Detection of Blackhole Attack in AODV Wireless Network

Asst. Prof Rashmirekha Swain
Asst. Prof,
Computer science and Engineering Department,
Hi-Tech college of Engineering,Odisha

Lokanath Moharathy

Abstract **- Mobile Ad-hoc network (MANET) connects all different nodes together without knowledge of network connection. A MANET is a collection of wireless neighbor hosts for the radio network with multi hop without any hub connection. Mobile Ad-Hoc Networks is decentralized wireless systems. A Mobile Ad-hoc Network (MANET) is a self-configuring network of wireless and hence mobile devices that create a network which change topology dynamically .These may be used in future theft operations, medical applications in networks. MANETs contain unreliable wireless connection for linking in between hosts where as it changes topologies with battery, bandwidth, lifetime, and computation of host nodes . It has security aspects that contain the presence or absence of wireless network nodes.**

Keywords: Wireless Ad-hoc Network, Black Hole Attack, Security,Intrusion Detection Systems.

INTRODUCTION

MANETs are habituated to types of attacks. These include packet drop, eavesdropping, impersonation, and denial-of service in network interaction. Intrusion can be prevented as authentication and accurate transmission to improve the security, performance of an ad-hoc network. The ad hoc networks detection techniques, which monitor security status of the network and identify malicious behavior. A set of nodes in a MANET may be compromised in such a way that it may not be possible to detect their malicious behavior easily. The host nodes generate new routing messages to connect with non-existent links, and provide incorrect link state information, and spread different nodes with routing traffic, making drastic failure in the network.ad hoc on-demand distance vector (AODV) routing protocol is the starting part of on-demand routing protocol. MANET is the collection of unknown mobile nodes without any discrete infrastructure. The floating of nodes changes the topological figure continuously. Establishment in MANET mobile node sends the route request through routing messages. Existing routing protocols mobile nodes unable to find malicious node in the network thus malicious node generates fake routing message to connection links also spreads wrong information. The nodes are connected through mobile phones, devices and laptops. There is no path to monitor the traffic .After opening for all nodes and malicious nodes can access it. Black hole is one of the most common attacks made against the reactive routing protocol in MANETs. It is otherwise called as sequence number attack .The black hole attack includes malicious node(s) that have the shortest and freshest route to the destination. The aim of this paper is to detect black hole & methods inside ad-hoc on demand distance vector (AODV) routing protocol. The rest of this paper is organized as follows. Manet minimizes their cost as well as deployment time.

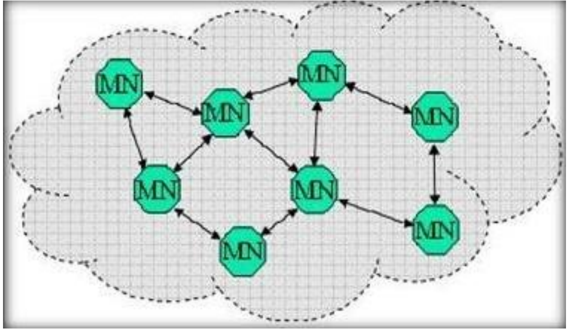
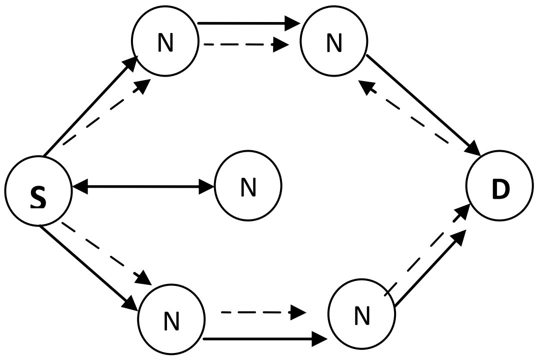


Diagram Of Manet

In MANET there are three types of protocols :

Routing Protocol

Reactive approach includes Ad-hoc On-Demand Distance Vector (AODV) Routing Protocol used for find a path to the destination in a network. **It** establish optimal path (min hops) between source and destination with minimum overhead and minimum bandwidth consumption so that packets are delivered in a timely way to larger mobile Multihop networks. The standard AODV routing protocol cannot fight the threat of Black Hole attacks, because during the phase of route discovery, malicious nodes may counterfeit sequence number and hop count in the routing message thereby, acquiring the route [3] , eavesdropping and dropping all the data packets as they pass or forward some selective packets to the destination.



1)RREQ ⟶2) RREP– – –3)RERR ⟷

Working of Aodv Protocol

Route Requests (RREQs), Route Replay (RREPs), Route Errors (RERRs) are control messages used for establishing a path to the destination. It has its source node, an intermediate node or a destination node in network communication [4]. By using all nodes, it varies behavior of a node. At first a source node wants to connect to a destination node, it checks in the existing route table first then check whether fresh route to that destination is available or not. If a fresh enough route is available, it uses the same. In Other case the node initiates a Route Discovery by broadcasting a RREQ control message to all of its neighbors.

