Journal of Korea Multimedia Society Vol. 12, No. 4, April 2009(pp. 540-549)

Ad-hoc 네트워크에서 모바일 디바이스 아이디 기반의 그룹 키 관리에 대한 연구

강서일[†], 이남훈[††], 이임영[†††]

요 약

Ad-hoc 네트워크는 모바일 디바이스가 무선 통신을 이용한 데이터를 전송 및 서비스를 제공한다. Ad-hoc 네트워크에서의 모바일 디바이스는 안전한 통신을 위해 인증과 암호 키 관리가 필요하다. 본 논문에서는 Ad-hoc 네트워크에서 인증과 그룹 키 관리의 동향에 대하여 알아보고, 아이디 기반의 상호 인증 및 그룹 키 설립 방안에 대하여 제안한다. 제안 방식의 아이디 기반의 상호 인증은 공유한 정보가 없는 상태에서 영지식을 이용하고, 세션 키 및 그룹 키를 설립하는데 활용된다. 또한 제안 방식을 Ad-hoc 네트워크에 적용하여 효율성 및 보안 기술에 대해 안전성을 높인다.

A Study on Group Key Management based on Mobile Device ID in Ad-hoc network

Seo-il Kang[†], Nam-hoon Lee[††], Im-Yeong Lee[†††]

ABSTRACT

An arbitrary mobile device configures Ad-hoc network to provide the transmission of a data and services using wireless communications. A mobile device requires authentication and encryption key management to securely communicate in the Ad-hoc network. This paper examines the trend of the authentication in the Ad-hoc network and the group key management and suggests the plan for ID-based mutual authentication and group key establishment. ID-based mutual authentication in proposed scheme uses zero knowledge in the absence of shared information and is applied to establish a session key and group key. In addition, the proposed scheme is applied to Ad-hoc network to increase the efficiency and the safety of security technology.

Key words: Group key management(그룹키 관리), authentication(인증), zero knowledge(영지식), Ad-hoc network(애드혹 네트워크)

1. 서 론

Ad-hoc 네트워크는 모바일 디바이스가 임의 네트워크망을 구성하여 데이터를 전송하는 것이다. 현재 게임 디바이스 및 휴대폰 디바이스간 연결에 활용이 높다. Ad-hoc 네트워크 연구는 기본적으로 안전한 라우팅, 인증 및 세션키 분배 방안에 대하여 진행되고 있다. 라우팅은 동적 네트워크 구성의 특성을 반영해야하고, 인증은 임의 디바이스간에 이루어질 수 있어야 한다. 세션키의 경우 참여 디바이스간에 이루

※ 교신저자(Corresponding Author) : 이임영, 주소 : 충남 아산시 신창면 읍내리 646(336-745), 전화 : 041) 542-8819, FAX : 041)530-1548, E-mail : imylee@sch.ac.kr
접수일 : 2008년 10월 10일, 완료일 : 2009년 2월 24일
[†] 준회원, 순천향대학교 컴퓨터공학부
(E-mail : kop98@sch.ac.kr)
[††] 정회원, 한국전자통신연구원 부설 연구소
(E-mail : nhlee@ensec.re.kr)
[†††] 종신회원, 순천향대학교 컴퓨터공학부 교수
※ "본 연구는 교육과학기술부와 한국산업기술재단의 지역혁신인력양성사업으로 수행된 연구결과임."

어져야 하며, 그룹 키는 가입과 탈퇴에 따른 보안 요구 사항을 만족시켜야 한다. Ad-hoc 네트워크이 참여하는 디바이스가 공통적으로 사용할 수 있는 것 중 하나가 아이디가 되며, 공유 정보가 없는 상황에서도 알 수 있다. 다음과 같이 Ad-hoc 네트워크의 인증 기술 분류는 아이디와 공개키 인증서, 그리고 공유 비밀 키 정보로 나누어진다[1-3].

1.1 Ad-hoc 네트워크의 인증 기술

인증은 네트워크 구성의 모바일 디바이스가 정당한지 확인하는 것으로 제 3자의 악의적인 모바일 디바이스가 접근하는 것을 막을 수 있는 방안이다. 다음과 같은 인증 기술이 많이 활용된다.

