Black hole Attack Avoidance Protocol for wireless Ad-Hoc networks

Ms. Namrata Maheswari[1] Mr. Raj Kumar Somani[2] Mr. Pankaj Singh Parihar[3]
[1]Research Scholar [M. Tech CSE] [2]Head [CSE] [3]Assistant. Professor
[1,2,3]Institute of Technology and Management , Bhilwara, Rajsthan

Abstract— A Mobile Ad-Hoc Network is a collection of mobile nodes or a temporary network set up by wireless mobile nodes moving arbitrary in the places that have no network infrastructure in such a manner that the interconnections between nodes are capable of changing on continual basis. Thus the nodes find a path to the destination node using routing protocols. However, due to security vulnerabilities of the routing protocols, wireless ad-hoc networks are unprotected to attacks of the malicious nodes. Various attacks and one of those attacks is the Black Hole Attack against network integrity absorbing all data packets in the network. Since the data packets do not reach the destination node on account of this attack, data loss will occur. Therefore, it is a severe attack that can be easily employed against routing in mobile ad hoc networks. There are lots of detection and defense mechanisms to eliminate the intruder that carry out the black hole attack. . Virtual Infrastructure achieves reliable transmission in Mobile Ad Hoc Network. Black Hole Attack is the major problem to affect the Virtual Infrastructure. In this paper, approach on analyzing and improving the security of AODV, which is one of the popular routing protocols for MANET. Our aim is to ensuring the avoidance against Black hole attack.

Keywords: MANET, Routing in MANET, Security Goals, Security Issues for MANET and Security Attach, AODV Routing Protocol.

I. INTRODUCTION

Mobile ad-hoc networks are composed of autonomous nodes that are self- managed without any infrastructure. In this way, ad-hoc networks have a dynamic topology such that nodes can easily join or leave the network at any time.

MANETs have some special characteristic features such as unreliable wireless media (links) used for communication between hosts, constantly changing network topologies and memberships, limited bandwidth, battery, lifetime, and computation power of nodes etc. MANETs are vulnerable to various types of attacks. One of the most critical problems in MANETs is the security vulnerabilities of the routing protocols. Intrusion prevention measures such as strong authentication and redundant transmission can be used to improve the security of an ad hoc network. However, these techniques can address only a subset of the threats.

Moreover, they are costly to implement. One of the most widely used routing protocols in MANETs is the ad hoc on demand distance vector (AODV) routing protocol [1]. It is a source initiated on-demand routing protocol. However, AODV is vulnerable to the well-known black hole attack. In the Black Hole attack, a malicious node absorbs all data packets in itself, similar to a hole which sucks in everything. In route discovery process of AODV protocol, intermediate nodes are responsible to find a fresh path to the destination, sending discovery packets to the neighbor nodes. Malicious nodes do not use this process and instead, they immediately respond to the source node with false information as though it has fresh enough path to the destination. Therefore source node sends its data packets via the malicious node to the destination assuming it is a true path. Black Hole attack may occur due to a malicious node which is deliberately misbehaving, as well as a damaged node interface. In any case, nodes in the network will constantly try to find a route for the destination, which makes the node consume its battery in addition to losing packets. In this paper, a mechanism is proposed to identify multiple black hole nodes cooperating as a group in an ad hoc network. The proposed technique works with slightly modified AODV protocol and makes use of the data routing information table in addition to the cached and current routing table.

II. MOBILE AD HOC NETWORK

This network is called Independent Basic Service Set (IBSS) Stations in an IBSS communicate directly with each other and do not use an access point. Because of the mobility associated with ad-hoc networks, they are commonly called MANET (Mobile Ad-hoc Network). MANETs are self-organized networks whose nodes are free to move randomly while being able to communicate with each other without the help of an existing network infrastructure. MANETs are suitable for use in situations where any wired or wireless infrastructure is inaccessible, overloaded, damaged or destroyed such as emergency or rescue missions, disaster relief efforts and tactical battlefields, as well as civilian MANET situations, such as conferences and classrooms or in the research area like sensor networks. MANETs eliminate this dependence on a fixed network infrastructure where each station acts as an intermediate switch.

