An Enhanced AODV Protocol for Removal of Wormhole Attack in MANET

Shivani Pawar[1], Harsh Goud[2]
[1] M.Tec Scholar, ECE Department, Institute of Engineering & Science IPS Academy, Indore
[2]Asst. Professor, ECE Department, Institute of Engineering & Science IPS Academy, Indore

Abstract- *Mobile Ad hoc Networks (MANETs) are lying down to a variety of attacks due to their rare characteristics like dynamic topology, open wireless medium, multi hop nature, resource constraints and absence of infrastructure. In MANET, a node appears not only as an end terminal but both as router and client. Hence, in MANETs multi-hop communication occurs and thus it becomes much more difficult task to set up a secure path between the source and destination. The objective of this work is to overcome a unique kind of attack called wormhole attack lofted by at least two colluding nodes within a network. This research paper work is carried out in Network Simulator (NS-2) to detect and remove wormhole attack in MANET. Wormhole attack detection and prevention algorithm has been implemented in modified AODV. Node verification has been used to detect malicious nodes and remove false positive problem that may arise in WADP algorithm. It also helps in mapping exact location of wormhole and is a kind of double verification for wormhole attack detection. Simulation results proves the theory.*

Keywords- MANET, AODV, Wormhole Attack Network Security, IDS.

I. INTRODUCTION

Mobile Ad-hoc network (MANET) that is a self-configuring network of mobile nodes connected by wireless links is considered as system without communication links. Routing protocol plays a critical role for efficient message between mobile nodes and functions on the basic supposition that nodes are fully supportive There are many routing attacks caused due to lack of security. One of the routing attack that will be addressed is the worm hole attack. In Worm hole attack a malicious node presents itself as it is having the smallest pathway to the destination. In MANETs, the nodes are free to move randomly and organize themselves randomly. In MANET, network's wireless topology may change rapidly and unpredictably. MANETs are generally setup in conditions of emergency for provisional operations. These types of networks function in the deficiency of any fixed communications, which makes them effortless to setup [1].The capability of self-configuration of these nodes makes them more apposite for urgently required network association. Extensive explore work in this area is evolved with main studies on diverse routing protocols such as Ad hoc On-demand Distance Vector (AODV), Dynamic Source Routing, Optimized Link State Routing and GRP.

In an Ad-hoc network, Networks are organizing on-the-fly, devices can permit to leave and join the network during its lifetime. Wireless devices communicate directly with devices inside their radio range in a peer-to-peer network topology. If they wish to communicate with a device which is outside of their range, Ad-hoc network can use a midway device or intermediate devices within their radio range to forward communications. Ad-hoc On-Demand Distance Vector (AODV) is one of the most common ad-hoc routing protocols used for mobile ad-hoc networks. AODV is an on-demand routing protocol that discovers a route only when there is a demand of data transfer exist for mobile nodes. In AODV routing protocol, a source mobile node, first transmits an RREQ (Route Request) message to find a fresh route to a desired target mobile node. If a mobile node discovers a fresh enough route, then the destination node uncast an RREP (Route Reply) message back along the saved path to the source mobile node or it otherwise re-broadcasts the RREQ message in Ad-Hoc network [2].

A spiteful node in the network receiving an RREQ message replies to the source nodes by sending a false RREP message that contains attractive parameters to be selected for packet delivery to destination nodes. After talented (by sending a fake RREP to validate it has a path to a purpose node) to source nodes that has an actual path to forward data, a malicious node starts to lose all the network traffic it receives from source nodes. Some active attacks that can be easily performed against MANETs are wormhole attack [3].

We propose a solution that is an enhancement of the basic AODV routing protocol, which will be capable to avoid worm holes. To reduce the probability of wormhole, we develop a IDS (Intrusion detection system) based methodology to identify worm-hole node [2]. The method works with to some extent modified AODV protocol give the method of preventing wormhole attack by using IDS algorithm. hole and find safe route to reach the neighboring nodes.

