Volume 4, Issue 3, March 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Survey of Flooding Attack and Its Countermeasures on MANET

Sathish.T
P.G Student ,Dept of IT.
K.S.R College of Engineering,
Tiruchengodu,Tamilnadu, India

Sasikala.E
Assistant Professor, Dept of IT.
K.S.R College of Engineering,
Tiruchengodu,Tamilnadu, India

Abstract - A mobile ad hoc network (MANET) is a dynamic wireless network that can be formed without any pre-existing infrastructure in which each node can act as a router. A unified security solution is in very much need for such networks to protect both route and data forwarding operations in the network layer. Attacks on ad hoc networks can be classified as passive and active attacks, depending on whether the normal operation of the network is disrupted or not. In this paper, the current security issues in MANET are investigated. Particularly, about flooding attacks and the different counter measures proposed by many authors to avoid those flooding attack is done in a detailed survey. The various solutions suggested for this problem like statistical analysis, threshold level, mixes, traceback method, reputation and flow based solutions are studied and reported.

Keywords – MANET, DOS, routing attacks, intrusion response.

I. INTRODUCTION

In a MANET, a collection of mobile hosts with wireless network interfaces form a temporary network without the aid of any fixed infrastructure or centralized administration and it can be formed quickly at very low cost. The other advantage of MANET is there resource constraints where it has limited bandwidth and battery power so it makes routing in MANET even more challenging so early research work would be needed to minimize the cost of bandwidth and battery power. There are several routing protocols proposed in MANET network and they are classified into two categories they are reactive and proactive routing protocols. In reactive routing protocols, such as the Ad hoc On Demand Distance Vector (AODV) protocol, nodes find routes only when they are in need where as in proactive routing protocols, such as the Optimized Link State Routing(OLSR) protocol, nodes will obtain routes by the periodic exchange of topology information. Mainly these routing protocols rely on the cooperation between the nodes due to the lack of a centralized administration and assume that all nodes are trustworthy and well-behaved. But still in a hostile environment, a malicious node can launch routing attacks to disrupt routing operations or denial-of-service (DoS) attacks to deny services to legitimate nodes.

In a MANET, nodes within each other's wireless transmission ranges can communicate directly; however, nodes outside each other's range have to rely on some other nodes to relay messages. Any routing protocol must encapsulate an essential set of security mechanism. These mechanisms are used to prevent, detect and respond to security attacks. There are five major security goals that need to be addressed in order to maintain a reliable and secure ad-hoc network environment. They are mainly:1. Confidentiality,2. Availability,3. Authentication ,4. Integrity.
5. Non-repudiation

The organization of the paper is as follows: Section II describes the different types of security attacks that will occur in MANET network. Section III gives the detailed study about different types of routing attack that will occur in the network. Section IV describes the counter measures that will avoid flooding attack in the Mobile ad hoc networks. Section V will conclude the process.

II. TYPES OF SECURITY ATTACKS

External attacks [1], in which the attacker aims to cause congestion, propagate fake routing information or disturb nodes from providing services. Internal attacks, in which the adversary wants to gain the normal access to the network and participate in the network activities, either by some malicious impersonation to get access to the network as a new node, or by directly compromising a current node and using it as a basis to conduct its malicious behaviors. The security attacks in MANET can be broadly classified into two major categories, namely passive attacks and active attacks. The active attacks further divided according to the layers.

A. Passive Attacks

A passive attack [1] is a type of attack operation which does not spoil the normal operation of the network; In passive attack the attacker tries to steal the data exchanged in the network without altering any of the network nodes and there also no changes in the data's being sent and received. So the metrics like confidentiality gets violated drastically due to the snooping process. Detection of passive attack is really a very difficult task since the operation in the network doesn't get affected. One of the solutions to this problem is to use powerful encryption and decryption mechanism to encrypt and decrypt the data being transmitted and received, thereby making it impossible for the attacker to get useful information from the data overhead. Some of the passive attacks are
1. Eavesdropping

2. Traffic Analysis & Monitoring.

B. Active Attacks

An active attack [1] is other kind of attack operation which attempts to change or demolish the data being exchanged in the network there by disturbing the normal functioning of the network. Active attacks can be either internal or can be external. External attacks are carried out by the nodes which does not belong to the same network whereas they belong to other network there by the attacker comes from other network. Internal attacks are carried out by the nodes that belong to the same network. Since the attacker is already part of the network, internal attacks are very severe and hard to detect than the external attacks. Active attacks, whether carried out by an external or an internal attackers compromised node involves actions such as modification, impersonation, fabrication and replication.