1.1.1 공개키 인증서

공개키 인증서를 이용하는 경우 신뢰된 기관이 공개키에 대해 전자서명을 제공하므로 인증을 제공하는데 편리하다. 그러나 인증서의 체인을 따라 공개키에 대한 전자 서명을 확인할 수 있어야 하며, 동적인 Ad-hoc 네트워크에서 활용하는데 있어 제약 사항이 될 수 있다.

1.1.2 공유 비밀 키

모바일 디바이스간의 마스터 키처럼 공유한 비밀키를 가지고 인증 메시지를 생성한다. 공유한 비밀키는 당사자만 확인만 가능하기 때문에 인증을 제공할 수 있으며, 세션 키를 성립하는데 있어서도 유용하게 활용된다. 그러나 모바일 디바이스 접근이 자유로운 Ad-hoc 네트워크에서는 비밀 키를 공유하기는 어렵다. 그러므로 비밀 키 공유방식은 실제 환경에 적용하기 힘들다. 만약 적용 할 수 있는 방안을 모색한다면 동일한 모바일 디바이스의 경우 모바일 디바이스 제조 업체에서 마스터 키를 삽입하거나 모바일 디바이스에 장착하는 칩을 이용하여 공유할 수 있다.

1.2 Ad-hoc 네트워크의 그룹 키 동향

Ad-hoc 네트워크 망을 구성하면 하나의 그룹으로 무선 통신 및 서비스를 활용할 수 있다. 그룹 내에서 통신의 효율성을 위해 그룹 키를 활용한다. 그룹 키의 경우 그룹내의 인증된 디바이스간의 키를 분배하여 이용하므로 세션 키를 이용하는 것보다 키 관리 및 통신 측면에서 효율성을 제공한다[1,4,5,9,-12].

본 논문은 2장에 기존의 연구 동향에 대하여 알아보고 3장에서 아이디 기반의 인증 및 그룹 키 방식을 제시하며, 4장에서 제안 방식을 분석한다. 그리고 마지막 장에서는 결론 및 향후 연구 방향에 대하여 논의 한다.

2. 연구 동향

Ad-hoc 네트워크의 보안 기술에 대한 연구 동향으로 인증과 그룹 키의 보안 기술에 대하여 기술한다.

2.1 클러스터 기반 방식

Varadharajan et al.s가 발표한 클러스 기반 방식은 모바일 디바이스와 클러스터로 구성되며, 클러스터에는 모바일 디바이스의 정보가 등록되고 전자서명 및 세션 키를 제공한다[6]. 그러므로 클러스터는 신뢰 객체라는 가정이 필요하다.

2.1.1 시스템 계수

Varadharajan et al.s 방식에서 사용되는 시스템 계수는 다음과 같다.

- CERT : 공개키 인증서
- mh : 모바일 디바이스
- T : 시간
- N : 난수
- HID : 클러스터 아이디
- SIG : 전자 서명 데이터
- ID : 모바일 디바이스 아이디
- H( ) : 안전한 일방향 함수로써 해쉬 함수
- GSK : 그룹키
- Kpvt : 개인키
- Kpub : 공개키

2.1.2 인증 과정

모바일 디바이스는 클러스터에 인증서($CERT_{mh}$)와 정보(mh)를 등록하기 위한 메시지($CERT_{mh}, mh, T, N, HID, SIG_{mh}$)를 전송한다. 클러스터는 전송 받은 메시지에서 전자 서명($SIG_{mh} = \mathrm{T,N,HID,IDK_{pvt-mh}}$)을 확인하여 메시지를 인증하게 된다. 클러스터는 응답 메시지로 그룹 키(GSK)와 세션 키(K_{HID-mh})를 모

바일 디바이스의 공개키로 암호화($K_{pub-mh}[GSK, K_{HID-mh}]$)하고 데이터를 검증할 수 있게 전자 서명($SIG_{HID} = \mathrm{GSK, K_{HID-mh}, ID, mh, T}, N+1\mathrm{K_{pvt-HID}}$)을 하여 제공한다.

