Comparative Study of Routing Attacks and Discuss the Solutions to Mitigate Black Hole and Flooding Attacks in AODV Based MANET

Arti Tiwari¹, Prof.Nilmani Verma²
¹(Department of Computer Science& Engg ., MATS University, Raipur, India Email: arti.tiwari01@gmail.com)
² (Department of Computer Science& Engg. , MATS University, Raipur, India Email: nilmaniv@matsuniversity.ac.in)

ABSTRACT
Mobile ad hoc network (MANET) is a self configuring network consisting of nodes working courteously in ad hoc manner without a fixed infrastructure. Due to technological encroachment, MANET have become the network of choice for use in various applications, but most noteworthy challenge that MANET is facing is the security issue. Mane are not well protected against a range of attacks due to the security susceptibility in the routing protocols. AODV is such a routing protocol which is prone to a variety of security threats against ad hoc network. In this paper, we study the various routing attacks in MANET and thrash out the solutions to alleviate Black hole and Flooding attacks. In future, we design an authentication scheme to defend the network from various attacks.

Keywords - Attacks Mitigation on MANET, Black Hole, EDRI, Flooding, Trust based Scheme.

I. INTRODUCTION

A MANET (Mobile ad hoc network) is a collection of two or more devices outfitted with wireless communications and network capability. Such devices can communicates with another node that is instantly within their radio range or one that is outside their radio range. An intermediate node is used to relay or forward the packet from the source toward the destination. This kind of network is well suited for the critical applications such as military operations, emergency relief, and terrorism response where no pre-deployed infrastructure exists for communication. There are number of liability exist in MANET as lack of fixed infrastructure , limited bandwidth, dynamic topology, resource constraints and principally limited battery lifetime and memory usage etc. The actual transmission is actually complicated in order to systematize due to typical circle topology improvements. Redirecting as well as circle operations are generally performed agreeably with the nodes hence forms multiple hop architectural mastery, where by every single node are number together with router that will forward packets for different nodes that will is probably not inside of strong transmission assortment. Due to its inherent nature of lacking of any centralized admittance control, secure restrictions and limited resources mobile ad hoc network are vulnerable to numerous attacks. Some of the attacks are limited transmission range, control overhead, bandwidth wastage, time varying wireless link distinctiveness, hidden terminal problem, packet losses due to transmission errors, mobility induced route changes, frequent network partitions, broadcast nature of wireless medium, among them, routing attacks is one of the grave one. The mechanism is accessible in AODV routing protocol. AODV is a combination of on-demand and distance vector that is hop-to-hop routing methodology. When a node desires to know routes to explicit destination it creates a ROUTE REQUEST. Hereafter the course request is usually forwarded by simply intermediate nodes which in turn also create a invert route regarding itself regarding destination. If your request gets to a node with method to destination that creates yet again, Replay which in turn contains the quantity of hops which have been entail to realize the destination. All nodes that participate in forwarding this reply to the source node create a forward route to destination .This route created from each node from source to destination is a hop-by-hop state and not the entire route as in source routing. AODV is one of such reactive routing protocols with a weaker devise, which is prone to numerous security threats including Denial-of-Service (DoS) attacks such as Black hole and Gray hole attack.
In this paper, we study a range of routing attacks and examine the solution to mitigate Black hole and Flooding attacks in AODV routing protocols. The remainder of this paper is structured as follows. In section II describe Literature review, Section III give a pithy description of various routing attacks in MANET, Section IV study and discuss the solution to detect black hole and flooding attacks and finally conclusion in Section V.

