International Journal of Cryptography and Security
ISSN: 2249-7013 & E-ISSN: 2249-7021, Volume 2, Issue 1, 2012, pp.-22-26.
Available online at http://www.bioinfo.in/contents.php?id=115

A REVIEW PAPER ON BLACK HOLE ATTACK AND COMPARISON OF DIFFERENT BLACK HOLE ATTACK TECHNIQUES

JATHE S.R. AND DAKHANE D.M.

Sipna's College of Engineering & Technology, Amravati, MS, India.
*Corresponding Author: Email- sonal_jathe@rediffmail.com, Sonaljathe1170@gmail.com

Received: February 21, 2012; Accepted: March 15, 2012

Abstract- communicating without a network infrastructure. Due to security vulnerabilities of the routing protocols, however, wireless ad hoc networks may be unprotected against attacks by the malicious nodes. One of the principal routing protocols used in Ad-Hoc networks is AODV (Ad-Hoc On demand Distance Vector) protocol. The security of the AODV protocol is compromised by a particular type of attack called 'Black Hole' attack [1]. In this attack a malicious node advertises itself as having the shortest path to the node whose packets it wants to intercept. In this paper we studied the details about blackhole attack, and comparison of different black hole attack techniques.
Keywords- Ad-hoc network, AODV, black hole, attack techniques.

Citation: Jathe S.R. and Dakhane D.M. (2012) A Review Paper on Black Hole Attack and Comparison of Different Black Hole Attack Techniques. International Journal of Cryptography and Security, ISSN: 2249-7013 & E-ISSN: 2249-7021, Volume 2, Issue 1, pp.-22-26.

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 [3] - [5]. 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 network. 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 network.

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.

Availability
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-repudiation
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.

Access Control
To prevent unauthorized use of network services and system resources, 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.

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 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. If it is not the destination, then it checks with its routing table to determine if it has got a route to the destination. If not, it relays the RREQ packet by broadcasting it to its neighbors. If its routing table does contain an entry to the destination, then the next step is the comparison of the 'Destination Sequence' number in its routing table to that present in the RREQ 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. The RREP packet gets relayed back to the source through the reverse route. The source node then updates its routing table and sends its packet through this route. During the operation, if any node identifies a link failure it sends a RERR (Route ERRor) packet to all other nodes that uses this link for their communication to other nodes. This is illustrated in Figs. 1a and b. Since AODV has no security mechanisms, malicious nodes can perform many attacks just by not behaving according to the AODV rules. A malicious node M can carry out many attacks against AODV. This paper provides routing security to the AODV routing protocol by eliminating the threat of 'BlackHole' attacks.

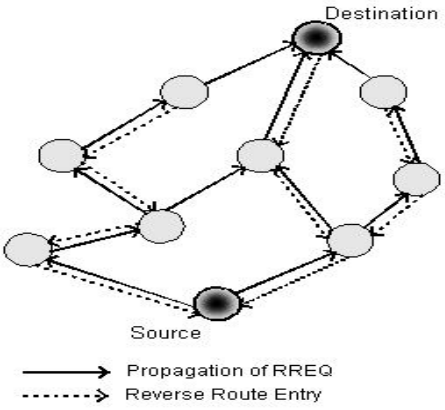

Fig. 1a- Propagation of RREQ.

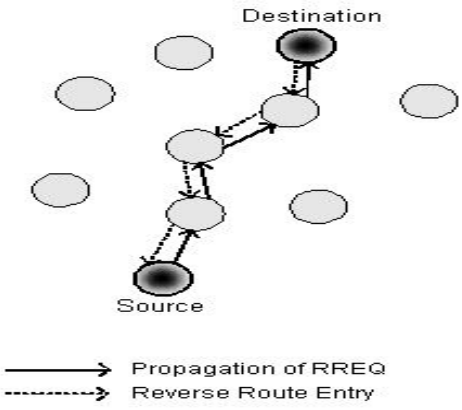

Fig. 1b- Propagation of RREP

Blackhole Attack and Classification

In Blackhole attack, all network traffics are redirected to a specific node which does not exist at all. Because traffics disappear into the special node as the matter disappears into Blackhole in universe. So the specific node is named as a Blackhole. A Blackhole has two properties. First, the node exploits the ad ho 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. Blackhole attacks in AODV protocol routing level can be classified into two categories: RREQ Blackhole attack and RREP Blackhole attack.

