ISSN NO. 2320-5407

Journal homepage: http://www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH

RESEARCH ARTICLE

Detection and prevention of Flooding attack in MANET using node reliability index

Neetu Singh Chouhan[1] and Prachi Jain[2]

1. Assit. Prof Department of CSE, MIT Ujjain, RGPV University, India.
2.Assit. prof. Department of EC, MIT Ujjain, RGPV University, India.

Manuscript Info

Manuscript History:

Received: 12 September 2013
Final Accepted: 24 September 2013
Published Online: October 2013

Abstract

The large number of any centralized infrastructure in mobile ad hoc networks (MANET) is one of the greatest security concerns in the deployment of wireless networks. Thus communication in MANET functions properly only if the participating nodes cooperate in routing without any malicious intention. However, some of the nodes may be malicious in their behavior, by indulging in flooding attacks on their neighbors. Some others may act malicious by launching active security attacks like denial of service.

This research work proposed defense in ad hoc networks against DOS attack. The DOS attack, called Ad Hoc Flooding Attack(AHFA), can result in denial of service when used against on-demand routing protocols for mobile ad hoc networks, such as AODV, DSR. The intruder broadcasts mass Route Request packets to exhaust the communication bandwidth and node resource so that the valid communication cannot be kept.

This research work develops Flooding Attack Prevention (FAP), a defense against the Ad Hoc Flooding Attack in mobile ad hoc networks. The results of this implementation show FAP can prevent the Ad Hoc Flooding attack efficiently. The performance of the reliability index is tested in an ad hoc network implementing the Ad hoc On-demand Distance Vector (AODV) protocol with three parameters throughput, packet delivery ratio and routing overhead. Simulation has been performed on the Ns-2 network simulator. Result shows that proposed approach prevents RREQ flooding attack and blacklists the attacker node.

Introduction

Ad-hoc networks are wireless networks where nodes communicate with each other using multi-hop links. There is no stationary infrastructure or base station for communication each node itself acts as a router for forwarding and receiving packets to/from other nodes

Mobile Ad hoc Network is an autonomous system of mobile nodes connected by wireless links. Each node operates not only as an end-system, but also as a router to forward packets. The nodes are free to move about and organize themselves into a network. Mobile ad hoc networks does not require any fixed infrastructure such as base stations, therefore, it is an attractive networking option for connecting mobile devices quickly and spontaneously, such as military applications, emergent operations, personal electronic device networking, and civilian applications like an ad hoc meeting or an ad-hoc classroom.

In this paper, I have present a new attack, the Ad Hoc Flooding Attack, which results in denial of service when used against all previously on on-demand ad hoc networks routing protocols. In this attack, the attacker either broadcasts a lot of Route Request packets for node ID who is not in networks, or sends a lot of DATA packets to consume the bandwidth so as to congest in links.

2. RELATED WORKS

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.

The first flooding attack prevention(FAP) method was proposed in [6]. In their paper, first they described RREQ flooding and data
flooding. This was the first paper that addressed the prevention of flooding attack in ad hoc network. The authors proposed the
separate approach for RREQ flooding and data flooding. To resist the RREQ flooding, they defined the neighbor 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 cutoff method. In this method when node identifies that sender is originating data flooding then it cutoff 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.

This limitation of FAP is eliminated by [12] 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.

In [11], the author proposed the distributive approach to resist the flooding attack. In this method they have used the two threshold
value; RATE_LIMIT and BLACKLIST_LIMIT. If RREQ count
of any node is less then RATE_LIMIT then the request is processed otherwise check whether it is less then BLACKLIST_LIMIT, if yes then black list the 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 queue time out occurs. This method can Handel the network with high mobility.

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.

In [1], the author used the extended DSR protocol based on the trust function to mitigate the effects of flooding attack. In this work, based on the trust value they categorized the nodes in three categories: Friends, acquaintance and stranger. Stranger are the non trusted node, friends are the trusted node 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 neighbor node. The main problem with this method was it does not work well with higher node mobility.

