International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Evading Flooding Attack in MANET Using Node Authentication

Anup A. Wanjari[1], Vidya Dhamdhere[2]

[1]Pune University, G.H. Raisoni College of Engineering and Management, Wagholi, Pune, India

Abstract: ***MANET is becoming wide range application as its more abilities and less cost compare to wired network. We should provide security as MANET is of inherent nature. Attack of flooding is belonging to DOS attacks. Attack of flooding disturbs performance by generating the floods of request packets. It blocks the original data packet, which supposed to travel to destination. It weakens the MANET by consuming power batteries space and the bandwidth. Malicious node flooded the hello packets continuously. So the next node cannot send packets to destination. In this case one of neighbor send the error packet to source and source again start the rout discovery function. SO the hello interval value updated and informs other node securely. This process will avoid attack of flooding considerably. This process calculates packet delay, packet delivery ratio, throughput etc. Algorithm achieved by the AODV and will get test in ad hoc network. It will decrees control overhead by 2%.***

Keywords: AODV protocol, Detection of malicious node, Network authentication, SHA-1 Algorithm.

1. Introduction

MANET is consisting of nodes, which are mobile in nature and the links between the mobile nodes. These are getting disturb due to the various attacks occurred on MANET. Components mobile nodes and links construct network. MANET defines their characteristics according to such components. Nodes consisting of characters like mobility, constrained resources, poor physical protection. Wireless link have unique properties like bandwidth and open transmission medium. It shows in fig.1, MANET is influenced by different kind of attacks. DOS is one who make the MANET harmed. This attack is consisting of attack of flooding, wormhole and black hole. These kinds of attacks increase delay, packet loss, and usage of bandwidth. It affects the throughput. In black hole attack source received the fake rout reply from attacked node. In such case node do not forward the packet to destination. In wormhole attack only one attacked node is getting involved.

In attack of flooding message from source is delivered to all nodes and it has relevance in ad hoc networks. For example, algorithms like AODV and DSR depends on flooding to get routing data. Flooding is belonging to DoS attack, and it floods either the control packets or data packet too. It damages the network. It affects resources power, and bandwidth. In the discovery of rout process it may flood RREP or RREQ packets. In such scenario source becomes malicious node. When new node enters in MANET, it will send RREQ to its neighboring nodes for validity in network.

Then neighboring 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 neighboring 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 neighboring nodes. This elaborated in fig1..

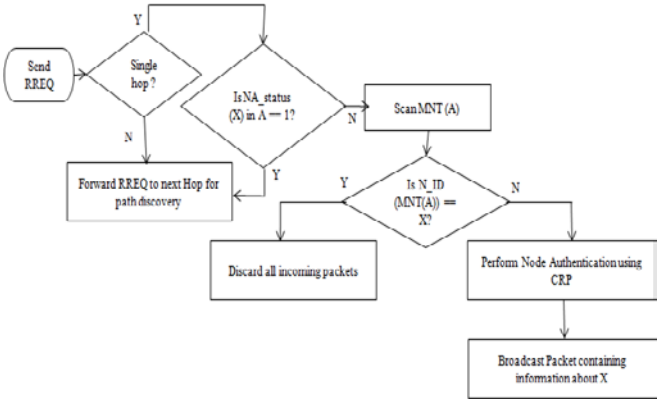

Figure 1: System flow

Neighboring 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 Malicious Node Table (MNT) and will broadcast a data packet containing information about malicious node. Then neighboring node will discard all incoming messages from malicious node, which prevents flooding a routing table or other scars resources in node.

When SENDER node wants 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 neighboring nodes will reply to sender using RRES as per the route available to destination node.
- A sender node then checks the routing path with MNIT 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.

If any one of the malicious node intents to disrupt either the network operations or other node's activity in the network, the malicious node initiates the route discovery process.

