Journal of Korea Multimedia Society Vol. 13, No. 8, August 2010(pp. 1202-1211)

Ad-hoc 네트워크에서 식별자를 이용한 인증 아이디에 관한 연구

문종식[†], 변상구[††], 이임영[†††]

요 약

Ad-hoc 네트워크에서 디바이스들의 연결은 신뢰를 기반으로 각 디바이스들간 네트워크망을 구성한다. 이러한 네트워크 환경에서 임의의 디바이스가 접근하거나 탈퇴하는 경우가 빈번히 발생하므로 악의적인 디바이스의 접근 및 공격에 대비하여 디바이스 인증 및 보안 기술이 필요하다. 기존의 연구는 인증서 및 아이디를 이용한 인증과 대칭키 및 공개키를 이용한 보안기술을 적용하였으나 Ad-hoc 네트워크의 특성상 공유 비밀값을 이용한 기존의 보안기술은 인증 시 디바이스의 오버헤드 및 빠른 인증 서비스를 제공하기에 많은 문제점이 발생한다. 따라서 본 논문에서는 보안 통신을 설립하는 두 디바이스간 사전에 공유한 정보 없이 식별자를 이용하여 인증 아이디를 생성하고 이를 통해 키를 설립하는 방식을 제안한다. 인증 아이디를 이용하므로 공유한 비밀정보 없이 상호간의 신뢰가 형성될 수 있으며, 대칭키 방식을 이용하여 통신에 안전성 및 효율성을 제공한다.

A Study on Authentication ID using Identifier in Ad-hoc Network

Jong Sik Moon[†], Sang-Gu Byeon[††], Im-Yeong Lee[†††]

ABSTRACT

The connection between devices in Ad-hoc network a network based on trust. Because a temporary device frequently join or leave, the authentication and security technology should be prepared for malicious device of a third-party attacks. The authentication scheme with the existing certification and ID, and the security technology using symmetric key and the public key is used. Therefore, in this paper we proposed two devices not having shared information use to generate each other's authentication ID. The use of authentication ID can establish the mutual trust and, provide security and efficiency for communication uses to generate a symmetric key.

Key words: Ad-hoc(애드혹), Authentication(인증), Device(디바이스), Identifier(식별자)

1. 서 론

Ad-hoc 네트워크는 임의의 디바이스가 무선 통신으로 이루어지는 네트워크망을 말하며 디바이스의 참여와 탈퇴가 자유롭게 이루어지는 환경이다. 이와 같은 네트워크망의 특성에 따라 임의의 사용자 접근에 대한 제한이 어려우며, 악의적인 목적을 가지고 있는 디바이스의 접근에 대한 보안이 취약하다. 따라서 이러한 보안 취약점을 해결하기 위해 인증 및 암호 키 관리에 대한 연구가 지속적으로 이루어지고

※ 교신저자(Corresponding Author) : 이임영, 주소 : 충남 아산시 신창면 읍내리 순천향대학교 멀티미디어관 607호 (336-745), 전화 : 041)542-8819, FAX : 041)530-1548, E-mail : imylee@sch.ac.kr
접수일 : 2010년 3월 3일, 수정일 : 2010년 4월 9일
완료일 : 2010년 5월 11일
[†] 준회원, 순천향대학교 컴퓨터학과 박사과정
(E-mail : jsmoon@sch.ac.kr)
[††] 준회원, 공주대학교 바이오정보학과 박사수료
(E-mail : sgbyon@hanmail.net)
[†††] 종신회원, 순천향대학교 컴퓨터학부 교수
※ 본 연구는 교육과학기술부와 한국산업기술진흥원의 지역혁신인력양성사업으로 수행된 연구 결과임.

있으며, 대표적으로 보안 라우팅 프로토콜을 포함하여 통신 경로에 대한 안전성, 참여 디바이스에 대한 인증 및 키 설립 방안에 대한 논의가 활발하게 이루어지고 있다[1,2]. 본 논문은 아이디를 이용하는 디바이스가 상대방의 디바이스와 통신을 통해서 인증 아이디를 생성하고, Ad-hoc 네트워크 내에서는 인증 아이디를 이용하여 세션키를 설립하여 신뢰성을 제공한다. 가입과 탈퇴가 빈번한 Ad-hoc 네트워크에서 서버를 이용하지 않고 디바이스간의 정보를 이용하여 인증 아이디를 생성함으로써 네트워크의 로드를 줄일 수 있으며, 안전성 및 효율성을 제공할 수 있다. 본 논문의 구성은 다음과 같다. 2장에서는 Ad-hoc 네트워크의 특성과 요구 사항에 대하여 알아보고, 기존의 연구에 대해서는 3장에서 기술한다. 4장에서는 인증 아이디에 대한 제안 방식 및 세션키에 대하여 기술한다. 5장에서는 기존의 요구 사항에 대하여 분석하고 마지막으로 6장에서는 결론 및 향후 연구 방향에 대하여 논의한다.

