International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 12 (2015) pp. 31249-31255

http://www.ripublication.com

A Cost Efficient Technique To Enhance The Life Time Of Ad Hoc Networks Under RREQ Flooding Attack

S Nitya Muneendra and K Jeeevan Pradeep

M.Tech, Dept. of CSE, Asst. Professor Dept. of CSE
Sree Vidyanikethan Engineering College, A.Rangampet, Tirupati, 517102, India
nityamuneendra@gmail.com, kjpradeep2011@gmail.com

Abstract

A Mobile ad-hoc network consists of a set of mobile nodes which forms a temporary network without using any centralized point. In *Mobile Ad hoc Networks (MANET)*, various types of attacks are possible because of the inherent limitations of its routing protocols. The attack of initiating / forwarding fake *Route Requests (RREQs)* can lead to exhaust of network resources and hence denial of service to genuine nodes. This type of attack is hard to detect since malicious nodes mimic normal nodes in all aspects except that they do route discoveries much more frequently than the other nodes. The forwarding services conducted by all intermediate nodes exhaust their energy and processing resources. And thus the energy of all nodes will be depleted and therefore the lifetime of ad hoc networks will be shortened. A *Reliability Index Scheme (RIS)* is proposed to mitigate such situations and reduce the loss of throughput. The proposed mechanism could prevent this specific kind of attack and expecting simulation results would reveals that proposed mechanism will enhance the lifetime of ad hoc networks.

Keywords: AODV, routing protocols, flooding attack, Mobile Ad hoc Networks

1. Introduction

A mobile ad hoc network (MANET) is a wireless LAN (Local Area Network) model without the need of central base stations and operated as a self-organized, dynamically changing multi-hop network. MANETs can be applied in medical emergencies, during natural catastrophes, for military applications and conducting geographic exploration. Mobile and wireless devices belonging to a MANET are

usually called mobile nodes. These nodes are characterized by high mobility, low power, limited storage, limited transmission range and finite energy budget without recharging gears. Mobile nodes communicate through bi-directional radio links and data transmission is a key challenge. MANET communication events are called sessions. The two communicating parties, namely the source node and the destination node comprise a session pair (or source–destination pair). A mobile node can communicate directly with other nodes if such a link exists within the radio transmission range. If the distance between a session pair is too large to establish direct contact, the data must then be sent via intermediate nodes connecting the two parties.

2. 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 RREQ flooding attack the attacker selects many IP addresses which are not in the network or select random IP addresses depending on knowledge about scope of the IP address in the network. A single threshold is set up for all the neighbour nodes.

To resist the RREQ flooding, they defined the neighbour suppression method which prioritizes the node based on the number of RREQ received. A node gets higher priority if it sends less numbers of RREQ packets and defined the threshold value. To deal with data flooding they used path cut off method. In this method when node identifies that sender is originating data flooding then it cut off the path and sends the route error message. In this way attack is prevented up to some extent but the disadvantage of this method is flooding packet still exists in the network.

In [9], the author analyzed the flooding attack in anonymous communication. They used the threshold tuple 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 neighbor 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.

This limitation of FAP is eliminated by [8] presented threshold prevention. In this method they defined the fixed threshold value for every node in the network. If any node receives the RREQ flooding packet more than the threshold value then the sender is assumed as a attacker and all the packets from attacker is discarded by the receiver node. This method eliminates the flooding packet but if the intruder has the idea about the threshold value then it can bypass the TP mechanism. Normal node with high mobility is treated as the malicious node.

To extend the method proposed in [6, 7] for higher node mobility, this work proposed the concept of waiting queue. Consider the situation where the node mobility is very higher so all most all the nodes relationship status can be suspect or attacker because to become a reliable to its neighbour, node has to forward many

packets successfully to its neighbour. But because of the higher mobility nodes changes its position frequently so possibility of reliable relationship is very low. The threshold value of the suspect or attacker is lower than the reliable so if any node sends many RREQ packets per unit time because of the mobility this is considered as misbehaviour because its count exceeds threshold limits. Then according to method proposed in [5] the neighbour node discards the packets and declare the node as an intruder or malicious node, which is not true. So to deal with such kind of situations this work proposed the concept of waiting queue here.

3. Proposed approach to prevent RREQ flooding attack

3.1 Problem:

In route request (RREQ) flooding attack, attackers would launch massive RREQ packets with an out-of-domain IP address being its destination node. The reception and re-dissemination of fraudulent RREQ packets would undoubtedly consume much energy.