III. DIFFERENT TYPES OF ROUTING ATTACKS

A.Flooding Attack

Flooding attack is one kind of routing attack which will [2] exhaust the network resources such as bandwidth and will consume lot of node's resources, such as bandwidth and battery power or it will disrupt the routing operation which will cause severe degradation in network performance. 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. During the route discovery process the flooding attack either it may flood RREQ or RREP packets.In this attack the source may act as malicious node. If any one of the malicious node intent to disrupt either the network operations or other node's activity in the network, the malicious node will initiates the route discovery process. The following diagram will represent the flooding attack types.

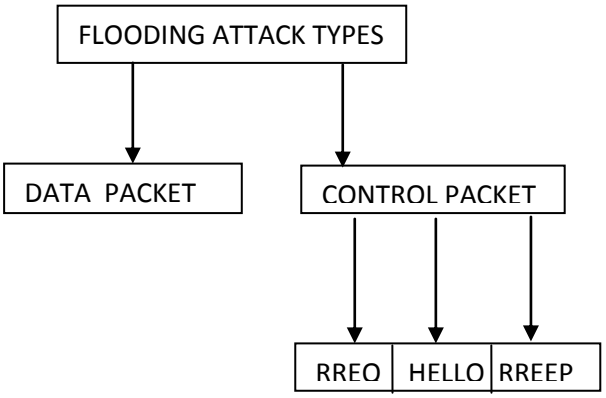

Fig. 1 Flooding attack types

A control packet flooding attack is a Denial of Service attack in which the malicious node takes advantage of either the route discovery process or to maintain a local connectivity between the nodes. In the route discovery process either the malicious node floods the RREQ or RREP packets. So there will be a overflow in the routing table in the intermediate node is the effect of this malicious activity. Hello flood is one type of active attacks. If the malicious node floods the hello packet unnecessarily, neighbors of the malicious node cannot receive other packets regularly which results in congestion, exhaustion of battery power, bandwidth wastage and degrades in throughput.

B. Blackhole Attack

In a blackhole attack [3], a malicious node sends fake routing information, claiming that it has an optimum route and causes other good nodes to route data packets through the malicious one.

C. Link Withholding Attack

In this attack [2], a malicious node ignores the requirement to advertise the link of specific nodes or a group of nodes, which can result in link loss to these nodes. This type of attack is particularly serious in the OLSR protocol.

D. Link Spoofing Attack

In a link spoofing attack [2], a malicious node advertises fake links with non-neighbours to disrupt routing operations.

E. Repaly Attack

In a MANET, topology frequently changes due to node mobility [5]. This means that current network topology might not exist in the future. In a replay attack, a node records another node's valid control messages and resends them later. This causes other nodes to record their routing table with stale routes. Replay attack can be misused to impersonate a specific node or simply to disturb the routing operation in a MANET.

F. Wormhole Attack

A wormhole attack [4] is one of the most sophisticated and severe attacks in MANETs. In this attack, a pair of colluding attackers record packets at one location and replay them at another location using a private high speed network. The seriousness of this attack is that it can be launched against all communications that provide authenticity and confidentiality.

G. Colluding Misrelay Attack

In this attack [2], multiple attackers work in collusion to modify or drop routing packets to disrupt routing operation in a MANET. This attack is difficult to detect by using the conventional methods such as watchdog and pathrater.

IV. COUNTER MEASURES AGAINST FLOODING ATTACK IN MANET

In [6], the authors proposed an adaptive technique to mitigate the effect of a flooding attack in the AODV protocol. This technique is based on statistical packet dropping mechanism to detect malicious RREQ floods and avoid forwarding of such packets. Each node monitors the RREQ it receives and maintains a count of RREQs received from each sender during the preset time period. The RREQs from a sender whose RREQ rate is above the threshold will be dropped without forwarding. It even works in situations when the identity of the malicious node is unknown and won't use additional network bandwidth. The key advantage of this approach is that it is simple to implement and maintains or improves network throughput when there are no malicious nodes but the disadvantage of these system is that the network is congested with excess traffic.

In [7], the authors use the Flooding Attack Prevention (FAP) technique which is an adaptive technique that will prevent the flooding attack in the network. During the route request process when the intruders send excessive amount of route request packets the immediate neighbor record the rate of the route request being received. If the threshold level is greater than the expected level then the neighbor node deny any further route request packets from the intruders, the node records the ID of this neighbor in a blacklist. Then, the node drops any future RREQs from nodes that are listed in the blacklist. The limitation of this approach is that it cannot prevent against the flooding attack in which the flooding rate is below the threshold. The advantage of these approach is Flooding Attack prevention(FAP) can effectively prevent the flooding attack nodes but the cons is it is severely affected by Denial of Service attack.