2. Ad-hoc 네트워크의 요구 사항

Ad-hoc 네트워크는 임의의 디바이스 접근이 용이한 특징을 가지고 있으며, 디바이스의 접근으로 인해서 네트워크가 유동적으로 구성된다는 것이 특징이며 이런 특성은 네트워크의 단절을 피할 수 있는 방안이다. 이와 같이 임의의 디바이스 간 연결을 통해서 지속적으로 통신이 가능하지만 디바이스의 이동으로 인해 네트워크 통신 경로가 매번 바뀌며, 새로운 디바이스가 참여하거나 탈퇴하는 경우가 빈번하게 발생한다. 이로 인해 공유키를 이용하는 암호기술은 적용하기 어려우며, 공개키 인증서를 이용하는 경우 디바이스의 인증서를 검증해야 하기 때문에 통신의 연산량이 증가된다. 이와 반대로 아이디 기반의 보안 기술은 공유키 및 사전 정보 없이 상대방의 아이디를 이용함으로써 안전성을 제공할 수 있다. 그러나 인증 기술은 아이디를 검증해야하기 때문에 사전 정보가 필요하다. 특히 아이디, 패스워드 인증 기술은 사용자와 서비스 서버간의 인증 기술로 많이 활용되지만 Ad-hoc 네트워크의 경우 사전 인증 정보의 등록이 없기 때문에 기존의 인증 기술을 적용하기에 어려움이 존재한다. 따라서 사전 정보가 공유되어 있지 않은 디바이스간의 인증은 통신에서 상대방이 제공하는 정보를 이용하여 제공할 수 있다. 아이디 기반 보안 기술은 아이디를 공개키 및 대칭키 생성 시 파라미터로 이용하여 상대방과 키를 설립할 수 있다. 이러한 Ad-hoc 네트워크에서의 고려해야 할 보안 요구사항은 다음과 같다.

- 디바이스 인증 : 빈번하게 가입과 탈퇴가 이루어지는 Ad-hoc 네트워크에서는 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 : Ad-hoc 네트워크에서는 통신로상의 데이터에 대한 기밀성 및 무결성에 대한 취약점이 존재할 가능성이 높다. 따라서 네트워크 경로를 유지하여 통신을 하는 데이터를 암호화 할 수 있어야 하며, 이를 제공하기 위해 세션키를 설립할 수 있어야 한다.

본 논문에서 사용하는 아이디 기반의 인증 기술은 아이디를 이용하여 상대방을 인증하며, 인증 아이디를 이용하여 통신을 하게 된다. 인증 아이디 기술을 이용하기 위해서는 다음과 같은 사항을 만족해야 한다.

- 공유 정보가 없는 인증 기술 : 임의의 디바이스들 간의 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.

3. 아이디 기반의 보안 기술의 동향

아이디는 네트워크상에서 공개되어 쉽게 알 수 있기 때문에 이를 이용하여 보안 기술을 제공하는 방안에 대한 연구가 진행되어져 왔다. 특히 아이디를 기반한 공개키 생성이나 대칭키 생성을 통해서 공유한 키가 없는 상태에서 서로간의 암호 통신을 할 수 있는 방안에 대한 많은 연구가 진행되어 왔다[3-7].

본 장에서는 아이디를 기반으로 하는 기존 연구 동향에 대하여 분석한다.

3.1 Ad-hoc 환경에서 아이디 기반의 라우팅 프로토콜

본 방식은 2004년 Bohio와 Miri가 발표한 논문으로

타원 쌍곡선을 이용하여 아이디 기반의 공개키를 통해 보안기술을 제공하는 방안에 대하여 제시하였다[8]. 타원 쌍곡선의 공개키를 생성하는 점으로 해시한 아이디를 이용하였으며, 쌍곡선의 식을 $y^2 = x^3 + 1$로 정의하고, 여기에 공개키를 생성하는데 있어 입력되는 y의 좌표값(y_0)을 아이디에 해시한 값($y_0 = H_1(ID)$)으로 입력하여 공개키를 다음과 같이 생성한다.

step 1. y_0에 대응되는 x_0는 $x_0 = (y^{2_0} - 1)^{1/3}$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 l이 된다. 이용된 점의 좌표가 아이디의 해시값이므로 공개키는 아이디에 기반하여 생성되었다. 이와 같이 알려져 있는 아이디를 기반으로 하여 공개키를 생성하여 제공하므로 상대방이 공개키를 이용하는 경우 자신의 아이디 기반의 값인 $Q = (x_0, y_0)$를 활용하였음을 알 수 있게 된다. 동일하게 상대방도 자신의 아이디를 이용하여 공개키를 생성하고 전송한다. 이와 같은 방식으로 공유한 정보가 없이도 양자간 안전성을 제공할 수 있으나 아이디에 대한 검증 과정이 없으며, 아이디를 신뢰한다는 가정을 두고 있다. 또한 임의의 공개키를 생성하여 암호키를 검증하므로 Ad-hoc 네트워크에 적용하기에 키에 대한 안전성 및 효율성이 떨어진다.

3.2 Ad-hoc 환경에서 아이디 기반의 프레임워크

2008년 Hung-yu와 Ru-Yu가 발표한 아이디 기반 프레임워크의 키 생성[9]은 기존[8] 방식의 키 생성방식을 이용한다. 그러나 키의 교환에서는 서로 P의 값을 전송하여 [8] 방식보다 안전성을 높였다. 안전성을 강화한 아이디 기반의 프레임워크 방식은 다음과 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 교환하기 때문에 동일한 P를 이용한 키 생성 방식보다 안전성을 강화시켜 세션키를 생성할 수 있다. 그러나 이 방식 역시 아이디를 검증 할 수 없어 악의적인 공격자에 의한 위장공격이 가능하다.

