Prevention Of Black Hole Attacks In AODV-Based Manets Using Secure Route Discovery

Hansraj Bhakte
Department of Computer Engineering,
Sinhgad Institute of Technology Lonavala,
Savitribai Phule Pune University Maharashtra,
India
Email: rajhans.bhakte@gmail.com

Prof. Rahul Kulkarni
Department of Computer Engineering,
Sinhgad Institute of Technology Lonavala,
Savitribai Phule Pune University Maharashtre,
India
Email: kulkarnirahul1@gmail.com

***Abstract*—Without an establishment of infrastructure or a central network authority Mobile Ad-hoc Networks (MANETs) allow communication of mobile with each other over a network. Due to this condition, the MANETs have dynamic topologies, this case is because the nodes can easily join or leave the network at any time. MANETs are vulnerable to various types of malicious attacks, for this situation a security design perspective is necessary. Ad-hoc On-demand Distance Vector (AODV), which is one of the standard MANET protocols, can be attacked by malicious nodes. The one type of malicious attack is a black hole attack that can be easily employed against data routing in MANETs .In this case a black hole node replies to route requests rapidly from the shortest path and the highest destination sequence number. Without any active route and without any specified destination associated with it the black hole node drops all of the data packets that it receives. My mechanism that provides Secure Route Discovery for the AODV protocol in order to prevent black hole attacks. Security is a key feature in MANETs so by using cryptography technique for securing route discovery and data transmission.**

Keywords—MANETs; AODV; Black Hole Attack; Public key; Private key; Cryptographic Technique;

I. INTRODUCTION

A Mobile Ad-hoc Network (MANET) is a self-organized wireless network of mobile nodes without any fixed infrastructure. Nodes roam through the network, causing its topology to change rapidly and unpredictably over time. New nodes can join the network, whereas at the same time other nodes leave it or just fail to connect (temporarily) because they move to a region that is not in the cover range of the network. Nodes are typically wireless devices such as PDAs, laptops or cellular phones. From the very beginning, the use of MANETs has been appealing for both military and civilian applications, especially in the last decade because of development of wireless LAN technology. Due to their inherent characteristics of dynamic topology and lack of centralized management security, MANET is vulnerable to various kinds of attacks. These include passive eavesdropping, active interfering, impersonating, and denial-of-service. Black Hole attack is one of many possible attacks in AODV-based MANETs. In this attack, a malicious node sends a forged route reply packet to source node that initiates the route discovery in order to pretend to be the destination node.

The standard of AODV protocol, the source node compares the destination sequence number contained in RREP packets when a source node received multiple RREP, it judges the greatest one as the route contained in that RREP packet. In case the sequence numbers are equal, it selects the route with the smallest hop count. As the result, the data transmission will flow toward the malicious node by source node and it will be dropped. The ultimate goal of the security solutions for AODV protocol is to provide security services, such as authentication, confidentiality, integrity, anonymity and availability to mobile users. In order to achieve these goals, we will concentrate in addressing a security concern related to routing discovery and data exchange. A modified protocol will be proposed that accumulate the routing, authentication, generation and secure exchange of public key, private key and session key. They would be facilitating the users to establish parameters during the route discovery session and the parameters would subsequently be used to ensure confidentiality and integrity of data exchange.

The remaining of the paper is organized as follows. Section II introduces related work. Implementation detail and propose our mechanism is described in section III and section IV presents implementation result. Finally, the conclusion is depicted in section V.

II. RELATED WORK

The research in MANETs is a broad topic covering routing and security. Moreover, there are many research papers about the Black Hole attack defense strategies in MANETs. This section only gives a brief discussion of some researches that closely relate to the idea of this paper: MANET has many applications such as defense, disaster recovery and communication. This sector shows research on

