Volume 3, Issue 11, November 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Preventing Flooding Attack in MANET Using Node-to-Node Authentication

Komal Joshi
Student, PVPIT, Pune University, India

Veena Lomte
PVPIT, Pune University, India

Abstract -- MANET is self-configuring infrastructureless wireless network. It means that any node can enter in the network at any time and can left the network at any time. In MANET, for packet delivery, each node has to communicate with other node to establish a route and each node has to maintain a Routing table which provides a fresh route from source node to destination node. MANET faces a flooding attack whose purpose is to drain off scarce resources in other MANET node such as battery power and routing table by flooding a specific node with RREQ messages or false routing information. This prevents registration of any new route in the routing table of victim node. To avoid this problem we need to focus on secure access of route request(RREQ) and route response(RRES) from node to node. In our approach, we are using node-to-node authentication using challenge-response protocol and hash function) framework in which one authenticated node can respond to route request from other authenticated node only. Also, we are using Malicious_Node_Table (MNT) which stores information about malicious nodes present in network. For packet forwarding from source node to destination node, AODV routing protocol will be used . The goal of this approach is to provide node availability and better security for packet delivery in MANET. This paper describes proposed work of our approach to prevent flooding attack in MANET.

Keywords : MANET, Flooding attack, Challenge-response protocol, MNT, AODV

I. INTRODUCTION

Wireless networks use some sort of radio frequencies in air to transmit and receive data. Wireless networks are formed by routers and hosts. Ad-hoc networks are wireless networks where nodes communicate with each other using multi-hop links. Networks that support mobile wireless ad hoc architecture are typically called mobile ad hoc networks (MANET). A mobile ad hoc network (MANET) is a group of mobile devices connected by wireless link without the requirement of fixed common infrastructure in place like wireless access point or radio base station. The MANET provides dynamic topology where devices or nodes in the network can change their position or fade away from the network rapidly. MANET faces two major challenges are limited resources such as battery lifetime and also the security of its routing protocol. In MANET, for packet delivery, each node has to communicate with other node to establish a route and each node has to maintain a Routing table which provides a fresh route from source node to destination node.

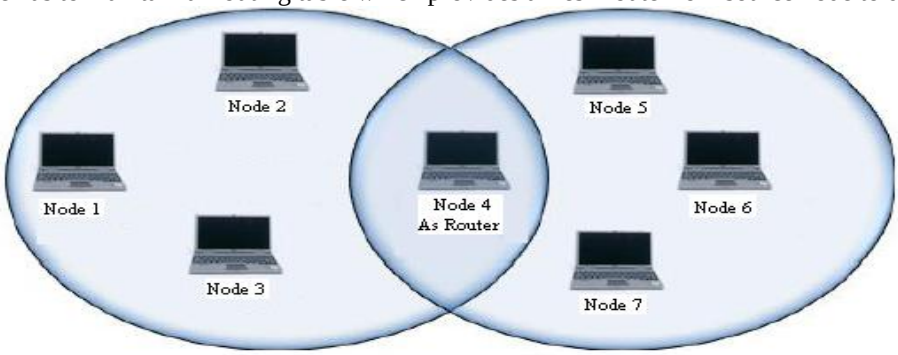

Figure 1: Mobile Ad-Hoc Network with Seven Nodes

Figure 1 shows a simple mobile ad-hoc network with seven nodes. The outermost nodes, nodes 1, 2, 3, 5, 6, 7 are not within the transmitter range of each other. However, the middle node, node 4, can be used to forward packets between the outermost nodes. Node 4 is acting as a router and the seven nodes have formed a MANET.

In this work, we focus on flooding attack in MANET, in which a malicious node sends a frequent RREQ packets or false routing information to it's neighbouring nodes which floods routing table of neighbouring node. This prevents registration of any new route in the routing table of victim node. This type of attack is hard to detect since any normal node with frequently broken routes could legitimately initiate frequent route discoveries. One or more malicious nodes flooding the MANET with RREQ control packets related to false route discoveries can cause a sharp drop in network throughout. To prevent this problem, node-to-node authentication via challenge-response protocol and MNT

(MaliciousNodeTable) will be used. A challenge-response protocol can be chosen where users and nodes can prove their identities by demonstrating knowledge of a shared secret known to be associated with them.

