2nd International Conference on Recent Advances in Management, Architecture, Technology and Engineering (ICRAMATE'16)
1st -2nd April 2016
Organized by
International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Volume 2, Special Issue 10, April 2016

Firewall based signature enhancement for flooding attack in MANET

Harikrishnan Nair M P[1], Sreeja Nair M P[2]
UG Scholar, Department Of ECE,PSN College Of Engineering and Technology, Tirunelveli, Tamilnadu, India [1]
Asst.Prof, Department Of CSE, Cochin University College of Engineering Kuttanad, Alappuzha, Kerala,India[2]

Abstract:A mobile adhoc network (MANET) is a continuously self-configuring, infrastructure-less network of mobile devices connected without wires. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. This document gives formatting instructions for authors preparing papers for publication in the Proceedings of an MANETs are vulnerable to various types of attack because of its features like continuous changing topology, resource constraints and unavailability of any centralized infrastructure. Many denial of service type of attacksare possible in the MANET and one of these type attacks is flooding attack in which malicious node sends the useless packets to consume the valuable network resources. In this paper we present a novel technique to prevent flooding attack in MANET.

Keywords: DoS Attack,MANET,Flooding

I. INTRODUCTION

A Mobile Ad-hoc Network (MANET) is a temporarywireless network composed of mobile nodes without aninfrastructure. A MANET may be suitable for networks withinairports, meeting rooms, and open spaces due to botheconomical and technological feasibilities. Because theMANET is based upon IP protocol suites, a node in theMANET cannot take part in unicast communications until it isconfigured with a free IP address.[1]

Mobile adhoc networks have been gaining popularity because ofavailability of low cost mobile devices and its ability to provideinstant wireless networking capabilities where implementation ofwired network is not possible or costly. MANET is a collection ofmobile node with routing capabilities and connected with wirelesslink. Mobile node can directly communicate to each other if theyfall in the radio coverage range of each other [4]. In order toforward the packet to the node which is beyond the coveragerange, MANET uses the concept of multi hop communication.Nodes in the MANET are free to move, which dynamicallychanges the topology of the network. It does not require anyexpensive infrastructure to support the mobility [2][4]. Creating theAd hoc networks is possible where implementation ofinfrastructure is not possible or expensiveMANET is generally formed for short range communication.The performance/speed of the network depends on the number ofdevices; it degrades as the number of device increases because allthe devices share the available network resources.Like conventional wired network MANET also uses routingprotocols to route the packets to its destination. Ad hoc networksrouting protocols are divided into two categories: Proactive andreactive [5].Proactive routing protocols are also known as "table driven"routing.In this, all the nodes store the routing information aboutother node present in the networks and routing updates are propagated in the network whenever network topology changes.

The advantage of proactive routing protocol is that nodeexperiences minimal delay when route is needed and unexpiredroute is available in the routing table but the disadvantage ofproactive routing is that these are not scalable and maintenance ofrouting table requires substantial network resources.

In the case ofreactive routing protocol, route between the nodes is searchedonly when node wants to communicate with other node. Todiscover the routes they use route discovery procedure which inturns uses the flooding method. In this, initiator forwards theRREQ packet to its entire neighbor's. If neighbor has the route fordestination they reply otherwise forward the RREQ to the nextnode. In this way RREQ packet reaches to the destination whichsends the reply to RREQ. But the method which is used tofacilitate route discovery are used by the Intruders or themalicious node to consume the network resources which may leadto flooding attack [2][6].

In this paper, we propose a novel technique which uses thefirewall based signature routing protocol to reduce the effect of RREQflooding attack in the networks with high node mobility.

II. ATTACKS

Mobile Ad hoc networks are vulnerable to various attacks not only from outside but also from within the network itself. Ad hoc network are mainly subjected to two different levels of attacks. The first level of attack occurs on the basic mechanisms of the ad hoc network such as routing. Whereas the second level of attacks tries to damage the security mechanisms employed in the

network. The attacks in MANETs are divided into two major types [6].

1. External Attack: External attacks are carried out by nodes that do not belong tothe network. It cause

congestion sends false routing information or causes unavailability of services [6].

2. Internal Attack: Internal attacks are from compromised nodes that are part of the network. In an internal attack the malicious node from the network gains unauthorized access and impersonates as a genuine node. It can analyse traffic between other nodes and may participate in other network activities.

External attacks can classify into two categories:

- Passive attack
- Active attack

2.1 Passive attack

A passive attack does not actually disrupt theoperation of the network.'e.g.snooping: Snooping is anauthorized access toanother person's data.