3.3 식별자를 이용한 클러스터 기반 방식

2007년 Lee와 Chang이 발표한 식별자를 이용한 클러스터 기반 방식[10]은 그림 1과 같이 아이디 기반의 키($K = e(\log g(MID^2)) \bmod \phi(n)$)를 생성하여 인증 및 키 분배에 이용한다. 인증 및 그룹 키 분배를 위해 클러스터가 클러스터 헤드의 아이디($CHID$) 및 자신의 아이디(CID)를 전송하면, 모바일 디바이스는 아이디 기반의 키($K = e(\log g(MID^2)) \bmod \phi(n)$) 및 세션키($K_{MH} = (CHID^2)^{H(T)*K} \bmod n$)를 생성한다. 그

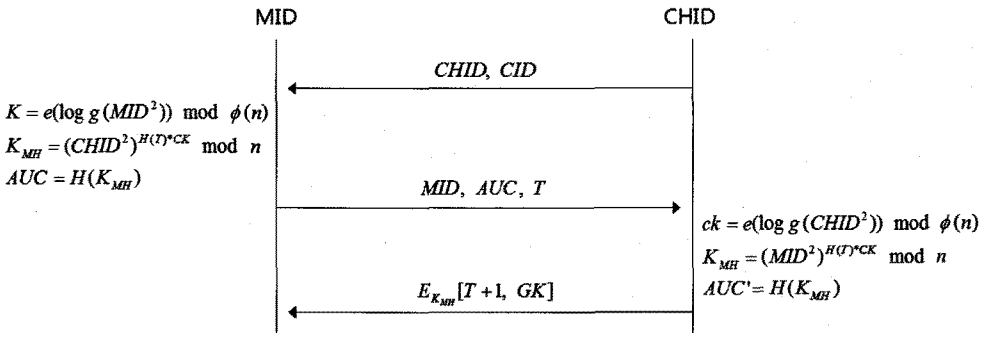

그림 1. Lee와 Chang 방식의 인증 및 그룹키 분배

리고 세션키에 해시하여 검증 값($AUC = H(K_{MH})$)을 클러스터에 전송한다.

클러스터는 AUC를 검증하고 세션키(K_{MH})로 그룹키(GK) 및 타임스탬프(T)의 증가 값을 암호화($E_{K_{MH}}[T+1, GK]$)하여 모바일 디바이스에게 전송한다. 식별자를 이용한 방식은 아이디를 기반으로 하여 암호키를 생성하며, 인증은 기본적으로 아이디를 통해서 제공된다고 가정한다. 이러한 경우 아이디가 위조되거나 다른 사용자의 의해 악용되는 경우 이를 검증하는 방안이 매우 어렵다는 취약점을 가지고 있기 때문에 본 논문에서는 아이디를 인증할 필요성을 제시하여 인증 아이디를 이용한 인증 방식을 제안한다.

4. 아이디를 이용한 인증 아이디 제안 방식

본 제안 방식은 Ad-hoc 네트워크에서 디바이스간 공유한 정보가 없는 상태에서 식별자를 이용하여 상호인증을 제공하고 인증 아이디를 통해 상대방과 정당하게 통신할 수 있는 방안에 대하여 제시한다. 인증 아이디 생성 프로토콜은 양자간 디바이스 인증 방식과 다자간 디바이스 인증 방식을 제안하였다. Ad-hoc 네트워크에서는 다수의 다바이스가 통신에 참여하기 때문에 양자간 디바이스 인증 외에 다자간 디바이스 인증 및 그룹간의 인증방식이 반드시 필요하다. 또한 상호인증 후 세션키를 설립하여 안전하게 통신을 할 수 있도록 하였다. 그림 2는 Ad-hoc 네트워크 구성 및 인증 아이디 제안 방식의 개념도이며, 그림과 같이 Ad-hoc 네트워크 디바이스는 다양한 디바이스 간의 상호 인증을 제공하고 통신할 수 있도록 한다.

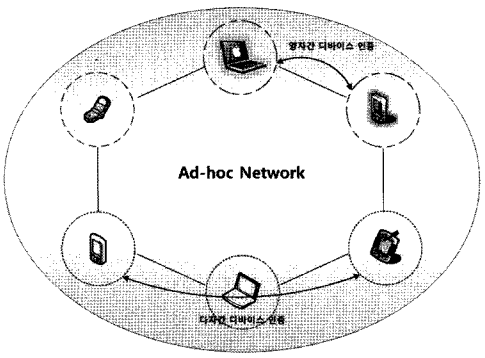

그림 2. Ad-hoc 네트워크에서의 제안 방식 개념도

4.1 시스템 파라미터

본 제안 방식에서 사용되는 시스템 파라미터는 다음과 같다.

- $*$: 참여 디바이스
- ID_* : $*$의 아이디
- AID_* : $*$의 인증 아이디
- r_* : $*$이 생성한 난수 값
- x_* : 디바이스가 생성한 비밀 값 (x_a, x_b를 a, b로 표시)
- R_* : $*$가 난수를 기반으로 생성한 인증 값
- t_* : $*$이 생성한 타임스탬프
- g : 모듈러 함수의 밑수
- p : 모듈러 함수의 법수
- K_{**} : $*$와 $*$간의 세션키
- $E_k[]$: k를 이용한 암호화
- $H()$: 안전한 일방향 해시함수

4.2 양자간 디바이스 인증 방식

양자간 디바이스 인증 방식은 Ad-hoc 네트워크의 두 디바이스 간에 상호 인증을 제공한다. 제안 방식에서 기본적으로 아이디를 디바이스가 생성한 비밀값을 지수승($ID_* = g^x \bmod p$)한 값을 이용한다. 지수승의 모듈러를 이용하는 경우 지수의 값을 알기 어렵기 때문에 양자간 디바이스 인증 방식에서 안전성을 제공할 수 있다. 제안 방식의 단계는 다음과 같으며, 그림 3은 양자간 디바이스 인증방식의 전반적인 흐름도이다.

