ISSN:0975-9646

Security Improvement of Mobile Ad Hoc Networks using Clustering Approach

Upendra singh
M Tech student PCST College
Indore,India

Makrand Samvatsar
HOD (CSE) PCST College
Indore, India

Neeraj Arya
Assistant Prof SGSITS Indore
Indore,India

ABSTRACT: **Mobile Ad Hoc networks (MANETs) are wireless networks which are infrastructure less, means it does not require any central authority for communication between mobile nodes. The security is an issue in such networksand the networks are vulnerable to many attacks. Routing in MANET in general is not secure because of vulnerability due to attacks like flooding and Jelly-Fish attacks. We have used the term integrated attack to mean combination of one or more of these attacks which occur on the network layer of OSI model. The proposed mechanism uses novel hierarchical clustering based approach. This mechanism uses the concept of multi mesh tree (MMT). It reduces the impact of these attacks on the performance of MANET. The simulation results show that the proposed mechanism gives better performance under the integrated attacks in terms of packet delivery ratio (PDR), end to end delay (ETD) and throughput.**

Index Terms: - Jelly Fish Attack, Flooding attack, clustering and Mobile ad hoc network.

I INTRODUCTION

In Latin "ad hoc" phrase means "for this "meaning "for this special purpose only, by expansion it is a special network for a particular application. an ad-hoc wire–less network consists of a set of mobile node (hosts) that are connected through the wireless inks .in ad –hoc wireless network, communication is based on the principle of broadcast l inks radio channel and reception of electromagnetic waves [1]. A MANET is referred to as a network that is autonomous , self –configuring and network without infrastructure where mobile nodes communicate via wireless links Nodes within each other's wireless transmission ranges can communicate directly ;however, nodes outside each other's rang use the concept of multi –hop communication where several intermediate hosts relay the packet sent by the source host before they reach the destination host [2]. In MANETs, Every node functions both as a host and as a router. The nodes in MANETs move freely, in any direction or speed and allowed to organize themselves arbitrarily.

in MANET s, the network topology changes dynamically and unpredictably .A Node can forward data to any other node often in a peer –to-peer , multi–hop mode .Therefore , MANETs possess a need to dynamically determine routing based on availability or visibility of nodes. MANET also has nodes whose energy storage is very limited. Often, they are battery equipped, with very limited to no recharging or replacement possible. Another limited resource in MANET s, is bandwidth.

In MANTE s, security is a major concern. Due to lack of a fixed infrastructure. Dynamic topology and limited resources securing MANET becomes very; challenging [3]. There is a wide variety of attacks in MANTEs, An adversary can launch a malicious node in the network or a legitimate node may become selfish in order to save its resources. Such nodes termed as malicious nodes have to be detected and are to be avoided in forwarding of data .Guaranteeing data safety and reliability is a major concern.

Fig 1 Showing scenario of MANET

II MOTIVATION

The connectivity of mobile nodes in MANET strongly relies on the fact that ensures cooperation among the nodes in the network. Recently variety of network layer attacks have been identified and heavily studied in research papers. As a consequence of attacking networking layer, adversaries can easily disturb and absorb network traffic, inject themselves into the selected data transmission path between the source and destination. and thus control the network traffic flow, as shown fig 1, where a malicious node M can interface between any of the intermediate nodes participating in the communication in the chosen path (in the fig 1 to n represents the number of intermediate nodes) between source S and destination D [4].

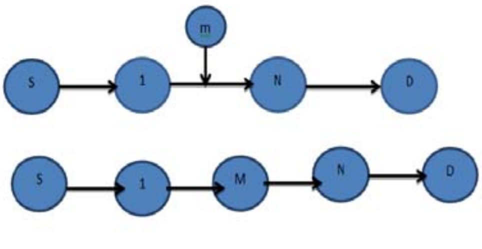

Fig 2

The packets in the network traffic could be dropped completely or forwarded selectively which introduces significant packet losses in the network. The adversaries send some factious routing updates to create routing loops or to introduce severe congestion n some portions of the presence of malicious nodes in the network in accessible. The main effect of the presence of malicious nodes in the network is excessive network control traffic which intensifies the network congestion and an s result the performance of the network degrades. Since MANET have a variety of application, as discussed in previous section, detection of such nodes is critical for the success of MANET. Since, protection at the network layer is of prime importance, we focus our work on network layer attacks. A lot of efforts have been made in this direction. But, all of them have one or more limitations. Therefore, there is still a need of a solution which overcomes all limitations. Therefore, there is still a need of a solution which overcomes all limitations and is able to detect malicious nodes effectively.

