Securing AODV Routing Protocol in Mobile Ad-hoc Networks

Phung Huu Phu, Myeongjae Yi, and Myung-Kyun Kim

Network-based Automation Research Center and
School of Computer Engineering and Information Technology
University of Ulsan, Ulsan Metropolitan City, 680-749, Republic of Korea
{phungphu, ymj, mkkim}@mail.ulsan.ac.kr

Abstract. In this paper, we have proposed a security schema for Ad-hoc On-Demand Distance Vector (AODV) routing protocol. In this schema, each node in a network has a list of its neighbor nodes including a shared secret key which is obtained by executing a key agreement when joining a network. One key principle in our schema is that before executing route discovery steps in AODV protocol, each node executes message authentication process with the sender to guarantee the integrity and non-repudiation of routing messages and therefore, could prevent attacks from malicious nodes. Comparing with other recently proposed security routing protocols, our security schema needs less computation power in routing transactions and does not need any centralized element in mobile ad-hoc networks.

1 Introduction

The AODV routing protocol [1] is being considered by the Internet Engineering Task Force (IETF) for Mobile Ad-hoc Network (MANET) routing protocol standardization. AODV is improved from DSR [2] routing protocol and both of them are reactive routing protocols. In general, the AODV routing protocol fulfills the requirements of routing protocol in MANETs and it is efficient in terms of network performance. However, security aspects have not been considered in the protocol; attackers, therefore, can use many kinds of attacks via route discovery or path maintenance process such as advertising falsified route information, redirecting routes, launching denial-of-service attacks, sending falsified error reports and so on.

Recently, a number of researches have been investigated for secure routing protocols in MANETs. Some focus on AODV and others examine general solution for secure routing in MANETs. Most routing security solutions make unrealistic assumptions about the availability of key management infrastructures that are in contrast with the very nature of ad hoc networks. Integrity of transactions between neighbor nodes, which is required to protect against fabrication attacks, is not examined in most of these protocols.

In this paper, we examine and discuss recent secure routing protocols in order to identify the flaws of current security approaches. Based on the analysis,

a security schema for AODV routing protocol has been proposed to eliminate the security flaws in the protocol and compensate identified security weaknesses in recent secure routing approaches.

The remainder of this paper is organized as follows. Section 2 examines current approaches of security routing, then the scope of problems which needs to be solved in this research is stated. In section 3, we detail our proposed schema to secure AODV. We discuss and analyze our schema in section 4. Finally, we conclude our contribution and specify future work in section 5.

2 Problem statement

Lately, there are a number of solutions for securing routing protocols in MANETs. In this section, however, we briefly describe only two schemas: ARAN [4] and SAODV [5] since they are closely related to our approach. In [4], the authors categorized three kinds of threats which are modification, impersonation and fabrication in AODV and DSR. On the basic of these analysis, the authors proposed a protocol called ARAN (Authenticated Routing for Ad hoc Networks) using cryptographic certificates to bring authentication, message-integrity and non-repudiation to the route discovery process based on the assumption of existing of a trusted certificate server. It is not appropriate with ad hoc networks because it forms a centralized element. Moreover, in this protocol, because the source node cannot authenticate intermediate nodes in the routing path, intermediate malicious nodes can use error message attacks to networks. In [5], the authors extend the AODV routing protocol to guarantee security based on the approach of key management scheme in which each node must have certificated public keys of all nodes in the network. This work uses two mechanisms to secure the AODV messages: digital signature to authenticate the fixed fields of the messages and hash chains to secure the hop count field. This protocol uses public key distribution approach in the ad hoc network; therefore, it is difficult to deploy and computationally heavy since it requires both asymmetric cryptography and hash chains in exchanging messages. The protocol also did not consider the authentication of intermediate nodes; hence it could not prevent the attack of falsifying error messages in ad hoc networks.

In general, the existing schemas for secure routing are based on the assumptions of the availability of key management infrastructures which are unrealistic and contrast to the ad-hoc network concepts. Moreover, these schemas do not consider intermediate nodes during the routing steps; therefore, the nodes may perform fabrication attacks. From these weaknesses of current approaches, our goal is to design a schema which performs point-to-point message authentication without a deployed key management infrastructure.

3 The proposed security schema for AODV

The principle of our schema is that messages in AODV must be authenticated to guarantee the integrity and non-repudiation so that the protocol can be pre-

vented against several kinds of attacks. Each node in a network has its own a pair of public key e and private key d following RSA Public-key Crypto-system [6] by self-generation, and each node contains a list of neighbor nodes with records containing the information of a neighbor node including neighbor address, neighbor public key, and a shared secret key. This information is formed after the key agreement between two neighbor nodes to negotiate a pair of keys and a shared secret key. The details of our security schema for AODV are described as the following sections.

