Wormhole Attack Detection By Clustering Approch using Bogus Request AODV Routing

Jitendra Kumar Mishra
Department of Computer Science & Engg.
I.E.T., Lucknow, U.P.

Dr. S. P. Tripathi
Department of Computer Science & Engg.
I.E.T., Lucknow, U.P.

Abstract: MANET'S are without a doubt self arranging and versatile systems that may be fashioned and distorted on-the-fly with out the want of any focused agency. It by means of and huge works by way of TV the records and utilized air as medium. It's telecasting nature and transmission medium likewise help assailant to disturb system. Numerous type of attack ought to be feasible on such Mobile Ad Hoc Network. The accentuation of this paper to examine wormhole attack, a few detection technique and one-of-a-kind strategies to prevent network from those attack. In multi-hop wi-fi systems, the want for cooperation among nodes to relay each other's packets exposes them to a extensive range of protection assaults. A especially devastating attack is the wormhole attack and the hassle is to stumble on the wormhole assault previous to AODV routing supplying the minimum delay. In wormhole assault, malicious node acquire facts packet at one factor within the network and tunnels them to any other malicious node. The tunnel exist among two malicious nodes is called a wormhole. The purpose of this studies in Network Security is to locate the wormhole assault in Mobile Adhoc Networks using AODV Protocol to enhance the security of MANET.

Keywords-- AODV Protocol, Adhoc Network, Clustering, MANET and Wormhole

1 Introduction:

A Mobile Adhoc Network is a collection of independent mobile nodes that can communicate to each other via radio waves. The mobile nodes that are in radio range of each other can directly communicate, whereas others needs the aid of intermediate nodes to route their packets. Each of the node has a wireless interface to communicate with each other. [1] These networks are fully distributed, and can work at any place without the help of any fixed infrastructure as access points or base stations.

Fig 1 shows a simple ad-hoc network with 3 nodes. [1] Node 1 and node 3 are not within range of each other; however the node 2 can be used to forward packets between node 1and node 2. The node 2 will act as a router and these three nodes together form an ad-hoc network.

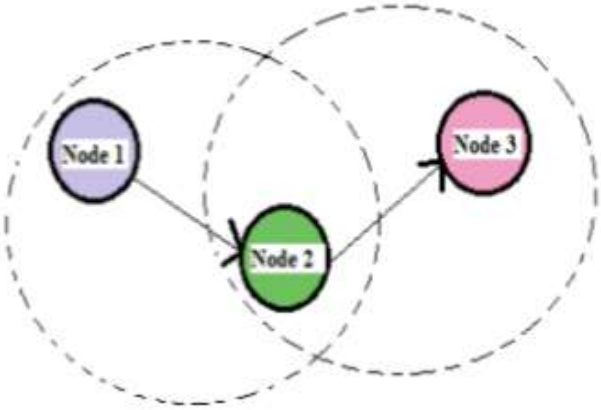

Fig 1: Mobile Adhoc Network

Mobile advert hoc networks are independent systems constituted of a number of cellular nodes that communicate the usage of wireless transmission. They are self-prepared, self-configured and self managed infrastructure-much less networks. This sort of network has the benefit of being capable of be installation and deployed quick as it has a simple infrastructure set-up and no relevant administration. Obvious examples are in the military or the emergency offerings. One state of affairs is organising verbal exchange among various retailers in a catastrophe recuperation operation where e.G. Fire opponents need to connect to neighborhood ambulances and traffic control in circumstances where the everyday verbal exchange infrastructure is destroyed or otherwise rendered unusable. In such situations a collection of cellular nodes with wi-fi community interface can shape a transitory network. These networks are in particular useful to those mobile users who need to speak in situations where no constant stressed infrastructures are available. However, the salient feature of creating a community 'at the fly' without requiring any prearranged infrastructure gave cell advert hoc networks an favored interest in both industrial and military structures.