2.1.3 세션키 설립 과정

통신을 원하는 모바일 디바이스는 클러스터를 통해 난수를 송/수신하고 세션키를 생성한다. 그림 1은 모바일 디바이스(A, B)간의 세션키 설립 과정을 보여준다. 그림 1에서 모바일 디바이스는 세션키의 설립에 필요한 정보(KS_1, KS_2)을 클러스터를 통해서 전송한다. 세션키 $KS(f(KS_1, KS_2))$를 설립한 다음 서로 암호화 된 메시지를 전송하게 된다. 그러나 클러스터가 세션키 설립 정보(KS_1, KS_2)를 알게 되어 세션키(KS)를 생성하여 도청할 가능성이 존재한다.

2.2 식별자를 이용한 클러스터 기반 방식

Jung-san Lee와 chin-chang가 발표한 식별자를 이용한 클러스터 기반 방식은 아이디 기반의 키($K = e(\log g(MID^2)) \bmod \phi(n)$)를 생성하여 인증 및 키 분배에 이용한다[7].

2.2.1 시스템 계수

Jung-san Lee와 chin-chang가 발표한 방식에서 사용되는 시스템 계수는 다음과 같다.

- MID : 모바일 디바이스 아이디
- CHID : 클러스터 헤드 아이디
- CID : 클러스터 아이디
- K_* : *간의 공유한 세션키

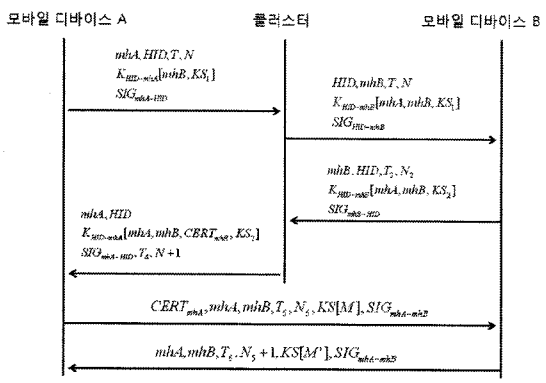


그림 1. 클러스터 기반 방식 세션키 설립 과정

- AUC : 세션키 인증 값
- GK : 그룹키
- $H()$: 안전한 일방향 해쉬 함수
- T : 타임스탬프

2.2.2 모바일 디바이스의 인증 및 그룹 키 분배

인증 및 그룹 키 분배를 위해 클러스터가 클러스터 헤드 아이디(XD) 및 자신의 아이디(CID)를 전송한다. 그러면 모바일 디바이스는 아이디 기반의 키($K = e(\log g(MID^2)) \bmod \phi(n)$) 및 세션키($K_{MH} = (\mathrm{CHID}^2)^{\mathrm{H(T)*K}} \bmod n$)를 생성한다. 그리고 세션키에 해쉬를 하여 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 전송한다(그림 2 참조).

2.2.3 모바일 디바이스간의 세션키 설립

Jung-san Lee, chin-chang 방식에서는 통신 환경에 따라 세션키 설립 방법을 다르게 한다. 대상의 모바일 디바이스가 한 홉내에 있는 경우 당사자간의 세션키를 설립하고, 한 홉 이상 떨어진 경우는 클러스터를 통해서 세션키를 설립한다. 그림 3는 통신 환경에 따른 세션키 설립 방식을 보여 주고 있다. 그러나 한 홉이상 떨어진 모바일 디바이스간의 통신에서는 클러스터를 통해 난수를 송/수신하므로 2.1 방식과 동일한 클러스터의 도청 문제가 존재한다.

