Review of Flooding Attack Detection in AODV Protocol for Mobile Ad-hoc Network

Parth C. Bhatiya1 Hitesh M. Barot2
1, 2 PG Student [Computer Engineering] 1KLDRP- ITR, Gandhinagar 2ACET, Khatraj, Gandhinagar

Abstract—Ad Hoc Networks are extremely vulnerable to attacks due to their dynamically changing topology, absence of conventional security infrastructures, vulnerability of nodes and channels and open medium of communication. Denial of Service (DoS) and Distributed DoS (DDoS) attacks are two of the most harmful threats to the network functionality. The Prevention methods like authentication and cryptography techniques alone are not able to provide the security to these types of networks. Therefore, efficient intrusion detection must be deployed to facilitate the identification and isolation of attacks. Major attacks on Mobile Ad hoc networks are flooding, selective forwarding, sinkhole, wormhole etc. We have presented various intrusion detection techniques in MANET. Then we have proposed a method to detect flooding attack in MANET.

Keywords: MANET, flooding attack, Denial of Service (DOS), packets, route request.

I. INTRODUCTION

Mobile ad hoc network (MANET) 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. These nodes change position frequently. The main classes of routing protocols are Proactive, Reactive and Hybrid.

A Reactive (on-demand) routing strategy is a popular routing category for wireless ad hoc routing. It is a relatively new routing philosophy that provides a scalable solution to relatively large network topologies. The design follows the idea that each node tries to reduce routing overhead by sending routing packets whenever a communication is requested.

MANET is a kind of wireless ad-hoc network and it is a self-configuring network of mobile routers (and associated hosts) connected by wireless links – the union of which forms an arbitrary topology. The routers, the participating nodes act as router, are free to move randomly and manage themselves arbitrarily; thus, the network’s wireless topology may change rapidly and unpredictably. Such a network may operate in a standalone fashion, or may be connected to the larger Internet [1].

In Figure 1 nodes A and C must discover the route through B in order to communicate. The circles indicate the nominal range of each node’s radio transceiver. Nodes A and C are not in direct transmission range of each other, since A’s circle does not cover C [1].

II. RELATED WORK

AODV is a reactive routing protocol [6] in which the network generates routes at the start of communication. Each node has its own sequence number and this number increases when links change. Each node judges whether the channel information is new according to sequence numbers. When a node wants to find a route to a destination node, it broadcasts a Route Request (RREQ) message with a unique RREQ ID to all its neighbors. When a node receives a RREQ message, it updates the sequence number of source node and sets up reverse routes to the source node in the routing tables. If the node is the destination or the node has a valid route to the destination, it unicasts a route reply (RREP) back to the source node. The source node or the intermediate nodes that receives RREP will update its forward route to destination in the routing tables. Otherwise, it continues broadcasting the RREQ. If a node receives a RREQ message that has already processed, it discards the RREQ and does not forward it. When a link is broken, route error packets (RERR) are propagated to the source node along the reverse route and all intermediate nodes will erase the entry in their routing tables.

The source node or the intermediate nodes that receives RREP will update its forward route to destination in the routing tables. Otherwise, it continues broadcasting the RREQ. If a node receives a RREQ message that has already processed, it discards the RREQ and does not forward it. In AODV, sequence number (SN) plays a role to indicate the freshness of the routing information and guarantee loop-free routes. Sequence number is increased under only two conditions: when the source node initiates RREQ and when the destination node replies with RREP. Sequence number can be updated only by the source or destination. Hop count (HC) is used to determine the shortest path and it is increased by 1 if RREQ or RREP is forwarded each hop. When a link is broken, route error packets (RERR) are propagated to the source node along the reverse route and all intermediate nodes will erase the entry in their routing tables. AODV maintains the connectivity of neighbor nodes by sending hello message periodically.