II. LITERATURE SURVEY

This section involves the different research efforts and the techniques that are as, Distance and location Based Packet Leash Technique, Special Hardware Based Approaches, and Hop-count, also, Analysis Technique & Neighbor node monitoring technique

Distance and location Based Packet Leash Technique [6]: Many methods were proposed using a packet leash technique for the detection of the wormhole attack. The packet leash (Yih -Chun Hu et.al, 2003) is a method that defends against wormhole attack. In this paper, a mechanism of packet leashes has been introduced for wormhole attack detection. Here two kind of leashes have been presented one is geographical and the other one is temporal leash. A geographical leash ensures that the recipient of packet is within a certain distance from the sender. It requires a loosely synchronized clock when sending packet. The sending mode includes its own location and time of sending. The receiver node compares this value to its own location and the time at which it received the packet. In the temporal approach, an upper bound is kept on the packet's lifetime which restricts the maximum travel distance of the packet. Here all the nodes must have a tightly synchronized clock. An expiration time in the packet is included after which the receiver does not accepts the packet any more.

Special Hardware Based Approaches: In [4], a method was suggested in which mobile nodes are equipped with special directional antennas to defend against wormholes. Their assumption is that if there is no wormhole attack and if one node sends packets in a given direction, then its neighbor will get that packet from the opposite direction. The neighboring nodes examine the directions of the signals received from each other with a shared witness. Only when the directions of both pairs match, the neighboring relation is confirmed. Disadvantages of using directional antenna are each node is to be equipped with the special hardware. This method does not prevent multiple endpoint attacks. Directional errors are possible in this method.

Hop-count Analysis Technique: In [5] author describes an end to end detection of wormhole attack (EDWA) in wireless ad hoc network has been proposed. This approach consists of three phases. In first phase a location based end to end detection is done. Here wormhole detection by the source is done based on smallest hop count estimation between source and destination. If the hop count of the received shortest route is much smaller than the estimated hop count, then a wormhole is detected and source node raises an alert message to other nodes about the existence of wormhole. In second phase identification of wormhole is done. Here source node confirms the end points of the wormhole by a TRACKING procedure provided there are multipath existing between source and destination. Once the endpoints are identified, the results are broadcasted into the network to warn the other nodes about the malicious nodes. Finally in the last phase, a genuine route is selected for data communication which is legitimate and free from the presence of wormhole. Thus, this approach is both detection and identification method where there are no special hardware requirements and no need of clock synchronizations. But, this proposed method is effective only when the source and destination are not too far away.

Neighbor node monitoring technique: In this paper [6] every node collects information about their one hop and two hop neighbors. When a node receives a packet from its one hop neighbor and the one hop neighbor did not received the packet from its one hop neighbor, shows that the route might be suffering from a wormhole. Another approach [7] presents an effective method called wormhole attack prevention (WAP) without using any hardware and location information of time synchronization. It can detect both hidden and exposed attacks. Here, all nodes monitor their neighbor's behavior when they send route request messages to destination by using their neighbor list. The information of wormhole is stored at the source node to prevent them from taking part in routing again. For neighbor node monitoring, when a node sends RREQ, it starts the wormhole prevention timer (WPT), it also records the RREQ sequence number and sending time. Then on overhearing a RREQ from neighbor node, it records the neighbor node's address and time of receiving the packet. If node overhears RREQ after WPT, it considers that the neighbor node sending route request as affected by wormhole and increases its count value by one. In case of the exposed ones, where malicious nodes acts like legitimate, it is difficult to detect wormhole route by using only neighbor node monitoring scheme. In this case the source node calculates time delay per hop in the route using route reply packet.

III. MOBILE AD HOC NETWORK (MANET)

MANET often is affected from imprecise security attacks because of its features like autonomous and infrastructure-less, dynamic network topology, multi-hop routing, limited physical security, supportive algorithms and unclear mechanism. In the previous few years, various researchers have studied performance of Ad-Hoc in terms of Packet Delivery Ratio, End-to-End Delay, throughput, energy, within wireless mobile networks[7]. Due to the specific issues related to wireless ad hoc networks, it is expected that the

performance of AODV will be affected considerably in these environments.

