# Ad-hoc네트워크에서 인증 아이디에 관한 연구

강서일*, 이남훈**, 이임영*
*순천향대학교 컴퓨터학부
**한국전자통신연구원 부설연구소
e-mail:kop98@sch.ac.kr

# A Study on Authentication ID in Ad-hoc Network

Seo-il Kang*,Nam-hoon Lee**, Im-yeong Lee*
*Division of Computer Science and Engineering, Soonchunhyang University
**National Security Research Institute

요 약

Ad-hoc 네트워크에서의 디바이스들의 연결은 신뢰를 기반으로 네트워크망을 구성한다. 임의 디바이스가 접근하거나 탈퇴하는 일이 빈번히 발생하므로 제 3자의 악의 적인 디바이스가 신뢰성에 대하여 공격에 대비하여 인증 및 보안 기술이 필요하다. 그러므로 기존의 인증서 및 아이디를 이용한 인증과 대칭키 및 공개키를 이용한 보안기술을 활용한다. 본 논문에서는 공유한 정보가 없는 두 디바이스가 서로의 인증 아이디를 생성하여 활용한다. 인증한 아이디를 이용하므로 상호간의 신뢰가 기반될 수 있으며, 대칭키를 생성하여 통신에 대한 보안 기술을 활용한다.

## 1. 서론

Ad-hoc 네트워크는 임의 디바이스가 무선 통신으로 이루어지는 네트워크망을 말하며, 디바이스의 참여와 탈퇴가 자유롭게 이루어지는 환경이다. 이와 같은 네트워크망의 특성에 따라 임의 사용자 접근에 대한 제한이 어려우며, 악의적인 목적을 가지고 있는 디바이스의 접근에 대한 보안이 취약하다. 그러므로 취약성을 극복하기 위한 방안으로 보안 기술을 위한 암호 키 관리 및 인증 기술에 대한 연구가 지속적으로 진행된다. 기본적으로는 보안 라우팅 프로토콜을 포함하여 통신 경로의 상황에 대한 안전성, 그리고 참여 디바이스에 대한 인증, 키 설립 방안에 대한 논의가 활발하게 이루어지고 있다. 본 논문은 아이디를 이용하는 디바이스가 상대방의 디바이스와의 통신을 통해서 인증 아이디를 생성하고 Ad-hoc 네트워크내에서는 인증 아이디를 신뢰성과 세션키 설립을 제공한다. 2장에서는 Ad-hoc 네트워크의 특성과 요구 사항에 대하여 알아보고, 기존의 연구에 대해서는 3장에서 기술한다. 제 4장에서는 인증 아이디에 대한 제안 방식 및 세션키에 대하여 기술한다. 제 5장에서는 기존의 요구 사항에 대하여 분석하고 마지막으로 결론에서는 향후 연구 방향에 대하여 논의한다.

## 2. Ad-hoc 네트워크의 요구 사항

Ad-hoc 네트워크는 임의 디바이스의 접근이 용이한 특징을 가지고 있으며, 디바이스의 접근으로 인해서 네트워크망이 유동적으로 구성된다는 것을 가장 큰 장점으로 가지고 있다. 이러한 특성은 네트워크망의 단절을 피할 수 있는 방안이다. 이와 같이 임의 디바이스간의 연결을 통해서 지속적으로 통신이 가능하지만 단점으로 네트워크 통신 경로가 매번 바뀌며, 새로운 디바이스가 참여하거나 탈퇴하는 경우가 발생한다. 이와 같은 사항으로 공유키를 이용하는 암호기술을 적용하기 어렵고, 공개키 인증서를 이용하는 경우 디바이스의 인증서를 검증하고, 통신의 연산에 있어 제약사항이 된다. 아이디 기반의 보안 기술은 상대방의 아이디를 이용하여 암호기술을 사용함으로써 공유키나 사전 정보가 필요없다. 하지만 인증 기술에 있어서는 사전 정보가 필요하게 되는데 이유는 아이디를 검증할 수 있어야 하기 때문이다. 특히 아이디, 패스워드 인증 기술은 사용자와 서비스 서버간의 인증 기술로 많이 활용된다. 하지만 Ad-hoc 네트워크의 경우 사전 인증 정보의 등록이 없기 때문에 기존의 인증 기술을 이용하기에 취약점이 존재한다. 특히 아이디와 패스워드의 사전 공유가 없는 상태에서는 아이디 기반의 인증 기술을 이용하기 어렵다. 또한 사전 정보가 공유되어 있지 않은 디바이스간의 인증은 상대방이 제공하는 정보를 활용하여야 한다. 아이디 기반의 보호 기술은 아이디를 공개키의 생성 정보나 대칭키를 생성에 이용하여 상대방과 동일한 키를 생성하여 이용할 수 있다. Ad-hoc 네트워크에서의 보안에 대한 특성은 아래와 같다.

