A PKI Based Mesh Router Authentication Scheme to Protect from Malicious Node in Wireless Mesh Network*

Kwang Hyun Lee and Choong Seon Hong**

Department of Computer Engineering Kyung Hee University
Seocheon, Giheung, Gyeonggi, 446-701 Korea
khlee@networking.khu.ac.kr, cshong@khu.ac.kr

Abstract. Wireless mesh network can increase service coverage by low-cost multiple-paths between a source and a destination. But because of the wireless nature, wireless mesh network is vulnerable to diversified threats. Especially attacks by malicious nodes can decrease the performance or ravage the network. Many protocols, based on Public Key Infrastructure (PKI), have been proposed to ensure security however; these protocols cannot efficiently prevent the cases of compromised nodes. In this paper, we propose a mesh router authentication scheme to solve this problem of existing protocols. Although our scheme increases the end-to-end delay, the proposed mesh router authentication scheme can guarantee secure wireless mesh network communication from malicious nodes.

Keywords: Wireless mesh network, Security, Wormhole attack, PKI.

1 Introduction

Wireless mesh network [1] can be deployed more efficiently in a wide network area. In case of Wi-Fi to extend network area, the cost of deployment will be highly increased [2]. But a network can be extended in an efficient and a low-cost way using wireless mesh network in comparison to the Wi-Fi network.

Wireless mesh network structure is similar to MANET (Mobile Ad-hoc Network) [3]. Wireless mesh network and MANET have to apply policy of high level security because of the ad hoc nature of these networks. But MANET cannot apply heavy security policy due to the performance limitation. On the contrary, wireless mesh network has the processing ability to apply heavy security policies. In this paper, we propose mesh router authentication scheme for adapting optimized algorithm for security in wireless mesh network. By using the proposed mesh router authentication

* This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education, Science and Technology (R01-2008-000-20801-0).

** Corresponding author.

C.S. Hong et al. (Eds.): APNOMS 2009, LNCS 5787, pp. 405–413, 2009.

scheme, delay time is increasing. We are able to detect malicious nodes in the network and delete them from the network.

This paper is organized as follows. In Section 2, we give a brief overview of wireless mesh network and security threats due to malicious nodes. We describe proposed mesh router authentication scheme in Section 3. In Section 4, we explain the scenario for the attack prevention scheme. The performance evaluation is presented in Section 5. Finally, the conclusion and future works are provided in Section 6.

2 Background

Wireless mesh network consist of one or more mesh routers and mesh clients. The mesh clients are mobile ad hoc nodes with scarce resources while the mesh routers have no mobility, and they communicate each other using high bandwidth radio links. The mesh routers are used to forward the mesh client packets to the mesh gateway. The mesh gateway connects the mesh clients to the Internet. As the mesh routers have functions of self-configuration, self-healing and self-organization, mesh routers can compose or modify routes by themselves.

The wireless mesh network can be classified as three types. First type is Infrastructure/Backbone wireless mesh network. It provides the basic routing backbone consisting of only mesh routers. Second type is Client wireless mesh network. Client wireless mesh network seems like simple ad-hoc networks. It consists of just client that also work as routers or forwarding nodes. The last type is Hybrid wireless mesh network. This type has the combined characteristics of both Infrastructure/Backbone and Client wireless mesh network.

2.1 Problem Statement

Wireless mesh network is vulnerable to diversified threats. A malicious node can launch an attack during the mesh network initialization. Especially, Wormhole attack, which can easily breakdown the network and affects its performance significantly. The following provides a brief description of the Wormhole attacks [4].

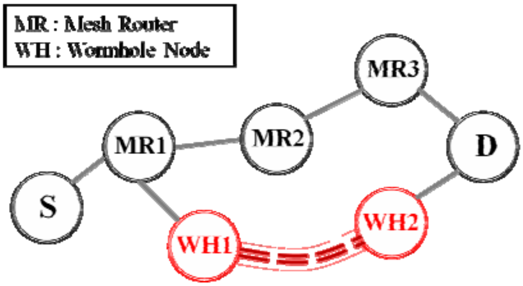


Fig. 1. An example of Wormhole attack

Wormhole attack is different from other network attacks. The majority of the network attacks consist of single node. However, in an attacker uses two nodes and makes an optimized tunnel between them. This can be achieved by using high bandwidth links, wired line, or encapsulation. This optimized link appears tempting for other nodes of the network. As a consequence, network nodes start to use the optimized, but compromised link for data forwarding. At first sight, Wormhole tunnels appear to be good, as they provide fast links for data forwarding. However, Wormhole nodes can do sniffing, modifying and dropping of data packets. Therefore, nodes have to establish the network without Wormhole nodes.

