# ad-hoc 네트워크에서의 안전한 라우팅 기법에 관한 연구

論 文
8-2-2

## A Note on a Secure Routing Method for ad-hoc Networks

황 정 연*, 김 경 신**, 김 형 중***, 이 동 훈***
Jung-Yeon Hwang, Kyung-Sin Kim, Hyoung Joong Kim, Dong-Hoon Lee

## Abstract

Kim et al. recently proposed an identity-based aggregate signature scheme to construct a secure routing protocol in ad-hoc networks. In this note, we unfortunately show that the identity-based aggregate signature scheme is universally forgeable, that is, anyone can forge the signature of any messages of its choice. This subsequently means that their secure routing protocol is not secure.

**Keywords** : Secure Routing Protocol, Authentication, ID-based Aggregate Signature, Universal Forgery

## I. 서 론

Ad-hoc 네트워크는 네트워크의 위상과 그 구성원의 변화에 대한 네트워크를 설계하는 데 있어 유용한 유연성을 제공한다. 그러나 이러한 동적 특성으로 인해 ad-hoc 네트워크는 노드 인증의 안전성에 대한 위협에 쉽게 노출될 수 있다. 따라서 ad-hoc 네트워크에서는 한 노드가 자신과 통신하는 다른 노드를 인증하기 위한 신뢰할 수 있는 라우팅 프로토콜을 설계할 필요가 있다. 그간의 연구에서 전자 서명은 네트워크상에서 (노드)인증을 얻기 위한 방법으로 주로 사용되었다. 전자 서명에서 서명자의 공개키를 아는 누구라도 서명을 검증할 수 있지만 서명자의 비밀키를 모르고 서명을 위조하는 것은 계산적으로 불가능하다.

ID 기반 모음 서명 기법(aggregate signature)은 ad-hoc 네트워크의 라우팅 프로토콜을 위한 근본적인 primitive로 사용될 수 있다[1-3]. 모음 서명 기법이란 $n$명의 사용자로부터의 메시지 $n$개와 각 메시지에 대한 서명이 주어질 때, $n$개의 모든 서명을 하나의 짧은 서명(short signature)으로 모으는 기법이며 이 때 검증자는 짧은 서명을 통해 n명의 사용자가 정말로 각자의 메시지에 대해 서명한 것임을 확신할 수 있어야 한다. 모음 서명 기법은 라우터 상의 중간 노드들을 인증하면서 서명을 목적 노드까지 전달하기 위해 생성되는 많은 서명들을 압축하는 데 사용될 수 있다. 게다가 ID 기반의 모음 서명 기법은 라우팅 프로토콜에 적용될 때 서명 목록 의 크기 및 인증서 체인의 크기와 같은 통신 오버헤드를 효과적으로 감소시킬 수 있다. 또한 공개키 기반 시설(Public Key Infrastructure)의 필요성을 없앰으로써 ad-hoc 네트워크가 갖는 부적절한 가정을 피할 수 있다.

Kim 등은 최근 ID 기반의 암호시스템을 이용해 ad-hoc 네트워크에서의 인증성 강화를 위한 안전한 라우팅 프로토콜을 제안하였다[4]. 그들은 안전한 라우팅 프로토콜의 설계를 위해 새로운 ID 기반 모음 서명 기법을 제시하였으며(편의를 위해 여기서부터는 KSY IBAS 기법이라 지칭한다) 제안한 ID 기반 모음 서명 기법을 이용하여 DSR[5] 또는 AODV[6]와 같은 on-demand 라우

접수일자 : 2009년 3월 26일
최종완료 : 2009년 5월 23일
*ETRI 선임연구원
**고려대학교
***고려대학교 정보경영공학전문대학원
교신저자, e-mail: khj-@korea.ac.kr

팅 프로토콜에 기반한 안전한 라우팅 프로토콜을 설계하였다.

본 논문에서 우리는 Kim 등의 ID 기반의 모음 서명 기법이 일반적 위조(Universal forgery)가 가능함을 보인다. 공격자는 자신이 선택한 어떠한 메시지에 대해서도 서명을 위조할 수 있다. 이는 바로 Kim 등이 설계한 ad-hoc 네트워크에서의 라우팅 프로토콜이 안전하지 않음을 의미한다.

## II. KSY IBAS 기법

본 장에서는 KSY IBAS 기법을 간단히 살피도록 한다[4]. KSY IBAS 기법은 [7]에서와 같이 bilinear map을 사용한다. $q$를 위수로 갖는 두 순환군 $G_1$, $G_2$가 있다고 가정하자. bilinear map $e: G_1 \times G_1 \rightarrow G_2$ 는 다음의 성질을 만족한다.

