A Survey on Secure Routing Schemes Against Flooding Attack

Pooja Raval[1] , Prof. M. M. Patel[2]
[1]PG Department, Smt. S.R. Patel Engineering College,
Dabhi, Gujarat, India
2Asssociate Professor of PG Department, Smt. S.R. Patel Engineering College,
Dabhi, Gujarat, India
[1]poojaraval2130@gmail.com
[2]it43manish@gmail.com

Abstract **- Mobile Ad hoc Network (MANET) is an autonomous system of mobile nodes connected by wireless links. The communication may be via intermediate nodes from source to destination. The nodes are free to move in the network. Ad Hoc On Demand Vector (AODV) routing protocol is superior than different routing protocols in MANET. MANET faces many attacks because of its characteristics. Now-a-days Denial-of-Service attack is grown up and has disturbed whole Ad hoc Network. In this paper we are going to represent work on Flooding Attack by different authors. Flooding Attack is one kind of Denial-of-Service attack in which intruder floods (broadcast) exceed packets in the network so the actual communication cannot be kept. In this paper, secure methods against flooding attack are presented which are surveyed by us.**

Keywords **– MANET, AODV, Security, Denial of Service (DoS), Flooding attack**

I. INTRODUCTION

MANET is an infrastructure less network in which autonomous nodes are wirelessly connected with each other, communicate and create multi hop network for a short period of time or temporarily. In MANET individual nodes are free to move anywhere in the network or out of the network. The nodes of these networks act as routers, which are able to find and maintain routes to other nodes in the network. Mobile Nodes can be anything like laptop, mobile phone, PDA, personal computer etc.

MANETs have many characteristics like Autonomous terminal, Distributed operation, Multi hop routing, Dynamic network topology, fluctuating link capacity, Light weight terminals, Automatic Self configuration, Quick Deployment, Constrained Resources (Battery Power, Wireless Transmitter Range etc.)

Fig.1 Mobile Ad hoc Network[15]

There are few advantages of MANET like,

- Scalable
- Easy to Setup
- Infrastructure less
- Less expensive compare to wired network
- Self-Configuring Network
- Very useful in emergency situations

As shown in beloved figure, there are mainly three types of routing protocols used like Proactive (DSDV, OLSR), Reactive (AODV) and Hybrid (ZRP) protocols in MANET. Proactive protocols found route automatically, maintain all information of each node and also update information regularly. Reactive protocols are also called as on-demand routing protocol. It means when any node wants to communicate to other node in the network, at that time the path will be established and maintain till the communication necessary. Hybrid protocols having the properties of both the protocols proactive protocols and reactive protocols.

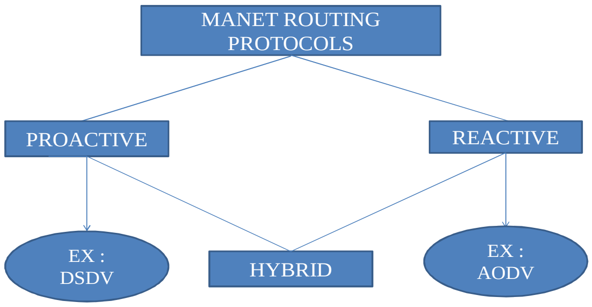

Fig. 2 Routing Techniques in MANET

In Real world, Mobile Ad hoc Network applied in Military battlefield, Commercial Sector, Local Level like conference, Civilian Environments etc. and Personal Area Network. MANET is established in an emergency situations as described above.

The Security services are required in MANET because of nodes are dynamic in mobile ad hoc network. In MANET security issues are,

- Confidentiality
- Integrity
- Availability
- Non-repudiation
- Authentication
- Authorization
- Anonymity

II. ROUTING ATTACKS ON MANET

Because of weak security and decentralized structure, various attacks are occurred by the attacker in the network. The various attacks are classified in two types – First is Active Attack and second is Passive Attack. Active Attack is a type of attack in which attacker can modify the data or information and in Passive attack attacker only can read the data or can observe the pattern of data, he cannot modify the data.