Blackhole attack caused by RREQ

An attacker can send fake RREQ messages to form Blackhole attack. In RREQ Blackhole 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 Blackhole 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 (Blackhole);
- Increase the source sequence number by at least one, or decrease the hop count to 1.

The attacker forms a Blackhole attack between the source node and the destination node by faked RREQ message as it is shown in Fig. 2.

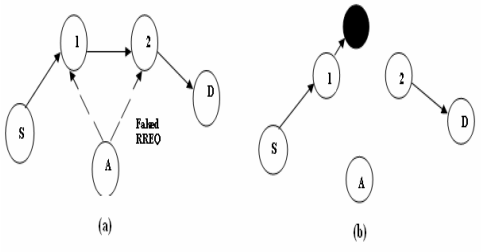

Fig. 2- Blackhole is Formed by Faked RREQ

Blackhole attack caused by RREP

The attacker may generate a RREP message to form Blackhole 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 (Blackhole).

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 Blackhole is formed as it is shown in Fig. 3.

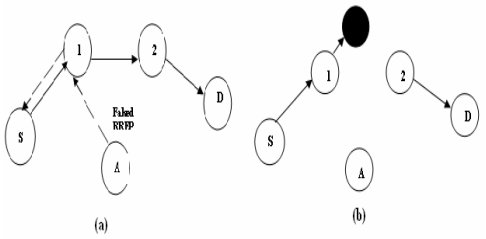

Fig. 3- Blackhole is Formed by Faked RREP.

A number of protocols were proposed to solve the black hole problem. It requires a source nod e to initiates a checking procedure to determine the reliability of any intermediate node claiming that it has a fresh enough route to the destination. Payal N. Raj, Prashant B. Swadas proposed DPRAODV (detection, prevention and reactive AODV) to prevent security of black hole by informing other nodes in the network. It uses normal AODV in which a node receives the Route reply (RREP) packet which first checks the value of sequence number in its routing table. The RREP is accepted if its sequence is higher than that in the routing table. It also check whether the sequence number is higher than the threshold value, if it is higher than threshold value than it is considered as the malicious node. The value of the threshold value is dynamically updated in the time interval. The threshold value is the average of the difference of destination sequence number in each time slot between the sequence number in the routing table and the RREP packet. The node that is detected as the anomaly is black listed and ALARM packet is sent so that the RREP packet from that malicious node is discarded. The routing table for that node is not updated nor is the packet forwarded to others. Their solution increases the average end to end delay and normalized routing overhead. Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon and Kendall Nygard proposed a method for identifying multiple black hole nodes. They are first to propose solution for cooperative black hole attack. They slightly modified AODV protocol by introducing data routing information table (DRI) and cross checking. Every entry of the node is maintained by the table. They rely on the reliable nodes to transfer the packets. The Route request (RREQ) is sent by source to every node and it send packet to the node from where it get the RREP. The intermediate node should send NHN and the DRI entry to the table. The source node (SN) check own DRI whether intermediate node (IN) node is reliable or not. The SN send the further request to next hop node (NHN) for IN. If SN uses IN to send A number of protocols were proposed to solve the black hole problem. It requires a source nod e to initiates a checking procedure to determine the reliability of any intermediate node claiming that it has a fresh enough route to the destination. Payal N. Raj, Prashant B. Swadas proposed DPRAODV (detection, prevention and reactive AODV) to prevent security of black hole by informing other nodes in the network. It uses normal AODV in which a node receives the Route reply (RREP) packet which first checks the value of sequence number in its routing table. The RREP is accepted if its sequence is higher than that in the routing table. It also check whether the sequence number is higher than the threshold value,