step 1. 디바이스 A와 B는 각각 아이디($ID_A = g^a \bmod p, ID_B = g^b \bmod p$)를 생성하고, 디바이스 B는 자신의 아이디(ID_B), 난수(r_B)와 타임스탬프(t_B)를 지수승한 인증 값($R_B = g^{r_B t_B} \bmod p$)을 생성하고 디바이스 A에게 전송한다.

step 2. 디바이스 A는 자신이 난수값(r_A)과 타임스탬프(t_A)를 지수승하여 인증값($R_A = g^{r_A t_A} \bmod p$)을 생성한다. 그리고 디바이스 B에게 전송받은 인증값(R_B)에 자신의 비밀값(a)을 지수승하여 인증 아이디($AID_A = (R_B)^a = g^{a \cdot r_B t_B} \bmod p$)를 계산하고 디바이스 B에게 자신의 인증 아이디(AID_A), 인증값(R_A), 아이디를(ID_A)를 전송한다.

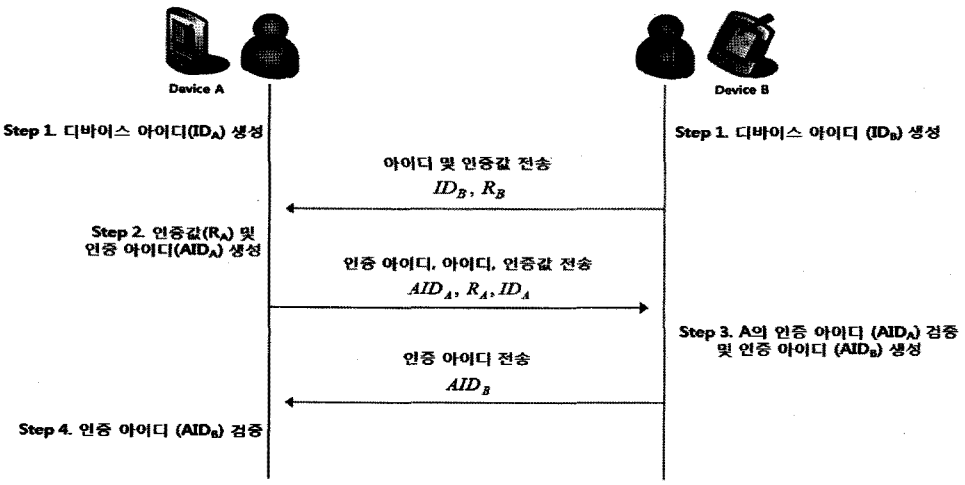

그림 3. 양자간 디바이스 인증방식 흐름도

step 3. 디바이스 B는 디바이스 A의 아이디(ID_A)에 자신의 난수값(r_B)과 타임스탬프(t_B)를 이용하여 디바이스 A의 인증 아이디($AID_A = (ID_A)^{r_B t_B} = g^{a \cdot r_B t_B} \bmod p$)를 검증한다. 그리고 전송받은 디바이스 A의 인증값(R_A)에 자신의 비밀값(b)를 지수승하여 디바이스 B의 인증 아이디($AID_B = (R_A)^b = g^{b \cdot r_A t_A} \bmod p$)를 생성하여 디바이스 A에게 전송한다.

step 4. 디바이스 A는 B로부터 전송받은 인증 아이디(AID_B)를 검증한다.

검증 연산 : $AID_B \stackrel{?}{=} AID_B' = (ID_B)^{r_A t_A} = g^{b \cdot r_A t_A} \bmod p$

이후 두 디바이스는 인증된 아이디를 이용하여 통신하게 된다. 이와 같이 인증 아이디는 상호 인증값에 응답을 통해 생성하게 된다.

4.3 다자간 디바이스의 인증 방식

Ad-hoc 네트워크의 경우 셋 이상의 디바이스가 네트워크를 구성하여 통신을 하게 된다. 따라서 네트워크에 참여하는 디바이스간의 인증이 필요하며, 이때 공유하고 있는 정보가 없는 상태에서 다자간 디바이스의 인증이 필요하다. 본 논문에서는 3개의 디바이스로 구성된 네트워크에서의 다자간 인증 방식을 설명하며, 이는 n(디바이스의 수)자간 디바이스의 인증 방식으로 확장이 가능하다. 다자간 디바이스의 인증 방식에서는 Ad-hoc 네트워크에서 이웃한 디바이스간의 인증 아이디를 이용하는 방안을 제안하였다(그림 4 참조).

step 1. 디바이스 A, 디바이스 B, 디바이스 C가 Ad-hoc 네트워크에서 상호간의 인증을 하고자 할 때, 디바이스는 각각 아이디($ID_A = g^a \bmod p$, $ID_B = g^b \bmod p$, $ID_C = g^c \bmod p$와 인증값($R_{A1} = g^{r_A t_A} \bmod p$, $R_{B1} = g^{r_B t_B} \bmod p$, $R_{C1} = g^{r_C t_C} \bmod p$)을 생성하여 브로드캐스팅한다.

step 2. 디바이스 A는 B와 C로부터 브로드캐스팅으로 전송받은 B의 인증값(R_{B1}), C의 인증값(R_{C1})에 자신의 인증값(R_{A1})과 비밀값(a)을 이용하여 인증 아이디($AID_A = (R_{A1} R_{B1} R_{C1})^a = g^{(r_A t_A + r_B t_B + r_C t_C)a} \bmod p$)를 생성한다. 또한 각 디바이스에게 전송할 검증데이터를 생성하고 디바이스 B와 C에게 자신의 인증 아이디(AID_A)와 각각의 검증 데이터를 전송한다.

