without the aid of any established infrastructure or centralized administration. It has many numbers of applications mainly in the areas of Sensor Networks (SN), medical military and rescue operations. MANETs works on TCP/IP structure in order to provide the communication between the work stations. Work stations are mobile, that is why the traditional TCP/IP model needs to be modified to compensate the MANETs mobility and provide efficient functionality of the network. Based on that routing protocol, ad-hoc networks are classified into two main categories; Proactive routing protocol such as Optimized Link State Routing (OLSR) and Reactive Routing Protocol such as Ad-Hoc on Demand Distance Vector (ADOV). Despite of routing protocols, the nature of such networks increased threat of attacks while MANETs must have a secure way for transmission and communication which is quite challenging and vital issue. One of the attacks is the black hole attack.**

***Index Terms*— MANET, Ad-Hoc on Demand Routing Protocol (AODV), Open Link State Routing (OLSR) and Black Hole Attack**

I. INTRODUCTION

WIRELESS network is the network of mobile computer nodes or stations that are not physically wired. The main advantage of this is communicating with rest of the world while being mobile. The disadvantage is their limited bandwidth, memory, processing capabilities and open medium. Two basic system models are fixed backbone wireless system and Wireless Mobile Ad hoc Network (MANET). An ad hoc network is a collection of nodes that do not rely on a predefined infrastructure to keep the network connected. So the functioning of Ad-hoc networks is dependent on the trust and co-operation between nodes. MANET is widely used in military purpose, disaster area, personal area network and so on [1]. Nodes help each other in conveying information about the topology of the network and share the responsibility of managing the network. Hence in addition to acting as hosts, each mobile node does the function of routing and relaying messages for other mobile nodes [2].

In these networks, besides acting as a host, each node also acts as a router and forwards packets to the correct node in the network once a route is established. To support this connectivity nodes use routing protocols such as AODV or OLSR. Wireless ad-hoc networks are usually susceptible to different security threats and black hole attack is one of these. In our study, we simulated black hole attacks in wireless ad-hoc networks and evaluated their effects on the network performance.

The aim of this work is to provide a comparative analysis of black hole attack in MANET using both AODV, OLSR in order to provide an insight of which protocol is more vulnerable to black hole attack than the other, and how much impact does this attack will affect the two protocols. The performance analysis will be evaluated with respect to throughput, end-to-end delay and network load using OPNET modeler simulator.

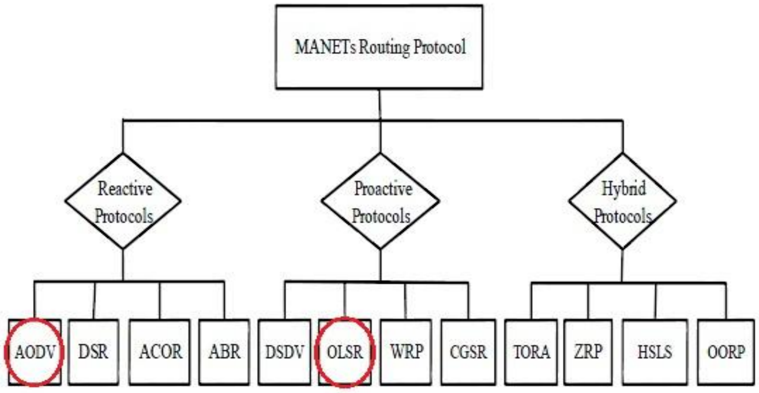

Figure 1: Classification of MANETs Routing Protocols

II. ROUTING PROTOCOLS IN MANET

These are classified into three different categories as shown in Figure 1:

A) Reactive Protocols

Reactive methods are based on demand for data transmission. Routes between hosts are determined only when they are explicitly needed to forward packets. Reactive methods are also called on-demand methods. They can significantly reduce routing overhead when the traffic is lightweight and the topology changes less dramatically, since they do not need to update route information periodically and do not need to find and maintain routes on which there is no traffic. Ad-hoc On-demand Distance Vector (AODV) is an example of Reactive Protocol.

1) AODV Protocol

Ad hoc On-demand Distance Vector Routing (AODV) is a novel algorithm for the operation of ad hoc networks [3]. Each mobile node operates as a specialized router and routes are obtained as needed i.e. on-demand with little or no reliance on periodic advertisements. The new routing algorithm is quite suitable for a dynamic self-starting network as required by users wishing to utilize ad hoc networks. AODV provides loop free routes even while repairing broken links. Because the protocol does not require global periodic routing advertisements, the demand on the overall bandwidth available to the mobile nodes is substantially less than in those protocols that do necessitate such advertisements.

