International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 02 Issue: 07 | Oct-2015 www.irjet.net p-ISSN: 2395-0072

Avoidance of Wormhole Attack by using Delphi method

Swaijit Kaushal [1], Reena Aggarwal[2]

[1] *M.Tech Student, ECE, Lovely Professional University, Punjab, India*
[2] *Assistant Professor, ECE, Lovely Professional University, Punjab, India*

Abstract - ***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. This paper provides the information about wormhole attack and explains how to provide security to the path of the packets by using Delphi method. By using delay per hop method, nodes which are the cause of wormhole attack can be isolated. With the help of hop count method and using the AODV routing protocol, the malicious node can be detected and a new path is formed to transfer the packets to their destination. In this way, packet loss problem can be reduced. The performance metrics used for evaluating network performance are packet loss, throughput and end to end delay. All the simulations are done in ns2.35.***

Key Words: *MANET, AODV, Wormhole and Delphi*

1. INTRODUCTION

With the rapid development in wireless technology, ad hoc networks have emerged in many forms. These networks operate in the license free frequency band and do not require any investment in infrastructure, making them attractive for military and selected commercial applications. However, there are many unsolved problems in ad hoc networks; securing the network being one of the major concerns. Ad hoc networks are vulnerable to attacks due to many reasons; amongst them are lack of secure boundaries, threats from compromised nodes inside the network, lack of centralized management facility, restricted power supply, scalability etc [1]. Network layer is the third lowest layer of OSI reference model. The function of network layer in OSI layer model is to provide the services for exchanging the individual piece of data/information over the network between identified end devices. The network layer in MANET uses ad hoc routing and does packet forwarding. In MANET nodes act as host and router. Therefore router discovery and router maintains in the MANET is effectively concern. Thus attacking on MANET routing protocol not only disrupt the communication on the network even worst it paralyzed the whole communication all over the network. Therefore, a security in network layer plays a vital role to ensure the secure data communication in the network [3]. The wormhole attack is one of the most dangerous and merciless attacks, which is present within network. In this attack two collaborating attackers establishes the so called wormhole link (using private high speed network e.g. over Ethernet cable or optical link) connection via a direct low latency communication link between two separated distant points within MANET. As soon as the direct bridge (wormhole link) is built up one of the attacker captures data exchange packets, sends them via the wormhole link to the second one and replays them.

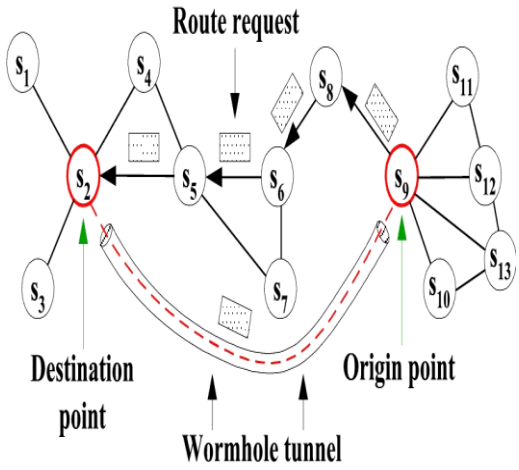

Fig 1: Wormhole Attack

In fig 1, wormhole attack, a tunnel is created between two nodes that can be used to secretly transmit packets. In a wormhole attack, an attacker receives packets at one point in the network, tunnels them to another point in the network and then replays them into the network from that point. For tunneled distances longer than the normal wireless transmission range of a single hop, it is simple for the attacker to make the tunneled packet arrive sooner than other packets transmitted over a normal multi hop route, for example through use of a single long range directional wireless link or through [2] a direct wired link to a colluding attacker. It is also possible for the attacker to forward each bit over the wormhole directly, without waiting for an entire packet to be received before beginning to tunnel the bits of the packet, in order to minimize delay introduced by the wormhole. If the attacker performs this tunneling honestly and reliably, no harm is done, the attacker actually provides a useful service in connecting the network more efficiently. When wormhole attack is used against an on demand routing

protocol such as DSR or AODV, a powerful application of the wormhole attack can be mounted by tunneling each ROUTE REQUEST packet directly to the destination target node of the REQUEST. When the destination node's neighbors hear this REQUEST packet, they will follow normal routing protocol processing to rebroadcast that copy of the REQUEST and then discard without processing all other received ROUTE REQUEST packets originating from this same Route Discovery.

