On-demand Secure Routing Protocol for Ad Hoc Network using ID based Cryptosystem

Youn-Ho Lee, Heeyoul Kim, Byungchun Chung, Jaewon Lee and Hyunsoo Yoon
Division of Computer Science, Department of Electric Engineering and Computer Science
Korea Advanced Institute of Science and Technology, Taejon, Korea
Email: (yhlee,hyoon)@camars.kaist.ac.kr

Abstract- The routing protocol that is appropriate for an ad hoc network is essentially needed. But the researches about the routing protocols for ad hoc networks so far are mainly target the efficiency and assume the trusted environment. But these protocols are not well operated at the networks that adversaries exist in. In this paper, we propose a new on-demand secure routing protocol for ad hoc networks using ID based cryptosystem. Our protocol can authenticate all nodes in the routing path with less network resource consumption than previous secure routing protocols. And our protocol does not need the fixed infrastructure without unrealistic assumptions because of using ID based cryptosystem.

Keywords (3-8 words): Network Security, ID based cryptosystem, ad hoc network routing

I. Introduction

Unlike the wired network, an ad hoc network has the feature that each node in the network can move freely and the topology of the entire network is frequently changed. So we can't have the enough performance for ad hoc networks using the routing algorithms that is used for the wired network. For this reason, many routing protocols that are compatible for the characteristics of ad hoc networks are proposed. But, many researches so far zero in on the purpose of the efficiency of the routing performance. The characteristics of the ad hoc network enable itself to be used for the military applications and the communication between the unmanned devices that is needed for the dangerous environment. So routing protocols for the ad hoc network used in such applications must have the secure and reliable feature.

The concept of the ID based cryptosystem is proposed by Shamir in 1984. It is different from the common public key infrastructure system(PKI) in that the public key of one's user is the ID of one itself. It is of benefit to us that we don't need to access the directory server to know the public key of other users. Therefore, the fixed infrastructure is not needed after the initialization process of distributing the private keys of the users. This is the common required environment that Ad hoc networks need.

In this paper, we propose the secure routing protocol using ID based cryptosystem. Differently from the existing protocols, our protocol can authenticate all the intermediate nodes that are in the routing path. And it needs only constant cryptographic parameters for a route request/reply packet with no dependency of the path length. So it can reduce the additional network resource for the cost of routing protocols being secure. Our protocol uses public key cryptosystem without the fixed infrastructure in operating the network. By this reason, our protocol doesn't need the additional network resource consumption for exchanging the certificate of the nodes in the network. From the point concerned above, out protocol suits the purpose of the ad hoc network routing. Our protocol can be applied to the on demand source routing protocol such as DSR[1,2].

II. Related Work

For the routing protocols with security feature, some methods are proposed[3-10]. But we mention only three recently proposed methods. We discuss Ariadne, ARAN (Authenticated Routing for Ad hoc Networks), SRP (Secure Routing Protocol)[8-10]. They are using hash chain, public key cryptosystem and symmetric cryptosystem each for securing their protocols. These three schemes were used in almost all existing methods for the secure routing protocols targeting on ad hoc networks.

ARAN uses the public key infrastructure that needs certificate authority (CA) for its security feature. In ARAN protocol, all nodes in the network must attach their certificate signed by CA when they perform the route recovery protocol or route maintenance protocol. So ARAN has a weak point that all nodes consume additional network resources for sending their certificates. Not only this point, the source node that want to know the routing path to the destination node cannot authenticate the intermediate nodes that are in the routing path. Only previous node that sends the route reply packet directly and the destination node can be authenticated.

SRP assumes the shared symmetric key between the source node to request route path and the destination node. So If the route request packet generated by the source node arrives in the destination node, destination node authenticates the path in the route request packet by using message authentication code (MAC) and reply it to the source node. The major problem of this protocol is that it also cannot authenticate the intermediate node in the routing path. For this reason, the malicious intermediate

- This work was supported by the Korea Science and Engineering Foundation (KOSEF) through the Advanced Information Technology Research Center(AITRC)

0-7803-7840-7/03/$17.00 ©2003 IEEE.

nodes can longer the routing path by inserting fictitious node. And this protocol assumes the shared key between two nodes. So if one node wants to know the path to the node that does not have the shared key with the one node, they must perform the key agreement protocol for sharing a common key. Its cost is comparable with the public key operation. Using such operation reduces the efficiency benefit of using the efficient symmetric operation in SRP protocol.

