Analysis of Blackhole attacks on AODV Routing Protocol in MANET

L. Raja[1], Dr. S. Santhosh Baboo[2]

[1]*Dept. of Computer Applications,*
Pachaiyappa's College, Chennai

[2]*Dept. of Computer Applications,*
D.G. Vaishnav College, Arumbakkam, Chennai

Abstract-A Mobile Adhoc Network is a collection of autonomous nodes or terminals which communicate with each other by forming a multihop radio network without the aid of any established infrastructure or centralized administration such as a base station. Routing is an important component in mobile ad hoc networks and it has several routing protocols, which are affected from different attacks. Ad hoc On demand Distance Vector (AODV) is one of the most suitable routing protocol for the MANETs and it is more vulnerable to black hole attack by the malicious nodes. In this paper we attempt to focus on analyzing and improving the security of one of the routing protocol (AODV). Our main focus will be on the effect of black hole attack in MANET

Keyword: MANET, Black hole, Routing protocol, AODV

1.INTRODUCTION

Wireless networks can be basically either infrastructure based networks or infrastructure less networks. The infrastructure based networks uses fixed base stations, which are responsible for coordinating communication between the mobile hosts. Infrastructureless wireless network is a network of mobile nodes without having any central controller**.** MANET(Mobile Ad-hoc Networks) does not rely on predefined infrastructure to keep the network connected, therefore it is also known as infrastructureless networks.

Mobile Ad-hoc Networks are a collection of two or more devices equipped with wireless communications and networking capability. These devices can communicate with other nodes that immediately within their radio range or one that is outside their radio range. For the later, the nodes should deploy an intermediate node to be the router to route the packet from the source toward the destination. The Wireless Ad-hoc Networks do not have gateway, every node can act as the gateway.

The Routing protocols can be divided into proactive, reactive protocols, depending on the routing topology. Proactive protocols are typically table-driven. In table driven routing protocols, the protocols consistent and up-to-date routing information to all nodes is maintained at each node. Examples of this type include Destination Sequence Distance Vector (DSDV). 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 "On-Demand" means that it builds routes between nodes only as desired by source nodes. Example of this type includes Dynamic Source Routing (DSR) and Ad Hoc On-Demand Distance Vector (AODV).

Section 2 describes about Routing Protocol. Section 3 describes function of AODV. Section 4 describes the black hole attack in AODV. Section 5 describes the challenges of MANET followed by conclusion in the section 6.

2. ROUTING PROTOCOL

A **Routing Protocol** is a protocol that specifies how routers communicate with each other, disseminating information that enables them to select routes between any two nodes on a computer network, the choice of the route being done by routing algorithms. Each router has *a priori* knowledge only of networks attached to it directly. A routing protocol shares this information first among immediate neighbors, and then throughout the network.

The primary goal of routing protocols in ad-hoc network is to establish optimal path (min hops) between source and destination with minimum overhead and minimum bandwidth consumption so that packets are delivered in a timely manner. There are three classes of routing Protocols which can be divided into **proactive, reactive and hybrid protocols**, depending on the routing topology. They are summarized as follows:

A . Table-Driven Routing Protocols:

Proactive protocols are typically table-driven. Based on the periodically exchanging of routing information between the different nodes, each node builds its own routing table which it can used to find a path to a destination. Every node maintains one or more tables representing the entire topology of the network. These tables are updated regularly in order to maintain up-to-date routing information from each node to every other node. To maintain the up-to-date routing information, topology information needs to be exchanged between the nodes on a regular basis, leading to relatively high overhead on the network. Examples of the protocols of this class are, Destination Sequenced Distance Vector routing protocol(DSDV), Wireless Routing Protocol (WRP), Cluster-Head Gateway Switch Routing protocol and Source Tree Adaptive Routing protocol(STAR).

