International Journal of Research and Development in Applied Science and Engineering (IJRDASE)
ISSN: 2454-6844

Identification of Worm Hole Attack in MANET using Cluster based Approach

Prakhar Mishra
Electronics & Communication
SHUATS, Allahabad (U.P.), India
prakhar391@gmail.com

Ashutosh Kispotta
Electronics & Communication
SHUATS, Allahabad (U.P.), India
ashutosh.kispotta@shiats.edu.in

Abstract--Ad Hoc system are well known and helpful on account of infrastructure less nature. Ad-hoc Network is a gathering of hubs, in which singular hubs corporate by sending packets for each other to permit hubs to convey past direct transmission range. Security is principally worry with a specific end goal to give ensured correspondence between mobile nodes in hostile environments. Countless conventions for MANET has been proposed to empower brisk and effective system creation and rebuilding MANET (Mobile Ad-hoc Network) alludes to a multi-hop packet based wireless network made out of an arrangement of versatile hubs that can convey and move in the meantime , without utilizing any sort of settled wired foundation . MANET'S are really self arranging and versatile systems that can be shaped and distorted on-the-fly without the need of any concentrated organization. It by and large works by TV the data and utilized air as medium. It's telecasting nature and transmission medium likewise help assailant to disturb system. Numerous kind of assault should be possible on such Mobile Ad Hoc Network. The accentuation of this paper to study wormhole attack, some detection method and different techniques to prevent network from these attack. In multi-hop wireless systems, the need for cooperation among nodes to relay each other's packets exposes them to a wide range of security attacks. A particularly devastating attack is the wormhole attack and the problem is to detect the wormhole attack prior to AODV routing providing the minimum delay. In wormhole attack, malicious node receive data packet at one point in the network and tunnels them to another malicious node. The tunnel exist between two malicious nodes is referred to as a wormhole. The goal of this research in Network Security is to detect the wormhole attack in Mobile Adhoc Networks using AODV Protocol to enhance the security of MANET.

Keywords MANET (Mobile Adhoc Network), AODV (Adhoc On-demand Distance Vector Routing), Wormhole:

I. INTRODUCTION

Mobile Ad Hoc Networks (MANETs) has become one of the most prevalent areas of research in the recent years because of the challenges it pose to the related protocols. MANET is the new emerging technology which enables users to communicate without any physical infrastructure regardless of their geographical location, that's why it is sometimes referred to as an ―infrastructure less‖ network. The proliferation of cheaper, small and more powerful devices make MANET a fastest growing network. An ad-hoc network is self-organizing and adaptive. Device in mobile ad hoc network should be able to detect the presence of other devices and perform necessary set up to facilitate communication and sharing of data and service. Ad hoc networking allows the devices to maintain connections to the network as well as easily adding and removing devices to and from the network. Due to nodal mobility, the network topology may change rapidly and unpredictably over time. The network is decentralized, where network organization and message delivery must be executed by the nodes themselves. Message routing is a problem in a decentralize environment where the topology fluctuates. While the shortest path from a source to a destination based on a given cost function in a static network is usually the optimal route, this concept is difficult to extend in MANET. The set of applications for MANETs is diverse, ranging from large-scale, mobile, highly dynamic networks, to small, static networks that are constrained by power sources. Besides the legacy applications that move from traditional infrastructure environment into the ad hoc context, a great deal of new services can and will be generated for the new environment. MANET is more vulnerable than wired network due to mobile nodes, threats from compromised nodes inside the network, limited physical security, dynamic topology, scalability and lack of centralized management. Because of these vulnerabilities, MANET is more prone to malicious attacks. As Wireless networks have become increasingly popular in the past few decades, particularly within the 1990's when they are being adapted to enable mobility and wireless devices became popular. As the popularity of mobile devices (MDs) and wireless networks significantly increased over the past years, wireless ad hoc networks has now become one of the most lively and active fields of communication and networking research. As there are many attractive future applications of mobile ad hoc networks (MANETs), there are still some critical challenges and open problems to be solved.