2.3.1 키 분배 시스템

1982년도에 Ingemarsson외 2명이 발표한 그룹 키 생성 방식으로 다자간의 지수승 연산을 이용한다[1]. 초기 그룹 키 생성 과정을 보면 원형으로 돌아가면서 지수승 값을 통신하는 모바일 디바이스에게 전송하여 공유하게 되고 동일한 그룹 키를 생성한다(그림

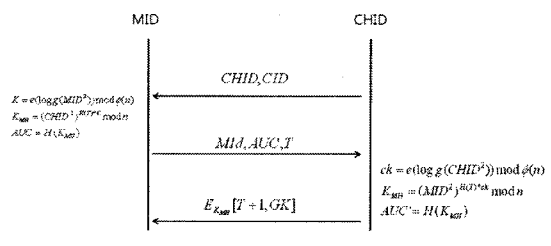


그림 2. 식별자를 이용한 클러스터 방식의 인증 및 그룹 키 분배

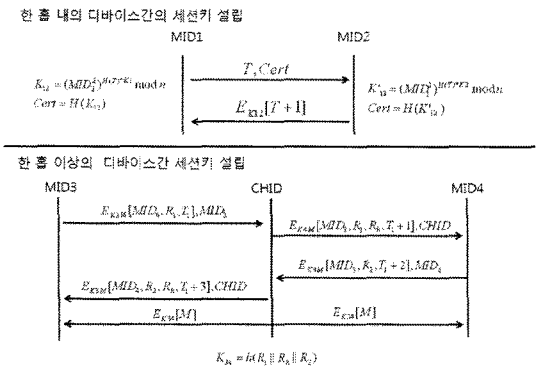


그림 3. 식별자를 이용한 클러스터 방식의 세션키 생성

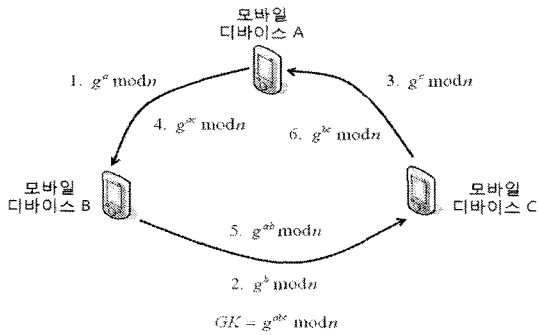


그림 4. 키 분배 시스템의 흐름도

4 참조). 새로운 모바일 디바이스의 가입이나 탈퇴의 경우 모든 모바일 디바이스가 통신에 참여하여 다시 그룹 키를 갱신하여야 한다.

2.3.2 D-H 그룹 키 분배 방식

Mischeal steiner외 2명은 D-H을 이용한 그룹키 분배 방식으로 순차적으로 그룹 키 생성에 필요한 인자를 분배하는 방식으로 모바일 디바이스는 각각의 전송된 값을 통해서 그룹 키를 생성한다[8]. 그림 5에서 키 동의를 통한 그룹 키 생성 방식을 보여 준다. 참여 디바이스 개수가 동일한 경우 2.3.1 방식보다 메시지량이 적으며 효율적이다. 그림 5의 버전 2는 브로드캐스팅 방식을 이용하여 버전 1보다 효율성을 제공한다.

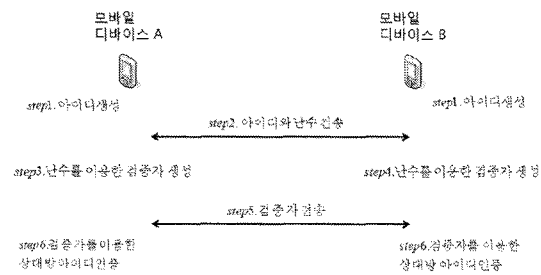


그림 5. 상호 인증 흐름도

3. 제안 방식

아이디 기반의 제안 방식은 인증 및 세션키를 생성한 후, 그룹 키를 생성하는 방식으로 진행된다. 인증 방안으로 아이디를 이용한 영지식 증명으로 상호 인증한다. 그룹 키 방식은 그룹 아이디를 이용하여, 하이브리드 방식(중앙 집중형과 분산형의 혼합)을 이용한다.

3.1 시스템 기호

제안 방식은 다음과 같은 시스템 기호를 이용한다.