Ariadne is based on the on-demand routing protocol. It uses TESLA (Timely Efficient loSs toLeration Authentication protocol), the broadcast message authentication scheme[11-12]. TESLA assumes the maximum time synchronization error between all nodes participating in the protocol. And it uses the hash chain for the nodes in the network to authenticate the packet of other nodes. Different from the above two routing protocols, Ariadne has a good merit of providing the source nodes to authenticate all intermediate nodes in the routing path using the TESLA MACs in the route reply packet. But it has some drawbacks. The first one is that it assumes the time synchronization between the nodes and maximum transmission delay of the links. These assumptions are somewhat impractical for ad hoc networks. And the second weak point of this protocol is using the hash chain. In Ariadne, all nodes must know the hash chain values of all the other nodes and these hash chain values must be updated after the last value of the hash chain is used. For updating hash value, nodes must perform the public key operation. It also decreases the efficiency merits of Ariadne. The last drawback is that the intermediate nodes must add their MACs to the received route request packet. So the route request packet is much longer than that is without using security features of only adding their addresses to it.

III. ID-Based Cryptosystem

ID based cryptosystem was proposed by Shamir in 1984[13]. The essential point of ID based cryptosystem is that any string can become the public key. Shamir explained this with giving the example of the e-mail system. If Alice wants to send the encrypted mail message to Bob that has the email address of B@hotmail.com, Alice can get the public key of Bob easily by using B@hotmail.com itself. So ID based cryptosystem has the merit that all nodes participant does not need to access the public key directory.

Until a few years ago, the practical scheme that meets the concept of the ID based cryptosystem had not been proposed. But in 2001, Boneh and Franklin proposed an efficient scheme using Weil-paring [14]. After this, many researches are being performed for ID based cryptosystem and its applications.

Boneh and Franklin's scheme is based on the Weil-paring. Weil-paring works on the particular super-singular elliptic curve E / F_p and it maps the two points on the curve that are the elements of some group G_1 of order q (q is prime) to an element of G_2 in F_{p^2}.

We present only the basic property of modified Weil-paring that can be easily applicable for the cryptographic operation. The detailed description about Weil-paring is omitted.

– The basic property of modified Weil-paring $\hat{e} : G_1 \times G_1 \rightarrow G_2$[14]

1) Bilinear : For all $P,Q \in G_1$ and $a,b \in Z$, $\hat{e}(aP,bQ) = \hat{e}(P,Q)^{ab}$
2) Non-degenerate : $\hat{e}(P,P) \in F_{p^2}$ is an element of order q, in fact a generator of G_2
3) Computable : Given $P,Q \in G_1$, there exists an efficient algorithm for computing $\hat{e}(P,Q)$ and its complexity is comparable to that of the modular exponentiation in F_p

IV. Proposed Secure Routing Protocol

In this chapter, we present new secure routing protocol. Our route discovery protocol can authenticate all nodes in the routing path and need less network resource consumption than existing protocols. We apply the Boneh and Franklin's scheme to our secure routing protocol for adding the efficient security features. We assume that all nodes participate in ID based cryptosystem. In first section, we describe the environmental assumptions for our protocol and we present our secure routing protocol in second section.

1 Environment

The assumptions for our proposed protocol is described below. Each node i in the ad hoc network has the following information. It is almost exactly the same that of Boneh and Franklin's ID based cryptosystem.

*** System parameters**

- A large k-bit prime p
($p = 2 \bmod 3,\ p = 6q - 1\ (q : prime\ )$)
- An arbitrary point $P \in E / F_p$ of order q
(E: $y^2 = x^3 + 1\ over\ \mathrm{F_p}$).
- Public point $P_{pub} = sP$

*** Cryptographic hash functions**

$H_1 : F_{p^2} \rightarrow \{0,1\}^n , G : \{0,1\}^n \rightarrow F_p$,

$H_2 : \{0,1\}^n \rightarrow E / F_p$ for some n

$H_3 : \{0,1\}^n \times \{0,1\}^n \rightarrow F_q$,

$H_4 : \{0,1\}^* \rightarrow \{0,1\}^n$

*** Public information**

- Identification value : ID_i ,
it can be directly derived to public key of i , $n_i P = H_2(ID_i)$

- ID_i can be known to any one in the network
- n_i is unknown value and cannot compute it.