검증데이터 : $(R_{A1} R_{C1})^a = g^{(r_A t_A + r_C t_C)a} \bmod p$, $(R_{A1} R_{B1})^a$

$$= g^{(r_A t_A + r_B t_B)a} \bmod p$$

step 3. 디바이스 B는 A로부터 전송받은 검증데이터($(R_{A1} R_{C1})^a$)에 자신이 아이디(ID_A), 난수값(r_B)과 타임스탬프(t_B)를 이용하여 디바이스 A의 인증 아이디(AID_A)검증한다. 그리고 A와 C로부터 브로드캐스팅으로 전송받은 A의 인증값(R_{A1}), C의 인증값(R_{C1})에 자신의 인증값(R_{B1})과 비밀값(b)을 이용하여 인증 아이디($AID_B = (R_{A1} R_{B1} R_{C1})^b = g^{(r_A t_A + r_B t_B + r_C t_C)b} \bmod p$)를 생성한다. 또한 각 디바이스에게 전송할 검증데이터를 생성하고 디바이스 A와 C에게 자신의 인증 아이디(AID_B)와 각각의 검증데이터를 전송한다.

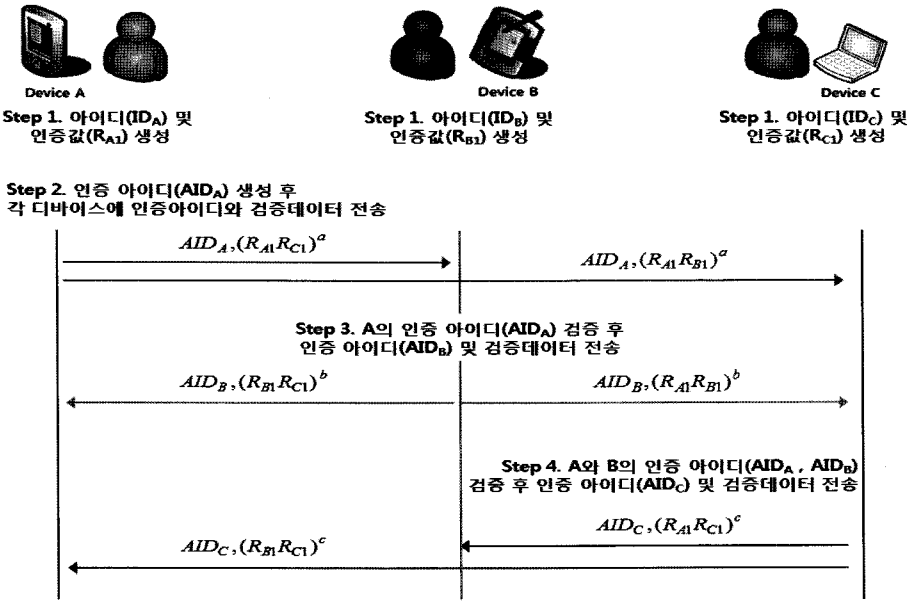

그림 4. 다자간 디바이스의 인증 방식 흐름도

검증 연산 :

$$AID_A \stackrel{?}{=} AID_A' = (R_{A1}R_{C1})^a ID_A^{r_B t_B} = g^{(r_A t_A + r_C t_C)a} g^{a r_B t_B} \bmod p$$

$$= g^{(r_A t_A + r_B t_B + r_C t_C)a} \bmod p$$

검증데이터 : $(R_{A1}R_{B1})^b = g^{(r_A t_A + r_B t_B)b} \bmod p, (R_{B1}R_{C1})^b$

$$= g^{(r_B t_B + r_C t_C)b} \bmod p$$

step 4. 디바이스 C는 A와 B로부터 전송받은 검증데이터($(R_{A1}R_{C1})^a$, $(R_{A1}R_{B1})^b$)를 기반으로 디바이스 A의 인증 아이디(AID_A)와 디바이스 B의 인증 아이디(AID_B)를 검증한다. 그리고 자신의 인증 아이디($AID_C = (R_{A1}R_{B1}R_{C1})^c = g^{(r_A t_A + r_B t_B + r_C t_C)c} \bmod p$)와 검증데이터를 생성한 후, 디바이스 A와 B에게 전송한다.

검증 연산 :

$$AID_A \stackrel{?}{=} AID_A' = (R_{A1}R_{B1})^a ID_A^{r_C t_C} = g^{(r_A t_A + r_B t_B)a} g^{a r_C t_C} \bmod p$$

$$= g^{(r_A t_A + r_B t_B + r_C t_C)a} \bmod p$$

$$AID_B \stackrel{?}{=} AID_B' = (R_{A1}R_{B1})^b ID_B^{r_C t_C} = g^{(r_A t_A + r_B t_B)b} g^{b r_C t_C} \bmod p$$

$$= g^{(r_A t_A + r_B t_B + r_C t_C)b} \bmod p$$

검증데이터 : $(R_{A1}R_{C1})^c = g^{(r_A t_A + r_C t_C)c} \bmod p$, $(R_{B1}R_{C1})^c$

$$= g^{(r_B t_B + r_C t_C)c} \bmod p$$

이와 같이 디바이스간의 인증 아이디를 이용하여 상호 공유 정보가 없이도 인증이 가능하다.