In [8], the authors propose the mix technique where the traffic from source to destination has to pass through some series of mixes where the mix reorders and re-encrypts the incoming packet where the incoming and outgoing packet cannot be related so the attacker can't find the end to end connection and they also used the rate Limitation method where each incoming packets has to pass through the rate- Limitation component before forwarded to the next-hop neighbor and each node should necessarily share its bandwidth with the neighbors in that environment. To achieve these all the nodes should use the threshold-tuple which is the list of thresholds that has to be followed before packet forwarding. The advantage of these technique is it effectively isolate the malicious node from the network but the threshold level should be fixed accurately else the attack node will participate in the network.

In [9], to minimize blocking in a network the author uses the RREQ_RATELIMIT technique where the node cannot create more RREQ messages per second and the nodes which violate these limit won't be allowed to participate, so because of these the communication bandwidth is fatigued. To avoid these problem a new hybrid technique like support vector machine (SVM) is used which will improve the MANET performance drastically where SVM takes a set of input data and predicts for every given input whether it belong to normal node or malicious node. It collect the behavior of every node and by using those data it find the malicious node accurately. The advantage of these method is it is easy to implement and flooding attack problem can be merely avoided by using the metrics like Packet Delivery Ratio, Control Overhead, Packet Misroute Rate to identify the behavior of each node.

In [10], all the nodes locally run the intrusion detection code and cooperate with each of the other nodes to detect and prevent flooding attack in the network. To make this possible Dynamic Source Routing (DSR) protocol along with the trust estimation function is used. Because the communication between the node in the network depends on the cooperation and trust level of its neighbors so to calculate the trust level the trust estimation function in the Route discovery phase of the basic DSR routing protocol will calculate the trust level of each neighboring node and to find the malicious node and the trust level between the neighbor nodes is calculated using the trust estimation function. The parameters that are used to calculate the trust estimation are 1)Total number of RREQ packet sent by the neighbor per unit time 2)Total number of packet successfully transmitted by the neighbor 3) Ratio of number of packet received correctly from the neighbor to the total number of received packet. To calculate the relationship between the nodes they are broadly classified into three types. They are Stranger, Acquaintance, Friend.

In [11], the author use the security mechanism like Public key cryptography and digital signatures to control the spread of RREQ packets and to reduce their impact in the MANET networks. The use of these mechanisms is it enables a node to authenticate routing messages from any node in the network so the malicious node cannot spoof the originator and destination IP address in the RREQ packet and they also proposed the filter method which is used to detect the misbehaving nodes and to reduce their impact by limiting the rate of RREQ packets in the network by maintaining two threshold value. They are Rate-limit and Blacklist-limit metrics. Rate-limit parameter denotes the number of RREQs that can be accepted and processed as normal per unit time by a node. Each node monitors the route requests it receives and maintains a count of RREQs received for each RREQ originator during a preset time period. Blacklist-limit parameter is used to specify a value that aids in determining whether a node is acting malicious or not. If the number of RREQs originated by a node per unit time exceeds the value of Blacklist-limit, one can safely assume that the corresponding

node is trying to flood the network. The advantage of these technique is that it doesn't increase the overhead but the cons is DOS attack won't be completely avoided.

In [12], the authors proposed the behavior based traceback mechanism which is used to identify the actual source of any packet sent across the Internet i.e the flooding attack origin because tracing the attacker is equal to identifying the malicious node from normal node. To achieve these identification there is a need to observe their behaviors. So based on the behavior monitoring the nodes that continuously propagate attack packets are malicious nodes. To differentiate the attack nodes the packet differentiation technique is used where it will classify the packets as normal and malicious based on their behavior. Once the differentiation is done then the attack identification mechanism is used to identify the attack the node is currently having and once it is done then the attack isolation metrics is used to stop forwarding the packets that are being send by the malicious node. The advantage of these technique is it is able to trace packets that are multi-source and distribute the flooding attack in MANET and the added advantage is it can accurately identify the malicious nodes but the disadvantage is traceback need to be accurate always else there is a chance for error.

To avoid the distributed denial of service attack [13], the authors created the disable IP broadcast technique where a broadcast is a data packet that is destined for multiple hosts in the network. Broadcasts can occur at the data link layer and at the network layer. Data-link broadcasts are sent to all hosts attached to a particular physical network. Network layer broadcasts are sent to all hosts that are attached to a particular logical network. The Transmission Control Protocol/Internet Protocol (TCP/IP) supports the following type of broadcast packets. They are 1) All ones - setting broadcast address to ones then all the host in the network will receive the broadcast 2) Network – By setting broadcast address to specific network number then only the specific network will receive a broadcast 3) Subnet – By setting the broadcast address to a specific network number and a specific subnet number, all hosts on the specified subnet receive the broadcast. The proposed scheme is distributed in nature which has the capability to prevent Distributed Denial of Service attack. The performance of the proposed scheme in a series of simulations shows that the proposed scheme provides a better solution than existing schemes is their mere advantage.