*** Private information**

- Private key of node i, $sn_i P$
- Private key of each node is only known to itself.

The network assumptions are as follows. The adversaries in the network cannot attack below the network layer such MAC (Medium Access Control) layer attack. And the adversaries can inject, modify, and remove the packets that are sent to them. And we assume the source node that initiate route discovery protocol and the destination node are trusted nodes.

2 Proposed Secure Routing Protocol

In this section, we describe the detailed procedure of proposed routing protocol. It consists of two parts. The one is route discovery protocol and the other is route maintenance protocol.

● Route discovery protocol

For any node S in the network, it can have the routing path information from S to the destination D to perform the following procedure. We assume the intermediate nodes in the routing path are 1~k. The form of route request packet is described in figure 1. In the route request packet, W, U, V are cryptographic parameters and seq is the sequence number of the packet that is generated and managed by each node. $Sign_A(M)$ is the result of signing a message M using a private key A. Our protocol uses the signature schemes that are proposed before[15].

$$\begin{array}{|l|}\hline < \mathrm{RReq}, SourceID, DestinationID, seq, \\ Sign_S(M), (IntermediateID-list), W, U, V> \\ (M = (\mathrm{RReq} \,\|\, SourceID \,\|\, DestinationID \,\|\, seq \,\|\, W)) \\ \hline \end{array}$$

Fig. 1 form of route request packet

A node S that initiates route discovery protocol perform the following procedure

1) Generate a random string $\sigma_S \in \{0,1\}^n$ and using its $ID_s \in \{0,1\}^n$, compute $r = H_3(ID_s, \sigma_S) \in F_q$

2) Using r generated in 1) and its private key $sn_s P$ compute the values below.

$$\hat{e}(rP, sn_s P) = g^{rsn_s} \quad (g = \hat{e}(P,P))$$

$$(\hat{e}(sP, H_2(ID_D)))^r \oplus r = (\hat{e}(sP, n_D P))^r \oplus r$$

$$= g^{rsn_s} \oplus \mathrm{r} \quad (g = \hat{e}(P,P))$$

3) Using the values generated in 1), 2) make the following packet and broadcast it.

$$< \mathrm{RReq}, ID_S, ID_D, seq, Sign_S(M), (),$$

$$rP, g^{rsn_S} \times \sigma_S, g^{rsn_d} \oplus r >$$

The intermediates node i $(1 \le i \le k)$ that receives route request packet does the followings. A received packet has the form.

$$< \mathrm{RReq}, ID_S, ID_D, Sign_S(M), seq, (ID_1, .. ID_{i-1}), W, U, V >$$

1) Verify the signature value. If it is correct, adds ID_i to the *intermediateID-list*. And the compute the new value of U by following procedure.

$$U = U \times \hat{e}(rP, sn_i P)$$

2) Rebroadcast the packets generate in 1). The content of new packet is as follows.

$$< \mathrm{RReq}, ID_S, ID_D, seq, Sign_S(M), (ID_1, ..., ID_k), W, U, V >$$

A destination node D that received routing request packet and whose ID is matched to value of *DestinationID* field in the packet performs the following procedure. The form of received route request packet is as follows.

$$< \mathrm{RReq}, ID_S, ID_D, seq, Sign_S(M), (ID_1, ..., ID_k), W, U, V >$$

1) Compute r' using private key of D and the values of packet received

$$r' = V \oplus \hat{e}(W, sn_D P)$$

2) Get the public keys of the IDs that are described in *intermediateID-list* by following computation.

$$\{n_i P \mid n_i P = H_2(ID_i), 1 \le i \le k\}$$

3) Using system parameter sP and the values computed in previous steps, compute A value.

$$A = \{\hat{e}(sP, \textstyle\sum_{i=l}^{k} n_i P)\}^r$$

4) Using A value, Compute σ' by computing $\sigma' = U \times V^{-1}$. And compare r' and $H_3(\sigma', ID_S)$ if two values are equal, go to next step and otherwise, the received packet is dropped.