4.4 다자간 디바이스의 세션키 생성

인증 아이디를 통해서 다자간 상호 인증을 하게 되면 세션키를 설립하여 통신로상의 데이터를 안전하게 암호화하고 전송할 수 있다. 세션키는 이미 브로드캐스팅된 인증값을 이용하여 생성하게 된다. 본 논문에서는 디바이스 A와 디바이스 C간의 세션키 생성을 설명하며, 디바이스 A와 C의 통신은 다음과 같다(그림 5 참조).

step 1. 디바이스 A와 C는 상호간의 인증 아이디(AID_A, AID_C)를 검증하여 가지고 있으며, 4.3의 step 1에서 브로드캐스팅된 각각의 인증값($R_{A1} = g^{r_A t_A} \bmod p$, $R_{C1} = g^{r_C t_C} \bmod p$)을 보유하고 있다. 디바이스 A는 디바이스 C의 인증값(R_{C1})에 자신의 난수(r_A)와 타임스탬프(t_A)를 지수승하여 세션키($K_{AC} = (R_{C1})^{r_A t_A} \bmod p = g^{r_A t_A r_C t_C} \bmod p$)를 생성한 후 자신의 인증값($R_{A1}$)과 타임스탬프($t_A$)를 이용하여 새로운 인증값($R_{A2} = g^{R_{A1} t_A} \bmod p$)을 계산한다. 그리고 갱신된 인증값($R_{A2}$)을 세션키로 암호화하고 해시한 인증값($H(R_{A2})$)과 인증 아이디를 디바이스 B에게 전송한다.

step 2. 디바이스 B는 전송된 데이터의 인증 아이디를 확인하고 디바이스 C에서 전송되는 내용임을 알 수 있다. 그러므로 전송 받은 데이터를 그대로 통과시켜 디바이스 C에 전송한다.

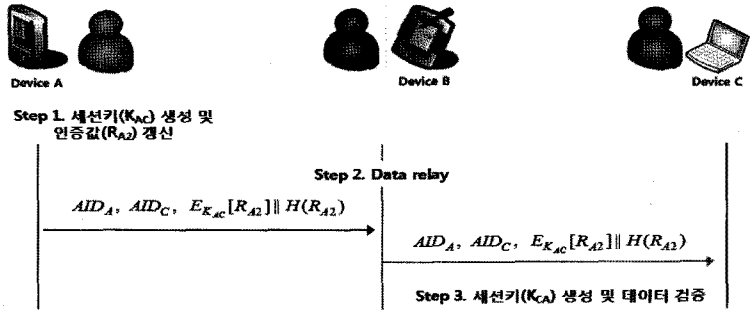

그림 5. 세션키 생성 흐름도

step 3. 디바이스 C는 A의 인증값(R_{A1})에 자신의 난수(r_C)와 타임스탬프(t_C)를 지수승하여 세션키 ($K_{CA} = (R_{A1})^{r_C t_C} \bmod p = g^{r_A t_A r_C t_C} \bmod p$)를 생성한 후, 세션키로 암호화한 갱신된 인증값을 복호화하고 해시값을 검증한다. 동일한 해시값을 검증하게 되면 세션키가 올바르게 생성되었다는 것을 알 수 있고, 이후 디바이스 A와 통신하는 데이터를 세션키로 암호화하여 전송한다.

5. 제안 방식에 대한 보안 분석

제안 방식의 인증 아이디 생성 단계에서 제 3자가 악의적인 목적을 가지고 위조 및 재전송공격이 가능한지 분석하며, 세션키를 이용한 통신에서 기밀성 및 무결성 제공에 대하여 검증한다. 또한 기존 방식과 인증 및 통신에 따른 연산량을 비교분석한다.

5.1 인증 아이디 위조

인증 아이디를 제 3자가 위조하기 위해서는 기본 아이디 $ID_A = g^a \bmod p$에서 a를 변경하거나 인증값 $R_B (= g^{r_B t_B} \bmod p)$에서 r_B를 변경하여야 한다. 공격자 디바이스가 AID_A를 위조하기 위해서 $AID_A' = g^{a' r_B t_B} \bmod p$ 를 생성하여 전송하는 경우 $ID_A = g^a \bmod p$에서 a가 변경되어 연산되었기 때문에 디바이스 B는 기존의 ID_A를 이용하여서는 AID_A를 검증 ($AID_A' = g^{a' r_B t_B} \bmod p \neq g^{a r_B t_B} \bmod p = ID_A R_B$)할 수 없게 된다. r_B를 변경하는 경우는 디바이스 B가 자신이 생성한 값이므로 바로 부정이 발생하였다는 것을 알 수 있게 된다. 인증 아이디는 디바이스의 아이디를 기반으로 생성하므로 아이디를 생성할 때 입력한 비밀 정보를 모르면 공격자는 인증 아이디를 생성할 수 없다.

5.2 인증 아이디의 재사용

제 3자가 기존의 인증 아이디를 가지고 재사용하거나 기존 정보를 재전송하여 인증에 대한 불법적인 행위를 할 수 있다. 그러나 이를 막기 위해서 인증값(R)을 이용하여 세션시마다 새로운 인증 아이디를 생성하여야 한다. 그리고 재전송에 대하여 대비하기 위해서 세션에 연결할 때마다 타임 스탬프(t)를 이용하고 있다. 이로 인해 제 3자의 인증 아이디에 대한 재사용 및 재전송공격으로 부터 안전하다.