While securing MANET there are certain challenges to be faced because of some of its inherent characteristic. Like, nodes in MANETs are highly mobile and topology changes in sometimes unpredictable manner. MANETs lack fixed traffic points, i.e. there are no firewalls or routers as in classical computer networks, and each node acts as a router. Also, host-resident network intrusion detection systems have their limitations in case of MANETs. Sometimes, detectors may also become the target of an attack. Wireless communication (RF medium) is susceptible to eavesdropping, jamming, interference and many other MAC threats that may result in loss of packets and connectivity. The resources in MANET environment are limited, e.g. energy (battery operated nodes), varying throughput because of dynamic topology configuration. All these factors have to be considered while designing a technique for malicious node detection.

III Attacks In Manet

3.1 Black hole Attack in AODV

The difference of black hole attacks compared to gray hole attacks is that malicious nodes never send true control messages initially. To carry out a black hole attack, malicious node waits for neighbouring nodes to send RREQ messages. When the malicious node receives an RREQ message. Without cheeking its routing table, immediately sends a false RREQ message giving a route to destination over itself, assigning a high sequence number to settle in the routing table of the victim node, before other nodes send a true one. Therefore requesting nodes assume that route discovery process is completed and ignore other RREP messages and begin to send packets over malicious node. Malicious mode attacks all RREQ messages this way and takes over all routes. Therefore all packets are sent to a point when they are not forwarding anywhere. This is called a black hole to give real meaning which swallows all objects and matter. To succeed a black hole attack, malicious node should be positioned at the centre of the wireless network. If malicious node masquerades false RREP message as if it comes from another victim node instead of itself, all messages will be forwarded to the victim node. By doing this, victim node will have to process all incoming messages and is subjected to a sleep deprivation attack [24].

Gray hole attacks against one or two nodes in the network to isolate them, where as black hole attack affects the whole network. Moreover, the malicious node that attempts gray hole attacks cannot be perceived easily since it does not send false messages. Behaviour of failed or overloaded nodes may seem like selfish nodes attacks or gray hole attacks due to dropping of messages. But , since failed nodes cannot fabricate a new control message, they cannot form a black hole attack although they will drop the message later.

3.2 Flooding Attack in AODV

The flooding attack is one form of DoS attacks. Instead of attacking any particular node, it aims to paralyze the whole network by exhausting network bandwidth. An attacker causes the congestion in network by generating an excessive amount of traffic. The attacker node continuously sends the huge amount of unwanted data packets into the network. This cause a huge congestion of unwanted packet in to the network. Due to the congestion the data packets, RREQ, RREP or RERR packet send by the genuine node

IV Proposed Approach

The proposed methodology works in three phases to avoid the integrated attacks in the MANET. Multi-hop cluster formation is the first phase in which whenever a node joins the network it will organize itself into a cluster and an ‘n’ digit UID (Unique Identifier) will be assigned to that node. The second phase is cluster head election in which a node will be elected as a CH (Cluster Head) from that cluster by applying cluster head election algorithm. All the data, traffic must go through that cluster head even if the source and destinations are in different cluster or in the same cluster. The third phase of our methodology is path cut-off in which fake RREQ request will be dropped by neighbour of the attacker node if it is not routed from cluster head.

4.1 Multi-hop Cluster Formation

The mobile nodes organize themselves into clusters in this process. All data, traffic must go through the cluster head, even if the source and destination nodes are in the same cluster. The cluster formation algorithm are as follows:-

Step 1. When a node joins the network a UID (Unique Identifier) of ‘n’ digit is assigned to node.

Step 2. After joining network the node broadcast the Hello message from the neighbour table.

