Detection and prevention of Routing Attacks in MANET using AODV

Meenakshi Patel  
Oriental Institute of Sc. & Tech.  
Bhopal, India

Sanjay Sharma  
Oriental Institute of Sc. & Tech.  
Bhopal, India

Abstract—Absence of infrastructure and dynamic nature of MANET invites intruder to launch attack, one of them is flooding. On demand routing such as AODV is more popular than proactive routing use flooding to discover route. Attackers used this concept to launch DoS attack like flooding; black hole and gray hole are the known attack in MANET. In this paper we have proposed a new method based on AODV behavioral metrics to detect and prevent MANET attacks. In this method we have used the RREQ, RREP, PDR, and PMIR as metrics to calculate the QoS of a link and into prediction of attacks. Our proposed scheme will be implementing on NS-3 test bed.

Keywords-MANET, Flooding, Black hole, Gray hole, NS-3, AODV

I. INTRODUCTION

In modern era, there is a tremendous growth in the sales of communication with computation capability devices such as Laptop, mobile, portable computers etc. Recently many network researchers are studying networks based on new communication techniques, especially wireless communications. Wireless networks allow hosts to travel without the constraints of wired connections. Hosts and routers in a wireless network can move around. Therefore, the network topology can be dynamic and unpredictable. A MANET uses multi-hop peer-to-peer routing as an alternative of fixed network infrastructure to provide network connectivity. There are no permanent routers- instead each node acts as router and frontwards traffic from other nodes. Due to highly dynamic nature topology in MANET makes routing procedure more complicated and insecure and therefore nodes are more susceptible to compromise and are particularly vulnerable to denial of service attack (DoS) attacks launched by malicious nodes or intruders [1].

In this paper we have proposed a routing based method to detect DoS attack like flooding, black hole and a method for gray hole. Our propose method is based on AODV [2]. AODV is a well known and popular reactive type’s protocol used in MANET.

Rest of the paper as organize as follow section 2 discuss basic terminology our wireless MANET, section 3 gives brief literature on types of attack and exiting work related to prevention and detection, section 4 insight into our proposed work to detect flooding attack, black hole and gray hole attack, and finally section 5 describes the conclusion of the paper.

II. BACKGROUND AND TERMINOLOGY

A. MANET

A mobile ad hoc network is formed by mobile hosts. Some of these mobile hosts are willing to forward packets for neighbors. Examples include vehicle-to-vehicle and ship-to-ship networks that communicate with each other by relying on peer-to-peer routings.

Two important characteristics of MANET make it popular—mobility and absence of infrastructure [3].

B. AODV Routing in MANET

Broadly MANET use two types of routing proactive and reactive, in this section we are going to discuss well known reactive routing protocol called AODV [2].

AODV is a reactive routing protocol [2] designed for mobile ad hoc networks. AODV is used for unicast, multicast and broadcast announcement. AODV is grouping of together DSR and DSDV. It adopts the basic on demand method of Route Discovery and Route preservation from DSR and the use of hop by hop steering sequence number and sporadic beacons from DSDV [4] is a reactive routing protocol, AODV only desires to preserve the routing information about the active paths. In AODV, routing information is maintained in routing tables at nodes. Each mobile node keeps a next-hop routing table, which contains the destinations to which it presently has a route. A routing table admission expires if it has not been used or reactivated for a pre-specified termination time. Moreover, AODV adopts the destination sequence number procedure used by DSDV in an on-demand way.

Hello messages can be used to identify and supervise links to neighbors. If Hello messages are used, all vigorous nodes sporadically broadcast a Hello message that all its neighbors entertain. Since nodes sporadically send Hello messages, if a node fails to entertain numerous Hello messages from a neighbor, a link split is detected.

C. Flooding and its used in Attack

Flooding is a requisite message spreading technique for network-wide broadcast within mobile ad hoc networks (MANETs). Flooding is appropriate for MANETs as it requires no topological awareness [30]. All the routing protocol is based on the on-demand routing is established...
route using the flooding technique. While attacker used this flooding to disrupt the communication it’s called flooding attacks.

III. RELATED WORK

Primarily Statistical analysis has been used to detect malicious node who floods in the network using RREQ messages, [7] has proposed a statistical approach to avoid the forwarding of such packets using the concept of RREQ counts.

Author Bo-Cang Peng and Chiu-Kuo Liang of [8] has suggested the concept of friendship table for detection of intrusion on MANET. Friendship table is used to store the relationship status of any node with its neighbors. The friendship table has two columns. First the identifier or name of its entire neighboring node and second its relationship status with the neighbor node that could be friend, Acquaintance or stranger. This table is referred every time when any node receives the packets. Initially NODE treat as stranger while newly joined the network. If the trust value is optimal node will treat as acquaintance, If node receives many packets to or from any node successfully, then trust level is very high the node is considered as a friend.