Mobile Ad Hoc Networks (MANETs) has emerge as one of the most frequent areas of research within the current years because of the demanding situations it pose to the related protocols. MANET is the new rising era which allows users to talk with none physical infrastructure no matter their geographical area, that's why it's miles from time to time called an —infrastructure much less network. The increase of inexpensive, small and greater powerful devices make MANET a fastest growing net-paintings. An ad-hoc community is self-organizing and adaptive. Device in cell advert hoc community need to be capable of discover the presence of different devices and perform important set up

to facilitate communication and sharing of facts and provider. Ad hoc networking allows the gadgets to maintain connections to the community as well as effortlessly adding and removing gadgets to and from the community. Due to nodal mobility, the community topology might also alternate unexpectedly and unpredictably over the years. The community is decentralized, where community enterprise and message transport need to be achieved by using the nodes themselves. Message routing is a hassle in a decentralize surroundings in which the topology differ. While the shortest route from a supply to a vacation spot based totally on a given cost function in a static community is commonly the most useful path, this concept is difficult to extend in MANET. The set of packages for MANETs is miscellaneous, starting from massive-scale, cellular, exceptionally dynamic networks, to small, static networks which might be constrained via strength sources. As Wireless networks have emerge as more and more famous inside the beyond few decades, particularly within the 1990's while they are being adapted to enable mobility and wireless devices became popular. As the popularity of cellular gadgets (MDs) and wi-fi networks substantially multiplied during the last years, wireless ad hoc networks has now grow to be one of the most energetic and lively fields of communique and networking research. As there are many attractive future programs of cellular advert hoc networks (MANETs), there are nevertheless a few vital challenges and open issues to be solved.

2. Related Work:

In multi-hop wi-fi systems, the need for cooperation amongst nodes to relay every different's packets exposes them to a huge variety of security assaults. A particularly devastating assault is the wormhole assault, in which a malicious node facts manage visitors at one location and tunnels it to any other compromised node, possibly a long way away, which replays it regionally. Routing security in ad hoc networks is often equated with sturdy and feasible node authentication and light-weight cryptography. Unfortunately, the wormhole attack can infrequently be defeated with the aid of crypto graphical measures, as wormhole attackers do now not create separate packets. They genuinely replay packets already existing on the community, which pass the cryptographic checks. Existing works on wormhole detection have frequently targeted on detection the usage of specialised hardware, such as directional antennas, and so forth. In this paintings, we gift a cluster primarily based counter-measure for the wormhole attack, that alleviates those drawbacks and efficiently mitigates the wormhole assault in MANET. Simulation effects on MATLab show off the effectiveness of the proposed algorithm in detecting wormhole attacks with the aid of **Debdutta Barman Roy, Rituparna Chaki, Nabendu Chaki (2009) [1].**

Rutvij H. Jhaveri et. Al. (2010) [2], in line with them in this era of wireless devices, Mobile Ad-hoc Network (MANET) has come to be an indivisible part for verbal exchange for cellular gadgets. Therefore, interest in studies of Mobile Ad-hoc Network has been growing because previous few years. In this paintings we have mentioned some fundamental routing protocols in MANET like Destination Sequenced Distance Vector, Dynamic Source Routing, Temporally-Ordered Routing Algorithm and Ad-hoc On Demand Distance Vector. Security is a large issue in MANETs as they're infrastructure-less and self sustaining. Main objective of scripting this paintings is to cope with some simple safety issues in MANET, operation of wormhole assault and securing the famous routing protocol Ad-hoc On Demand Distance Vector. Their work might be a outstanding assist for the people undertaking studies on actual international problems in MANET safety.

The infrastructure of a Mobile Ad hoc Network (MANET) has no routers for routing, and all nodes should proportion the identical routing protocol to help every different while transmitting messages. However, nearly all not unusual routing protocols at present consider performance as first priority, and feature little defense functionality against the malicious nodes. Many researches have proposed numerous protocols of higher safety to guard against assaults; however, every has precise protection objects, and is unable to guard towards particular assaults. Of all the types of assaults, the wormhole assault poses the greatest threat and is very difficult to save you; therefore, **A.Vani et. Al. (2011) [3],** focused on the wormhole assault, with the aid of combing three techniques. So that our proposed scheme has three techniques based totally on hop depend, decision anomaly, neighbor list be counted strategies are combined to discover and isolate wormhole assaults in advert hoc networks. That manages how the nodes are going to behave and which to direction the packets in secured way.

