Effects of Black Hole Attack on MANET Using Reactive and Proactive Protocols

Irshad Ullah* and Shahzad Anwar
Department of Computer Science, Iqra National University, Hayatabad Phase II
Peshawar, K.P.K 25000, Pakistan

Abstract

Wireless networks are gaining popularity to its peak in the present era and therefore appealing the users for wireless connectivity irrespective of their geographic position. There is an increasing threat of attacks on the Mobile Ad-hoc Networks (MANET). Black hole attack is one of the security threat in which the traffic is redirected to such a node that actually does not exist in the network.

The scope of this paper is to study the effects of Black hole attack in MANET using both Proactive routing protocol (i.e. Optimized Link State Routing (OLSR) and Reactive routing protocol Ad-Hoc On Demand Distance Vector (AODV)). Comparative analysis of Black Hole attack for both protocols is taken into consideration. The impact of Black Hole attack on the performance of MANET is evaluated exploring which protocol is more vulnerable to the attack and it was found that AODV is 10% more vulnerable to Black Hole attack as compared to OLSR. The measurements were taken in the light of throughput, end-to-end delay and network load. Simulation is done in Optimized Network Engineering Tool (OPNET).

Keywords: *MANET, Black Hole, Routing Protocols***.**

1. Introduction

Mobile Ad-Hoc Networks are autonomous and decentralised wireless systems. MANETs consist of mobile nodes that are free in moving in and out in the network. Nodes are the systems or devices (i.e. mobile phone, laptop, personal digital assistance, MP3 player and personal computer) that are participating in the network and are mobile. These nodes can act as host/router or both at the same time [1, 2]. They can form arbitrary topologies depending on their connectivity with each other in the network. These nodes have the ability to configure themselves and due to their self-configuration capability, they can be deployed urgently without the need of any infrastructure. Internet Engineering Task Force (IETF) has MANET working group (WG) that is devoted for developing IP routing protocols. Routing protocols is one of the challenging and interesting research areas. Many routing protocols have been developed for MANETS, i.e. AODV, OLSR, DSR etc. [5, 6, 7 and 8].

Security in Mobile Ad-Hoc Network is the most important concern for the basic functionality of network. The availability of network services, confidentiality and integrity of the data can be achieved by assuring that security issues have been met. MANETs often suffer from security attacks because of its features like open medium, changing its topology dynamically, lack of central monitoring and management, cooperative algorithms and no clear defense mechanism. These factors have changed the battle field situation for the MANETs against the security threats.

The MANETs work without a centralized administration where the nodes communicate with each other on the basis of mutual trust. This characteristic makes MANETs more vulnerable to be exploited by an attacker inside the network. Wireless links also makes the MANETs more susceptible to attacks, which make it easier for the attacker to go inside the network and get access to the ongoing communication [7, 19]. Mobile nodes present within the range of wireless link can overhear and even participate in the network. MANETs must have a secure way for transmission and communication and this is quite challenging and vital issue as there is an increasing threat of attack on the Mobile Networks. Security is the voice of the day. In order to provide secure communication and transmission, the experts must understand various types of attacks and their consequences on the MANETs. Wormhole attack, Black hole attack, Sybil attack, flooding attack, routing table overflow attack, Denial of Service (DoS), selfish node misbehaving, impersonation attack are kind of attacks that a MANET can suffer from[3, 4, 9, 10, 11,12, 13 ,17 and 30]. A MANET is more open to these kinds of attacks due to the phenomena that the communication is based on mutual trust between the nodes. There is no central point for network management, no authorization facility, vigorously changing topology and limited resources.

2. Review of the State of Art

Previously works reported on MANETs focuses mainly on various security threats and attacks such as DoS, DDoS, Impersonation, Wormhole, Jellyfish, and Black Hole attack [11, 12, 17, 30 and 31]. Black Hole amongst these attacks involved in MANET is evaluated based on reactive routing protocol like Ad-Hoc On Demand Distance Vector (AODV) and its effects are elaborated by stating how this attack disrupt the performance of MANET. Very limited attention has been paid to the fact to study the impact of Black Hole attack in MANET employing both Reactive and Proactive protocols and to compare the vulnerability of both these protocols against the attack. There is a need to address both these types of protocols under the attack, as well as the impacts of the attacks on the MANETs. This Paper analyzes Black Hole attack in MANETs using AODV and OLSR which are reactive and proactive respectively in nature.

Despite the fact of popularity of MANET, these networks are very much exposed to attacks [9, 23]. Wireless links also makes MANET more susceptible to attacks which make it easier for the attacker to enter the network and have access to the communication [9, 21]. Various attacks have been analyzed in MANET and their effect on the network. MANETs routing protocols are also being exploited by the attackers in the form of flooding attack, which is done by the attacker either by using RREQ or data flooding [16].

