A Survey of Black hole and Worm hole Attack on Routing Protocol AODV in MANET

Sanket P. Gulhane
1st Year,M Tech,
WCEM, Nagpur.

Ram Kumar Solanki
HOD,CSE
WCEM, Nagpur

Nitesh A. Timande
1st Year,M Tech,
WCEM, Nagpur.

ABSTRACT

Ad hoc On-demand Distance Vector routing (AODV) is a widely adopted network routing protocol for Mobile Ad hoc Network (MANET). An Ad-hoc network is a self-organized network, without a central coordinator, and which frequently changes its topology. The design of AODV, however, paid little attention to security considerations, hence resulting in the vulnerability of such MANET to the black hole attack and Wormhole attacks. In this paper, we have study the performance of Mobile Ad-hoc Networks (MANET) under black hole and wormhole attack.

Key Words*:* AODV, RREQ, RREP, Blackhole, Wormhole

1. INTRODUCTION

1.1 AODV (Ad-hoc On-demand Distance Vector) and Black Hole In MANET using AODV, AODV's routing discovery process allows the middle node send RREP to the source node, in order to reply the RREQ received. When a malicious node in network receives RREQ, it can forge a RREP, claim it has a latest and shortest route to destination node. If this malicious RREP reaches the source node before the correct RREP, which are sent by the real destination node or an intermediate nodes who have a real route to destination node, the source node will mistake that it finds a route to reach the destination node, and sends application layer data to the destination node along the corresponding opposite direction route of the malicious RREP. The source node will think that the data has been sent to the destination node, in fact, these data has been discarded by the malicious node. It is equivalent that malicious node makes a black hole to devour the data, so that the malicious node carries so-called black hole attack [1] to MANET using AODV.

2. AODV (AD-HOC ON-DEMAND DISTANCE VECTOR) AND WORMHOLE

For sending messages to destination, it broadcasts RREQ messages to its immediate neighbors. These neighbors in turn rebroadcast them to their neighbors. This process continues unless the RREQ message reaches the destination. Upon receiving the first RREQ message from the source node, it sends a RREP to the source node following the same reverse path [2], [3]. All the intermediate nodes also set up forward route entries in their table. Upon detecting error in any link to a node, the neighboring nodes forward route error message to all its neighbors using the link. These again initiate a route discovery process to replace the broken link. The AODV routing protocol is vulnerable to wormhole attack [4]. Since the colluding nodes involved in wormhole attack uses a high speed channel to send messages, it is possible that the RREQ packet through them reaches the destination faster compared to usual path. According to this protocol, the destination discards all the later RREQ packets received, even though they are from authenticated node. The destination therefore chooses the false path through wormhole for RREP [5].

3. SECURITY CHALLENGES IN MANET

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 network. [6][7].

Challenges to MANET are discussed as follows:

Confidentiality: It ensures that classified information in the network is never disclosed to unauthorized entities. In MANETs, this is more difficult to achieve because intermediates nodes (that act as routers) receive the packets for other recipients, so they can easily eavesdrop the information being routed. Sensitive information, such as strategic military decisions or location information requires confidentiality. Leakage of such information to enemies could have devastating consequences.

Availability: Availability is the most basic requirement of any network. It assures that the services of the system are available at all times and are not denied to authorized users.

Integrity: It guarantees that a message being transferred between nodes is never altered or corrupted and the message must be genuine. Data can be altered either intentionally by malicious nodes in the network or accidentally because of benign failures, such as radio propagation impairment or through hardware glitches in the network.

Authenticity: Enables a node to safeguard the characteristics of the peer node it is communicating, without which an attacker would duplicate a node, thus attaining unauthorized admission to resource and sensitive information and snooping with operation of other nodes.

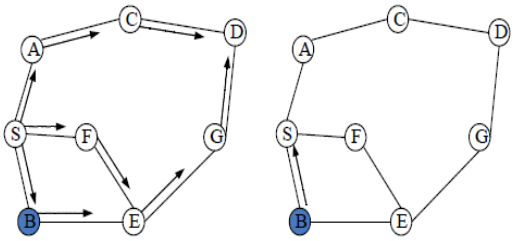
Non-repudiation: It ensures that the information originator cannot deny having sent the message. Non-repudiation is useful for detection and isolation of compromised nodes.