- * : 모바일 디바이스 사용자
- MID_* : 모바일 디바이스의 아이디(예 모바일 디바이스 A의 아이디 : MID_A)
- g : 모듈러 연산의 밑수 (p-1 이하의 정수)
- n : 모듈러 연산의 법
- R_{*_i} : *의 i번째 난수($i=1,\ldots,m$)
- SK_{**} : *와 *간의 세션키
- GID_{**} : *와 *간의 그룹 디바이스 아이디
- $h()$: 안전한 일방향 해쉬 함수
- $E_*[M]$: *의 키를 이용하여 메시지 M을 암호화
- GK_{**} : *와 *간의 그룹 키
- || : 메시지 연접 기호

3.2 아이디 기반의 상호 인증

모바일 디바이스의 아이디를 이용한 영지식 증명으로 상호 인증한다. 영지식 증명은 상대방에게 자신이 알고 있는 비밀 정보를 노출 없이 확인 시키는 방안이다. 모바일 아이디를 비밀인자로 생성하고 상대방에 비밀인자를 알려주지 않은 상태에서 동일한 모바일 아이디를 검증할 수 있도록 한다. 이를 통해서 비밀인자 노출없이도 모바일 아이디 검증을 제공할 수 있게 된다. 모바일 디바이스 아이디 생성에 적용하여 아이디의 생성 인자를 노출 없이 검증 시켜 자신이 정당한 모바일 디바이스 아이디의 소유자라는 것을 증명할 수 있게 된다(그림 6 참조).

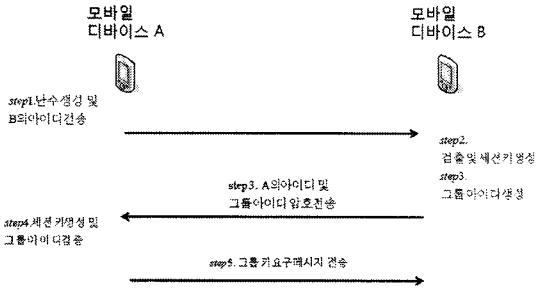


그림 6. 세션키 생성 흐름도

step 1. 모바일 디바이스 A와 B는 각각의 비밀 지수값(a, b)를 이용하여 아이디($MID_A = g^a \bmod n$, $MID_B = g^b \bmod n$)를 생성한다.

step 2. 모바일 디바이스 A는 첫 번째 난수(R_{A1})와 자신의 모바일 디바이스 아이디(MID_A)를 모바일 디바이스 B에 전송한다. 모바일 디바이스 B도 첫 번째 난수(R_{B1})와 자신의 모바일 디바이스 아이디(MID_B)를 모바일 디비이스 A에 전송한다.

step 3. 모바일 디바이스 A는 두 번째 난수(R_{A2})를 생성하고, 전송 받은 난수(R_{B1})를 이용하여 상대방이 검증할 수 있는 $w_A(g^{R_{A2}} \bmod n)$와 $S_A(a - R_{A2}R_{B1})$를 생성한다.

step 4. 모바일 디바이스 B도 두 번째 난수(R_{B2})를 생성하고, 전송 받은 난수(R_{A1})를 이용하여 동일하게 상대방이 검증할 수 있는 $w_B(g^{R_{B2}} \bmod n)$와 $S_B(b - R_{B2}R_{A1})$를 생성한다.

step 5. 모바일 디바이스 A, B는 각각 생성한 검증값 w_A, S_A와w_B, S_B를 상대방에게 전송한다.

setp 6. 모바일 디바이스 A, B는 각각의 검증 연산을 한다. 모바일 디바이스 A는 모바일 디바이스 B의 아이디(MID_B)를 이용하여 $MID_B \stackrel{?}{=} g^{S_B} w_B^{R_{A1}}$인지를 검증하게 된다. 즉 다음과 같이 동일한 모바일 디바이스 B의 아이디가 검출되어야 한다.

$$g^{S_B} w_B^{R_{A1}} = g^{b - R_{A1}R_{B2}} g^{R_{A1}R_{B2}} = g^b = MID_B$$

모바일 디바이스 B도 동일하게 모바일 디바이스 A의 아이디(MID_A)를 이용하여 $MID_A \stackrel{?}{=} g^{S_A} w_A^{R_{B1}}$를 검증하게 된다. ($g^{S_A} w_A^{R_{B1}} = g^{a - R_{B1}R_{A2}} g^{R_{B1}R_{A2}} = g^a = MID_A$)

상호 전송한 난수를 통해 모바일 디바이스의 아이디를 검증하므로 정당한 소유자라는 것을 인증 할 수 있게 된다.