In [14], Reputation based model was proposed by the authors to establish the connection in the network. Nodes with high reputation value alone are considered to forward the packets towards destination. Here the malicious nodes are only excluded from forwarding the packets whereas they can act themselves as a source targeting the network by sending bogus RREQ packets so to overcome these bogus rreq problem reputation based protocol integrates four main features of distributed reputation systems. Each node in a MANET collects the reputation information through direct observation of its neighbors i.e subjective observation and gathers indirect reputations from other nodes. In addition to using historical observations these protocol uses reputation discounting to ensure that old reputations will fade away giving more chance for nodes to reclaim their reputation by consistently behaving in a cooperative manner. It also has reputation noise detection and cancellation, deviation test and secondary response that are used to increase the accuracy and reliability of the reputation resolution are their advantages.

In [15], the authors propose the flow based detection mechanism technique where the primary use of these techniques is that it uses 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. Two flow based detection scheme have been proposed in these technique they are 1) Detection feature against address spoofing - each RREQ packet sent out by each attack node is allocated a random (SA, DA). Hence, when attack occurs, a large number of RREQ flows will emerge in the network and majority of them are new to mobile nodes 2) Detection feature against non-address spoofing - each attacker uses fixed (SA, DA) for all RREQ packets it sends out. Therefore, when the attack takes place, network nodes will receive many identical RREQ flows in a certain number of successive sampling intervals and it will remain as long as the attack lasts. The percentage of new flows and ratio of identical flows are used for evaluation. The traffic pattern analysis states any change in statistical process can bring change in the probability distribution. The advantage of these technique is both ASF and NASF are all will be detected accurately.

In [16], the authors proposed the new technique called reliability index which is used to avoid the denial of service attack in the network. Reliability index is Ratio of number of packet received correctly from the neighbor to the total number of received packet. Based on their relationship with the neighboring node, the nodes are divided into two categories that are 1) Not reliable node - 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. 2) Reliable node – They are the most trusted nodes or the nodes with highest reliable level can be treated as reliable. Here the higher reliability level means neighbors had received or transfer many packets successfully through this particular node. The result of reliability index is the relationship status of all of neighbors as reliable or not reliable is the advantage of these technique.

In [17], the authors proposed the technique called behavior based anomaly detection which is used to avoid the Denial of service attack problem. IDS is the process of detecting malicious activity in the network by applying signature or anomaly detection technique. In signature based approach it compares present behavior with known attack signatures and if attack is found it raises the alert. While in the case of anomaly detection the system checks the deviation of current profile (behavior) with the normal profile and if there is any deviation it will generate alert for announcing the activity to be suspicious in the system. The following metrics are used to detect the malicious nodes they are 1) Packet Delivery Ratio 2) Control Overhead 3) Packet Misroute Rate. The advantage of these technique is it is able to detect all new types of flooding attacks that occurs and it is also easy to implement.

In [18], the authors proposed the technique called node to node authentication where only the authenticated node has to respond to the route request from other authenticated node only. So the advantage of these technique is only the authenticated nodes are allowed to participate in the packet forwarding and the malicious nodes are not allowed to participate and can't enter the authenticated network group. The other method which is used in these approach is Malicious-Node-Table where it stores information about malicious node present in the network. For forwarding all the packets in these network AODV protocol is used. The advantage of these approach is it provide node availability and better security for packet delivery in MANET network.

In [19], the author used the enhancement of packet processing technique to avoid the malicious node in the network. The size of the receiving buffer of a mobile node is denoted as Rbuffer where it is classified as control buffer and data buffer. These concept is the series of steps to be followed where if the RREQ is greater then control buffer and data packets are greater than data buffer then the nodes are prioritized in ascending order. Suppose if the data packets is less than data buffer then it won't be allowed and these process continues until the connection is terminated. The advantage of these technique is the packet processing is improved and the packet delivery ratio is also enhanced by using packet processing technique.