III. ROUTING IN MANET

MANETs have special limitation and properties such as limited bandwidth and power, highly dynamic topology, high error rates etc. Moreover, compared to infrastructure based networks, in a MANET, all nodes are mobile and can be connected dynamically in an arbitrary manner. Nodes of MANET behave as router and take part in discovery and maintenance to establish a reliable route of each other. Therefore, routing protocols for wired networks cannot be directly used in wireless networks and numerous protocols have been developed for MANETs. These routing protocols are divided into two categories based on management of routing tables. These categories are Table Driven Routing Protocols and On-Demand Routing Protocols, shown in the Table 1 and they are explained below:

In this, we have used Ad-Hoc On-Demand Distance Vector Routing (AODV) and implemented Black Hole attack to this protocol.

MANET ROUTING PROTOCOLS
Table Driven Routing Protocols
Destination-Sequenced Distance Vector Routing Protocol (DSDV)
Wireless Routing Protocol (WRP)
Global State Routing (GSR)
Fisheye State Routing (FSR)
Hierarchical State Routing (HSR)
Zone-based Hierarchical Link State Routing Protocol (ZHLS)
Clusterhead Gateway Switch Routing Protocol (CGSR)
On-Demand Routing Protocols
Ad-Hoc On-Demand Distance Vector Routing (AODV)
Cluster based Routing Protocols (CBRP)
Dynamic Source Routing Protocol (DSRP)
Temporally Ordered Routing Algorithm (TORA)
Associativity Based Routing (ABR)
Signal Stability Routing (SSR)

Table (1): Classification of MANET routing protocols

IV. SECURITY GOALS

Security involves a set of investments that are adequately funded. In MANET, all networking functions such as routing and packet forwarding, are performed by nodes themselves in a self-organizing manner. For these reasons, securing a mobile ad-hoc network is very challenging. The goals to evaluate if mobile ad-hoc network is secure or not are as follows:

1) Availability
2) Confidentiality
3) Integrity
4) Authentication
5) Non-repudiation
6) Anonymity

V. SECURITY ISSUES FOR MANET AND SECURITY ATTACH

Securing wireless ad-hoc networks is a highly challenging issue. Understanding possible form of attacks is always the first step towards developing good security solutions. Security of communication in MANET is important for secure transmission of information. [4]Absence of any central co-ordination mechanism and shared wireless medium makes MANET more vulnerable to digital / cyber-attacks than wired network there are a number of attacks that affect MANET. These attacks can be classified into two types:

A. Passive Attacks

Passive attacks are the attack that does not disrupt proper operation of network .Attackers snoop data exchanged in network without altering it. Requirement of confidentiality can be violated if an attacker is also able to interpret data gathered through snooping .Detection of these attack is difficult since the operation of network itself does not get affected.

B. Active Attacks

Active attacks are the attacks that are performed by the malicious nodes that bear some energy cost in order to perform the attacks. Active attacks involve some modification of data stream or creation of false stream. Active attacks can be internal or external. External attacks are carried out by nodes that do not belong to the network. Internal attacks are from compromised nodes that are part of the network. Since the attacker is already part of the network, internal attacks are more severe and hard to detect than external attacks. Active attacks, whether carried out by an external advisory or an internal compromised node involves actions such as impersonation (masquerading or spoofing), modification, fabrication and replication.

1) Black hole.
2) Gray hole
3) Worm hole
4) Jellyfish attack
5) Spoofing.
6) Sybil attack

C. Black Hole Attack

To carry out a black hole attack, malicious node waits for neighboring nodes to send RREQ messages. When the malicious node receives an RREQ message, without checking its routing table, immediately sends a false RREP message giving a route to destination over itself, assigning a high sequence number to settle in the routing table of the victim node, before other nodes send a true one. Therefore requesting nodes assume that route discovery process is completed and ignore other RREP messages and begin to send packets over malicious node.

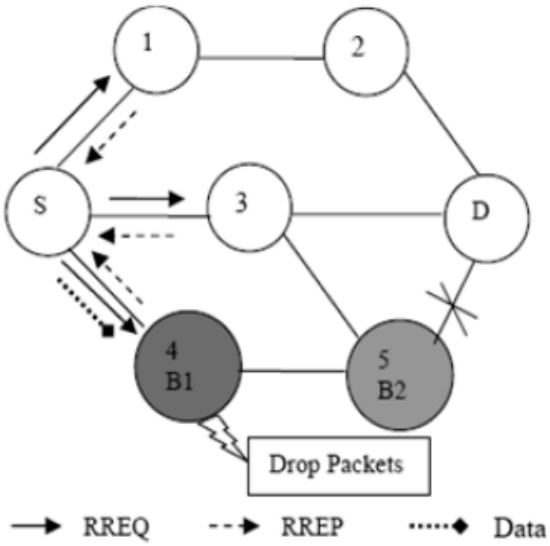

Fig. 1: Black Hole Attack

Malicious node attacks all RREQ messages this way and takes over all routes. Therefore all packets are sent to a point when they are not forwarding anywhere. This is called a black hole akin to real meaning which swallows all objects and matter. To succeed a black hole attack, malicious node should be positioned at the center of the wireless network. If

