International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 7, Issue 3, March 2018, ISSN: 2278 – 1323

Performance Analysis of Network Layer attacks in Mobile Ad Hoc Networks

Mr. SachinKorde, Dr. M. V. Sarode, Dr. V. M. Thakare
***PhD Scholar*[1]*, Head of Department*[2, 3]**
***SGBAU, Amravati*[1]**
***Government Polytechnic, Yavatmal*[2]**
***SGBAU, Amravati*[3]**

Abstract-: Mobile ad hoc networks are viewed as much a group regarding networks consisted over wireless systems who developing together a network together with self-arrangement capability. These networks hold no constant communication infrastructure and makes use of central nodes in conformity with communicate together with other nodes. Despite a lot of advantages, these networks face severe security challenges, when you consider that theirs channels are wireless and each node is linked to central node. One of these issues is the chance of black hole stacks destructive mobile ad hoc networks routing protocols. Through that process, the Attacker node proclaims itself as the nearest to destination node; then, network nodes choose such as the medium node when transmitting their data packets. As a result, that node can delete its delivered packets alternatively transmitting. In this paper, impact of network layer attacks such as blackhole, grayhole and wormhole is studied, Simulation results revealed that the how attacks impact on AODV protocol under attack in terms of packet delivery rate, throughput, end to end delay.

Keywords: Routing protocols, Security, MANET, attacks.

I. INTRODUCTION

Mobile Ad hoc Networks are autonomous and decentralized wireless systems. Mobile Ad hoc Networks correspond regarding mobile nodes that are arbitrary within transferring in and outdoors within the network. Nodes are the systems or units i.e. mobile phone, laptop, personal digital assistance, MP3 player and private computer systems that are collaborating between the network and are mobile.

These nodes perform work namely host/router or each at the identical time. They perform shape unrestricted topologies depending on theirs connectivity together with every mean within the network. These nodes bear the capacity to configure themselves and because of theirs self-interest formal ability, they can be deployed urgently barring the need on someone infrastructure. Internet Engineering Task Force (IETF) has Mobile Ad hoc Networks working group (WG) that is committed in imitation of developing IP routing protocols. Routing protocols are some regarding the challenging and strong research areas. Many routing protocols hold been developed for Mobile Ad hoc Networks, i.e. AODV, DSDV, DSR etc. Security in Mobile Ad hoc Network is the nearly vital difficulty for the simple functionality on the network. The availability regarding network services, confidentiality and morality regarding the facts perform stand executed by way of assuring so much protection issues have been met.

Mobile Ad hoc Networks often suffer from security attacks due to the fact of its applications like open medium, altering its topology dynamically, absence of middle monitoring and management, cooperative algorithms and no manifest defense mechanism. These elements have changed the battlefield situation because of the Mobile Ad hoc Networks against the safety threats. The Mobile Ad hoc Networks work barring a centralized administration the place the nodes communicate with each other regarding the basis about mutual trust. This characteristic makes Mobile Ad hoc Networks extra susceptible to be exploited with the aid of an attacker inside the network. Wireless links additionally redact the Mobile Ad hoc Networks more susceptible to attacks, which make such less complicated because the attacker to continue 2 interior the network and reach access in conformity with the permanent communication. Mobile nodes current within the measure of wireless link perform overhear and too take part among the network.

Mobile Ad hoc Networks ought to hold a secure access because transmission and communication and it is a quite challenging and imperative problem as like so is growing threats on attack on the Mobile Networks. Security is the allege about the day. In system in

accordance with grant secure communication and transmission, the engineers need to understand different kinds concerning attacks and their consequences over the Mobile Ad hoc Networks.

Wormhole attack, Black hole attack, Sybil attack, flooding attack, routing table overflow attack, Denial of Service (DoS), selfish node misbehaving, impersonation assault are the type regarding attacks that Mobile Ad hoc Networks may go through from. A Mobile Ad hoc Networks is greater open to these types concerning attacks because communication is based of mutual trust between the nodes, so is no medium point because network management, no endorsement facility, vigorously changing topology and constrained resources.

II. SECURITY ASPECTS OF MANETS

Some well-known Mobile Ad Hoc network applications are:

Collaborative Work: For some business environments, the need for collaborative computing might be more important outside office environments than inside. After all, it is often the case where people do need to have outside meetings to cooperate and exchange information on a given project.

Crisis-Management Applications: By using Ad Hoc networks, a communication channel could be set up in hours instead of days/weeks required for wire-line communications.