1.1 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 [12] 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 [13] 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 [14].

1.2 Problem Statement

This section describes wormhole attack and problem statement. 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 [11] attack on MANET routing where two attackers connected by a high speed off-channel link, are strategically placed at different ends of a network. Inside and outside attacks are possible in MANET, which are responsible for the degradation of the performance of the network. In inside attacks a node within the network become malicious node and it launched attacks on network. In outside attacks a malicious node which is outside the network, it become the member of the networks and then launched the attack on network. In throughput sensitive wormhole attack, the packet is dropped so it cannot reach to destination and performance of the network is degraded. Packet Drop is detected using ICMP packet. By drop detection, the performance can be easily improved by using the mechanism of Delphi. Delay per hop is noticed in every path and it is provided that delay per hop for the best path is shorter than the wormhole path. If the path has noticeable high delay per hop, then the corresponding paths is affected by the wormhole attack.

2. METHODS TO HANDLE WORMOLE ATTACK

Distance & Location Based Packet Leash Technique Hu et al. proposed a mechanism, called packet leashes, whose goal is to limit the distance travelled by the packet in the network. There are two approaches to achieve this goal, one is a space based approach, called as Geographical Leashes which establishes an upper bound on the distance that a packet can travel. Before sending a packet, node appends its current position and transmission time to it. On receiving packet, receiving node computes the distance with respect to the sender and the time required by the packet to traverse the path. The receiver can use this distance information to deduce whether the received packet passed through a wormhole or not. The drawback of this scheme is that, each node must know its own location and all nodes must have loosely synchronized clocks. In Time based approach called as Temporal Leashes, the sending node includes in the packet the time at which it sends the packet, when receiving a packet, the receiving node compares this value to the time at which it received the packet. The receiver is thus able to detect if the packet traveled too far, based on the claimed transmission time and the speed of light. Alternatively, a temporal leash can be constructed by instead including in the packet an expiration time, after which the receiver should not accept the packet; based on the allowed maximum transmission distance and the speed of light, the sender sets this expiration time in the packet as an offset from the time at which it sends the packet. The drawback of this is that they need highly synchronized clocks [6]. In hop count method the hop count is the minimum number of node-to-node transmissions. This method uses protocol Delay per Hop Indicator (Delphi) [7] proposed by Hon Sun Chiu and King-Shan Lui, can detect both hidden and exposed wormhole attacks. In Delphi, attempts are made to determine every available disjoint route between a source and a destination. To identify wormhole, delay time and length of each route are measured and the average delay time per hop along each route is computed. According to this, the route containing a wormhole link will have a greater Delay per Hop (DPH) value. This mechanism can detect both modes of wormhole attack; however, pinpoint the location of a wormhole cannot be determined. Wormhole Geographic Distributed Detection is another model to detect the wormhole attack dependent on the existence of disorder in the network due to this attack is called “Wormhole Geographic Distributed Detection” [5] which was designed in 2008 by Xu. In this

model to detect wormhole attack is used hop-count technique Then, the local map is re-built finally; a method is utilized to identify the irregularity in the network which is named "diameter". The main advantage of using a distributed wormhole detection algorithm is that the proposed algorithm can approximately detect the location of a wormhole.