V. CONCLUSION

Mobile Ad Hoc Networks have the ability to setup networks on the fly in a harsh environment where it may not possible to deploy a traditional network infrastructure. Whether ad hoc networks have vast potential, still there are many challenges left to overcome. Security is an important feature for deployment they can be applied in various situations ranging from emergency operations and disaster relief to military service and task forces. Obviously, providing security in such scenarios is critical. For countermeasures, their advantages as well as their drawbacks identified. Our studies showed that although many solutions have been proposed, still they are not perfect in terms of tradeoffs between effectiveness and efficiency. In this paper, i have overviewed the challenges and solutions for the flooding attacks in mobile ad hoc networks. Future research efforts should be focused not only on improving the effectiveness of the security schemes but also on minimizing the cost to make them suitable for a MANET environment.

REFERENCE

[1] Pradip M. Jawandhiya, Mangesh M. Ghongea "Survey of Mobile Ad Hoc Network Attacks",*International Journal of Engineering Science and Technology*,vol. 2,pp. 4063-4071,2010.

[2] Rashid Hafeez Khokhar, Md Asri Ngadi, "A Review of Current Routing Attacks in Mobile Ad Hoc Networks", *International Journal of Computer Science and Security*, vol. 2 no. 3,2008.

[3] Bo Sun, Yong Guan and Pooch "Detecting black Hole Attack in Mobile Ad Hoc Networks", *Personal Mobile Communication Conference*, 2003.

[4] Y.C Hu, A. Perrig and D. Johnson, "Wormhole Attacks in Wireless Networks", *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, Feburary 2006.

[5] C. Adjih, D. Raffo and P. Muhlethaler, "Attacks Against OLSR: Distributed Key Management for Security", 2nd OLSR Workshop, Palaiseau, France, pp:28–29, July 2005.

[6] S. Desilva, R. V. Boppana, "Mitigating Malicious Control Packet Floods in Ad Hoc Networks", *IEEE Wireless Communication and Networking Conference*,vol.4,pp:2112-2117, 2005.

[7] P. Yi et al., "A New Routing Attack in Mobile Ad Hoc Networks", *International Journal of Information Technology*, vol. 11,no. 2, 2005.

[8] Venkat Balakrishnan, Vijay Varadharajan, Uday Tupakula "Mitigating Flooding Attacks in MANET Supporting Anonymous Communications", *International conference on wireless broadband*,2007.

[9] Sanjay Sharma, Meenakshi Patel "Detection and Prevention of Flooding Attack Using SVM", *International Conference on communication system and Network Technologies*,2013.

[10] Shishir K. Shandilya, Sunita Sahu "A Trust Based Security Scheme for RREQ Flooding Attack in MANET",*International Journal of Computer Applications*, vol.5, no.12, August 2010.

[11] Jian Hua Song,Fan Hong, Yu Zhang "Effective Filtering Scheme against RREQ Flooding Attack in MANET",*International Conference on Parallel and Distributed Computing*,2009.

[12] Yinghua Guo, Sylvie Perreau, "Trace Flooding Attack in Mobile Ad Hoc Networks", *International conference on wireless broadband*, Melbourne,pp:329-334, 2006.

[13] Mukesh Kumar, Naresh Kumar, "Detection and prevention of DDOS attack in MANET using disable IP broadcast technique" *International journal of application in engineering*, vol.2, no.7, pp:29-36, 2013 .

[14] Samesh R. Zakhary, Milena Randenkovic, "Reputation based security protocol for MANET's in highly mobile disconnection prone environments",*International conference on Wireless On-demand Network Systems and Services*, Kranjska Gora, pp:161-167, 2010.

[15] Steven Gordon, Sylvie Perreau, "A flow based detection mechanism against flooding attack in mobile ad hoc networks", *International conference on wireless communication and Networking Conference, Kowloon*, pp:3105-3511, 2007.

[16]Neetu Singh Chouhan, Prachi Jain, "Detection and prevention of Flooding attack in MANET using node reliability index", *International Journal of Advanced Research*, vol.1, no.8, pp:645-651, 2013.

[17] Simmi Jain, Hitesh Gupta, "Evaluation and Mitigation of DoS attack using behavior Anomaly Detection approach using NS-3", *International Journal of Computer Science and Information Technologies*, vol.4, no.3, pp: 446-450, 2013.

[18] Komal Joshi, Veena Lomte, "Preventing Flooding Attack in MANET Using Node-to-Node Authentication", *International Journal of Advanced Research in Computer Science and Software Engineering*, vol.3, no.11, 2013.

[19] HyoJin Kim, Ramachandra Bhargav Chitti and JooSeok Song, "Handling Malicious Flooding Attacks through Enhancement of Packet Processing Technique in Mobile Ad Hoc Networks", *Journal of Information Processing Systems*, vol.7, no.1, March 2011.