Ad hoc networking is not a new concept. As a technology for dynamic wireless networks, it has been deployed in military since 1970s. Commercial interest in such networks has recently grown due to the advances in wireless communications. A new working group for MANET [3] has been formed within the Internet Engineering Task Force (IETF), aiming to investigate and develop candidate standard Internet routing support for mobile, wireless IP autonomous segments and develop a framework for running IP based protocols in ad hoc networks. The recent IEEE standard 802.11 has increased the research interest in the

field. Many international conferences and workshops have been held by e.g. IEEE and ACM. For instance, Mobi Hoc (The ACM Symposium on Mobile Ad Hoc Networking & Computing) has been one of the most important conferences of ACM SIGMOBILE (Special Interest Group on Mobility of Systems, Users, Data and Computing). Research in the area of ad hoc networking is receiving more attention from academia, industry, and government. Since these networks pose many complex issues, there are many open problems for research and significant contributions [3].

II. SECURITY ATTACKS IN MANET

Due to its characteristics like wireless medium, dynamic topology, Manet is vulnerable to various kinds of security attacks. [6] The attacks can be categorized on the basis of behaviour of the attack i.e.

A. 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.

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. Active external attacks can be carried out by outside sources that do not belong to the network. Internal attacks are from malicious nodes which are part of the network, internal attacks are more severe and hard to detect than external attacks. These attacks generate unauthorised access to network that helps the attacker to make changes such as modification of packets, DoS, congestion etc.

Wormhole Attack

Wormhole is conjectural feature of topology that provides the short-cut through space. It is like a tunnel with two end points. The wormhole attack is the most severe attack in the network security which involves two malicious nodes and high speed tunnel called wormhole link. [1] In this attack, an attacker at one location receives the packet and transmit it to another attacker which is very far-way, by a high speed wormhole tunnel in the network.

In this Fig1, Node S is Source node and Node D is destination Node. [1] when the Source node S wants to communicate with the Destination Node D with the help of using routing protocols using MANET. Source Node S broadcasts the Route Request RREQ to its neighbour nodes. Here nodes M1 and M2 are two malicious nodes that are connected with each other by a high speed communication channel which is known as wormhole tunnel. Malicious node M1 is also a member of Source node S , as soon as M1 receives the RREQ from Node S it instantly sends RREP back to node S having route to destination node D with less number of hops.

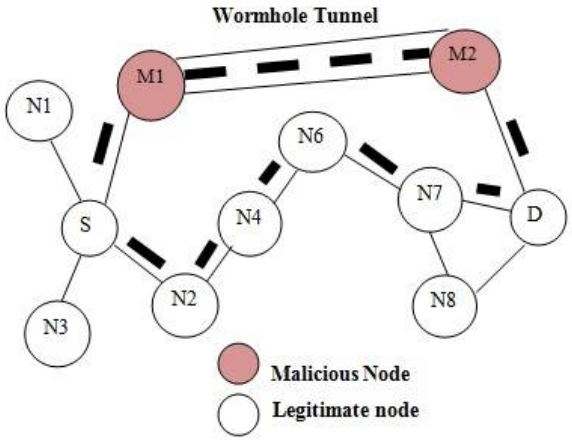


Fig 1 Example of Wormhole Attack in MANET

The source node S sends the packet through node M1 as it offers the shortest path. Then M1 node receives the packet from source node S and sends it to other malicious node M2 through wormhole tunnel. The malicious node can drop the packet or selectively forward the packet to destination. When the same Route Request RREQ that flows through legitimate nodes will arrive at destination, the destination node rejects these RREQ because it has already received the same Route request (RREQ) through the malicious node M2 .Hence, it results in the disruption of routing protocols when the routing protocols are disrupted means whole network will be disturbed.

III. RELATED WORK

Jyoti Thalor et. al., (2013) [8], according to them MANET (Mobile Ad-hoc Network) refers to a multi-hop packet based wireless network composed of a set of mobile nodes that can communicate and move at the same time , without using any kind of fixed wired infrastructure . MANET'S are actually self organizing and adaptive networks that can be formed and deformed on-the-fly without the need of any centralized administration. It generally works by broadcasting the information and used air as medium. It's broadcasting nature and transmission medium also help attacker to disrupt network. Many type of attack can be done on such Mobile Ad Hoc Network. The emphasis of this work to study wormhole attack, some detection method and different techniques to prevent network from these attack.