AODV can be called as a pure on-demand route acquisition system, in this nodes do not lie on active paths neither maintain any routing information nor participate in any periodic routing table exchanges. Further, a node does not have to discover and maintain a route to another node until it needs to communicate. To maintain the most recent routing information between nodes the concept of destination sequence numbering will be used. Each ad hoc node maintains a monotonically increasing sequence number counter which is used to supersede stale cached routes.

The advantage of AODV is that it creates routes only on demand, which greatly reduces the periodic control message overhead associated with proactive routing protocols. The disadvantage is that there is route setup latency when a new route is needed, because ADOV queues data packets while discovering new routes and the queued packets are sent out only when new routes are found. This situation causes throughput loss in high mobility scenarios, because the packets get dropped quickly due to unstable route selection.

B) Proactive Protocols

Proactive methods maintain routes to all nodes, including nodes to which no packets are sent. Such methods react to topology changes, even if no traffic is affected by the changes. They are also called table-driven methods. Thus using a proactive protocol, a node is immediately able to route (or drop) a packet. Optimized Link State Routing Protocol (OLSR) is an example of Proactive Protocol.

1) OLSR Protocol

OLSR is a proactive or table driven, link-state routing protocol [4]. Link-state routing algorithms choose best route by determining various characteristics like link load, delay, bandwidth etc. Link-state routes are more reliable, stable and accurate in calculating best route and more complicated than hop count. To update topological information in each node, periodic message is broadcast over the network. Multipoint relays are used to facilitate efficient flooding of control message in the network. Route calculations are done by multipoint relays to form the rout from a given node to any destination in the network. The OLSR protocol is developed to work independently from other protocols. Conceptually, OLSR contain three generic elements: a mechanism for neighbor sensing, a mechanism for efficient flooding of control traffic, and a specification of how to select and diffuse sufficient topological information in the network in order to prove optimal routes [5], [6].

In OLSR, neighbor nodes related information are gathered with HELLO messages which are send over network periodically [7]. These HELLO messages detect changes in neighbor nodes and related information such as interface address, type of link symmetric, asymmetric or lost and list of neighbors known to the node. Each node update and maintain an information set, describing the neighbor and two-hop neighbor periodically after some time.

The idea of multipoint relays is to minimize the overhead of flooding message in the network by reducing redundant retransmission in the same region. In MPR (Multi Point Relay) a node which is selected by its one hop neighbor to retransmit all the broadcast messages that it receive from other node, provided that the message is not a duplicate, and that the time to live field of the message is greater than one [7]. In OLSR protocol, Multi Point Relays use of HELLO message to find its one hop neighbor and its two hop neighbors through their response. Each node has a Multi-Point Relay selection set, which indicates, which node acts as a MPR. Message is forward after the node gets new broadcast message and message sender’s interface address in the MPR Selector Set. MPR Selector Set is update continuously using HELLO message which are periodic because neighbor nodes is called of dynamic nature of MANET.

Topology Control messages are diffused with the purpose of providing each node in the network with sufficient link-state information to allow route calculation [7]. TC messages are broadcast periodically by a node. Like HELLO messages with these TC messages the topological information are diffused over the entire network. A minimum criteria for the node is to send at least the link of its MPR Selector Set [5], [8].

The advantage of OLSR is that it reduces control information and efficiently minimizes broadcast traffic bandwidth usage. Although OLSR provides a path from source to destination, it is not necessarily the shortest path, because every route involves forwarding through a MPR node. A further disadvantage is that OLSR also has routing delays and bandwidth overhead at the MPR nodes as they act as localized forwarding routers.

C) Hybrid Protocols

Hybrid routing protocol combines the advantages of both proactive and reactive routing protocols, the routing is initially established with some proactively prospected routes and then serves the demand from additionally activated nodes through reactive flooding.

III. BLACKHOLE ATTACK

A black hole attack is [9] used by a malicious node which makes all the traffic travel through it by claiming to have the shortest route to all other nodes in the network. Then, instead of forwarding the packets, the malicious node simply drops it. In a blackhole attack, a malicious node impersonates a destination node by sending a spoofed root reply packet to a source node that initiates a route discovery. The source node *traffic* can be deprived by malicious node. A variant of this black hole is the gray hole, attack, which selectively transmits some packets and drops others. Other attacks towards an adhoc network include partitioning and replay attacks.