if it is higher than threshold value than it is considered as the malicious node. The value of the threshold value is dynamically updated in the time interval. The threshold value is the average of the difference of destination sequence number in each time slot between the sequence number in the routing table and the RREP packet. The node that is detected as the anomaly is black listed and ALARM packet is sent so that the RREP packet from that malicious node is discarded. The routing table for that node is not updated nor is the packet forwarded to others. Their solution increases the average end to end delay and normalized routing overhead.Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon and Kendall Nygard proposed a method for identifying multiple black hole nodes. They are first to propose solution for cooperative black hole attack. They slightly modified AODV protocol by introducing data routing information table (DRI) and cross checking. Every entry of the node is maintained by the table. They rely on the reliable nodes to transfer the packets. The Route request (RREQ) is sent by source to every node and it send packet to the node from where it get the RREP. The intermediate node should send NHN and the DRI entry to the table. The source node (SN) check own DRI whether intermediate node (IN) node is reliable or not. The SN send the further request to next hop node (NHN) for IN. If SN uses IN to send the reply packet and then it sends a Further- Request to the next hop to verify that it has a route to the intermediate node who sends back the Further reply message, and that it has a route to the destination node. Latha Tamilselvan, Dr. V Sankaranarayanan proposed a solution with the enhancement of the AODV protocol which avoids multiple black holes in the group. A technique is give to identify multiple black holes cooperating with each other and discover the safe route by avoiding the attacks. It was assumed in the solution that nodes are already authenticated and therefore can participate in the communication. It uses Fidelity table where every node that is participating is given a fidelity level that will provide reliability to that node. Any node having '0' value is considered as malicious node and is eliminated. The fidelity level of each RREP is checked and if two are having same level then one is selected having highest level. The responses are collected in the response table. A valid route is selected among the received based on the threshold value. After getting the acknowledgement the fidelity level of the node is updated proving it safe and reliable. The black hole node is accomplished by ALARM packets. Simulation result provides a better packet delivery ratio as the nodes are in motion. Hesiri Weerasinghe proposed the solution which discovers the secure route between source and destination by identifying and isolating cooperative black hole nodes. This solution adds on some changes in the solution proposed by the Ramaswamy to improve the accuracy. This algorithm uses a methodology to identify multiple black hole nodes working collaboratively as a group to initiate cooperative black hole attacks. This protocol is a slightly modified version of AODV protocol by introducing Data Routing Information (DRI) table and cross checking using Further Request (FREQ) and Further Reply (FREP). The simulation result shows that the AODV and the solution proposed by Deng et al. highly suffer from cooperative black hole in terms of throughput and packet losses. The performance of the solution is good and having better throughput and minimum packet loss percentage over other solutions. the reply packet and then it sends a Further- Request to the next hop to verify that it has a route to the intermediate node who sends back the Further reply message, and that it has a route to the destination node. Latha Tamilselvan, Dr. V Sankaranarayanan proposed a solution with the enhancement of the AODV protocol which avoids multiple black holes in the group. A technique is give to identify multiple black holes cooperating with each other and discover the safe route by avoiding the attacks. It was assumed in the solution that nodes are already authenticated and therefore can participate in the communication. It uses Fidelity table where every node that is participating is given a fidelity level that will provide reliability to that node. Any node having '0' value is considered as malicious node and is eliminated. The fidelity level of each RREP is checked and if two are having same level then one is selected having highest level. The responses are collected in the response table. A valid route is selected among the received based on the threshold value. After getting the acknowledgement the fidelity level of the node is updated proving it safe and reliable. The black hole node is accomplished by ALARM packets. Simulation result provides a better packet delivery ratio as the nodes are in motion. Hesiri Weerasinghe [13] proposed the solution which discovers the secure route between source and destination by identifying and isolating cooperative black hole nodes. This solution adds on some changes in the solution proposed by the Ramaswamy to improve the accuracy. This algorithm uses a methodology to identify multiple black hole nodes working collaboratively as a group to initiate cooperative black hole attacks. This protocol is a slightly modified version of AODV protocol by introducing Data Routing Information (DRI) table and cross checking using Further Request (FREQ) and Further Reply (FREP). The simulation result shows that the AODV and the solution proposed by Deng et al. highly suffer from cooperative black hole in terms of throughput and packet losses. The performance of the solution is good and having better throughput and minimum packet loss percentage over other solutions.