Mobile Adhoc Networks(MANET's) refers to self organizing in nature. In MANET's communication is done through multi hops with dynamic topology. Mobile nodes send data through wireless links, which means less secure environment and vulnerable to various attacks. There are various types of attacks which effect the data when it transfers from the source node to the destination node but wormhole attacks are most dangerous attacks and very frequently occurred in the wireless environment. In this work **Chandandeep kaur and Dr. Navdeep Kaur, (2014)**

[9], discussed the various detecting and preventing techniques for wormhole attacks.

Mobile Adhoc Networks (MANET) are self organizing, decentralized networks and possess dynamic topology, which make them attractive for routing attacks. Attacks on ad hoc networks can be classified as passive and active attacks, depending on whether the normal operation of the network is disrupted or not. The security of the AODV and DSR protocol is compromised by a particular type of attack called 'Worm hole attack'. Wormhole attack is a network layer attack observed in MANET, which completely disrupts the communication channel. In This work **Mohamed Otmani, and Dr. Abdellah Ezzati, (2014)** [7], analysed the performance of AODV and DSR routing protocols with and without wormhole attack using Network Simulator 2. For analyzing the performance they considered total packets received, total bytes received, first packet received, last packet received, average end-to-end delay and throughput as measures.

The current demand of MANET is its security and robustness. MANET's operational performance also depends on security. An attacker can easily attack on MANET because of its open nature and bandwidth constraint. Most of research has been done on the MANET security. Wormhole attack is most severe threat to security of MANET. In which two faraway malicious nodes are linked to each other with high speed link called wormhole tunnel. Most of previous research work done on detection and prevention of wormhole attacks uses packet leashes, extra hardware (GPS, Directional Antenna etc.) and few modifies the source code of routing protocols to improve security. In this work, we propose a security model that will detect and avoid the wormhole attack in MANET using routing protocol i.e., AODV protocol. **Gulzar Ahmad Wani, and Dr. Sanjay Jamwal (2015)** [1], proposed security model has three phases. In the first phase, detection of malicious node is done by using Bogus RREQ and in second phase normal AODV operation is performed for detection of shortest path from source to destination. In the third phase, once again detection of attacker is done by using delay metric if there is presences of wormhole attack then it repeats from phase one otherwise selects the shortest route to destination discovered in phase second.

Samuel Jacob, D D Ambavade, and K T V Talele, (2015) [2] according to them the Mobile Ad hoc Networks (MANETs) is a collection of wireless nodes which interact with each other by sending packets to one another or on behalf of another node, without any central network infrastructure to control data routing. For communication, the nodes cooperatively forward data packets to other nodes in network by using the routing protocol. But, these routing protocols are not secure, thus paving the way for the MANET to be open to malicious attacks. A malicious attack which is commonly observed in MANET environment is wormhole attack. The objective of this work was to analyze the performance parameters of throughput, delay and packet loss in AODV with the existence of wormhole attack. Simulation results have shown that the performance parameters are affected very much when there is an attack due to wormholes.

IV. METHODOLOGY

A. AODV Protocol

Recreation is a critical apparatus in the advancement of portable specially appointed systems; it gives an incredible situation to examination and check directing convention accuracy. Be that as it may, re-enactment does not ensure that the convention lives up to expectations practically speaking, in light of the fact that test systems contain suppositions and improved models that may not really reflect genuine system operation. After a convention is completely tried in recreation, a usage is the sensible next step. A working execution is important to accept that the directing convention determination performs under genuine conditions. Something else, suppositions made by the convention outline can't be checked as right. Moreover, an execution can be utilized to perform proving ground and field tests. In the end it can be utilized as a part of a conveyed framework, for example, [4].