● 디바이스 인증

디바이스의 인증을 통해서 제 3자의 위장을 막을 수 있어야 한다.

● 가입과 탈퇴에 따른 그룹 유지

네트워크에 참여하는 디바이스의 그룹 멤버를 유지할 수 있어야 한다.

● 데이터 통신의 기밀성 및 무결성

네트워크 경로를 유지하여 통신을 하는 데이터에 암호화

를 할 수 있는 세션키를 생성하여야 한다.

본 논문에서 사용하는 아디이 기반의 인증 기술은 아이디를 이용하여 상대방을 인증하며, 인증한 아이디를 이용하여 통신을 하게 된다. 인증 아이디 기술을 이용하기 위해서는 다음과 같은 사항에 만족하여야 한다.

● 공유 정보가 없는 인증 기술

임의 디바이스들간의 이루어지는 인증 기술로써 공유한 정보가 없는 상태에서 인증을 할 수 있어야 한다.

● 인증 아이디 위조

제 3자가 인증 아이디를 생성하여 이용할 수 없어야 한다.

● 인증 아이디 재사용

제 3자가 이미 사용된 인증 아이디를 사용할 수 없어야 한다.

인증 아이디는 기존의 아이디를 기반으로 해서 생성하므로 기존 아이디를 생성한 비밀 정보를 모르면 인증 아이디를 생성할 수 없다. 이를 통해서 서로 공유정보가 필요하지 않으면서 인증하는 방안에 대하여 제시한다.

## 3. 아이디 기반의 보안 기술의 동향

아이디는 이미 여러 상대에게 공개되어 알려짐으로써 활용방안에 대한 연구가 진행되어져 왔다. 특히 아이디를 기반한 공개키 생성이나 대칭키 생성을 통해서 공유한 키가 없는 상태에서 서로간의 암호 통신을 할 수 있는 방안으로 활용된다. 본 장에서는 아이디를 기반으로 하는 기존 연구 동향에 대하여 알아본다.

### 3.1 Ad-hoc 환경에서 아이디 기반의 라우팅 프로토콜

Bohio와 Miri가 발표한 논문으로 타원 쌍곡선을 이용하여 아이디 기반의 공개키를 생성하여 제공하는 방안에 대하여 제시하였다. 타원 쌍곡선의 공개키를 생성하는 점으로 해쉬한 아이디를 이용하였다. 우선 쌍곡선의 식을 $y^2 = x^3 + 1$로 정의하고, 여기에 공개키를 생성하는데 있어 입력되는 $y$의 좌표값($y_0$)을 아이디에 해쉬한 값 ($y_0 = H_1(ID)$)으로 입력하여 공개키를 다음과 같이 생성한다.

step 1. $y_0$에 대응되는 $x_0$는 $x_0 = (y^{2_0} - 1)^{1/3}$으로 연산되어 체 F에 속하게 된다.

step 2. $Q = (x_0, y_0)$는 타원 쌍곡선의 점이고 이를 이용하여 $Q_{id-x} = lQ$로 공개키를 생성할 수 있다.

그러므로 공개키는 $Q_{id-x}$가 되고, 개인키는 $l$이 된다. 이용된 점의 좌표가 아이디의 해쉬 값이므로 공개키는 아이디에 기반하여 생성되었다. 이와 같이 알려져 있는 아이디를 기반으로하여 공개키를 생성하여 제공하므로 상대방이 공개키를 이용하는 경우 자신의 아이디 기반의 값인 $Q = (x_0, y_0)$를 활용하였음을 할 수 있게 된다. 동일하게 상대방도 자신의 아이디를 이용하여 공개키를 생성하여 전송하게 된다.