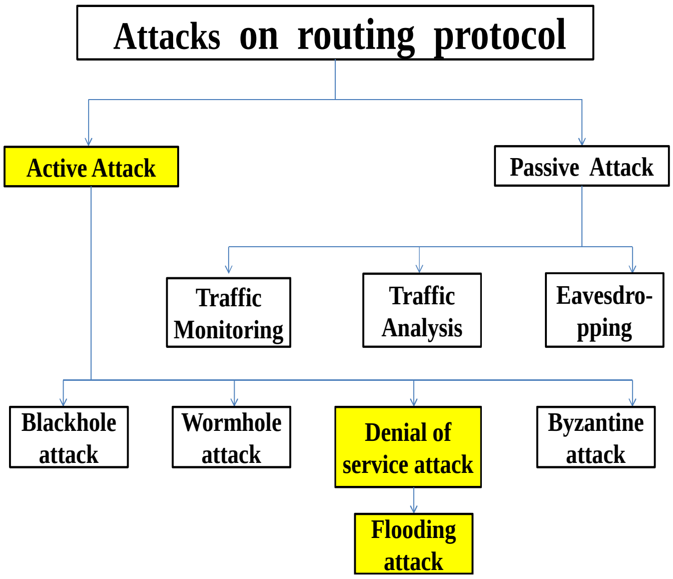

Fig. 3 Routing Attacks

A. *Active Attack*

1) *Black hole Attack :* This attack is a type of Active Attack. In this attacker receive the packet from the previous genuine node and drop that packet, he does not forward this packet to other node.

2) *Gray hole Attack :* Gray hole attack is also called as “Selective Forward Attack” because in this attack the malicious entity will drop some selective means important packets and remaining packets will be forwarded to the next hop in genuine path.

3) *Sybil Attack :* In Sybil attack, attacker node creates a fake identities with the use of other legitimate nodes IP and pretend that I am a genuine node. This type of attack will be difficult to detect.

4) *Denial of Service Attack :* In this Attack, Attacker will send extreme messages in the network so the genuine or legitimate mobile

nodes cannot interact or communicate with each other. The intent of attacker is only that the network will jam and traffic will be created.

5) *Byzantine Attack :* In this method malicious node creates routing loops, forward packets through non-optimal paths or selectively drop packets which results in disruption or degradation of routing techniques.

6) *Worm hole Attack :* In worm hole attack there are minimum two malicious entities. These two entities are create one tunnel between them in the network and whenever one malicious node receive a data packet from the neighbor or any legitimate node it forwards that packet directly to the second malicious node through the tunnel which was created between them.

B. Passive Attack

1) *Eavesdropping* **:** The main goal of eavesdropping is to gain confidential data which should be secret during communication process. This confidential data is like private key or any secret key of nodes.

2) *Traffic Analysis :* In this type of passive attack attacker only observe that which node will communicating with which node at a time.

3) *Traffic Monitoring :* Traffic monitoring states for any wireless network like satellite, wireless LAN, cellular to developed or determine the communication and functional information for the initiation of attacks.

III. INTRODUCTION TO FLOODING ATTACK

Flooding attack is a denial of service type active attack. In this attack, attacker aims to flood the network with the number of fake RREQ control packets or data packets until the network will be saturated with those packets and the genuine communication can’t take place.

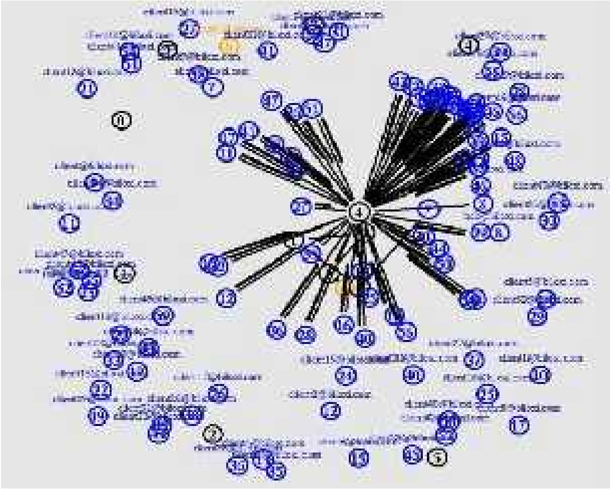

Fig.4 Network under flooding attack[11]