Making a working usage of an impromptu steering convention is non-insignificant and more troublesome than adding to a reproduction. In reproduction, the engineer controls the entire framework, which is essentially just a solitary part. A usage, then again, needs to interoperate with an extensive, complex framework. A few parts of this framework are the working framework, attachments, and system interfaces. Extra usage issues surface on the grounds that present working frameworks are not fabricated to bolster specially appointed directing conventions. Various required occasions are unsupported; support for these occasions must be included. Since these occasions incorporate numerous framework parts, the segments and their associations should likewise be investigated. Thus it requires altogether more push to make an impromptu directing convention execution than a reenactment. In any case, as a vital stride in examining the AODV directing convention [5], we made the AODV-UCSB usage. We performed tests and approved the AODV directing convention configuration utilizing our execution. Understanding the operation and configuration procedure of our framework will assist different specialists with the improvement of their own impromptu directing conventions. Distinguishing the qualities and shortcomings of our execution additionally helps framework creators choose whether our AODV usage fits their prerequisites. In particular, the commitments of this work are the accompanying:

- Definition of required AODV triggers at present unsupported by working frameworks.
- Discussion of diverse outline systems.
- Description of the picked outline for our AODV-UCSB usage.
- Presentation of openly accessible AODV usage outlines.

B. Proposed Model

The Proposed model uses a mechanism to detect the wormhole attack in the Mobile Ad-hoc network where a wormhole attacker will get caught by its characteristic i.e., offering the source node fake route to the destination. I named this mechanism as DAODV (Decoyer Ad-hoc Distance Vector) model. This mechanism has some assumptions.

Assumptions

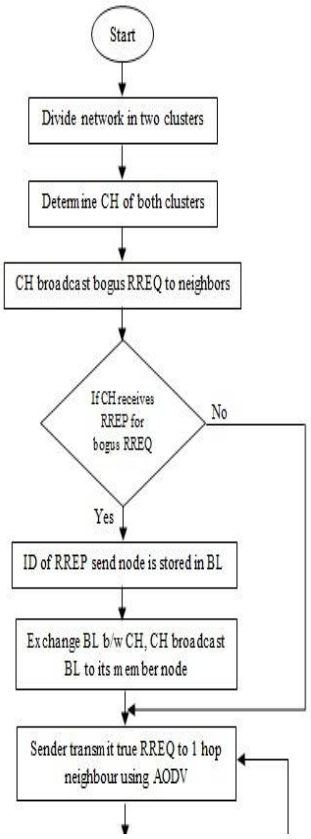
- Wormhole attacker node does not act as source and destination node.
- The entire network is geographically divided into two disjoint clusters.
- Each cluster is monitored by only one cluster head.

Algorithm

Step1: Initiate the network with two cluster w.r.t the distance of nodes nearest to the source and destination.
Determine the distance of each node from S and D node, the nodes are either kept in source cluster if it is closer to the S otherwise it is kept in destination cluster.
Step2: After cluster formation determine the centroid of both cluster and the node within a cluster nearest to the centroid of the cluster is considered as cluster head of CHS or CHD.
Step3: Each node stores the information of its immediate neighbours in its neighbour table.
Step 4: CH broadcasts bogus RREQ to neighbours. Both CH behaves as source and broadcast a bogus request by putting a non-existing destination id.
Step5: If CH receives RREP for bogus RREQ, identity of node sending RREP will be stored in BL.
The path is formed by expanding the hops using AODV algorithm since destination is non-existing the path will never terminate but in case any malicious node come in path it will respond for the destination accessing and such path are considered and the node just prior to non-existing destination id is the malicious one.
Step6: Exchange the BL between the two CH After determining the malicious node from both S and D sides clusters the CH exchanges the malicious node ids.
Step7: The CH broadcast this BL to all of its member nodes.
Step8: Source node transmits the REQ to 1-hop neighbour using AODV.
Every node excludes the malicious node from their neighbour node list and only send RREQ to non-malicious node while finding nearest neighbour during path formation by AODV.
Step9: Compare RREP with BL:
IF RREP matches with the BL
Then (drop)
Else choose node with min distance.
Step10: If neighbour node is the destination,
a) Add it to path and send RREP to the source node.
else
b) Increment hop count and rebroadcast RREQ to its neighbour.
b.1) if neighbour node is destination, repeat step 10.