Personal Area Networking and Bluetooth: A personal area Network (PAN) is a short-range, localized network where nodes are usually associated with a given person. These nodes could be attached to someone's pulse watch, belt, and so on. In these scenarios, mobility is only a major consideration when interaction among several PANs is necessary.

There are five major security goals that are needed to maintain a reliable and secure Ad hoc network environment.

There are mainly as following:

Confidentiality of Data- keeps data secret (usually accomplished by encryption).

Integrity of Data- prevents data from being altered (usually accomplished by encryption).

Availability of Data- data should be available on request.

Authenticationof Data- verification that the data or request came from a specific, valid sender.

III. DESCRIBES THE AODV ROUTING PROTOCOL

The Ad Hoc On-Demand Distance Vector (AODV8) routing protocol is an adaptation of the DSDV protocol for dynamic link conditions (Perkins et al 2000). (Charles et al 2003). Every node in an Ad-hoc network maintains a routing table, which contains information about the route to a particular destination. Whenever a packet is to be sent by a node, it first checks with its routing table to determine whether a route to the destination is already available. If so, it uses that route tsend the packets to the destination. If a route is not available or the previously entered route is inactivated, then the node initiates a route discovery process. A RREQ (Route Request) packet is broadcasted by the node. Every node that receives the RREQ packet first checks if it is the destination for that packet and if so, it sends back an RREP (Route Reply) packet. If it is not the destination, then it checks with its routing table to determine if it has got a route to the destination. If not, it relays the RREQ packet by broadcasting it to its neighbors. If its routing table does contain an entry to the destination, then the next step is the comparison of the 'Destination Sequence' number in its routing table to that present in the RREQ packet. This Destination Sequence number is the sequence number of the last sent packet from the destination to the source. If the destinationsequence number present in the routing table is lesser than or equal to the one contained in the RREQ packet, then the node relays the request further to its neighbors. If the number in the routing table is higher than the number in the packt, it denotes that the route is a 'fresh route' and packets can be sent through this route. This intermediate node then sends a RREP packet to the node through which it received the RREQ packet. The RREP packet gets relayed back to the source through the reverse route. The source node then updates its routing table and sends its packet through this route. During the operation, if any node identifies a link failure it sends a RERR (Route Error) packet to all other nodes that uses this link for their communication to other nodes. This is illustrated in figure 1 and 2.

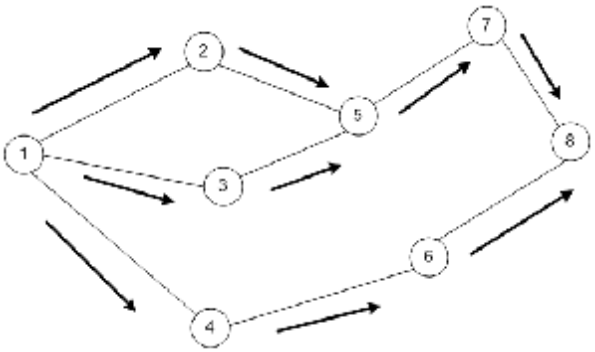

Figure. 1. Broadcast to AODV route discovery

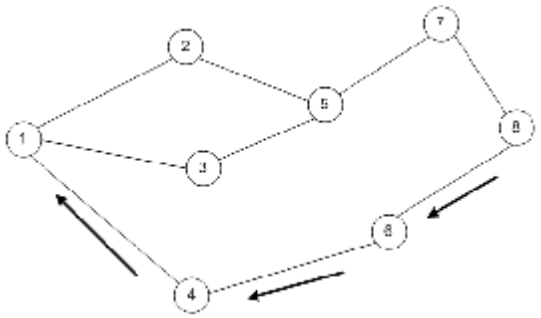

Figure. 2. A sample of route discovery in AODV protocol

IV. THREATS IN MOBILE AD HOC NETWORKS

4.1 BLACK HOL ATTACK

Black hole attack, a malicious node uses its routing protocol in order to With the release of false news, having the shortest path to the destination node or to the packet it wants to avoid the. This black hole node advertises its availability of fresh routes irrespective of checking its routing table. in the attacker node will always have the availability in replying to the route request and thus intercept the data packet and retain it (Biswas et al 2007). In protocol based on flooding, the black hole node reply will be received by the requesting node before thereception of reply from actual node; hence a black hole and forged route is created. When this route is establish, now it's up to the node whether to drop all the packets or forward it to the unknown address (Pegueno et al 2006). (1) The Solution how black hole node Proportional in the data routes varies. Fig. 4 shows how black hole Problems, here node "E" want to send data packets to destination node "D" and The initial process of route discovery. So if node "F" is a black hole node then it will claim that it has active route to the specified destination as soon as it receives RREQ packets. It will then send the response to node "E" before any other node. In this way node "E" will think that this is the active route and thus active route discovery is complete. Node "E" will ignore all other replies and will start seeding data packets to node "F". In this way all the data packet will be lost consumed or lost.