IV. SIMULATION SETUP

We have conducted extensive simulation study to evaluate the performance of different mobile ad hoc networks routing protocols reactive AODV and proactive OLSR. Three types of network scenarios are designed: AODV, OLSR and blackhole attack using both protocols .We used OPNET 14.5 simulator to carry out simulation study [10], which is used for network modeling and simulation results as it has fastest event simulation engine.

Mobility Model: Mobile nodes in the simulation area move according to random waypoint model [12].

Radio Network Interfaces: The physical radio characteristics of each mobile node's network interface, such as the antenna gain, transmit power, and receiver sensitivity, were chosen to approximate the direct sequence spread spectrum radio [13].

Media Access Control: The distribution coordination function (DCF) of IEEE 802.1 1b was used for underlying

MAC layer [13]. Default values are used for MAC layer parameters.

Network Traffic: In order to compare simulation results for performance of each routing protocol, communication model used for network traffic sources is FTP.

Traffic Configuration: For traffic configuration, all experiments have one data flow between a source node to a sink node consisting of TCP file transfer session and TCP transmits with the highest achievable rate. TCP is used to study the effect of congestion control and reliable delivery [9].

V. SIMULATION ENVIRONMENT

It consists of 50 wireless nodes which were placed uniformly and forming an ad hoc network, moving about over a 500 X 500 meters area for 10800 seconds of simulated time. All mobile nodes in the network are configured to run AODV and OLSR and changing the seed for the random number generator used for node placement. The simulation parameters are summarized in Table 1.

Table 1: Simulation Parameters

SIMULATION PARAMETERS	
Simulator	OPNET Modeler 14.5
Examined protocols	AODV and OLSR
Simulation time	10800 seconds
Simulation area	500 x 500 meters
Number of Nodes	50
Traffic Type	TCP
Performance Parameter	Routing Traffic Sent, Routing Traffic Received, Delay, Load and Throughput
Transmission Range	300 meters
Number of seed	50,100,200,300 and 400
Mobility (m/s)	10 meter/second
Packet size (bits)	0.005
Transmit Power(W)	11 Mbps
Date Rate (Mbps)	Random waypoint
Mobility Model	

Below in Figure 2 and Figure 3 it is showing the simulation environment of the two scenario having 50 mobile nodes for AODV and OLSR routing protocol.