MANETs. Marti et al [3] presented method to detect black hole attack. It enables neighbor nodes to detect malicious nodes by finding nodes that are discarding packets. Firstly it assigns default value to nodes present in network and observes the values its changes or not. It is monitoring the transmitting behavior of the nodes. The value for node changes after the period of time. If the value for a node is below a certain threshold, the node is added to the black hole list, but this method cannot handle collaborate attacks if the neighbor nodes occurs also a black hole attack. Lu et al [4] proposed SAODV black hole detection scheme but it does not recover full security to the route. Singh [5] implemented routing aspects in AODV that include password security each of the Routing nodes and routing table. Ramaswamy [6] identify cooperative black hole attack. They altered AODV protocol slightly by the Data Routing Information (DRI) table and cross checking table is maintain information of existing node, new node and leave node and it only uses reliable nodes for transmission of data packet from source to destination. Agrawal [7] proposed that routing security in wireless network. It asks every intermediate node to return next of hope information a route to a destination has been determined. The source node does not transmit data to any other node immediately source node waits for route reply and the next hope information and then send further regents to determining the path for source to destination. Lu et al proposed a Black Hole detection scheme (so called SAODV) for MANETs that addressed some security weaknesses of AODV and withstand the Black Hole attack. An enhanced version of this SAODV protocol was provided by Deswal and Singh5, where a password security was used for each routing node and routing tables were updated in a timeliness fashion. Secure Routing with AODV (SRAODV), a series of security mechanism, including Key Exchange, Secure Routing, Data Protection, are proposed by A. Pirzada and C. McDonald. Considering about secure routing mechanism, the author recommended peer-to-peer symmetric encryption to all routing information in RREQ, RREP and RRER, using a group session key negotiated by neighbor nodes. However, this design requires each node to maintain a table along with associated group members and session keys. It would become less efficient as the number of nodes in ad hoc network increase. And moreover, a compromised node could still juggle hop count or destination sequence number to interrupt the normal routing procedure.

The most of research papers above are discussed about secure routing protocol on MANET to avoid some attacks based on the AODV protocol and other protocols. However, our solution in this paper provides the security on routing packets by using the cryptographic technique in one step for preventing Black Hole attacks on AODV-based MANET.

III. IMPLEMENTATION DETAILS

A. Problem Statement

1. AODV Routing Protocol

Ah-hoc On-demand Distance Vector (AODV) is used to find a route between source and destination as needed and there are three significant types of messages used in this routing protocol such as route request (RREQ), route reply (RREP) and route error (RRER). The information fields of these messages, such as source IP address, destination IP address, source and destination sequence number, hop count and etc. Each node uses this information which contains in a routing table for routing to a specific destination.

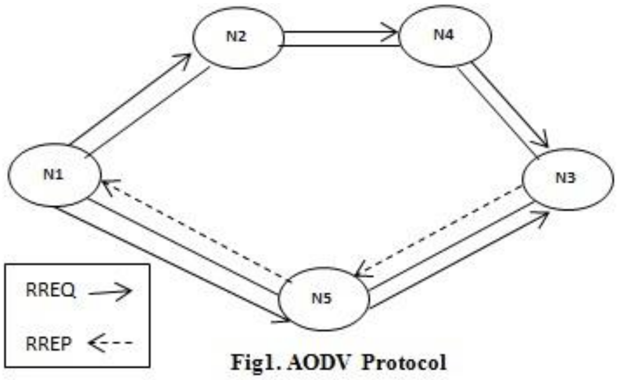

Fig1. AODV Protocol

When a source node wants to communicate with a destination and there is no any route between them in the routing table, at first step the source node broadcasts RREQ as shown in the Fig1. The RREQ is received by intermediate nodes that they are in the transmission range of the sender. These nodes broadcast and forward this RREQ packet until it is received by destination or an intermediate node that has fresh enough route to the destination. Then the destination sends RREP unicast toward the source as shown in the Fig. 1. Hence, a route among the source and destination is established. A fresh enough route is a valid route entry that its destination sequence number is at least as great as a destination sequence number in RREQ packet. The source sequence number is used to determine freshness about route to the source. In addition, the destination sequence number is used to determine freshness of a route to the destination. When destination sequence number and hop count, it creates or updates a forward route entry in its routing table for that destination.

In Route Maintenance procedure, nodes keep an entry for each active route in their routing table and periodically broadcast Hello message to its neighbors in order to detect a possible link failure. If a node detects a link failure, it knows that all active routes via this link fail. So a Route Error message (RERR) is sent to announce all relative source nodes. The source nodes then will decide whether to refresh the route or not.