2.2 Active attack

An active attack attempts to alter or destroy the databeing exchanged in the network

TYPES OF ACTIVE ATTACKS ON VARIOUS LAYERS IN PROTOCOL STACK [2]

Layers	Types of Attacks
Application	Malicious code, Data corruption, viruses and worms
Transport	Session hijacking attack, SYN Flooding attack
Network	Black hole, wormhole, Sinkhole,Link spoofing, Rushing Attack, Replay attacks, Link Withholding, Resource Consumption Attack, Sybil attack
Data Link	Selfish misbehavior, malicious behavior, traffic analysis
Physical	Eavesdropping, jamming

Table 1

There are a lot of security attacks in each layers ofnetwork. In wired networks, well defined routers areavailable, In MANETS theintermediate nodes actasrouters, because of this, the network user and the malicious attacker can access each and every node unlike wired network. The table 1 gives a clear picture of the functionsand security issues on the major layers of the network.

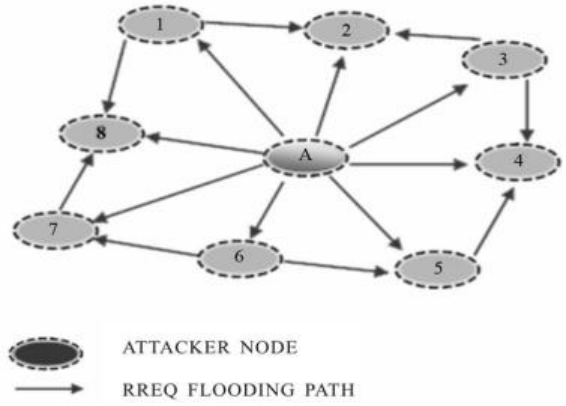
FLOODING ATTACK

In flooding attack, attacker exhausts the network resources, such as bandwidth and to consume a node's resources, such as computational and battery power or to disrupt the routing operation to cause severe degradation in network performance [2]. For example, in AODV protocol, a malicious node can send a large number of RREQs in a short period to a destination node that does not exist in the network. Because no one will reply to the RREQs, these RREQs will flood the whole network. As a result, all of the node battery power, as well as network bandwidth will be consumed and could lead to denial-of-service.

Flooding attack is a denial of service type of attack in which the adversaries' node broadcast the redundant false packet in the network to exhaust the available resources and reduces the throughput of the network so that valid or legitimated user can not able to use the network resources for well-defined communication. The flooding attack is possible in all most all the secure on demand routing like SRP, SAODV, ARAN, Ariadne etc. Flood attacks occur when a network or service becomes so weighed down with packets initiating incomplete connection requests that it can no longer process genuine connection requests. By flooding a server or host with connections that cannot be completed, the flood attack eventually fills the host's memory buffer. Once this buffer is full no further connections can be made, and the result is a Denial of Service. The number of RREQ that can be originated per second is limited. After broadcasting a RREQ, the initiator will wait for a ROUTE REPLY. If a route is not received within round-trip milliseconds, the node may try again to discover a route by broadcasting another RREQ; until it reaches a maximum of retry times at the maximum TTL value. But for the second RREQ, the time to wait for the ROUTE REPLY should be calculated according to a binary exponential back off, by which the waiting time now becomes 2 * round-trip time. Depending upon the type of packet used to flood the network, flooding attack can be categorized in two categories.

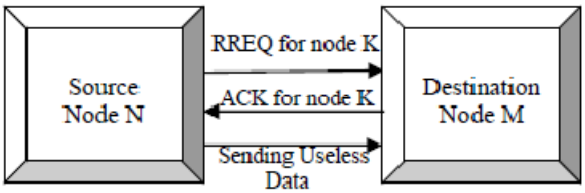
RREQ FLOODING [2]: In RREQ flooding attack the attacker selects many IP addresses which are not in the network or select random IP addresses depending on knowledge about scope of the IP address in the network. In Malicious RREQ Flooding attack an intruder broadcasts a RREQ with a destination IP address and does not wait for the ring traversal time and continuous

resending the same packets with higher TTL value.



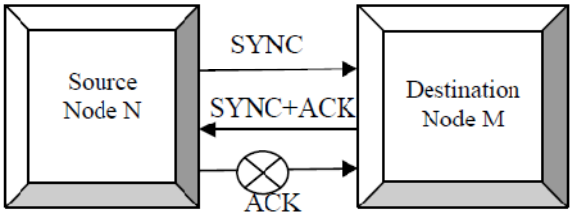
RREQ Flooding Attack

DATA FLOODING: In the data flooding, malicious node flood the network by sending useless data packets. In the data flooding, first malicious nodebuilt a path to all the nodes then sends the large amount of fake data packets[2].



