Volume : 4 | Issue : 6 | Special Issue June 2015 • ISSN No 2277 - 8179

Security Enhancement of AODV Routing Protocol in MANET- A Survey

Engineering

KEYWORDS:PSR, Mobile adhoc network, Adhoc On demand Distance Vector, Security mechanisms, Routing.

Ummu Habeeba K. Student, Department of Computer Science and Engineering , MES College of Engineering, Kerala, India.

Shiju Kumar P.S. Asst. Professor, Department of Computer Science and Engineering, MES College of Engineering, Kerala, India.

ABSTRACT

MANET is a highly challenged network area due to its special characteristics such as decentralization, dynamic topology and neighbor based routing. The primary challenges faced by MANET are routing and secure transmission of data over the network. In high mobility and heavy traffic communication AODV (Adhoc On demand Distance Vector) can run well, which is a well-known reactive routing protocol. In this paper a survey on different enhancements in the field of security used by AODV routing protocol in MANET are presented.

I. INTRODUCTION

Networks are used in various fields for various kinds of applications. The popularity of network has motivated the development of mobile ad-hoc networks. Mobile mesh network, which is a synonym for mobile ad-hoc network and is a kind of decentralized wireless system and is also a growing dynamic network [1]. Due to the collaborative and open systems nature of MANET and by limited availability of assets, it has various kinds of security concern problems. Immediate network formation and trusted route establishment for the communication are required for several application areas such as battle field, emergency and disaster environments. Mesh network is the suitable network for such type of application areas. All the existing MANET protocols are simply trust their neighbors and make a route through the neighbors. By intruders and internal attackers or malicious nodes this neighbor based routing is disturbed [2].

Routing protocols [3] in MANET are normally classified into proactive and reactive protocol. An example of reactive routing protocol for ad hoc network available today is Ad hoc On-demand Distance Vector (AODV) protocol. For the detection of the existence of malicious attack such as the Black hole attack, there was no protection mechanisms built in AODV. One of the most common attack is the black hole attack for AODV routing protocol whereby malicious node will pretend to have the shortest and freshest route to destination by constructing false sequence number in routing control messages.

The AD HOC ON-DEMAND DISTANCE VECTOR

The AODV [4] is categorized as a dynamic reactive routing protocol. In such a routing protocol, route will be established based on demand (upon request by source node). The process to discover routing path to destination node is illustrated in Figure 1. In AODV route discovery, there are two important control messages namely Route Request (RREQ) and Route Reply (RREP). Both control messages carry an important attribute called destination sequence number and has an incremental value to determine freshness of a particular route.

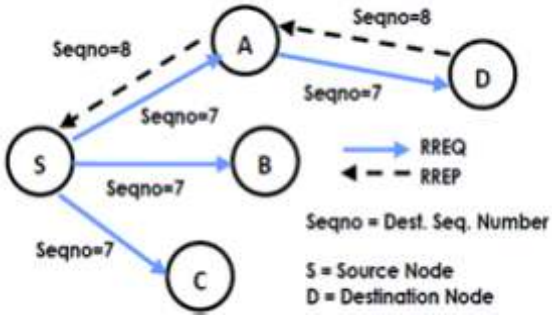

Figure 1. AODV route discovery process

In Figure 1, source node S will broadcast control packets, RREQ message to its neighbors A, B and C in order to find the best possible path to destination node D. Upon receiving RREQ message, the received node either:

a) reply to the source node with a RREP message if received node is the destination node or an intermediate node with a "fresh enough route information" to the destination, or

b) update the routing table entry which will be used in the reverse path and rebroadcasting of RREQ message until destination node or intermediate node with a "fresh enough route" is reached .

An intermediate node is believed to have a "fresh enough routes" to destination node if destination sequence number in its routing table is greater than or equal (with less hop count) to destination sequence number in RREQ message.

Upon receiving RREQ message from node A, destination node D will reply with RREP message to node S by forwarding the message to node A. The route entry for destination D will be updated by this function if either one of this condition is met.

a) The routing table containing destination sequence number is less than destination sequence in RREP message or

b) The destination sequence number in routing table is equal with destination sequence number in RREP message but with hop count is less than the one in routing table.