3 Proposed Mesh Router Authentication Scheme

If there is no authentication scheme, malicious nodes can execute an attack such as Wormhole. Therefore, if mesh routers are authenticated for each communication, a malicious node cannot harm the network. In this section, we explain our proposal for mesh router authentication based on PKI (Public Key Infrastructure) to protect the network from malicious nodes in wireless mesh network.

3.1 Assumptions

We maintain some assumptions, as follows:

- There is a CA (Certification Authority), which has the list of public key of all mesh routers.
- All mesh routers have hash function and public key of the CA.
- Both sender and receiver can listen to the transmission of each other.
- Routing protocol used is DSR (Dynamic Source Routing) [5].

SEQ	Source Address	Destination Address	Path	Digital Signature	...	Path	Digital Signature
Random Message							

Fig. 2. Proposed RREQ message format

3.2 Proposed PKI Based Mesh Router Authentication Scheme

During the network initialization, each mesh router broadcasts the RREQ message. The format of RREQ packet is shown in Fig. 2. Our scheme includes a digital signature to authenticate mesh router. If mesh router receives the RREQ message, the mesh router creates the digital signature with the help of private key and random message. The created digital signature is then added in the RREQ message. The RREQ message is then rebroadcasted for route discovery. Using the digital signature, we can authenticate the mesh router.

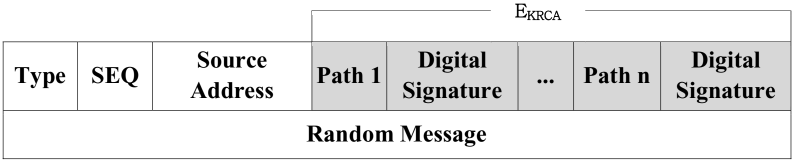
Our scheme uses two ways for the authentication, first scheme works during initialization of the network. On the other hand, second schemes works after any route update. In first method, intermediate nodes authenticate the mesh router. In second method, intermediate mesh routers just check the broadcast time of next hop node by WPA (Wormhole Prevention Algorithm) [6].

3.2.1 Mesh Router Authenticated by Intermediate Mesh Router

An intermediate mesh router which called MR1, broadcasts the RREQ message to configure path and wait for receiving RREQ message from the next hop mesh router (by overhearing). The MR1 then uses a WPT (Wormhole Prevention Timer) to detect the Wormhole node. The WPT can be calculated by following equation:

$$WPT = \frac{2 \times Transmission\ \ Range(TR)}{The\ \ propagation\ \ speed\ \ of\ \ a\ \ packet} \tag{1}$$

If the RREQ message is arrived within WPT, the intermediate mesh router (MR1) encrypts the path and next hop node's digital signature by CA`s public key, and sends the RAREQ (Router Authentication Request) message to the CA. Fig. 3 shows the RAREQ message format. The RAREQ message is used for confirmation of mesh router's digital signature by the CA. The CA compares the RAREQ with the digital signature of the mesh router and then, the CA sends the RAREP message that has the result of the comparison to the requester mesh router. Using this authentication way we can find the malicious mesh router in a faster way even though this scheme has large overhead.



			E_{KRCA}				
Type	**SEQ**	**Source Address**	**Path 1**	**Digital Signature**	**...**	**Path n**	**Digital Signature**
Random Message							

Fig. 3. Proposed RAREQ message format

3.2.2 Mesh Router Authenticated by Source Mesh Router

The intermediate mesh router overhears the next hop mesh router's RREQ message. At this time, if the RREQ message is not arrived within WPT, the intermediate mesh router just drop the RREQ message as it was not sent to confirm the router authentication. If the source mesh router's RREQ message is arrived at the destination mesh router, it encrypts paths and digital signatures of source and unicast the RREP message into reverse direction. After the source mesh router receives the RREP message, it sends the encrypted paths and digital signatures to the CA using the request message (RAREQ) message.

As we mentioned above, the CA compares encrypted path nodes with their digital signatures present at the CA. And then the CA replies the RAREP (Router Authentication Reply) message that contains comparing results.