Wireless links also make the MANET more susceptible to attacks which make it easier for the attacker node to go inside the network and get access to the ongoing message or communication. These challenges in authorized access, securing the important data and improving the performance of communication in Ad-Hoc network that can open new approaches and solutions. One such active interruption attack in MANET on-demand routing protocol is the worm hole attack, in which, the source node ignores the RREP packet received from other nodes and begins to send the data packets through the malicious node. Thus, the nasty or malicious node takes every route going towards itself. It does not allow forwarding of any packet anywhere. This attacker node is called a worm hole[5]. Worm hole attack may be attained by a single node or more than one node which can collaboratively perform the attack. Thus, security features must be incorporated in the on-demand routing protocols to mitigate the wormhole attack. These challenges in securing the information and improving the performance of communication in Ad-Hoc network can open new approaches and solutions.

Short comings of MANET

Some of the disadvantages of MANETs are as follows:

- Limited Resources
- Scalability problems
- No central check on the network.
- Dynamic topology, where it is hard to find out malicious nodes

IV. PROBLEM DOMAIN & METHODOLOGY

The main aim of this research is to develop secure on-demand routing protocols for data transmission under Worm Hole attack in MANET. The proposed protocols must be efficient in terms of Packet Delivery Ratio, End-to-End Delay Throughput and Energy. Based on the motivations to provide new security features to be incorporated in popular routing protocols AODV, the aim has been further segregated down into a number of objectives:

1. Implement secure on-demand routing (TAODV) protocols for data transmission in MANET.
2. Detect worm hole node in MANET scenario using TAODV protocol.
3. Prevent the network from worm hole attack and improve the packet delivery fraction, throughput, energy and end-to-end delay, even with the presence of worm hole attacks.
4. The results of both AODV and TAODV compare to analyze which of these two types of protocols gives better performance.

Problem Statement

In this work we focus our attention to one special active attack called wormhole attack. In wormhole attack the router will advertise in the network that it has a fresh route to the destination and after that may drop all the packets that it receives. Here, Intermediate nodes can lead to inconsistent , If the source sequence number is old and intermediate node have value higher than a source node then malicious node take advantage of this high sequence number and sending fake Route reply to the source without having actual route and drops all the receiving packets. It gives serious damage. In wormhole attack, a specific malicious node which does not exist in the network, redirected all network traffics. Because traffics disappear into the special node as if the matter disappears into Wormhole in universe.

Proposed Methodology

Mobile Ad-hoc Network consists of some nodes that are standing randomly in operational environment without any predefined infrastructure and mobility which are vulnerable for intrusion and attack. Security is an important field in this type of network. Use IDS (intrusion detection system) based approach to detect and prevent Worm hole in MANET. In ad-hoc network IDS detect and report the malicious activity. Intrusion detection systems (IDSs) do just that: monitor audit data, look for intrusions to the system, and initiate a proper response.

V. PROPOSED ALGORITHM

The proposed algorithm is based on the trust values of individual nodes. All the nodes of wireless ad-hoc network have a specific trust value. The algorithm encompasses the following steps:

[A] Initialization:

1. By specific previously assigned trust value, initialization of trust values of all the participating nodes is achieved.
2. Initialize the trust value of every node with 100.
3. Postulation: 1 trust value = 10 packets dropped.

[B] Updating of trust values:

1. If the packets are correctly transmitted from one node to another node:

(a) If the no. of packets correctly transmitted is between 1 and 10, then trust values of the respective nodes will be incremented by one.
Updated trust value = out dated trust value + 1;

(b) If the correctly transmitted number of packets is greater than 10,then the updated trust value will be:
Updated trust value = out dated trust value + (correctly transmitted packets / 10);

2. If the packets are dropped/delayed :
   (a) If the number of packets dropped or delayed is between 1 and 10,then the trust value of that respective nodes will be decremented by one.
   Updated trust value = out dated trust value – 1;
   (b) If the numbers of dropped or delayed packets are greater than 10, then trust value of that particular node will be,
   Updated trust value = out dated trust value – (Packet dropped or delayed / 10);
   (c) Isolating the Packet drop node from the network:
3. If the trust value of particular node is negative, then print "Invalid node".

1. If (Updated trust value < Threshold trust value)
   Then the particular node is treated as malicious node (Worm hole node)
2. If (Updated trust value > Threshold trust value)
   Then the particular node is treated as authenticated node.

Stop comparing the trust values of nodes with threshold

VI. RESULT ANALYSIS

A. Simulation Environment

This section is the major portion of the thesis, it is important to setup simulation environment to observer protocols behavior over MANET. Quantitative analysis is conducted to with the help of NS-2 tool.

