International Journal of All Research Education and Scientific Methods (IJARESM)
ISSN: 2455-6211, Volume 5, Issue 6, June 2017, Impact Factor: 2.287

A Review Paper on Black Hole Attack in MANET

Gourav Ahuja[1], Mrs. Sugandha[2]

M. Tech (CSE), Vaish College of Engineering, Rohtak, Haryana.
Astt. Prof. (CSE Dept.), Vaish College of Engineering, Rohtak, Haryana.

ABSTRACT

Ad-hoc networks have become a new standard of wireless communication in infrastructure less environment. MANET is a Mobile Ad-hoc Network in which the nodes get connected with each other without an access point. Messages are exchanged and relayed between nodes. Routing algorithms are utilized for forwarding packets between indirect nodes i.e not in direct range with aid of intermediate nodes. They are spontaneous in nature and absence of centralized system makes them susceptible to various attacks. Black hole attack is one such attack in which a malicious node advertises itself as the best route to the destination node and hinders the normal services provided by the network.

Keywords: Manet, Aodv, Black Hole Attack, Digital Signature;

I. INTRODUCTION

MANET is a multi-hop temporary communication network of mobile nodes equipped with wireless transmitters and receivers without the aid of any current network infrastructure. MANET is an emerging research area with practical applications. However, MANET is particularly vulnerable due to its fundamental characteristics, such as open medium, dynamic topology, distributed cooperation, and constrained capability. Routing plays an important role in the security of the entire network. Thus operations in MANET introduce some new security problems in addition to the ones already present in fixed networks.

According to the criterion that whether attackers disrupt the operation of a routing protocol or not, attacks in MANET can be divided into two classes: passive attacks and active attacks. In a passive attack, the attacker does not disrupt the operation of a routing protocol but only attempts to discover valuable information by listening to the routing traffic. In an active attack, however, these attacks involve actions performed by adversaries, modification and deletion of exchanged data to attract packets destined to other nodes to the attacker for analysis or just to disable the net-work. Some typical types of active attacks can usually be easily performed against MANET, such as, Denial of Service (DoS), impersonation, disclosure, spoofing and sleep deprivation. Most important networking operations include routing and network management. Routing protocols can be divided into proactive, reactive and hybrid protocols, depending on the routing topology. Proactive protocols are typically table-driven. Examples of this type include DSDV, WRP. Reactive or source-initiated on-demand protocols, in contrary, do not periodically update the routing information. It is propagated to the nodes only when necessary. Example of this type includes DSR, AODV and ABR. Hybrid protocols make use of both reactive and proactive approaches. Example of this type includes TORA, ZRP. Security is a major concern in all forms of communication networks, but ad hoc networks face the greatest challenge due to their inherent nature. As a result, there exist a slew of attacks that can be performed on an Ad hoc net-work.

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 .Due to absence of any kind fixed infrastructure and open wireless medium security implementation is difficult. In manet each node function as a host as well as router, forwarding packets for another nodes in the network. MANET is vulnerable to various kind of attacks. These include active route interfering, imprecation and denial of service. Black hole attack is one of many possible attacks in MANET. In this attack, a malicious node sends a forged Route REPLY (RREP) packet to a source node that initiates the route discovery in order to pretend to be a destination node. The malicious node launches this attack by advertising fresh route with least hop count and highest destination sequence number to the node which starts the route discovery.

II. AODV ROUTING PROTOCOLS

The AODV routing protocol is an adaptation of the DSDV protocol for dynamic link conditions. Every node in an ad hoc network maintains a routing table, which contains information about the route to a particular

destination. Whenever a packet is to be sent by a node, it first checks with its routing table to determine whether a route to the destination is already available. If so, it uses that route to send the packets to the destination. If a route is not avail-able or the previously entered route is inactivated, then the node initiates a route discovery process.

AODV is an on demand distance vector routing protocol. In on demand routing a route is established between communicating nodes only. There is no fixed existing route as in table driven systems. Whenever a node needs to send data packets it has to initiate route discovery process. Route discovery consists of two messages: Route Request (RREQ) and Route Reply (RREP).

The source node broadcasts the RREQ messages to its neighbors which further broadcasts them to their neighbors and so on. In response to RREQ, either the destination node replies with RREP or intermediate node having route to destination replies with RREP. When intermediate node replies it is called Gratuitous Route Reply. Validity and freshness of route is decided by destination sequence number. If destination sequence number is higher than before than route is considered valid. Source selects the path for data packets transmission from which it received RREP first. Further received RREPs are discarded.

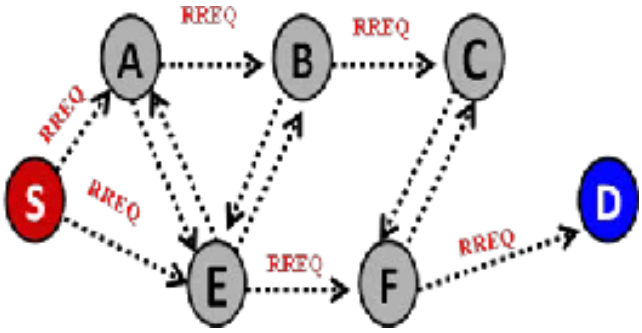


Fig: 1, AODV routing protocol with RREQ and RREP message

For route maintenance nodes periodically send HELLO messages to neighbor nodes. If a node fails to receive three consecutive HELLO messages from a neighbor, it concludes that link to that specific node is down. A node that detects a broken link sends a Route Error (RERR) message to any upstream node.