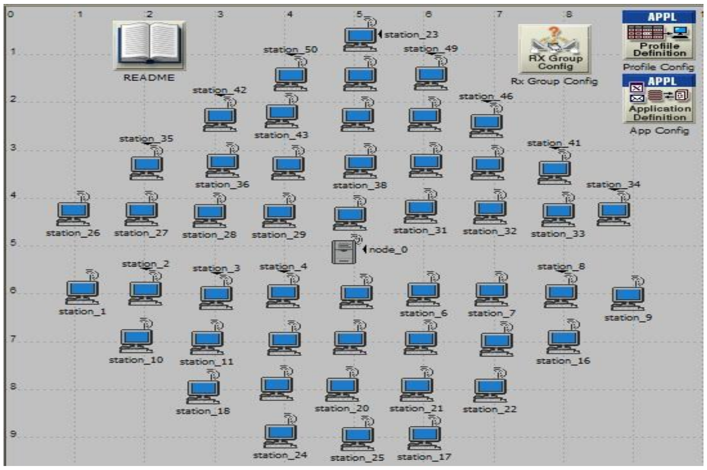

Figure 2: AODV network

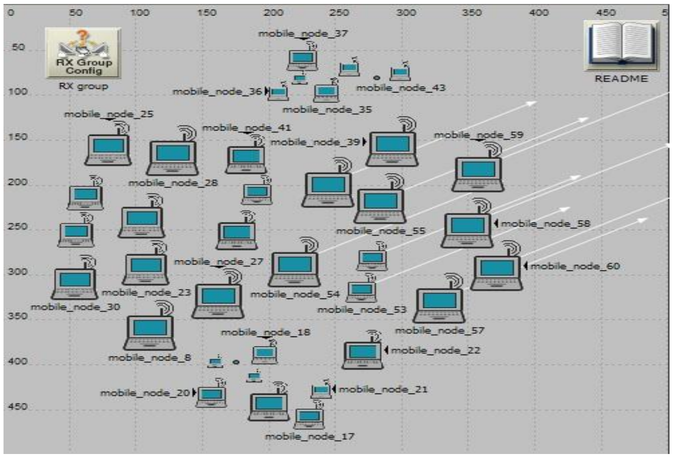

Figure 3: OLSR network

Figure 4 it is showing the simulation environment of the third scenario having 50 mobile nodes in MANET and the attack is done by black hole for both protocols AODV and OLSR. It is consists of 4 work domain, each domain contain 12 node (10 of them standard node as Figure 5 and Figure 2 of them act as a malicious node as Figure 6.

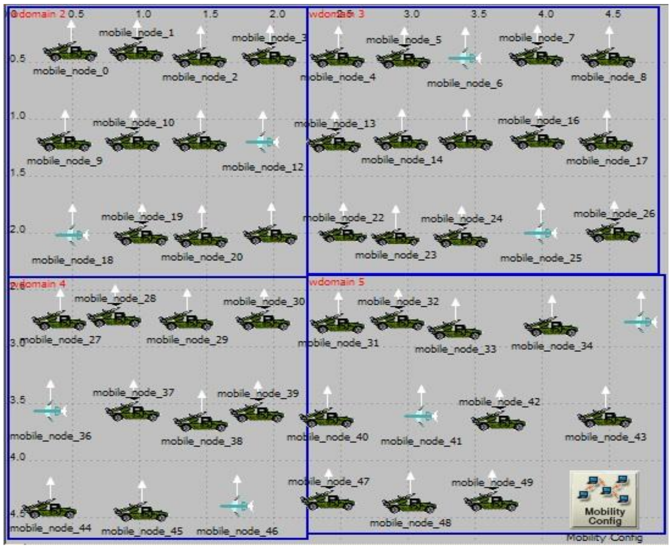

Figure 4: Black hole attack

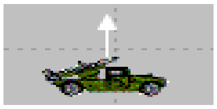

Figure 5: Standard node

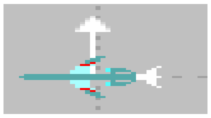

Figure 6: Malicious node

VI. METRICS

In our simulation study, performance comparisons are made using following parameters:

Routing Traffic Sent (bits/sec) is the amount of routing traffic sent in bits/sec in the entire network

Routing Traffic Received (bits/sec) is the amount of routing traffic received in bits/sec in the entire network.

Delay (sec) is the end to end delay of all the packets received by the wireless LAN MACs of all WLAN nodes in the network and forwarded to the higher layer.

Load (bits/sec) is the total load (in bits/sec) submitted to wireless LAN layers by all higher layers in all WLAN nodes of the network.

Throughput (bits/sec) is the total number of bits (in bits/sec) forwarded from wireless LAN layers to higher layers in all WLAN nodes of the network.

VII. RESULTS AND GRAPHS

Figure 7 – Figure 11 comparing the results obtained for both protocols AODV and OLSR from the simulation based on the Routing Traffic Sent (bits/sec), Routing Traffic Received (bits/sec), Delay (sec), Load (bits/sec) and the throughput.

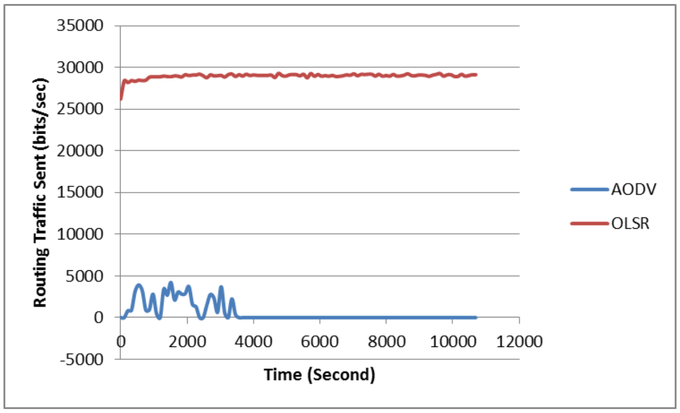

Figure 7: Routing Traffic Sent (bits/sec)