3.1 Key agreement process between neighbor nodes

A node joining a network requires to send key agreement messages to its neighbors to negotiate a shared secret key. The concept of this process is based on HELLO message in ad-hoc routing protocols. The node broadcasts a message indicating the negotiation request with neighbor nodes: *<AGREEMENT_REQ, request_id, sender_addr,* e_S*>*. On receiving this request, nodes reply a message: *<AGREEMENT_REP, request_id, sender_addr, neighbor_addr,* e_N*>* (where e_S *and* e_N are the public key of the sender node and replying node, respectively; *request_id* is a sequence number generated by the sender node) to indicate the receiving of the request message and inform that it is ready for the key agreement process. For each received message, the request node creates a new record in its neighbor list. Each record contains filled neighbor address and filled neighbor public key; the other fields of the record are empty. For each new record in the list, the request node (A) negotiates a secret key with the neighbor node (B) by the following steps:

1. *Generate a key* K_s *by using a secure random number generator,*
2. *Encrypt* K_s *with* e_B *(node B's public key) =* $encrypt_{e_B}(K_s)$*,*
3. *Send an offer message <KEY_OFFER,* $encrypt_{e_B}(K_s)$*> to B,*
4. *Wait ACK from B and check message integrity to finish the negotiation*

When node B receives the offer message, it decrypts $encrypt_{e_B}(K_s)$ by its private key (d_B)to get the shared key K_s. Then, node B sends the ACK message *<KEY_OFFER_ACK, request_id,* h_{K_s}*(request_id)>* to indicate successful shared secret key negotiation, where h_{K_s}*(request_id)* is the hashed message of *request_id* by the shared key K_s.

Since RSA algorithm is used in the negotiation, the confidentiality of the shared key is guaranteed between the two nodes. The shared key is used for authenticating messages between two adjacent nodes later in AODV routing protocol. In the case a node does not have a shared key with its neighbor nodes, it can not participate in routing transactions.

3.2 Route request

Route request (RREQ) is initiated by a source node (S) and then propagated by intermediate nodes until the message reaches its destination node (D). On

receiving RREQ, an intermediate node I, according to AODV routing protocol, checks whether the message will be re-broadcasted or not. If the message needs to be re-broadcasted and the sender is in node I's neighbor list, it will send (unicast) a message to request the authentication process from the sender: *<AUTHEN_RREQ_REQ, src_addr, broadcast_id>*. When receiving the authentication request, the sender creates an authentication reply message containing *<AUTHEN_RREQ_REP, src_addr, broadcast_id,* $hash_{K_s}$*(RREQ)>* where $hash_{K_s}$*(RREQ)* is the hashed value of RREQ message by the shared key K_s between the two nodes. The authentication reply message is unicasted back to node I. Node I on receiving the message will check the integrity of the RREQ message by hashing the message with using the shared key K_s and then comparing with the received hashed digest. If the comparison is successful (the integrity of the RREQ message is guaranteed), node I continues steps following AODV such as set up reverse path, increase the hop count, rebroadcast the message and so on; otherwise, the RREQ will be discarded. The process continues until the message reaches the destination. The destination also authenticates the sender of RREQ (neighbor of the destination) by the same procedure.

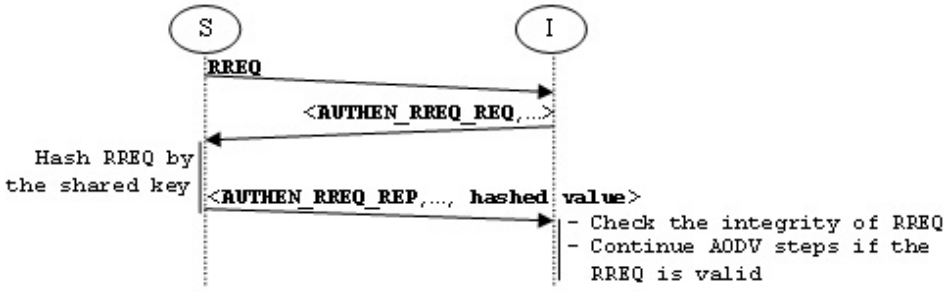

Fig. 1. Illustration of the message authentication

3.3 Route reply and route maintenance

Route replies (RREP) in AODV are also targets for attacks by malicious nodes. In our schema, when receiving a RREP, a node requests the sender to proof the integrity and non-repudiation of the message by sending an authentication message . The request for authentication is *<AUTHEN_RREP_REQ, dest_addr, dest_seq_#>* and the reply is *<AUTHEN_RREP_REP, dest_addr, dest_seq_#,* $hash_{K_s}$*(RREP)>* where $hash_{K_s}$*(RREP)* is the hashed value of RREP message by the shared key K_s between the two nodes. After the authentication process is successful, a node continues to the steps in AODV, otherwise, the node drops RREP since it is invalid.

