International Journal of Engineering Research and Modern Education (IJERME)
Impact Factor: 6.525, ISSN (Online): 2455 - 4200
(www.rdmodernresearch.com) Volume 2, Issue 1, 2017

DETECTION MECHANISM OF WORMHOLE ATTACK USING ON DEMAND ROUTING SCHEME IN WIRELESS ENVIRONMENT

Upendra Kumar Purohit*, Umesh Barahdiya & Manoj Jakhenia*****
Electronics and Communication Engineering, Nagaji Institute of Technology and Management, Gwalior, Madhya Pradesh

Cite This Article: Upendra Kumar Purohit, Umesh Barahdiya & Manoj Jakhenia, "Detection Mechanism of Wormhole Attack Using on Demand Routing Scheme in Wireless Environment", International Journal of Engineering Research and Modern Education, Volume 2, Issue 1, Page Number 48-52, 2017.

Abstract:

Security is the one of the major issue that exists in Mobile Ad hoc network. Mobile Ad hoc network is infrastructure less network so it is vulnerable to several security attacks that are on different layers. Wormhole attack is one of the serious routing attack on network layer. This paper focuses on the wormhole attack. The application of multi-path techniques in wireless ad hoc networks is natural, as multi-path routing (MR) allows diminishing the effect of unreliable wireless links and the constantly changing network topology. In this paper we have used multipath scheme for detection and prevention of Wormhole attack. This approach is an improvement over the existing technique and the simulation results of proposed technique show better performance in comparison to the existing technique.

Key Words: MANETs, Wormhole Attack, Wormhole Detection Technique, AODV & NS-2

1. Introduction:

Mobile Ad hoc Network (MANET) has distributed mobile wireless nodes, which do not have pre-determine topology and pre-existing infrastructure mobile nodes that can arbitrarily change their geographic locations and random mobility with constrained resources, ad hoc networks are vulnerable due to their structure less property. Mobile Ad hoc Network (MANET) is used most commonly all around the world, because it has the ability to communicate with each other without any fixed network. A proper security solution is needed for networks to protect both route and data packet delivery operations in the network layer. Security is an essential requirement in MANET. The malicious node in the network act as a normal node, so there is a need of security solution to prevent from various attacks. Various security issues are present in Mobile Ad hoc networks [2]. Attacks are of two types:

Passive Attack - which does not destroy or disrupt network but uses the useful information, it violate confidentiality.

Active Attack - which steal, destroy, manipulate the useful information and as well as disrupt the operations of network. Wormhole attack and black hole attacks are active attacks. A Mobile Ad-Hoc Network (MANET) is a collection of wireless mobile nodes can form without using any

In this paper, we have discuss about worm hole attack. During the wormhole attack, a malicious node captures packets from one location in the network, and "tunnels" them to another malicious node at a distant point, which replays them locally. We identify two types of wormhole attacks. In the first type, malicious nodes do not take part in finding routes, meaning that, legitimate nodes do not know their existence. In the second type, malicious nodes do create route advertisements and legitimate nodes are aware of the existence of malicious nodes, just do not know they are malicious. Some researchers have proposed detection mechanisms for the first type. In this paper we represent a mechanism which is helpful for prevention of wormhole attack, through observing the delay of different path to receiver and verification of digital signature. Our mechanisms detect pinpoint location of wormhole and prevent them. This method requires neither synchronized clocks nor special hardware equipped mobile nodes. The rest of the paper begins with performance analysis of multi-path routing under wormhole attack. Because the results show that multi-path routing is vulnerable to wormhole attack, a statistical multipath aodv analysis proposed in Section 3 and extensive simulations are carried out to evaluate the effectiveness of the proposed scheme. And section 9 display the simulation graph with discussion and last section discussed about conclusion.

