Volume 3, Issue 8, August 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

DPCOBHA (Deduction and Prevention of Cooperative Black Hole Attack) in MANET

H.Lakshmipriya[1],
[1]M.phil scholar, Department of Computer Applications,
Bharathidasan University, Trichy

Mrs.M.Lalli[2]
[2]Asst.Professor, Department of Computer Applications,
Bharathidasan University, Trichy

Abstract: A mobile ad hoc network (MANET) is a collection of autonomous nodes that communicate with each other by forming a multi-hop radio network and maintaining connections in a decentralized manner. Security remains a major challenge for these networks due to their features of open medium, dynamically changing topologies, reliance on cooperative algorithms, absence of centralized monitoring points, and lack of clear lines of defence. Most of the routing protocols for Manets are thus vulnerable to various types of attacks. Ad hoc on-demand distance vector routing (AODV) is a very popular routing algorithm. However, it is vulnerable to the well-known black hole attack, where a malicious node falsely advertises good paths to a destination node during the route discovery process. This attack becomes more sever when a group of malicious nodes cooperate each other. In this paper, a defence mechanism is presented against a coordinated attack by multiple black hole nodes in a MANET. The simulation carried out on the proposed scheme has produced results that demonstrate the effectiveness of the mechanism in detection of the attack while maintaining a reasonable level of throughput in the network.

Keywords: MANET, Wormhole Attack, Byzantine Attack, Black hole Attack, Information Disclosure, Resource Consumption Attack, MAODV Algorithm.

1. Introduction:

An ad hoc network is a collection of nodes that do not have any predefined Infrastructure to keep the network connected. Nodes help each other in conveying information about the topology of the Network. The Mobile Ad-hoc Networks (Manets) differ from existing networks by the fact that they depend on no fixed infrastructure. Nodes forming the network perform all functionality of the network with each node performs the functionality of both host and router. A Mobile ad hoc network is also called as "short live" networks. [1].

1.1. Characteristics of MANET

1. In MANET, each node acts as both host and router. That is it is autonomous in behavior.
2. Multi-hop radio relaying- When a source node and destination node for a message is out of the radio range, the MANETs are capable of multi-hop routing.
3. Distributed nature of operation for security, routing and host configuration. A centralized firewall is absent here.
4. The nodes can join or leave the network anytime, making the network topology dynamic in nature.
5. Mobile nodes are characterized with less memory, power and light weight features.
6. The reliability, efficiency, stability and capacity of wireless links are often inferior when compared with wired links. This shows the fluctuating link bandwidth of wireless links.
7. Mobile and spontaneous behavior which demands minimum human intervention to configure the network.
8. All nodes have identical features with similar responsibilities and capabilities and hence it forms a completely symmetric environment.
9. High user density and large level of user mobility.
10. Nodal connectivity is intermittent.

1.2. Application areas

1. Military or police exercises
2. Disaster relief operations
3. Mine site operations
4. Urgent business meetings
5. Robot data acquisition

1.3. Merits of MANET

1. They provide access to information and services regardless of geographic position.
2. These networks can be set up at any place and time.
3. These networks work without any pre-existing infrastructure.

1.4. Demerits of MANET

1. **Limited resources:** Limited resource invokes the problem of limited security
2. **Lack of authorization facilities:** Intrinsic mutual trust is vulnerable to attacks
3. **Time varying topology:** Volatile, changing network topology makes it hard to detect malicious nodes.
4. Security protocols for wired network cannot work for ad-hoc networks.

2. Network Layer Attack:

1. Wormhole Attack
2. Black hole Attack
3. Byzantine Attack
4. Information Disclosure
5. Resource Consumption Attack

2.1. Wormhole Attack.

In wormhole attack, a malicious node receives packets at one location in the network and tunnels them to another location in the network, where these packets are resent into the network. [2] This tunnel between two colluding attackers is referred to as a wormhole. It could be established through wired link between two colluding attackers or through a single long-range wireless link. In this form of attack the attacker may create a wormhole even for packets not addressed to itself because of broadcast nature of the radio channel.

2.2. Black hole Attack.

The black hole attack has two phases. In the first phase, the malicious node exploits the ad hoc routing protocol such as AODV to advertise itself as having a valid route to a destination node, with the intention of intercepting packets, even though the route is spurious. In the second phase, the attacker node drops the intercepted packets without forwarding them. There is a more subtle form of this attack when an attacker node suppresses or modifies packets originating from some nodes, while leaving the data packets from other nodes unaffected. This makes it difficult for other nodes to detect the malicious node. [3].