### 3.2 Ad-hoc 환경에서 아이디 기반의 프레임워크

Hung-yu와 Ru-Yu가 발표한 아이디 기반의 프레임워크는 키의 생성은 3.1 방식을 이용하여 생성한다. 그러나 키의 교환에서는 서로 p의 값을 전송하여 3.1 방식보다 보안을 강화시킨다. 보안을 강화하는 방식은 아래의 단계와 같다.

step 1. 디바이스 A는 랜덤수 a를 선택하여 $P_A (= aP)$를 생성하여 전송한다.

step 2. 디바이스 B도 랜덤수 b를 선택하여 $P_B (= bP)$를 생성하여 전송한다.

step 3. 디바이스 A는 $x (= aP_B = abP)$를 연산하여 세션키 $K (= H(K_{AB} \| A \| B \| x)$를 생성한다. 이때 디바이스 B도 동일하게 $x' (= bP_A = baP)$를 통해서 동일한 세션키 $K' (= H(K_{BA} \| A \| B \| x')$를 생성할 수 있게 된다. $K_{AB}$는 다음의 연산과 같이 상대방의 공개키를 이용하여 동일하게 생성된다.

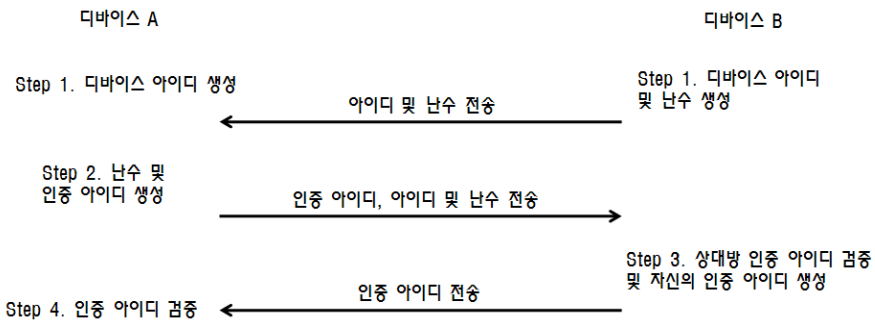
$$K_{AB} = e(S_A, P_B)e(aQ_B, P_{KGC}) = e(Q_A, P)^{bs}e(Q_B, P)^{as} = e(bQ_A, P_{KGC})e(S_B, P_A) = K_{BA}$$

이 방식에 P의 값에 랜덤 수를 곱하여 서로 교환하여 동일한 P를 이용하여 키를 생성하는 방식보다 보안을 강화시켜 세션키를 생성할 수 있게 된다.

기존의 연구의 경우를 보면 아이디를 기반하여 암호키를 생성하는 방안으로 이루어져 있다. 모두 인증은 기본적으로 아이디를 통해서 된다는 가정으로 진행되는 것이다. 이러한 경우 아이디가 위조되거나 다른 사용자의 의해 악용되는 경우 이를 검증하는 방안이 매우 어렵다는 취약점을 가지고 있다. 그러므로 본 논문에서는 아이디를 인증할 필요성을 제시하여 인증 아이디를 사용하게 되는 것이다.

## 4. 아이디를 이용한 인증 아이디 제안 방식

본 제안 방식은 Ad-hoc 네트워크에서 공유한 정보가 없는 상태에서 상호 인증을 통해서 인증 아이디를 생성하여 제공하고, 이를 통해 상대방과 정당하게 통신할 수 있는 방안에 대하여 제시한다. 인증 아이디 생성 방안으로 두 가지를 제시하는데 하나는 두 디바이스간이고 다른 하나는 다자간의 디바이스에서의 인증 아이디 방식이다. 다자간의 디바이스에서 인증 아이디 생성 방안을 제시하는 이유는 Ad-hoc 네트워크에서는 통신 경로에 여러 디바이스의 참여로 이루어지기 때문에 꼭 다자간 혹은 그룹간의 인증 방안에 대하여 제시되어야 하기 때문이다.




(그림 1) 디바이스간의 인증 아이디 제공

### 4.1 시스템 기호

본 제안 방식에서 사용되는 시스템 기호는 다음과 같다.