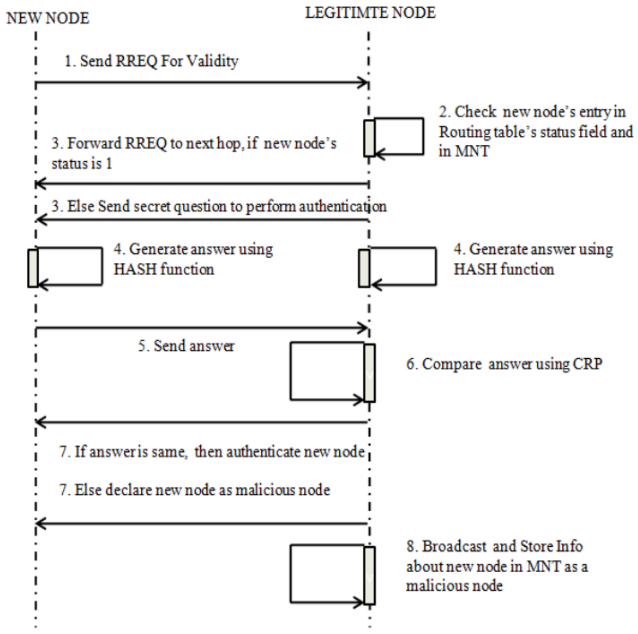

Figure 2: Characteristics and vulnerabilities of MANET

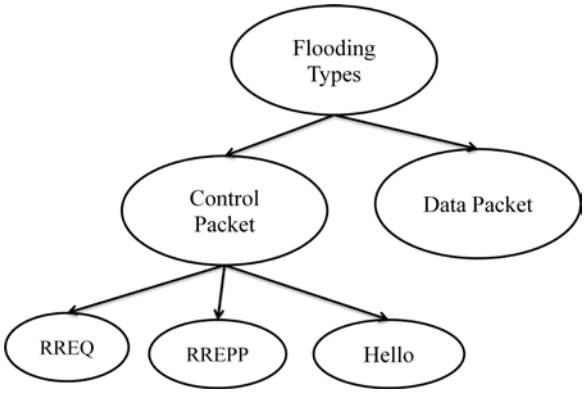

Figure 3: Attack of flooding Types

In Fig.3, there is a control packet named RREP, RREQ and Hello packets. IN DOS attack these control packets get flooded and malicious node does this in process of route discovery. In this process control packets get flooded. It causes overflow of routing tableful the intermediate node. This is due to malicious activity. There are many active attacks. Hello also the same. If hello packets flooded at the malicious node, other packets cannot receive by the neighbor nodes. So the network gets congested. It also exhausted the battery power. It occur wastages of bandwidth and throughput gets degraded.

2. Related Work

Till now so many works have done to secure MANET. But no one can handle the attack of flooding in MANET. First time attack of flooding prevention was defined in [4]. Here they are explained request (RREQ) packet data and flooding packet flooding. They approached separately for request and data flooding. To immune the request (RREQ) flooding, neighbor suppression method was proposed. A node, which sends less RREQ packets, gets maximum priority. It will define threshold value. To overcome data flooding, it approaches path cutoff. Here when node is identified by it, which originated by source then path gets cut off and sends error. Such way attack tries to prevent but up to certain extent but still attack. This overcomes by threshold prevention was define in [5]. This fixed threshold value for each node.

Sender becomes an attacker in case any node in network receives flooding packet greater than threshold. So receiver node discarded packets origin from attacker. We can avoid the flooding issues. But if the intruder knows about threshold then intruder can bypass this mechanism. So the nodes, which are normal in behavior, are treated as malicious node.

In [6], attack of flooding tries to resist by distributive approach. Here two threshold values are proposed named rate limit and blacklisted threshold. If request count of node is lesser than rate limit, the request gets successfully processed else it gets compare with blacklisted threshold. If it is less then node is getting black listed. But if request count lesser than blacklisted threshold and more than RREQ limit then RREQ added to delay queue. The attack of flooding is analyzed by author in [7]. They use the tuple. It contains three components: blacklist threshold, white item threshold and transmission threshold. If RREQ are increasing more than transmission threshold then neighbor node discards packets. If request exceeds transmission threshold then it adds to blacklist. They set the white listing threshold to deal with blacklisting.