2.1 AODV in MANET

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 [11] 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 [8] [9] [10].It can lead to heavy control overhead. In AODV there is unnecessary bandwidth consumption. Much of the complexity of the protocol is to lower the number of messages to conserve the capacity of the network. For example, each request for a route has a sequence number. Nodes use this sequence number so that they do not repeat route requests that they have already passed on. The advantage of AODV is that it creates no extra traffic for communication along existing links. Also, distance vector routing is simple, and doesn't require much memory or calculation. However AODV requires more time to establish a connection, and the initial communication to establish a route is heavier than some other approaches.

2.2 Proposed Technique

Research methodologies for the proposed technique are related to the analysis of the misbehaving nodes which are responsible for the wormhole attacks in the MANET. Mainly in the Wormhole attack, traffics for the network are redirected to the mobile node in the network which not at all exists in the network. Thus in [1] this case the network traffic is redirected into one of the special mobile node such node is called as *wormhole node*. The wormhole attack has two characteristics: first one, the misbehaving node advertise itself regarding to the information that it has shortest route to the destination with the intention of dropping the packets or intercepting packets in the routing protocols like DSR, AODV. Intercepted [1] packets then consumed by the node: this is the second characteristics. The proposed technique is focused on the detection of the misbehaving nodes and tries to prevent doing wormhole attack on the network by preventing those nodes from the current routing paths and select the alternative path by again doing the route discovery procedure for the same. The technique is known as Delphi method. The advantage of Delphi is that it does not require clock synchronization and position information and it does not require the mobile nodes to be equipped with some special hardware, which in turn provide higher power efficient. The Disadvantage of Delphi method is it cannot pinpoint the wormhole location. This disadvantage of Delphi method can be overcome by using Wormhole Geographic Distributed Detection which is another method to detect the wormhole attack dependent on the existence of disorder in the network. The wireless ad hoc network is deployed in a fixed area and with the fixed number of nodes, the network deployed in decentralized in nature and each node is capable of moving freely from one to the other location. After deploying the wireless ad hoc network the path is established from source to the destination with the help of the AODV routing protocol. The source node floods the route request packets in the network for the path establishment to the destination and the adjacent nodes of the destination will reply back to the source node with the route reply packets After the sending of the route request packets and the route reply packets, the best path is selected from the paths for sending the packets from the source to the destination. The malicious node those exist in the path will trigger wormhole attack and are responsible to increase the delay between the source and destination. By calculating the delay per hop for each node existing in the path the malicious node is detected. After that the neighbor of each node is traced in the network and its distance from the source node is calculated. This helps to find out the location of the node responsible for the wormhole attack. Then the malicious node is removed from the network and new path is formed from the source to the destination to send the data packets. The graphs of throughput, energy loss, end to end delay and packet loss for both the scenarios, with and without the wormhole attack in the network are plotted. The result shows the great differences.

3. SIMULATION ENVIRONMENT

Simulation is a fundamental tool in the development of routing protocols, because the difficulty to deploy and debug them in real networks. The simulation eases the analyzing and the verification of the protocols, mainly in large-scale systems. Network Simulation is an event based

simulator. The network simulator is discrete event packet [1] level simulator. It covers a very large number of different kinds of protocols application of different types of applications and packets. In it scripting language is used. It contains "NAM" files through which animation is run. Front End- OTCL scripting language is used. Back End- Programming language is used. NS2 has different types of agents. In- built protocols are used in it like AODV, DSDV and DSR.