III. BLACKHOLE ATTACK

Black hole problem in MANET is a serious security problem to be solved. In this problem, a malicious node uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept.

Internal Black Hole Attack

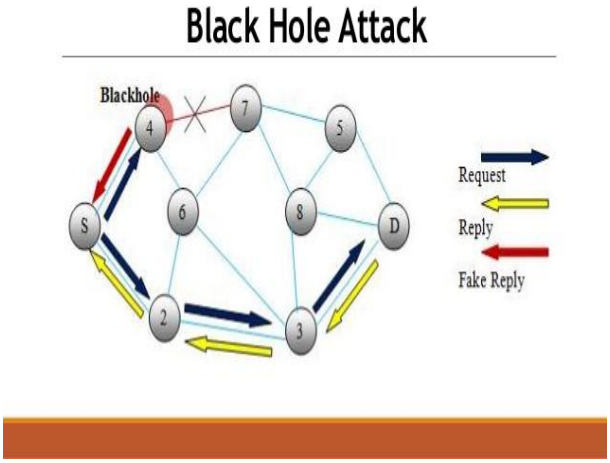
In this attack malicious node fits in between the routes of source and destination. As its present internally so this node make itself an active data route element. Now that node is capable of conducting attack in network. Internal attack is more sever then external attack.

External Black Hole Attack

External attacks physically stay outside of the network and deny access to network traffic or creating congestion in network or by disrupting the entire network. External attack can become a kind of internal attack when it take control of internal malicious node and control it to attack other nodes in MANET. In this

- Malicious node detects the active route and notes the destination address.
- Then Malicious node sends a route reply packet (RREP) including the destination address field spoofed to an unknown destination address. Hop count value is set to lowest values and the sequence number is set to the highest value.
- Malicious node send RREP to the nearest available node which belongs to the active route. This can be send directly to the data source node if route is available.
- The RREP received by the nearest available node to the malicious node will relayed via the established inverse route to the data of source node. The new information received in the route reply will allow the source node to update its routing table.

- New route selected by source node for selecting data. The malicious node will drop now all the data to which it belong in the route because is presented inside the network.



IV. SECURITY GOALS

In providing a secure networking environment some or all of the following service may be required.

Authentication:- This service verifies the identity of node or a user, and to be able to prevent impersonation. In wired networks and infrastructure-based wireless networks, it is possible to implement a central authority at a point such as a router, base station, or access point. But there is no central authority in MANET, and it is much more difficult to authenticate an entity. Authentication can be providing using encryption along with cryptographic hash function, digital signature and certificates.

Confidentially :-Keep the information sent unreadable to unauthorized users or nodes. MANET uses an open medium, so usually all nodes within the direct transmission range can obtain the data. One way to keep information confidential is to encrypt the data, and another technique is to use directional antennas. It also ensures that the transmitted data can only be accessed by the intended receivers.

Integrity:- Ensure that the data has been not altered during transmission. The integrity service can be provided using cryptography hash function along with some form of encryption. When dealing with network security the integrity service is often provided implicitly by the authentication service.

Availbility:-Ensure that the intended network security services listed above are available to the intended parties when required. The availability is typically endure by redundancy, physical protection and other non-cryptographic means, e.g. use of robust protocol.

Non- Repudation:- Ensure that parties can prove the transmission or reception of information by another party, i.e. a party cannot falsely deny having received or sent certain data. By producing a signature for the message, the entity cannot later deny the message. In public key cryptography, a node A signs the message using its private key. All other nodes can verify the signed message by using A's public key, and A cannot deny that its signature is attached to the message.

V. SOLUTION

This research will focus on providing an efficient technique in the network that detect the malicious node in the network. Malicious node has 2 properties: it always attack on the active route in the network and it sends the RREP first before the others. I have using the verification technique Digital signature for the solution. Every node in the network has its own digital signature. It gives the better security.

VI. CONCLUSION

This paper mainly focused on the black hole attack in network. How it is detect from the network .How can we prevent our data from malicious node . Due to their dynamic nature, it will require higher security. A future scope of this is to find an effective solution to the black hole attack on AODV.

REFRENCES

[1]. Deng Hongmei, Li Wei and Agrawal D.P. (2002) IEEE Communications Magazine, 70-75.
[2]. Papadimitratos P. and Haas Z. Communication Networks and Distributed Systems Modeling and Simulation.
[3]. Semih Dokurer, Erten Y.M. and Acar C.E. (2007) Performance analysis of ad-hoc networks under black hole attack. 148-153.
[4]. Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamal pour and Yoshiaki Nemoto (2007) International Journal of Network Security, 5(3), 338-346.