3. Materials and Methods

MANET contains routing protocols named reactive, hybrid and proactive. It considers protocol named Reactive outing and postponement of AODV for the security purpose. The reactive protocols reflect the movements begin from source to destination nodes or the middle node that knows route to the destination. The reactive routing protocol is of phases named discovery of Route and transmission of Data. For e.g. route detection process inherits actions as (1) The Route deliver the request from Source node;(2) Every node (except source and node has the way to destination) in path accepts a Request from the preceding node and onwards it; (3) Afterward getting the Request the responding node answers with a Reply message; 4) Reply message is forwarded by a middle node in opposite path. Secure AODV is alike to AODV. Secure AODV uses Cryptographic Mechanism for providing the security in a reactive protocol.

SAODV provides the safety for changeable and non-changeable packet contents. Though, there is possibility of insider outbreaks, like whoosh/tunneling eruptions and the Medium Access Control (MAC) layer misbehavior. Misbehaving of the contributed nodes in network is named Insider attacker. SAODV protocol does not design to endure DOS attacks. The study contracts with attacks exactly for flooding. Fig 5 demonstrations the handling sequence of SAODV. SAODV is the security extension of AODV, founded on public key cryptography. SAODV messages are digitally given to assurance their truth and authenticity (Guerrero, 2001). Therefore, a node makes a routing message symbols it with private key. Nodes receive message verify the signature by the sender's public key.

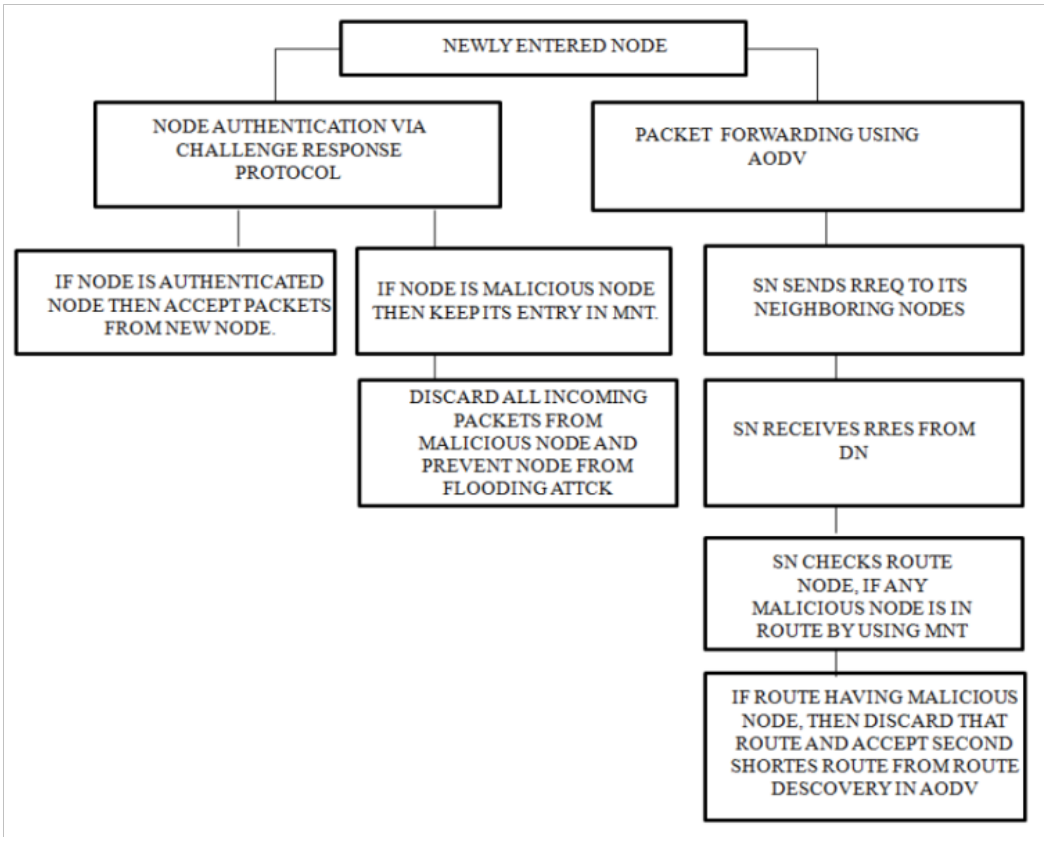

Figure 4: Handling sequence of SAODV

3.1 Hello Message and its Operations

Hello message is a RREP with TTL is 1. It is also signed like RREP. But the hello intervals are not signed because other than active route nodes available in the network, they aren't able to obtain this message. Hello packet is with following fields:

- Destination IP
- Destination Sequence
- Hop Count
- Lifetime

Value is resolute using underneath: HELLO_INTERVAL and ALLOWED_HELLO_LOSS control neighbor's connectivity. HELLO_INTERVAL is period between message broadcasts. ALLOWED_HELLO_LOSS is extreme number of periods of HELLO_INTERVAL to delay without getting a message before and it detects loss the connectivity by its neighbors. HELLO_INTERVAL=1 second and 3 packets of ALLOWED_HELLO_LOSS.

Each node up holds its table of neighbor for preserving native connectivity info about its neighbors. Whenever hello message received by node from its neighbors it does checking route to neighbor node exist in a table of neighbor. It updates the route info by informing period of that neighbors by ALLOWED_HELLO_LOSS*HELLO_INTERVAL else that node makes the entrance for the route in neighbor table. After allowing the entrance of route present node use this route to onward the data. Routes formed by hello messages can't use by other routes and can't generate RERR if any neighbor node travels away and a timeout occurs.

Message called Hello transmitted between neighbors nodes are shown in fig 5.Messages have linked both directionally. In absence of Hello message alongside certain interval by assuming the neighbor assuming the neighbor leaves node away from this network. The route error message is delivered. And the Nodes will respond to message to preserve local connectivity. In attack of flooding, number Hello packets are delivered via node in malicious behavior without seeing interval. The above process reduces time and sending more sums of packets to neighbor and distracted the effort of nodes. Even though, the SAODV is the secured protocol and suffered from inside attackers.

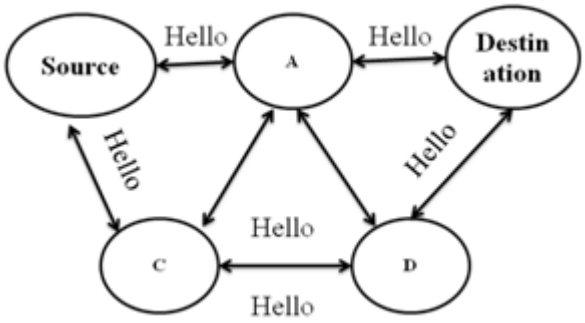

Figure 5: Hello message transmission

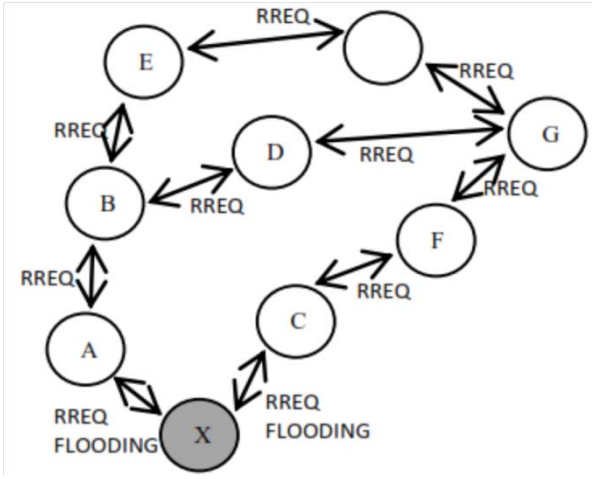

Figure 6: Hello attack of flooding

The Attacks Aware SAODV (FAA-SAODV) provides the answer for flooding. This algorithm is modified from SAODV. After the broadcast the request packet, these nodes are beginning to send Hello packet to neighboring node. Generally the hello interval changes in random way but it is restricted between max and min hello interval values. FAA-SAODV, firstly all nodes are acting normally. Afterward very small time period the malicious sends the hello packet constantly without seeing the intermission.

The goal of study is to know the attack of flooding and prevention method. To preserve the locality is significant work. Some unruly nodes flood the Hello packet constantly without maintaining the interval. It produces the operation. This operation distracts the genuine node's action in network. Fig. 6 specifies flooding.