Flooding RREQ packets in the whole network will consume a lot of resource of network. To reduce congestion in a network, the AODV protocol adopts some methods. A node cannot originate more than RREQ_RATELIMIT RREQ messages per second. After broadcasting a RREQ, a
node waits for a RREP. If a route is not received within round-trip milliseconds, the node may try again to discover a route by broadcasting another RREQ, up to a maximum of retry times at the maximum TTL value. Repeated attempts by a source node at route discovery for a single destination must utilize a binary exponential back off. The first time a source node broadcasts a RREQ, it waits round-trip time for the reception of a RREP. If a RREP is not received within that time, the source node sends a new RREQ. When calculating the time to wait for the RREP after sending the second RREQ, the source node MUST use a binary exponential back off. Hence, the waiting time for the RREP corresponding to the second RREQ is \( 2 \times \) round-trip time. The RREQ packets are broadcast in an incrementing ring to reduce the overhead caused by flooding the whole network. The packets are flooded in a small area (a ring) first defined by a starting TTL (time-to-live) in the IP headers. After RING TRAVERSAL TIME, if no RREP has been received, the flooded area is enlarged by increasing the TTL by a fixed value. The procedure is repeated until an RREP is received by the originator of the RREQ, i.e., the route has been found.

Fig. 2: Demonstration of flooding attack [9]

Simple mechanism proposed to prevent the flooding attack in the AODV protocol [7]. In this approach, each node monitors and calculates the rate of its neighbors’ RREQ. If the RREQ rate of any neighbor exceeds the predefined threshold, 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. Another drawback of this approach is that if a malicious node impersonates the ID of a legitimate node and broadcasts a large number of RREQs, other nodes might put the ID of this legitimate node on the blacklist by mistake.

In [8], the authors proposed an adaptive technique to mitigate the effect of a flooding attack in the AODV protocol. This technique is based on statistical analysis to detect malicious RREQ floods and avoid the forwarding of such packets. Similar to [7], in this approach, 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. Unlike the method proposed in [7], where the threshold is set to be fixed, this approach determines the threshold based on a statistical analysis of RREQs. The key advantage of this approach is that it can reduce the impact of the attack for varying flooding rates.

Resisting flooding attacks in ad hoc networks presented in [9] describes two flooding attacks: Route Request (RREQ) and Data flooding attack. 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. Using neighborhood suppression, a single threshold is set up for all neighboring nodes. 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.

A new trust approach based on the extent of friendship between the nodes is proposed which makes the nodes to co-operate and prevent flooding attacks in an ad hoc environment in [10]. All the nodes in an ad hoc network are categorized as friends, acquaintances or strangers based on their relationships with their neighboring nodes. A trust estimator is used in each node to evaluate the trust level of its neighboring nodes. The trust level is a function of various parameters like length of the association, ratio of the number of packets forwarded successfully by the neighbor to the total number of packets sent to that neighbor, ratio of number of packets received intact from the neighbor to the total number of received packets from that node, average time taken to respond to a route request etc. Accordingly, the neighbors are categorized into friends (most trusted), acquaintances (trusted) and strangers (not trusted).

To prevent RREQ flooding, the threshold level is set for the maximum number of RREQ packets a node can receive from its neighbors [10]. To prevent DATA flooding, the intermediate node assigns a threshold value for the maximum number of data packets it can receive from its neighbors. If \( X_{rs} \), \( X_{ra} \), \( X_{rf} \) be the RREQ flooding threshold for a stranger, acquaintance and friend node respectively, \( X_{rf} > X_{ra} > X_{rs} \). If \( Y_{rs} \), \( Y_{ra} \), \( Y_{rf} \) be the DATA flooding threshold for a stranger, acquaintance and friend node respectively then \( Y_{rf} > Y_{ra} > Y_{rs} \). If the specified threshold level is reached, further RREQ packets from the initiating node are ignored and dropped. Thus, flooding is prevented in the routing table.

III. PROBLEM STATEMENT

Security Attacks on Protocol Stacks

The attacks in MANET can roughly be classified into two major categories, namely passive attacks and active attacks, according to the attack means [8] [15]. A passive attack obtains data exchanged in the network without disrupting the operation of the communications, while an active attack involves information interruption, modification, or fabrication, thereby disrupting the normal functionality of a MANET. Examples of passive attacks are eavesdropping, traffic analysis, and traffic monitoring. Examples of active attacks include jamming, impersonating, modification, denial of service (DoS), and message replay. The attacks can also be classified into two categories, namely external attacks and internal attacks, according to the domain of the attacks. Some papers refer to outsider and insider attacks.
[19]. External attacks are carried out by nodes that do not belong to the domain of the network. Internal attacks are from compromised nodes, which are actually part of the network. Internal attacks are more severe when compared with outside attacks since the insider knows valuable and secret information, and possesses privileged access rights.