In any network, the sender wants its data to be sent as soon as possible in a secure environment efficiently. Many attackers advertise themselves to have the shortest and high bandwidth available for the transmission such as in wormhole attack. The attackers get themselves in strong strategic location in the network and make the best use of their location (i.e. they have shortest path between the nodes) [12, 17]. One of the most arising issues in MANET is the limited battery, attackers take an advantage of this flaw and tries to keep the nodes awake until all energy of the attacked node is lost and the node go into permanent sleep [18]. Many other attacks MANET such as jellyfish attack, modification attack, misrouting attack and Routing Table Overflow have been studied and exposed [19, 13, and 20].

Distributed denial of Service (DDoS) is another kind of attack in MANET, where the attacker aims multiple nodes within the network. This attack is employed to break into hundreds and thousands of machines; these machines are used to launch number of attacks against the aimed targets. These attacks are used in order to consume the bandwidth of the targets and to block, jam and restrict access of any other machine to the network [30]. In [31] a spatial correlation detection technique is proposed. This method first approximates the abnormality of every origin destination flow. Once estimation is performed subsequently origin destination flow with same destination is compared and spatial correlation is derived between their abnormality. DDoS attacked can be detected by any abrupt change in the spatial correlation.

In black hole attack, a malicious node uses its routing protocol in order to advertise itself for having the shortest path to the destination node or to the packet it wants to intercept.

This hostile node advertises its availability of fresh routes irrespective of checking its routing table. In this way attacker node will always have the availability in replying to the route request and thus intercept the data packet and retain it [23, 24]. Detecting Black Hole attack is also one of the important issues in order to secure the network from such attacks. In [3] a path based detection method is proposed, in which every node is not supposed to watch every other node in their neighborhood, but in the current route path it only observes the next hop. There is no overhead of sending extra control packets for detecting Black Hole attack. This paper is organized as follow section 3 is about Problem statement and main contribution, section 4 discusses Black Hole attack, section 5 is about Performance Matrics, section 6 discusses Results and section 7 discusses Conclusion and Future Work.

3. Problem Statement and Main Contribution

Aims and objectives of this study work are summarized as follow

- The study focus on analysis of black hole attack in MANET and its consequences.
- Analyzing the effects of black hole attack in the light of Network load, throughput and end-to-end delay in MANET.
- Simulating the black hole attack using Proactive and Reactive routing protocols.
- Comparing the results of both Proactive and Reactive protocols to analyze which of these two types of protocols are more vulnerable to Black Hole attack.

The ultimate goal of any network is to ensure successful transmission between the devices in the network in a secure environment. In ordered to investigate, in the case, when there is an attack in the network, the impact of the attack and vulnerability of the routing protocols. This paper addresses the followings.

Initially in this paper we will discuss what are the consequences of black hole attack on MANET? This question is important because of the factor to know how severe the attack is, how much the network is destabilized. This would help the researcher to work on the isolation of such threats in MANETs. The paper also measures the performance impact of MANETs in a normal operation as well as under the Black Hole attack. Investigation will be carried out which one of these two types of routing protocols is more vulnerable to the Black Hole attack on MANET? Comparing the results for both types of protocols under the attack, to analyze which of these two types of protocols are more vulnerable to black hole attack and has more impact on the MANET. The importance of this question is that once it is identified which protocol is more vulnerable to attack would lead us to research more on that particular protocol in order to make it more secure in such type of attack.

4. Black Hole attack

In black hole attack, a malicious node uses its routing protocol in order to advertise itself for having the shortest path to the destination node or to the packet of its interest to intercept [3, 4, 33].This hostile node advertises its availability of fresh routes irrespective of checking its routing table. Therefore attacker node will always have the availability in replying to the route request and hence interception will occur [21]. Protocol based on flooding, the malicious node reply would be received by the requesting node before the reception of reply from actual node; consequently a malicious and forged route is created. Once this route is establish, now up to the node whether to drop all the packets or forward it to the unknown address [22].

The method how malicious node fits in the data routes varies. A Black Hole problem such as shown in the Fig.1, here node ‘A’ want to send data packets to node ‘D’ and initiate the route discovery process. So if node ‘C’ is a malicious node then it will claim that it has active route to the specified destination as soon as it receives Route Request (RREQ) packets. It will then send the response to node ‘A’ before any other node. In this way node ‘A’ will consider that this is the active route and thus active route discovery is complete. Node ‘A’ will ignore all other replies and will start seeding data packets to node ‘C’. In this way all the data packet will be lost consumed or lost.