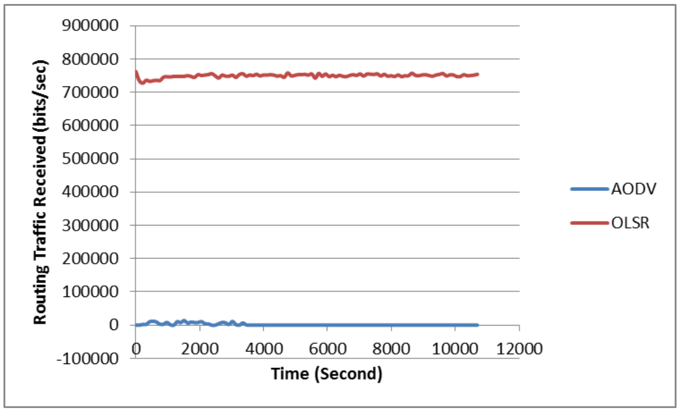

Figure 8: Routing Traffic Received (bits/sec)

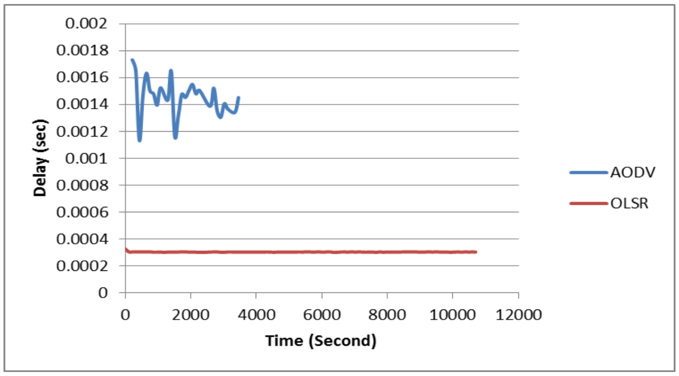

Figure 9: Delay (sec)

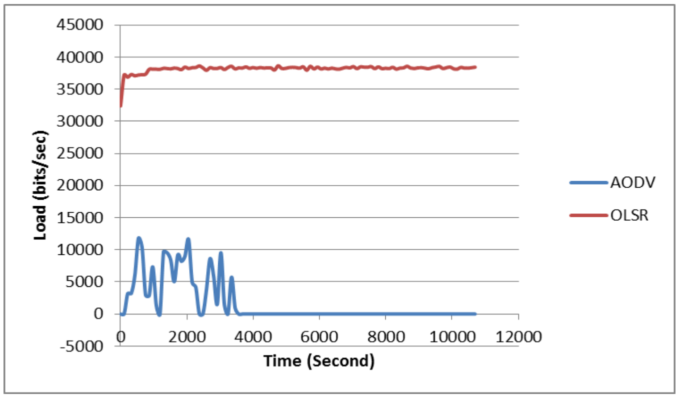

Figure 10: Load (bits/sec)

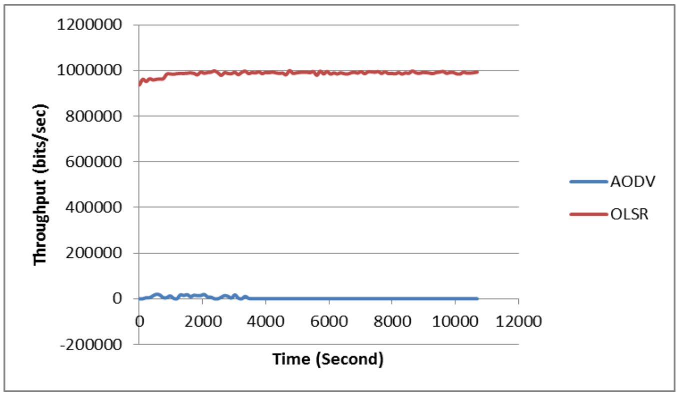

Figure 11: Throughput (bits/sec)

Figure 12, Figure 13 and Figure 14 analyzing the effect of the black hole attack in both the AODV and OLSR protocols in terms of delay, load and throughput.