The remainder of this paper is organised as follows: section II. Problem definition, section III. Related work, section IV. Proposed system, section V. Expected results, section VI. Conclusion.

II. PROBLEM DEFINITION

When a new node enters in MANET, it needs to send RREQ packet to its neighbouring nodes to establish a route in MANET for packet delivery. A newly entered node may be a malicious node whose aim is to drain off scarce resources of MANET node such as battery power or routing table by repeatedly sending RREQ packet or false routing information to its neighbouring node. Which results in data packet loss due to wrong routing information stored in routing table of victim node, also malicious node flood the routing table of victim node which prevents registration of any new route in the routing table of victim node.

The Route Request (RREQ) Flooding Attack is a type of denial-of-service attack, which aims to flood the network with a large number of RREQ control packets to the destinations in the network. In this attack, the malicious node will generate a large number of RREQs, into the network until the network is saturated with RREQs and unable to transmit data packets. Many different reactive (on-demand) dynamic routing protocols proposed for MANETs can suffer from this kind of attack. In an on-demand dynamic routing protocol, it usually uses a "route discovery" process to dynamically obtain a route when a node attempts to send a data packet to a destination for which it does not already know the route. The route discovery works by flooding the network with route request (RREQ) control packets. A node that receives a RREQ rebroadcasts it, unless it has already picked it up from another neighbor or it has a route to the destination indicated in the RREQ. If the received RREQ is a duplicate, it will be dropped. If a node has the route because it is the destination or it has learned it in another route discovery, then it replies to the RREQ with a route reply (RREP) packet that is routed back to the original sender of the RREQ. A drawback of blind flooding based route discovery process is the high control overhead. As we know, in an ad hoc wireless network, bandwidth and energy are the two key elements presenting research challenges. Ad hoc network provides limited bandwidth, which makes a network easily congested by control signals such as RREQ, RRES of the routing protocol. As the mobility and load of the network increases, the RREQ control packets used for route discoveries may consume more bandwidth than the data packets. Malicious nodes could exploit this potential weakness of routing protocols. Attackers can initiate much more REEQ control packets than the normal nodes to consume network resource. Since control packets are given higher priority over data packets in transmitting, then at high loads, the wireless channel usage can be completely dominated by the control packets used for route discoveries. In this situation, valid communication can't be kept and normal network nodes cannot be served, then it leads to a kind of denial-of-service attack.

III. RELATED WORK

Significant works have been done in securing the ad hoc network. Some researches defined the method for secure routing but secure routing also can not able to handle the flooding attack.

In [6], the author proposed the distributive approach to prevent the flooding attack. Three threshold values are used in this technique; RATE_LIMIT and BLACKLIST_LIMIT and BLACKLIST_TIMEOUT. If RREQ count of any node is less than RATE_LIMIT then the request is processed else check whether it is less than BLACKLIST_LIMIT, if yes then declared node as black list node but, if the count is greater than RREQ_LIMIT and less than BLACKLIST_LIMIT then put the RREQ in the delay queue and process after BLACKLIST_TIMEOUT occurs. This method can Handel the network with high mobility.

In [7], the author analyzed the flooding attack in anonymous communication. Here the threshold tuple is used which consist of three components: transmission threshold, blacklist threshold and white listing threshold. if any node generates RREQ packet more than transmission threshold then its neighbour discards the packet if it crosses the transmission threshold more than blacklist threshold then it black list the node. But to deal with accidental blacklisting they defined white listing threshold. If any node performs good for number of intervals equal to white listing threshold then it again start treating as a normal node. In [8], the author used the extended DSR protocol based on the trust function to mitigate the effects of flooding attack. In this technique, authors have categorized the nodes in three categories based on the trust value: Friends, acquaintance and stranger. Friends are trusted nodes, Stranger are non trusted nodes, and acquaintance has the trust values more than stranger and less than friends. Based on relationship they defines the three threshold value. If any node receives the RREQ packets then checks the relationship and based on that it checks for the threshold value if it is less than the threshold then forward the packet otherwise discard the packet and blacklist the neighbour node. The main problem with this method was it does not work well with higher node mobility. In [1], the author used the zero knowledge protocol and challenge response protocol for node authentication. The work is divided into two steps. In step-one, the node authentication procedure attempts to determine the true identity of the communicating nodes through a non-interactive zero knowledge protocol. In step-two the authentication procedure seeks again the identities of the communicating nodes through a challenge-response protocol They used challenge response protocol for node to node authentication. The main problem with this method was increased network overhead due to multiple packets used for node authentication. In our work, we are using concept of node authentication via challenge response protocol(CRP) same as [1], which will prevent authenticated node flooding from malicious node. Also we are using MNT for storing information about malicious node detected by CRP. For packet forwarding, we are using AODV routing protocol, security will be maintain by MNT.