2. Black Hole Attack

Routing protocols are exposed to a variety of attacks. Black Hole attack is one kind of Denial of Service attack in which a malicious node makes use of the vulnerabilities of the route discovery packets of the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. This attack aims at modifying the routing protocol so that traffic flows through a specific node controlled by the attacker. During the Route Discovery process, the source node sends RREQ packets to the intermediate nodes to find fresh path to the intended destination. The malicious node responds immediately to the source node without following the routing protocol rules. The source node assumes that the route discovery process is complete, ignores other RREP messages from other nodes and selects the path through the malicious node to route the data packets. The malicious node does this by assigning a high sequence number to the reply packet. The attacker now drops the received messages instead of relaying them as the protocol requires.

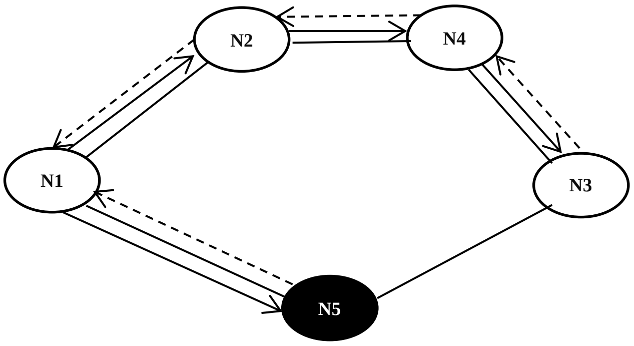

Fig2. Black Hole Attack

Therefore, in order to fake AODV using Black Hole attacks, the attacker uses two methods:

1. Send RREP packet towards the source node with highest enough sequence number.
2. Send RREP packet to source node with small enough hop count number

In most cases, the Black Hole attack gains the route if the routing protocol does not protect itself. Black Hole attack does not follow the routing protocol rules by not spending a long time to reply. Hence, Black Hole attack produces quicker reply of RREP than the real destination node or other node in the network by coping source and destination address from RREQ packet, decreasing hop count and increasing highest sequence number.

B. Existing System

MANETs to find secure path between source and destination. This solution is a new protocol that involves modifications of the standard MANET AODV protocol. It is called Secure Route Discovery for AODV-based MANET (SRD-AODV).

A. Threshold Area

The minimum (MIN) and maximum (MAX) values for the sequence numbers (SEQ) are based on signed 32-bit arithmetic. Therefore

$MIN_{SEQ} = 0$ Initial node

$MAX_{SEQ} = 4294967$ 2^{32} node

Where MIN_{SEQ} represents the minimum sequence number and MAX_{SEQ} represents the maximum sequence number. In the proposed mechanism, we define three thresholds for classifying real nodes and malicious nodes in three different types of environments.

Small environment (TH_S) includes locations that contain a small number of mobile nodes, such as locations in the country side or locations that are far from the public gathering places. For this type of location, the threshold is defined as follows:

$$TH_S = (MAX_{SEQ} \text{ X } 94)/100$$

Medium environment (TH_M) includes locations that have a medium amount of mobile nodes, public gathering place in provinces. For this type of location, the threshold is defined as follows:

$$TH_M = (MAX_{SEQ} \text{X } 96)/100$$

Large environment (TH_L) includes locations that consist of many mobile nodes, such as a capital city or a public gathering place in a city. For this type of location, the threshold is defined as follows:

$$TH_L= (MAX_{SEQ} \text{ X } 98)/100$$

After defining the thresholds for each environment, we add two extra functions to the mobile nodes. First, the source nodes use the defined thresholds to verify the multiple RREP messages from their neighbor nodes. Second, the destination nodes use the defined thresholds to verify the RREQ messages from the source nodes. Additional function process on a source node illustrates the process flow for the additional function on a source node. If there is a black hole attack node present on the network, then a source node will receive at least two RREP messages, one from its neighbor nodes and another one from the black hole node. Therefore, the source node must determine which of the messages is an authentic RREP message from the destination node (active route or secure route) and which one is a fake RREP message from the black hole node.

C. Propose System

AODV protocol would be the basis of our propose work. Route Request (RREQ), Route Reply (RREP) and Route Error (RRER) are the message types defined by AODV. In addition to our previous work of securing route discovery in ADOV protocol, we propose a new mechanism for two ways of securing not only route discovery, but also data transmission by using a cryptography technique. This protocol is a new protocol based on the traditional AODV protocol. The designed protocol encompasses the routing mechanism and exchange security parameters in a single step. This would be considered as a major change from the current security techniques used in AODV and conventional security protocols affiliated with the network and transport layer.

