A study of different types of attacks in MANET and performance analysis of AODV protocol against wormhole attack

Swaijit Kaushal, Reena Aggarwal

Lovely professional University, Phagwara, Punjab

Abstract- **Wireless networks are gaining popularity to its peak today, as the users want wireless connectivity irrespective of their geographic position. There is an increasing threat of attacks on the Mobile Ad-hoc Networks (MANET) . Security is one of the main issues in the MANET especially with respect to size and complexity of the network. The main reason of security issues in manet is that there is no physical link between the nodes and the nodes are mobile in nature. Consequently there is no fix topology. Some protocols do not consider the security issues, treat all the nodes as non-malicious nodes etc. The aim is to detect and analyze the performance of MANET using AODV as the routing protocol, under the launch of wormhole attack in the wireless network. Various types of wormhole detection algorithms in MANET has been proposed and studied and particularly a new algorithm for detecting a malicious node has been proposed. Graphs have come for network parameters are throughput ratio, total packets received and packet delivery ratio. All the simulations are done in ns2.35.**

Index terms- **MANET,Routing protocols,Wormhole,AODV**

I. INTRODUCTION

Mobile ad hoc network got outstanding success as well as tremendous attention due to its self maintenance and self configuration properties or behavior. Mobile Ad-Hoc Networks are autonomous and decentralized wireless systems. MANET consists of mobile nodes that are free in This ch 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. They can form arbitrary topologies depending on their connectivity with each other in the network. These nodes have the ability to configure themselves and because of their self configuration ability, they can be deployed urgently without the need of any infrastructure. 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. Security in Mobile Ad-Hoc Network is the most important concern for the basic functionality of network. MANET often suffers 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 MANET against the security threats.

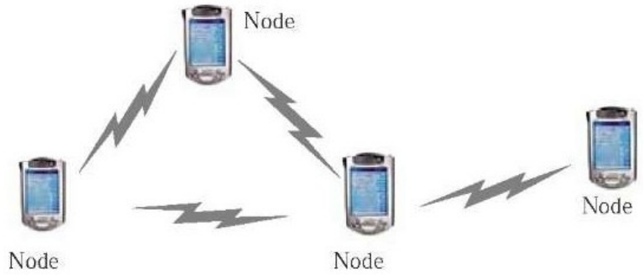

figure1; Ad hoc networks

The MANET works without a centralized administration where the nodes communicate with each other on the basis of mutual trust. This characteristic makes MANET more vulnerable to be exploited by an attacker inside the network. 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. A MANET is more open to these kinds of attacks because 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 [5] [20] [21].

II. RELATED WORK

Neha Rani et.al determined the detection of the performance of mobile ad-hoc network using AODV as the routing protocol, under the launch of wormhole attack in the wireless network using ns2.35 simulator and network parameters are throughput ratio, total packets received and packet delivery ratio. For such networks-proactive routing protocols, reactive routing protocols and hybrid routing protocols[1] are considered. *Manju Ojha et.al* compared the performance of AODV before and under WORMHOLE attack on different AODV parameters such as on throughput, route discovery time delay and packet loss using ns2.35 simulator. It gave [2] the complete analysis of AODV protocol under wormhole nodes which will help researchers to find more accurate or better Wormhole avoidance or prevention techniques. *Richa gulati* evaluated different metrics of the proposed protocol from simulation on NS2 on different scenarios i.e. with worm hole attack and without worm hole attack and there has been a noticeable improvement in the throughput and energy consumption is also reduced. Network parameters that are considered for comparison are throughput and energy comparison. . The proposed work is free of number of hardware support which not only increases the cost but also much complicated to implement [4].

III. MANET AND ITS PROTOCOLS

A MANET is a type of an ad- hoc network that can change locations and configure itself on the fly. MANET can be a model wi-fi connection, or another standard, like a cellular or satellite transmission. MANET has many applications like military, communication, conference meeting, automated battlefield, creating virtual classrooms.
Topology because nodes are self managed without any pre existing structure. MANET has different characteristics bandwidth constraint and limited physical security.
MANET used routing protocols for sending data source to destination [6] [7] [8] [9]. Routing protocols are organized as:

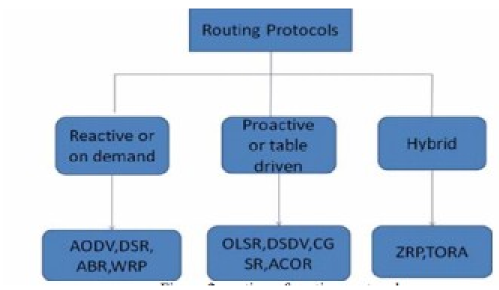

figure 2; Sorting of routing protocols [6]