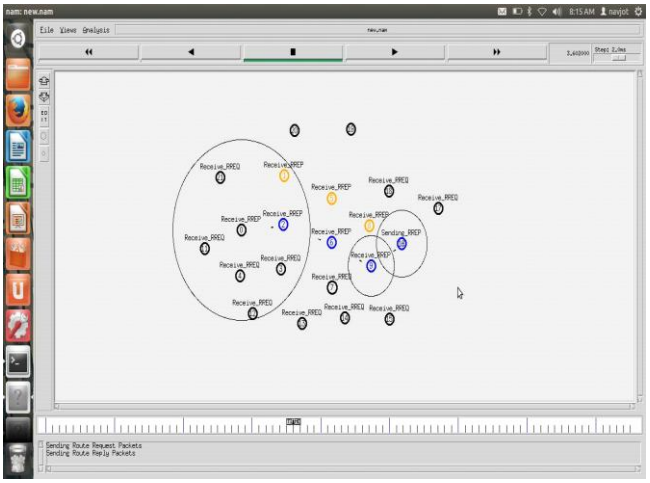

Fig 2: Path establishment

As shown in figure 2, the wireless ad-hoc network is deployed in the fixed area and with fixed number of nodes. The network is the decentralized type and nodes can move freely from one location to other location. The AODV routing protocol is used to establish path from source to destination. The source node flood route request packets in the network for path establishment to destination. The adjacent nodes of destination will reply back to source node with the route reply packets.

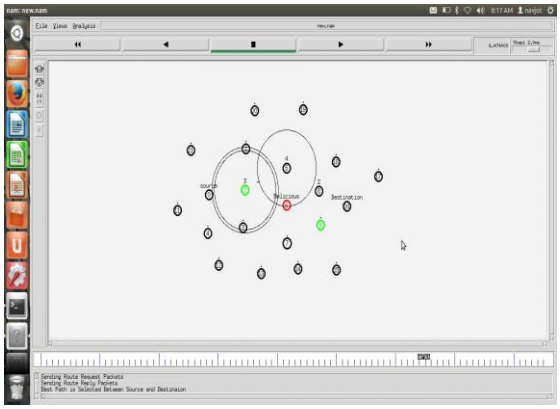

Fig 3: Isolation of attack

As shown in figure 3, the wireless ad-hoc network is deployed in the fixed area and with fixed number of nodes. The network is the decentralized type and nodes can move freely from one location to other location. The AODV routing protocol is used to establish path from source to destination. The source node flood route request packets in the network for path establishment to destination. The adjacent nodes of destination will reply back to source node with the route reply packets. The best path will be selected between source and destination. The malicious node exits in the path which will trigger wormhole attack and increase delay between source and destination. The delay in the established path will be increased and using the position used detection technique malicious node is detected and isolated from the network. The new path will be established between source and destination to send data packets.

4. RESULTS AND ANALYSIS

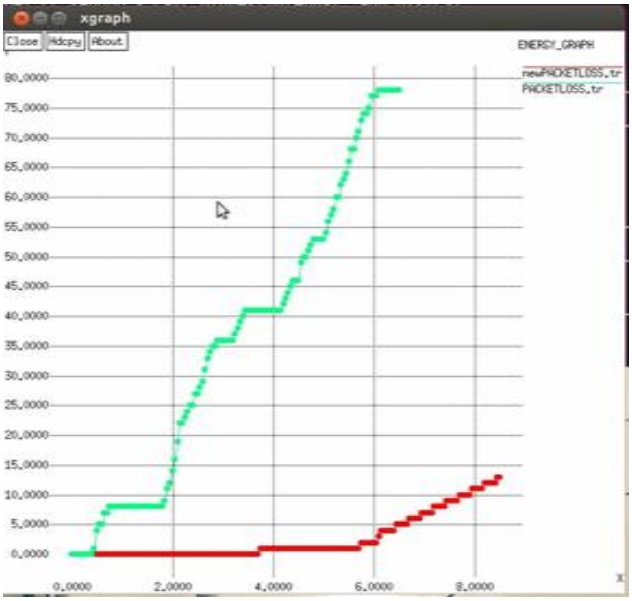

Fig 4: Packets loss graph

As illustrated in figure 4, the packet loss graph is shown in packet loss of attack scenario and packet loss in isolation scenario is shown. When the attack will be isolated from the network packet loss will be reduced.