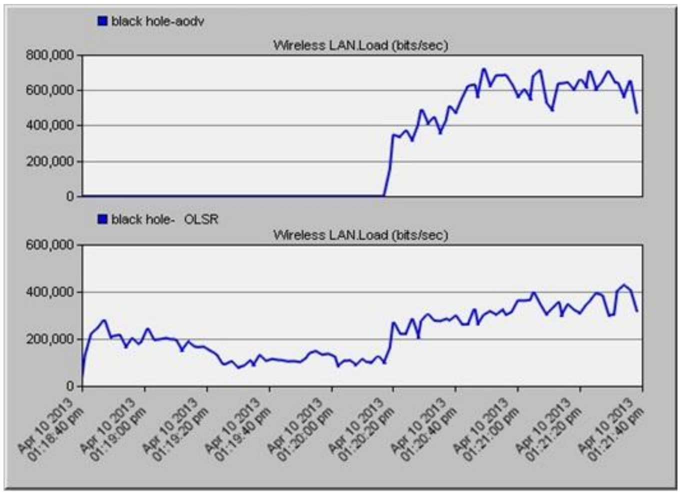

Figure 12: Wireless LAN delay (sec) in black hole attack

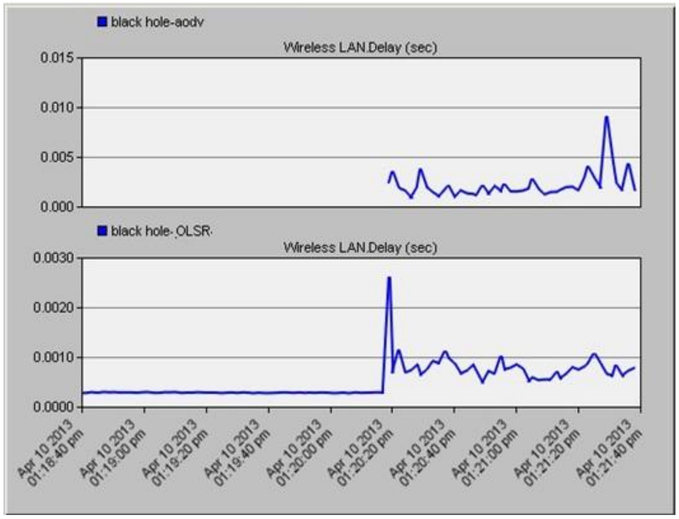

Figure 13: Total load (bits/sec) in black hole attack

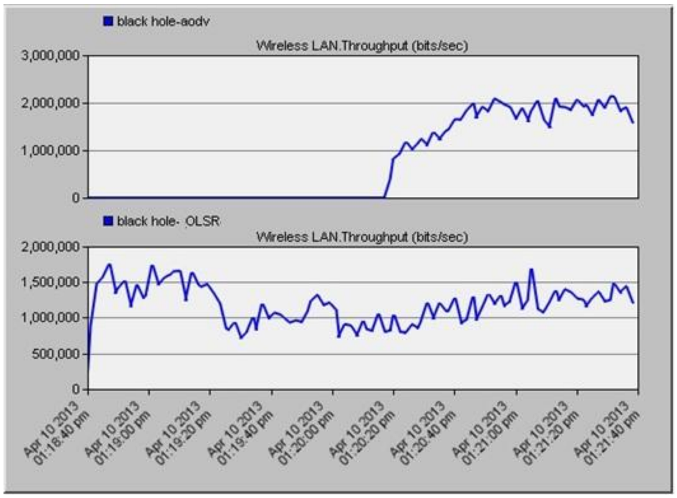

Figure 14: Throughput in wireless LAN (bits/sec) in black hole attack

VIII. CONCLUSION

The mobile nodes' mobility management is key area since mobility causes route change and frequent changes in network topology, therefore effective routing has to be performed immediately. This paper makes contributions in two areas. Firstly, this paper proposed a comparative analysis of the performance of reactive ad hoc on demand distance vector protocol and proactive optimized link state routing protocol in mobile ad hoc networks. Secondly, Black Hole attack is simulated and its impact on the MANETs is analyzed with three performing matrices i.e. End-to-End delay, Network Load and Throughput. The results obtained from simulation are analyzed deeply in order to draw the final conclusion. Different mitigation plans are studied in detail and we come up with mitigation plan that suits best to eliminate Black Hole attack. The impact of Black Hole attack on the MANETs we found that AODV is much more affected by the attack as compared to OLSR. From our research we conclude that AODV protocol is more vulnerable to Black Hole attack than that of OLSR protocol regarding to various measured parameters so we present that OLSR is the most appreciate to works under Attacks.

IX. FUTURE WORK

In future, the performances of other reactive and proactive protocols under other security attack [14] can be evaluated, to make these results more justified and scope of suitable detection and prevention techniques [15], [16], [17] will always be there.