5.3 데이터의 기밀성 및 무결성

제안 방식에서는 Ad-hoc 네트워크에서 디바이스 간의 세션키를 생성하게 된다. 그러므로 디바이스 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 해시값을 통해서 검증이 가능하기 때문이다.

5.4 제안 방식과 기존 방식의 비교

표 1을 참고하면 기존의 방식은 아이디를 기반으로 암호키를 생성하였다. 이 방식의 장점은 알려져 있는 아이디를 이용하므로 아이디에 대한 안전성이 제공되고 암호키 검증에서 아이디만을 이용하기 때문에 효율성을 제공하게 된다. 그러나 아이디에 대한 검증은 이루어지 않고 아이디에 대한 정당성이 가정으로 되어 있다. 따라서 제 3자가 위조한 아이디를 이용하여 암호키를 생성하고 이를 분배하는 취약점이 발생할 수 있다. 이러한 방식에 비해 제안 방식은

표 1. 기존방식과 제안방식 기반 기술 비교

	3.1 방식[8]	3.2 방식[9]	3.3 방식[10]	제안 방식
인증	ID 인증 (가정)	ID 인증 (가정)	ID 인증 (가정)	AID 인증 (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

상호 인증을 통해서 인증 아이디를 이용함으로써 안전성을 제공한다.

또한, 제안방식은 상호 인증을 이용하기 때문에 제3자가 접근하기 어려우며, 세션키는 아이디로부터 독립적이기 때문에 아이디의 생성에 취약점이 발생하더라도 세션키의 취약성으로 연결되지 않는다. 표 2에서 기존방식과 제안방식의 안전성을 비교하면 제안 방식은 기존의 방식의 인증 기술 부분을 상호 인증으로 제시하였으며, 사전의 공유 정보가 없는 상태에서 인증 아이디를 생성할 수 있도록 진행된다. 그러므로 본 방식은 Ad-hoc 네트워크에서 임의의 디바이스가 접근하는 경우에도 인증 기술을 활용할 수 있게 된다.

5.5 인증 및 통신에 따른 연산량 분석

기존 방식 중 식별자를 이용한 클러스터 기반 방식[10]과 인증 및 통신에 따른 연산량을 분석하면 표 3과 같다. 기존 방식은 디바이스 인증 시 디바이스간 인증 방식이 아닌 클러스터 기반 인증 방식을 사용하고 있다. 디바이스 인증에 따른 연산량을 비교하면 제안 방식에 비해 대칭키 연산 및 해시함수 연산량이 높으며, 동일 네트워크 디바이스간 데이터 암호화 통신 시 클러스터를 거쳐 통신하므로 제안 방식에 비해 통신 연산량이 높다. 또한 기존 방식은 서로 다른 네트워크에 속해있는 디바이스 간 통신 시 각 네트워크에 존재하는 클러스터를 이용하여 통신함으로써 디바이스 간 통신에 매우 높은 연산을 수행한다. 그러나 제안 방식은 디바이스간 인증에는 지수승 연산만을 이용하여 안전성을 제공하며, 디바이스간 통신 시 동일 네트워크 및 서로 다른 네트워크 디바이스와 통신 하더라도 동일한 연산량을 가진다. 그림 6과 그림 7은 이를 기반으로 디바이스 인증 및 통신량 비교 분석 결과이며, 서로 다른 네트워크 디바이스간 통신은 기존 방식과 제안 방식 모두 초기 설립 메시지 통신량은 동일하기 때문에 통신량 측정에서 제외한다. 디바이스 인증에 따른 연산량은 제안방식이 기존 방식보다 지수승 연산을 많이 사용하여 인증 당시 통신량이 많은 것을 볼 수 있으나, 제안방식이 인증

표 2. 기존방식과 제안방식의 안전성 비교

	3.1 방식[8]	3.2 방식[9]	3.3 방식[10]	제안 방식
인증	△ (ID 신뢰 가정)	△ (ID 신뢰 가정)	△ (ID 신뢰 가정)	○ (상호 인증)
암호키 검증	△ (임의 공개키 생성)	△ (임의 공개키 생성)	○ (ID로 키 검증)	○ (난수 데이터로 키 검증)
데이터 기밀성 및 무결성	○ (세션키 제공)	○ (세션키 제공)	○ (세션키 제공)	○ (세션키 제공)

[○ : 제공, 안전성 높음 △ : 부분적 제공, 안전성 취약]

표 3. 인증 및 통신량에 따른 연산량 분석

	디바이스 인증에 따른 연산량	동일 네트워크 디바이스간 통신 연산량	서로 다른 네트워크 디바이스간 통신 연산량
3.3 방식[10]	$2\alpha + 4\beta + 4\delta$	$8\beta + 2\delta$	$12\beta + 2\delta$
제안 방식	8α	2β	2β

[α : 지수승 연산량, $\beta\beta$: 대칭키 연산량, $\delta\delta$: 해시함수 연산량]