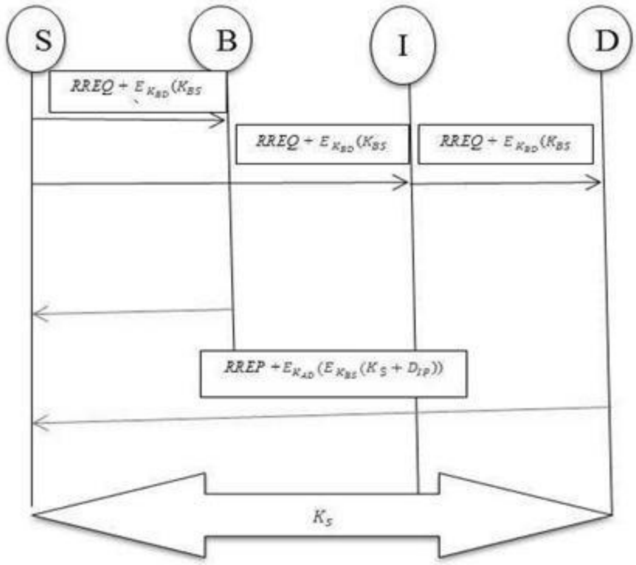
S
B
I
D
RREQ + $E_{K_{BD}}(K_{BS}$
RREQ + $E_{K_{BD}}(K_{BS}$
RREQ + $E_{K_{BD}}(K_{BS}$
RREP +$E_{K_{AD}}(E_{K_{BS}}(K_S + D_{IP}))$
K_S

Fig3. System Architecture

The proposed modifications on the existing AODV protocol have been a successful integration of routing and exchange of data security key which include:

- Source public and private key by source node.
- Destination public and private key by destination node.
- Session key by destination node

The added parameters in the RREQ message include:

- Source public key is encrypted by destination public key

On the reception of RREQ, the destination responds with RREP having additional parameters including:

- Session key and destination IP address are encrypted by source public key and continue to encrypt by destination private key

Certificates can be issued to all participating nodes in relation to their MAC address or IP address, personal credentials or on any agreed pattern. The mechanism of issuing certificates by CA is considered out of the scope of this paper. It is assumed that trust relationship exists only between a source and destination node. Intermediate nodes participating in routing are out of trust relationship.

Our proposed work includes the following ideas:

- The Certification Authority (CA) will be used to request destination public key by only source node.
- The concept of asymmetric cryptography (public key and private key cryptography) will be used for the secure route discovery and exchange of session key.

proposed options, source node (S), destination node (D), Black Hole node (B), Intermediate node (I), Source IP address (S_{IP}) , Destination IP address (D_{IP}) , Public key of x (K_{BX}) , Private key of x ($K_{AX})$, where x is either source or destination. (E_K) encryption using key K, (D_K) decryption using key K, Session key (K_S) , Routing Request (RREQ) and Routing Reply (RREP).

D. Security Mechanism

The secure route discovery and data transmission process of MANET on AODV protocol as we mention above, the trust relationship already existed between source node and destination node. Therefore, destination node's public key is known by CA. In our mechanism, we assume that source node already got the destination public key (K_{BD}) from CA. The originating node or source node generates a Route Request (RREQ), and attaches its public key (K_{BS}) decrypted by destination public key (K_{BD}) from CA. his packet is broadcasted by source node to all neighbor nodes or intermediate nodes for route discovery of destination. On the network, both intermediate nodes and Black Hole nodes receive the same this packet.

1. The process of intermediate nodes:

On reception of the *RREQ* + $E_{K_{BD}}(K_{\mathrm{BS}})$ packet, the intermediate node initials checking destination IP address in RREQ by verifying this IP address in its routing table. The *RREQ*+$E_{K_{BD}}(K_{BS})$ packet will be forwarded with increasing hop count plus one in RREQ if this node is not a destination. Typically, the *RREQ* +$E_{K_{BD}}(K_{\mathrm{BS}}$)packet will be forwarded by the intermediate nodes until it reaches the destination without decrypts source public key $E_{K_{BD}}(K_{BS}$).

