Volume: 04 Issue: 04 Pages:1695-1699 (2013) ISSN : 0975-0290

Examination of Impact of Flooding attack on MANET and to accentuate on Performance Degradation

Bhuvaneshwari. K
Scholar, Department of Information Science Engineering, Oxford College of Engineering, Bangalore, India
Email:bhuvana.karthikeyan@gmail.com
Dr.A.Francis Saviour Devaraj
Professor, Department of Information Science Engineering, Oxford College of Engineering, Bangalore, India
Email:saviodev@gmail.com

----------**ABSTRACT**----------
Mobile Adhoc Networks (MANET) are new paradigm of wireless networks providing unrestricted mobility to nodes with no fixed or centralized infrastructure. Each node participating in the network acts as router to route the data from source to destination. This characteristic makes MANET more vulnerable to routing attacks. Flooding attack is one such attack which consumes more resource like bandwidth, battery power, etc. Reactive routing protocols like Adhoc On Demand Distance Vector (AODV) and Dynamic Source Routing (DSR) used in MANET has route discovery scheme and this makes it more easy for malicious node to launch flooding attack by flooding the route request packets(RREQ) in the network. In this paper, the behavior of flooding attack and the performance impact of flooding attack on AODV protocol is studied. The NS2 network simulator is used to evaluate the impact of flooding attack on AODV.

Keywords - **AODV, Bandwidth, Flooding attack, MANET, RREQ**

Date of Submission: January 04, 2013 Date of Acceptance: February 10, 2013

1. INTRODUCTION

A Mobile Adhoc Network (MANET) is a collection of wireless devices that moves in a random direction and there by communicating with one another without any fixed or centralized infrastructure[1].The dynamic network topology, distributed operation, infrastructure less network characteristics of MANET[2] makes it appealing for various security attacks like black hole attack, flooding attack, wormhole attack, routing attack, etc. conventional security schemes used in wired networks cannot be directly applied here. Among the security attacks, MANET is particularly susceptible to flooding attack due to the facts that resources are limited and broadcast mechanism is resource consuming. The availability of the resource is also questioned because of this attack. Further the security requirements like authentication, availability and confidentiality has not met because of the inherent limitation of the routing protocols [3].

RREQ flooding attack [4] is a network layer attack launched by the malicious node by sending massive amount of control packets to the network and thereby deplete the network bandwidth, in turn prevent the network from providing services to legitimate users. The flooding attack can target the destination victim or the network as a whole. Here the malicious node behaves like normal node in all aspect except that they initiate frequent RREQ control packet floods. It is very hard to detect these types of attack when the genuine participating nodes turn to be malicious node and exhibit the flooding attack.

This paper aims at studying the flooding attack behavior and its performance impact on AODV routing protocol using NS2 network simulator. Rest of the paper is organized as follows: Section II explains how flooding attack is launched in AODV routing protocol and the attack scenarios. Section III presents the related work done to detect and prevent the flooding attack in MANET. Section IV describes the attack model used for study, simulation study of flooding attack in AODV and its result analysis. Section V explains the conclusion and future work.

2. FLOODING ATTACK IN AODV ROUTING PROTOCOL

AODV is a reactive routing protocol and it establishes route on demand. It has two phases route discovery and route maintenance [5].Route request (RREQ), Route reply (RREP) and Route Error (RERR) are message type defined by AODV. In route discovery process it sends out RREQ message to all its one hop neighbors by broadcast mechanism. Once the route to destination is found then the RREP message is unicast to the source node. Here the intermediate node acts as router to forward the packets from source to destination and vice versa. Whenever an error occurs like link breakage then an RERR message is send. Hello message is sent periodically to know about neighbor node and link connectivity.

AODV routing protocol is vulnerable to RREQ flooding attack because of the route discovery scheme and its

Volume: 04 Issue: 04 Pages:1695-1699 (2013) ISSN : 0975-0290

broadcast mechanism. In AODV there is limit of how much RREQ can be originated by a node. The default value of RREQ_RATELIMIT [6] is 10 as proposed by RFC 3561.Malicious node would exploit this weakness and initiate much more RREQ packets than the normal node in order to consume the network or victims resource. The RREQ packets are given more priority than the data packets; the nodes spend more time in processing the RREQ packets and there by delay the service for the legitimate users.