5) Make the following route reply packet. It is sent through the reverse list of *intermediateID-list* in route request packet.

$$< \mathrm{RRep, seq}, (ID_S, ID_1, .., ID_k, ID_D), W, V \oplus \sigma', Sign_D(M) >$$

$$(M = (\mathrm{RouteReply} \mid \mathrm{seq} \mid ID_S \mid ID_1 \mid ... \mid ID_k \mid ID_D \mid W \mid V \oplus \sigma'),$$

$$Sign_D : signature\ of\ D)$$

After receiving the route reply packet, the intermediate nodes in routing path and source node S verify the signature of D. And if it is correct, they add the path in the packet to their route cache.

● Route maintenance protocol

Assume a node A want B to send a packet that is originated from S. If the link between A and B is broken, A sends the following route error packet to S.

$$< \mathrm{RErr, seq, (node\text{-}list\,in\,path\,from\,A\,to\,S)}, (ID_A, ID_B), Sign_A(M) >$$

$$(M = (\mathrm{RErr} \mid seq \mid \mathrm{(node\text{-}list\,in\,path\,from\,A\,to\,S)} \mid ID_A \mid ID_B))$$

The intermediate nodes in the path from A to S verify its signature and apply this information to their routing cache.

V. Security Analysis

In this chapter, we discuss the security of the proposed protocol. The first section describes the security of the cryptographic techniques used in the protocol and presents the proof sketch that is need for the integrity of the route request packet in our routing protocol being preserved.

1. Security of integrity and unforgeability

Almost all cryptographic schemes in our protocol are applied from the previous result of Boneh and Franklin's IBE scheme. The procedure of making V value in our protocol is the same that of the encryption procedure in IBE scheme. And the signature scheme used in our protocol is the result of previous research.

Therefore the security proofs of these schemes are already done in the papers that propose these schemes [14,15]. So our security proof is focused on the security of U value. In other words, the essential point of the security of our protocol is whether the active attacker can modify U value without using his private key or not. For solving this problem, we proved the following theorem.

Theorem 1. For any sum of two public keys $(n_1 + n_2)P$ that is derived by ID_1, ID_2 , one cannot find any two other ID values of ID_3, ID_4 such that

$$(n_1 + n_2)P = (n_3 + n_4)P$$

Simple proof

For the elliptic curve discrete logarithm problem, the attacker cannot know the value $n_1 + n_2$ and any n_i value from public key $n_i P$ derived by ID_i . So the attacker can use only the value $(n_1 + n_2)P$. In this case, the attacker must solve the problem of finding matched ID_i for any given value $n_i P$. But the hash function H_2 has one way-ness property. So if this property is preserved then the attacker cannot solve the problem. By these two reasons, the theorems are preserved. ■

The theorem described above can be extended to $k(\geq 2)$ public key case. By this fact, the U value used in our protocol is generated by only the nodes in the routing path described in the route request packet. So the only way to modify the *intermediateID-list* is using the private key of some node or attacker himself. But the private key is generated by only key distribution center. So if the attackers cannot pass the authentication procedure of key distribution center or cannot know the master-key value s, they cannot modify the route request packet.

The route reply packet is protected by the signature of the private key. So if the signature is not forgeable the integrity of the packet is preserved.

2. Security against resource consumption attack

Proposed protocol is using ID based cryptosystem which is one of the public key cryptosystems. So it is relatively more vulnerable than existing protocols using symmetric key cryptosystem. But the resource consumption attack can be prevented by using other network features such as counting number of packets per some duration and additional policy. For example, we make the policy such as if a node that send invalid packets for several times, or sends packets beyond agreed number of packets per a second, drop all the packets originated from the node for some times. The attacker can do the resource consumption attacks using valid packets of passing the verification procedure. But the attackers cannot get the private key unless they cannot pass the authentication procedure of the key distribution center. Although the attacker gets the private key of some user, they cannot perform resource consumption attack because performing signature operation of large packets needs much computational resources too.