As per the type of packet used to flood in the network, it is classified into three categories which are shown below,

In HELLO mechanism, nodes are broadcast HELLO messages and declare themselves to their neighbors. But some malicious entities in the network flood the excessive HELLO packets without maintaining the time interval it is called **HELLO flooding attack.**

In **RREQ flooding**, the intruder floods the more number of RREQ packets to the node so the legitimate nodes cannot communicate and consume the bandwidth of the network or getting down the network.

In **DATA flooding**, attacker first create a path with the other nodes and after that it sends extreme no. of fake data packets to their neighbors and create a traffic . This attack is very difficult to detect.

IV. SECURE ROUTING METHODS AGAINST FLOODING ATTACK

A. SVM based detection technique[9]

In this technique, the behavior of every node collected initially and save into the XML file. Then this XML file passes to the Support Vector Machine. This machine first extract this file and then it checks the threshold value, if the

node cross the threshold limit they detected as malicious entity or node through the SVM.

B. *Prevent Flooding using Trust level*[14]

In this method every nodes have trust calculator which calculate the trust of their neighbor nodes. Trust level calculate on the basis of three factors. First is a ratio of no. of packets received impact from the neighbor to the total no. of received packet from that node. Second is a ratio of the no. of packets forwarded successfully by the neighbor to the total no. of packets sent to that neighbor. And third is the average time taken to respond to a route request. According to this, the neighbors have categorized into three categories.

- Friends (most trusted)
- Acquaintances (trusted)
- Strangers (non-trusted)

C. *Based on Real time host intrusion detection*[10]

This technique follows the knowledge based intrusion detection methodology to detect intrusions in the network. It operates locally in each node in the network and depends on the network traffic observed by the node. To observe the pattern of the attack, the AODV traffic is analyzed in it is normal scenario and when the attack is in progress. It is based on the idea of Neighbor Suppression algorithm. Here the knowledge based technique is very time consuming task and it should be very careful in analysis of each vulnerabilities.

D. *Restrictive Model (RM) for detect and prevent INVITE flooding attack*[11]

INVITE flooding attack is perform on application layer and related to SIP(Session Initiation Protocol)-based phones. These phones have an ability to initiate a number of calls simultaneously. These type of attacks are difficult to detect because the attacker used the trusted client for launching an attack on SIP server. Trusted client is a authorized person through the previously done authentication process. [Here SIP is most used for signaling and controlling multimedia communication sessions.]

E. *RFAP (RREQ Flooding Attack Prevention) Technique*[13]

In this technique, if node will break the predefine threshold value, it gets punished. First find the attacker node, remove it from the network, give punishment and after that again consider that node as a fault nodes. If attacker breaks rule first time it will punished less but the punishment level will increases when the violation of rules by the attacker are more. In this method malicious node will be recovered after some punishment if their behavior will be genuine.

V. Comparative Analysis

No.	Methods	Advantages	Drawbacks
A.	*SVM based detection technique*[9]	This method is very easy and fast and implementing with NS3	If SVM is crashed then this method cant work.
B.	*Prevent Flooding using Trust level*[14]	Simple and trustful method where nodes are easily identified with their trust relationship	It delays the detection of misbehaving node by allowing him sends

			more packet until delay queue timeout occurs.
C.	*Based on Real time host intrusion detection* [10]	Take the appropriate countermeasure to Reduces the effect of the attack	Knowledge based is time consuming task , It should be very careful in analysis of each vulnerabilities.
D.	*Restrictive Model (RM) for detect and prevent INVITE flooding attack*[11]	Provides a quicker detection of malicious node compare to existing methods , very high detection accuracy	
E.	*RFAP (RREQ Flooding Attack Prevention) Technique*[13]	Gives some punishment to the node which breaks the threshold value and after reasonable punishment re-considers that node as fault nodes.	It only detect the malicious node but don't prevent the attack and cant stop the illegal data packets.