B. On-Demand Routing Protocols:

Reactive are on-demand protocols. The nodes do not exchange any routing information. A source node obtains a path to a specific destination only when it needs to send some data to it. These protocols do not attempt to maintain correct routing information on all nodes at all times. Routing information is collected only when it is needed, and route determination depends on sending route queries throughout the network. Examples of the protocols of this class are, Dynamic Source Routing protocol (DSR), Ad Hoc On-Demand Distance-Vector Routing protocol (AODV), and Temporally Ordered Routing Protocol (TORA).

C . Hybrid Routing Protocols:

Hybrid protocols make use of both reactive and proactive approaches. Nodes are grouped into zones based on their geographical locations or distances from each other. Inside a single zone, routing is done using table-driven mechanisms while an on-demand routing is applied for routing beyond the zone boundaries. Both routing table size and update packet size are reduced by including in them only art of the network (instead of the whole); thus, control overhead is reduced. Example of this type includes Zone Routing Protocol (ZRP).

3. Function Of AODV

AODV is a reactive routing protocol that does not require maintenance of routes to destination nodes that are not in active communication. Instead, it allows mobile nodes to quickly obtain routes to new destination nodes. Every mobile node maintains a routing table that stores the next hop node information for a route to the destination node. When a source node wishes to route a packet to a destination node, it uses the specified route if a fresh enough route to the destination node is available in its routing table. If such a route is not available in its cache, the node initiates a route discovery process by broadcasting a *RouteRequest* (RREQ) message to its neighbors. On receiving a RREQ message, the intermediate nodes update their routing tables for a reverse route to the source node. All the receiving nodes that do not have a route to the destination node broadcast the RREQ packet to their neighbors. Intermediate nodes increment the hop count before forwarding the RREQ. A *RouteReply* (RREP) message is sent back to the source node when the RREQ query reaches either the destination node itself or any other intermediate node that has a current route to the destination. As the RREP propagates to the source node, the forward route to the destination is updated by the intermediate nodes receiving a RREP. The RREP message is a unicast message to the source node.

AODV uses sequence numbers to determine the freshness of routing information and to guarantee loop-free routes. In case of multiple routes, a nodeselects the route with the highest sequence number. If multiple routes have the same sequence number, then the node chooses the route with the shortest hop count. Timers are used to keep the route entries fresh. When a link break occurs, *RouteError* (RERR) packets are propagated along the reverse path to the source invalidating all broken entries in the routing table of the intermediate nodes. AODV also uses periodic *hello* messages to maintain the connectivity of neighboring nodes.

4. Blackhole Attacks

In networking, black holes refer to places in the network where incoming traffic is silently discarded (or "dropped"), without informing the source that the data did not reach its destination. These black hole nodes are invisible and can only be detected by monitoring the lost traffic. A Blackhole attack is one of the active DoS attacks possible in MANETs. In this attack, a malicious node sends a *false* RREP packet to a source node that initiated the route discovery, in order to pose itself as a destination node or an immediate neighbor to the actual destination node. In such a case, the source node would forward its entire data packets tothe malicious node, which originally was intended for the genuine destination. The malicious node, eventually may never forward any of the data packets to the genuine destination. As a result, therefore, the source and the destination nodes became unable to communicate with each other.

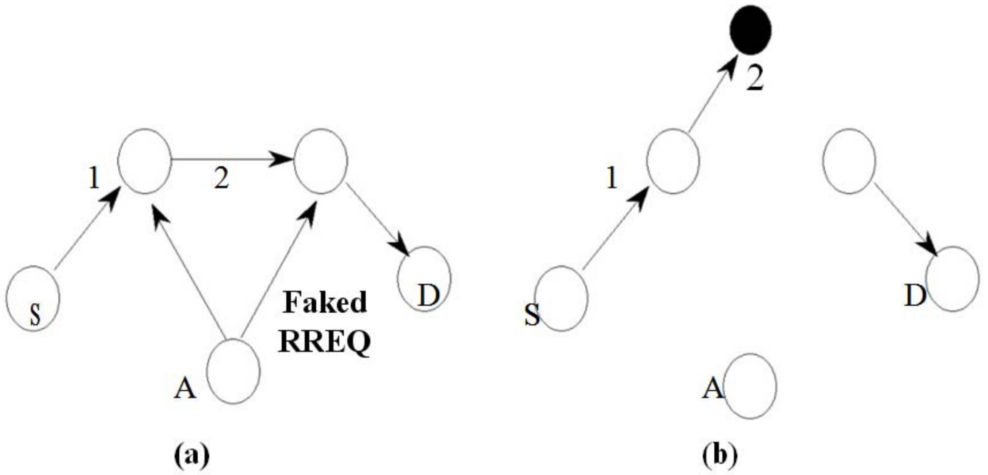
A black hole has two properties. First, the node exploits the ad hoc routing protocol, such as AODV, to advertise itself as having a valid route to a destination node, even though the route is spurious, with the intention of intercepting packets. Second, the node consumes the intercepted packets. Black hole attacks in AODV protocol routing level can be classified into two categories -- RREQ Blackhole attack and RREP Blackhole attack .