In [9][10][11] has used the concept of dynamic routing metrics like RREQ, RREP and the idea of route freshness calculated using destination sequence number for detection and prevention of flooding and black hole attacks of MANET.

The author Fan-Hsun Tseng, Li-Der Chou and Han-Chieh Chao of [13] has experience that a higher packet delivery ratio is obtained with only minimal delay and overhead. But the end-to-end delay might be raised visibly when the suspicious node is away from the source node. The experiment have been performed using global mobile simulator (GloMoSim).

Time-based Threshold Detection Scheme [14] Latha Tamilselvan et al. propose a solution based on an enhancement of the original AODV routing protocol. The major design concept is setting timer in the Timer Expired Table for collecting the other request from other nodes after receiving the first request. It will store the packet’s sequence number and the received time in a Collect Route Reply Table (CRRT), counting the timeout value based on the arriving time of the first route request, judging the route belong to valid or not based on the above threshold value.

Author Tamilselvan L, Sankaranarayanan [14] has used to concept of feedback to detect cooperative black holes, the node that ultimately eats up the data packets gets trapped. Moreover, Source Node decides the location of a black hole by the feedback of more than one neighboring node. Hence the detection and elimination of malicious node has been possible.

Sun et al [16] presented a general approach for detecting the black hole attack. They devised a neighborhood-based technique to detect the intruder and a routing recovery protocol to set up an accurate path to the true destination. One drawback of this scheme is that there must be a public key infrastructure or the detection is still susceptible.

Patcha et al [17] proposed a collaborative method for black hole attack prevention. A watchdog method is introduced to incorporate a collaborative architecture to tackle collusion amongst nodes. In this algorithm, nodes in the network are classified into trusted, watchdog, and ordinary nodes. Every watchdog that is elected should observe its normal node neighbors and decide whether they can be treated as trusted or malicious.

Gao et al [27] proposed to use aggregate signature algorithm to trace packet dropping nodes. The proposal was consisted of three related algorithms: 1) the creating proof algorithm. 2) The checkup algorithm. 3) The diagnosis algorithm.

Shila et al [31] presented a solution to defend selective forwarding attack (gray hole attack) in Wireless Mesh Networks. The first phase of the algorithm is Counter-Threshold Based and uses the detection threshold and packet counter to identify the attacks. The second phase is Query-Based and uses acknowledgment from the intermediate nodes to localize the attacker.

Author D.S.J.D. Couto; D. Aguayo; J. Bicket; R. Morris of [19] has proposed has based on detect black and gray hole nodes, the sender occasionally check through all available routes to determine if the destination received all of its messages undamaged. In order to circumvent any black hole nodes that might interfere with message traffic, the sender broadcasts a "check" request message and the destination's response would follow the same route as the request.

Some researchers also discussed and proposed a solution to a black hole attack by disabling the ability for intermediate nodes to reply to an RREP, and only allowing the destination to reply.

Payal N. Raj, Prashant B. Swadas [21] proposed DPRAODV (detection, prevention and reactive AODV) to prevent security of black hole by informing other nodes in the network. It uses normal AODV in which a node receives the Route reply (RREP) packet which first checks the value of sequence number in its routing table. The RREP is accepted if its sequence is higher than that in the routing table. It also check whether the sequence number is higher than the threshold value, if it is higher than threshold value than it is considered as the malicious node. The value of the threshold value is dynamically updated in the time interval.

Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantadhyya, John Dixon and Kendall Nygard [22] proposed a method for identifying multiple black hole nodes. They are first to propose solution for cooperative black hole attack. They slightly modified AODV protocol by introducing data routing information table (DRI) and cross checking. Every entry of the node is maintained by the
table. They rely on the reliable nodes to transfer the packets. The Route request (RREQ) is sent by source to every node and it send packet to the node from where it get the RREP. The intermediate node should send NHN and the DRI entry to the table. The source node (SN) check own DRI whether intermediate node (IN) node is reliable or not. The SN send the further request to next hop node (NHN) for IN. If SN uses IN to send the packet then it is considered as reliable node otherwise not. Cross checking is done on the intermediate nodes. It is one time procedure. The cost of cross checking is more. It can be minimized by letting nodes sharing their trusted nodes list with each other. Mohammad Al-Shurman, Seong-Moo Yoo and Seungjin Park [23] proposed two different approaches to solve the black hole attack. The first solution the sender node needs to verify the authenticity of the node that initiates the RREP packet by utilizing the redundancy of the network. The idea of this solution is to find more than one route for the destination. The SN unicast the ping packet using different routes. The IN or destination node or malicious node will ping requests. The SN checks the acknowledgment and processes them to check which one is safe or having malicious node. In the meantime the SNbuffered its packet until it found the safe route. When the route is identified the buffered packets will be transmitted to it. The drawback of the solution is the time delay. The second solution is to store the last sent packet sequence number and the last received packet sequence number in the table. It is updated when any packet is arrived or transmitted. When node receives reply from another node it checks the last sent and received sequence number. If there is any mismatch then an ALARM indicates the existence of a black hole node. This method is faster and more reliable and has no overhead.