B. Simulation Parameter

Table 1: Simulation Parameter

Simulation tool	Network simulator-2.35
IEEE scenario	MANET(802.11)
Mobility model	Two ray ground
Number of nodes	20,40,60
Node movement speed	10m/sec,28m/sec.
Traffic type	UDP
Antenna	Omni direction antenna
MAC Layer	IEEE 802.11
Routing Protocol	AODV,WAODV,TAODV
Queue limit	50 packet
Simulation area(in meter)	1000*1000
Queue type	Drop-tail

C. Performance Metrics

'The following metrics are used in this work for the detection and prevention of the Worm-hole attack with AODV routing protocol.

1) *Packet Delivery Ratio*: This is the fraction of the data packets received by the destination to those sent by the source. This classifies the ability of the protocol to discover routes.
2) *End to End Delay*: This is the mean delay between the sending of the data packet by the source and its receipt at the corresponding receiver. This includes all the delays caused during route acquisition, buffering and processing at intermediate nodes.
3) *Residual Energy*: It is the total amount of remaining energy by the nodes after the completion of Communication or simulation. If a node is having 100% energy initially and having 70% energy after the simulation than the energy consumption by that node is 30%.The unit of it will be in Joules.
4) *Throughput*: Throughput is the ratio of the total amount of data that reaches a receiver from a sender to the time it takes for the receiver to get the last packet. It is expressed in bits per second or packets per second. Factors that affect throughput in MANETs include frequent topology changes, unreliable communication, limited bandwidth and limited energy. A high throughput network is desirable.

D. Implementation and Result Analysis

In this work, the random way point mobility model is used for the simulation of MANET routing protocols. The source-destination pairs are spread randomly over the network where the point to point link is established between them. In this work UDP agent along CBR traffic, with 40 packet size and 10kbps rate is used for the transmission. The simulation configuration for mobile nodes consists of many network components and simulation parameters that are shown in the table in detail. Generally network simulators try to model the real world networks. The principle idea is that if a system can

be modeled, then futures of the model can be changed and the corresponding results can be analyzed.

Table 2: Packet Delivery Ratios Comparisons

No. of node	Attack	Pre	Without
20node	0	99.75	99.08
40node	0	99.63	99.57
60node	0	98.94	98.71

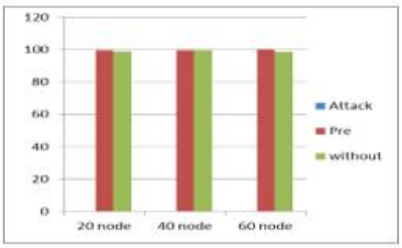

Figure 1: Packet Delivery Ratios comparisons

1) *Simulation results for Packet Delivery Ratio:* This is the fraction of the data packets received by the destination to those sent by the source. This classifies the ability of the protocol to discover routes. Figure and table shows the Packet delivery ratio under Worm hole attack detection and its prevention through Trust based mechanism i.e. AODV, WAODV and TAODV for the various node densities it is shown in figure 1 and table 2.

2) *Simulation results for Throughput:* This is the fraction of the data packets received by the destination to those sent by the source. This classifies the ability of the protocol to discover routes. Figure and table shows the Throughput under Worm hole attack detection and its prevention through Trust based mechanism i.e. AODV, WAODV and TAODV for the various node density.

Table 3: Packet Delivery Ratios Comparisons

No. of node	Attack	Pre	Without
20 node	10.3938	13.4536	19.2717
40 node	5.2639	8.93254	11.1819
60 node	4.5048	20.0851	21.2035

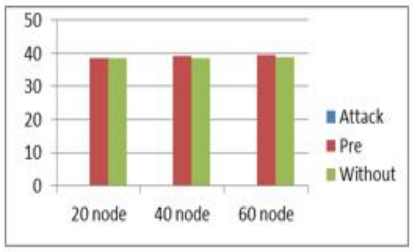

Figure 2: Throughputs comparisons

3) Simulation results for End to End Delay: This is the delay connecting the sending of the data packet by the source and its receiving at the corresponding receiver. This contains all the delays caused during route attainment, buffering and processing at in between nodes. The End to End Delay under Worm hole attack detection and its prevention through Trust based mechanism i.e. AODV, WAODV and TAODV for the various node densities is shown in the following figure and table.