malicious node masquerades false RREP message as if it comes from another victim node instead of itself, all messages will be forwarded to the victim node. By doing this, victim node will have to process all incoming messages and is subjected to a sleep deprivation attack.

VI. AODV ROUTING PROTOCOL

The Ad Hoc On-demand Distance Vector (AODV) routing protocol is an adaption of the DSDV protocol for dynamic link conditions [2][6]. 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 the 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 available or the previously entered route is inactivated, then the node initiates a route discovery process. A RREQ (Route Request) packet is broadcasted by the node. Every node that receives the RREQ packet first checks if it is the destination for that packet and if so, it sends back an RREP (Route REPly) packet. This Destination Sequence number is the sequence number of the last sent packet from the destination to the source. If the destination sequence number present in the routing table is lesser than or equal to the one contained in the RREQ packet, then the node relays the request further to its neighbors. If the number in the routing table is higher than the number in the packet, it denotes that the route is a „fresh route" and packets can be sent through this route. This intermediate node then sends a RREP packet to the node through which it received the RREQ packet. Since AODV has no security mechanisms, malicious nodes can perform many attacks just by not behaving according to the AODV rules.

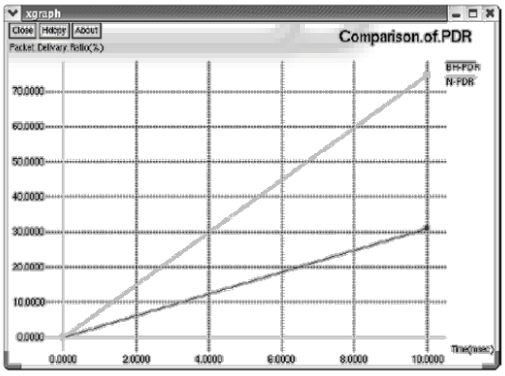

Fig. 2: PDR(%) Vs Time

VII. SIMULATION

The experiments for the evaluation of the proposed scheme have been carried out using the network simulator ns-1. The 802.11 MAC layer implemented in ns-1 is used for simulation. An improved version of random waypoint model is used as the model of node mobility [13]. Performances of the three protocols are evaluated:

(i) Standard AODV protocol,

(ii) AODV with two malicious nodes cooperating in a black hole attack,

(iii) AODV with the proposed algorithm. The scenarios developed to carry out the tests use two parameters: the mobility of the nodes and the number of active connections in the network. Every point in the graph is an average of the values obtained after the experiment is repeated five times.

In Fig. 2, packet delivery ratio is plotted against the Time (m/sec). It is observed that AODV performs better for lower node mobility rates. The delivery rate starts dropping with increasing mobility of the nodes. The performance of the network significantly reduces when AODV is under the cooperative black hole attack, and when the mobility of the nodes in the network increases. This behavior of the protocol is expected due to the following reason. With increasing mobility of the nodes the topology of the network changes faster, resulting in frequent route request generation. This gives an opportunity to a malicious node to send more false RREP packets. AODV under black hole attack exhibits a decrease in delivery ratio to 36%. The proposed algorithm increases the delivery ratio to 52%, resulting in an average improvement of 16%.

VIII. EVALUATION OF THE SIMULATION

In the first scenario where there is not a Black Hole AODV Node, connection between Node 5 and Node 4 is correctly flawed when we look at the animation of the simulation, using NAM. Figure 3 shows the data flow from Node 2 to Node 5.