4.1 Black hole attack caused by RREQ

An attacker can send fake RREQ messages to form black hole attack. In RREQ Black hole attack, the attacker pretends to rebroadcast a RREQ message with a non-existent node address. Other nodes will update their route to pass by the non-existent node to the destination node. As a result, the normal route will be broken down. The attacker can generate Black hole attack by faked RREQ message as follows:

- Set the type field to RREQ (1);
- Set the originator IP address to the originating node's IP address;
- Set the destination IP address to the destination node's IP address;
- Set the source IP address (in the IP header) to a non-existent IP address (Black hole);
- Increase the source sequence number by at least one, or decrease the hop count to 1.

The attacker forms a Black hole attack between the source node and the destination node by faked RREQ message.



Black Hole is formed by fake RREQ

4.2 Black hole attack caused by RREP

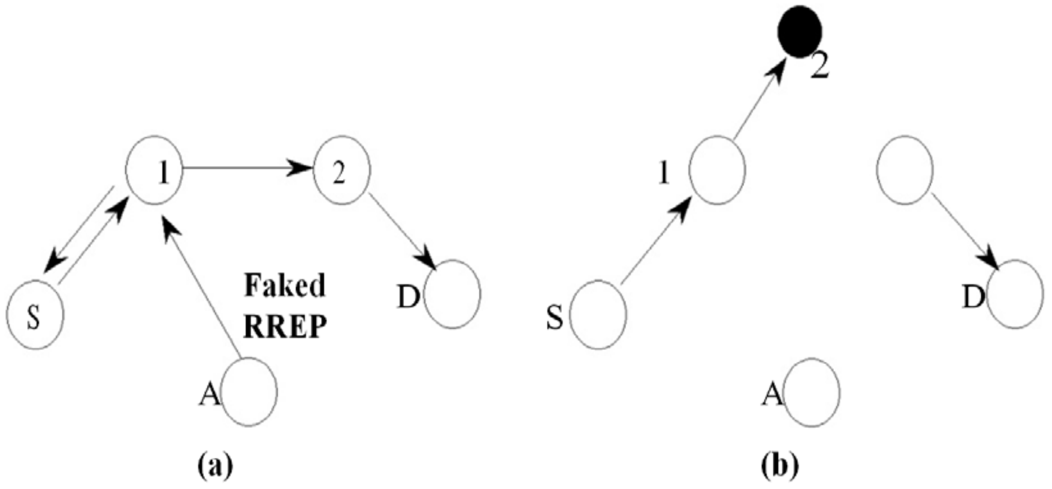
The attacker may generate a RREP message to form Black hole as follows:

- Set the type field to RREP (2);
- Set the hop count field to 1;
- Set the originator IP address as the originating node of the route and the destination IP address as the destination node of the route;
- Increase the destination sequence number by at least one;

Set the source IP address (in the IP header) to a non-existent IP address (Black hole).