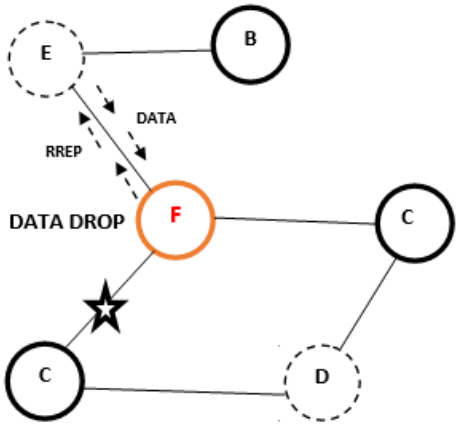

Figure. 4. Problems of black hole attacks

4.2WORM HOLE ATTACK

Wormhole attack which is considered as a severe attack in mobile ad hoc network. Minimum two malicious nodes are required to perform this attack; more than two malicious nodes are also used to perform this attack. In this attack the two malicious nodes resides in the two ends of the network and they form a link between them using an out-of-band hidden channel like wired link, packet encapsulation or high power radio transmission range (Azer et al 2008). After they form a tunnel between them as shown in figure 1, whenever a malicious node receives packets it tunnels them to the other malicious node and in turn it broadcasts the packet there. Since the packet is travelling through the tunnel it reaches the destination speeder than other route and moreover the hop count through this path is going to be less so this path is established between the source and the destination (Reshmi et al 2010). Once the path is established between the source and the destination through wormhole link they can misbehave in many ways in the network like continuously dropping the packets, selective dropping the packets, analyzing the traffic and performing Denial of Service attack. Figure 5 shows an example of this attack.

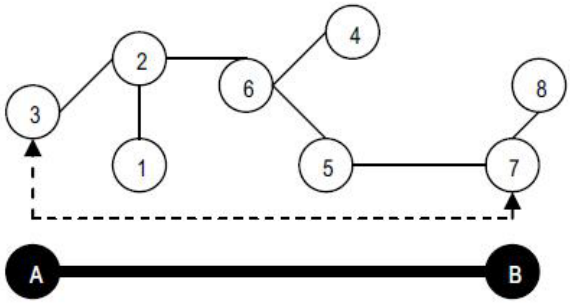

Figure. 5. An example of a wormhole attacks

4.3 GRAY HOLE ATTACK

We now explain the gray hole attack on MANETs. The gray hole attack has two stages. In the first stage, an attacker exploits the AODV protocol to advertise itself as having a valid route to a destination node, with the intention of intercepting packets, even though the route is spurious. In the second stage, the node drops the intercepted packets with a certain probability. This attack is harder to detect than the black hole attack where the attacker drops the received data packets with certainly. A gray hole may display its attacker behavior in different ways. It may drop packets coming from (or destined to) certain specific node(s) in the network while forwarding all the packets for other nodes. Another type of gray hole node may behave maliciously for some time duration by dropping packets but may switch to normal behavior later. A gray hole may also display a behavior which is a combination of the above two, thereby making its detection even more difficult (Pradip et al 2010).

V. EXPERMENTAL DATA AND ANALYSIS

Table 1 employs the simulation setup of a single scenerio comprising of 30 mobile nodes moving at a constant speed of 10 meter per seconds. Total of 12 scenarios have been developed, all of them with mobility of 10 m/s. Number of nodes were varied and simulation time was taken 1000 seconds. Simulation area taken is 1000 x 1000 meters. Packet Inter-Arrival Time (sec) is taken exponential (1) and packet size (bits) is exponential (1024).

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

Simulator	Ns-2(version 2.32)
Simulation Time	500 (s)
Number of Mobile Nodes	10,20,30,40,50
Topology	700 * 700 (m)
Routing Protocol	AODV, blackhole, grayhole, wormhole
Traffic	Constant Bit Rate (CBR)
Pause Time	10 (m/s)
Max Speed	20 (m/s)

Packet Delivery Ratio: The ratio between the number of packets originated by the "application layer" CBR sources and the number of packets received by the CBR sink at the final destination.

End-to-End Delay

Packet end-to-end delay in case of Black Hole attack and without attack depends on the protocol routing procedure and number of nodes involved.