1. Bilinearity: $\forall P, Q \in G_1$과 $\forall a, b \in Z_q$에 대해 $e(aP, bQ) = e(P, Q)^{ab}$를 만족한다.
2. Non-degeneracy: $e(P, P) \neq 1$은 $G_2$의 생성원이 된다.
3. Computability: $P, Q \in G_1$에 대해 $e(P, Q)$를 계산할 수 있는 효율적인 알고리즘이 존재한다.

KSY IBAS 기법은 다음 여섯 개의 알고리즘으로 구성된다.

- 설정단계: 키 생성 센터(Key generation Center, KGC)는 $G_1$에서의 생성원 $P$와 마스터 비밀키 $s \in Z_q$를 선택해 $P_{pub} = sP$를 계산한다. 그리고 두 개의 해쉬 함수 $H_1: \{0,1\}^* \rightarrow Z_q$와 $H_2: \{0,1\}^* \rightarrow G_1$을 선택한다. 키 $s$는 오직 KGC만이 아는 값이며 나머지는 공개된다.
- 키생성단계: 서명자가 자신의 ID에 대한 개인키를 요청하면 KGC는 $D_{ID} = sH_2(ID)$를 계산해 서명자에게 전송한다. 이 때 서명자의 공개키는 $Q_{ID} = H_2(ID)$가 된다.
- 서명단계: 서명자의 개인키 $D_{ID}$와 메시지 $M \in \{0,1\}^*$이 주어질 때 서명자는 임의의 $r \in Z_q$을 선택해 $U = rQ_{ID}$와 $h = H_1(M)$, 그리고 $V = (r+h)D_{ID}$를 계산한다. 이 때 서명은 $\sigma = (U, V)$가 된다.
- 검증단계: $ID$와 메시지 $M$, 서명 $\sigma$가 주어질 때, 검증자는 $h = H_1(M)$와 $Q_{ID} = H_2(ID)$을 계산한 후 $e(hQ_{ID} + U, P_{pub}) \stackrel{?}{=} e(V, P)$ 를 검사한다. 두 값이 같으면 서명은 유효하며 그렇지 않은 경우 서명은 유효하지 않으며 검증자는 서명을 받아들이지 않는다.
- 모음단계: 서로 다른 메시지 $M_1, \ldots, M_{i-1}$에 대한 모음서명 $\sigma' = (U', V')$와 메시지 $M_i$에 대한 서명 $\sigma_i = (U_i, V_i)$가 주어질 때, 집합자(aggregator)는 우선 $M_i$가 나머지 메시지들과 다른지를 확인한다. 서로 다를 경우 집합자는 $U = U' + U_i \in G_1$, $V = V' + V_i \in G_1$를 계산한다. 그러면 메시지 $M_1, \ldots, M_i$에 대한 모음 서명은 $\sigma = (U, V)$가 된다.
- 모음서명검증단계: $ID_1, \ldots, ID_n$과 서로 다른 메시지 $M_1, \ldots, M_n$, 모음 서명 $\sigma = (U, V)$가 주어질 때 검증자는 $1 \leq i \leq n$인 모든 $i$에 대해 $h_i = H_1(M_i)$를 계산한다. 그리고 $e(\sum_{i=1}^{n} h_i Q_{ID_i} + U, P_{pub}) \stackrel{?}{=} e(V, P))$인지 검사한다. 검증을 통과한다면 $\sigma$에 모아진 모든 서명은 유효하며, 검증을 통과하지 않는다면 적어도 하나 이상의 서명은 유효하지 않다.

Kim 등은 위의 기법의 안전성이 Boneh[2] 등이 제시한 기법과 유사하게 증명될 수 있다고 주장한다[8]. 그러나 다음 장에서 위의 기법이 안전하지 않음을 보인다.

## III. KSY IBAS 기법에 대한 일반적 위조(universal forgery) 공격

본 장에서 우리는 KSY IBAS 기법이 안전하지 않음을 보인다. KSY IBAS 기법은 일반적 위조가 가능하여 누구라도 원하는 메시지에 대해 위조된 서명을 생성할 수 있다. 다음에서 우리는 간단한 위조 방법을 제시한다.

위조자 $F$는 $n$개의 $ID$, $ID_1, \ldots, ID_n$과 $n$개의

서로 다른 메시지 $M_1, \ldots, M_n$를 임의로 선택한다. 위조자는 임의의 $r \in Z_q$를 선택해 $V'$와 $U'$를 다음과 같이 계산한다:

$$U' = rP - \sum_{i=1}^{n} h_i Q_{ID_i}, \quad V' = rP_{pub}$$

여기서 $h_i = H_1(M_i)$이며 $Q_{ID_i} = H_2(ID_i)$이다.