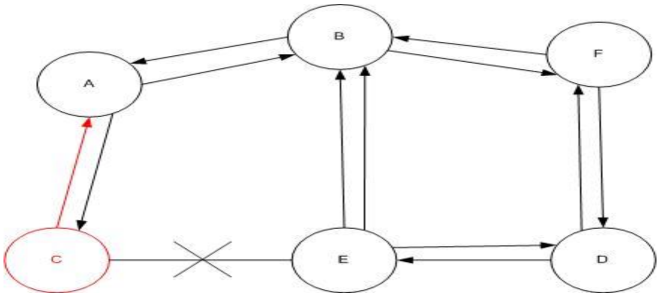


Fig. 1 Black Hole attack in AODV

In Optimized Link State Routing (OLSR) black hole attack, a malicious node forcefully selects itself as Multi Point Rely (MPR). Malicious node keeps its willingness field to (will always) constantly in its HELLO message. So in this case, neighbors of malicious node would always select it as MPR. Hence the malicious node earns a privileged position in the network which it exploits to carry out the denial of service attack.

5. Proposed Method

The performance metrics chosen for the evaluation of black hole attack are packet end-to-end delay, network throughput and network load. The packet end-to-end delay is the average time in order to traverse the packet inside the network. This includes the time from generating the packet from sender up till the reception of the packet by receiver or destination and expressed in seconds. This includes the overall delay of networks including buffer queues, transmission time and induced delay due to routing activities.

The second parameter is throughput; it is the ratio of total amount of data which reaches the receiver from the sender to the time it takes for the receiver to receive the last packet. It is represented in bits/sec or pack/sec. In MANETs throughput is affected by various changes in topology, limited bandwidth and limited power. Unreliable communication is also one of the factors which adversely affect the throughput parameter.

The third parameter is network load, it is the total traffic received by the entire network from higher layer of MAC which is accepted and queued for transmission. It indicates the quantity of traffic in entire network. It represents the total data traffic in bits per seconds received by the entire network from higher layer accepted and queued for transmission. It does not include any higher layer data traffic rejected without queuing due to large data packet size.

The tool used for the simulation study is OPNET 14.5 modeler. OPNET is a network and application based software used for network management and analysis [24]. OPNET models communication devices, various protocols, architecture of different networks and technologies and provide simulation of their performances in virtual environment. OPNET provides various research and development solution which helps in research of analysis and improvement of wireless technologies like WI-MAX, Wi-Fi, UMTS, analysis and designing of MANET protocols, improving core network technology, providing power management solutions in wireless sensor networks.

In this study we employed OPNET for modelling the network nodes, selecting its statistics and then running its simulation to obtain the result for the analysis. Fig. 2 employs the simulation setup of a single scenerio comprising of 30 mobile nodes moving at a constant speed of 10 meter/sec. Total of 12 scenarios have been developed, all of them with mobility of 10 m/s. Number of nodes were varied and the simulation time was taken 1000 seconds. This time is taken so that the simulation get stable, in the first 300 seconds simulation is varying subsequently start getting stable for rest of the time. Simulation area taken is 1000 x 1000 meters, which enough for 16 and 30 nodes to move freely without being crowded. Second reason is if we take area more than the one taken, the distance between each node will increase that will introduce extra delay due to the long distance between the nodes. Packet Inter-Arrival Time (sec) and packet size (bits) is taken exponential (1) is exponential (i.e.1024) respectively.

The data rates for mobile nodes are 11 Mbps with the default transmitting power of 0.005 watts. Random point mobility was selected with the constant speed of 10 meter/seconds and with pause time of constant 100 seconds. This pause time is taken after data reaches the destination only.

Our goal was to determine the protocol which shows less vulnerability in the case of black hole attack. AODV and OLSR routing protocols were chosen, which reactive and proactive protocols respectively are. In both case AODV and OLSR, malicious node buffer size is lowered to a level which increase packet drop. Table.1 shows Architectural experiments.