IV. PROPOSED WORK

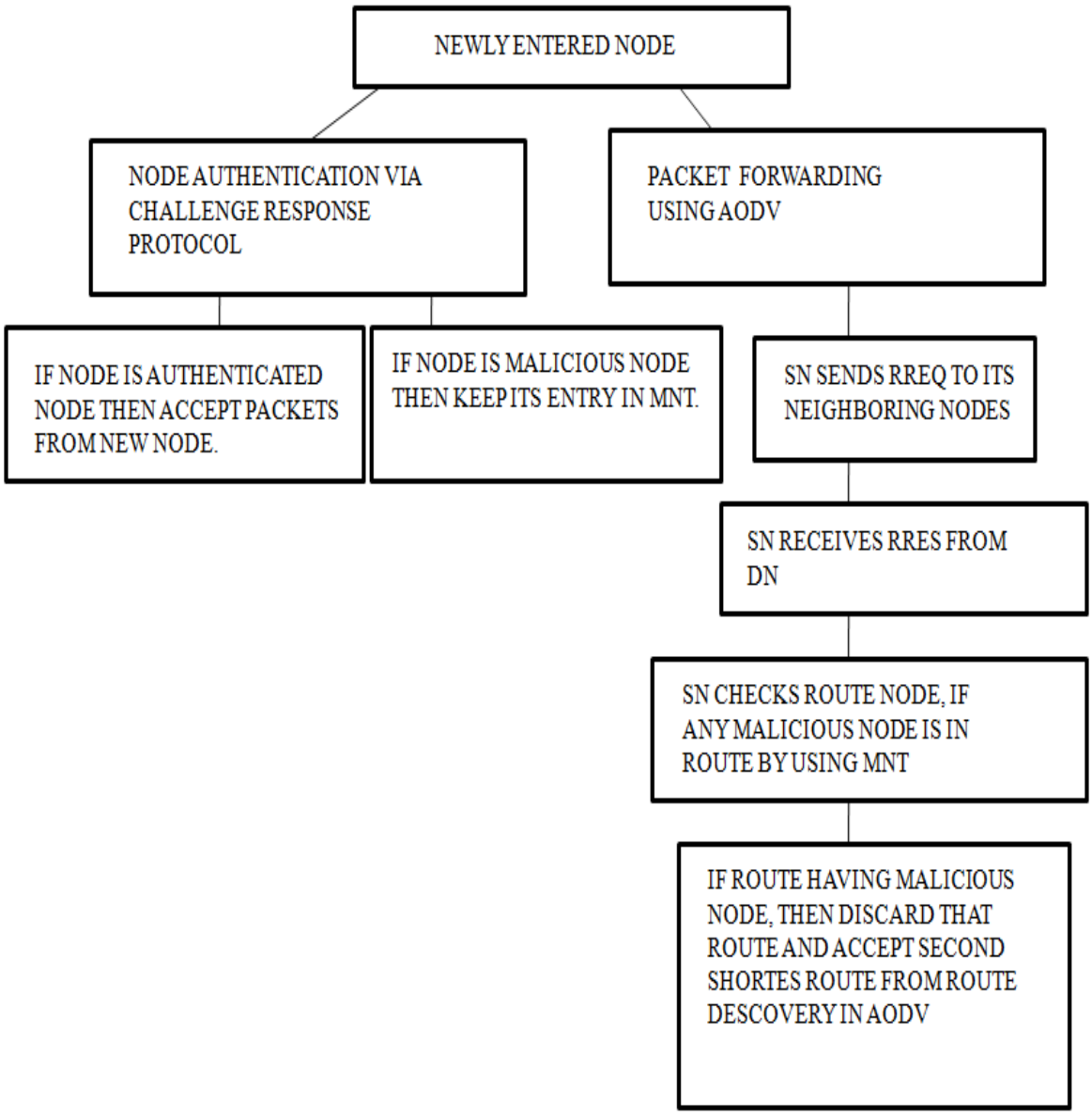

Fig 2: System Flow

- As shown in figure 2, When a new node enters in MANET, it will send RREQ to its neighbouring nodes A and E for validity in network.
- Then neighbouring node will send a data packet containing one secret question using a CRP (challenge-response protocol) and a hash key to newly entered node. (CA will provide a common Hash key to all authenticated nodes in MANET)
- If the newly entered node is authenticated node, then it will use same hash key to answer the question and reply to neighbouring nodes.
- If the newly entered node is not an authenticated node, then it will use its own hash key to answer the question and reply to neighbouring nodes.
- Neighbouring node will check a reply packet, if answer is same as expected then it will forward a RRES packet to newly entered node, else it will declare newly entered node as malicious node and keep its information in MNT (MaliciousNodeTable). And will broadcast a data packet containing information about malicious node.