CONCLUSION

MANET's are the most promising field of research but there are always security threats from attacker due to their characteristics. And now-a-days denial of service attacks are very dangerous for MANET. Flooding Attack is the part of this attack. In this survey paper we surveyed some techniques for secure routing against flooding attack in MANET, which detect and prevent the flooding attack. It is the most challenging attack for every wireless ad hoc network.

REFERENCES

[1] L. Abusalah, A. Khokhar, G. BenBrahim, W. ElHajj "TARP: Trust Aware Routng Protocol" (ACM 1-59593-306-9/06/0007, 2006)

[2] Indira N, "Establishing a secure routing in MANET using a Hybrid Intrusion Detection System", (IEEE 978-1-4799-8159-5/14, 2014)

[3] Partha Sarathi Banerjee, Krishanu Das, Subhankar Das, S. R. Bhadra Chaudhuri, "AMSPR: A Secure Multipath Routing in Mobile Ad Hoc Networks (MANET)", (IEEE 978-1-4799-6052-1/14, 2014)

[4] Lu Han, "Wireless Adhoc Networks", October 8, 2004.

[5] Himadri Nathsaha, Dr. Debika Bhattacharya and Dr. P.K. Banrejee, "Secure Multipoint Relay based routing in MANET", ACM 978-1-4503-1310-0/12/10, CCSEIT-2012 Coimbatore.

[6] Jai Shree Mehta, ShilpaNupur, and Swati Gupta, "An Overview of MANET: Concepts, Architecture & Issues", International Journal of Research in Management, Science & Technology (E-ISSN: 2321-3264), April 2015.

[7] Ankur O. Bang andPrabhakar L. Ramteke, "MANET: History, Challenges and Applications", International Journal of Application or Innovation in Engineering &Management (IJAIEM) September 2013, ISSN 2319 – 4847.

[8] Prof**.** B.N. Jagdale and Mrunal S. Patil , "Emulating Cryptographic Operations for Secure Routing in Ad-hoc Network " , IEEE

2015 , International Conference on Pervasive Computing (ICPC).

[9] Jiwen CAI , Ping YI , Jialin CHEN, Zhiyang WANG, Ning LIU , “An Adaptive Approach to Detecting Black and Gray Hole Attacks in Ad Hoc Network ”, 2010 24th IEEE International conference on Advanced Information Networking and Applications.

[10] Mohamed M. Ibrahim , Nayera Sadek , Mohamed EI-Banna, “Prevention of Flooding Attack in Wireless AdHoc AODV-based networks using Real-time Host Intrusion Detection” (IEEE 978-1-4244-3474-9/09 , 2009)

[11] Muhammad Asif Raza,Asim-ur-Rehman Khan and Muhammad Raza, “A Restrictive Model (RM) for Detection and Prevention of INVITE Flooding Attack”, (IEEE 978-1-4673-5885-9/13, 2013)

[12] Meenakshi Patel, Sanjay Sharma, Sanjay Sharma, “Detection and Prevention of Flooding Attack Using SVM”, (IEEE 978-0-7695-4958-3/13, 2013)

[13] Kashif Laeeq,"RFAP, A Preventive Measure against Route Request Flooding Attack in MANETS", *IEEE*, 2012.

[14] Ms. Neetu Singh Chauhan, Ms. Shweta Yadav, “Flooding Attacks Prevention in MANET”, IJCTEE, 2011

[15]https://www.google.co.in/search?q=mobile+ad+hoc+network&biw=1366&bih=667&tbm=isch&tbo=u&source=univ&sa=X&ved=0ahUKEwicnIWm8KbMAhVHbY4KHRuAAjAQsAQIKw#imgrc=1aQVBe1kdu9aKM%3A