- * : 참여 디바이스 사용자
- $ID_*$ : 참여 디바이스 아이디
- $AID_*$ : *의 인증 아이디
- $R_*$ : *가 생성한 난수
- $t$ : 타임스탬프(년도, 날짜, 시간으로 구성됨)
- $g$ : 모듈러 함수의 밑수
- $p$ : 모듈러 함수의 법수
- $K_{**}$: *와 *간의 세션키
- $E_k[]$: k를 이용한 암호화
- $H()$: 안전한 일방향 해쉬 함수

### 4.2 두 디바이스간의 인증 방안

제안 방식은 기본적으로 아이디를 $ID_* = g^* \bmod p$로 생성한다. 모듈러를 이용하는 경우 지수의 값을 알기 어렵기 때문에 차후 지수승 값을 이용하는 방식에서 안전성을 제공할 수 있다. 제안 방식의 단계는 아래와 같다.(그림 2참조)

step 1. 디바이스 A, B는 아이디($ID_A = g^a \bmod p, ID_B = g^b \bmod p$)를 생성하고, B는 자신의 아이디($ID_B$)와 난수($R_{B_1} = g^{R_B} \bmod p$)를 전송한다.

step 2. 디바이스 A는 난수($R_{A_1} = g^{R_A t} \bmod p$)를 생성하고, 상대방의 난수($R_{B_1}$)를 이용하여 인증 아이디($AID_A = g^{aR_B} \bmod p$)를 생성하여 디바이스 B에 인증 메시지($AID_A, R_{A_1}, ID_A$)를 전송한다.

step 3. 디바이스 B는 자신의 난수($R_{B_1}$)를 이용하여 상대방의 인증 아이디를 검증하고, 디바이스 A의 난수($R_{A_1}$)를 이용하여 인증 아이디($AID_B = g^{bR_A t} \bmod p$)를 생성하여 전송한다.

검증 연산 : $AID_A \stackrel{?}{=} ID^{R_B t_A} = g^{aR_B t} \bmod p = AID'_A$

step 4. 디바이스 A는 전송받은 상대방의 인증 아이디($AID_B$)를 받아 검증한다.

검증 연산 : $AID_B \stackrel{?}{=} ID^{R_A t} = g^{bR_A t} \bmod p = AID'_B$

이후 두 디바이스는 인증된 아이디를 이용하여 통신하게 된다. 이와 같이 인증 아이디는 상호 난수에 응답값으로 생성하게 된다.

## 5. 제안 방식에 대한 보안 분석

제안 방식의 인증 아이디 생성 단계에서 제 3자가 악의적인 목적을 가지고 위조 및 재전송이 가능한지 분석한다. 또한 세션키를 이용한 통신에서 기밀성 및 무결성 제공에 대하여 검증한다.

### 5.1 인증 아이디 위조

인증 아이디를 제 3자가 위조하기 위해서는 기본 아이디 $ID_A = g^a \bmod p$에서 $a$를 변경하거나 난수 $R_{B_1}(= g^{R_B} \bmod p)$에서 $R_B$를 변경하여야 한다. 디바이스 D가 $AID_A$를 위조하기 위해서 $AID'_A = g^{a' R_B} \bmod p$를 생성하여 전송하는 경우 $ID_A = g^a \bmod p$에서 $a$가 변경되어 연산되었기 때문에 디바이스 B는 기존의 $ID_A$를 이용하여서는 $AID_A$를 검증($AID'_A = g^{a' R_B} \bmod p \neq g^{aR_B} \bmod p = ID_A R_{B1}$)할 수 없게 된다. $R_B$를 변경하는 경우는 디바이스 B가 자신이 생성한 값이므로 바로 부정이 발생하였다는 것을 알 수 있게 된다.

### 5.2 인증 아이디의 재사용

제 3자가 기존의 인증 아이디를 가지고 재사용하거나

기존 정보를 재 전송하여 인증에 대한 불법적인 행위를 할 수 있다. 그러나 이를 막기 위해서 재사용에 대하여 난수 $R_B$를 이용하여 세션시마다 새로운 인증 아이디를 생성하여야 한다. 그리고 재 전송에 대하여 대비하기 위해서 세션에 연결시 마다 $t$(타임 스탬프)를 이용하고 있다. 이로 인해 제 3자의 인증 아이디에 대한 재사용 및 재 전송은 불가능하게 된다.

### 5.3 데이터의 기밀성 및 무결성

Ad-hoc네트워크에서 4.3을 보면 디바이스간의 세션키를 생성하게 된다. 그러므로 디비이스 A와 C가 통신하는데 있어 중간 통신로 역할을 제공하는 B는 데이터에 대하여 수정 및 위조 변조를 할 수 없다. 우선 암호키를 알 수 없고 만약 변경을 시도하게 되면 해쉬의 값을 통해서 검증이 가능하기 때문이다.