Fig. 4 shows the RAREP message format. As shown in Fig.4, the path and the comparing results are encrypted using the source node's public key. In this case, the network traffic is lower in amount as compared to the case of the intermediate authentication. However if malicious mesh router broadcasts the RREQ message, the source mesh router waits for receiving the destination router's RREP message.

			E_{KUSN}				
Type	**SEQ**	**Destination Address**	**Path 1**	**Comparing result**	**...**	**Path n**	**Comparing result**

Fig. 4. Proposed RAREP message format

3.3 The Mesh Router Reliability Table

The mesh router maintains a mesh router reliability table by using authentication results with the neighbor mesh routers. Because mesh networks use the multi-path routing protocol [7], the mesh router reliability tables are maintained by comparing results information of neighbor mesh routers. If the networks have a malicious mesh router, the malicious mesh routers are detected by its neighbor nodes. Then neighbor nodes report to other node. The mesh routing reliability table stores a value against each neighbor router.

This value indicates the number of times the RREQ was heard by a neighbor node without hearing the forwarded RREQ message by the same router node. This value is maintained to identify the malicious neighbor router nodes. For instance, if any router received the RREQ message and did not forward the RREQ message, we can doubt this node as a malicious node. Each time this happens, the value is increased. If any routing path has this value more than the threshold value, the mesh routers is removed from the routing path in the routing table.

4 Protecting Scenario of Proposed Scheme

Proposed scheme supports more robust security than the traditional scheme. The traditional scheme has threats such as the case of malfunction mesh router or attack from an authenticated mesh router. But these attacks can be prevented by rechecking the mesh router in case of already authenticated mesh routers. In this section, we explain a scenario of our proposed scheme.

4.1 In Case of Wormhole Node Just Can Forward the RREQ Message

As shown in fig. 5, we can prevent the malicious mesh router that has no broadcasting function. If router A needs to configure the path, the router A broadcasts the RREQ message with the RM (Random Message). At this time, if the wormhole nodes have no broadcasting function, the RREQ message cannot attach router A within WPT.

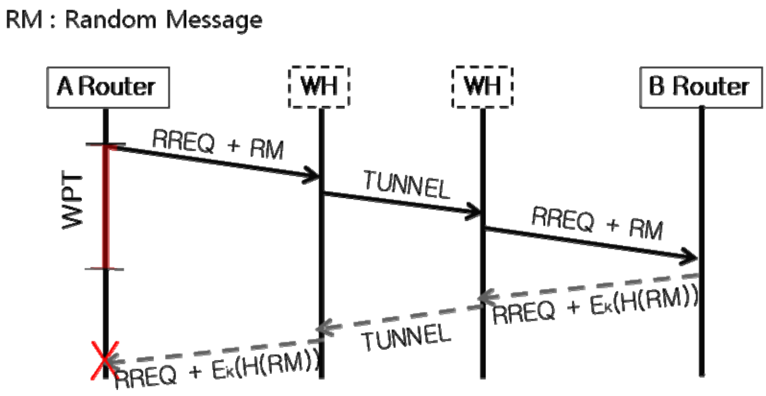


Fig. 5. In case of wormhole node just can forward the RREQ message

4.2 In Case of Wormhole Node Can Broadcast RREQ Message

If the wormhole node can broadcast the RREQ message, the traditional scheme (ex. WPA) cannot prevent the wormhole node. However our scheme can prevent the wormhole node as follows.

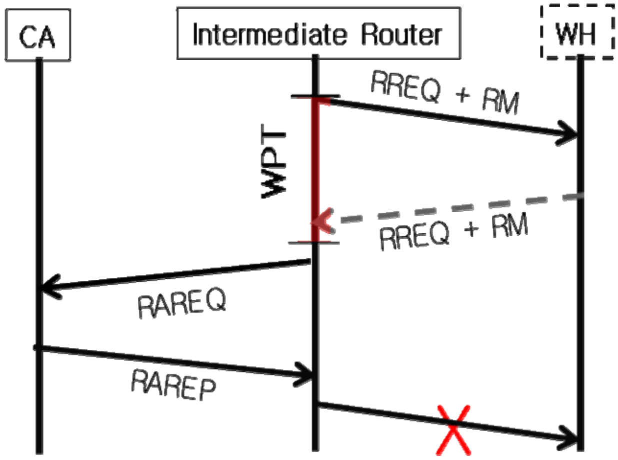


Fig. 6. Mesh router authenticated by intermediate mesh router

In case of the mesh router is authenticated by the intermediate mesh router, the intermediate mesh router sends the RAREQ message to the CA. After receiving the RAREP message from the CA, the Intermediate mesh router decides whether the path is removed or not. Fig 6 shows a simple example of preventing wormhole node.