In case where node S receives multiple RREP messages, this function will select the RREP message with the highest destination sequence number value.

Many possible attacks in MANET can compromise the security of AODV in mobile ad hoc network.

Internal attacks: The attacker acts as any one of the nodes in this type of attack and gains direct access to the network either by impersonation or by compromising a proper given node and by using it to do its malicious activities.

External attacks: The attacker attacks from outside the network in this type, due to congestion in the network traffic by propagating non meaningful messages throughout the network, thereby disturb the entire communication of the network.

A. Impersonation

This type of attack is fall in the category of the most severe attacks. The attacker can act as an innocent node and join the network in this type of attack. Similar way, when several this type of nodes join the

network, they gain the full control of the network and conduct malicious behavior. They spread fake routing information and they also gain access to confidential information. A network is vulnerable to such attacks if it does not employ a proper authentication mechanism.

B. Denial of Service

This type of attack is first making sure that a specific node is not available for service. So the entire service of the network might be disturbed due to this attack.

C. Eavesdropping

The main goal of the attacker is to get some private information in this type of attack, while it is being transferred from one node to the other. This attack is very much complex to find out and the secret information like private and public key, password, etc. of the nodes can get compromised due to this attack.

D. Black hole attack

A black hole is created with the opponent at the main center. The opponent traps the traffic of the network close to a compromised in this type of attack. Basically the attacker offers an attractive path to the neighboring nodes. This attack can also be paired with other attacks like packets dropping, denial of service, replay of knowledge, selective forwarding.

E. Wormhole attack

Here the opponent connects two distant parts of the network and convey messages received in different part of the network to the other. A lower latency link is used to pass the messages in this type of network.

F. Sybil attack

In this type of an attack, a particular node in the network tries to have several different fake identities. Thus this way helps the malicious node to gain more and more specific information about the network. The validness of fault tolerant schemes like multipath topology in routing, distributed storage, maintenance etc. has a great decrease.

II. COMPARATIVE STUDY

A. ERDA

The ERDA (Enhanced Route Discovery AODV) [4] is designed to reduce the route discovery overhead. The solution provides minimum modification to existing AODV algorithm. There are three new elements introduced to improve the existing AODV in recvReply() function namely are 1) the rrep_table to store incoming RREP packet, 2) mali_list to keep the detected malicious nodes identity and 3) the rt_upd, parameter to control the routing table update. Generally, the method is divided into two parts; securing routing table update, detecting and isolating malicious node.

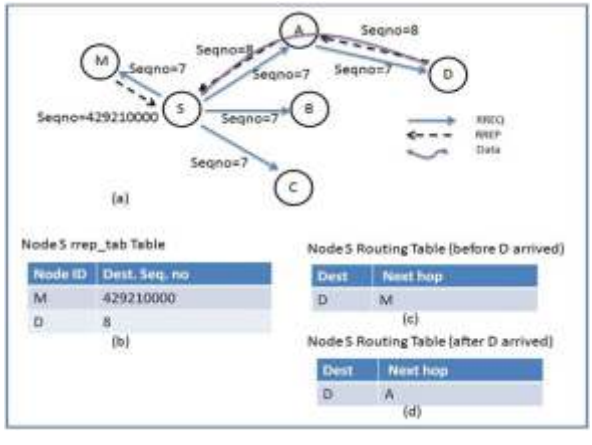

Figure 2. Routing update in the ERDA

Figure 3 shows how ERDA works during route discovery phase and how it updates routing table. Route request (RREQ) message is sent out by a source node S to find a fresh route to destination node D in AODV route discovery process. All neighboring nodes that have received this request and have "fresh enough route information" in their routing will respond to node S including the destination node D as illustrated in Figure 2(a). rrep_tab table stores the RREPs received by node S. Figure 2(b) shows the information contained in the rrep_tab table for node S. Assuming that the network is under Black hole attack, malicious node M would be the first node to respond to node S, the routing table of node S is updated with the information provided by node M as depicted in Figure 2(c). Since the value of the rt_upd parameter in the ERDA is set to "true", the routing update does not stop but allows next RREP message to update as well. Thus, when node S receives the RREP message from node A, the message will be accepted although the destination sequence number is smaller than the one in the routing table. As a result, in Figure 2(d) the former route entry is overwritten by the later RREP from node A. When RREP message from the destination node D is received, then false value will be set to rt_upd parameter.