In route maintenance process, only route error report message (RERR) is a target for attacks in AODV protocol. Our schema requires the authentication

process in sending route error messages to prevent attacks from malicious nodes. The authentication request and response for RERR is $<AUTHEN\_RERR\_REQ,$ *unreachable_dest_addr, unreachable_dest_seq_#*$>$, and $<AUTHEN\_RERR\_REP,$ *unreachable_dest_addr, unreachable_dest_seq_#,* $hash_{K_s}(RERR)>$, respectively.

4 Security analysis

Our schema proposes a new fully distributed authentication process which does not require any third parties. The schema does not supply the confidentiality but it provides the integrity and non-repudiation of messages. Our schema has a similar approach with SAODV or ARAN in supplying the integrity and non-repudiation of messages. However, it uses point-to-point authentication process, therefore, it can authenticate intermediate nodes in routing steps and it does not require a certificate server (like ARAN) or assumption of key distribution (SAODV).

By supplying integrity of exchanging messages, our schema can prevent against attacks from malicious nodes. A malicious node can not forms loops by spoofing nodes thanks to authentication process between neighbor nodes. Based on the integrity of exchanging messages, the schema also can prevent falsified error messages or modification attacks during route discovery process. However, the end-to-end authentication process has not been considered yet in our current work, some kinds of attacks such as impersonating a source node, a destination node, or neighbor of destination could not been prevented if malicious nodes comply with the proposed procedure. It is assumed that after time of working, trust relationship between two neighbor nodes will be established; a node that continues to perform malicious activities will be detected and excluded from trust list and therefore, so it can not participate in future routing. This aspect is expected to be studied in future.

In general, the proposed security schema needs heavy computation when a node joins a network, but during routing transactions, it needs less computation power compared to existing approaches since it only uses hash algorithm to authenticate between two nodes and it does not need a centralized element in the network which causes heavy computation in the existing secure routing protocols. In our opinion, the proposed schema is more appropriate to the MANETs since there is no centralized element. This approach differs from most routing security solutions which make unrealistic assumptions about the availability of key management infrastructures that are in contrast with the very nature of ad hoc networks.

5 Conclusions and future work

Our work focuses on AODV routing protocol, which is under consideration as a standard for routing in MANETs. A security schema for AODV has been proposed to prevent common kinds of attacks and compensate for the security flaws of recent related works. The approach of our work is that exchanging

messages in AODV are required to be authenticated in point-to-point step by using hash chains during a transaction. When joining a network, a node must execute key agreement with neighbor nodes so that each two neighbor nodes have a shared secret key. Before executing steps in AODV, each node performs message authentication process with the sender by requesting hashed digest value of the message and then checking the integrity and non-repudiation of routing messages from the hashed message in order to prevent attacks from malicious nodes. However, some kinds of attacks such as tunneling attacks or selfishness problems (so far, no security schema has been able to detect these [5]) have not been considered in this work.

This work has proposed a point-to-point and fully distributed authentication approach for securing AODV. It can compensate for weaknesses in SAODV or ARAN as above-mentioned since it can authenticate intermediate nodes in transactions and it does not need any centralized element such as certificate server. Recently, this work just focuses on AODV routing protocol; however, future work will investigate on applying the schema to other routing protocols in MANETs. The implementation and simulation of the schema will be investigated to compare security features with similar approaches in particular kind of attacks. The end-to-end authentication procedure will be added to the current approach in order to improve our current schema.

6 Acknowledgement

The authors would like to thank Ministry of Commerce, Industry and Energy, Ulsan Metropolitan City, University of Ulsan, and the Network-based Automation Research Center (NARC) which partly supported this research. The authors also thank Prof. Hoon Oh (University of Ulsan) and the anonymous reviewers for their carefully reading and commenting this paper.

References

1. Charles, E. P. and Elizabeth, M. R.:Ad hoc On-Demand Distance Vector Routing. In Proc. of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, New Orleans, LA (1999) 90–100.
2. Johnson, D. and Maltz, D.: Dynamic source routing in ad hoc wireless networks. T. Imielinski and H. Korth(eds.), Mobile computing, Kluwer Academic Publ. (1996).
3. Refik, M. and Pietro, Mi.: Security in Ad hoc Networks. Lecture Notes in Computer Science, Springer-Verlag GmbH, Volume 2775 (2003) 756 – 775.
4. Kimaya, S. et al: Authenticated routing for ad hoc networks. Journal on Selected Areas in Communications, IEEE, Vol. 23, Issue 3 (2005) 598–610.
5. Zapata, M. G. and Asokan, N.: Securing Ad hoc Routing Protocols. In Proc. of the ACM workshop on Wireless security, Atlanta, USA (2002) 1–10.
6. Man, Y. R.: Interner Security-cryptographic: principles, algorithms and protocols. Wiley Publishing House (2004).
7. Panagiotis, P. and Zygmunt, J. H.: Secure Routing for Mobile Ad hoc Networks. In SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), San Antonio, TX (2002).