Data Flooding Attack

SYN Flooding: In SYN flooding attack, attacker or flooder node sends the number of synchronization packet to the destination node. Hence the large amount of memory will be consumed through this attack.[2]



SYN Flooding Attack

III.RELATED WORK

In Fan Hong, Yu Zhang and Jian-Hua Song, the author planned the new methodology to conflict the flooding attack. In this technique they implementing two thresholds value namely, ratelimit and blacklistlimit. If no. of RREQ is less than ratelimit then the request succeeded else check it is less than blacklistlimit or not. If yes then make node black listed but if the no. of nodes greater than rreqlimit and less than blacklistlimit then place the RREQ in the delay queue. Then process after time out occurs. These techniques can handle the network with high mobility.

In Venkat Balakrishnan, Vijay Varadharajan and Uday Tupakula, they analyzed the flooding attack in unidentified communication. In this technique mainly three components are used: blacklist threshold, whitelisting threshold and transmission threshold. Efficiently recognize & reject the nodes which flood the network. In this unidentified network it's impossible to track back destination and source nodes.

In M. Pushpalatha, T. Rama Rao and Revathi Venkataraman, they presented the extended AODV protocol based on the trust factor. 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 which has the trust factor less than the friends and greater than the stranger is called acquaintance. This technique does not work with higher node mobility.

In Komal Joshi and Veena Lomte, the authors introduce a node-to-node verification technique using challenge-response protocol and MNT (Malicious Node Table). Challenge- response protocol (CRP) checks genuine node flooding from malicious node and MNT (Malicious Node Table) used for storage information about malicious node noticed by CRP. AODV routing protocol is used for packet forwarding and security will be maintained by MNT. The aim of this technique is to provide node accessibility and better security for packet transfer in MANET. It does not provide better packet delivery ratio, throughput and control overhead.

In Kashif Laeeq , author introduces RFAP technique for transforming the RREQ (route request) flooding attack on AODV protocol in MANET. The result analysis shows that, the RFAP technique can identify the malicious flooder node and protects the network properties from flooder or attacker node (flooding attack). At the time of flooding attack, original AODV protocol can create defective result compare to RFAP technique. RFAP technique can easily find the flooder or attacker node and defend the network from RREQ flooding attack. The RFAP technique cannot stop the illegal data packets.

IV.PROPOSED SYSTEM

In this paper, we propose a novel technique which uses the firewall based signature routing protocol to reduce the

effect of RREQ flooding attack in the networks with high node mobility.

In computing, a firewall is a network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules.[3] A firewall typically establishes a barrier between a trusted, secure internal network and another outside network, such as the Internet, that is assumed to not be secure or trusted. Firewalls are often categorized as either network firewalls or host-based firewalls. Network firewalls are a software appliance running on general purpose hardware or hardware-based firewall computer appliances that filter traffic between two or more networks. Host-based firewalls provide a layer of software on one host that controls network traffic in and out of that single machine. Firewall appliances may also offer other functionality to the internal network they protect such as acting as a DHCP or VPN server for that network.

Originally, a firewall was a wall that was built to stop (or slow down) the spread of a fire. In terms of computer security, a firewall is a piece of software. This software monitors the network traffic. A firewall has a set of rules which are applied to each packet. The rules decide if a packet can pass, or whether it is discarded. Usually a firewall is placed between a network that is trusted, and one that is less trusted. Three parts are: (1) Attack Detection Agent (ADA), (2) Defense Service Provider (DSP), and (3) Rate Limiter (RL).

ADA is installed as a software or hardware in the victim or the firewall. It is responsible for sending an alert and a defense request to the DSP, as soon as an attack is detected. The DSP is responsible for processing the defense service orders and provide defense services. When it receives a defense request, it verifies its authenticity to make sure that, it is not a new DoS attack. It then performs rate limit decision-making and sends rate limit commands to RL. The RL is responsible for limiting the rate of one specific flow. It also reports the approximate real-time rate information to the local DSP. RL is deployed by the Internet Service Provider and managed by the local DSP server in the same domain.

V.TECHNOLOGY BACKGROUND

ARBITRATED DIGITAL SIGNATURE AS AN ATTACK DETECTION AGENT

Every signed message from a sender to a receiver Y first goes to an arbiter A(Here router),who subjects the message and its signature to a number of tests to check it's origin and content. The message is then dated and sent to Y with an indication that it has been verified to the satisfaction of an arbiter.[3]

Here we used a public key scheme arbitrated digital signature.In this case, X double encrypts amessage M first with X's private key,PR_X and then with Y'S public key,PU_Y.This is the signed secret version of the message.This signed message,together with X's identifier is again encrypted with PR_X and together with ID_X,is sent to A.The inner double encrypted message is secure from arbiter (and everyone else except Y).However A can decrypt the outer encryption to assure that the message must have come from X(because only X has PR_X).A checks to make sure that X's private/public key pair is still valid and,if so verifies the message. Then A transmit the message to Y, encrypted with PR_a.The message includes ID_X, the double encrypted message and a time stamp.[3]