Step 3. When a neighbour table is formed, cluster head election algorithm elects the cluster head (CH).

Step 4. Cluster head advertises their UID as an advertising node VID in its neighbourhood.

Step 5. When a neighbour of advertising node receives the advertisement, it sends a joining request to advertising node.

Step 6. Advertising node accepts the request of requesting node as a child and allocates the child

VID that is its own VID appended with a single digit integer.

Step 7. After allocation of VID the child node sends a registration request to CH with their UID and assigned VID via advertising node.

Step 8. The Cluster head checks the cluster size and hop size constraints for child node and then provides the acceptance and maintain a link between CH to child node via advertising node.

Step 9. After that child node advertises its VID, if a node has more than one VID, it advertises the smallest length VID, in its neighbourhood.

Step 10. Go to Step 5.

4.2 Allocation of UID and VID

Each node in the network can have two types of address Unique Identifier (UID) and Virtual Identifier (VID). This hierarchical addressing technique is used for detecting and preventing the integrated attack in the proposed mechanism. Unique Identifier is unique for each node and has one to one relationship in the network. Virtual identifier is a non-unique id of the node. Each node in the network can have more than one virtual identifier. The number of virtual identifiers of node depends upon the number of nodes in the cluster. These are assigned to each node by the cluster head of each cluster as shown in figure 5.1. The VID of the node will contain UID of the cluster head appended with a digit which identifies that node in the cluster.

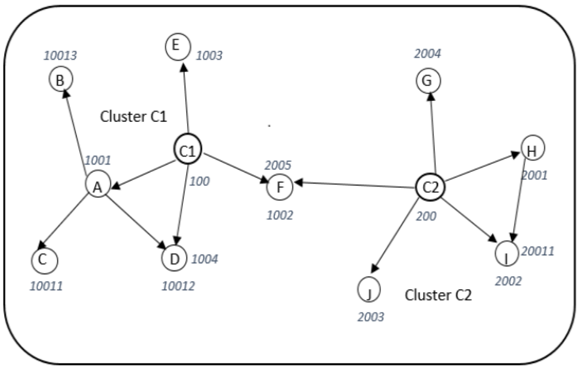

Figure 3. Hierarchal addressing scheme

4.3 FLOWCHART OR ROUTING PROCESS

A hybrid approach of routing is used for communication in cluster-based network after cluster conceptualization. Figure 4 shows flowchart of routing algorithm. The source CC initiates route discovery process to a destination CC. Source CC sends a route request to its CH using its primary VID. The VID carries route information from CC to CH. Every CC has one or multiple numbers of VID. A CC has single VID means it has a single route towards its CH. Any CC has multiple VIDs then the concept of secondary VIDs is originated. Nodes that have more than one VIDs, classify their VIDs into primary VID (that has the least digits, and hence the shortest hops to reach the CH), and the remaining as secondary VIDs. The secondary VIDs were acquired by these nodes by overhearing the advertisements from their neighbours and joining as their children. The multiple VIDs thus result in various routes (also known as multiple branches). The dynamic multiple proactive route establishments provide robust connectivity with low overhead. CH receives the route request of source CC and extracts the destination CH, VID using parsing technique.

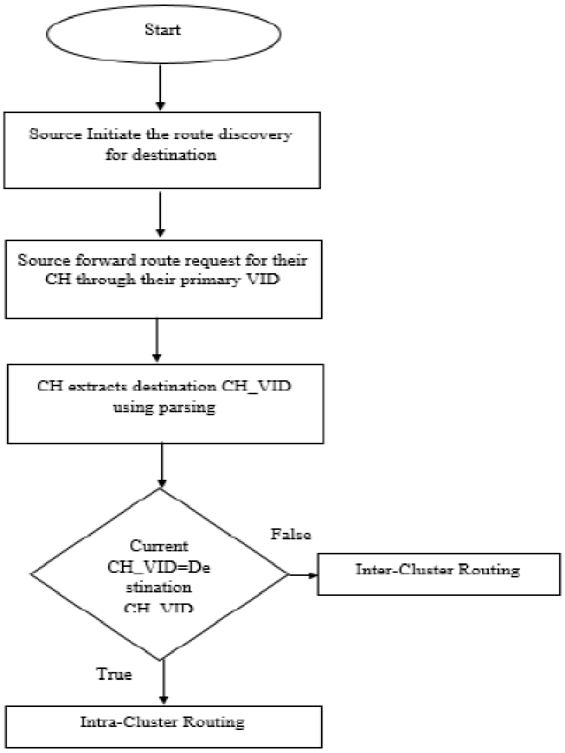
Start
Source Initiate the route discovery for destination
Source forward route request for their CH through their primary VID
CH extracts destination CH_VID using parsing
Current CH_VID=De stination CH_VID
False
Inter-Cluster Routing
True
Intra-Cluster Routing