제시된 위조 방식은 정확성(correctness)을 갖는다. 다음을 살핌으로서 우리는 $ID$와 메시지 $M$들에 대해 위조된 서명 $(U', V')$가 KSY IBAS 기법의 검증 식을 통과함을 볼 수 있다.

$h_i = H_1(M_i)$이고 $Q_{ID_i} = H_2(ID_1)$일 때,

$$\begin{aligned} & e(\sum_{i=1}^{n} h_i Q_{ID_i} + U', P_{pub}) \\ &= e(\sum_{i=1}^{n} h_i Q_{ID_i} + rP - \sum_{i=1}^{n} h_i Q_{ID_i}, P_{pub}) \\ &= e(rP, P_{pub}) \\ &= e(rsP, P) \\ &= e(V', P) \end{aligned}$$

## VI. 결 론

ad-hoc 네트워크의 라우팅 프로토콜을 위해 ID 기반 모음 서명 기법이 사용될 수 있다. Kim 등은 ID 기반 모음 서명을 이용한 라우팅 프로토콜을 제시하였으나 우리는 Kim 등이 제시한 ID 기반 모음 서명 기법이 일반적 위조 공격에 안전하지 않음을 보였다. 이는 Kim 등의 라우팅 프로토콜이 안전하지 않음을 의미한다.

## [ 참 고 문 헌 ]


[1] J. C. Cha and J. H. Cheon, "An Identity-based signature from gap Diffie-Hellman groups," *in Practice and Theory in Public Key Cryptography -PKC'*, pp. 18-30, 2003.

[2] C. Gentry and Z. Ramzan, "Identity-based aggregate signatures," *in Practice and Theory in Public Key Cryptography-PKC'*, pp. 257-273, 2006.

[3] A. Boldyreva, C. Gentry, A. O'Neill, and D. Yum, "Ordered multisignatures and Identity-Based sequential aggregate signatures, with applications to secure routing," *in Proceedings of the 14th ACM Conference on Computer and Communications Security,* pp. 276-285, 2007. The full version is available at www.cc.gatech.edu/aboldyre/publications.html

[4] H. Kim, J. Song, and H. Yoon, "A practical approach of ID-based cryptosystem in ad-hoc networks," *Wireless Communications and Mobile Computing*, vol 7, pp. 909-917, Wiley, 2007.

[5] D. Johson, "Routing in ad-hoc networks of mobile hosts," *in Proceedings of the IEEE Workshop on Mobile Computing Systems and Applications*, pp. 158-163, 1994.

[6] C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing," *in Proceedings of the 2nd IEEE 2003 Workshop on Mobile Computing Systems and Applications*, pp. 90-100, 2003.

[7] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," *in Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology,* pp. 213-229, 2001.

[8] D. Boneh, C. Gentry, B. Lynn, and H. Shacham "Aggregate and verifiably encrypted signature from bilinear maps," *in Proceedings of Advances in Cryptology*, pp. 416-432, 2003.


### Biography


**황 정 연**

1999년 고려대학교 수학과 졸업
2003년 고려대학교 정보보호대학원(공학석사)
2006년 고려대학교 정보보호대학원(공학박사)
2008년~2009년 고려대학교 BK21 유비쿼터스 정보보호사업단 연구교수
2009~현재 ETRI 선임연구원
<관심분야> 암호프로토콜, 정보보호이론
<e-mail> videmot@cist.korea.ac.kr



**김 경 신**

2008년 고려대학교 산업시스템정보공학과 졸업
2008년~현재 고려대학교 정보경영공학전문대학원 석사과정
<관심분야> 암호프로토콜, 정보보호이론
<e-mail> alienk2s@korea.ac.kr

**김 형 중**

1978년 서울대학교 제어계측공학과 졸업
1986년 서울대학교 제어계측공학과(공학석사)
1989년 서울대학교 제어계측공학과(공학박사)
1990년~2006년 강원대학교 교수
2006년~현재 고려대학교 정보경영공학전문대학원 교수

<관심분야> Parallel Computing, Data Compression, Steganography
<e-mail> khj-@korea.ac.kr

**이 동 훈**

1984년 고려대학교 경제학과 졸업
1987년 U. of Oklahoma 전산학과(석사)
1992년 U. of Oklahoma 전산학과(박사)
1993년~2001년 고려대학교 전산학과 교수
2001년~현재 고려대학교 정보경영공학전문대학원 교수

<관심분야> 암호이론, 암호프로토콜, 정보보호
<e-mail> donghlee@korea.ac.kr