In multihop wi-fi adhoc networks, cooperation between nodes to direction each other's packets exposes these nodes to a wide variety of security attacks. Also due to the vulnerability of the routing protocols, the wi-fi ad-hoc networks face numerous protection risks. A in particular severe protection attack that affects the adhoc network routing protocols, is called the wormhole attack. The wormhole attack is performed as a phase manner released by way of one or multiple malicious nodes. In the primary phase, those malicious nodes, called as wormhole nodes, try and entice valid nodes to ship facts thru them by means of collaborating within the network. In the second segment, wormhole nodes should exploit the facts & affect the verbal exchange by misbehaving. In this paintings **Pirzada Gauhar Arfaat, Dr. A.H. Mir (2011) [4],** have simulated the wormhole attack in wi-fi adhoc networks & Manet's. And then they evaluated & mentioned the impact at the community by using evaluating the consequences without and with wormhole attack. The Wormhole assault changed into simulated the usage of different eventualities. Thus they studied the effect of the wormhole attack at the respective networks. The parameters like throughput, packet loss and end-to-give up postpone have been calculated the use of distinct eventualities for comparing the effect on wireless adhoc networks and Manet's.

A Mobile Ad hoc Network (MANET) is a group of self configurable cellular node linked through wireless hyperlinks. In MANET nodes which can be inside the variety of each different can join at once in which as nodes which aren't in the region of each different rely upon the intermediate node for verbal exchange. Each node in MANET can work as a sender, receiver as well as router.

Communication in the network depends upon the believe on each other. In wormhole attacks, one malicious node tunnels packets from its vicinity to the opposite malicious node. Such wormhole assaults result in a false route with fewer. If supply node chooses this faux path, malicious nodes have the choice of delivering the packets or losing them. It is hard to detect wormhole attacks due to the fact malicious nodes impersonate valid nodes The wormhole attack is possible even if the attacker has not compromised any hosts and even if all verbal exchange affords authenticity and confidentiality. In this work, **Ajay Prakash Rai, Vineet Srivastava, and Rinkoo Bhatia (2012), [5]** analyzed wormhole assault nature in ad hoc and sensor networks and existing methods of the defending mechanism to come across wormhole attacks without require any specialised hardware. This evaluation capable of provide in organising a method to lessen the price of refresh time and the reaction time to come to be extra faster.

3.Methodology:

Hybrid routing protocols [11, 12] aggregates a set of nodes into zones in the network topology. Then, the network is partitioned into zones and proactive approach is used within each zone to maintain routing information. To route packets between different zones, the reactive approach is used. Consequently, in hybrid schemes, a route to a destination that is in the same zone is established without delay, while a route discovery and a route maintenance procedure is required for destinations that are in other zones. The zone routing protocol (ZRP) and zone-based hierarchical link state (ZHLS) routing protocol provide a compromise on scalability issue in relation to the frequency of end-to-end connection, the total number of nodes, and the frequency of topology change. Furthermore, these protocols can provide a better trade-off between communication overhead and delay, but this trade-off is subjected to the size of a zone and the dynamics of a zone. Thus, the hybrid approach is an appropriate candidate for routing in a large network. At network layer, routing protocols are used to find route for transmission of packets. The merit of a routing protocol can be analyzed through metrics-both qualitative and quantitative with which to measure its suitability and performance. These metrics should be independent of any given routing protocol. Desirable qualitative properties of MANET are Distributed operation, Loop-freedom, Demand-based operation, Proactive operation, Security, Sleep period operation and unidirectional link support. Some quantitative metrics that can be used to assess the performance of any routing protocol are End-to-end delay, throughput, Route Acquisition Time, Percentage Out-of-Order Delivery and Efficiency. Essential parameters that should be varied include: Network size, Network connectivity, Topological rate of change, Link capacity, Fraction of unidirectional links, Traffic patterns, Mobility, Fraction and frequency of sleeping nodes [1,9,10].

The entire network is geographically divided into a few disjoint clusters. First one, the network is considered to be layered then a cluster head at the inner layer is represented as CH (1,i), where 1 signifies inner Layer, and i stands for the cluster number and finally each cluster is monitored by only one cluster head.

Algorithm:

Step 1: Initiate the network with two cluster and each cluster have some nodes.
Step 2: The node within a cluster having minimum node ID becomes Cluster Head. The node ID for each node is provided when the node enter into the cluster.
Step 3: Each node stores the information of its immediate neighbors in its neighbor table.
Step 4: CH broadcasts bogus RREQ to neighbours.
Step 5: If CH receives RREP for bogus RREQ, identity of node sending RREP will be stored in BL.
Step 6: Broadcast BL to CH at layer2 which will broadcast it to all the CH at layer1.
Step 7: The CH broadcast this BL to all of its member nodes.
Step 8: Source node transmit the REQ to 1-hop neighbour using AODV.
Step 9: Compare RREP with BL:
IF matched (drop)
else choose node with min distance.
Step 10: If neighbour node is 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.
Step 11: Route establishment takes place.
Step 12: Communication takes place.
Step 13: Nodes calculate neighbour node delay.
Step 14: If calculated delay > threshold delay ,
go to step 4.
else (end)

4. Result and Discussion:

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 2. 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.