II. LITERATURE SURVEY

Many Researchers have proposed a various methodology for prevent black hole and flooding attack in MANET. S. Marti et al [1] in Mitigating Routing Misbehavior in Mobile ad hoc network proposed trace malicious nodes by using watchdog/ pathrater. In watchdog when node forward a packet, the node’s watchdog verifies that the next node also forwards the packet in the path by promiscuously listening to the next node transmissions. If watchdog find that the next node does not forward the packet in predefined threshold time, the watchdog find that the node is malicious. In pathrater each node uses watchdog monitored results to rate its one-hop neighbors, further the node exchange their ratings. So that the pathrate can rate the path and choose a path with highest rating for routing. Deng, Li and Agrawal [2] proposed a mechanisms of defense against a black hole attack on AODV routing protocol. In their scheme, when the Route Reply packet is received from one of the Intermediate node, another route request is sent from the source node to the neighbor node of the intermediate node in the path. This ensures that whether there is such path actually exits from the intermediate node to the destination node. This scheme purge the black hole attack by a single attacker but fail to identify a cooperative black hole attack concerning multiple malicious nodes. Ramaswamy et al [3] proposed a methodology to shielding against the cooperative black hole attacks by using Data Routing Information (DRI) Table to keep track of past routing information among mobile nodes in the network and Cross checking of RREP messages from intermediate nodes by source nodes. The main negative aspect of this technique is that mobile node has to sustain an extra database of past routing experiences wastes memory space as well as overwhelming much more processing time that lead to slow communication. Ning et al [4] studied the insider attacks against mobile ad hoc routing protocols using AODV. They proposed a methodical analysis composed of two aspects. The first aspect is a set of all possible atomic misuse action that inside attacker may take to use wrongly a routing message. The second aspect is a set of misuse goals that a inside attacker may want to achieve. In [5] authors discussed how sinkhole attack can be launched in DSR and developed two rules called Sinkhole Intrusion Indicators(SIIS) for detecting sinkhole attack on DSR protocol. They did not discuss the consequence of the attack on DSR performance, rather they paying attention more on detection of the attack. Shandilya et al [6] studied flooding attacks and their countermeasures using DSR protocol for MANET. They propose a trust based estimation function for detection and prevention of RREQ flood attack. Humaira Ehsan et al [7] studied the implementation and analysis of routing attacks in manet. They propose the mechanism to compare various attacks with performance metrics such as throughput, average end to end delay etc.Author Arpita Raverkar [8] has been define three constraint Route discovery, throughput and delay for detection of flooding attack. Abdur Rashid Sangi et al [9] has been discuss regarding attack has been done by authorized node to interrupt the network called Byzantine attack. They emphasize the performance of AODV routing protocols. Gundeep Singh Bindra et al [10] anticipated a solution to tackle black hole and gray hole attack by maintaining an Extended Data Routing Information (EDRI) Table at each node in accumulation to the Routing Table of AODV protocol. The mechanisms are capable of detecting malicious node It also maintains a history of the preceding malicious node for identifying gray behavior. Rutvij H.Jhaveri [11] discuss the earlier work R-AODV, to detect and segregate multiple black hole and gray hole nodes during route discovery process and recommend a modified version to progress the performance of MANET.

III. ROUTING ATTACKS ON MANET

Mobile ad hoc network use routing protocols with the supposition that all the nodes can the perform operation in collective manner, but this supposition is not true when their some malicious node occurs which can disturb the network by sending fake messages many times, artificial direction-finding facts, and promotion artificial back links in order to affect direction-finding surgical procedures. Below us all handle a number of important direction-finding violence.

A. Black Hole Attack
In black hole attack, a malicious node sends fake routing information, claiming that it has the most favorable route and causes other good nodes to route data packets through the malicious one. For example, in AODV, the attacker can send a fake RREP (including a fake destination sequence number that is fictitious to be equal or higher than the one enclosed in the RREQ) to the source node, claiming that it has a suitably fresh route to the destination node. This causes the source node to select the route that passes through the attacker. Therefore, all traffic is attracted towards the attacker and attacker can misuse, drop the packet or not transmit the traffic.

Figure 1: Black-hole attack on AODV

B. Gray Hole Attack
A Gray hole attack is deviation of black hole attack, where an antagonist first behaves as an candidate node during the route discovery process, and then drops few or all of the data packets sent to it for further forwarding even when no congestion occurs. It is difficult to detect gray hole attack because nodes can drop packets in some measure not only due to its malicious nature but also due to excess, congestion or selfish nature.