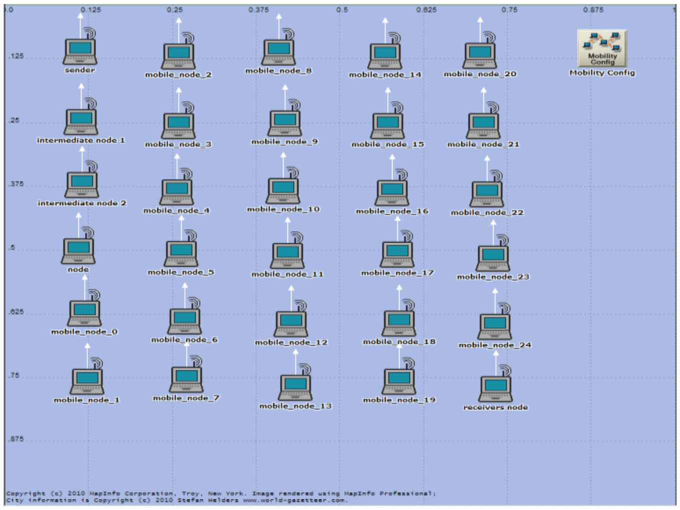


Fig. 2 Proposed Experimental Setup

Table.1 Simulation Parameters

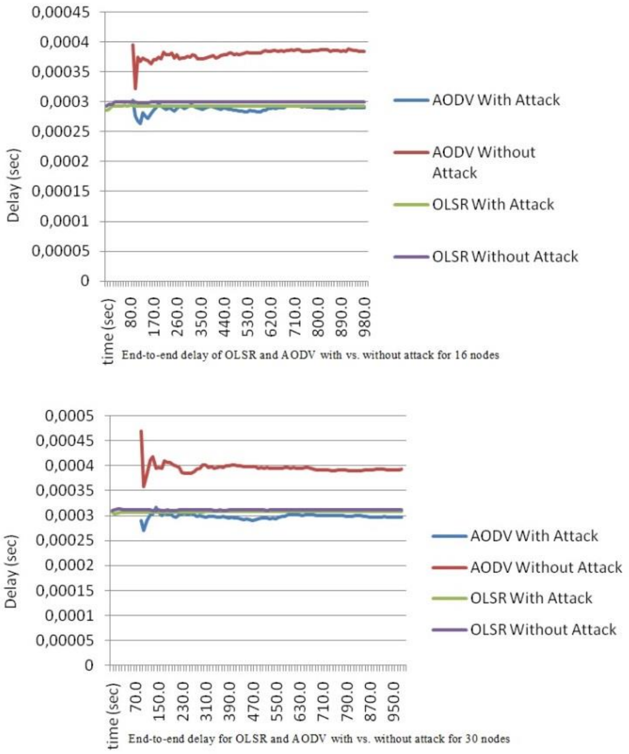
SIMULATION PARAMETERS	
Examined protocols	AODV and OLSR
Simulation time	1000 seconds
Simulation area (m * m)	1000 *1000
Number of Nodes	16 and 30
Traffic Type	TCP
Performance Parameter	Throughput, delay, Network Load
Pause time	100 seconds
Mobility (m/s)	10 meter/second
Packet Inter-Arrival Time (s)	exponential(1)
Packet size (bits)	exponential(1024)
Transmit Power(W)	0.005
Date Rate (Mbps)	11 Mbps
Mobility Model	Random

6. Results

Packet end-to-end delay for the case of Black Hole attack and without attack depends on the protocol routing procedure and number of nodes involved. In Fig. 3, delay in the case of 16 nodes for AODV and OLSR is high (when there is no attack on the network nodes). This is because during the Black Hole attack, there is no need of RREQs and RREPs as the malicious node already sends its RREQs to the sender node prior to the destination node reply having less delay. Also comparatively AODV exhibits high delay as compared to OLSR due to its route search and reactive nature.

In the case of 30 nodes the delay is 5 percent more as compared to the case of 16 nodes. This increase in delay is due to the additional nodes in the topology through which the data passes to the destination node. As the number of nodes increases the delay increased. The overall impact of delay on AODV and OLSR is same as it was observed in

16 nodes. However increase in the numbers of nodes also increases the difference of delay in AODV in case (of Black Hole attack) with comparison to a simple AODV scenario.



End-to-end delay of OLSR and AODV with vs. without attack for 16 nodes

End-to-end delay for OLSR and AODV with vs. without attack for 30 nodes

Fig. 3 End-to-end delay for OLSR and AODV (with vs. without attack)

Fig. 3 and Fig. 4 show the average packet end-to-end delay in presence of a malicious node only. Fig. 3 shows that OLSR has slightly higher delay than to AODV (for 16 and 30 nodes) respectively. This is consistent if the numbers of nodes are less. However with the increase in number of node an increase in the delay of AODV has been observed as shown in Fig.4, for 30 nodes. In terms of delay the performance of OLSR improves with the increase in number of nodes because of its table driven nature. It maintains up to date routing information from each node to every other node in the network.

From Fig. 5, (for 16 nodes), it could be observed that the throughput for OLSR is high compared to that of AODV. Also in OLSR throughput for the case with no attack is higher than the throughput of OLSR under attack. This is because of the fewer routing forwarding and routing traffic. Here the malicious node discards the data rather than forwarding it to the destination, thus effecting throughput.