The flooding attack can be launched by both external attacker and inside attacker [7]. In case of external attacker we can use any of the authentication mechanisms and restrict the external attacker from entering the network and prevent the attack. In case of inside attack it is difficult to detect and the attack intensity is also more. The inside attacker behaves like normal node and send out the genuine route request but the only difference is that it send more amount of route request.

Further the flooding attack scenarios [8] can be classified as four types based on their origination. In first case the attacker send the control packets to the destination that do not exist in the network. Here the network will get congested with control packets hence cannot provide services for genuine users. The network resources like bandwidth also get wasted. In second case the attacker send the control packets from same source to different destination in the network targeting the individual nodes resource. Here each target nodes resource such battery power and memory is wasted. In third case the attacker uses randomized source and destination address there by making it more difficult to identify the attacker. In fourth case the attacker uses different source targeting single destination. It is kind of distributed attack where the attack intensity is diluted by different sources making it difficult to trace the attacker.

3. RELATED WORK

In cryptographic approaches like s-AODV [9], Aridane [10] and SEAD [11], the routing packets are encrypted using symmetric or asymmetric algorithm and hence external or inside attacker cannot modify the packets. However the problem with cryptographic approaches is the increased consumption of processing power and flooding attack can also be launched without forging the packets.

The flooding attack prevention method [12] proposed threshold based prevention technique. If any node RREQ exceeds by predefined threshold value the node refuses to entertain the RREQ from the source node and it is treated as attacker. Packets coming from the attacker are discarded by the receiver node. The malicious node is also suppressed from sending request to other nodes by path cut of process.Here the threshold is static whereas the nodes are highly mobile and the threshold cannot hold good for long time.

Trust [13] and reputation [14] based schemes are used for identifying the attacker inside the network. Here the genuine nodes which turn to be malicious nodes are considered as inside attacker. The trust and reputation value is set as high and low based on how they co-operatively participate in the network. Here the false positive rate is high.

In case of the priority based scheme [15] the priority of the RREQ is reduced. When the malicious node broadcast excessive RREQs ie more the defined limit as per RFC, the priority of those packets will be reduced. The timestamp of the RREQs received are recorded to schedule the priority. Here the genuine RREQ priority can also be at stake.

In route request flooding defence mechanism [16] three components are considered: RREQ binary exponential back off, route discovery cycle binary exponential back off and fast recovery. Here each node should ensure that its neighbour node follows the binary exponential back off. If RREQ are send faster than what is allowed then excessive RREQ is dropped. This process can leave the genuine node to be penalised by dropping the genuine RREQ packets.

In Enhanced packet processing technique [17], the legitimate packet processing at each node is considered. Here the packet processing time for RREQ and data packets at each node is estimated. The buffer size with respect to nodes local density is also considered.

The capability based defence mechanism [18] exchanges the capability messages among the nodes and each node has to maintain a global view of the overall resource usage in the network. Here the destination decides the capability to assign and the intermediate nodes to adhere to the assignment policy However the capability based system are deny by default policy based.

The flow based [19] detection mechanism use the cumulative sum algorithm for effectively detecting the attack based on the characteristics of the malicious node flooding the route request with respect to timestamp The percentage of new flows and ratio of identical flows are used for evaluvation.The traffic pattern analysis states any change in statistical process can bring change in the probability distribution.

4. SIMULATION STUDY

4.1 Scope of study

In this work, flooding attack is simulated in ns2 [20] by using the timer based approach in AODV routing protocol. As per RFC the rate limit for RREQ is defined as 10 per sec.This is overwritten by using the Flood generator function. This function will keep on generating the RREQ irrespective of the rate limit .Hence over a period of time the network has more number of RREQ targeting the destination D. The source generating the RREQ flooding is the node H as shown in Fig.1.