2. AODV:

The Ad Hoc On-Demand Distance Vector routing protocol [14] is an adaptation of the dynamic link conditions. 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 to send 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. Route Discovery process is initiated by broadcasting a Route Request (RREQ) packet

to its neighbors. Each neighboring node either responds the RREQ by sending a Route Reply (RREP) back to the source node or rebroadcasts the RREQ to its own neighbors after increasing the hop count field. If a node cannot respond by RREP, it keeps track of the routing information in order to implement the reverse path setup or forward path setup. The destination sequence number specifies the freshness of a route to the destination before it can be accepted by the source node. Eventually, a RREQ will arrive to node that possesses a fresh route to the destination. If the intermediate node has a route entry for the desired destination, it determines whether the route is fresh by comparing the destination sequence number in its route table entry with the destination sequence number in the RREQ received. The intermediate node can use its recorded route to respond to the RREQ by a RREP packet, only if, the RREQ's sequence number for the destination is greater than the recorded by the intermediate node. 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 a 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 destination sequence 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 packet, 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 [4-7].

Route Request (RREQ) Message: This type of message is used by AODV at first in order to locate a destination; this message contains identification of request, sequence number, destination address and also a count of hop initialed by zero.

Route Reply (RREP) Message First: This type of message contains the same fields like Route Request (RREQ) Message, and it sent in the same route of reception of RREQ message. When the source received this message it means that the destination is ready to accept information and the rout is working correctly.

Route Error (RERR) Message: Sometimes a node detect a destination node that not exists in network, in this scenario another message (Route Error RERR) is sent to the source informing that the data is not received. RERR is like an alert message used to secure table of routing.

In link breakage to the next hop is detected by the absence of hello messages in the allowed time interval (or with any of the methods above). The routes affected by the link breakage in the routing table are invalidated and the nodes affected by the link breakage are notified using RERR messages. If the link breakage occurs on an active route, a local repair mechanism can be initiated. In this mechanism new RREQ messages are broadcast to the destination by nodes on the existing route who detect the link breakage.

3. Multipath AODV:

Ad hoc On-demand Distance Vector Routing protocol, which was issued as RFC by the IETF MANET working group, is one of the most popular routing protocols for MANETs. Like other MANET routing protocols, AODV support single path. In this algorithm used Multiple Route Discovery Procedure is the process by which multiple paths are discovered. One observation of AODV is that, though the source actually discovers multiple paths during the route discovery process, it chooses only the best route and discards the rest. Also, frequent route breaks cause the intermediate nodes to drop packets because no alternate path to the destination is available. This reduces the overall throughput and the packet delivery ratio by using this methodology to efficient data delivered and solve out link break problem. The multipath process shown in figure in below:

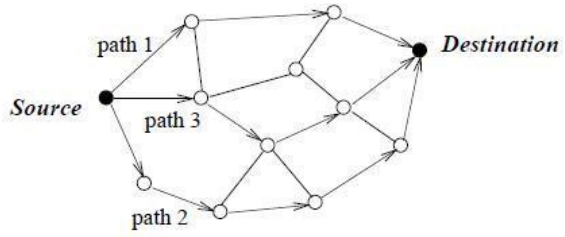
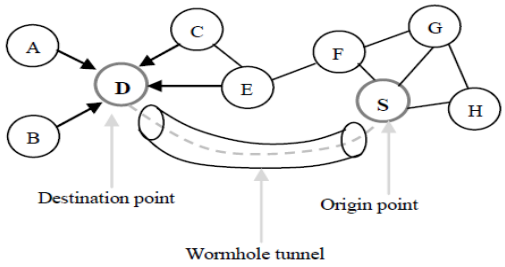


Figure 1: Multiple path using data transmission in Ad-hoc Network

4. Wormhole Attack:

Worm Hole attack consist of two nodes the attacker nodes that are connected to each other with a link basically this link is known as tunnel. The attacker node present in the network at one side captures the packet from the legitimate node and encapsulate the packet and with the help of tunnel transmit it to the other attacker