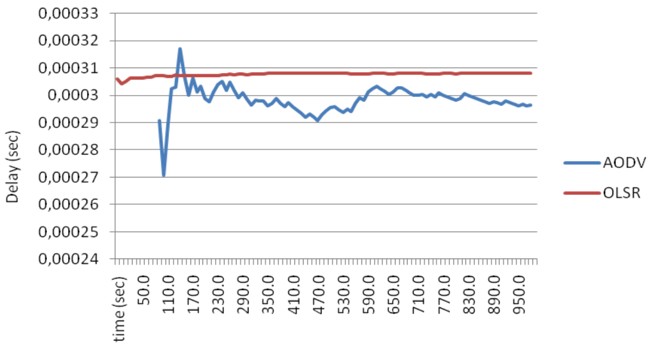
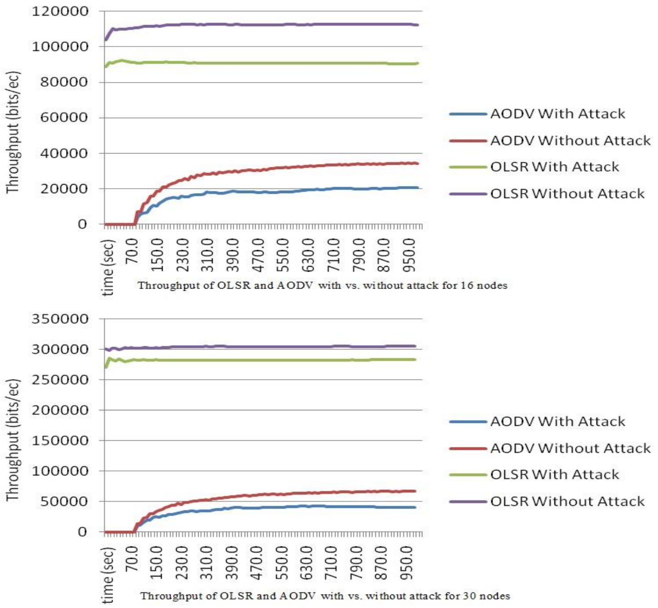


Fig. 4 End-to-end delay 30 nodes AODV vs. OLSR (with attack)

The same is observed in the case with AODV, without attack, its throughput is higher than in the case with under attack because of the packets discarded by the malicious node. Similarly in Fig. 5 (for 30 nodes), the throughput is high because of the high number of nodes however the trend of throughput with attack and without attack remains the same as in 16 numbers of nodes.



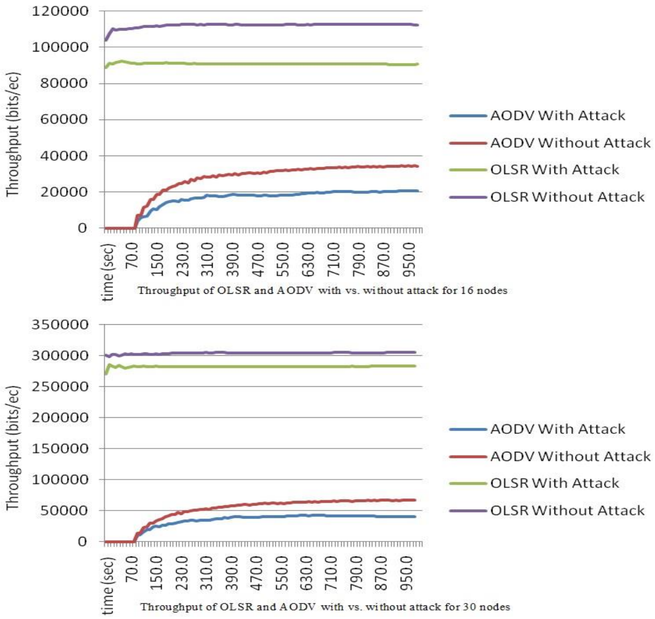
Throughput of OLSR and AODV with vs. without attack for 16 nodes

Throughput of OLSR and AODV with vs. without attack for 30 nodes

Fig. 5 Throughput for OLSR and AODV (with vs. without attack)

Fig. 6 shows that the throughput of AODV and OLSR in the presence of a single malicious node. It is obvious from both figures that OLSR by far outperforms AODV in case of both 16 and 30 sources. OLSR being proactive routing protocols makes sure that the availability of routing path exists, before routing the traffic. It have been observed that the high number of sources gives less difference in throughput as compare to less number of sources, since higher number of sources offers more congestion. Over all, OLSR ensures consistent routing paths in the network, helping in lower the delay there. Since throughput is the ratio of the total data received from source to the time it takes till the receiver receives the last packet. A lower delay translates into higher throughput. The overall low throughput of AODV is due to route reply. The malicious node immediately sends its route reply and the data is sent to the malicious node which discards all the data. The network throughput is considerably lower.

The network load graphs of OLSR and AODV with and without presence of a malicious node have been shown in Fig. 7. The network load of OLSR is high as compare to AODV. In the case of attack, OLSR has less network load as compare to without attack. In case of 16 nodes the network load of OLSR is three times higher in case of without attack which implies that it is actually routing its packet to the entire destination properly. However under attack it cannot send its packet (i.e. packet discarding leads to a reduction of network load).