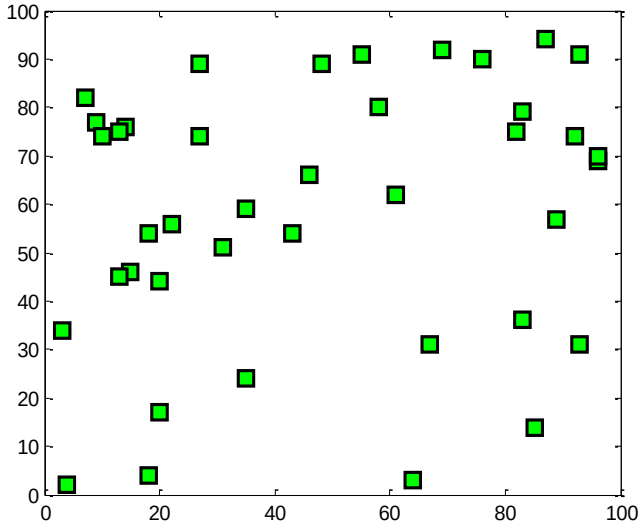

Fig 2: Node distribution of MANET system in 50x50 m^2 area.

The algorithm displays S for source and destination label as D in the figure as per respective source and destination co-ordinates as shown in figure 3.

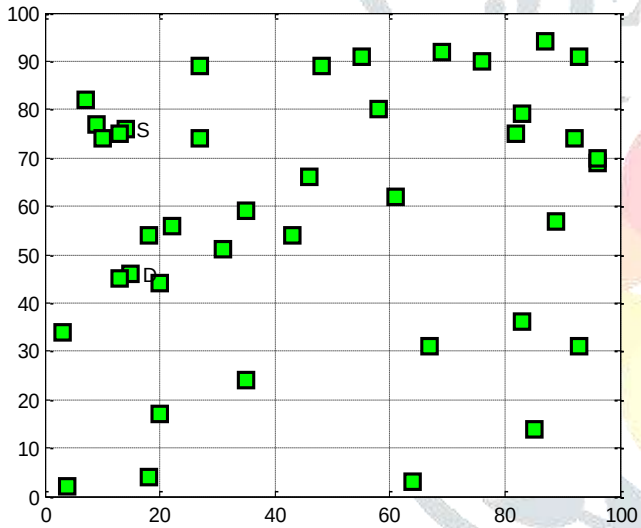

Figure 3: Network displays S and D at source and destination positions.

Similarly nodes at different location are developed to check the network performance are shown in figure 4 to 7.

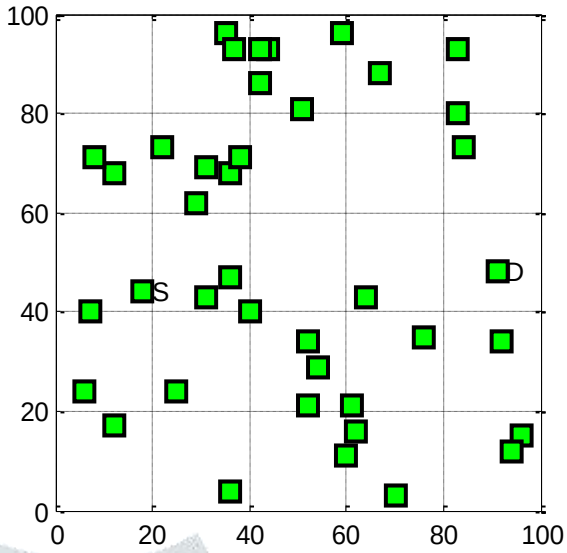

Figure 4: MANET at node positions 2.