Fig 4 Flow of Routing Process

V Simulation & Result Analysis

Table I shows the detail about the resources required to simulate the network. The mechanism is implemented for providing the secure routing in MANET.

Table 1. Simulation Parameters

Parameter	Value
Simulation Area	1250×1250m^2
MAC Protocol	IEEE 802.11
Mobile Nodes	46
Antenna Type	Omni-Antenna
Propagation Model	Two Ray Ground
Number of Connections	10
Packet Size	1024 bytes
Routing Protocols	AODV,CAODV
Traffic Source	TCP
Simulation Time	100s
Pause Time	10,20,30,40,50,60,70,80,100
Rate	10 Packets/s
Maximum Speed	50 m/s

5.1 Result Analysis

The performance of network is measured in terms of three different metrics such as throughput, packet delivery ratio and end to end delay. This performance is compared with the standard approach the Ad hoc on Demand Distance Vector routing protocol (AODV).

5.1.1 Throughput

The average rate of effective packet delivery in network is regarded as throughput of the network.

Figures 3,4 and 5 shows that the integrated attack avoidance technique and the normal behavior of the routing protocol with respect to no of malicious nodes. If there is increase in the size of the network the attack of malicious node increases but the avoidance technique reduces the effect of the attacker's node in the network.

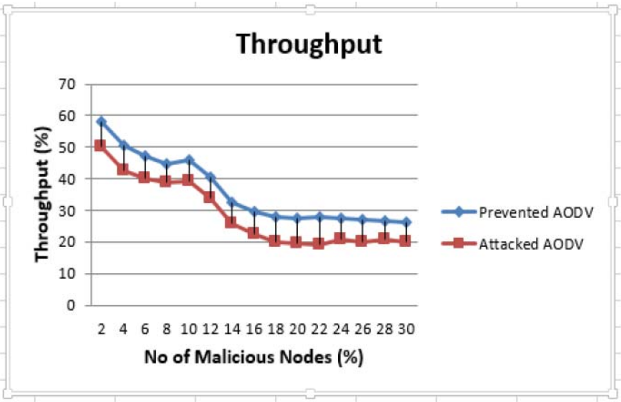

Figure 5.Throughputas a function of no of malicious nodes

5.1.2 Packet Delivery Ratio

PDR is the ratio of number of packets received at the destination node with respect to total data packets generated at the source node.

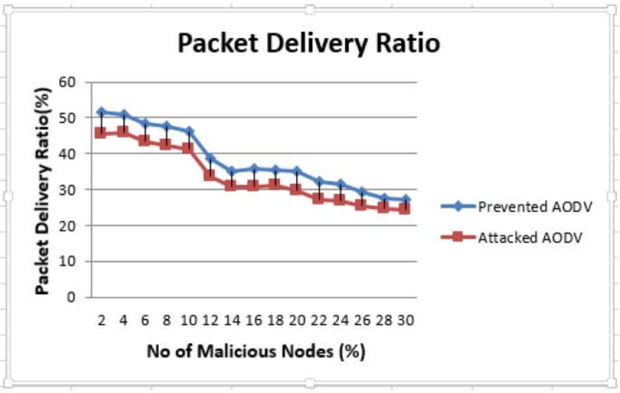

Figure 6. Packet Delivery Ratio as a function of no of malicious nodes

The above figure 4 shows the normal behaviour of the aodv routing protocol and behaviour under unifide attack and the behaviour under avoidance of the unifide attack. The bhehaviour of the network under normal routing protocol and avoidance of floodig attack is nearly same. This makes the routing protocol more robust and secure.