Chang Wu Yu, Tung-Kuang, Wu, Rei Heng, Cheng, and Shun Chao Chang [24] proposed a distributed and cooperative procedure to detect black hole node. In this each node detect local anomalies. It collects information to construct an estimation table which is maintained by each node containing information regarding nodes within power range. This scheme is initiated by the initial detection node which first broadcast and then it notifies all one-hop neighbors of the possible suspicious node. They cooperatively decide that the node is suspicious node. Immediately after the confirmation of black hole, the global reaction is activated to establish proper notification system to send warning to the whole network. The simulation result show the higher black hole detection rate and achieves better packet delivery. When the network is busier it achieves less overhead.

Satoshi Kurosawa, Hidihisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto [25] use an anomaly detection scheme. It uses dynamic training method in which the training data is updated at regular time intervals. Multidimensional feature vector is defined to express state of the network at each node. Each dimension is counted on every time slot. It uses destination sequence number to detect attack. The feature vector include Number of sent out RREQ messages, number of received RREP messages, the average of difference of destination sequence number in each time slot between sequence number of RREP message and the one held in the list. They calculate mean vector by calculating some mathematical calculation. They compare distance between the mean vector and input data sample. If distance is greater than some threshold value then there is an attack. The updated data set to be used for next detection. Repeating this for time interval T anomaly detection is performed.

Hongmei Deng, Wei Li, and Dharma P. Agrawal [26] proposed a solution for single blackhole node detection. In this method, each intermediate node is used to send back the next hop information when it sends back an RREP message. After getting the reply message, the source node does not send the data packets but extracts the next hop information from the reply packet and then it sends a Further- Request to the next hop to verify that it has a route to the intermediate node who sends back the Further reply message, and that it has a route to the destination node.

Hesiri Weerasinghe [32] proposed the solution which discovers the secure route between source and destination by identifying and isolating cooperative black hole nodes. This solution adds on some changes in the solution proposed by the Ramaswamy to improve the accuracy. This algorithm uses a methodology to identify multiple black hole nodes working collaboratively as a group to initiate cooperative black hole attacks. This protocol is a slightly modified version of AODV protocol by introducing Data Routing Information (DRI) table and cross checking using Further Request (FREQ) and Further Reply (FREP). The simulation result shows that the AODV and the solution proposed by Deng et al. highly suffer from cooperative black hole in terms of throughput and packet losses. The performance of the solution is good and having better throughput and minimum packet loss percentage over other solutions.

IV. PROPOSED METHOD

Our proposed method is based on [29]. Flooding RREQ packets in the whole network will devour a lot of resource of network. To decrease blocking in a network, the AODV protocol adopts some methods. A node can not originate more than RREQ_RATELIMIT RREQ messages per second. After spreading a RREQ, a node waits for a RREP. If a path is not received within round-trip milliseconds, the node may try again to find out a route by broadcasting another RREQ, up to a upper limit of retry times at the greatest TTL value. Continual attempts by a source node at route detection for a single destination may exploit a binary exponential back off. The former time a source node broadcasts a RREQ, it counts roundtrip time for
the reception of a RREP. If a RREP is not received within that time, the source node sends another RREQ. When conniving 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 consequent to the second RREQ is 2*t round-trip time. The RREQ packets are teleivve in an incrementing ring to reduce the overhead caused by flooding the entire network. The packets are flooded in a small area (a ring) primary 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 engorged by increasing the TTL by a fixed value. The process is continual until an RREP is received by the originator of the RREQ, i.e., the route has been created.

In the Ad Hoc Flooding Attack, the attack nodes infringe the above rules to fatigue the network resource. Initially, the attacker chooses many IP addresses which are not in the networks if he knows the span of IP address in the networks. Because no node can answer RREP packets for these RREQ, the quash route in the route table of node will be preserved for longer. The attacker can choose arbitrary IP addresses if he cannot identify scope of IP address. Secondly, the attacker consecutively originates mass RREQ messages for these void IP addresses. The attacker tries to send unnecessary RREQ without considering RREQ_RATELIMIT within per second. The attacker will resend the RREQ packets exclusive of waiting for the RREP or round-trip time, if he uses out these IP addresses. The TTL of RREQ is set up to a highest exclusive of using growing ring search method. In the Flooding Attacks, the entire network will be full of RREQ packets which the attacker sends. The communication bandwidth is bushed by the flooded RREQ packets and the resource of nodes is bushed at the same time. For example, the storage of route table is restricted. If crowd RREQ packets are up coming to the node in a little time, the storage of route table in the node will drain so that the node cannot receive fresh RREQ packet. As a result, the genuine nodes cannot set up paths to send data.