VI. Performance Analysis

In this chapter we discuss the performance of proposed protocol. Our protocol has the following efficiency and functional merits that existing protocols do not have. First, our protocol enables to authenticate all nodes in the routing path. Ariadne has the same property but our protocol need less network resource than Ariande. Compared to Ariadne, our protocol needs only 4 cryptographic parameters per route request packet but the number of cryptographic parameters in the route request packet of Ariadne is proportions to number of intermediate nodes in routing path. In computational aspects, our protocol needs more computational resources than Ariadne. But Ariadne needs some time delay because it is using the time synchronization assumption. In Ariadne, they assumes maximum time synchronization error time is 0.2 seconds that is comparable to the time that is needed for performing public key operation in recent common PC.

VII. Conclusion

In this paper, we proposed a new secure routing protocol for ad hoc networks using ID based cryptosystem. It need not fixed infrastructure such as certificate authority after initial key setup procedure is done. And our protocol can authenticate all nodes in the routing path using less network resource consumption than old protocols. In the future, we will apply the ID based cryptosystem using Weil-paring to other security systems for ad hoc networks. ID based cryptosystem has the same characteristics that of ad hoc networks in not needing fixed infrastructure. In addition, It has many useful properties such as no communication being needed for two-party key agreement. Therefore, ID based cryptosystem will be able to be applied to many fields in ad hoc network security.

VIII. References

[1] David B.Johnson, "Routing in Ad Hoc Networks of Mobile Hosts",In Proceedings of the IEEE Workshop on Mobile Computing Systems and Applications (WMCS'94),pp158-163,1994.12

[2] David B.Johnson and David A. Maltz, "Dynamic Source Routing in Ad Hoc Wireless Networks", In Mobile Computing, edited by Tomasz Imielinski and Hank Korth, chapter 5, pp153-181,Kluwer Academic Publishers,1996.

[3] Lidong Zhou and Zygmunt J. Haas. Securing Ad Hoc Networks. *IEEE Network Magazine*, 13(6):24-30,1999.11.

[4] Manel Guerrero Zapata. Secure Ad hoc On-Demand Distance Vector (SAODV) Routing. IETF MANET Mailing List,
Message-ID :3BC17B40.BBF52E09@nokia.com

[5] Steven Cheung. An Efficient Message Authentication Scheme for Link StateRouting. In *13th Annual Computer Security Applications Conference*, pages 90-98,1997

[6] Ralf Hauser, Antoni Przygienda, and Gene Tsudik. Reducing the Cost of Security in Link State Routing. In *Symposium on Network and Distributed Systems Security (NDSS '97)*, pages 93-99, February 1997.

[7] Kan Zhang. Efficient Protocols for Signing Routing Messages. In *Proceedings of the Symposium on Network and Distributed Systems Security (NDSS '98)*, March 1998.

[8] Yih-Chun Hu, Adrian Perrig and David B.Johnson. Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks, MobiCom'02 , Sep. 2002

[9] Bridget Dahill, Brian Neil Levine, Elizabeth Royer, and Clay Shields,"A Secure Routing Protocol for Ad Hoc Networks.", Technical Report UM-CS-2001-037, EECS. University of Michigan, 2001.

[10] Panagiotis Papadimitratos and Zygmunt J.Haas, "Secure Routing for Mobile Ad hoc Networks" , Proc. The SCS Communication Networks and Distributed Systems Modeling and Simulation Conference, 2002.1

[11] Adrian Perrig, Ran Canetti, J.D.Tygar, and Dawn Song,"Efficient and Secure Source Authentication for Multicast",In Network and Distributed System Security Symposium,NDSS'01,pp35-46,2001.2

[12] Adrian Perrig, Ran Canetti, J.D.Tygar and Dawn Song,"Efficient Authentication and Signing of Multicast Streams over Lossy Channels", In IEEE Symposium on Security and Privacy, pp 56-73 , 2000.5

[13] A. Shamir, "Identity-based cryptosystems and signature schemes", Proc. Crypto'84 pp47-53

[14] Dan Boneh, Matthew Franklin,"ID-Based Encryption from the Weil-Pairing", Proc. Asiacrypt'02 ,2002.12

[15] K.Peterson, "ID-based Signatures from Pairings on Elliptic Curves", Cryptology-eprint-archive", 2002-04