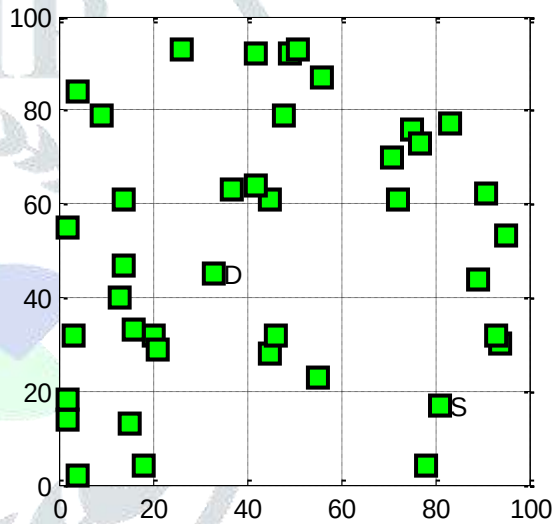

Fig 5: MANET at node positions 3.

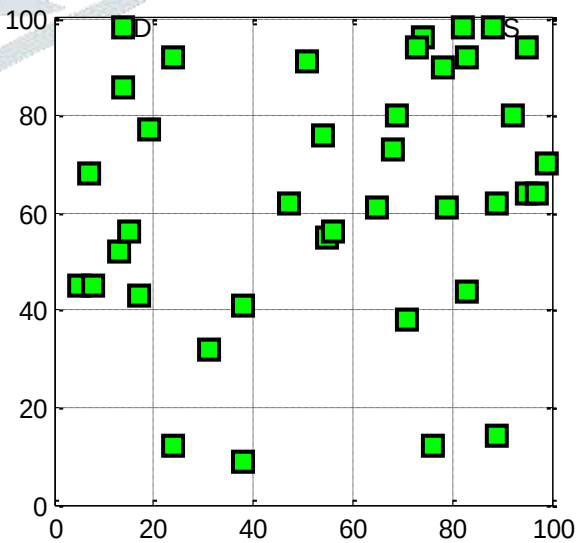

Fig 6. MANET at node positions 3.

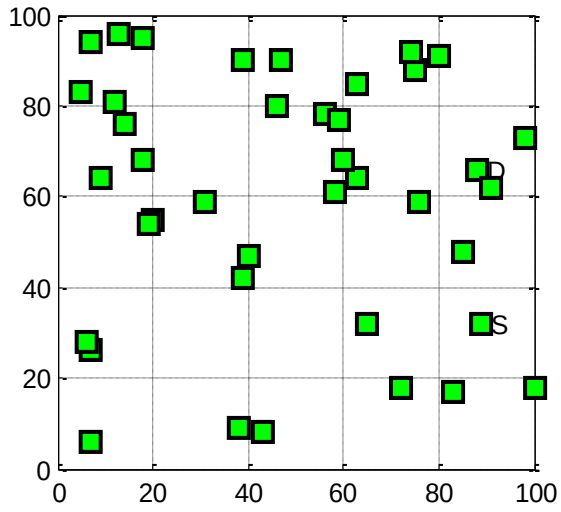

Fig 7. MANET at node positions 4.

5. Conclusion:

We have focused our thesis 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 broad casting 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] Debdutta Barman Roy, Rituparna Chaki, Nabendu Chaki, "A New Cluster-Based Wormhole Intrusion Detection Algorithm For Mobile Ad-Hoc Networks", International Journal of Network Security & Its Applications (IJNSA), Vol 1, No 1, April 2009.

[2] Rutvij H. Jhaveri et. al., "MANET Routing Protocols and Wormhole Attack against AODV", IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.4, April 2010.

[3] A.Vani et. al., " A Simple Algorithm for Detection and Removal of Wormhole Attacks for Secure Routing In Ad Hoc Wireless Networks", International Journal on Computer Science and Engineering (IJCSE), Vol. 3 No. 6 June 2011.

[4] Pirzada Gauhar Arfaat, Dr. A.H. Mir, "The Impact of Wormhole Attack on the Performance of Wireless Ad-Hoc Networks", IJCST Vol. 2, Issue 4, Oct . - Dec. 2011.

[5] Ajay Prakash Rai, Vineet Srivastava, and Rinkoo Bhatia, "Wormhole Attack Detection in Mobile Ad Hoc Networks", International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 2, August 2012.

[6] L. Sudha Rani , R.Raja Sekhar, "Detection And Prevention Of Wormhole Attack In Stateless Multicasting", International Journal of Scientific & Engineering Research Volume 3, Issue 3, March -2012.

[7] Aarti et. al., "Study of MANET: Characteristics, Challenges, Application and Security Attacks", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013.

[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.

[10] 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).

[11] 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.

[12] 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.