Throughput of OLSR and AODV with vs. without attack for 16 nodes

Throughput of OLSR and AODV with vs. without attack for 30 nodes

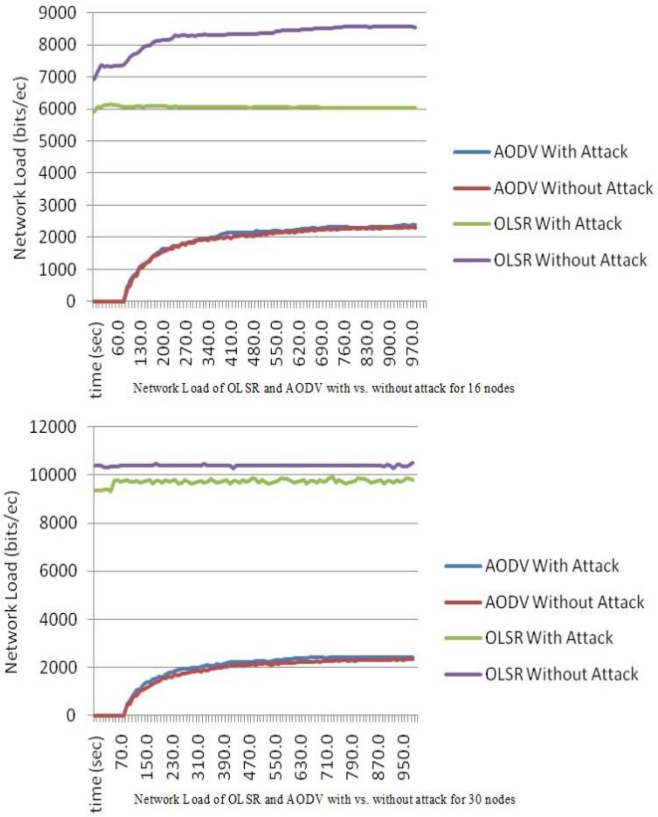
Fig. 6 Throughput for AODV vs. OLSR (with attack)

In case of 30 nodes there is a slight variation in between OLSR with and without attack. This is due to the high number of nodes which leads to more increase in routing traffic, however AODV show no changes (in both cases of 16 and 30 number of nodes).

In case of network load Fig. 8 shows that OLSR has a high network load in presence of a malicious node as compare to that of AODV. With 16 nodes and 30 nodes OLSR has high network load because the routing protocols are able to adjust its changes in it during node restart and node pausing. This is different at different speeds, at high speeds the routing protocols take longer time for adjusting and afterward sending the traffic to a new route.

In the case of higher number of nodes AODV react quickly as compare to OLSR which made the difference in network load much wider. The node began to pause and restarts, hence its mobility after the starting time having more stability, and this make the network load more pronounced.

Mobile Ad-Hoc networks are widely used networks due to their flexible nature i.e. easy to deploy regardless of geographic constraints, where a traditional network infrastructure environment cannot possibly be deployed.



Network Load of OLSR and AODV with vs. without attack for 16 nodes

Network Load of OLSR and AODV with vs. without attack for 30 nodes

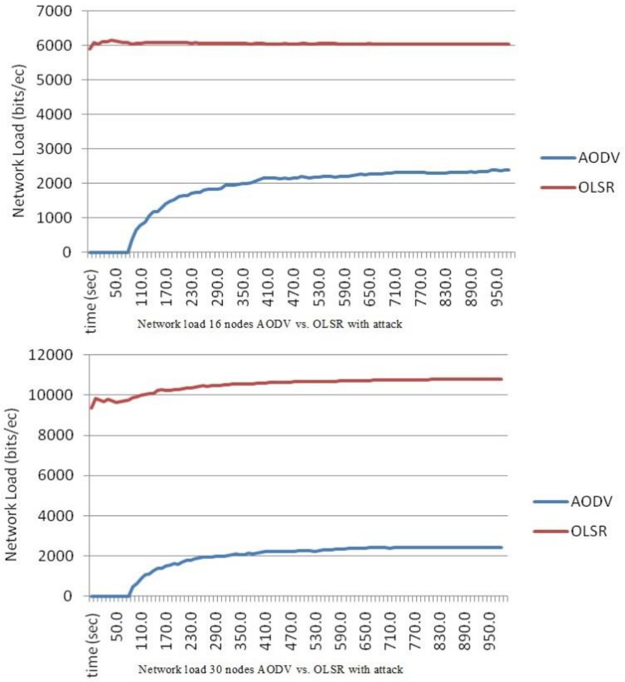
Fig. 7 Network Load of OLSR and AODV (with vs. without attack)

These networks are exposed to both external and internal attacks as there is not centralized security mechanism. With the importance of MANET comparative to its vast potential it has still many challenges left in order to overcome. Security of MANET is one of the important features for its deployment. In the paper, we have analyzed the behaviour and challenges of security threats in mobile Ad-Hoc networks. 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 analysed deeply in order to draw the final conclusion.