2. *The process of Black Hole nodes:*

The Black Hole attack manner does not follow the routing rule and spends a lot of time to reply the Route Reply (RREP) packet. When it receives *RREQ* + $E_{K_{BD}}(K_{\mathrm{BS}})$ packet, it suddenly generates RREP to the source node by copying destination and source IP address from RREQ, setting hop count to lowest as 1 and increasing destination sequence number to maximum of sequence number as 4294967295 [2]. The Black Hole attack cannot get the source public key because it doesn't have the destination private key (K_{AD}) to decrypt the destination public keys

(K_{BD}). The fake RREP packet generated by Black Hole node suddenly is replied to the source node.

3. *The process of destination nodes:*

After checking its IP address in RREQ, the destination node gets the source public key (K_{BS}) by using its private key (K_{AD}) to decrypt $E_{K_{BD}}\,(K_{BS})$.

$$D_{K_{AD}}\left(E_{K_{BD}}\,(K_{BS})\right) \qquad (2)$$

A session key $(K_S)$and a Route Reply (RREP) are generated by destination node and destination node uses the source public key (K_{BS}) to encrypt the session key $(K_S)$and destination IP address(D_{IP}).

$$E_{K_{BS}}(K_S + D_{IP}) \qquad (3)$$

The destination node then encrypts $E_{K_{BS}}(K_S + D_{IP})$ with its private key (K_{AD}) for authentication.

$$E_{K_{AD}}\left(E_{K_{BS}}\,(K_S + D_{IP})\right) \qquad (4)$$

Finally, the Route Reply (RREP) attached with $E_{K_{AD}}(E_{K_{BS}}\,(K_S + D_{IP}))$ is unicasted toward to the source node along the route by destination node

$$RREP+E_{K_{AD}}\left(E_{K_{BS}}\,(K_S + D_{IP})\right) \qquad (5)$$

4. *The process of source node when receives packet:*

The originating node or source node receives two packets from its neighbors. The source node will consider whether which one is a secure packet by following using the algorithms:

(a) The packet from destination node

- The source node obtains the source and destination IP address from Route Reply (RREP)
- The source node confirms the authenticity of destination node by using the destination public key (K_{BD}) to decrypt destination private key (K_{AD}).

$$D_{K_{BD}}\left(E_{K_{AD}}\left(E_{K_{BS}}(K_S + D_{IP})\right)\right) \qquad (6)$$

- The source node decrypts $E_{K_{BS}}\,(K_S + D_{IP})$ obtained from the previous algorithm $D_{K_{BD}}(E_{K_{AD}}\,(E_{K_{BS}}(K_S + D_{IP})))$ by using the source private key (K_{AS}) for session key (K_S) and destination IP address (D_{IP}).

$$D_{K_{AS}}(E_{K_{BS}}\,(K_S + D_{IP})) \qquad (7)$$

(b) The packet from Black Hole attack node

- The source node obtains the source and destination IP address from Route Reply (RREP)
- No encryption packet

The source node will consider the self-route using the following criteria :

- Verify whether the destination IP addresses both from RREP packet and its encrypted attachment $(E_{K_{AS}}(E_{K_{BS}}\,(K_S + D_{IP}))$ are equal.
- High destination sequence number (D_{SEQ})
- Low hop count

Otherwise, the other received packet will be discarded by source node. The source node uses the session key (K_S) generated by destination node for secure data transmission between the source node and destination node.

E. Experimental Setup:

In this part we can estimate our proposed work. Initially we calculate right protection method and have to take care of whether it retains original distance graph of the original Dataset or not. We then compare our approach with the existing system approach. We can check our approaches on different datasets. Usually, most of the experiments were conducted on 2.16GHz Intel CPU with 3GB RAM. And also, the scalability checking experiments have been conducted on a 3.40GHz Intel CPU with 16GB RAM. We are using Java framework (version jdk 6) on Windows platform. The Net beans (version 6.9) are used as a development tool.

IV. EXPERIMENTAL RESULTS

We consider node scenarios to analyze the results based on the performance metrics as below:

- Packet delivery ratio: This represents the ratio between the number of packets originated by the “application layer” CBR sources and the number of packets received by the CBR sink at the final destination.
- Network Throughput: This represents the average rate of successful message delivery over a communication channel and can be measured as bits per second (bps).