To prevent the flooding attack in MANET that can work well in higher node mobility situation, we proposed a novel technique which uses the trust estimation function and delay queue in basic AODV routing protocol.

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 neighbor nodes. The given solution is neighbor suppression.

In Data flooding attack the attack node first sets up the path to all the nodes and send useless packets. The given solution is that the data packets are identified in application layer and later path cutoff is initiated. After the data flooding has occurred, the steps are being initiated to curb the flooding attack. Similar solutions are proposed in [9] where a rate-limitation component is added in each node. This component monitors the threshold limit of request packets sent by the neighboring nodes and accordingly, drops the packets if the limit is exceeded.

Data Flooding is also addressed in this work. In our scheme we have categorized the neighboring nodes as strangers, acquaintances and friends with different thresholds Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. and provide a cutoff once the threshold is reached by using the AODV protocol [3]. A generalized trust model and evaluation metric as proposed in [1], is integrated into our extended DSR model. Simulation and analysis is to be carried out wherein the network model is to be test run with different types of attacks. We have modified the AODV protocol to prevent the flooding attack by the neighboring nodes.

3. PROPOSAL FOR FLOODING ATTACK PREVENTION

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

Various parameters which are used for reliability index are: Total number of RREQ packet sent by the neighbour per unit time, Total number of packet successfully transmitted by the neighbour, 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 neighbors. There are high chances of malicious behavior 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.

Initially when node joins the networks they are considered as a suspect. A node is considered as a suspect if nodes have never sent or receive message to or from the neighbor. A node is considered as an attacker if its reliability index is very neither low nor too high means node receives some packet through this neighbor. If node receives many packets to or from any node successfully, then reliability index is very high the node is considered as a reliable node. There is very high probability of attack from suspicious node but very low probability from reliable node. Different threshold values are defined for different types of neighbors to become reliable node, attacker or suspicious. T_a and T_r are the threshold values for the attacker and the reliable respectively. Along with this every node maintains a local counter to count RREQ that is compared with threshold value of neighbors. If RREQ count is less than T_r then neighbor is considered as a reliable and if it is less than T_a and greater than T_r then neighbor is attacker otherwise considered as a suspect.

To extend the method proposed in [6, 7] for higher node mobility, this work proposed the concept of delay 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 neighbor, node has to forward many packets successfully to its neighbor. 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 misbehavior because its count exceeds threshold limits. Then according to method proposed in [11] the neighbor 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 delay queue here.

In this research, 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. X_{tr}, X_{ts} and X_{ta} represents threshold value of reliable node, suspect node and attacker node.

1. 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.

2. It checks the Reliability table to check what type of relationship it is having with this neighbour. It could be Reliable or attacker.

3. 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] is below the threshold value X_{tr} 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] is less than X_{ts} then it forwards the packet otherwise put the node in to the delay queue and allow the node to forward the some packets 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] is less than X_{ta} then forward otherwise discard the packet and blacklist the node.

Algorithm shown in table 3.3 and their description are as follows-

Because RREQ_count sets up 0 every second, it can stand for reliability level which every neighbor node originates. If the RREQ exceeds the threshold, this work may make a judge that it is attacker. When node receives a packet, node firstly look up source ID of packet. If source ID is in Blacklist, node directly discards the packet. If source ID is not in Blacklist, node disposes the packet by normal the threshold is the maximum of originating RREQ in a period time, such as 1 second. If the frequency of originating RREQ of the attacker exceeds the threshold, the node will not receive the RREQ from the attacker any more.

Algorithm shown in table 3.3 and their description are as follows-

Because RREQ_count sets up 0 every second, it can stand for reliability level which every neighbor node originates. If the RREQ exceeds the threshold, this work may make a judge that it is attacker. When node receives a packet, node firstly look up source ID of packet. If source ID is in Blacklist, node directly discards the packet. If source ID is not in Blacklist, node disposes the packet by normal the threshold is the maximum of originating RREQ in a period time, such as 1 second. If the frequency of originating RREQ of the attacker exceeds the threshold, the node will not receive the RREQ from the attacker any more.