A. Prevention of flooding attack

<table>
<thead>
<tr>
<th>TABLE I. - CALCULATION OF TIME OF RREQS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step1. received a RREQ;</td>
</tr>
<tr>
<td>Step2. if the RREQ is forwarded then quit;</td>
</tr>
<tr>
<td>Step3. look up node ID who send the RREQ in the table of Rate_RREQ;</td>
</tr>
<tr>
<td>Step4. Find node ID and RREQ_time:=RREQ_time+1;</td>
</tr>
</tbody>
</table>

To calculate the rate of RREQ and find the intruder, the Algorithm 2 is run one time every second.

<table>
<thead>
<tr>
<th>TABLE II. - DETECTION OF MALICIOUS NODE</th>
</tr>
</thead>
</table>

For every item of Rate_RREQ do
If RREQ_time > threshold then put Node_ID into Blacklist and RREQ_time:=0;
Else RREQ_time:=0;

B. Black Hole Attack:

In this type of attack, a malicious node sends bogus routing information, claiming that it has a unsullied (best) route and causes other good nodes to route data packets throughout the malicious one. For example, in AODV, the attacker can lunch a bogus RREP (including a bogus destination sequence number that is fabricated to be equivalent or elevated than the one restricted in the RREQ) to the source node, claiming that it has a brand new route (due to superior seq. no) to the destination node. This causes the source node to choose the path that passes through the attacker. Therefore, all traffic will be routed throughout the attacker, and therefore, the attacker can mistreat or abandon the traffic.

This malicious node then can select whether to drop the packets to execute a denial-of-service attack or to use its place on the path as the first step in a man-in-the-middle attack.

1) Proposed solution:

We have take additional metrics for route confirmation request (Conf_REQ) and route confirmation reply (Conf_REP) to shun the blackhole attack. In this approach, the intermediate node not only sends REPVs to the source node but also sends ConfREQs to its next-hop node toward the destination node. After receiving a Conf_REQ, the next-hop node looks up its cache for a path to the destination. If it has the path, it sends the Conf_REP to the source. Upon getting the Conf_REP, the source node can confirm the validity of the path by comparing the path in RREP and the one in Conf_REP. If both are matched, the source node judges that the route is truthful. One drawback of this approach is that it cannot avoid the black hole attack in which two consecutive nodes work in collusion, that is, when the next-hop node is a colluding attacker sending Conf_REP that support the incorrect path.

C. Gray Hole Attack:

A gray hole is a node that selectively drops and forwards data packets after it advertises itself as having the unswerving path to the destination node in retort to a route request message from a source node. The gray hole attack has two phases. In the first phase, a malicious node exploits the AODV protocol to publicize itself as having a legal route to a destination node, with the intention of intercepting packets, even though the route is spurious. In the second phase, the node drops the intercepted packets with a certain probability. This attack is more intricate to detect than the black hole attack where the malicious node drops the received data packets with certainty [5]. A gray hole may exhibit its malicious activities in different ways. It may drop...
packets coming from (or destined to) certain specific node(s) in the network whereas forwarding all the packets for other nodes. Another type of gray hole node may act maliciously for some time period by dropping packets but may change to normal activities later. A gray hole may also exhibit activities which are a mishmash of the above two, thereby making its detection even trickier.

Prevention Method: This type of attacks is more complicated to detect and prevent, for this type of attack we will use the concept of “Anomaly Detection” or behavioral scheme, in this scheme we define a normal profile of node using its communication behavioral to other nodes (like PDR, PMR, PMIR) if any node deviate from their regular profile that means the node is abnormal and further prevention mechanism will take to stop such type of activities.

We will simulate our proposed method using NS-3 [28] simulator.

V. CONCLUSION

In this paper we have discuss different types of attack that have been launch during routine procedure like a Flooding, Black Hole and Gray Hole. Than we have a presented a related work of detection and prevention of Black Hole and Gray Hole. Flooding is a type of attack launched using routing request. In this paper we have proposed a solution detection and prevention of Flooding, Black Hole and Gray Hole. Our approach is easy and fast and we will implement our proposed method using NS-3 Simulator.

REFERENCES


[8] Bo-Cang Peng and Chiu-Kuo Liang"Prevention techniques for flooding attack in Ad Hoc Networks"


ISSN: 2277 – 9043
International Journal of Advanced Research in Computer Science and Electronics Engineering
Volume 1, Issue 1, March 2012

All Rights Reserved © 2012 IJARCSEE

43