A. *REACTIVE ROUTING PROTOCOLS*

Reactive protocols tend to decrease the control traffic messages overhead at the cost of increased latency in discover a new routes. Source initiated route discovery in reactive routing protocols and less delay. In reactive protocols there is no need of distribution of information [5]. It consumes bandwidth when transfer data source to destination. Reactive Protocols are AODV (ad-hoc on demand distance vector), DSR (distance vector routing) and ABR. MANET is also called Mesh network. It is high adaptable and rapidly deployable network. MANET has a dynamic topology [11] [12] [13].

a) *AODV*

AODV stands for Ad-hoc On-Demand Distance Vector Routing. It establishes a route to a destination only on demand AODV is capable of both unicast, broadcast and multicast routing. AODV have some join feature of DSR and AODV.AODV avoids the counting to-infinity problem of other distance-vector protocols by using sequence numbers on route updates. AODV reacts relatively quickly to the topological changes in the network and updating only the hosts that may be affected by the change, using the RREQ message. Hello messages, be dependable for the route maintenance, are also imperfect so that they do not create unnecessary overhead in the network. The RREQ and RREP messages are responsible for the route discovery**.**The AODV protocol is basically flat routing protocol.In AODV routes established on demand and that destination sequence numbers are applied for find the latest route to the destination. The connection setup delay is lower. The AODV protocols are a loop free and avoid the counting to infinity problem. At most one route per destination maintain at each node [14] [15] [16].It can lead to heavy control overhead. In AODV there is an unnecessary bandwidth consumption.

B. *PROACTIVE OR TABLE DRIVEN*

In Proactive routing protocols every node store information in the form of tables and when any type of change accrue in network topology need to update these tables according to update. The node swaps topology information so they have route information any time when required. There is no route discovery delay associated with finding a new route. In proactive routing fixed cost generate, as normally greater than that of a reactive protocols. Proactive protocols Traditional distributed shortest-path protocols Based on periodic updates high routing overhead. Proactive routing protocols are DSDV (destination sequenced demand vector), OLSR (optimized link state routing protocols) [11] [12] [13].

a) *OLSR*

Optimized Link State routing protocol is a proactive link state routing protocol, which uses hello and topology control (TC) messages to discover and then disseminate link state information throughout the mobile ad-hoc network. Individual nodes utilize this topology information to work out next hop destinations for all nodes in the network using shortest hop forwarding paths. Being a proactive protocol, routes to all destinations within the network are known and maintain before using it. Having the routes available within the standard routing table can be useful for some systems and network applications as there is no route discovery delay associated with finding a new route. The routing operating cost generates, although commonly greater than that of a reactive protocol and does not increase with the number of routes being created. Being a link-state protocol, OLSR requires a reasonably large amount of bandwidth and CPU power to compute optimal paths inside the network [17] [18].

C. *HYBRID ROUTING PROTOCOLS*

Hybrid routing protocols combination of both reactive and proactive routing protocols. It was proposed to reduce the control overhead of proactive routing protocols and also decrease the latency caused by route discovery in reactive routing protocols. Hybrid routing protocols are ZRP (Zone routing protocol) and TORA (Temporarily Ordered Routing algorithm) [12] [13] [19].

IV. CATEGORIZING NETWORK ATTACKS

A. *EXTERNAL ATTACKS*

These types of attacks try to cause congestion in the network, denial of services (DoS), and advertising wrong routing information etc. External attacks prevent the network from normal communication and producing additional overhead to the network. External attacks can classify into two categories [27].

a) *PASSIVE ATTACKS*

MANETs are more susceptible to passive attacks. A passive attack does not alter the data transmitted within the network. But it includes the unauthorized "listening" to the network traffic or accumulates data from it. Passive attacker does not disrupt the operation of a routing protocol but attempts to discover the important information from routed traffic [27].

b) *ACTIVE ATTACKS*

Active attacks are very severe attacks on the network that prevent message flow between the nodes. However active attacks can be internal or external. These attacks generate unauthorized access to network that helps the attacker to make changes such as modification of packets, DoS, congestion etc. The active attacks are generally launched by compromised nodes or malicious nodes. Malicious nodes change the routing information by advertising itself as having shortest path to the destination [27].

B. *INTERNAL ATTACKS*

Internal attacks are directly leads to the attacks on nodes presents in network and links interface between them [27].