Attacks can also be classified according to network protocol stacks. Some security attacks use stealth [18], whereby the attackers try to hide their actions from either an individual who is monitoring the system or an intrusion detection system (IDS). But other attacks such as DoS cannot be made stealth.

IV. FLOODING ATTACK
Flooding attack is a Network layer attack in which 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. 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.

A simple mechanism proposed to prevent the flooding attack in the AODV protocol [13]. In this approach, each node monitors and calculates the rate of its neighbors’ RREQ. If the RREQ rate of any neighbor exceeds the predefined threshold, 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. Another drawback of this approach is that if a malicious node impersonates the ID of a legitimate node and broadcasts a large number of RREQs, other nodes might put the ID of this legitimate node on the blacklist by mistake. In [13], the authors show that a flooding attack can decrease throughput by 84 percent.

Similar to [13], in this approach, 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. Unlike the method proposed in [13], where the threshold is set to be fixed, this approach determines the threshold based on a statistical analysis of RREQs. The key advantage of this approach is that it can reduce the impact of the attack for varying flooding rates.

In this paper, we present a new attack, the Ad Hoc Flooding Attack, which results in denial of service when used against all previously 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 so as to congest in links. To defend routing protocols against the Ad Hoc Flooding attack, we develop a generic secure component, called Flooding Attack Prevention (FAP), which can be applied to AODV routing protocol to allow that protocol to resist the rushing attack.

V. RREQ FLOOD ATTACK DETECTION ALGORITHM
Flooding unnecessary broadcast messages into the network to disturb the normal operations of the network. A malicious node sends a huge number of RREQ packets in an attempt to consume the network resources. The source IP address is forged to a randomly selected node and the broadcast ID is intentionally increased.

In AODV protocol routes are generated on demand because it is a reactive routing protocol. When a node wants to find a route to a destination node, it broadcasts a Route Request (RREQ) message with a unique RREQ ID to all its neighbors. When a destination node receives a RREQ message, it sends a RREP (Route Reply) message to the source. A malicious node generates a large no. of Route Request packets and creates congestion in the network. Due to flooding attack, a non-malicious genuine node cannot fairly serve other nodes due to the network-load imposed by the fake RREQs and useless data packets. This leads to several problems, as follows:

- Wastage of bandwidth
- Wastage of nodes’ processing time, thus increasing the overhead
- Overflow of the routing table entries, causing exhaustion of an important
- network resource like memory
- Exhaustion of the nodes’ battery power
- Degraded throughput

Most of the network resources are wasted in trying to generate routes to destinations that do not exist or routes that are not going to be used for any communication. To detect such type of attack is very crucial in MANET because it consume lots of network resources. Our RREQ flood attack detection algorithm is as follows:

Algorithm for RREQ Flooding Attack

Begin
An intermediate node receives RREQ flooding packet from node „x” then
1. if node „x” is a member and P = 1
2. if Rx < Tm
3. forward the RREQ packet and increment Rx
4. else
5. drop the RREQ packet and set P = 0
6. if node „x” is a guest and P = 1
7. if Rx < Tg
8. forward the RREQ packet and increment Rx
9. else
10. drop the RREQ packet and set P = 0
End

VI. CLASSIFICATION OF FLOODING DETECTION SCHEMES

Fig. 3: DoS Attacks Classification Schemes
DoS detection schemes may be classified into three categories as shown in Fig.3.

A. Based on router data structure.
B. Based on statistical analysis for packet flow.
C. Based on Artificial Intelligence (fuzzy logic and neural network).

A. Router-Based Detection Scheme using Bloom-Filter

A bloom filter is a space-efficient data structure used in router for pattern matching in many network communications. It is used to inspect packets and detect malicious packets based on many algorithms [18], [19], [20] focuses on the low-rate agent and present a router-based detection scheme for it.