Fig 7 shows the case of the mesh router authenticated by the source mesh router. If the destination mesh router receives the RREQ message, the destination mesh router encrypts paths and the digital signature by using CA`s public key. And the destination mesh router unicast the RREP message and encrypted message through reverse path to the source mesh router. The destination mesh router encrypts path and the digital signature because if the destination mesh router cannot encrypt the message, the malicious nodes can modify the digital signature. Therefore, in the proposed scheme; during the transmission process, encrypted message cannot be modified by the malicious nodes. The CA decrypts this message and after confirming the mesh router and signature, the destination mesh router sends the RAREP message to the source node.

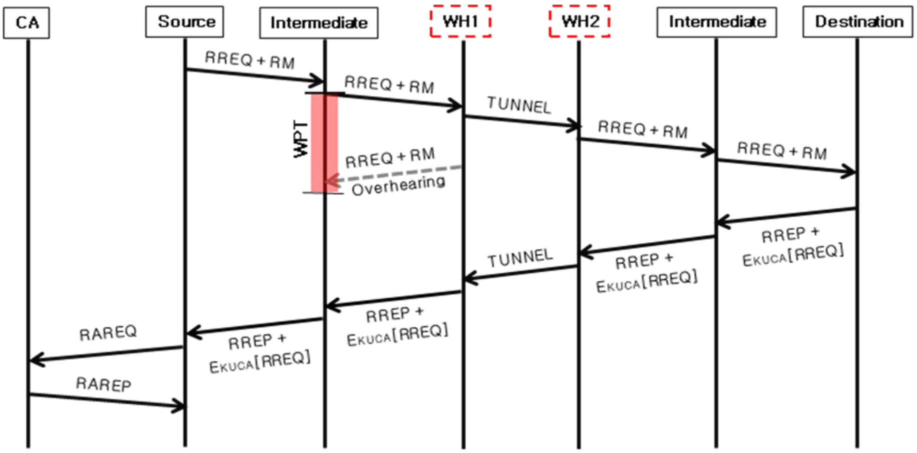


Fig. 7. Mesh router authenticated by source mesh router

5 Simulation Result

Parameter	Value
Simulation code	C++
Network form	Grid topology
The number of nodes	10~60
Total number of simulation	100

To evaluate the performance of our scheme we perform the simulation in C++. We assume that network topology is grid topology and mesh routers have uniform distance in between them. We select the source mesh router and the destination mesh router randomly. We perform our simulation 100 times. We increase nodes to check changing value depending on the number of nodes.

As shown in Fig. 8, x-axis denotes the number of nodes and y-axis denotes time (in milliseconds) of finding destination mesh router. Two lines show the traditional DSR and our proposed scheme, respectively. As the numbers of nodes are increased, the time to detect the destination mesh router is also increased. As shown in the fig. 8, our scheme works slower than the traditional scheme. But it provides better security, as it uses public key encryption between the source router node and the destination router