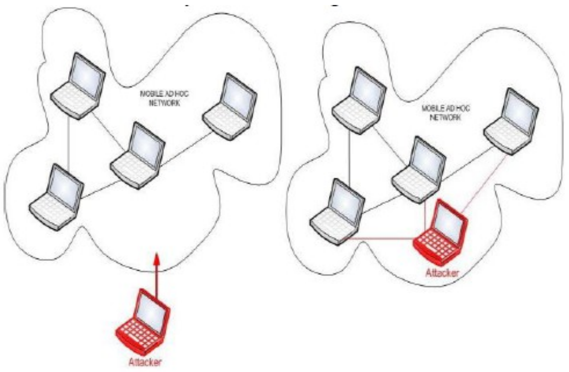

figure3; External and internal attacks in MANET

C. *WORMHOLE ATTACK*

Wormhole refers to an attack on MANET routing protocols in which colluding nodes create an illusion that two remote regions of a MANET are directly connected through nodes that appear to be neighbors but are actually distant from one another[4][22]. A wormhole attack is a particularly severe attack on MANET routing where two attackers, connected by a high speed off-channel link, are strategically placed at different ends of a network. In figure3 [23] node A sends RREQ to node B and nodes X and Y are malicious nodes having an out-of-band channel between them. Node X tunnel the RREQ to Y, which is legitimate neighbor of B. B gets two RREQ – A-X-Y-B and A-C-D-E-F-B. The first route is shorter and faster then the second, and chosen by B. Since the transmission between two nodes has relied on relay nodes, many routing protocols have been proposed for ad hoc network. The resulting route through the wormhole may have lower hop count than normal routes. In with this leverage, attackers using wormhole can easily manipulate the routing priority in MANET to perform eavesdropping, packet modification or perform a DOS attack. The entire routing system in MANET can even be brought down using the wormhole attack [23] [4].

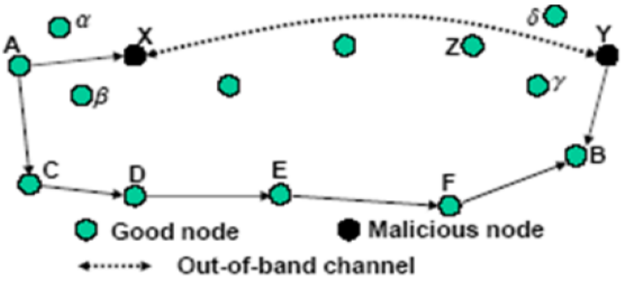

Figure4; The Wormhole attack in MANET

The other type of wormhole attack is known as in band wormhole attack [24]. In this type of attack the attacker builds an overlay tunnel over the existing wireless medium. This attack is potentially very much harmful and is the most preferred choice for the attacker.

D. *BLACK HOLE ATTACK*

In a black hole attack, a malicious node sends fake routing information, claiming that it has an optimum route and causes other good nodes to route data packets through the malicious one.For example, in AODV, the attacker can send a fake RREP (including a fake destination sequence number that is fabricated to be equal or higher than the one contained in the RREQ) to the source node, claiming that it has a sufficiently fresh route to the destination node. This causes the source node to select the route that passes through the attacker. Therefore, all traffic will be routed through the attacker, and therefore, the attacker can misuse or discard the traffic.

E. *FLOODING ATTACK*

The aim of the flooding attack [25] is to exhaust the network resources, such as bandwidth and to consume a node's resources, such as computational and battery power or to disrupt the routing operation to cause severe degradation in network performance. For example, in AODV protocol, a malicious node can send a large number of RREQs in a short period to a destination node that does not exist in the network. Because no one will reply to the RREQs, these RREQs will flood the whole network. As a result, all of the node battery power, as well as network bandwidth will be consumed and could lead to denial-of-service.

F. *LINK SPOOFING ATTACK*

In a link spoofing attack, a malicious node advertises fake links with non-neighbors to disrupt routing operations. For example, in the OLSR protocol, an attacker can advertise a fake link with a target's two-hop neighbors. This causes the target node to select the malicious node to be its MPR. As an MPR node, a malicious node can then manipulate data or routing traffic, for example, modifying or dropping the routing traffic or performing other types of DoS attacks. Figure 2 shows an example of the link spoofing attack in an OLSR MANET. In the figure, we assume that node A is the attacking node, and node T is the target to be attacked. Before the attack, both nodes A and B are MPRs for node T. During the link spoofing attack, node A advertises a fake link with node T's two-hop neighbor, that is, node D. According to the OLSR protocol, node T will select the malicious node A as its only MPR since node A is the minimum set that reaches node T's two-hop neighbors. By being node T's only MPR, node A can then drop or withhold the routing traffic generated by node T.