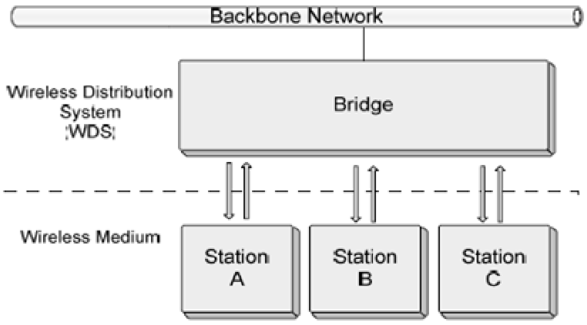


Diagram Of Wireless Distributed System

This RREQ message will further be forwarded (again broadcasted) by the intermediate nodes to their neighbors. This process will continue until the destination node or an intermediate node having a fresh route to the destination. At this stage eventually, a RREP control message is generated. Thus, a source node after sending a RREQ waits for RREPs to be received[5].

Routing protocols in MANETs are classified into proactive, reactive and hybrid protocols

1. Proactive Routing Protocol

This protocol otherwise known as Table Driven protocol. Since they maintain the routing information even before it is needed. Each and every node in the network maintains routing information to every other node in the network. Routes Information is generally kept in the routing tables and is periodically updated as the network topology changes. There exist some differences between the protocols that come under this category depending on the routing information being updated in each routing table. Furthermore, these routing protocols maintain different number of tables[6]. The proactive protocols are not suitable for larger networks, as they need to maintain node entries for each and every node in the routing table of every node. This causes more overhead in the routing table leading to consumption of more bandwidth.

2. Reactive Routing Protocol

These protocols are also called On Demand routing protocols since they don't maintain routing information or routing activity at the network nodes if there is no communication. If a node wants to send a packet to another node then this protocol searches for the route in an on-demand manner and establishes the connection in order to transmit and receive the packet [3]. The route discovery usually occurs by flooding the route request packets throughout the network. Reactive search procedures can also add a significant amount of control traffic to the network due to query flooding. Because of these weaknesses, reactive routing is less suitable for real-time traffic or in scenarios with a high volume of traffic between a large numbers of nodes[7].

3. Hybrid Routing Protocol

This type of protocols combines the advantages of proactive and of reactive routing. The routing is initially established with some proactively prospected routes and then serves the demand from additionally activated nodes through reactive flooding. The basic idea is that each node has a pre-defined zone centered at itself in terms of number of hops[9]. For nodes within the zone, it uses proactive routing protocols to maintain routing information. For those nodes outside of its zone, it does not maintain routing information in a permanent base.

BLACK HOLE ATTACK

Black hole attack is one of the possible attacks in MANETs. After initiated path with route discovery a malicious node sends a false RREP packet in order to pose itself as a destination node or an immediate neighbor to the actual destination node. It attracts all the packets by falsely claiming after receiving valid route to destination node[8]. It disturbs the routing protocol once receiving RREQ messages the attacker replies RREP messages directly and claims that it is the destination node or had valid route to destination node. The source node sends data packets to the black hole instead of the destination node. When the source node transmits data packets through the black hole, the attacker discards them without sending back a RERR message.

When a source node broadcasts the RREQ message for any destination, the black hole node with an RREP message immediately responds that includes the highest sequence number and this message is received as if it is coming from the destination or from a node route to the destination .It discards the other RREP Packets from source to destination coming from other nodes. Source itself starts to send out its data packets to the black hole destination. Without checking a malicious node sends RREP messages its routing table to a destination. They cannot transmit data from source to destination.

Source node unable to communicate with destination [2]. The malicious node always sends RREP when it receives RREQ without any AODV operations, with high Sequence number.

Related work

Hidehisa Nakayama [1] has been analyzed black hole attack, it initiates a route discovery that a malicious node impersonates a destination node by sending a route reply packet to a source node . It deprive the traffic from the source node. In order to prevent this kind of attack, it is crucial to detect the abnormality occurs during the attack.

Michael Hitchens [2] presented a scheme for providing security services for routing of control messages in an ad-hoc network .Our focus is on on-demand routing protocols for ad-hoc networks, specifically the Dynamic Source Routing Protocol.