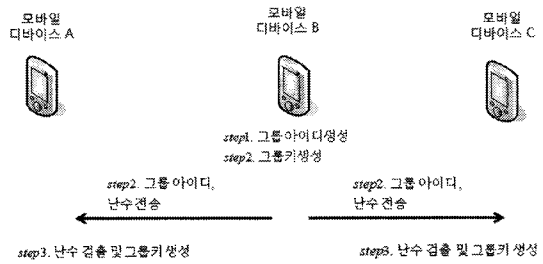


그림 7. 그룹 키 생성 흐름도

3.3 아이디를 이용한 세션키 생성

상호 인증 이후 세션키를 생성하게 된다. 서로의 모바일 디바이스 아이디를 인증하였으므로 다음과 같이 세션키를 생성한다. (그림 7 참조)

step 1. 모바일 디아비스 A는 난수(R_{A3})를 생성한다. 그리고 인증된 모바일 디바이스 B의 아이디(MID_B)에 다음을 계산하여 B에게 전송한다.

$$(MID_B)^{R_{A3}} = g^{bR_{A3}} \bmod n$$

step 2. 모바일 디바이스 B는 전송 받은 데이터($(MID_B)^{R_{A3}} = g^{bR_{A3}} \bmod n$)에 b의 역수($b^{-1}$)를 지수승하여 모바일 디바이스 A가 전송한 $g^{R_{A3}} \bmod n$은 검출 한다. 또한 검출된 값에 난수(R_{B3})를 지수승하여 세션키($SK_{AB} = g^{R_{A3}R_{B3}} \bmod n$)를 생성한다.

step 3. 모바일 디바이스 B는 모바일 디바이스 A의 아이디(MID_A)에 난수(R_{B3})를 지수승($(MID_A)^{R_{B3}} = g^{aR_{B3}} \bmod n$)하고, 세션키($SK_{AB}$)로 그룹 아이디($GID_{AB} = h(MID_A \| MID_B)$)를 암호화($E_{SK_{AB}}[GID_{AB}]$)하여 함께 전송한다.

step 4. 모바일 디바이스 A는 전송 받은 데이터($(MID_A)^{R_{B3}} = g^{aR_{B3}} \bmod n$)에 역수($a^{-1}$)를 이용하여 동일하게 세션키($SK_{AB}$)를 생성하고 암호화 데이터를 복호화하여 그룹 아이디(GID_{AB})를 검증해 상호 동일한 세션키를 설립하였는지 확인한다.

step 5. 모바일 디바이스 A는 세션키의 검증 과정이 완료되면 그룹키 생성의 요구 메시지($GK-request$)를 전송하게 된다.

3.4 그룹 키 생성

그룹 키의 생성에서는 모바일 디바이스의 가입과 탈퇴를 고려해야 한다. 그룹 키 생성은 3개 이상의

표 1. 모바일 디바이스가 저장하고 있는 정보

	모바일 디바이스 A	모바일 디바이스 B	모바일 디바이스 C
세션키	SK_{AB}	SK_{AB}, SK_{BC}	SK_{BC}
그룹 아이디	$GID_{AB} = h(MID_A \| MID_B)$	$GID_{AB} = h(MID_A \| MID_B)$ $GID_{BC} = h(MID_B \| MID_C)$ $GID_{ABC} = h(MID_A \| MID_B \| MID_C)$	$GID_{BC} = h(MID_B \| MID_C)$