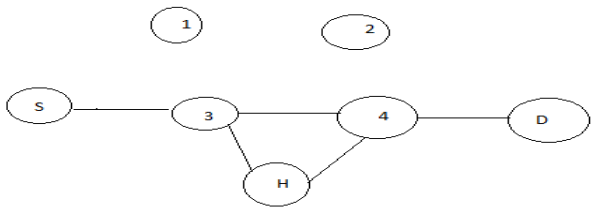

Fig.1 Flooding attack model with attacker node H

Volume: 04 Issue: 04 Pages:1695-1699 (2013) ISSN : 0975-0290

Here the source is S and the destination D which is observed under normal traffic flow. The attacker node H sends the RREQ targeting destination D and also broadcast RREQ to node 3 and 4 to reach D. The AODV.cc file is modified for timer () and broadcast () function. The RATE_LIMIT parameter is added and overwritten. The new agent is created for the modified AODV and attached to the attacker node H.

4.2 Simulation Parameters

The parameters shown below are configured in ns2 network simulator. In our work we used AODV routing protocol and 50 nodes with random way point mobility model [21]. The Mac 802.11 protocol is used. The scenario of two sources targeting the same destination is selected for the following simulation study.

Table.1 Parameters used for simulation

PARAMETER	**VALUE**
Area	1000 * 1000 m
Simulation Time	20s
Number of nodes	50
Traffic Model	CBR
Mobility model	Random Way Point
Number of attacker	2
Data rate	2Mbps
Packet size	512 bytes

4.3 Result Analysis

Performance of AODV routing protocol with and without flooding attack is analyzed in terms of bandwidth consumption, packet delivery ratio and End to end delay.

4.3.1 Bandwidth consumption

It is measured as the average number of packets received by the intermediate node from source to destination over a period of time and expressed in Mbps. Fig.2 shows the bandwidth consumption without attack and with flooding attack in AODV.The bandwidth consumption is more in case of flooding attack as it send out more RREQ packets into the network throughout the simulation time. The percentage difference of how much bandwidth is consumed if flooding attack is launched is shown in the TABLE.2.Here consumption increases as the network is flooded with more RREQ.These RREQ packets occupy the bandwidth of the channel which would otherwise be available for the genuine RREQ or the data packets send by the genuine node.

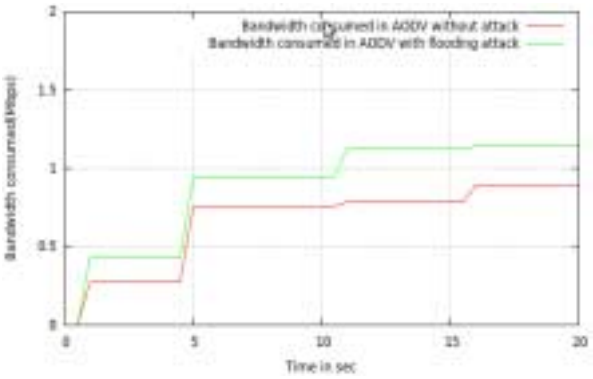

Fig.2 Bandwidth consumption is more for flooding attack than normal AODV

Table.2 Bandwidth consumption in Mbps

Simulation time in sec	Normal AODV in Mbps	Flooding AODV in Mbps	Percentage increase in Bandwidth consumption
5	0.27466132	0.42495641	15%
10	0.75799677	0.94532151	19%
15	0.78889349	1.124932287	33%
20	0.82022096	1.169170742	35%

4.3.2 End to end delay

It is the total time taken for the packet to reach from source to destination and it is measured in seconds.Fig.3 shows the delay with and without flooding attack in AODV. The delay is more in case of flooding attack as the RREQ packets capture the intermediate nodes, the time taken by genuine packets to reach the destination is more. The intermediate nodes are busy processing the fake RREQ and hence delay is more. The difference in delay compared to normal working of AODV is shown in TABLE.3.Here the delay percentage increases as the intermediate nodes give priority to RREQ than the data packets and they are busy processing them.