Step11: Route establishment takes place.
Step12: Communication takes place.
Step13: Nodes calculate neighbour node delay.
Step14: If calculated delay > threshold delay ,
go to step 4.
else (end)

Flow Chart



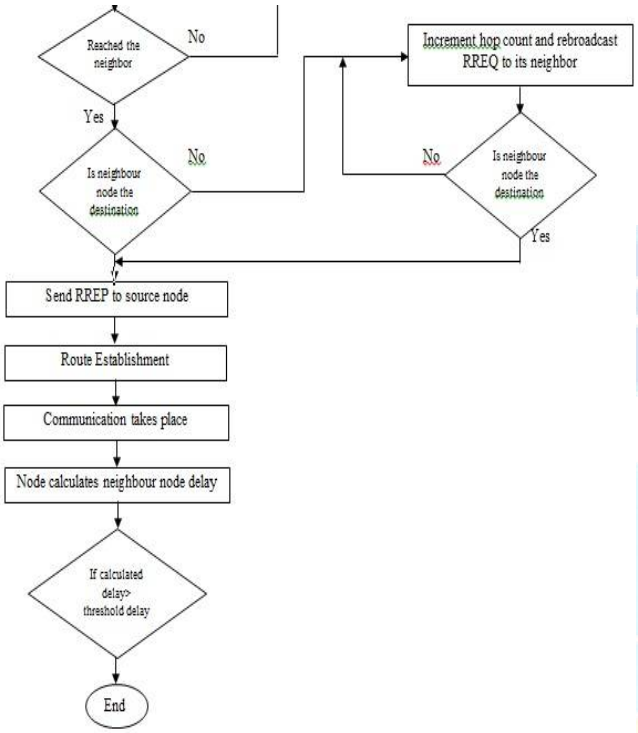


Fig 2 Flow Chart of DAODV Model

V. RESULT AND DISCUSSION

In this paper we are describing the working of MANET based wormhole detection algorithm developed using the MATLAB10 based programming language. The algorithm develops a MANET system of sensor nodes distributed randomly in the area of field width 100x100 m^2. All the nodes are shown as square shaped markers in the figure 3.The node position changes on each running of algorithm. All the nodes are capable of sending and receiving request and data within a communication range .We have considered a source node and if it wants to send the data to destination node then the algorithm determines the co-ordinates of source and destination node. For example if source node is considered as node of id 1 and it want to send data to destination node of id 5.Then it will generate RREQ message having source address 1 and destination address 5.

RREQ : Src: 1 Dst: 5.

Source coordinates: x= 14 , y= 76;

Destination coordinates: x= 15 , y= 46.

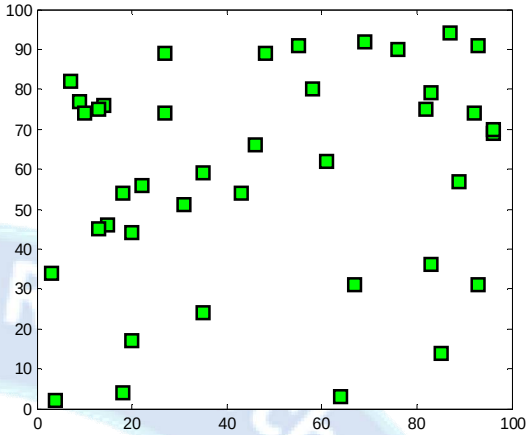


Fig 3: Node distribution of MANET system

The path with minimum number of hops is selected and data is transmitted over the path as shown in figure 4.The total average delay consumed in path establishment is calculated as:

total delay = 0.0177 seconds.

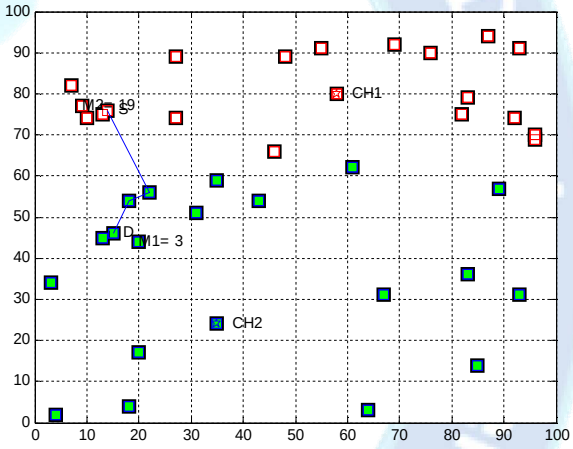


Fig. 4: Network with established path from source to node using AODV routing.