This method considers interval values are changed in a random. Value encoded and attached in the header part. Node is getting placed in the coverage area are able to process the header part of the packet and update this hello interval value by changing time of sending hello packets its neighbor. But the malicious won't focus the processing of other packets; it constantly sends huge number packets to neighbors. It is unaware of these changes of hello interval.

FAA-SAODV identifies and prevents from this hello attack of flooding it is grounded upon their relationship with neighboring node. It is classified as consistent, malicious nodes. The random intervals used to recognize flooder. Malicious nodes are unaware of change of interval, so it is not changed interval and constantly sends the packet to neighbor.

This behavior exhibits the confirmation of malicious activity and neighbor node ignores the processing of packet. Figure no 5 indicate the general process of FAA-SAODV. Red lines are indicating the malicious action of attacker node. The nodes A and D unable process the continuous hello packets so it is indicated as unidirectional.

FAA-SAODV is used to differentiate node which is malicious founded on 2 step process. Initially all the nodes agreed by sending a hello packet in a fixed interval. First stage is an analysis of the time duration of received packets. Node which has a difference in fixed interval will be assumed as a normal node. Then it performs instant stage for taking decision either a normal or a malicious. Calculation of allowed hello loss is also varying based on the hello interval.

3.2 Malicious Node

The strangers are the unbelievable node. Firstly when node connects the network, then trust connection with its all the neighbor nodes are low or sometime negligible that node is treated as stranger or malicious.

3.3 Normal Node

Friends are most believable nodes, based on the random hello interval. These kinds of nodes are not used to fix hello interval value. Random hello interval value is greater compared to fixed value. Here the highest believable node is mean usage of the randomly changed interval values.

4. Expected Result

The first and foremost goal is to prevent the MANET from attack of flooding and have a reliable network services, so we are implementing one of the reliable and novel method using node authentication. Node authentication made by challenge response protocol. We maintain the Malicious Node Table (MNT) in authenticated node. For security of packets broadcast AODV used. Also we will be trying to improve some of the factors from packet delay, Data Delivery Ratio, overhead, Throughput and Number of nodes.

5. Conclusion

Here we firstly summarized the general working of MANET, AODV and attack of flooding. The existing scheme is provided with their disadvantages. This system has proposed to get improved solution to flooding. The attacks will get undertaken by using authentication and MNT. In future work, scheme which proposed will be simulated to measure the different performance metrics like packet delay Data Delivery Ratio, throughput, control overhead and count of nodes.

References

[1] Nikos Komninos, Dimitris Vergados, Christos Douligeris, "A Two-Step Authentication Framework in Mobile AdHoc Networks,2005.
[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 inmanet", IJETAE, volume 3, issue 1 jan 2013.
[4] Ping Yi, Zhoulin Dai, Yiping Zhong, Shiyong Zhang "Resisting Attack of floodingin Ad Hoc Networks", IEEE,657 - 662 Vol. 2,4-6 April 2005.
[5] Bo-Cang Peng and Chiu-Kuo Liang "Prevention techniques for attack of flooding in Ad Hoc Networks", Volume 3, Issue 11, November 2013.
[6] Jian-Hua Song1, 2, Fan Hong1, Yu Zhang1 "Effective Filtering Scheme against RREQ Attack of flooding in

Mobile Ad Hoc Networks", Proceedings of the Seventh International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT'06) 0-7695-2736-1/06 , 2006 IEEE

[7] Venkat Balakrishnan, Vijay Varadharajan, and Uday Tupakula " Mitigating Attack of flooding in Mobile Ad-hoc Networks Supporting Anonymous Communications" Wireless Broadband and Ultra Wideband Communications, 2007. AusWireless 2007. The 2nd International Conference on Sydney, NSW,IEEE,10.1109/AUSWIRELESS.2007.46,Sydney.

[8] Revathi Venkataraman, M. Pushpalatha, Rishav Khemka and T. Rama Rao "Prevention of attack of flooding in mobile ad hoc network", ACM New York, NY, USA ,2009.

[9] Y. Zhang , W. Lee, "Intrusion detection in wireless ad-hoc networks", Proceedings of the 6th annual international conference on Mobile computing and networking, Conference on Mobile Computing and Networking (MobiCom'2000), August 6–11, 2000, Boston, Massachussetts.)