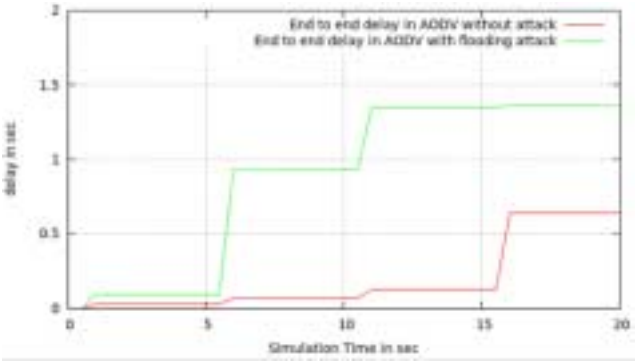

Fig.3 End to end delay more for flooding attack than normal AODV

Volume: 04 Issue: 04 Pages:1695-1699 (2013) ISSN : 0975-0290

Table.3 End to end delay in sec

Simulation time in sec	Normal AODV in sec	Flooding AODV in sec	Delay percentage
5	0.032438	0.095283	63%
10	0.070926	0.932756	86%
15	0.127620	1.349955	92%
20	0.631664	1.574211	94%

4.3.3 Packet delivery ratio (PDR)

The packet delivery ratio is the ratio of number of packets received at destination node to that of number of packets sent by the source node. It is expressed in percentage.Fig.4 shows the delivery ratio with flooding attack and without attack. Here the PDR for flooding attack is less compared to normal AODV. In case of flooding attack the number of packets reaching the destination is delay or dropped due to excess RREQ packets in the network targeting the destination. The destination node is busy replying the fake RREQ and hence packets reaching destination is delayed or lost. TABLE.4 shows the delay percentage comparative study and it drops through the simulation time.

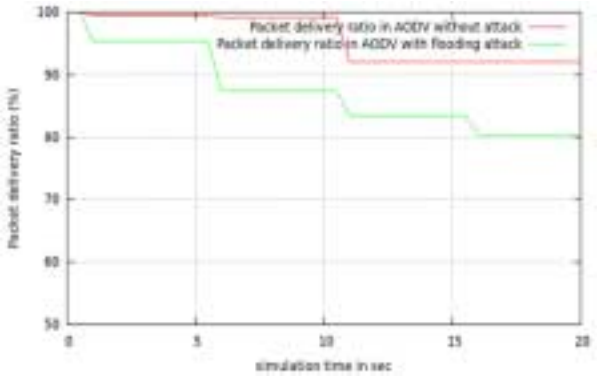

Fig.4 PDR is less for flooding attack than normal AODV

Table.4 Packet delivery ratio

Simulation time in sec	Normal AODV delivery percent	Flooding AODV delivery percent
5	99.5 %	95.3 %
10	99.2 %	87.3 %
15	91.5 %	80.8%
20	91.1%	80%

V. CONCLUSION AND FUTURE WORK

In this paper, the study of flooding attack in AODV routing protocol and its performance impact in terms of bandwidth consumption, end to end delay, and packet delivery ratio has been discussed. The same has been simulated using ns2 and the results are analyzed in detail.

In future a profile based distributive scheme to detect flooding attack on MANET would be proposed and the simulation results for the same would be captured and analyzed to show the effectiveness of the proposed detection mechanism

REFERENCES

[1] 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.

[2] R.H. Khokhar, Md. A.Ngadi, S. Manda. "A Review of Current Routing Attacks in Mobile Ad Hoc Networks", *International Journal of Computer Science and Security*, 2 (3), pp. 18-29, 2008.

[3] C.E Perkins, E.M Royer, "The Ad-hoc on-demand distance vector protocol (AODV)", in *Ad-hoc networking, Addison-Wesley*, pp 173-219, 2001.

[4] P.Ning,K.Sun,"How to Misuse AODV:A Case Study of Insider Attacks against Mobile Ad hoc Routing Protocols",*Proceedings of the 4th Annual IEEE Information Assurance Workshop*,60(2003).

[5] Lee K. Thong. "*Performance Analysis of Mobile Adhoc Network Routing Protocols*". Thesis Paper submitted to the Department of Computer Science, Naval Post Graduate School, Monterey, CA, 2004.

[6] Y.Guo, S.Gordon, "Defending multi-hop ad hoc networks against distributed flooding attacks that use address spoofing", *Proc.ACoRN WMN Workshop*,Sydney,Australia,July,2006

[7] M.G. Zapata and N. Asokan, "Securing Ad hoc Routing Protocols", *Proceedings of the ACM, Workshop on Wireless Security* , pp.1-10,September 2002

[8] J.Mirkovic and P.Reiher,"A source-end defence against flooding denial of service attacks", *IEEE Trans.Dependable and Secure Computing*, Vol.2, No.3, 2005, pp.216-232.