Fig 4 shows the route established using AODV routing this is the smallest route for all possible neighbor node of the source. The detected malicious nodes are M1 and M2 having node id 19 near the source S as M2 and 3 near the destination D as M1. Delay time is measured for different time on the MANET 1 network for the route establishment procedure as shown below:

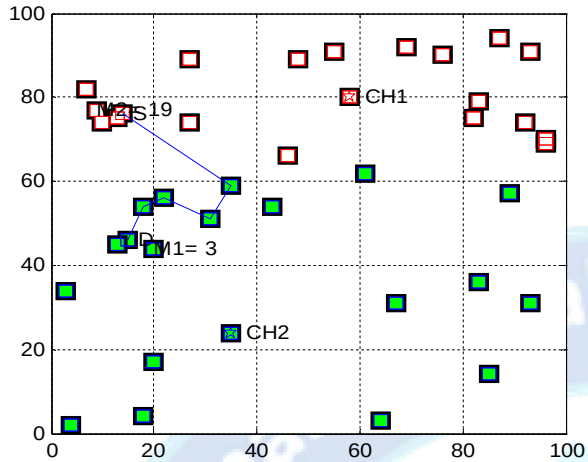


Fig 5a:Total delay 0.0358,Mal. Node {3 ,19}

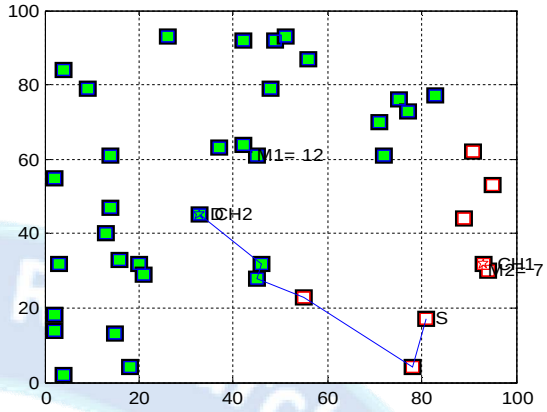


Fig 5d:Total delay 0.0335,Mal.Node {12,7}

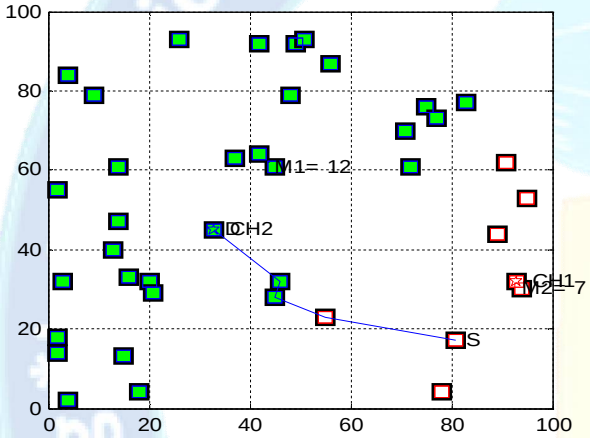


Fig 5b: Total delay 0.03,Mal. node {12,7}

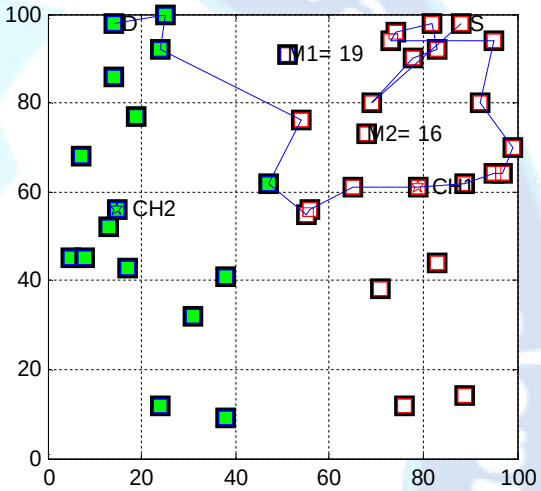


Fig 5e: Total delay 0.1464,Mal. Node {19 16}

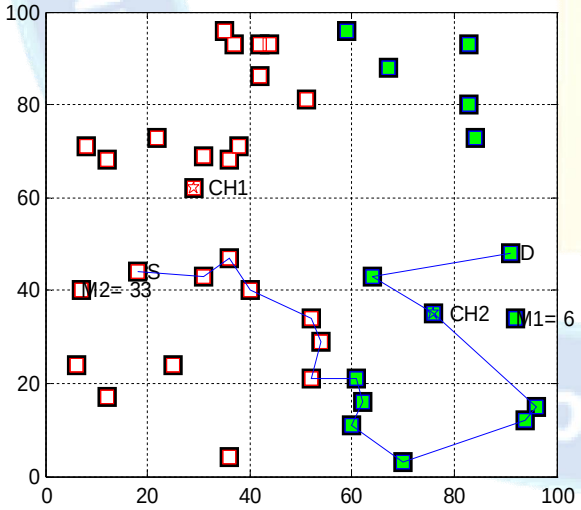


Fig 5c: Total delay 0.1074 , Mal. Node [6, 33]

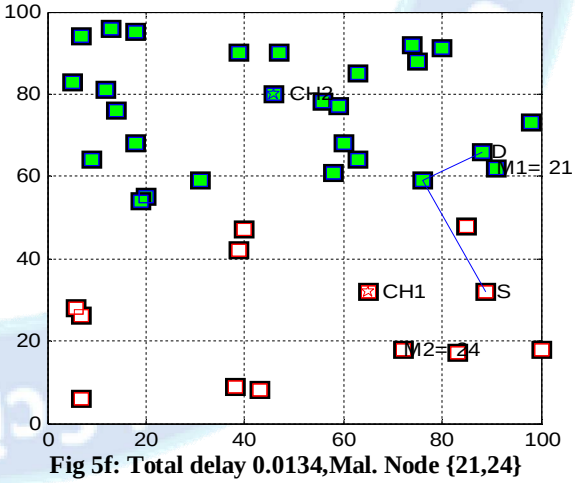


Fig 5f: Total delay 0.0134,Mal. Node {21,24}