And also excessive route entries would be added and maintained in the route table of each embroiled nodes for trying to conduct the bogus path discovery. Hence the **Operational lifetime** for the whole ad hoc network would be alleviated accordingly.Issues regarding High Mobility were ignored which leads to denial of service to legal nodes.The existing system fails to enhance the lifetime of ad hoc networks as these techniques itself causes extra processing overhead within addition to the forwarding services carried by the nodes in the network.

3.2 Solution Strategy:

To explore possible solutions for prior flooding attacking issues, a Reliability Index Scheme (RIS) is proposed to mitigate the impact from flooding attacks.

Reliability index is Ratio of number of packet received correctly from the neighbour to the total number of received packet.

Based on their relationship with the neighbouring node, the nodes are divided into two categories that are given below.

- Not reliable node
- Reliable node

The **Not Reliable** node means a node with minimum reliability level. Any new node entering ad hoc network will be not reliable to all its neighbours. There are high chances of malicious behaviour from not reliable nodes.

Reliable node is most trusted nodes or the nodes with highest reliable level can be treated as reliable. Here the higher reliability level means neighbours had received or transfer many packets successfully through this particular node.

During the route discovery phase of the AODV Routing protocol, the reliability index is also computed for all the neighbours of any node. The result of reliability index is the relationship status of all of neighbours as reliable, or not reliable.

3.3 Algorithm

Algo 1:Algorithm RREQ flooding prevention call periodically at interval t

```
Begin
For each Neighbour node i
Do
If node " i " is not blacklisted then
If RRQ_COUNT [i] > Th
I[i] = RI [i] -1;
Else
RI [i] = RI [i] + 1;
End if
End if
If RI[i] == -2 then
Black list node i
End if
Reset RRQ_COUNT [i] = 0
Done
```

Alg 2:Algorithm When intermediate node received RRQ from node i

```
If node i is black listed then
Drop packet from i
Else
RRQ_COUNT [i] = RRQ_COUNT [i] +1
End if
```

4. Implementation andPerformance Evaluation

To detect the flooding attack, when any node receives the RREQ from its neighbours then it performs the following steps:

Where R[i] is used represent received counter. Xtr, Xts and Xta represents threshold value of reliable node, suspect node and attacker node.It increments the R[i] (Received counter) by one which is a counter maintained by one which is a counter maintained by every node for its neighbour which indicates how many RREQ packets it has received from its neighbour.

It checks the Reliability table to check what type of relationship it is having with this neighbour. It could be Reliable or attacker.Compares the R[i] with the corresponding threshold values which is a node maximum number of RREQ packets that can be allowed from its neighbour.

- If the neighbour is Reliable node then it compares whether the **R[i] <Xtr**then it forwards the packet to next hop otherwise discard the packet and blacklist the node.
- If the neighbour is suspicious and the **R[i] < Xts** then it forwards the packet otherwise put the node in to the **WaitingQueue** and allow the node to wait and analyze its behaviour continuously, if still it is misbehaving then declare as a intruder and blacklist the node otherwise treat a normal node.

- If the neighbour is attacker and **R[i] < Xta**then forward otherwise discard the packet and blacklist the node.

In order to evaluate and verify the proposed approach **NS2** (**N**etwork **S**imulator), a network simulation tool was used results show that the proposed approach prevents the RREQ flooding attack and improves throughput. And then the Network lifetime is increased with the prevention of fake requests made by the attackers and shows better performance compared to existing system mechanisms.

Fig: 1 shows the result when node is 10. The X-axis shows number of attacker node & Y-axis shows throughput. Fig: 1 shows throughput is higher in AODV_DEF_Throughput as compare to normal AODV. Fig: 2 shows the Comparison of routing overhead by varying malicious nodes in scenario 10 node. In defended AODV the best result between 200-250 value and In AODV without defense this value between100-150.