- Then neighbouring node will discard all incoming messages from malicious node, which prevents flooding a routing table or other scars resources in node.
- when SENDER node want to send a data packet to DESTINATION node, it will broadcast a RREQ for routing information to forward a packet using AODV routing protocol.
- Its neighbouring nodes will reply to SENDER using RRES as per the route available to destination node.
- A sender node then checks the routing path with MNT to check if any node in route is malicious node. If it found any malicious node in rout, it will discard that route and select next shortest route.
- In this way with a secure path, data packet will be delivered to destination node.

A) System architecture

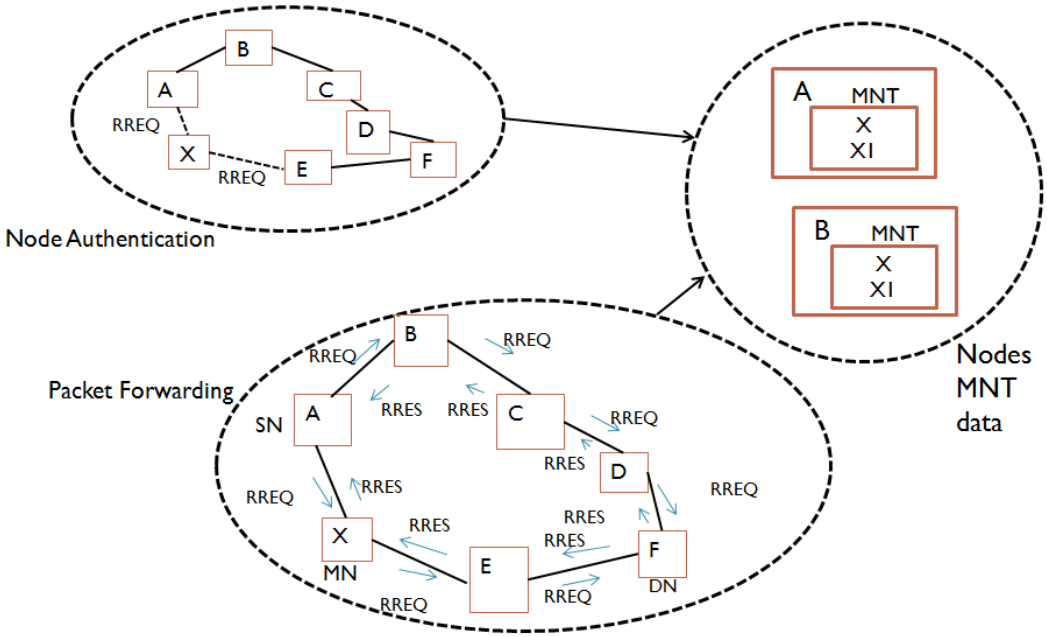

Fig 3 : System Architecture

Where,
X : Newly entered node
A, B, C, D, E, F : Authenticated nodes in MANET
RREQ : Route Request
RRES : Route Response
MN : Malicious node
SN : source node
DN : Destination node
MNT : Malicious Node Table

As shown on figure 3**,** this system is mainly divided into two parts, 1. New Node authentication, and 2. Packet forwarding.