The attacker unicasts the faked RREP message to the originating node. When originating node receives the faked RREP message, it will update its route to destination node through the non-existent node. Then RREP Black hole is formed

We use a reactive routing protocol known as Ad hoc On-demand Distance Vector (AODV) routing for analysis of the effect of the black hole attack when the destination sequence numbers are changed via simulation. Then, we select features in order to define the normal state from the characteristic of black hole attack. Finally, we present a new training method for high accuracy detection by updating the training data in every given time intervals and adaptively defining the normal state according to the changing network environment.



Black Hole is formed by fake RREP.

5. Challenges In Manet

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. Ad hoc networks have to cope with the same kinds of vulnerabilities as their wired counterparts, as well as with new vulnerabilities specific to the ad hoc context. The complexity and diversity of the field (different applications have different security constraints) led to a multitude of proposals that cannot be all surveyed in this article. Detailed analyses of ad hoc networking security issues and solutions can be found in. Below we summarize only the main directions of security in ad hoc networks. Active attacks involve actions such as the replication, modification and deletion of exchanged data. Certain active attacks can be easily performed against an ad hoc network.

These attacks can be grouped in: Impersonation, Denial of service, and Disclosure attack.

Secure routing : Secure routing protocols cope with malicious nodes that can disrupt the correct functioning of a routing protocol by modifying routing information, by fabricating false routing

information and by impersonating other nodes. Recent studies brought up also a new type of attack that goes under the name of wormhole attack mentioned earlier.

Cooperation enforcing : A basic requirement for keeping an ad hoc network operational is to enforce ad hoc nodes contribution to basic network functions such as packet forwarding and routing. Unlike networks using dedicated nodes to support basic network functions including packet forwarding, routing, and network management, in ad hoc networks those functions are carried out by all available nodes. This difference is at the core of some of the security problems that are specific to ad hoc networks. As opposed to dedicated nodes of a classical network, the nodes of an ad hoc network cannot be trusted for the correct execution of critical network functions. For example, routing is vulnerable in ad hoc networks because each device acts as a router. Forwarding mechanism is cooperative, as well. Communications between nodes, more than 1-hop away, are performed by exploiting intermediate relaying nodes.

A node that does not cooperate is called a misbehaving node. Routing–forwarding misbehaviors can be caused by nodes that are malicious or selfish. A malicious node does not cooperate because it wants to intentionally damage network functioning by dropping packets. On the other hand, a selfish node does not intend to directly damage other nodes, but is unwilling to spend battery life, CPU cycles, or available network bandwidth to forward packets not of direct interest to it, even though it expects others to forward packets on its behalf. Such a node uses the network but does not cooperate.

6. Conclusion

In the coming years, Mobile computing will keep flourishing, and an eventual seamless integration of MANET with other wireless networks, and the fixed Internet infrastructure, appears inevitable.

Ad hoc networking is at the center of the evolution towards the 4th generation wireless technology. Its intrinsic flexibility, ease of maintenance, lack of required infrastructure, auto-configuration, self-administration capabilities, and significant costs advantages make it a prime candidate for becoming the stalwart technology for personal pervasive communication. The opportunity and importance of ad hoc networks is being increasingly recognized by both the research and industry community. Moving forward towards fulfilling this opportunity, the successful addressing of open technical and economical issues will play a critical role in achieving the eventual success and potential of MANET technology.

In the next generation of wireless communication systems, there will be a need for the rapid deployment of independent mobile users. Since network scenarios cannot rely on centralized and organized connectivity and can be conceived as applications of Mobile Ad-hoc Networks. So, it solves different network problems.