7. Conclusion and future work

We analysed that Black Hole attack with four different scenarios with respect to the performance parameters of end-to-end delay, throughput and network load. In a network it is important for a protocol to be redundant and efficient in term of security. An investigation on the vulnerability of two protocols OLSR and AODV have been made.



Network load 16 nodes AODV vs. OLSR with attack

Network load 30 nodes AODV vs. OLSR with attack

Fig. 8 Network load AODV vs. OLSR (with attack)

It was observed that when there is higher number of nodes and more route requests, it affect the network performance more. The percentage of severances in delay under attack is 2 to 5% and in case of OLSR, where as it is 5 to 10% for AODV. The throughput of AODV is effected by twice as compare of OLSR. In case of network load however, there is effect on AODV by the malicious node is less as compare to OLSR. Addressing the second research question, from the impact of Black Hole attack on the MANETs it was found that AODV is much more affected by the attack as compared to OLSR. From the research, it was found that AODV protocol is more vulnerable to Black Hole attack than that of OLSR protocol.

An effort has been made to discuss and analyse the impact of Black Hole attack in MANETs employing AODV and OLSR protocols. There is a need to analyze Black Hole attack in other MANETs routing protocols such as DSR, TORA and GRP. Other types of attacks such as Wormhole, Jellyfish and Sybil attacks are needed to be studied in comparison with Black Hole attack. They can be categorized on the basis of how much they affect the performance of the network. Black Hole attack can also attack the other way around i.e. as Sleep Deprivation attack. A study on the detection of this behavior of Black Hole attack as well as the elimination strategy for such behavior is currently under consideration.

References

[1] C.E.Perkins and E.M.Royer, “Ad-Hoc On Demand Distance Vector Routing,” Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, pp.90-100, Feb, 1999.

[2] C.M barushimana, A.Shahrabi, “Comparative Study of Reactive and Proactive Routing Protocols Performance in Mobile Ad-Hoc Networks,” Workshop on Advance Information Networking and Application, Vol. 2, pp. 679-684, May, 2003.

[3] C.Jiwen, Y.Ping, C.Jialin, W.Zhiyang, L.Ning, “ An Adaptive Approach to Detecting Black and Gray Hole Attacks in Ad Hoc Network,”24th IEEE International Conference on Advance Information Networking and Application (AINA 2010), pp. 775-780, April,2010.

[4] Aishwarya Sagar Anand Ukey and Meenu Chawla, “Detection of Packet Dropping Attack Using Improved Acknowledgement Based Scheme in MANET”, International Journal of Computer Science Issue, pp. 12-17, vol. 7(4-1), July 2010

[5] C.Parkins, E.B.Royer, S.Das, A hoc On-Demand Distance Vector (AODV) Routing. July 2003, [Online]. Available: http://www.faqs.org/rfcs/rfc3561.html. [Accessed: February. 11, 2013]

[6] M.Abolhasan, T.Wysocki, E.Dutkiewicz, “A Review of Routing Protocols for Mobile Ad-Hoc Networks,” Telecommunication and Information Research Institute University of Wollongong, Australia, June, 2003.

[7] T.Clausen, P.Jacquet , “Optimized Link State Routing Protocol (OLSR),”October, 2003, [Online]. Available: http://www.faqs.org/rfcs/rfc3626.html. [Accessed: April. 10, 2010].

[8] Z.J.Hass, M.R.Pearlman, P.Samar, “The Zone Routing Protocol (ZRP) for Ad Hoc Networks,” July, 2002, [Online]. Available: http://www.ietf.org/proceedings/55/I-D/draft-ietf-manet-zone-zrp-04.txt, [Accessed: April. 10, 2010].

[9] P.V.Jani, “Security within Ad-Hoc Networks,” Position Paper, PAMPAS Workshop, Sept. 2002.

[10] M.Parsons, P.Ebinger, “Performance Evaluation of the Impact of Attacks on mobile Ad-Hoc networks,” [Online].

Available: www.cse.buffalo.edu/srds2009/dncms2009_submission_person.pdf, [Accessed: April. 10, 2010].

[11] D.B.Roy, R.Chaki and N.Chaki, “A New Cluster-Based Wormhole Intrusion Detection Algorithm for Mobile Ad-Hoc Networks,” International Journal of Network Security and Its Application (IJNSA), Vol. 1, No.1, April, 2009.

[12] H.L.Nguyen, U.T.Nguyen, “Study of Different Types of Attacks on Multicast in Mobile Ad Hoc Networks,” International Conference on System and Networks and International Conference on Mobile Communications and Learning Technologies (ICN/ICONS/MCL 2006), pp.149-149, April, 2006.