표 1을 참고하면 기존의 방식은 아이디를 기반으로 암호화 키를 생성하였다. 이 방식의 장점은 알려져 있는 아이디를 이용하므로 아이디에 대한 안전성이 제공되고 암호화 키 검증에서 아이디만을 이용하기 때문에 효율성을 제공하게 된다. 그러나 아이디에 대한 검증은 이루어지 않고 아이디에 대한 정당성이 가정으로 되어 있다. 만약 제 3자가 위조한 아이디를 이용하여 암호키를 생성하고 이를 분배하는 취약점이 발생할 수 있다. 그러한 방식에 비해 제안 방식은 상호 인증을 통해서 인증 아이디를 이용하게 된다. 상호 인증을 이용하기 때문에 제 3자가 접근하기 어려운 장점을 가지고 있다. 또한 세션키는 아이디로부터 독립적이기 때문에 아이디의 생성에 취약점이 발생하더라도 세션키의 취약성으로 연결되지 않는다.

## 6. 결론 및 향후 연구 방향

본 논문은 인증 아이디를 생성하여 제공하는 것으로써 인증 아이디는 상호 인증을 제공한다. 인증 아이디를 이용하므로 식별자 정보를 사전에 공유할 필요가 없으며, 기존의 아이디를 기반하여 제공하므로 초기 아이디를 생성한 사용자를 인증 할 수 있게 된다. 이와 같은 방식을 통해서 Ad-hoc 네트워크에 참여하는 디바이스들의 인증 아이디를 성립하게 된다. 또한 세션키를 성립에 있어 인증 아이디 생성에 이용된 난수를 이용함으로 인증 아이디가 검증되면, 세션키 생성에 있어서도 안전성이 제공된다. 이와 같은 연구를 통해서 Ad-hoc 네트워크이 보안성을 강화할 수 있으며, 안전한 서비스를 위한 기초를 제공할 수 있게 된다. 그러나 향후 연구로는 인증 아이디 생성을 위해서 통신 회수 및 데이터가 증가하게 되는데 이를 효율적으로 관리할 수 있는 방안이 필요하다. 또한 세션키를 이용하므로 참여 디바이스가 증가 할수록 키 관리가 어려워지는 상황이 발생한다. 그러므로 인증 아이디에서 그룹 키를 이용하는 방식 추가되어 본 논문의 키 관리에 효율성을 제공할 수 있는 방안이 지속적으로 연구가 이루어져야 할 것으로 사료된다.

### 참고문헌

[1] Roger S. Pressman "Software Engineering A Practltiners' Approach" 3rd Ed. McGraw Hill

[1] D.Boneh, M. Franklin, "Identity-based encryption from the weil pairing", in: Advances in Cryptology-CRYPTO 2001. LNCS 2139, 2001, pp.213-229

[2] G.V.S. Raju and Rehan Akbani, "Mobile Ad Hoc Networks Security", Annual Review of Communications, Volume 58,pp.625-628.

[3] Hung-Yu chien, Ru-Yu Lin, "Improved ID-based security framework for ad hoc network", Ad hoc networks 6 (2008), pp. 47-60

[4] Jung-San Lee and chin-Chen Chang, "Secure communications for cluster-based ad hoc networks using node identities," Journal of Network and computer Applications 30 (2007), pp.1377-1396

[5] L.Chen, C. Kudla, "Identity based authenticated key agreement protocols from pairings.", Cryptology ePrint Archive, Report 2002/184, 2002

[6] Laurent Eschenauer and Virgil D.Gligor, "A key-Management Scheme for Distributed Sensor Networks", CCS'02, pp18-22, 2002

[7] M Bohio, A. Miri, " Efficient identity-based security schemes for a hoc network routing protocols", Ad hoc networks 3 (2004), pp.309-317

<표 1> 기존 방식과 기술 비교

| | 3.1 방식 | 3.2 방식 | 3.3 방식 | 제안 방식 |
|---|---|---|---|---|
| 인증 | ID 인증<br>( 가정 ) | ID 인증<br>( 가정 ) | ID 인증<br>( 가정 ) | AID 인증<br>( 상호 인증 데이터 활용 ) |
| 암호 기술 | 공개키 기반 | 공개키 기반 | 대칭키 기반 | 대칭키 기반 |
| 암호 키 생성 | 아이디 기반 | 아이디 기반 | 아이디 기반 | 아이디에서 독립적 |