node or malicious node present in the network. It consists of one or two malicious nodes and a tunnel between them. Wormhole nodes fake a route that is shorter than the original one within the network means it create illusion for the legitimate node so they believe that the route is shorter than the original one. But it is not necessary that the route through wormhole nodes may be shorter. Figure 1 shows example of wormhole [1]. In given Figure 1, here we have two malicious nodes. A wormhole attack is consisting of two attackers and a tunnel through which the data is transmitted. For creating the wormhole attack the attacker creates a direct link referred as wormhole tunnel. The network which is caused by wormhole attack is depicted in Figure. In wormhole attack [1], an attacker connects two distant points in the network, and then replays them into the network from that point. An example is shown in Fig. 2. Here and are the two end-points of the wormhole link (called as wormholes). In Fig. 2, wormhole attack is assumed between the node and node and their neighbor nodes, vice versa. The wormhole link can be established by many types such as by using ethernet cables, long-range wireless transmissions and an optical link in wired medium. Wormhole attack records packets at one end-point in the network and tunnels them to other end-point [2]. These attacks are severe threats to MANET routing protocols. For example, when a wormhole attack is used against an on-demand routing protocol such as AODV/ DSR, the attack could prevent the discovery of any routes other than through the wormhole.



Algorithm: RREQ packet forwarding and Wormhole attack avoidance
Step 1: The sender node initiates a route discovery by flooding the RREQ packets within the cluster.
Step 2; The cluster head of this cluster that the sender belongs to, receives the packet.
Step 3: The Cluster head extracts the source and destination addresses from the packet, and identify the mode of communication. If (mismatch occurs) then
Step 4: The cluster head sends the packet to the address specified in the Next Hop address.
Step 5: Repeat step – 3 to 4 until the packet reaches the destination.
Step 6: After the destination receives a RREQ packets, it can drop the packets if it came through a Wormhole link as follows:

- It first extracts the source and the destination address from the packet.
- Starts matching the two addresses and take the decision as follows:

Step 8: After this the receiver sends a RREP packet through the valid reverse path contained in the packet which has come through the valid path.
Step 9: After the sender receives the RREP packet, a link is established between the sender and the receiver through the path contained in the RREP packet and then the data transmission continuous using the path.
Step 10: End.

5. Related Work:

In this paper study and performance about wormhole attack. In wormhole, an attacker creates a tunnel between two points in the network and creates direct connection between them as they are directly connected. An example is shown in Figure. 1. Here S and D are the two end-points in the wormhole tunnel. S is the source node and D is the destination node. Node S is assuming that there is direct connection to node S so node D will start transmission using tunnel created by the attacker .This tunnel can be created by number of ways including long-range wireless transmission, With the help an Ethernet cable or using a long-range wireless transmission .Wormhole attacker records packets at one end in the network and tunnels them to other end-point in the network. This attack compromise the security of networks For example, when a wormhole attack is used against AODV, than all the packets will be transmitted through this tunnel and no other route will be discovered. If the tunnel is create honestly and reliably than it is not harmful to the network and will provides the useful service in connecting the network more efficiently. A potential solution is to avoid wormhole attack is to integrate the prevention methods into intrusion detection system but it is difficult to isolate the attacker using only software based approach because the packets sent by the wormhole are similar to the packets sent by legitimate nodes [9].on-demand routing protocol (AODV) is being used in dynamic wireless ad hoc networks, a new route will be discovered in response to every route break [10]. The route discovery requires high overhead. This overhead can be reduced if there are multiple paths and new route discovery is required only in the situation when all paths break. The application of multi-path techniques in wireless ad hoc networks is advantageous because multi-path routing provides means to combat the effect of unreliable wireless links and constantly changing network topology. In this paper, the performance of multi-path routing under wormhole attack is studied in both cluster

and uniform network topologies. Because multi-path routing is vulnerable to wormhole attacks, a scheme called Analysis of Multi-path is proposed to detect such attacks and to identify malicious nodes. Simulation results demonstrate that successfully detects wormhole attacks and locates the malicious nodes in networks. It remove the effect of wormhole attack in the wireless network by using alternative path algorithm this algorithm is known as multipath AODV [4, 6, 8, 12].