Table 4: End To End Delays Comparisons

No. of node	Attack	Pre	Without
20node	0	99.75	99.08
40node	0	99.63	99.57
60node	0	98.94	98.71

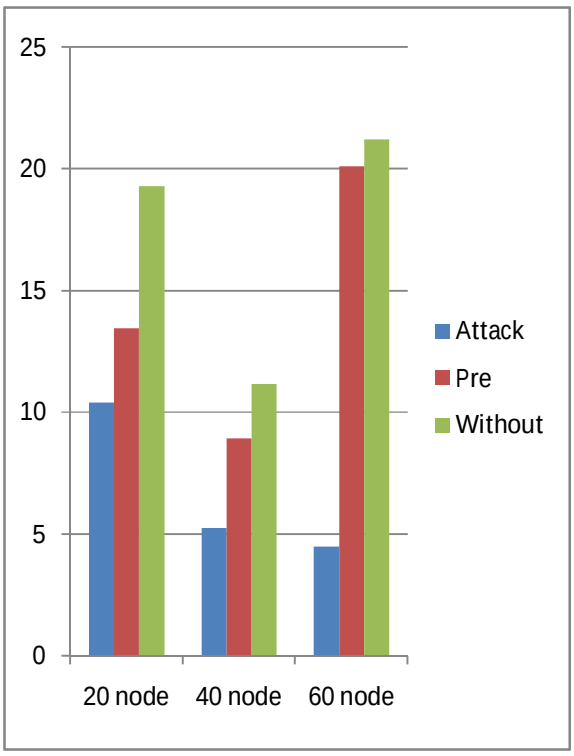

Fig.3 End to End Delays comparisons

4) *Simulation results for Residual Energy:* It is the total amount of remaining energy by the nodes after the conclusion of message or simulation. If a node is having 100% energy originally and having 70% energy after that simulation than the energy spending by that node is 30%.The unit of it will be in Joules. Figure and table shows the Residual Energy under Worm hole attack detection and its prevention through Trust based mechanism i.e. AODV, WAODV and TAODV for the various node density.

Table 5: Residual Energy Comparisons

No. of node	Attack	Pre	Without
20node	95.660646	31.577848	60.645677
40node	96.142797	20.934598	60.614828
60node	96.663887	26.332508	60.531506

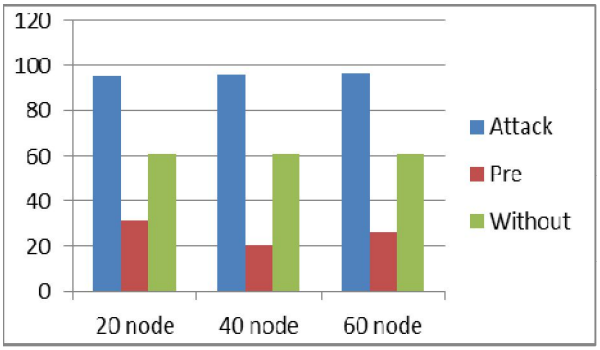

Fig.4 Residual Energy comparisons

VII. CONCLUSION

MANET has the ability to redistribute a network where a traditional network infrastructure environment cannot perhaps be deployed. Safety of MANET is one of the imperative features for its deployment, the detection and prevention of worm hole attack in the network exists as a challenging task. In this work analyzed the effect of worm hole attack in the presentation of AODV protocol and put off the network from worm hole attack using TAODV protocol. The simulation has been through using the network simulator (NS-2.35). The concert metrics like packet delivery ratio, throughput and average end to end delay has been measured and analyzed with the variable node density. From the simulation results it is clear that when the worm hole node exists in the network, it can be affected and decreased the performance of AODV routing protocol.

Here, we addressed the problem of identifying misbehaving nodes that refuse to forward packets in wireless ad hoc network and give the mechanism to prevent them. The impact of such nodes decreases network performance, lowering the network throughput and increasing the end-to-end delay. To mitigate the problem of malicious packet dropping, this work proposed a feasible solution for it on the top of AODV protocol to avoid the worm hole attack, and also prevented the network form further malicious behavior .Proposed method can be used to find the secured routes and prevent the worm hole nodes in the MANET .Our solution presents good performance in terms of packet ratio and throughput.