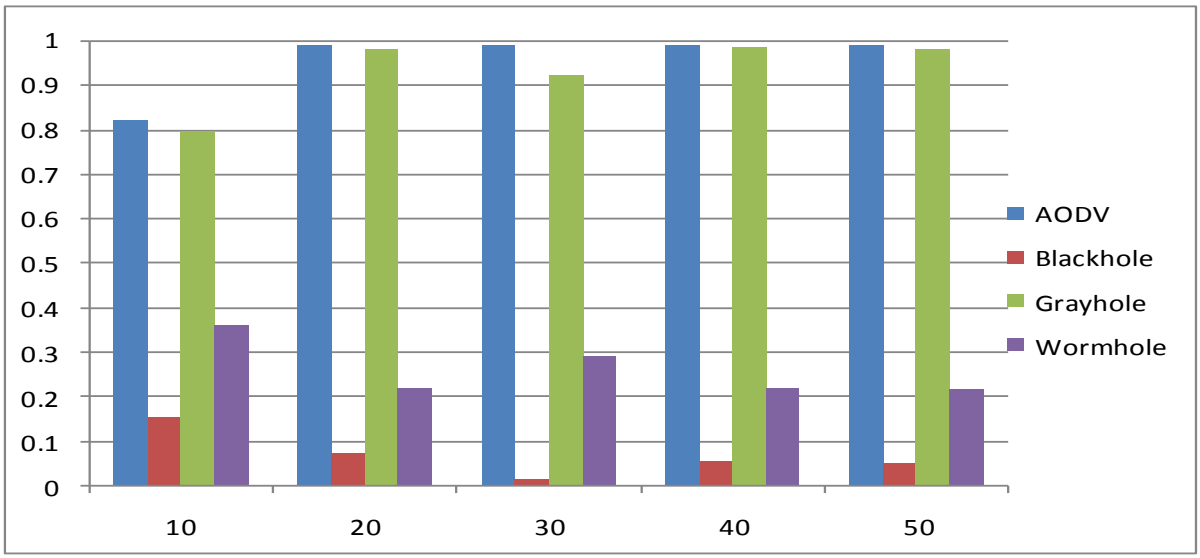

Figure 6 PDR Comparison of AODV, blackhole, grayhole& wormhole attack

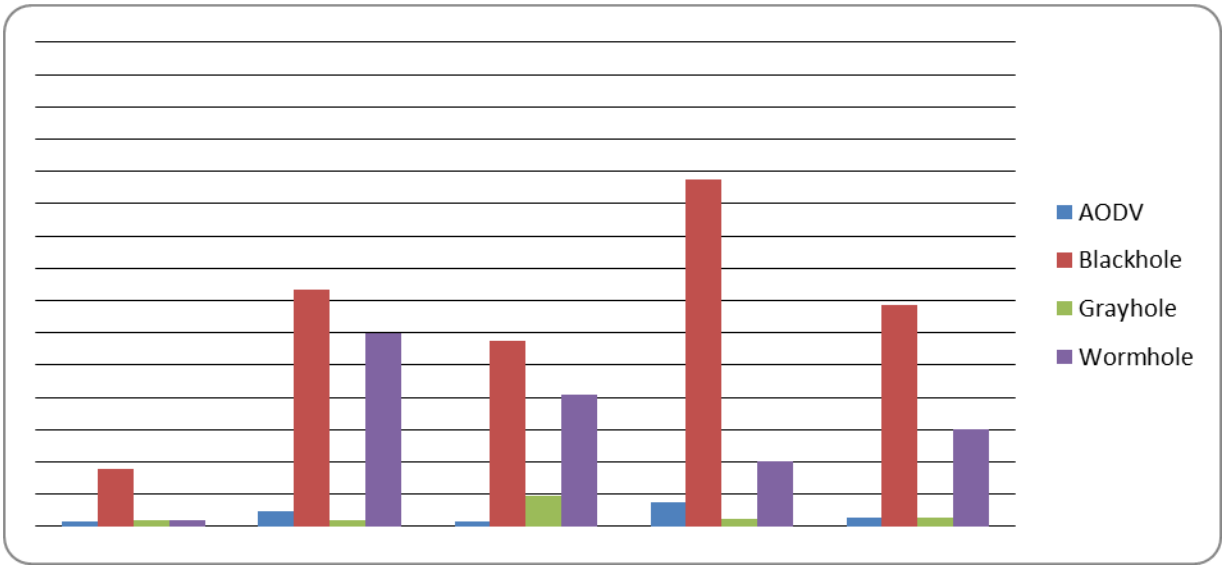

Figure 7 End to End Delay Comparison of AODV, blackhole, grayhole& wormhole attack

VI. CONCLUSION

In this study, we analyzed effect of the network layer attacks such as blackhole, grayhole, wormhole attack on AODV protocol. For this purpose, we implemented an AODV protocol that behaves as blackhole, grayhole, wormhole in NS-2. We simulated five scenarios where nodes vary from 10 to 50 that use AODV protocol and also simulated the same scenarios after introducing one blackhole node, one grayhole node and two wormhole nodes into the network. Result analysis shows impact of these network layer attacks on network.