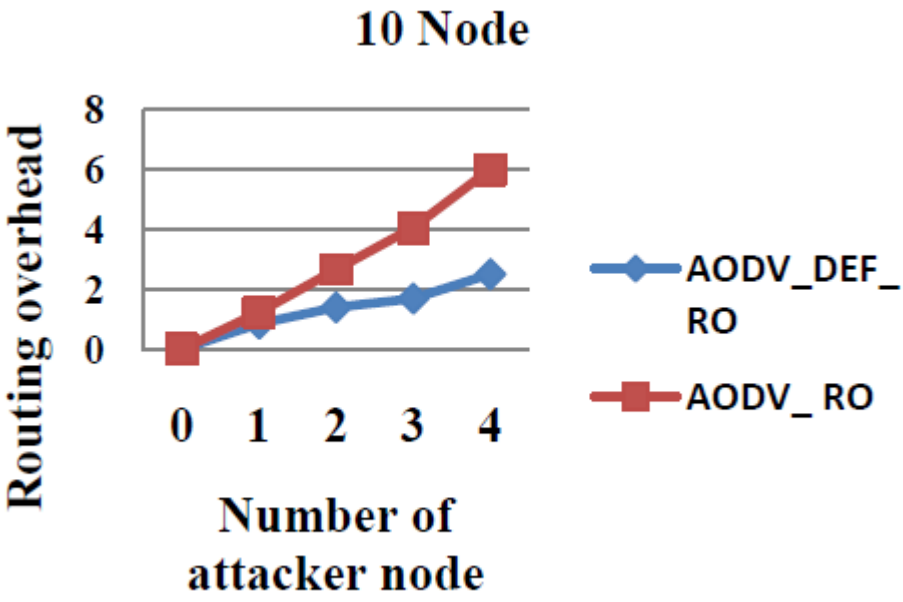

Fig 1: Comparison of Packet delivery ratio by varying malicious nodes in scenario 10 nodes

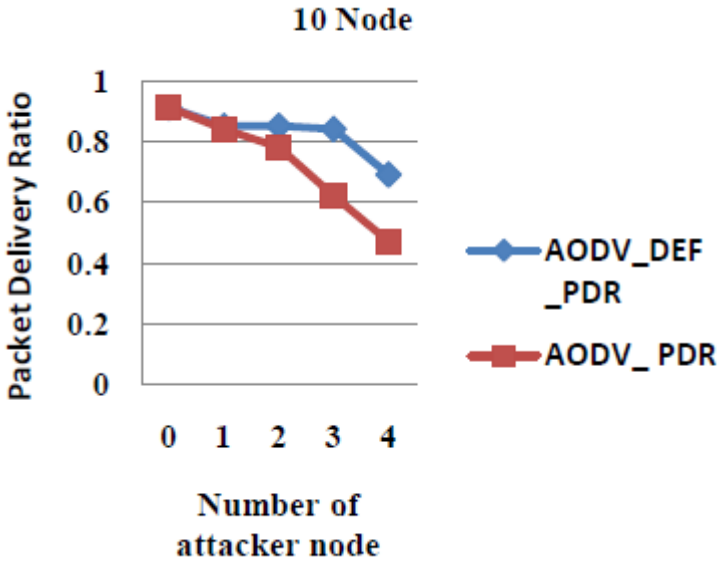

Figure 2: Comparison of Routing overhead by varying malicious nodes in scenario 10 node

5. Conclusion

In this paper, we present a cost efficient approach to detect and prevent the RREQ flooding attack enhances the lifetime of ad hoc networks during RREQ flooding attack. The effectiveness of the proposed technique depends on the selection of threshold values. Although, the concept of waiting queue reduces the probability of accidental blacklisting of the node but it also delays the detection of misbehaving node by allowing him sends more packet until wait queue time out occurs. Future work of this research can be optimise value of threshold and improve their performance.

References

[1] S. Corson, J. Macker, Mobile Ad Hoc Networking (MANET): RoutingProtocol Performance Issues and Evaluation Considerations, IETF RFC2501, January 1999. <ftp://ftp.rfc-editor.org/in-notes/rfc2051.txt>.

[2] C.E. Perkins, R.M. Royer, Ad hoc on-demand distance vector routing,in: The 2nd IEEE Workshop on Mobile Computing Systems andApplications (WMCSA'99), New Orleans, LA, 25–26 February 1999,pp. 90–100.

[3] C.E. Perkins, E.M. Royer, S.R. Das, Ad Hoc On-Demand DistanceVector (AODV) Routing, IETF Experimental RFC 3561, July 2003.<ftp://ftp.rfc-editor.org/in-notes/rfc3561.txt>.

[4] S. Li, Q. Liu, H. Chen, Tan, A New method to resist flooding attacks inad hoc networks, in: IEEE WiCOM 2006, September 2006, pp. 1–4.

[5] 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)0- 7695-2736-1/06 $20.00 © 2006

[6] Revathi Venkataraman, M. Pushpalatha: Security in Ad Hoc Networks: An extension of dynamic Source Routing in Mobile Ad Hoc Networks. In proceedings of the 10th IEEE International Conference on Communication Systems, Singapore, 2006.

[7] Y.Sun et al., Defense of trust management vulnerabilities in distributed networks, IEEE Communications Magazine, February 2008.

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

[9] Venkat Balakrishnan et al. Mitigating Flooding attacks in Mobile Ad hoc Networks Supporting Anonymous Communications. In proceedings of the 2nd International Conference on Wireless and Ultra Wideband Communications (Auswireless 2007).

[10] The Network Simulator Ns2 (2010). <http://www.isi.edu/nsnam/ns/>.