Table 3.3 Algorithm for prevention of RREQ flooding attack

Algo -1:
Algorithm RREQ flooding prevention call periodically at interval t :
1 begin
2 for each Neboure node i
3 do
4 if node ‘i’ is not blacklisted **then**
5 if RRQ_COUNT[[i] > Th
6 RI[i]=RI[i]-1;
7 Else
8 RI[i]=RI[i] + 1;
9 End if
10 Endif
11 If RI[i]==-2 then
12 black list node i
13 end if
14 reset RRQ_COUNT[i]=0
15 done
Algo-2:
Algorithm When intermediate node received RRQ from node i
1 If node i is black listed **then**
2 Drop packet from i;
3 else
4 RRQ_COUNT[[i] = RRQ_COUNT[[i] +1;
5 End if

Simulation Setup

NEST (Network Simulation Test bed) → REAL (Realistic and Large) → NS-1 → NS-2

NS-2 is a common network simulator

NS-2 is developed by the VINT project in order to reduce duplication of effort within the network research and develop community

NS2 is publicly available at **http://www.isi.edu/nsnam/ns/ns-build.html**

The performance analysis is done on Linux Operating System. Ns –allinone-2.34 was installed on the platform using cygwin.

Platform	Linux
NS version	Ns –allinone 2.34
Pause time	0, 10,20,50
Simulation time	200 s
Number of nodes	50 wireless nodes
Traffic	CBR(Constant Bit Rate)
CBR Packet size	512 bytes
Transmission Range	250 m
Simulation Area size	657 x 657 m
Node Speed	fixed to 20 m/s
Mobility model	Random WayPoint mobility

Figure 1: Comparison of Throughput by varying malicious nodes in scenario 10 nodes

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. In defended AODV the best result between 200-250 value and In AODV without defense this value between 100-150.

Figure 2: Comparison of Packet delivery ratio by varying malicious nodes in scenario 10 nodes

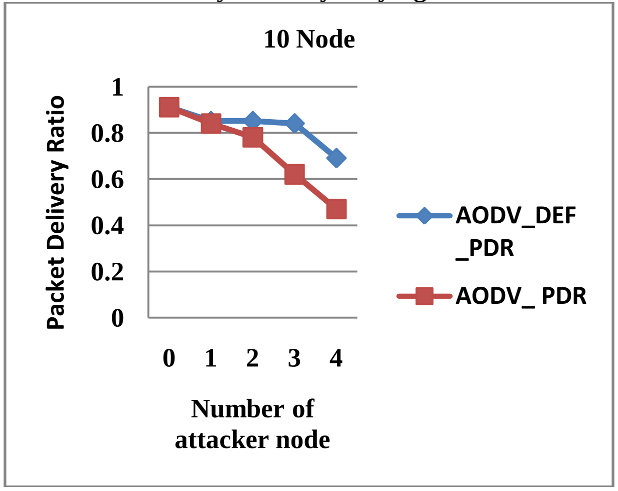
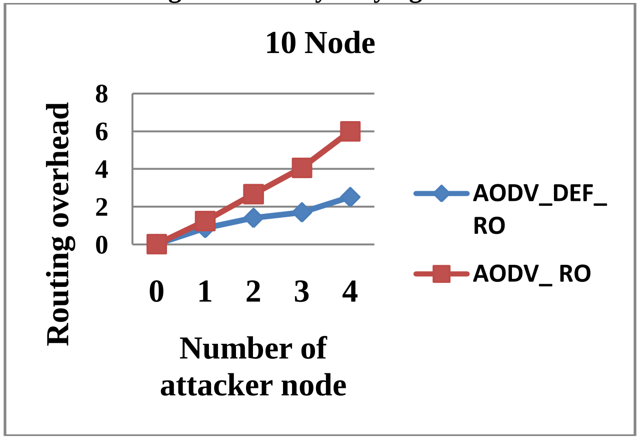


Figure 3: Comparison of Routing overhead by varying malicious nodes in scenario 10 node



The algorithm to prevent DATA flooding is similar to the algorithm discussed in Table 2. The only change is in the DATA flooding threshold values as discussed in this section. On receiving the DATA packets the states of the intermediate node can be obtained by changing the RREQ threshold values to DATA flooding threshold values .