C. Flooding Attack
In flooding attack, an attacker exhausts the network resources, such as bandwidth to consume, a node’s resources, computational and battery power or to disrupt the routings function to bring about ruthless destruction in network performance. One example is, in AODV method, a detrimental node may send a large number of Fake RREQ in a nutshell stretch of time to the particular destination node that doesn’t exist inside network, because nobody is accessible will reply to the RREQ, these RREQ will probably flood the full network, therefore, all on the node juice, as nicely as network bandwidth will be consumed and could lead to denial-of-service. The Flooding attack may be RREQ flooding or data flooding attacks. In data flooding the attacker first maintains a desired route to the destination and then sends the hopeless data packets to keep the network busy and stop the processing of valid data packets.

D. Sink Hole Attack
Sink hole attack can be categorized as route interference attacks. In these attacks a compromised node sends incorrect routing information to its neighbors and indicates that it has a low cost and most favorable route to the destination. Due to the manipulation of this routing information, it draws all or much of the traffic to itself. Neighbor nodes start sending all the packets through this node whether it drops all the packets or performs some other action.

E. Selfish Node Attack
The successful operation of MANET is depending on the collaboration of participation of each node in communication. The selfish node, which participates in the routing protocol correctly but does not forward the data packets to the destination. The malicious node may drop all or few of the data packets that are routed in the node and preserve the resources to satisfy their aspiration.

F. Link spoofing Attack
In Link spoofing attacks, a malicious node advertises fake links with non-neighbors to disrupt routing operations. It results in, malicious node influence the data or routing traffic.

G. Rushing Attack
Rushing attacks tend to be mainly up against the on-demand routing protocols. These kinds of attacks alter the way discovery process. On-demand routing protocols in which use identical restraint throughout route finding process tends to be defenseless for this attack. When sacrificed node is provided with a way request packet on the source node, it surges the bundle quickly through the entire network just before other nodes responding with reception on the same ask packet, they immediately forwards the actual control mail messages to get access to the multilevel.

IV. SOLUTION TO DETECT BLACK HOLE & FLOODING ATTACKS WITH THEIR DRAWBACKS

BLACK HOLE ATTACK-Some of the solutions to detect black hole attack and its drawback.
1. DRI Table and Cross Checking Scheme-
Hesiri Weerasinghe et al [13] proposed a solution to the use of Data Routing Information (DRI) to keep track of past routing information among mobile nodes along with cross checking of RREP messages from intermediate nodes by source node.

Drawback-
A. The main draw of these techniques is that the mobile node maintains an additional database of past routing information.
B. Large Wastage of memory space.
C. Increases 5-8% of communication overhead.

2. Mechanism of defense against black hole-
Deng et al [2] proposed a scheme, when the Route Reply packet is received from one of the intermediate node another Route Request is sent from the source node to the neighbor node of the intermediate node in the path. This check to ensure that the path really exist from the intermediate node to the destination. This scheme eliminates single black hole attack.

Drawback-
A. Routing Overhead.
B. It cannot prevent cooperatively black hole attacks.

3. Time based threshold detection scheme-
Tamilselvan L et al. [14] proposed a solution based on an augmentation of the original AODV routing protocol. The source node has to wait for replies with next hop information without sending the data packets to the destination. This scheme is based on the concept of timer in which after receiving the first request, it set the timer for collecting the request from the other nodes i.e. It sets timer in the “TimerExpiredTable”, to collect the further RREP’s from different nodes and are stored in “Collect Route Reply Table (CRRT)” with the “sequence number”, along with the time at which the packet arrives. The route validity is checked based on the arrival time of the first request and the threshold value.

Drawback-
A. Time delay.
B. Additional overhead incurred in Finding repeated next hop.

4. Redundant Route Method and Sequence Number Solution

M. Al-Shurman, S-M. Yoo and S. Park [15] proposed two different approaches to solve the black hole attack. The first solution the sender node needs to verify the authenticity of the node by which initiates this particular RREP packet by means of the redundancy from the network. Thinking concerning this solution is usually to find several routes to your destination. The drawback from the solution is the time hangs on. The instant solution is usually to store one more sent package sequence number plus the last acquired packet chain number inside table. It could be updated when any package is turned up or provided. When node receives reply via another node the item checks one more sent and also received chain number. When you have any mismatch after which it an SAFETY indicates this particular existence connected with any black pit node. That way is faster and much more reliable boasts no purchase.