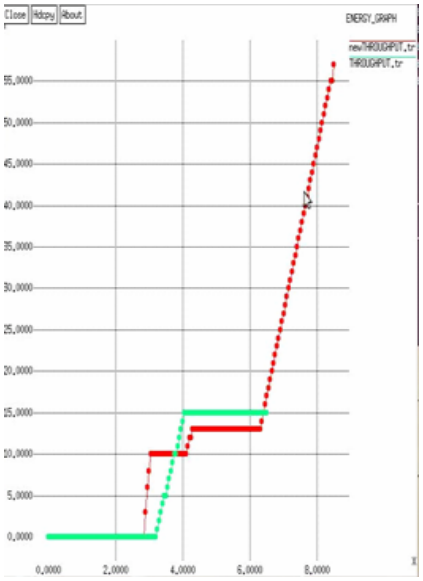

Fig 5: Throughput graph

As shown in figure 5, the throughput of attack scenario and isolated scenario is shown. When the attack will be isolated from the network throughput will be increased.

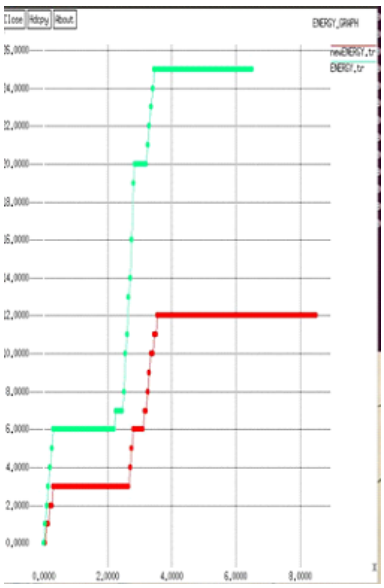

Fig 6: Delay graph

As illustrated in figure 6, the delay of the attack scenario and isolated scenario is shown. The delay in the attacked scenario will be increased and attack in the new scenario will be reduced.

5. CONCLUSIONS

The proposed study has broader scope. When the mobile nodes are mutually true, it leads to the reliable data transmission between the mobile nodes. But the main problem occurs during the drop of the packet. Drop of the packet is due to wormhole attack. Throughput sensitive wormhole attack is due to the drop of the packet. In this, malicious node drops the packet so that it cannot be reach destination. By using ICMP packets, nodes goes to the monitor mode. Here other nodes are also available than malicious nodes which detect the packet dropping and redirect them to the source node. So here low performance of system can be improved by prevent them from internal attacks i.e. by detecting packet dropping.

REFERENCES

[1] Yudhvir Singh," Wormhole Attack Avoidance Technique in Mobile Ad hoc Networks", 2013 Third International Conference on Advanced Computing & Communication Technologies.

[2] Donatas Sumyla, **"**Mobile Adhoc Networks**",** IEEE Personal Communications Magazine, April 2003, pp. 46-55.

[3] Amandeep Singh Bhatia and Rupinder Kaur Cheema, "Analysing and Implementing the Mobility over MANETS using Random Way Point Model" , International Journal of Computer Applications (0975 – 8887) Volume 68– No.17, April 2013.

[4] Priyanka Goyal, Vintra Parmar and Rahul Rishi , " MANET: Vulnerabilities, Challenges, Attacks, Application" , IJCEM International Journal of Computational Engineering & Management, Vol. 11, January 2011 ISSN (Online): 2230-7893 2011

[5] Dr. A.K Verma , " Mobile Adhoc Networks: An Introduction", 2003

[6] Karthikeyan U and Rajni ,"Security Issues Pertaining to Ad-Hoc Networks", 2004

[7] Safa RahimiMovaghar , "Introduction to MANET", Prentice Hall PTR, 2002

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

[9] 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.

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

[11] Swaijit Kaushal, Reena Aggarwal, "A Study of Different Types of Attacks in MANET and Performance Analysis of AODV Protocol Against Wormhole Attack", international journal of Advanced Research in Computer Science and Software Engineering.

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

[13] 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)

[14] 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.

[15] 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.

[16] 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.

[17] 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.

[18] Morigere Subramanya Bhatt, Shwetha .D, Manjunath .D and DevarajuJ.T,"Scenario Based Study of on demand 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.