An encryption algorithm with first Secret key used to secure AODV messages [5]. This initial process calculates signature with suitable encryption algorithm for given fields of an AODV message. This process also calculates signature with the secret key. Then, both given signatures will be transferred along with the AODV messages.

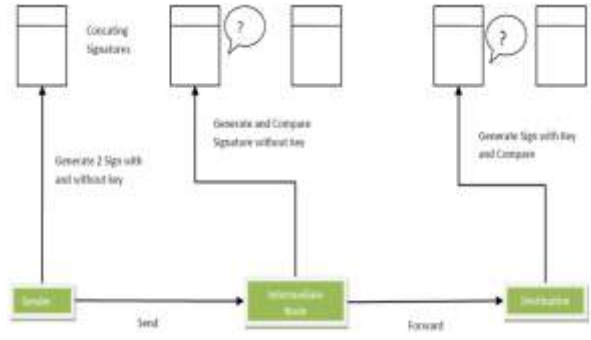

Figure 3. Secure AODV with two layer signature security scheme

In Figure 3, first a sender node generates the signature with the help of an encryption algorithm and concatenates it with given the AODV messages. This process make use of secure hash algorithm (SHA) value to generate signature. Then sender make use of a secret key to generate another signature and generate the same and also concatenates it with message. Afterwards, every time an intermediate node receives the AODV message, it checks the genuine character of the message by comparing concatenated signature with the newly produced signature. If it matches then final node will carry forward the message to the next node in the network. Before re-broadcasting a message, it will check the index of next node to check whether it is destination or not. Finally, if receiving final node matches the value of index by match them and find it is destination node then after it will count the signature with using private key for more security related purpose and compare it with concatenated special signature with key.

B. NMAC with HBKS Technique

The method used the authentication technique like nested message authentication code [6] to secure the routing packet in AODV and efficiently prevent most frequently occurred attacks such as black hole attacks, modifying routing information attacks and impersonation attacks. The key pre- distribution technique is used in this method to minimize the overhead caused by distributing and sharing the keys at the run time. The technique of selecting the keys from key table is according to value of hop count field in control packet and is named as hop count based key selection technique [6].