6. Simulation Parameters:

Simulation Parameters is as follows

Table-1

Parameters	Value
Simulator	NS-2.31
Routing protocol	AODV with and Without Worm hole Attack, Improved Aodv
Number of Nodes	20
Area	1200mx800m(Constant)
Packet size	512 byte
Simulation time	100s (Constant)
Pause time	1.0s to 5.0s(Variation)
Traffic type	CBR
Mac protocol	Mac/802.11
Maximum Speed	10 m/s (Constant)
Propagation model	TwoRayGround

7. Performance Metrices [5-9]:

We report performance metrics for the protocols:

Packet Delivery Ratio (Fraction) - It is calculated by dividing the number of packet received by destination through the number packet originated from source**.**

$$PDF = (Pr/Ps)$$

Where Pr is total Packet received and Ps is the total Packet sent.

Average End to End Delay - It is defined as the time taken for a data packet to be transmitted across an MANET from source to destination.

$$D = (Tr - Ts)$$

Where Tr is receive Time and Ts is sent Time.

Normalized Routing Overhead - It can also be defined as the ratio of routed packets to data transmissions in a single simulation. It is the routing overload per unit data delivered successfully to the destination node

8. Simulation Model:

The IEEE802.11 Distributed Coordination Function is used as a Medium Access Control (MAC) protocol. The mobility model uses the random way point model. Nodes move randomly within the field. A node starts its journey from a random location to a random destination at a randomly chosen speed. After it reaches its destination, another random destination is targeted after a pause. The author considered the case of continuous mobility (no pauses). To change node mobility, the author varies the maximum speed. Simulation environment consists of an area of 1200x800, where randomly 50 mobile nodes are placed. A source and a destination are selected randomly. Data sources generate data according to Constant bit rate (CBR) traffic pattern. Source destination pairs are spread randomly over the network. A packet size of 512 bytes is used. Mobility pattern of the mobile nodes is generated using Random waypoint model. A mobile selects another node in the network and constantly moves towards it at a given velocity. Once it reaches there, it waits for some pause time and selects another node and again starts moving. By observing the performance of the network under mobility we can test the stability of design in real time scenario with varying speed. Data rate of 2Mbps is used [2- 9].

9. Simulation Results Analysis:

In this section present the simulation results demonstrating the effectiveness of our algorithm in detecting wormhole attacks have been presented. The proposed method has been implemented in NS 2. and the experimental performance analysis are presented. In this section analyzed the performance under the effect of wormhole attack in the AODV routing scheme .we are simulating and analyzing the impact variation of under the wormhole attack on Ad Hoc On-Demand instance Vector routing. These overall performance metrics show with variation of maximum speed mobility.

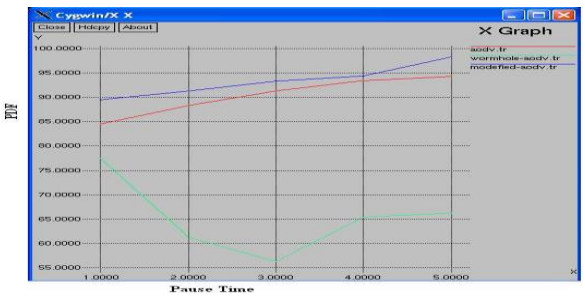


Figure: PDF V/s Maximum Speed

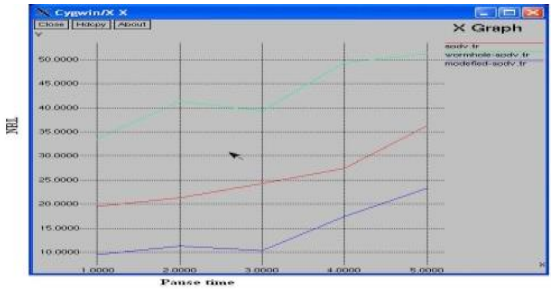


Figure: NRL V/s Maximum Speed

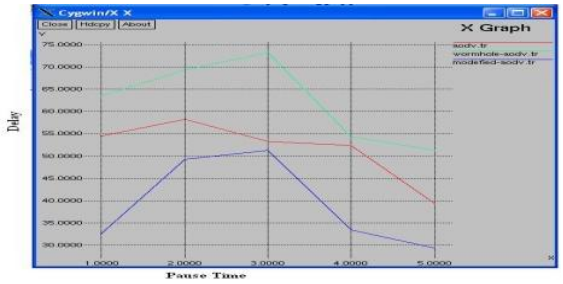


Figure: Average End to End Delay V/s Maximum Speed

When normal communication is taking place, initially the packet received, while during attack, node around which tunnel was created could not proper receive packet so resulting PDF is low compare than existing routing protocol further after detection and prevention when an alternate path is provided, again PDF value became high. The overall performance display by using X graph. In this section display the results of comparison worm hole attack aodv and Multpath AODV have done and variation shows in graph.