In this work, we simulated AODV protocol with diverse density, where each one has 10 nodes, 20 nodes, 40 nodes, 60 nodes and also simulated the same scenarios after introducing single Worm Hole Node into the network. Moreover, we simulated Secure AODV as per algorithm for detection of worm hole attack. Finally compare the results of solution with normal AODV attack using equivalent scenarios in NS-2 by varying diverse network limitations. Our simulation results are analyzed below:

Analyzing the results of PDR v/s Node Density shows the Packet Delivery Ratio of Normal AODV, AODV under worm hole attack, TAODV under worm hole attack; we found that there is increase in PDR for Secure AODV. This clearly shows that there is a significant benefit when the solution against Wormhole attacks is applied.

Analyzing the results of Throughput v/s Node Density shows the Throughput of Normal AODV, AODV under worm hole attack, TAODV under worm hole attack, where worm holes were fixed but number of nodes varied, there was significant rise in Secure AODV against normal AODV under Worm-Hole Attack, which indicates solution work better even though number of nodes increases.

Analyzing the results of End-to-End Delay v/s Node Density shows the End-to-End Delay of Normal AODV, AODV under wormhole attack, TAODV under worm hole attack; we found that there is a decrease in End-to-End Delay for Secure AODV compared to normal AODV. We can come to the conclusion from the above cases that Secure AODV give significant improvement in End-to-End Delay compared to that of normal AODV during wormhole attack.

REFERENCES

[1] Yih-Chun Hu, Adrian Perrig, and David B. Johnson, ―Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks, In Proceedings of the IEEE Conference on Computer Communications (Infocom), 2003, p. 1976-1986.

[2] L. Buttyan, L. Dora, I. Vajda, "Statistical Wormhole detection in sensor networks", Second European Workshop on Security and Privacy in Ad Hoc and Sensor Networks(ESAS 2005), Visegrad , Hungary, July 13-14,2005.

[3] C. Sun, K. Doo-young, L .Do-hyeon, and J. Jae-il, "WAP: Wormhole Attack Prevention Algorithm in Mobile Ad Hoc Networks," in Proceedings of the 2008 IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC 2008), June 2008, pp. 343-348.

[4] Xia Wang, Johnny Wong, “An End-to-end Detection of Wormhole Attack in Wireless Ad-hoc Networks” 31st Annual International Computer Software and

Applications Conference (C0MPSAC 2007) 0-7695-2870-8107@2007 IEEE

[5] L. Hu and D. Evans"Using directional antennas to prevent wormhole attacks" in Network and Distributed System Security Symposium (NDSS). The Internet Society, Feb 2004.

[6] Gunhee Lee, Dong–Kyoo Kim , Jungtaek Seo, "An Approach to Mitigate Wormhole Attack in Wireless Ad hoc Networks " in International Conference on Information Security and Assurance, Busan, 24-26 April2008,pages 220-225.

[7] Marianne A. Azer, Magdy S. El-Soudani," Sherif M. El-Kassas ," Immuning Routing Protocols from the Wormhole Attack in Wireless Ad Hoc Networks", fourth IEEE international Conference on System and network Communication.

[8] Yudhvir Singh, Avni Khatkar, Prabha Rani, Deepika, Dheer Dhwaj Barak, "Wormhole Attack Avoidance Technique In Mobile Adhoc networks" Third International Conference on Advance Computing & Communication Technologies, IEEE 2013.

[9] Weichao Wang, Bharat Bhargava, Yi Lu, Xiaoxin Wu, "Defending against Wormhole Attacks in Mobile Ad Hoc Networks", Conference of Wiley Journal Wireless Communications and Mobile Computing (WCMC), 2010

[10] Shaik Madhar Saheb A. K. Bhattacharjee, A. Vallavaraj and R. Kar, "A Cross-Layer based Multipath routing protocol for IEEE 802.11E wlan", IEEE, pp-5-8, GCC conference and exhibition, February, dubai 2011.

[11] Matthias Transier, "NS2 tutorial running simulations".