REFERENCES

[1]. Burbank JL, Chimento PF, Haberman BK, Kasch WT (2009) Key Challenges of Military Tactical Networking and the Elusive Promise of MANET Technology. IEEE Communication Magazine 44(11):39–45.

[2]. Latha Tamilselvan, Dr.V Sankaranarayanan, “Prevention of Blackhole Attack in MANET”. The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications (AusWireless 2007) India, 2007 IEEE

[3]. C. E. Perkins, E. M. Royer, I. D. Chakeres, “Ad hoc On-Demand Distance Vector (AODV) Routing Protocol”, draft-perkins-manet-aodvbis-00.txt, October 2003.

[4]. T. Clausen, C. Dearlove, P. Jacquet, “The Optimized Link State Routing Protocol version 2”, MANET Working Group, [Online] Available:http://www.ietf.org/internet-drafts/draft-ietf-manet-olsrv2-05.txt, February 2008.

[5]. T.H. Clausen, ”The optimized link state routing protocol evaluating through experiments and simulation” mindpass center for distributed system,Aalborg university ,Denmark

[6]. Kuldeep Vats, “Simulation and performance analysis of OLSR routing protocol using OPNET” IJARCSSE Volume 2, Issue 2, February 2012.

[7]. T. Clause, “Optimized link state routing protocol”, i.etf.org/rfc3626.txt,oct. 2003

[8]. P. Jacquet, ”Optimized Link State routing protocol”,draft –ieff-olsr-04.txt-work in progress,march 2001.

[9]. Shurman, M.A., Yoo, S.M., Park, S (ACMSE 2004), “Black hole attack in wireless ad hoc networks”, In Proc. of ACM 42nd Southeast Conference.

[10]. Opnet.com (2008), “The OPNET Simulator”, Available: http://www.opnet.com.

[11]. E. Nordstrom, P. Gunningberg, C. Rohner, O. Wibling, "A Comprehensive Comparison of MANET Routing Protocols in Simulation, Emulation and the Real World", Uppsala University, pp. 1-12, 2006.

[12]. H. Pucha, S. M. Das, Y. C. Hu, "The Performance Impact of Traffic Patterns on Routing Protocols in Mobile Ad Hoc Networks", Journal (COMNET), vol. 51(12), pp. 3595-3616, August 2007.

[13]. J. Broch, D. A. Maltz, D. B. Johnson, Y. C. Hu, J. Jetcheva, "A Performance Comparison of Multi-Hop Wireless Ad-Hoc Network Routing Protocols," Proceedings of the 4th ACM/IEEE International Conference on Mobile Computing and Networking MOBICOM'98, pp. 85-97, Texas, October 1998.

[14]. Hu, C. Y., Perrig, A., Johnson, B. D. 2002. SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks. In: IEEE Workshop on Mobile Computing Systems and Applications. (2002), 3-13.

[15]. Alfawar, M. Z., Alzoubi, S. 2009. A Proposed Security Subsystem for Ad Hoc Wireless Networks. In: International forum on Computer Science technology and Applications. (2009), 1-4.

[16]. Hu, C. Y., Perrig, A., Johnson, B. D. Aridane. 2002. A Secure On-Demand Routing Protocol for Ad Hoc Networks. In: Proceeding of the 8th Annual International Conference on Mobile Computing and Networking. Atlanta, Georgia, USA (2002).

[17]. Papadimitratos, P., Haas, J. Z. 2003. Secure Link State Routing for Mobile Ad Hoc Networks. In: Proceedings of IEEE Workshop on Security and Assurance in Ad Hoc Networks in Conjunction with the 2003 International Symposium on Applications and the Internet.. Orlando, FL (2003), 1-7.

Karim Shamekh received the B.S. degree in Computer Science from High Technology Institute in 2006. During 2007-2012, He is preparing the M.S. degree in Computers and Information Systems from the Arab Academy for Science, Technology and Maritime Transport. His research interests include Mobile Robots Ad Hoc Networks, image processing, security and communication Networks.

Essam-Eldean F. Elfakharany received his PhD degree in Systems Engineering in 1999 from The Ohio State University, He is the chair of Business Information Systems Department at the Arab Academy for Sciences, Technology, and Maritime Transport. He has more than 25 years of experience in Egyptian defense research centers as the manager of IT division of Egyptian air force operational department