Comparison

Few proposals assumed:

Single Black Hole node in a network

Multiple Black Hole nodes in the ad hoc network Black hole attack detection proposals can be categorized as below:

1. Single non malicious nodes identifying a black hole node
2. Multiple non malicious nodes identifying a black hole node.

Conclusion

In this paper we studied the information about the network, concept of wired and wireless network, why use of wireless network., we also see the introduction about MANET and various characteristics and application of MANET . In this paper we have studied about the blackhole attack, wormhole and DOS attack, and analyzed different Intrusion Detection Systems in MANET .Intrusion-Detection Systems aim at detecting attacks against computer systems and networks, or, in general, against information systems. IDS can be viewed as a guard system that automatically detects malicious activities within a host or network. This paper also analyzes comparison between the different intrusion detection systems in the MANET.

References

[1] Lidong zhou, Haas Z.J. (1999) *IEEE network, special issue*.

[2] Karpijoki V. (2000) *HUT TML*.

[3] Deng Hongmei, Li Wei and Agrawal D.P. (2002) *IEEE Communications Magazine*, 70-75.
[4] Hongmei Deng, Wei Li, and Agrawal D.P. (2002) *IEEE Communications Magzine*, 40(10), 1704-1710.
[5] Papadimitratos P. and Haas Z. *Communication Networks and Distributed Systems Modeling and Simulation*.
[6] Hongmei Deng, Wei Li, and Agarwal D.P. (2002) *IEEE Communications magazine*.
[7] Hu Yihchun, Johnson D.B. and Perrig A. (2002) *SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks, WMCSA*.
[8] Semih Dokurer, Erten Y.M. and Acar C.E. (2007) *Performance analysis of ad-hoc networks under black hole attack*. 148-153.
[9] Qifeng Lu (2002) *Vulnerability of wireless Routing Protocols*.
[10] Tamilselvan L. and Sankaranarayanan V. (2007) *The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications,* 21-21.
[11] Chen Hongsong, Ji Zhenzhou and Hu Mingzeng (2006) *Asian Journal of Information Technology*, 5(1), 54-60.
[12] Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon and Kendall Nygard. *Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks*.
[13] Mohammad Al-Shurman, Seong-Moo Yoon and Seungjin Park. *Black Hole Attack in Mobile Ad Hoc Networks*.
[14] Chang Wu Yu, Tung-Kuang, Wu, Rei Heng, Cheng and Shun Chao Chang (2007) *A Distributed and Cooperative Black Hole Node Detection and Elimination Mechanism for Ad Hoc Networks*, PAKDD Workshops, 538-549.
[15] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour and Yoshiaki Nemoto (2007) *International Journal of Network Security*, 5(3), 338-346.
[16] Latha Tamilselvan and Sankaranarayanan V. (2007) *The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications*.

Table 1- Comparison of various black hole node detection scheme

Proposal name	Approach	Assumption	Philosophy
Dynamic learning system using DPRAODV	DPRAODV	Multiple black hole	Single non- black hole node detects
Cooperative black hole node detection using DRI and cross checking	AODV	Cooperative black hole	Single non- black hole node detects
Black hole node detection using two different solutions	AODV	Multiple black hole	Single as well as Multiple non black node detects
Distributed and cooperative mechanism	AODV	Distributed and cooperative	Cooperative detection
Detecting Black hole Attack on AODV-based Mobile Ad Hoc using dynamic anomaly detection	AODV	Multiple black hole	Single non black hole node detects
Single black hole node detection	AODV	Single black hole	Single non black hole node detects
Prevention of Black hole Attack using fidelity table	Enhancement on AODV	Multiple black hole	Multiple non- black hole node
Detection of black hole using DRI and Cross checking	Modified version of AODV	Multiple black hole	Multiple non-black hole nodes detects
Detection using neighborhood based method	AODV	Multiple black hole nodes	Multiple non black hole nodes detects
Detecting Black Hole Attacks in Tactical MANETs using Topology Graphs	TOGBAD approach	Single black hole	Single black hole node detects.