The low rate DoS agent exploits the TCP’s slow time scale of Retransmission Time Out (RTO) to reduce TCP throughput. In this case, the DoS attacker can cause a TCP flow in RTO state by sending high rate requests for short-duration bursts. Therefore, The TCP throughput at the victim side will be reduced during the attacking time on low-rate DoS agent. The proposed scheme is based on the TCP SYN-SYN/ACK protocol pairs with the consideration of packet header information (both sequence and Ack. Numbers). The Counting Bloom Filter (CBF) is used to avoid the effect of ACK retransmission, and the change point detection method is applied to avoid the dependence of detection on sites and access patterns. See (Fig.4).

![Fig. 4: Router based Counter Bloom Filter Scheme](image)

B. Sample Flow-Statistical Analysis

Many efforts have been undertaken in using the sample flow of statistics to detect DoS attacks [26]-[28]. [29] presented a statistical scheme to detect the SYN-flooding accuracy on network anomalies using flow statistics obtained through packet sampling. The network anomalies generate huge number of small flows, such as network scans or SYN-flooding. Due to this reason, it is hard to detect SYN-flooding when performing packet sampling because the network flow may be either bursty (non-linear) or under the normal flow rate. Their model is based on two steps: the first step, analytical model was developed to quantitatively evaluate the effect of packet sampling on the detection accuracy and then investigated why detection accuracy worsens when the packet sampling rate decreases. In addition, it is shown that, even with a low sampling rate, the detection accuracy was increased because the monitored traffic was partitioned into groups. The results show that the proposed mechanism is demonstrated to have the capability of detecting SYN-flooding attack accurately.

According to [30], a new detection method for DoS attack traffic based on the statistical test has been adopted. Investigation of the statistics of the SYN arrival rate revealed that the SYN arrival rate can be modeled by a normal distribution. A threshold for maximum arrival rate to detect SYN-flooding attack traffic has been established. In addition, the threshold for incomplete three-way handshaking packet ratio to detect possible DoS traffic also has been determined. This mechanism was shown to be effective in detecting SYN-flooding attack, but for the normal traffic threshold, the value is not accurate for the whole packet flow, especially during the attacking time.

C. Detection Scheme using Fuzzy Logic and Neural Nets

Fuzzy logic and neural network was adopted by many research to design and implement intrusion detection systems for denial of service attacks [34]-[36]. A fuzzy logic based system for detecting SYN-flooding attacks has been adopted. Fuzzy logic helps solving the systems which have elements of uncertainty. Fuzzy logic is appropriate for approaching the nonlinear systems [37]. [38] proposed a system represented by two blocks shown in figure 5. The first one is the packet classification block which classifies incoming network traffic packets, where the header of each captured packet is checked to see if it is a TCP SYN packet; if the fragment offset value in the header is zero, and then it is a TCP packet. If the SYN flag of the flag bits in this TCP packet is one, then it is a SYN packet (attack possibility). The packet classification block collects the TCP SYN packets for a predetermined ∆t time and gives them to the fuzzy logic system, which is the second block of the proposed system. The ∆t in this work was 5 seconds, while the second block of the proposed system is a fuzzy logic system. This block is responsible for SYN-flooding attack detection. The detection accuracy of the proposed system was compared with Cumulative Sum (CUSUM) for five attacks and showed a high accuracy and low false-negative rate and generate an earlier alarm than CUSUM algorithm which it is an ideal algorithm for identifying DoS attacks based on the measurement for the mean in traffic before, and after they detect comparing with the threshold value.

![Fig. 5: Proposed System Based on Fuzzy Logic](image)

VII. CONCLUSION

This distributive approach to identified the 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. This works on security issues and trust establishment schemes. A proposal to effectively detect flooding attack using AODV Protocol is discussed. A better understanding and modeling of the security attacks is needed in MANETs if efficient secure routing algorithms are to be built in the network. Future work of this research can be optimize value of threshold and improve their performance.
REFERENCES

[31] L. Zong-Lin, Guang-Min, H., & Dan, Y. , “Global abnormal correlation analysis for DDoS attack