PACKET FILTERING FIREWALL AS A DEFENSE SERVICE PROVIDER

A packet filtering router applies a set of rules to each incoming and outgoing IP packets and then forwards or discards the packet. The router is typically configured to filter packets going in both directions. Filtering rules are based on information contained in the network packet:[3]

- Source IP Address
- Destination IP address
- Source and destination transport-level address
- IP protocol field
- Interface-port numbers

The packets filter typically setup a list of rules based on matches to fields in the IP or TCP header.If there is a match to one of the rules,that rule is invoked to determine whether to forward or discard the packet. If there is no match to any rule, then default action is taken. Two default policies are possible:

- Default=discard: That which is not expressly permitted is prohibited
- Default=forward: That which is not expressly permitted is prohibited

The default discard policy is more consecutive.Initially,everything is blocked,and must be added on case –by-case basis.This policy is more visible to users, who are likely to see the firewall as a hindrance. The default forward policy increases ease of use for end users but provides reduced security; the security administrator must, in essence,react each new security threats as it becomes known.

The digital signature authenticates and validates the message packets then the packet filtering firewall filters or forward or block packets to the destination.The Rate Limiter is the router itself.

VI.ADVANTAGES OF PROPOSED SYSTEM

- No Information is shared among the parties before communication,preventing alliances to defraud.
- No incorrectlydated message can be sent,even if PR_X is compromised,assuming PR_a is not compromised.
- The content of the message from X to Y is secret from A and anyone else.
- A firewall defines a single choke point that keeps unauthorisedusers out of the protected network,prohibits potentially vulnerable services from entering or leaving the network.
- A firewall provides a location for monitoring security related events

A firewall protects one part of the network against unauthorized access.
A firewall is often installed away from the rest of the network so that no incoming requests get directly to the private network resource. If it is configured properly, systems on one side of the firewall are protected from systems on the other side.

VII.CONCLUSION

A firewall can allow any traffic except what is specified as restricted. It relies on the type of firewall used; the source, the destination addresses, and the ports. A firewall can deny any traffic that does not meet the specific criteria based on the network layer on which the firewall operates.A digital signature validates date and time of data send with contents.If any different behaviour than normal case the proposed system block the transmission. Arbitrated digital signature is a good authentication tool. Double encryption is performed in this technique. Message packets are not visible to anyone.

ACKNOWLEDGMENT

The authors would like to thank S.Ramkumar for his inputs and support for this work. Thanks to parents.

REFERENCES

[1] Aziz Baayer, Nourddine Enneya, Mohammed Elkoutbi, "Enhanced Timestamp Discrepancy to Limit Impact of Replay Attacks in MANETs", Journal of Information Security, vol 3, 224-230, 2012.
[2] K.Geetha, "SYN Flooding Attacks in Mobile Adhoc Networks" International Journal of Computer Science and Information Technologies, Vol. 5 (4), 2014, 5033-5037.
[3] William Stallings,"Cryptography and Network Security",Fourth Edition, Pearson Education.
[4] Sreeja Nair M P, "An enhancement on Request Rate-Time-Bandwidth for limiting Replay attack in MANET",InternationalJournal For Advanced Research In Computer And Communication Engineering,volume4,issue 6,june 2015,2278-1021
[5] ZHANG FU- "Multifaceted DefenseagainstDistributed Denial of Service Attacks: Prevention Detection", Mitigation, Division of Networks and Systems Department of Computer Science and Engineering CHALMERS UNIVERSITY OF TECHNOLOGY Gothenburg, Sweden 2012.
[6] M.Padmadas,Dr.N.Krishnan, Sreeja Nair M.P, "RTB Rule Based Adaptive Selective Verification Protocol To Prevent DoS Attack", IEEE International conference 2013.
[7] Danai Chasaki, "Attacks and Defences in the Data plane of network",IEEE transactions, Vol.9, No.6.

BIOGRAPHY

Harikrishnan Nair M P, a Student member of Electronics and Communication Engineering in PSN College Of Engineering And Technology, Tirunelveli, Tamil Nadu. He was Completed his Diploma in ECE in N.S.S polytechnic College, Pandalam, Kerala. His Interested areas are Communication Engineering, Digital Electronics and Computer Networks.

Sreeja Nair M P, a faculty member of computer science and Engineering in Cochin University College of Engineering kuttanad ,Alappuzha, Kerala under Cochin University of Science And Technology. During the initial phase of her career, she worked as a lecturer in College of Engineering ,Adoor, Pathanamthitta, Kerala(2008-2012).she is doing her phd work self and will register soon. Her areas of interest include Network Security in Computer Networks and Mobile Networks. Also she is interested on cloud computing, Grid Computing and Digital Image Processing.