4. CONCLUSION

In this paper, we present a distributive approach to detect and prevent the RREQ flooding attack. The effectiveness of the proposed technique depends on the selection of threshold values. Although, the concept of delay 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 delay queue time out occurs. Further the proposed method can be extended to prevent data flooding also.Future work of this research can be optimise value of threshold and improve their performance**.**

5. REFERENCES

[1] George Theodorakopoulos and John S. Baras, On Trust Models and Trust Evaluation Metrics for Ad Hoc Networks. IEEE JSAC, Vol.24. No.2, February 2006.

[2] Imrich Chlamtac, Marco Conti, Jennifer J.-N. Liu, Mobile ad hoc networking: imperatives and challenges. Ad Hoc Networks I(2003)pages 13-64, Elseiver publications.

[3] Jie Li and Jien Kato, Future Trust Management Framework for Mobile Ad hoc Networks. IEEE Communications Magazine, April 2008

[4] P.Papadimitratos and Z. Hass and P.Samar. The Secure Routing Protocol (SRP) for Ad hoc Networks. Draft-papadimitratos-secure-routing-protocol-00.txt, Dec.2002.

[5] Ping Yi, Zhoulin Dai, Yiping Zhong, Shiyong Zhang: Resisting Flooding Attacks in Ad Hoc Networks. Coding and Computing. ITCC 2005. International Conference on Information Technology Volume 2, Issue, April 2005, 657 – 662.

[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] Y.Sun et al., Information Theoretic Framework of Trust Modeling and Evaluation for ad hoc networks. IEEE JSAC, vol.24, no.2, Feb.2006.

[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] Yi Ping, Hou Yafei, Bong Yiping, Zhang Shiyong & Dui Zhoulin, Flooding Attacks and defence in Ad hoc networks. Journal of Systems Engineering and Electronics, VoL. 17, No. 2, pp. 410- 416, 2006.

[11] 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

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

[13] 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).

[14] Ping Yi, Yue Wu and Futai Zou and Ning Liu, "A Survey on Security in Wireless Mesh Networks", Proceedings of IETE Technical Review, Vol. 27, Issue 1, Jan-Feb 2010.

[15]S.kannan,T.Kalaikumaran,S.Karthik and V.P.Arunachalam "A Review on attack prevention methods in MANET" journal of Modern Mathematics and Statistics 5(1): 37-42, 2011

[16] G. S. Mamatha1 and dr. S. C. Sharma2
"analyzing the manet variations, Challenges, capacity and protocol issues" International Journal of Computer Science & Engineering Survey (IJCSES) Vol.1, No.1, August 2010.

Books

[18] Ad Hoc Wireless Networks, Mohammad Ilyas, Florida Atlantic University, Boca Raton, Florida , Richard C. Dorf ,University of California, Davis

Sites

[19] http://www.isi.edu/nsnam/ns/index.html

[20] Charles E. Perkins , Elizabeth M. Belding-Royer , and Samir R. Das, Ad hoc On-Demand Distance Vector (AODV) Routing , RFC 3561 , July 2003
http://www.ietf.org/rfc/rfc3561.txt

[21] David B. Johnson, David A. Maltz, Yih-Chun Hu, The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR), Internet-Draft, draft-ietf-manet-dsr-09.txt, 15 April 2003,
http://www.ietf.org/internet-drafts/draft-ietf-manet-dsr-09.txt