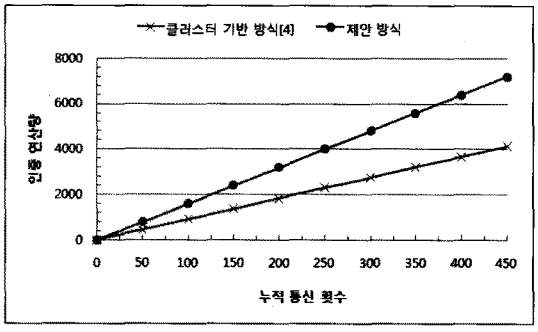

그림 6. 디바이스 인증에 따른 연산량 비교

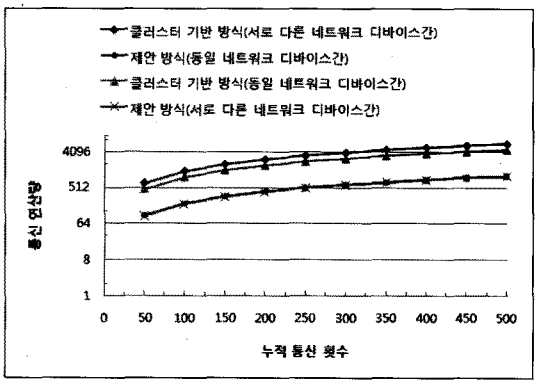

그림 7. 네트워크 디바이스간 통신 연산량 비교

이후에 통신량을 보면 동일 네트워크 디바이스간 통신 및 서로 다른 네트워크 디바이스간 통신 시 훨씬 낮은 것을 볼 수 있다. 인증은 통신 초기에 한번 발생하기 때문에 전체 통신량을 고려하였을 때 기존 방식보다 연산량 측면에서 효율성이 좋다. 향후 인증 통신량 측면에서의 연산량 감소를 고려하여 전체적인 통신 효율성을 고려해야 할 것으로 사료된다.

6. 결론 및 향후 연구 방향

본 논문은 Ad-hoc 네트워크에서 인증 아이디를 생성하여 통신함으로써 상호 인증을 제공한다. 인증 아이디를 이용하므로 식별자 정보를 사전에 공유할 필요가 없으며, 기존의 아이디를 기반으로 제공하므로 초기 아이디를 생성한 사용자를 인증 할 수 있게 된다. 이와 같은 방식을 통해서 Ad-hoc 네트워크에 참여하는 디바이스들의 인증 아이디를 성립하게 된다. 또한 세션키 설립에 있어 인증 아이디 생성에 이용된 난수를 이용함으로 인증 아이디가 검증되면, 세션키 생성에 있어서도 안전성이 제공된다. 이와 같은 연구를 통해서 Ad-hoc 네트워크의 안전성을 강화할 수 있으며, 안전한 서비스를 위한 기초를 제공할 수 있게 된다. 그러나 향후 연구로는 인증 아이디 생성을 위해서 통신 횟수 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 방식이 추가되어 본 논문의 키 관리에 효율성을 제공할 수 있는 방안 및 Ad-hoc 그룹키 및 그룹 관리에 관한 방안이 지속적으로 연구가 이루어져야 할 것으로 사료된다.

참 고 문 헌

[1] G.V.S. Raju and Rehan Akbani, "Mobile Ad Hoc Networks Security," International Engineering Consortium, Annual Review of Communications, Vol. 58, pp. 625-628, 2006.

[2] Wang changda and Ju shiguang, "Multilevel security model for ad hoc networks," *J. of Systems Engineering and Electronics*, Vol. 19, No.2, pp. 391-397, 2008.

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

[4] L. Chen and C. Kudla, "Identity based authenticated key agreement protocols from pairings," 16th IEEE Security Foundations Workshop, pp. 219-233, 2002.

[5] Laurent Eschenauer and Virgil D.Gligor, "A key-Management Scheme for Distributed Sensor Networks," Conference on Computer and Communications Security, pp. 41-47, 2002.

[6] Michael Steiner, Gene Tsudik, and Michael Waidner, "Diffie-Hellman key Distribution Extended to Group communication," Conference on Computer and Communications Security, pp. 31-37, 1996.

[7] Vijay Varadharajan, Rajan Shankaran, and Michael Hitchens, "Security for cluster

based ad hoc networks," *J. of Computer Communications*, Vol.27, No.5, pp. 488-501, 2005.

[8] M. Bohio and A. Miri, "Efficient identity-based security schemes for a hoc network routing protocols," *J. of Ad hoc networks*, Vol.2, No.3, pp. 309-317, 2004.

[9] Hung-Yu chien and Ru-Yu Lin, "Improved ID-based security framework for ad hoc network," *J. of Ad hoc networks*, Vol.6, No.1, pp. 47-60, 2008.

[10] Jung-San Lee and Chin-Chen Chang, "Secure communications for cluster-based ad hoc networks using node identities," *J. of Network and computer Applications*, Vol. 30, No.4, pp. 1377-1396, 2007.

문 종 식

2006년 2월 순천향대학교 정보기술공학부 학사
2008년 2월 순천향대학교 컴퓨터학과 석사
2008년 3월~현재 순천향대학교 컴퓨터학과 박사과정
관심분야 : AAA, 키 관리, IPTV 보안, Ad-Hoc 인증,

변 상 구

1989년 2월 계명대학교 전자계산학과 학사
1989년 1월~2000년 2월 대우통신(주) 종합연구소 선임연구원
2000년 2월~현재 프롬투정보통신(주) 기술본부 본부장
2004년 2월 공주대학교 응용수학과 석사
2007년 3월~2009년 8월 공주대학교 바이오정보학과 박사수료
관심분야 : 정보보호, 응용수학, 암호키 관리, 임베디드 솔루션

이 임 영

1981년 2월 홍익대학교 전자공학과 학사
1986년 2월 오사카대학 통신공학전공 석사
1989년 2월 오사카대학 통신공학전공 박사
1989년 1월~1994년 2월 한국전자통신연구원 선임연구원
1994년 3월~현재 순천향대학교 컴퓨터학부 교수
관심분야 : 암호이론, 정보이론, 컴퓨터보안