IJCAT International Journal of Computing and Technology, Volume 1, Issue 3, April 2014
ISSN : 2348 - 6090
www.IJCAT.org

Various Methods for Preventing Flooding Attack in MANET –A Comparative Analysis

[1]Neha K. Holey , [2]Sonal S. Honale

[1] Wireless Communication and Computing, Nagpur University,
Nagpur, Maharashtra, India

[2] Wireless Communication and Computing, Nagpur University,
Nagpur, Maharashtra, India

Abstract - The Mobile Ad hoc Network is an autonomous system of mobile nodes connected by wireless links. 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 a problem known as flooding attack, whose purpose is to drain off limited resources in other MANET node such as battery power and routing table by flooding a particular node with RREQ (Route request) messages or false routing information. This prevents registration of any new route in the routing table of victim node. In this paper survey of various methods for preventing flooding attack in MANET is done.

Keywords **- MANET, Flooding, Flooding attack.**

1. Introduction

An Adhoc network is a self-configuring network that is formed automatically by a collection of nodes without the help of a fixed infrastructure or centralized management. Each node is equipped with a wireless transmitter and receiver, which allow it to communicate with other nodes in its radio communication range. In order for a node to forward a packet to a node that is out of its radio range, the cooperation of other nodes in the network is needed; this is known as multi-hop communication [2]. Examples of ad hoc networks can be found in a range of environments, such as military battlefields, emergency missions, sensor networks, and even virtual classrooms. These networks all require a certain level of security that is network function dependent [1].

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. 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. Because of node mobility, network topology and hence the routes change frequently. Malicious nodes may become part of actively used routes and disrupt network operation. In such an environment, malicious intermediate nodes can be a threat to the security of conversation between mobile nodes. Examples of attacks include passive eavesdropping over the wireless channel, denial of service attacks by malicious nodes and attacks from compromised nodes. When a new node enters in MANET, it needs to send RREQ packet to its neighboring 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 neighboring node. This results in data packet loss due to wrong routing information stored in routing table.

Characteristics of MANET:

- Dynamic Topology
- No cellular infrastructure
- Multi-hop wireless links
- Longer transmission range
- Cost effective

Flooding attack:

Flooding attack is an attack that attempts to cause a failure in network by flooding the network with fake RREQs or data packets.

- It causes congestion of networks.
- It is a type of Denial of Service attack.

- Reduces the probability of data transmission of genuine node

Flooding attack in MANET (when malicious node sends frequent RREQ packets to its neighboring nodes) causes:

- It floods the routing table of neighboring node.
- Drain off scarce resources in other MANET node such as battery power.
- Prevents registration of any new route in routing table of victim node.
- Can cause a sharp drop in network throughput.
- Flooding Attack is hard to detect.

2. Literature Survey

Fan Hong 1 et al [4] presented the effective filtering mechanism to prevent the flooding attack. This technique uses a filter to detect misbehaving nodes and reduces their impact on network performance. The aim of the filter is to limit the rate of RREQ packets. Here each node maintains two threshold values RATE_LIMIT and BLACKLIST_LIMIT. The *RATE_LIMIT* parameter denotes the number of RREQs that can be accepted. If RREQ count of any node is less than RATE_LIMIT then the request is processed as normal. The *BLACKLIST_LIMIT* parameter is used to specify a value that determines whether a node is acting malicious or not. If the number of RREQs originated by a node per unit time exceeds the value of *BLACKLIST_LIMIT*, one can safely assume that the corresponding node is trying to flood the network with possibly fake RREQs. On identifying a sender node as malicious, it will be blacklisted. 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 handle the network with high mobility.

Sunita Sahu et al [7] presented a novel technique which uses the DSR on demand routing protocol to reduce the effect of RREQ flooding attack in the networks with high node mobility.

Netu Singh et al[8] presented a novel technique which uses the trust estimation function and delay queue in basic AODV routing protocol to prevent flooding attack in MANET.

Venkat Balakrishnan et al [5] analyzed the flooding attack in anonymous communication. Here, three components are used: transmission threshold, blacklist threshold and white listing threshold. Effectively identify & eliminate the nodes that are flooding the network. It is not possible to track back the source &destination nodes in an anonymous network.

Revathi Venkatraman et al [6] presented 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 define 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 neighbor node. The main problem with this method was it does not work well with higher node mobility.

Komal Joshi et al [11] presented a node-to-node authentication technique using challenge-response protocol and MNT (Malicious Node Table). Challenge-response protocol prevents authenticated node flooding from malicious node and MNT (Malicious Node Table) used for storing information about malicious node detected by CRP. For packet forwarding, AODV routing protocol is used, security will be maintained by MNT. The goal of this approach is to provide node availability and better security for packet delivery in MANET.

3. Comparative Analysis

Table 1: Comparative analysis of different methods for preventing Flooding attack in MANET

No.	***Methods***	***Advantages***	***Limitations***
1.	Effective filtering scheme [4].	It Handles the network with high mobility.	This method does not able to distinguish between genuine node and forged RREQs from the malicious or victim nodes.

2.	Anonymous Secure Routing protocol [5].	Effectively identify & eliminate the nodes that are flooding the network.	It is not possible to track back the source &destination nodes in an anonymous network.
3.	Extended DSR protocol based on the trust function [6].	The unnecessary traffic is reduced & hence the node able to process the data traffic.	This method does not work well with higher node mobility.
4.	Flooding attack prevention (FAP) [10].	When node identifies that sender is originating data flooding, it cut off path & send error message.	Flooding packet still exists in the network.
5.	Trust based security scheme [7].	Nodes are easily identified based on their relationship i.e stranger, friend and acquaintance.	.It get delay to detect the misbehaving node by allowing him to sends more packet until time out occurs.
6.	Node to node authentication using challenge response protocol and hash function framework [11].	Provide node availability and better security for packet delivery in MANET.	

4. Conclusions

Flooding attack in MANET results in congestion, exhaustion of battery power, wastages of bandwidth and degrades the throughput. In this paper, survey of various methods for preventing Flooding attack in mobile ad hoc network (MANET) is done.

.

References

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

[2] G.Naga Satish, Ch.V.Raghavendran, Prof .P .Suresh Varma, "Intrusion Detection and Prevention in Wireless Adhoc", International Journal of Advanced Research in Computer Science and Software Engineering 3(4), April - 2013, pp. 238-242

[3] Bo-Cang Peng and Chiu-Kuo Liang "Prevention techniques for flooding in Ad hoc networks".

[4] Jian-Hua Song1, Fan Hong1, "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.

[5] 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.

[6] 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).

[7] Shishir K. Shandilya, Sunita Sahu, "A Trust Based Security Scheme for RREQ Flooding Attack in MANET", International Journal of Computer Applications (0975 – 8887) Volume 5– No.12, August 2010.

[8] Ms. Neetu Singh Chouhan, Ms. Shweta Yadav**,** **"**Flooding Attacks Prevention in MANET",International Journal of Computer Technology and Electronics Engineering (IJCTEE) Volume 1, Issue 3, 2011.

[9] Madhavi, S. and K. Duraiswamy, "Flooding attack aware secure AODV", Journal of Computer Science, 9 (1): 105-113, 2013.

[10] 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.

[11] Komal Joshi, Veena Lomte, "Preventing Flooding Attack in MANET Using Node-to-Node Authentication", International Journal of Advanced Research in Computer Science and Software Engineering **,** Volume 3, Issue 11, November 2013.