10. Conclusion:

In this paper, we present an efficient mechanism MANETs is insecure and vulnerable to various attacks so it require a reliable, efficient and a secure protocol that can be rapidly deployed and use dynamic routing. AODV is prone to various attacks like modification in the sequence numbers or hop counts, source route tunneling, spoofing and fabrication in the error messages. Wormhole attack is a real threat against AODV protocol in MANET. Wormhole attack can be easily launched even in networks with provides confidentiality and authenticity. The malicious nodes usually target the routing control messages related to routing information. Therefore trustworthy techniques for detection and prevention of wormhole attack should be used. Some existing solutions cannot work well in the presence of more than one malicious node, while some other requires special hardware. So, there is still a lot of scope of research to provide security to the MANETs. describes the effect of wormhole attack on the various performance parameters. Hence we can conclude that the security against wormhole attack is a challenging task as multipath aodv techniques have been used for removed this problem. The proposed multipath scheme is best effort for solve out this problem and resulting performance metrics.

11. References:

1. Elizabeth M. Royer, and Chai-Keong Toh, "A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks," IEEE Personal Communications, pp. 46-55, April 1999.
2. Charles E. Perkins, (2001) Ad Hoc Networking, Addison-Wesley, Pearson edu.
3. Hongmei Deng & Wei Li, Dharma P. Agarwal (2002) "Routing security in wireless ad hoc networks",University of Cincinnati, IEEE Communications magazine, Vol. 40, No. 10.
4. Radhika Saini, Manju Khari, "Defining Malicious BehavIor of Node and its Defensive Methods in Ad hoc network" International jurnal of Computer Applications(0975-8887) Volume 20- No.4, April 2011.
5. Reshmi Maulik and Nabendu Chaki,"A Study on Wormhole Attacks in MANET" International journal of Computer Information Systems and Industrial Management Applications ISSN 2150-7988 Volume 3 (2011) pp. 271-279.
6. J. Biswas, A. Gupta and D. Singh, "WADP: A Wormhole Attack Detection and Prevention Technique in MANET using Modified AODV routing Protocol", 9th International Conference on Industrial and Information Systems (ICIIS), (2014).
7. P. Sharma, H. P. Sinha and A. Bindal, "A Review on Prevention of Wormhole Attack in Mobile Ad-hoc Network ", International Journal of Research in Information Technology, vol. 2, no. 3, (2014) March.
8. Z. Kasiran and J. Mohamad, "Throughput performance Analysis of the Wormhole and Sybil Attack in AODV", Fourth International Conference on Digital Information and Communication Technology and its Application Publication, (2014), pp. 81 – 84.
9. R. Maulik and N. Chaki," A comprehensive Review on Wormhole Attacks in MANET", in proceeding of 9th International Conference on Computer Information Systems and Industrial Management Applications, (2010), pp. 233-238.
10. Shobha Arya and Chandrakala Arya, "Malicious Node Detection in Mobile Ad- Hoc Networks", Journal of Information Operations Management, Vol. 3, pp- 210-212, ISSN: 0976-7754, January 2012.
11. Hu Y.-C., Johnson D. B. and Perrig A. SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks, In IEEE Workshop on Mobile Computing Systems and Applications (WMCSA), pp. 3–13 (2002).
12. S Upadhyay and B.K Chaurasia. Impact of Wormhole Attacks on MANETs, International Journal of Computer Science & Emerging Technologies, Vol. 2, Issue 1, pp. 77-82 (2011)