Access Control: To prevent unauthorized use of network services and system resources. Obviously, access control is tied to authentication attributes. In general, access control is the most commonly thought of service in both network communications and individual computer systems.

4. BLACK HOLE ATTACK

The black hole attack [6] is an active insider attack, it has two properties: first, the attacker consumes the intercepted packets without any forwarding. Second, the node exploits the mobile ad hoc routing protocol, to advertise itself as having a valid route to a destination node, even though the route is spurious, with the intention of intercepting packets. In an ad-hoc network that uses the AODV protocol, a black hole node pretends to have a fresh enough route to all destinations requested by all the nodes and absorbs the network traffic. When a source node broadcasts the RREQ message for any destination, the black hole node immediately responds with an RREP message that includes the highest sequence number and this message is perceived as if it is coming from the destination or from a node which has a fresh enough route to the destination. The source assumes that the destination is behind the black hole and discards the other RREP packets coming from other nodes. The source then starts to send out its data packets to the black hole trusting that these packets will reach the destination. Vulnerabilities of ad-hoc networks against black hole attacks are studied by different authors. Deng et.al. [8] addresses the black hole problem and proposes a solution based on modification of the AODV protocol. The authors propose to check the route through the next hop in the agreed upon path. This solution means that next hop information shall be added to the standard AODV header. Similar approach is adopted in [7] where the nodes are asked to send their neighborhood sets once the route is established. In [9] two solutions are proposed for detecting the black hole attack in ad-hoc networks. First solution involves sending a ping packet to the destination to check the established route. If the acknowledgement does not arrive from the destination, presence of a black hole is deduced. The other approach proposed is based on keeping track of sequence numbers as black holes usually temper with these sending packets with unusually high sequence numbers.

In MANET, a source node wants to send data packets to destination node, and initiates the routing discovery process. We assume node B to be a malicious node as shown in Fig.1. Using routing protocol, B claims that it has the routing to the destination node whenever it receives RREQ packets, and sends the response to source node at once. The destination node may also give a reply. If the reply from a normal destination node reaches the source node of the RREQ first, everything works well; but the reply from B could reach the source node first, if B is nearer to the source node. Moreover, B does not need to check its RT when sending a false message; its response is more likely to reach the source node firstly. This makes the source node thinks that the routing discovery process is completed, ignores all other reply messages, and begins to send data packets. The forged routing has been created. As a result, all the packets through B are simply consumed or lost. B could be said to form a black hole in the network, and we call this the black hole Attack as shown in Fig.1



(a)Network Floding of RREQ message (b) Propagation of RREP

Fig.1: Black Hole Attack

5. WORMHOLE ATTACK

In the wormhole attack, two colluding nodes are far apart are connected by a tunnel giving an illusion that they are neighbors. Each of these nodes receive route request and topology control messages from the network and send it to the other colluding node via tunnel which will then replay it into the network from there. By using this additional tunnel, these nodes are able to advertise that they have the shortest path through them. Once this link is established, the attackers may choose each other as multipoint relays (MPRs), which then lead to an exchange of some topology control (TC) messages and data packets through the wormhole tunnel. Since these MPRs forward flawed topology information, it results in spreading of incorrect topology information throughout the network [12]. On receiving this false information, other nodes may send their messages through them for fast delivery. Thus, it prevents honest intermediate nodes from establishing links between the source and the destination [10]. Sometimes, due to this, even a wormhole attacker may fall victim to its own success.

In [11] the wormhole attacks are classified as 1) In-band wormhole attack, which require a covert overlay over the existing wireless medium and 2) Out-of-band wormhole attack, which require a hardware channel to connect two colluding nodes. The in-band wormhole attacks are further divided in [11] as 1.1) Self-sufficient wormhole attack, where the attack is limited to the colluding nodes and 1.2) Extended wormhole attack, where the attack is extended beyond the colluding nodes. The colluding nodes attack some of its neighboring nodes and attract all the traffic received by its neighbor to pass through them.

In the second type of wormhole attacks [13], the intrusions are distinguished between a) hidden attack, where the network is unaware of the presence of malicious nodes and b) exposed attack, where the network is aware of the presence of nodes but cannot identify malicious nodes among them.