REFERENCES

1. K. Biswas and Md. Liaqat Ali, "Security threats in Mobile Ad-Hoc Network", MasterThesis, Blekinge Institute of Technology" Sweden, 22nd March 2007
2. G. A. Pegueno and J. R. Rivera, "Extension to MAC 802.11 for performance Improvementin MANET", Karlstads University, Sweden, December 2006
3. S. Lu, L. Li, K.Y. Lam, L. Jia, "SAODV: A MANET Routing Protocol that can WithstandBlack Hole Attack.," International Conference on Computational Intelligence and Security,2009.
4. M.T.Refaei, V.Srivastava, L.Dasilva, M.Eltoweissy, "A Reputation-Based Mechanism forIsolating Selfish nodes in Ad-Hoc Networks," Second Annual International Conference onMobile and Ubiquitous Systems, Networking and Services, pp.3-11, July, 2005.
5. S. Lu, L. Li, K.Y. Lam, L. Jia, "SAODV: A MANET Routing Protocol that can WithstandBlack Hole Attack.," International Conference on Computational Intelligence and Security,2009.
6. K. Biswas and Md. Liaqat Ali, "Security threats in Mobile Ad-Hoc Network", MasterThesis, Blekinge Institute of Technology" Sweden, 22nd March 2007
7. S.Marti, T.J.Giuli, K.Lai, M.Baker, "Mitigating Routing Misbehavior in Mobile Ad-HocNetworks".
8. M.T.Refaei, V.Srivastava, L.Dasilva, M.Eltoweissy, "A Reputation-Based Mechanism forIsolating Selfish nodes in Ad-Hoc Networks," Second Annual International Conference onMobile and Ubiquitous Systems, Networking and Services, pp.3-11, July, 2005.
9. N.Bhalaji, Dr.A.Shanmugam, "Association between nodes to combat blackhole attack inDSR based MANEr", Proc. Int. IFIP Conf. on Wireless and Optical Communications Networks,WOCN '09, India, pp. 1-5,2009.
10. V. Palanisamy, P. Annadurai, S.Vijayalakshmi ,"Impact of Black hole Attack on Multicastin Ad hoc Network (IBAMA)", Proc. In!. IEEE Conf. on Computational Intelligence andComputing Research (ICCIC), India, pp. 1-4,2010.
11. J. CAl, P. YI, Y. TIAN, Y. ZHOU, N. LIU, "The Simulation and Comparison of RoutingAttacks on DSR Protocol", Proc. Int. Conf. on Wireless Communications, Networking andMobile Computing, WiCom '09, China, pp. 1-4,2009.
12. A. Bala, M. Bansal, J. Singh,"Performance Analysis of MANET under Blackhole Attack",First International Conference on Networks & Communications, India, pI41-146, 2009.
13. Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and YoshiakiNemoto: "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Network by DynamicLearning Method", International Journal of Network Security, Vo1.5, PP.33S-346, (November,2007)
14. N. Bhalaji, A. Shanmugam, "A Trust Based Model to Mitigate Black Hole Attacks in DSRBased Manet", European Journal of Scientific Research, ISSN 1450-216X Vol.50 No.1,2011
15. Reza Fotohi, ShahramJamali, FatemeSarkohaki, ShahramBehzad,"An Improvement overAODV Routing Protocol by Limiting Visited Hop Count", IJITCS, vol.5, no.9, pp.87-93, 2013.DOI: 10.5815/ijitcs.2013.09.09
16. Azer, M.A., El-Kassas S.M., Hassan, A.W.F., El-Soudani M.S., "Intrusion Detection for Wormhole Attacks in Ad hoc Networks a Survey and a proposed Decentralized Scheme Marianne " IEEE Third International conference on Availability, Reliability and Security, 2008.
17. ReshmiMaulik, NabenduChaki "A comprehensive review on wormhole attacks in MANET" International Conference on Computer Information Systems and Industrail Management Applications(CISIM) 2010.
18. Pradip M, JawandhiyMangesh M Ghonge, "A Survey of Mobile Ad Hoc Network Attacks", International Journal of Engineering Science and Technology, vol. 2 no. 9, 2010, pp. 4063-4071.