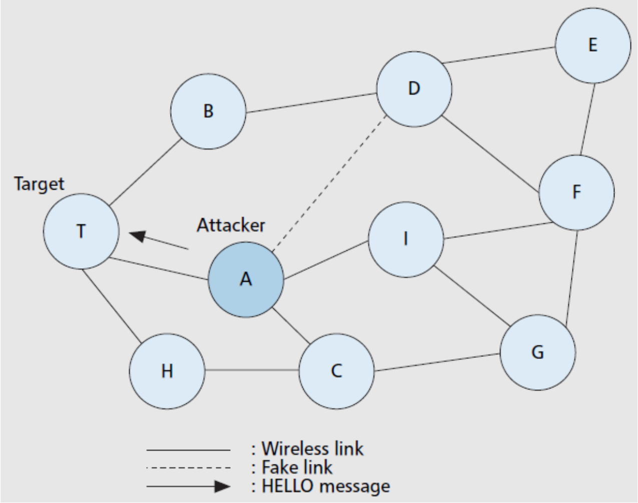

figure5; Example of Link Spoofing Attack on OLSR

G. *LINK WITHHOLDING ATTACK*

In this attack, a malicious node ignores the requirement to advertise the link of specific nodes or a group of nodes, which can result in link loss to these nodes. This type of attack is particularly serious in the OLSR protocol.

H. *REPLAY ATTACK*

In a MANET, topology frequently changes due to node mobility. This means that current network topology might not exist in the future. In a replay attack [26], a node records another node's valid control messages and resends them later. This causes other nodes to record their routing table with stale routes. Replay attack can be misused to impersonate a specific node or simply to disturb the routing operation in a MANET.

V. PROPOSED WORK

The objective is to find out the malicious node that performs the wormhole attack in network [1].

A. *ASSUMPTIONS*

A node interacts with its 1-hop neighbors directly and with other nodes via intermediate nodes using multi-hop packet forwarding. Every node has a unique id in the network, which is assigned to a new node by existing nodes.The entire network is geographically divided into a few disjoint or overlapping clusters. Each cluster is monitored by only one cluster head (monitoring node) [1].

VI. CONCLUSION

Wormhole attack refers to an attack on MANET routing protocols in which colliding nodes create an illusion that two remote regions of a MANET are directly connected through nodes that appear to be neighbors but are actually distant from one another. The wormhole attack is a particularly severe attack on MANET routing where two attackers connected by a high speed off-channel link, are strategically placed at different ends of a network. Study is done about various types of wormhole detection algorithms in MANET and a new algorithm for detecting a malicious node and various types of attacks in MANET by using AODV as routing protocol. Ns2.35 simulator is used for simulation and obtaining graphs. Wormhole attack affects the network performance which can be analyzed using various network parameters like total packets sent, total packets received, throughput and packet delivery fraction by the help of simulation and graphs etc. In future, the work can be extended by simulating the proposed protocol and comparing the effect of wormhole attack on various routing protocols in MANET. Other network parameters such as end to end delay in AODV protocol, packet drop rate can also be considered for comparison of performance of various routing protocols under this attack. In future other possible attacks such as black hole attack, rushing attack and their affects on network can also be considered.

REFERENCES

[1] Neha Rani, Vinay Rani," Detection and Performance Analysis of MANET under Wormhole Attack", International Journal of Enhanced Research in Science Technology & Engineering.

[2] Manju Ojha1, Rajendra Singh Kushwah2," Impact and Performance Analysis of Wormhole Attack on AODV in MANET using NS2", International Journal of Science and Research (IJSR).

[3] Richa gulati, Savita Shivani2,"Implementing Security algorithm to worm hole attack using AOMDV protocol & comparison using NS2 simulator**"**,IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 16, Issue 5, Ver. IV (Sep – Oct. 2014), PP 01-05.

[4] Jyoti Thalor,Ms.Monika," Wormhole Attack Detection and Prevention Technique in Mobile Ad Hoc Networks", A Review, International Journal of Advanced Research in Computer Science and Software Engineering.

[5] IRSHAD ULLAH SHOAIB UR REHMAN," Analysis of Black Hole Attack on MANETs Using Different MANET Routing Protocols", School of Computing Blekinge Institute of Technology Box 520 SE – 372 25 Ronneby Sweden.

[6] Harjeet Kaur, Varsha Sahni ,Dr. Manju Bala,"A Survey of Reactive, Proactive and Hybrid Routing Protocols in MANET",A Review", Harjeet Kaur et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 4 (3) , 2013, 498-500.