The features of wireless communication enable the malicious nodes to conduct wormhole attacks. As shown in Figure 2, when a legitimate node *u* in the network sends out a beacon, the malicious node *M*1 can use its antenna to eavesdrop the packet, and tunnel it through a dedicated long range channel to its colluder *M*2. When *M*2 retransmits the beacon, another legitimate node *v* will receive this packet and add *u* into its neighbor list. Fake neighbor connections are generated through wormholes. Later when data packets need to go through the wormhole, the malicious nodes may choose to discard them. Therefore, a wormhole fabricates a fake connection between *u* and *v* that is under the control of the attackers.

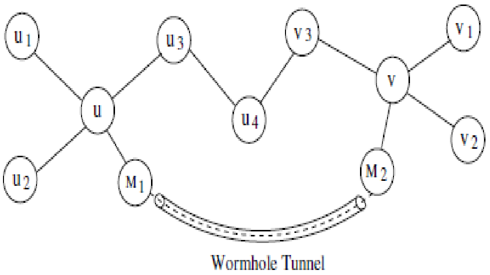


Fig. 2 : Worm Hole attack tunnel between pair of nodes u & v

6. CONCLUSION

Ad hoc networks relate to the issues of manageability, security, and availability of communication. Ad hoc routing protocols are subject to a variety of attacks that can allow attackers to influence a black hole attack or wormhole attack. In this paper, we have study the black hole and worm hole attack on routing protocol AODV in mobile ad hoc network.

REFERENCES

[1] Weerasinghe, H. and Huirong Fu. Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks: Simulation Implementation and Evaluation. In: Future generation communication and networking (fgcn 2007). Jeju: 2007. 362~367.

[2] R.H. Khokhar, Md. A.Ngadi, S. Manda. “A Review of Current Routing Attacks in Mobile Ad Hoc Networks”, *International Journal of Computer Science and Security*, 2 (3), pp. 18-29, 2008.

[3] Bounpadith Kannhavong, Hidehisa Nakayama, Yoshiaki Nemoto, Nei Kato, Abbas Jamalipour. “A Survey of Routing Attacks in Mobile Ad Hoc Networks”, *IEEE Wireless Communication*, 14 (5), pp. 85-91, 2007.

[4] Yih-Chun Hu, Adrian Perrig, David B. Johnson. “Packet leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks”. In *22nd Annual Joint Conference of the IEEE Computer and Communications Societies(INFOCOM)* , 3, pp. 1976-1986, 2003.

[5] R.H. Khokhar, Md. A.Ngadi, S. Manda. “A Review of Current Routing Attacks in Mobile Ad Hoc Networks”, *International Journal of Computer Science and Security*, 2 (3), pp. 18-29, 2008.

[6] Hongmei Deng, Wei Li, and Dharma P. Agarwal, “Routing Security in Wireless Ad Hoc Networks”, University of Cincinnati, IEEE Communications magazine, October 2002.

[7] Lidong zhou, Zygmunt J. Haas, “Securing Ad Hoc Networks”, IEEE network, special issue, November/December 1999.

[8] C.E. Perkins, S.R.Das, and E.Royer, “Ad-hoc Demand Distance vector (AODV)”, Mobile Ad Hoc Networking Working Group, *IETF Internet Draft*, http:/www.ietf.org/internet-draft/draft-ietf-manetaodv-05.txt March 2000.

[9] P.Ning and K.Sum, “How to misuse AODV: A case study of insider attack against mobile ad hoc routing protocol”, Tech Rep, TR- 2003-07, CS Department, NC University, April 2003.

[10] Kamanshis Biswas, Md. Liakat Ali. “Security Threats in Mobile Ad Hoc Network”. Thesis Paper submitted to the Department of Interaction and System Design, School of Engineering at Blekinge Institute of Technology, Thesis no: MCS-2007:07, 2007.

[11] V. Mahajan, M. Natu, A. Sethi. “Analysis of wormhole intrusion attacks in MANETS”. In *IEEE Military Communications Conference (MILCOM)*, pp. 1-7, 2008.

[12] F. Nait-Abdesselam, B. Bensaou, T. Taleb. “Detecting and Avoiding Wormhole Attacks in Wireless Ad hoc Networks”, *IEEE Communications Magazine*, 46 (4), pp. 127 - 133, 2008.

[13] H.S. Chiu and K. Lui. “DelPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks”. In *Proceedings of International Symposium on Wireless Pervasive Computing*, pp. 6-11, 2006.