Fig 5a shows the test results for detection of warm hole attack affected nodes for different positions of source and destination at different distribution and status of nodes. We can observe that at every time the algorithm is capable of detecting malicious node and find out the route from source to node without involving the malicious nodes. The total

delay in route establishment is also given in the figures along with the node id of malicious nodes.

All the delay that are observed for above described network is given below:

Table 1:Network Delay analysis during route establishment

Route No.	Network Node Distribution	Hops	Total delay (secs.)
1	Network 1	3	0.0177
2	Network 1	5	0.0358
3	Network 2	15	0.1074
4	Network 3	4	0.03
5	Network 3	5	0.0335
6	Network 4	18	0.1464
7	Network 5	2	0.0134
			Average Delay:0.0549

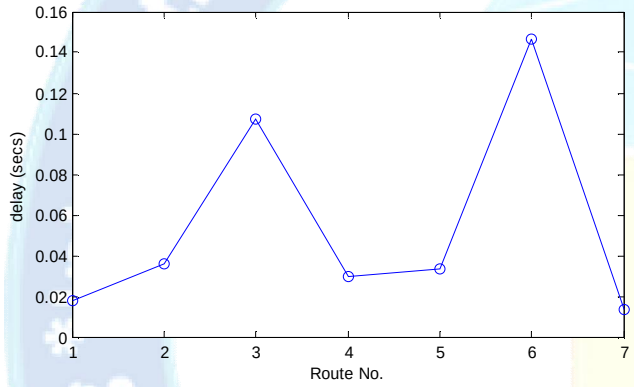


Fig 6. Delay in route establishment at different route discovery.