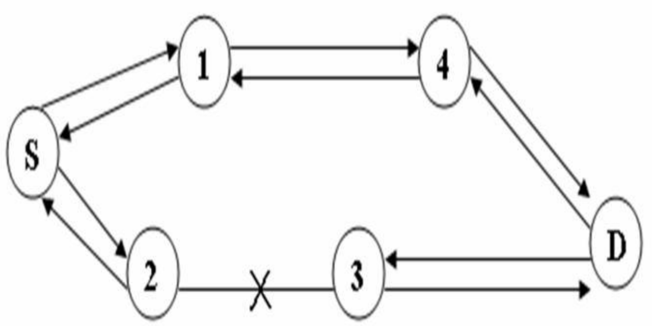

Figure: 1

2.3. Byzantine Attack

In this attack, a compromised intermediate node or a set of compromised intermediate nodes works in collusion and carries out attacks such as creating routing loops, forwarding packets on non-optimal paths and selectively dropping packets [4] which results in disruption or degradation of the routing services. It is hard to detect byzantine failures. The network would seem to be operating normally in the viewpoint of the nodes, though it may actually be showing Byzantine behavior.

2.4. Information Disclosure

Any confidential information exchange must be protected during the communication process. Also, the critical data stored on nodes must be protected from unauthorized access. In ad hoc networks, such information may contain anything, e.g., the specific status details of a node, the location of nodes, private keys or secret keys, passwords, and so on. Sometimes the control data are more critical for security than the traffic data. For instance, the routing directives in packet headers such as the identity or location of the nodes can be more valuable than the application-level messages. A compromised node may leak confidential or important information to unauthorized nodes present in the network. Such information may contain information regarding the network topology, geographic location of nodes or optimal routes to authorized nodes in the network.

2.5. Resource Consumption Attack:

In this attack, an attacker tries to consume or waste away resources of the other nodes present in the network [5]. The resources that are targeted are:

1. Battery power
2. Band width
3. Computational power

3. Problem Definition:

3.1. Cooperative Black Hole Attack:

The black hole attack has two phases. In the first phase, the malicious node exploits the ad hoc routing protocol such as AODV to advertise itself as having a valid route to a destination node, with the intention of intercepting packets, even though the route is spurious. In the second phase, the attacker node drops the intercepted packets without forwarding them. There is a more subtle form of this attack when an attacker node suppresses or modifies packets originating from some nodes, while leaving the data packets from other nodes unaffected. This makes it difficult for other nodes to detect the malicious node. In this work, however, a defense mechanism has been proposed against a cooperative black hole attack in a MANET that relies on AODV routing protocol.

In the standard AODV protocol, when the source node *S* (Fig. 2) wants to communicate with the destination node *D*, the source node *S* broadcasts the ***Route Request*** **(RREQ)** packet. Each neighboring active node updates its routing table with an entry for the source node *S*, and checks if it is the destination node or whether it has the current route to the destination node. If an intermediate node does not have the current route to the destination node, it updates the RREQ packet by increasing the hop count, and floods the network with the RREQ to the destination node *D* until it reaches node *D* or any other intermediate node that has the current route to *D*, as depicted in Fig.2.

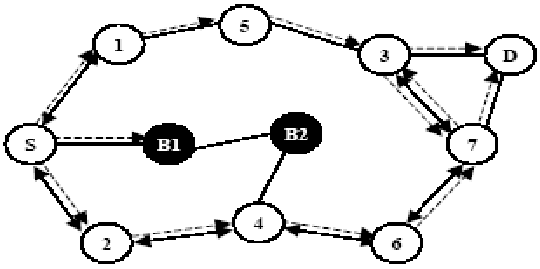

Fig.2. Network flooding by RREQ messages

The destination node *D* or any intermediate node that has the current route to *D*, initiates a ***Route Reply*** **(RREP)** in the reverse direction, as depicted in Fig. 3. Node *S* starts sending data packets to the neighboring node that responded first, and discards the other responses. This works fine when the network has no malicious nodes.

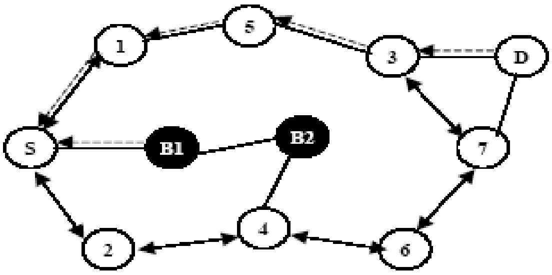

Fig.3. Propagation of RREP messages

In [7], authors have proposed a solution to identify and isolate a single black hole node. However, the security threat arising out of the situation where multiple black hole nodes act in coordination has not been addressed. For example, when multiple black hole nodes are acting in coordination with each other, the first black hole node B1 refers to one of its partners B2 as the next hop, as depicted in Fig. 2. In the mechanism propose in [7], the source node S sends a Further Request (FRq) to B2 through a different route (S-2-4-B2) other than via B1. Node S asks B2 if it has a route to node B1 and a route to destination node D. Because B2 is cooperating with B1, its “Further Reply (FRp)” will be “yes” to both the questions. According to the solution proposed in [7], node S starts sending the data packets assuming that the route S-B1-B2 is secure. However, in reality, the packets are intercepted and then dropped by node B1 and the security of the network is compromised.