[13] C.Wei, L.Xiang, B.yuebin and G.Xiaopeng, “A New Solution for Resisting Gray Hole Attack in Mobile Ad-Hoc Networks,” Second International Conference on Communications and Networking in china, pp.366-370, Aug, 2007.

[14] S.Marti, T.J.Giuli, K.Lai, M.Baker, “Mitigating Routing Misbehavior in Mobile Ad-Hoc Networks,” Proceedings of the 6th annual international conference on Mobile computing and networking, united states, pp. 255-265,

[15] Zhu, C. Lee, M.J.Saadawi, T., “RTT-Based Optimal Waiting time for Best Route Selection in Ad-Hoc Routing Protocols,” IEEE Military Communications Conference, Vol. 2, pp. 1054-1059, Oct, 2003.

[16] M.T.Refaei, V.Srivastava, L.Dasilva, M.Eltoweissy, “A Reputation-Based Mechanism for Isolating Selfish nodes in Ad-Hoc Networks,” Second Annual International Conference on Mobile and Ubiquitous Systems, Networking and Services, pp.3-11, July, 2005.

[17] V.Mahajan, M.Natue and A.Sethi, “Analysis of Wormhole Intrusion attacks in MANETs,” IEEE Military Communications Conference, pp. 1-7, Nov, 2008.

[18] F.Stanjano, R.Anderson, “The Resurrecting Duckling: Security Issues for Ubiquitous Computing,” Vol. 35, pp. 22-26, Apr, 2002.

[19] H.L.Nguyen,U.T.Nguyen, “Study of Different Types of Attacks on Multicast in Mobile Ad-Hoc Networks,” International Conference on Networking, Systems, Mobile Communications and Learning Technologies, Apr,2006.

[20] H.Deng, W.Li and D.P.Agrawal, “Routing Security in Wireless Ad-Hoc Networks,” University of Cincinnati, IEEE Communication Magazine, Oct, 2002.

[21] K. Biswas and Md. Liaqat Ali, “Security threats in Mobile Ad-Hoc Network”, Master Thesis, Blekinge Institute of Technology” Sweden, 22nd March 2007

[22] G. A. Pegueno and J. R. Rivera, “Extension to MAC 802.11 for performance Improvement in MANET”, Karlstads University, Sweden, December 2006

[23] S. Lu, L. Li, K.Y. Lam, L. Jia, “SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack.,” International Conference on Computational Intelligence and Security, 2009.

[24] Opnet Technologies, Inc. “Opnet Simulator,” [Online]. Available: www.opnet.com, [Accessed: March. 10, 2013].

[25] S. Kurosawa, H.Nakayama, N.Kato, A.Jamalipour, Y.Nemoto, “Detecting Blackhole Attack on AODV- Mobile Ad-Hoc Networks by Dynamic Learning Method,” International Journal of Network Security, Vol. 5, No.3, pp. 338-346, Nov, 2007.

[26] M. Al-Shurman, S-M. Yoo, and S. Park, “Black Hole Attack in Mobile Ad-Hoc Networks,” ACM Southeast Regional Conf. 2004.

[27] H. Deng, W. Li, Agrawal, D.P., “Routing security in wireless Ad-Hoc networks,” Cincinnati Univ.,OH, USA; IEEE Communications Magazine, , Vol.40, pp.70- 75, ISSN: 0163-6804, Oct. 2002.

[28] K. Sanzgiri, B. Dahill, B.N. Levine, C. Shields, E.M. Belding Royer, “Secure routing protocol for Ad-Hoc networks,” In Proc. of 10th IEEE International Conference on Network Protocols, Dept. of Computer. Science, California Uni., Santa Barbara, CA, USA. pp.78- 87, ISSN: 1092-1648, Nov. 2002.

[29] J. W. Creswell, Research Design: Qualitative, Quantitative and Mixed Methods Approach, 2nd Ed, Sage Publications Inc, California, July 2002.

[30] Kai Wang, Jia Chen, Huachun Zhou and Yajuan Qin,”Content-Centric Networking: Efect of Content Cachingon Mitigating DoS Attack”, International Journal of Computer Science Issue, pp.43-52, vol.9,(6-3),November2012

[31] L.Zonglin, H.Guangming, Y.Xingmiao, “ Spatial Correlation Detection of DDoS attack” International Conference on Communication, Circuits and System (ICCCAS 2009), pp. 304-308, July, 2009.

[32] X.Y.Zhang, Y.Sekiya, Y.Wakahara, “ Proposal of a method to detect black hole attack in MANET,” International Symposium on Autonomous Decentralized System (ISADS’09), pp. 1-6, March,2009.

[33] S.Sharma, Rajshree, R.P.Pandey, V.Shukla, “Bluff-Probe Based Black Hole Node Detection and Prevention, ”IEEE International Advance Computing Conference (IACC 2009), pp. 458-462, March, 2009.