Proposed Methodology

It is the Denial of service(DoS) otherwise called as sequence number attack Sequence number increases automatically RREQ and RREP message. It has the components like RREQ, RREP ,RERR , sequence number and hop count in DSDV. AODV routing protocol has every route entry is assigned by destination sequence number in the routing table . Malicious node receive the RREQ message from the neighboring node and more increase the destination sequence number and send reply message to the source node. When source node S wants to send data packet to destination node D. It creates route discovery process by using RREQ message having destination sequence number send to neighboring nodes.

Digital signatures is verification technique for blackhole attack by GSR. In AODV the route request is send to neighbor nodes by the source node. If destination node is one of them then ok otherwise route request broadcast to next node until the destination is found. The route request (RREQ) packet header contains the information of visiting node (node-id) in node information column and hop count column which contains the number of visiting nodes used in path. At the destination TTL scheme is used. the destination node select the shortest path with minimum number of nodes. the destination node unicast the reply whose header contain the column of node-id that contains the id of all nodes used in that path and digital signature column in which each visiting node adds its digital signature by WRP. When the receiving node received packet compare the digital signature of the previous node from its database. if the signature is match then that node is legitimate otherwise that node is considered as malicious node. When malicious node is detected then that info is broadcast to the neighbors. This process is repeated until the secure path is not found.

Algorithm:

Detection of Blackhole attack

```
Input: n nodes, Destination Point, Source Point;
Output: Detection of Black hole Attack,
Routing done by searching best path;
Start
    Search for the neighbor points or node of source , For source to destination Sending  Request to neighbor nodes for searching the destination. Direct path is established if starting node is the neighbor node otherwise Broadcast the RREQ to next neighbors .
End for
For destination to source
Select the path
If (Intermediate or destination node is malicious node)
```

Then add the malicious node information in malicious node column and again broadcast request (RREQ)
End for
End

SOLUTION

For the detection of malicious node the AODV protocol are required to find the closest path. The suggested criteria is, when the RREQ packets are broadcasted by sender, must slow down for reply. It first search for the nearest node for delivering the packet. If selected, anonymous packets are sending to its intermediate node. If there is no malicious node present then it can easily send the packet to next hop node . Wait for some time period for the conformed acknowledgement to destination point. Through different routes it send its requests .If destination node did not got any packet or null packet then it replies to the source for the fake packet by IDS .After getting dummy or duplicate packet it got the information about the malicious node near by it .After getting the packet it verify about the unwanted node if that was received then it reject that node .It has the network antenna by that it behaves positive when got the correct packet ,otherwise discard that packet.

FUTURE ENHANCEMENTS

After detection of the blackhole attack in the ad-hoc networks I will research for the simulation . In my study, AODV routing protocol the malicious nodes are detected and I will try to prevent this in near future. All routing protocols are expected to present different results. Therefore, the best routing protocol for minimizing the blackhole attack may be determined.

REFERENCES

(1) Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto, "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method".

(2) Rajan Shankaran, Vijay Varadharajan, Michael Hitchens, "Securing the Ad Hoc Dynamic Source Routing Protocol" IEEE 2006 .Nov. 2007.

(3) Ebrahim Mohamad, Louis Dargin. "Routing Protocols Security." In:Ad Hoc Networks". A Thesis at Oakland University School of Computer Science and Engineering.

(4) Performance comparison of two on demand routing protocols for ad hoc networks .C. Perkins, E. Royer, S. Das, and M. Marina. IEEE Personal Communications, 8(1): 16-28, 2001.

(5) A distributed adaptive cache update algorithm for the Dynamic Source Routing protocol. X. Yu and Z. Kedem. In Proc. 24th IEEE INFOCOM, March 2005. (An earlier version appeared as NYU CS Technical Report TR2003-842, July 2003.)

(6) Dynamic Source Routing in Ad Hoc wireless network http://www.comp.nus.edu.sg/bleong/geographic/related/johnson96dsr. Pdf

(7) Ensuring cache freshness in on-demand ad hoc network routing protocols. Y.-C. Hu and D. Johnson. In Proc. 2nd POMC, pp. 25-30,2002.

(8) The Dynamic Source Routing for mobile ad hoc networks D. Johnson, D. Maltz, and Y.-c. Hu., IETF Internet Draft. http://www .ietf.org/internet-drafts/draftietf-manet-dsr-l0.txt, July 2004.

(9) Predictive caching strategy for on demand routing protocols in wireless ad hoc networks. W. Lou and Y. Fang. Wireless Networks, 8(6): 671-679,2002.

ABBREVIATIONS

[1]MANET : Mobile Ad-Hoc Network

[2]DSDV : Destination-Sequenced Distance Vector Routing Protocol

[3]WRP : The Wireless Routing Protocol

[4]GSR : Global State Routing

[5]IDS : Intrusion Detection System

[6]DoS : Denial of Services

[7]RREQ : Route Request

[8]RREP : Route Replay

[9]RERR : Route Error