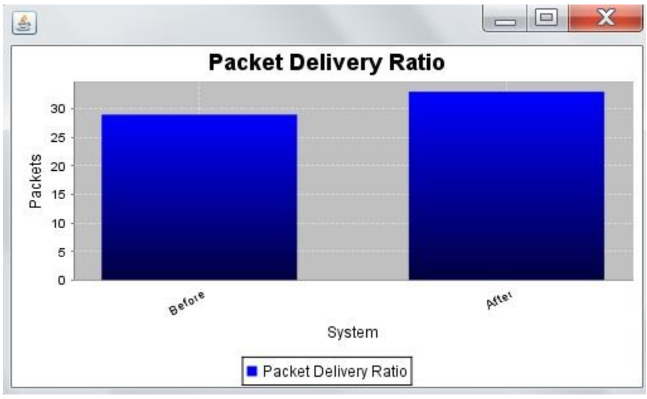

Fig4. Packet Delivery Ratio

Performance metric we used in the analysis of our mechanism is the packet delivery ratio. Fig. 4 depicts the effect of the packet delivery ratio on the node mobility in the presence of the Black Hole attack in the network, where node mobility is the rate at which the nodes are moving in the network. It can be observed that AODV suffers heavy loss in packets in the presence of a Black Hole node and consistent packet delivery ratio in the presence of a Black Hole node. This may be justified by the fact that the standard AODV does not have any built-in security mechanism.

V. CONCLUSION:

Security issues have been overlooked while designing routing protocols for ad-hoc networks. According to standard AODV protocol, it is susceptible to many malicious attacks including Black Hole Attacks. The proposed protocol, Secure Route Discovery and Data Transmission from Black Hole Attacks on AODV-based Mobile Ad-hoc Networks is the mechanism that uses the cryptographic technique (using public, private and session key) for securing route discovery and data transmission. In our proposed mechanism provides high ability to prevent Black Hole attack in the network thus the packet loss will be reduced. In future work, we will improve the credibility of AODV on route discovery and data transmission.

References:

[1] Seryvuth Tan, Keecheon Kim, “Secure Route Discovery for Preventing Black Hole Attacks on AODV-based MANETs” IEEE International Conference on Embedded and Ubiquitous Computing, 2013.

[2]. E. Çayırcı, C.Rong, “Security in Wireless Ad Hoc and Sensor Networks,” vol. I. New York, Wiley, pp. 10, 2009.

[3]. S. Marti, T. J. Giuli, K. Lai, and M. Baker, “Mitigating routing misbehavior in mobile ad hoc networks,” in Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (MobiCom), pp. 255-265, 2000.

[4]. S. Lu, L. Li, K-Y Lam, L. Jia, “SAODV: A MANET Routing Protocol that can Withstand BlackHole Attack”, Proc. of Intl. Conference on Computational Intelligence and Security (CIS '09), Dec. 11-14, Beijing, China, pp. 421-425, 2009.

[5]. S. Deswal and S. Singh, “Implementation of Routing Security Aspects in AODV”, Intl. Journal of Computer Theory and Engineering, Vol. 2, No. 1 Feb., 2010.

[6]. Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon, and Kendall Nygard, “Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks,” 2003 International Conference on Wireless Networks (ICWN 03), Las Vegas, Nevada, USA.

[7]. H. Deng, W. Li, and D. P. Agrawal, “Routing security in wireless ad hoc networks”, IEEE Communications Magazine, 40(10), pp. 70-75. doi:10.1109/MCOM.2002.1039859, 2002.

[8]. C. E. Perkins, E. M. B. Royer and S. R. Das, “Ad-hoc On-Demand Distance Vector (AODV) Routing,” Mobile Ad-hoc Networking Working Group, Internet Draft, draft-ietf-manetaodv- 00.txt, Feb. 2003.

[9]. M. Al-Shurman, S-M. Yoo, and S. Park, “BlackHole Attack in Mobile Ad Hoc Networks,” ACM Southeast Regional Conf. 2004.

[10]. Issariyakul, T., Hossain, E.: “Introduction to network simulation ns2