[7] Morigere Subramanya Bhat, Shwetha .D, Manjunath .D and DevarajuJ.T,"Scenario Based Study of on denmand Reactive Routing Protocol for IEEE-802.11 and 802.15.4 Standards", ISSN: 2249-57 Vol 1(2), 128-135 published in October-november 2011.

[8] Ashish Bagwari,Raman Jee,Pankaj Joshi,Sourabh Bisht, "Performance of AODV Routing Protocol with increasing the MANET Nodes and it's effects on QoS of Mobile Ad hoc Networks", 2012 International Conference on Communication Systems and Network Technologies.

[9] Xu Huang, Muhammad Ahmed and Dharmendra Sharm,"Protecting from Inside Attacks in Wireless Sensor Networks", 2011 Ninth IEEE International Conference on Dependable, Autonomic and Secure Computing.

[10] What is MANET http://manetattacks.blogspot.in/2012/10/what is manet. html .

[11] Morigere Subramanya Bhat, Shwetha .D, Manjunath .D and DevarajuJ.T,"Scenario Based Study of on denmand Reactive Routing Protocol for IEEE-802.11 and 802.15.4 Standards", ISSN: 2249-57 Vol 1(2), 128-135 published in October-november 2011.

[12] Naveen Bilandi and Harsh K Verma ,"Comparative Analysis of Reactive, Proactive and Hybrid Routing Protocols in MANET", International Journal of Electronics and Computer Science Engineering 1660 ISSN- 2277-1956.

[13] Rutvij H. Jhaveri, Sankita J. Patel and Devesh C. Jinwala ,"DoS Attacks in Mobile Ad-hoc Networks: A Survey", 2012 Second International Conference on Advanced Computing & Communication Technologies.

[14] Ashok M.Kanthe, Dina Simunic and Ramjee Prasad ,"Comparison of AODV and DSR on-Demand Routing Protocols in Mobile Ad hoc Networks".

[15] Prem Chand and M.K. Soni,"Performance comparison of AODV and DSR ON-Demand Routing protocols for Mobile ad-hoc networks", Published in July 2012.

[16] Michel Healy, Thomas News and Elfed Lewis, "Security for Wireless Sensors Networks", A Review".in Feb 2009.

[17] Harmandeep Singh, Gurpreet singh and Manpreet Singh, "Performance Evaluation of Mobile Ad Hoc Network Routing Protocols under Black Hole Attack",International Journal of Computer Applications (0975 – 8887) Volume 42– No.18, March 2012.

[18] Irshad Ullah Shoia Ur Rehman ,"Analysis of Black Hole Attack on MANETs Using Different MANET Routing Protocols",

[19] Fan-Hsun Tseng, Li-Der Chou and Han-Chieh Chao, "A survey of black hole attacks in wireless mobile ad hoc networks" ,Tseng et al. Humancentric Computing and Information Sciences 2011, a Springer open journal.

[20] P.V.Jani,"Security within Ad-Hoc Networks", Position Paper, PAMPAS Workshop, Sept. 16/17 2002.

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

[22] Viren Mahajan, Maitreya Natu, and Adarshpal Sethi, Nov. 2008, "Analysis of wormhole Intrusion Attacks In MANETS",IEEE Military Communications Conference,MILCOM 2008.

[23] R. S. Khainwar, A. Jain , J. P. Tyagi , Dec 2011 ,"Elimination of Wormhole Attacker Node in MANET Using Performance Evaluation Multipath Algorithm", *International Journal of Egineering Technology and Advanced Engineering*, Volume 1, Issue 2, pp. 40-47.

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

[25] P. Yi *et al.*, "A New Routing Attack in Mobile Ad Hoc Networks", *Int'l. J. Info. Tech.*, vol. 11, no. 2, 2005.

[26] C. Adjih, D. Raffo, and P. Muhlethaler, "Attacks Against OLSR: Distributed Key Management for Security",*2nd OLSR Interop/Wksp.*, Palaiseau, France, July 28–29, 2005.

[27] K. Sivakumar, M.Sc, MCA, M.Phil, (Ph.D). Assistant Professor, Dept of Comp Application, SNMV CAS, Cbe. Dr. G. Selvaraj, Professor, Dept of Comp. Sci & Engg, Oxford College of Engg, Thiruvannamalai," Analysis of Worm Hole Attack In MANET And Avoidance Using Robust Secure Routing Method", International Journal of Advanced Research in Computer Science and Software Engineering.

[28] Bounpadith Kanhavong, Hidehisa Nakayama, Yoshiaki Nemoto, And nei kato,tohoko University Abbas Jamalipour, University of sydney," A survey of routing attacks in mobile and ad hoc networks",security in wireless mobile ad hoc and sensor networks.