[9] S. Yi and R. Kravets, Composite Key Management for AdHocNetworks.*Proc. Of the 1st Annual InternationalConference on Mobile and Ubiquitous Systems: Networking and Services (MobiQuitous'04*), pp. 52-61, 2004.

[10] Hu, Y., Perrig, A., & Johnson, D. (2002). Ariadne: A Secure On-Demand Routing for Ad Hoc Networks. *Proc. of MobiCom 2002*, Atlanta

[11] R. Oppliger, Internet and Intranet Security, Artech House,1998.Hu, Y., Johnson, D., &Perrig, A. (2002). SEAD: Secure Efficient Distance Vector Routing in Mobile Wireless Ad-Hoc Networks. *Proc. of the 4th IEEE Workshop on Mobile Computing Systems and Applications (WMCSA'02)* (pp. 3-13).

[12] Ping Yi, Zhoulin Dai, YipingZhong, ShiyongZhang,"Resisting Flooding Attacks in Ad hoc Networks" *Proceedings of the International Conference on Information Technology: Coding and Computing (ITC'05)*,IEEE,2005

[13] Shishir K. Shandilya, SunitaSahu, "A trust based security scheme for RREQ flooding attack in MANET" *International Journal of Computer Applications* (0975 – 8887), Volume 5-No.12, August 2010.

[14] Samesh R. Zakhary and Milena Randenkovic,"Reputation based security protocol for MANETs in highly mobile disconnection –prone environments",*International conference on Wireless On-demand Network Systems and Services(WONS*),pp.161-167,Feb.2010.

Volume: 04 Issue: 04 Pages:1695-1699 (2013) ISSN : 0975-0290

[15] S.Desilva and R.V.Boppana, "Mitigating Malicious Control Packet Floods in Ad hoc Networks", *Proceedings of IEEE Wireless Communications and Networking Conference (WCN05),* pp.2112-2117, March 2005.

[16] ZhiAng EU and Winston Khoon Guan SEAH, "Mitigating Route Request Flooding Attacks in Mobile Ad hoc Networks", *Proceedings of International Conferences on Information networking* (ICOIN-2006),Sendai,Japan, 2006.

[17] HyoJin Kim, RamachandraBhargavChitti and JooSeokSong,"Handling Malicious Flooding Attacks through Enhancement of Packet Processing Technique in Mobile Ad Hoc Networks" *Journal of Information Processing Sytems,*Vol.7,No.1,March 2011.

[18] M. Li. An approach to reliably identifying signs of DDOS flood attacks based on LRD traffic pattern recognition. *Computers & Security*, 23(7): 549-558,2004.

[19] YinghuaGuo,StevenGordon,SylviePerreau,"A flow based detection mechanism against flooding attack in mobile ad hoc networks" in *proceedings of WCNC* 2007.

[20] The Network Simulator - ns-2, http://www.isi.edu/nsnam/ns/

[21] GeethaJayakumar, GopinathGanapathi. "Reference Point Group Mobility and Random Waypoint Models in Performance Evaluation of MANET Routing Protocols", *Journal of Computer Systems, Networks, and Communications*, 2008

Authors Biography

Bhuvaneshwari K is currently perusing her M.Tech in computer networks under VTU University. She has 5 years of software industry experience in Retail and healthcare domain providing ERP solutions Her research interest includes security issues in MANET, security in Cloud computing.

Dr A Francis Saviour Devaraj has done his B.Sc and M.Sc in Computer Science from St.Xavier's College, M.E (Computer Science & Engineering) from Anna University. He has obtained his PhD in Computer Science from Manonmaniam Sundaranar University, Tirunelveli. He has also obtained certification in CCNA. He is a life member in technical societies like CSI, ISTE, CRSI, and ISOC. He has around eleven years of teaching experience in leading educational institutions in India and abroad. He has authored/co-authored research papers at the national and international levels. He has attended/conducted national and international level workshops/ seminars/conferences.