When the Node 1 leaves the propagation range of the Node 2 while moving, the new connection is established via Node 3. The new connection path is shown in Figure 4

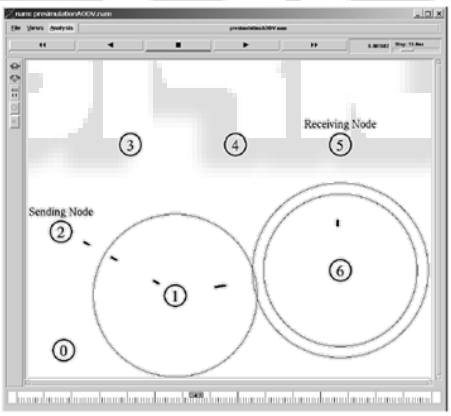

Fig. 3: Data flow between Node 2 and Node 5 via Node 1 and Node 6

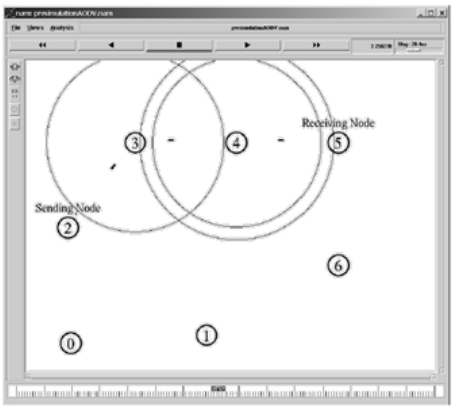

Fig. 4: Data flow between Node 2 and Node 5 via Node 3 and Node 4

IX. CONCLUSION

In this paper, 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. The proposed scheme has been evaluated by implementing it in the network simulator ns-1, and the results demonstrate the effectiveness of the mechanism. As a future scope of work, the proposed security mechanism may be extended so that it can defend against other attacks like resource consumption attack and packet dropping attack. Adapting the protocol for efficiently defending against gray hole attack- an attack where some nodes switch their states from black hole to honest intermittently and vice versa, is also an interesting future work.

REFERENCES

[1]. C. Perkins, E. Belding-Royer, and S. Das,(2003) "Ad-hoc on-demand distance vector (AODV) routing", Internet Draft, RFC 3561, July.

[2] Makki, Shamila, Pissinou, Nikki; Huang, Hui,(2004)," Solution to the black hole problem in mobile ad-hoc network, 5th World Wireless Congress", pp. 508-512

[3] Chen Hongsong, Ji Zhenzhou and Hu Mingzeng, (2006) "A Novel Security Agent Scheme for Aodv Routing Protocol Based on Thread State Transition". Asian Journal of Information Technology, 5 (1) : 54-60.

[4] P. Ning and K. Sun, "How to Misuse AODV: A Case Study of Insider Attacks Against Mobile Ad-Hoc Routing Protocols", Proc.of the 2003 IEEE Workshop on Information Assurance United States Military Academy, West Point, NY., June 2003.

[5] H. Deng, W. Li and D. P. Agrawal, "Routing Security inWireless Ad Hoc Networks". University of Cincinnati, IEEE Communication Magazine, October 2002.

[6] Yih-Chun, Adrian Perrig, David B. Johnson,(2002) "Ariadne: A secure On-Demand Routing Protocol for AdHocNetworks",parrow.ece.cmu.edu/~adrian/projects /secure routing/ariadne.pdf.

[7] S. Gupta, S. Kar, and S. Dharmaraja, "WHOP: Wormhole Attack Detection Protocol using Hound Packet", 7th IEEE Intl. Conf. on Innovation in IT (Innovation'11), 2011, pp. 226-231.

[8] M.A. Shurman, S.M. Yoo, and S. Park, "Black hole attack in mobile adhoc networks," 42nd ACM Southeast Regional Conf., 2004, pp. 11-14.

[9] Y.C Hu, and A. Perrig,"A survey of secure wireless adhoc routing", IEEE Security and Privacy, 2004, pp. 211-226.

[10] Lidong zhou, Zygmunt J. Haas(1999), "Securing Ad Hoc Networks", IEEE network, special issue on network security, Vol.13, no.6.

[11] F. Stajano and R. Anderson, "The Resurrecting Duckling: Security Issues for Ad-Hoc Wireless Networks", Security Protocols, 7th International Workshop Proceedings, Lecture Notes in Computer Science, 1999. University of Cambridge Computer Laboratory.

[12] Sukla Banerjee(2008) "Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks" Proceedings of the World Congress on Engineering and Computer Science San Francisco, USA

[13] S. Bansal and M. Baker,(2003) "OCEAN: Observation based cooperation enforcement in ad hoc networks", Technical Report, Stanford University.