Volume : 4 | Issue : 6 | Special Issue June 2015 • ISSN No 2277 - 8179

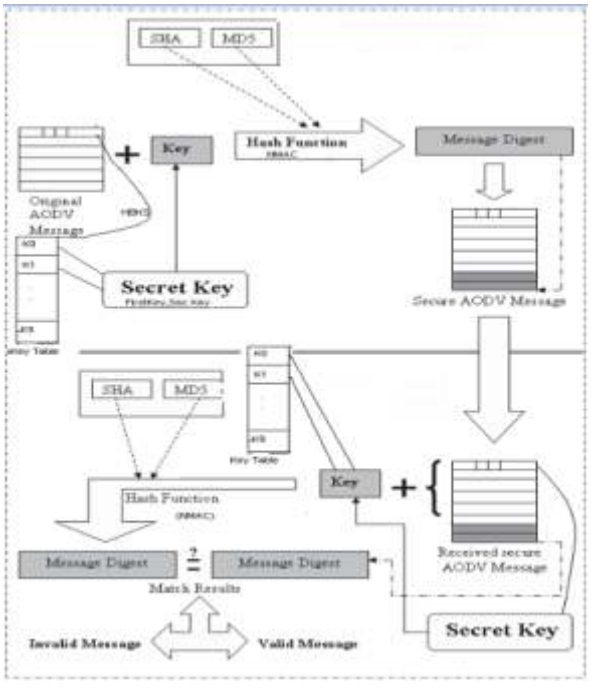

Figure 4. Message verification using authentication mechanism

In Figure 4, the digest of the packet using the NMAC is calculated before broadcasting the RREQ packet and then appended the digest with the original message. In NMAC, two keys are required which are selected according to the value in hop count field. At the sender the value of the hop count field is zero so first key from key table is used as the first key while next key from key table is used as second key. At the intermediate node to check the integrity of the received packet to get hop count for key generation the original message is separated from the digest and then the keys are selected from the key table accordingly. Then it generates the new digest of incoming message and compare with the incoming digest. If new and old digest are not matched then it discards the messages. If both are same it means the message is correct un-altered by any unauthorized entity. Then the value of hop count field is incremented by one. After this it generate the digest with incremented hop count value and appended with the message. Same procedure is followed at the destination. Similar procedure is used to checking the integrity of RREP, RERR and RREP-ACK packets.

A. Performance Analysis

The performance of the security mechanisms described here can be analyzed based on certain parameters that are listed in Table 1. The percentage of sent and received packets ratio between sender and recipient is called the packet delivery ratio.

Average End-to-End Delay (Delay) is the average time taken in second by a packet to travel from sender to recipient.

Security Mechanism	Cryptographic Overhead	Packet Delivery Ratio	End to End Delay	Average Throughput	Security issues	Communication Overhead and Memory utilization
ERDA	No	Low	Low	Low	High	Low
Two Layer Signature	Yes	Medium	High	Medium	Medium	Medium
NMAC with HBKS	Yes	High	High	High	Low	Comparatively high

Table 1. Performance analysis of the security mechanisms

Although the communication overhead and memory utilization in NMAC with HBKS technique is high, it provides better security and point to point authentication. And also the packet delivery ratio and average throughput will be high in this technique.

III. CONCLUSION

Secure transmission of information in MANET is a challenging task and AODV is a well-known reactive routing protocol used in MANET. In this paper, we analyzed some security mechanisms used by AODV routing protocol. In which ERDA secures the routing update algorithm, an encryption algorithm with Secret key is used to secure AODV messages in two layer signature scheme and NMAC with HBKS technique secure the routing packet in AODV and efficiently prevent most frequently occurred attacks. From the survey on AODV with different security mechanisms, we concluded that the best method is securing AODV using NMAC with HBKS.

ACKNOWLEDGMENT

We thank GOD almighty, who showered His abundant grace on us to make this paper. We express our heartfelt thanks and deep sense of gratitude to our Principal. We extend our deep gratitude to our Head of the Department for her valuable help and support.

REFERENCE

[1] Wei Liu, Hiroki Nishiyama, Nirwan Ansari, Jie Yang, and NeiKato, "Cluster-Based Certificate Revocation with Vindication Capability for Mobile Ad Hoc Networks", IEEE Transactions on parallel and distributed systems, vol. 24, no. 2, Feb. 2013. | [2] Ram Ramanathan and Jason Redi, "A brief overview of Ad-hoc Networks: Challenges and Directions", IEEE Communications Magazine May 2002, pp.20-22. | [3] Sheela Rani Arasu, and Immanuel Johnraja Jebadurai, Analysis of Different Routing Techniques for Opportunistic Data Transfer, International Journal of Computer Applications (0975 - 8887), volume 62 - No.5, January 2013. | [4] Kamarularin Abd Jalil, Zaid Ahmad, and Jamalul-Lail Ab Manan, "Securing Routing Table Update in AODV Routing Protocol", IEEE Conference on Open Systems, pp. 978-1-61284-931-7, September 2011. | [5] Morli Pandya, Ashish Kr. Shrivastava and Rajiv Gandhi Proudyogiki Vishwavidyalaya, "Improvising the Performance with Security of AODV Routing Protocol in MANETs", IEEE Nirma University International Conference on Engineering, pp. 978-1-4799-0727-4, 2013. | [6] K. V. Arya and Shyam Singh Rajput, "Securing AODV Routing Protocol in MANET using NMAC with HBKS Technique", IEEE International Conference on Signal Processing and Integrated Networks, pp. 978-1-4799-2866-8, 2014.IEEE International Conference on Signal Processing and Integrated Networks, pp. 978-1-4799-2866-8, 2014.