5.1.3 End to End Delay

End to End Delay (ETD) is the time taken by packet to travel from source node to the destination node.

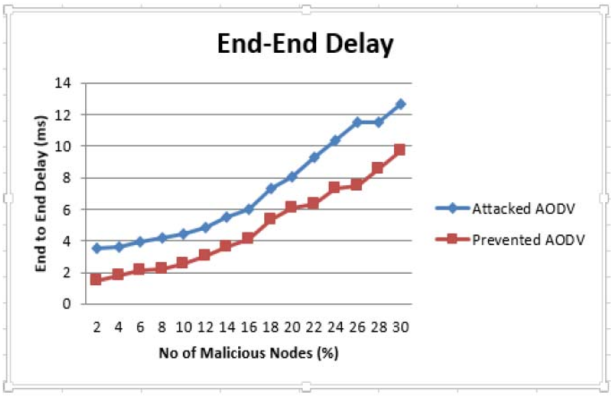

Figure 7 End to End Delayas a function of no of malicious nodes

The figure 5 shows that the ETD increases under the attack because the malicious node floods the fake RREQ packet to each node and it increases the congestion but the proposed mechanism reduces the unnecessary ETD. The graph shows the total number of transmitted packets in the network during the simulation

VI Conclusion

The proposed work describes a powerful mechanism against integrated Attack. The proposed integrated attack avoidance mechanism is based on hierarchical cluster technique. Each node in the network will be able to detect malicious node. All the communication between source node and the destination node will happen through cluster head even if both source and the destination node are in same cluster or in other cluster. Each node does not need to continuously observe the behaviour of the neighbour node in this technique

5.1 Future Scope

The proposed scheme is used to avoid the flooding attack in MANET. This mechanism can be used to avoid various network layer attacks such as wormhole attack, black hole attack and can improve the performance of the network. The prevention scheme can also be implemented along with this technique.

References

[1] Manjot Kaur, Malti Rani, AnandNayyar "A Comprehensive Study of Jelly Fish A Comprehensive Study of Jelly Fish attack in Mobile Ad hoc networks" published in International Journal of Computer Science and Mobile Computing, Vol.3 Issue.4, April- 2014, pg. 199-203

[2] Amneet Kaur, Prabhneet Sandhu "COMPARISN OF AODV, OLSR, AND TORA IN MANET UNDER JELLY FISH ATTACK" published in IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 1 Issue 5, July 2014.

[3] A. Jain and V. Tokekar. Classification of denial of service attacks in mobile ad hoc networks. In Proceedings of International Conference on Computational Intelligence and Communication Networks (CICN), pages 256–261, 2011

[4] J. Godwin Ponsam, R. Srinivasan "A Survey on MANET Security Challenges, Attacks and its Countermeasures", International Journal of Emerging Trends & Technology in Computer Science (IJETICS) Volume 3, Issue 1, January – February 2014

[5] Arminder Kaur, Dr. TanuPreet Singh" Securing MANET from jellyfish attack using selective node participation approach " published in International Journal of Engineering and Technical Research (IJETR) ISSN: 2321-0869, Volume-3, Issue-4, April 2015

[6] PriyaMaheshwari, Leenu Singh, "Analysis of Jelly Fish Reorder Atta on ZRP" International Journal of Computer Applications vol 109 No pp 5-7, January 2015

[7] Manjot Kaur1 Malti Rani2, AnandNayyar 3" A Comprehensive Study of Jelly Fish Attack in Mobile Ad hoc Networks" International Journal of Computer Science and Mobile Computing, IJCSMC, Vol. 3, Issue. 4, April 2014, pg.199 – 203

[8] Amandeep Kaur , Deepinder Singh Wadhwa "Effects of Jelly Fish Attack on Mobile Ad-Hoc Network's Routing Protocols" Int. Journal of Engineering Research and Applications ISSN : 2248-9622, Vol. 3, Issue 5, Sep-Oct 2013, pp.1694-1700.