In above figure 3, during node authentication phase, when X enters in MANET, it sends RREQ to A and E. Then node A and E perform CRP to authenticate new node. During packet forwarding phase, suppose node A wants to forward a data packet to node F, it broadcast RREQ to F through its neighbouring nodes. Then node F send RRES. Routes as shown in figure are, A-X-E-F and A-B-C-D-F. As A-X-E-F is shortest path, A will select this route and check all intermediate nodes, if any malicious node present in selected path using MNT. In this case we are considering X as malicious node. Therefore first selected route contains malicious node, so A will discard this route and select second shortest route.

V. EXPECTED RESULTS

The first and foremost goal is to prevent the MANET from flooding attack and have a reliable network services, so we are implementing one of the reliable and novel method using node-to-node authentication. Node-to-node authentication will be done by using challenge-response protocol. To have reliable service, we maintain the MNT (MaliciousNodeTable) in every authenticated MANET node. And for secure data packets transmission we are using AODV routing protocol for route discovery. Also we will be trying to improve some of the factors from packet delay, Data Packet Delivery Ratio, Throughput, control overhead and Number of nodes.

VI. CONCLUSION

In this work, we have firstly summarized the general working of MANET, AODV routing protocol and flooding attack in MANET. Also, the existing solutions are provided with their disadvantages. This scheme has been proposed to provide better solution to flooding attack in MANET. The flooding attack will be tackled here by using node-to-node authentication and MNT. In the future work, the proposed scheme will be simulated to measure the different performance metrics like packet delay Data Packet Delivery Ratio, throughput, control overhead and Number of nodes.

REFERENCES

[1] Nikos Komninos, Dimitris Vergados, Christos Douligeris, "A Two-Step Authentication Framework in Mobile Ad-Hoc Networks, *China Communication Journal.*

[2] C. Perkins et al., "Ad Hoc On-Demand Distance-Vector Routing (AODV)", *IETF draft*, 2001

[3] P T Tharani, K Muthupriya, C Timotta, "secured consistent network for coping up with fabrication attack in manet", *IJETAE*, volume 3, issue 1 jan 2013.

[4] Ping Yi, Zhoulin Dai, Yiping Zhong, Shiyong Zhang "Resisting Flooding Attacks in Ad Hoc Networks" *Proceedings of the International Conference on Information Technology: Coding and Computing* (ITCC'05) 0-76952315-3/05 $ 20.00 *IEEE International Journal of Computer Applications* (0975 – 8887) Volume 5– No.12, August 2010

[5] Bo-Cang Peng and Chiu-Kuo Liang"Prevention techniques for flooding attack in Ad Hoc Networks"

[6] Jian-Hua Song1, 2, Fan Hong1, Yu Zhang1 "Effective Filtering Scheme against RREQ Flooding Attack in Mobile Ad Hoc Networks", *Proceedings of the Seventh International Conference on Parallel and Distributed Computing, Applications and Technologies* (PDCAT'06)07695-2736-1/06 $20.00 © 2006

[7] Venkat Balakrishnan, Vijay Varadharajan,and Uday Tupakula" Mitigating Flooding attacks in Mobile Ad-hoc Networks Supporting Anonymous Communications" *The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications* (AusWireless 2007) 07695-2842-2/07 $25.00 © 2007

[8] Revathi Venkataraman, M. Pushpalatha, Rishav Khemka and T. Rama Rao "prevention of flooding attack in mobile ad hoc network". *International Conference on Advances in Computing, Communication and Control* (ICAC3'09).

[9] Y. Zhang , W. Lee, "Intrusion detection in wireless ad-hoc networks", *Proceedings of the 6th annual international conference on Mobile computing and networking*, p.275-283, Boston, Massachusetts, United States, 2000