In [2], authors have proposed a solution to identify and isolate a Cooperative black hole node. However the security threat arising out of the situation at a time he check one intermediate node for find path so we can loss more time for detect the attacker. However, in reality, the packets are intercepted and then dropped by attacker and the security of the network is compromised.

4. Proposed Solution:

In this the file is transferred from source node to destination node while transferring files, the file is split into packets and pass through intermediate node, detect the black hole,identify the trusted node and avoids packet drop.

1. Raise in performance
2. Secure file transfer
3. Avoid Packet Drops.

4.1. Algoritham:

Notations:

SN – Source Node IN- Intermediate Node
DN- Destination Node NHN-Next Hope Node
FRq – Further Request FRp- Further Reply
DRI – Data Routing Information
ID- Identify the Node

```
SN Broadcasts RREQ
SN receives RREP
IF(RREP is from DN or a reliable node){
Route Data Packets (Secure Route)}
Else {  Do {
Send FRq and ID of IN to NHN
Receive FRq.NHN of current NHN, DRI entry for
NHN's next hop ,DRI entry for current IN
IF(NHN is reliable node){
Check IN for blackhole  using DRI entry
IF ( IN is not black hole){
Route Data packets(Secure Route)
Else{
Insecure Route
IN is a Black hole
All the nodes along the reverse path from IN to
the node generate RREP are Black holes
}
}Else
Current IN=NHN
}While (IN is not a reliable node)}
```

4.2. Use case Diagram:

The Packet drop is identified in Intermediate Node, in this system(Fig:4) while transferring the file the intermediate node is checked by using information in the routing table and forward the packets by other path helps to avoid packet losing and secure data transfer.

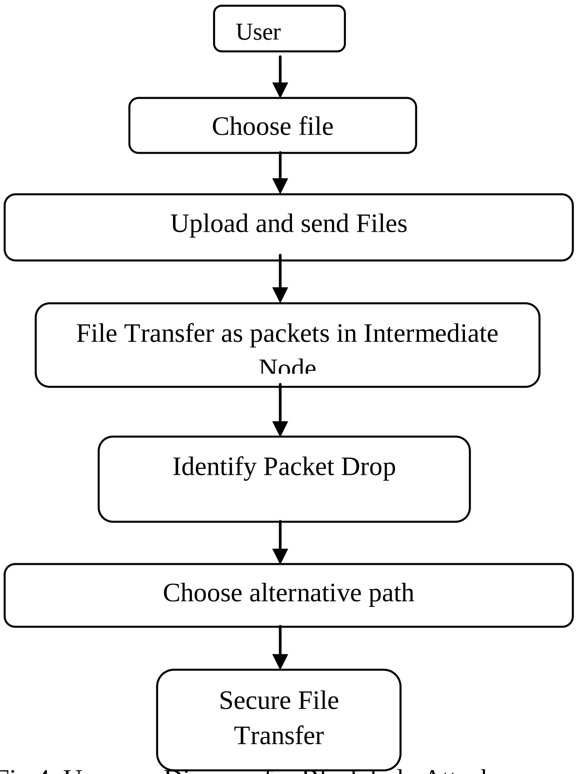

Fig 4. Use case Diagram for Black hole Attack

5. Conclusion:

In this paper, Routing security issues in MANETs are discussed in general, and in particular the cooperative black hole attack has been described in detail. A security protocol has been proposed that can be utilized to identify multiple black hole nodes in a MANET and thereby identify a secure routing path from a source node to a destination node avoiding the black hole nodes. As a future scope of the paper deals is an attempt to implant the algorithm and give the solutions to this black hole attack.

Reference:

[1]. Abhay Kumar Rai, Rajiv Ranjan Tewari & Saurabh Kant Upadhyay " Different Types of Attacks on Integrated MANET-Internet Communication"

[2]. Jaydip Sen1, Sripad Koilakonda2, Arijit Ukil3 "A Mechanism for Detection of Cooperative Black Hole Attack inMobile Ad Hoc Networks.

[3]. Rusha Nandy, Debdutta Barman Roy "Study of Various attacks in Manet and Elaborative discussion of Rushing attack on DSR with clustering scheme"

[4]. B. Awerbuch, D. Holmer, C. Nita Rotaru and Herbert Rubens. "An On-Demand Secure Routing Protocol Resilient to Byzantine Failures". Proceedings of the ACM Workshop on Wireless Security 2002, Pages 21-30, September 2002.

[5]. A. Mishra, K. Nadkarni, and A. Patcha, "Intrusion Detection in Wire- less Ad Hoc Networks," IEEE Wireless Communications, Vol. 11, Issue 1, pp. 48-60, February 2004.

[6]. Dr. A. A. Gurjar, A. A. Dande "Black Hole Attack in Manet's: A Review Study" International Journal of IT, Engineering and Applied Sciences Research (IJIEASR) ISSN: 2319-4413 Volume 2, No. 3, March 2013.

[7]. H. Deng, H. Li, and D. Agrawal, "Routing security in wireless ad hoc networks", IEEE communications Magazine, Vol. 40, No. 10, Oct 2002.