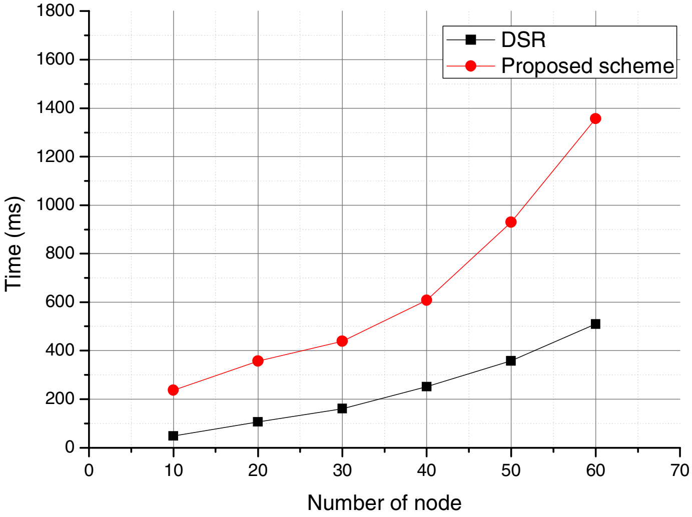


Fig. 8. The average time to detect destination mesh router

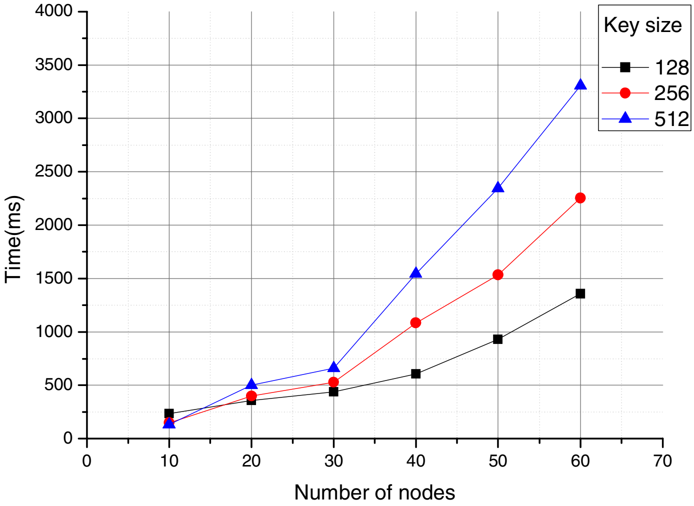


Fig. 9. The average time to detect destination mesh router with the increase of number of nodes for different key sizes

node. The DSR protocol does not use any kind of such encryption or authentication. So, the worm whole attacks are easily possible. Therefore, as our scheme has more delay but it is a trade-off between the security and delay.

Fig. 9 shows the time delay in detection of the destination router nodes with the increase of number of nodes for different key sizes. We perform the simulation using 128-bit, 256-bit and 512-bit public key encryption. We can see that the delay is increased with the use of higher bit key but the difference is not significant. As shown in Fig.9, when the number of nodes is smaller then the delay between using different keys is not significant. However, as the numbers of nodes increase, the delay is increased significantly. With this graph we can find the optimal value of number of nodes for a certain size of the public key. As the mesh nodes have the processing capability of performing the public key cryptography. And the number of router nodes in a wireless mesh network is not high. Hence, using higher bit keys seems to provide a good and secure solution for the wormhole attack problem.

6 Conclusion

We need to apply more robust scheme for secure networking because wireless mesh network have high performance,. In this paper, we propose a suitable enhanced scheme for wireless mesh network using a PKI based mesh router authentication scheme. Our scheme uses mesh routers' digital signatures to authenticate each other when detecting a path and a Route-Reply forwarding timeout to detect the malicious nodes, which causes the wormhole attacks. Therefore, our proposed scheme can prevent not only wormhole attack but also other attack from malicious nodes. Our proposed scheme has weak point that it has large overhead. We are currently working to make our scheme a lightweight scheme for wireless mesh network.

References

1. Akyildiz, I.F.: A Survey on Wireless mesh network. IEEE Radio Communications (September 2005)
2. Ben Salem, N., Hubaux, J.-P.: Securing Wireless mesh network. Wireless Communications, IEEE 13(2), 50–55 (2006)
3. Nandiraju, D., Santhanam, L., Nandiraju, N., Agrawal, D.P.: Achieving Load Balancing in Wireless mesh network Through Multiple gateways. In: Mobile Adhoc and Sensor Systems (MASS), October 2006, pp. 807–812 (2006)
4. Glass, S., Portmann, M., Muthukkumarasamy, V.: Securing Wireless mesh network. Internet Computing, IEEE 12(4), 30–36 (2008)
5. Johnson, D.B., Maltz, D.A.: Dynamic Source Routing in Ad Hoc Wireless Networks. Mobile Computing (1996)
6. Choi, S., Kim, D.-y., Lee, D.-h., Jung, J.-i.: WAP:Wormhole Attack Prevention Algorithm in Mobile Ad Hoc Networks. In: 2008 IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, June 11-13, pp. 343–348 (2008)
7. Nandiraju, N.S., Nandiraju, D.S., Agrawal, D.P.: Multipath Routing in Wireless mesh network. In: Mobile Adhoc and Sensor Systems (MASS), October 2006, pp. 742–746 (2006)