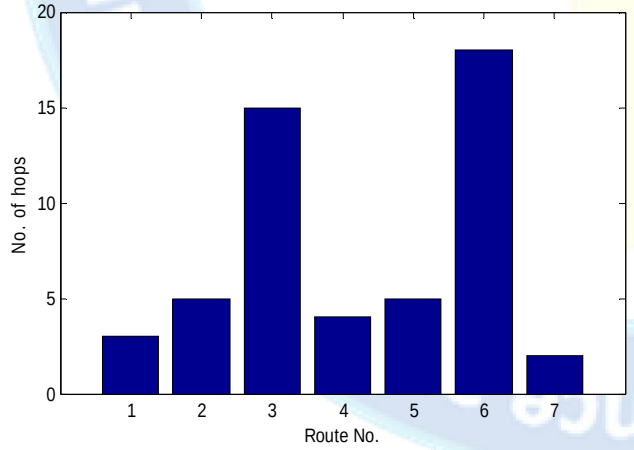


Fig. 7. Number of hops in established route by AODV routing.

6. Conclusion:

We have focused our paper on the MANETs that work without a centralized administration and the nodes communicate to each other on the basis of mutual trust. The developed algorithm is based on MATLAB programming environment and helps to demonstrate characteristic of MANETs which are vulnerable to be exploited by an attacker inside the network. The algorithm detects the wireless links which make the MANETs more susceptible to attacks to provide security from the attacker from prohibiting them to go inside the network paths and get access to the ongoing communication. In the proposed algorithm mobile nodes present within the range of wireless link has been treated as the neighbour nodes and due to prior detection of malicious node any attack can easily be suppressed during participation of nodes in the network communication. The proposed work provides high security in Mobile Ad-hoc Networks (MANETs) with the most important concern of high speed of route establishment for achieving the basic functionality without errors in detection of wormhole attacks. The response is tested at different positions of node distribution with variety of source and node destination locations. All the possible paths are checked at different network node position status, the malicious nodes going through wormhole attack are listed out and it has been observed that the proposed bi clustered parallel searching of advanced detection of malicious node by cluster heads is accurate in detecting the wormhole attack and the nodes list broadcasting is useful in reducing additional burden on source node and overall it is faster than the previous works that are found in detection of wormhole attack.

References:

[1] Gulzar Ahmad Wani, and Dr. Sanjay Jamwal, "Security Model to Detect and Avoid Wormhole Attack Using AODV Protocol", International Journal of Computer Science and Information Technologies, Vol. 6 (2) , 2015, 1044-1049.

[2] Samuel Jacob, D D Ambavade, and K T V Talele, "Performance Evaluation of Wormhole Attack In AODV" Int. Journal of Engineering Research and Applications, Vol. 5, Issue 1, (Part -6) January 2015, pp.70-72.

[3] Chlamtac, I., Conti, M., and Liu, J. J.-N. Mobile ad hoc networking: imperatives and challenges. Ad Hoc Networks, 1(1), 2003, pp. 13–6.

[4] Mykola Karpinskyy et. al., "Reliability of RSA Algorithm And Its Computational Complexity", International Scientific Journal of Computing, 2003, Vol. 2, Issue 3, 119-122.

[5] Scott Fluhrer et. al. , " Weaknesses in the Key Scheduling Algorithm of RC4", Springer-Verlag Berlin Heidelberg 2001.

[6] Dr. S.S Tyagi and Aarti “Study of Manet: Characteristics, Challenges, Applications and Security Attacks”, IJARCSSE International Journal of advanced Research in Computer Science & Software Engineering, Vol. 3, May 2013.

[7] Mohamed Otmani, and Dr. Abdellah Ezzati, "Effects Of Wormhole Attack On AODV And DSR Routing Protocol Through The Using NS2 Simulator", IOSR Journal of Computer Engineering (IOSR-JCE), Volume 16, Issue 2, Ver. XI (Mar-Apr. 2014).

[8] Jyoti Thalor et. al., "Wormhole Attack Detection and Prevention Technique in Mobile Ad Hoc Networks: A Review", International Journal of Advanced Research in

Computer Science and Software Engineering, Volume 3, Issue 2, February 2013.
[9] Chandandeep kaur and Dr.Navdeep Kaur, "Detection and Prevention Techniques for Wormhole Attacks", International Journal of Computer Science and Information Technologies, Vol. 5 (4) , 2014, 4926-4929.