Drawback-
A. Time Delay
B. Attacker can listen to the channel continuously and difficulty in updating the table for last sequence number each time when requesting the packet.

5. Fidelity Table Concept -
Latha Tamilselvan, Dr. V Sankaranarayanan in their paper about Prevention of Co-operative Black Hole Attack in MANET afforded a way of combat the Black opening attack. Within MANET, the absence of a repaired infrastructure, thus nodes have to cooperate so as to provide the necessary network functionality. One of the primary routing protocols used in Ad-hoc networks is AODV (Ad hoc on demand Distance vector) protocol. The security of the AODV protocol is compromised by a particular type of attack called Black Hole attack. In this attack a malicious node behaves itself as having the most optimal path to the node whose packets it wants to intercept. To reduce this prospect it is proposed to wait and check the replies from all the neighboring nodes to locate a safe route. His or her procedure for battle the Dark-colored hole episode. is to make use of a Fidelity Table wherein every participating node will be assigned a fidelity level that acts as a measure of reliability of that node, level of any node drops to 0, it is considered to be a malicious node termed as a Black hole and is eliminated.

Drawback- TimeDelay.

6. Detection and prevention of Cooperative Black hole & Gray hole using Extended DRI table-
Gundeep Singh et al. [10] proposed a fix that discusses black pit attacks simply by maintaining a long Data Redirecting Information (EDRI) Kitchen table at every single node beyond the Routing Table with the AODV process. The system is efficient at detecting a new malicious node. What's more, it maintains a history of the past node’s detrimental instances to be able to enlightenment for the gray habits. Refresh box, Renew Supply, BHID Supply, Further request and additional reply packets are also used beyond the existing packets (RREQ and also RREP). This technique is attained of locating string involving cooperating detrimental nodes that drop a tiny proportion involving packets.

Drawback- Fail to detect non consecutive cooperative node.

FLOODING ATTACK- Some of the solutions to detect flooding attack and its drawback.

1. Probabilistic model for flooding-
   Jian Hua[16] song proposed a probabilistic approach for flooding attack and attempting to take advantage of the phase transition phenomenon. When receiving a broadcast message for the first time, the host rebroadcast with the fixed probability P in order to maintain high trustworthiness.
   Drawback- In this mechanism, where a system undergoes diminutive changes of a given constraint in the system, induces a great alter in the system’s comprehensive behavior.

2. Filtering Scheme against RREQ Flood attack-
   In this effective scheme, a simple rate based control packet forwarding mechanism has been introduced to alleviate control packet. The advantage of this technique is that the protocol can be made secure against other type of probable DoS attacks.
   Drawback- This method does not able to distinguish between indisputable and counterfeit RREQs from the malicious node.

3. Trust based Security scheme –
   The Distributive approach has been proposed to detect and prevent the RREQ flooding attack. The effectiveness of the proposed technique depends on the solution of threshold values. This scheme used a trust based estimation function. The advantage of this scheme is that when the node identifies that sender is originating data flooding, it slash off the path and send error message.
   Drawback- It continuously sends packet until the time expired and getting delays to detect the misbehaving node occurs.

4. Period Based Defense Mechanism-
   The Period based defense mechanism is used to improve the throughput of burst traffic. It also guarantee Quality of Service (QoS) required for burst traffic.
   Drawback- When the number of packets per second is high, AODV cannot process packets because of the resource exhaustion.

5. Flooding attack using SVM (Support Vector Machine)-
   In this method primarily collect the behavior of every node then using this data to find out the flooded malicious node. For this collected behavior of every node pass the vector machine and check this to threshold limit if the node cross the threshold limit they are detect as a malicious node through he SVM.
   Drawback- maintain rate limit of the threshold value for the node.

V. CONCLUSION

In this paper, we have studied a various routing attacks in MANET and discuss the solution to detect Black hole and Flooding attack. In Future, we are planning to design an authentication scheme to provide network security with the malicious attack and improve the performance of the network.

VI. REFERENCES