References

1. Shiv Rama Murthi and Prasad “ Adhoc Wireless network” page no. 249-252, First edition, PHI, 2004
2. R. Ramanathan and J. Redi, “A Brief Overview of ad hoc networks: challenges and Directions,” IEEE Commun. Mag., vol. 40, no. 5, May. 2002.
3. HaoYang , Haiyun & Fan Ye “ Security in mobile adhoc networks : Challenges and solutions,”, Pg. 38-47, Vol 11, issue 1, Feb 2004
4. H. Deng, H. Li, and D. Agrawal, “Routing security in wireless ad hoc networks”, IEEE Communications Magazine, Vol. 40, No. 10, Oct 2002.
5. H.A. Esmaili, M.R. Khalili Shoja, Hossein gharaee, “Performance Analysis of AODV under Black Hole Attack through Use of OPNET Simulator”, World of Computer Science and Information Technology Journal (WCSIT), Vol. 1, No. 2, 49-52, 2011.
6. Al-Shurman, M., Yoo, S. and Park, S, "Black hole Attack in Mobile Ad Hoc Networks", ACM Southeast Regional Conference, pp. 96-97, 2004.
7. Nital Mistry, Devesh C Jinwala, Mukesh Zaveri, “Improving AODV Protocol against Blackhole Attacks”, proceedings of the International Multi Conference of Engineers and Computer Scientists 2010 Vol II, IMECS 2010.
8. Hoang Lan Nguyen, Uyen Trang Nguyen, A study of different types of attacks on multicast in mobile ad hoc networks in: Science Direct, Ad Hoc Networks 6 (2008) 32-46.
9. Bounpadith Kannhavong, Hidehisa Nakayama, Yoshiaki Nemoto, and Nei Kato, A Survey Of Routing Attacks In Mobile Ad Hoc Networks, IEEE Wireless Communications, 1536-1284/07.
10. Raja Mahmood, R.A.; Khan, A.I.; , "A survey on detecting black hole attack in AODV-based mobile ad hoc networks," High Capacity Optical Networks and Enabling Technologies, 2007. HONET 2007. International Symposium on , vol., no., pp.1-6, 18-20 Nov. 2007
11. Zh K. Lakshmi1, S.Manju Priya2 A.Jeevarathinam3 K.Rama4, K. Thilagam5, “Modified AODV Protocol against Blackhole Attacks in MANET”, International Journal of Engineering and Technology Vol.2 (6), 2010.

12. ao Min; Zhou Jiliu, "Cooperative Black Hole Attack Prevention for Mobile Ad Hoc Networks", Information Engineering and Electronic Commerce, 2009. IEEC '09. International Symposium on, vol., no., pp.26-30, 16-17 May 2009.
13. Hesiri Weerasinghe and Huirong Fu, Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks: Simulation Implementation and Evaluation. International Journal of Software Engineering and Its Applications, Vol. 2, No. 3, July 2008.
14. Sheenu Sharma, Roopam Gupta Simulation Study Of Blackhole Attack in the Mobile Ad hoc Networks. International Conference on Network Applications, Protocols and Services 2008, 21-22 November 2008, Executive Development Centre, Universiti Utara Malaysia
15. Hongmei Deng, Wei Li, and Dharma P. Agarwal, "Routing Security in Wireless Ad Hoc Networks", University of Cincinnati, IEEE Communications magazine, Vol.40, No.10, October 2002.
16. Mohammad Al-Shurman, Seong-Moo Yoon and Seungjin Park, “Black Hole Attack in Mobile Ad Hoc Networks”, ACM Southeast Regional Conference , Proceedings of the 42nd annual Southeast regional conference, 2004, pp 96-97
17. Bo Sun,Yong Guan,Jian Chen,Udo , “Detecting Black-hole Attack in Mobile Ad Hoc Network” , The institute of Electrical Engineers, Printed and published by IEEE, 2003.
18. Chen Hongsong, Ji Zhenzhou, Hu Mingzeng,“A novel security agent scheme for AODV routing protocol based on thread state transition”. Department of Computer Science and Technology Harbin Institute of Technology, 150001.
19. Charles E. Perkins and Elizabeth M. Royer. “Ad-Hoc On-Demand Distance Vector Routing.” In: *Proceedings of the Second IEEE Workshop on Mobile Computing Systems and Applications (WMCSA’99)*, pages 90–100, February 1999.
20. Satoshi Kurosawal, Hidehisa, Nakayama, Nei Kato, Abbas Jamalipour and Yoshiaki Nemoto. “Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method.” In: *International Journal of Network Security*, Vol. 5, No.3, pp.338–346, Nov. 2007.