디바이스가 연결되어 생성한다. 세션키 생성 이후 그룹 키를 생성을 하기 위해서는 참여 디바이스는 그룹 아이디를 공유하여 하며, 그룹 아이디는 모든 참여 디바이스의 아이디를 연접하여 해쉬한다. 그룹 아이디를 생성하는 디바이스 중에서 그룹 키를 생성하는 주체는 그룹 아이디를 생성하는 여러 디바이스 중에서 이전에 생성된 그룹 아이디가 변경된 디바이스가 된다. 표 1을 보면 모바일 디바이스 B는 모바일 디바이스 A와 GID_{AB}를, 모바일 디바이스 C와 GID_{BC}를, 그리고 모든 디바이스 그룹 아이디 GID_{ABC}를 생성하여 그룹키 생성의 주체가 된다.

step 1. 각각의 모바일 디바이스는 그룹 아이디를 생성한다. 모바일 디바이스 A는 GID_{AB} , 모바일 디바이스 B는 GID_{AB}, GID_{BC} 와 GID_{ABC}로 세 개를 생성하고, 모바일 디바이스 C는 GID_{BC}를 생성한다.

step 2. 모바일 디바이스 B는 생성된 그룹 아이디(GID_{ABC})로 자신의 그룹에 모바일 디바이스 A와 C를 포함한다. 모바일 디바이스 B는 난수(R_{B4})를 생성하여, 그룹키 $GK_{ABC}(= h(g^{R_{B4}} \| GID_{ABC}))$ 생성한다. 그리고 각각의 모바일 디바이스의 아이디에 연산 $((MID_A)^{R_{B4}}, (MID_C)^{R_{B4}})$한다. 모바일 디바이스 A에는 $GID_{ABC}, MID_C, E_{SK_{AB}}[(MID_A)^{R_{B4}}, R_{B4}]$가 전송되고 모바일 디바이스 C에는 $GID_{ABC}, MID_A, E_{SK_{BC}}[(MID_C)^{R_{B4}}, R_{B4}]$가 전송된다.

step 3. 모바일 디바이스 A와 C는 다음의 연산을 통해서 GK_{ABC}를 생성한다. 모바일 디바이스 A는 전송받은 데이터($(MID_A)^{R_{B4}}$)에 A가 보유한 난수 a의 역수를 이용하여 연산($(MID_A^{R_{B4}})^{a^{-1}} = g^{aR_{B4}a^{-1}} = g^{R_{B4}}$)한다. 그 후 그룹 키 $GK_{ABC}(= h(g^{R_{B4}} \| GID_{ABC}))$를 생성한다. 모바일 디바이스 C도 $(MID_C)^{R_{B4}}$에 보유한 난수 c의 역수를 이용하여 연산($(MID_C^{R_{B4}})^{c^{-1}} = g^{cR_{B4}c^{-1}} = g^{R_{B4}}$))을 통해, 동일한 그룹 키 $GK_{ABC}(= h(g^{R_{B4}} \| GID_{ABC}))$를 생성한다.

3.4.1 그룹 가입

모바일 디바이스 D가 그룹 GID_{ABC}에 접근하여 가입하게 되면 모바일 디바이스 C는 새로운 그룹 아이디($GID_{ABCD}(h(MID_A \| MID_B \| MID_C \| MID_D))$)를 생성하여 그룹 키 변경에 주체가 된다.(그림 9 참조)

step 1. 모바일 디바이스 C는 GID_{ABC}에서 GID_{ABCD}를 생성하고, 난수(R_{C1})를 이용하여 $GK_{ABCD}(= h(g^{R_{C1}} \| GID_{ABCD}))$를 생성한다.

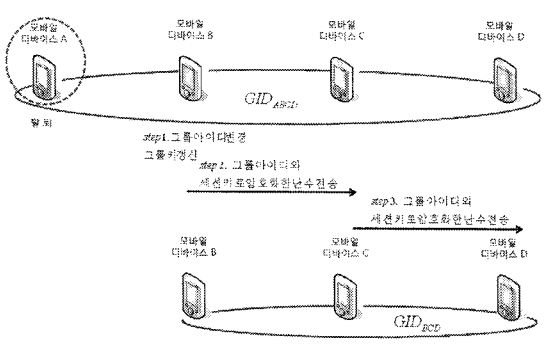


그림 8. 탈퇴(모바일 디바이스 A)에 따른 그룹 키 갱신 흐름도

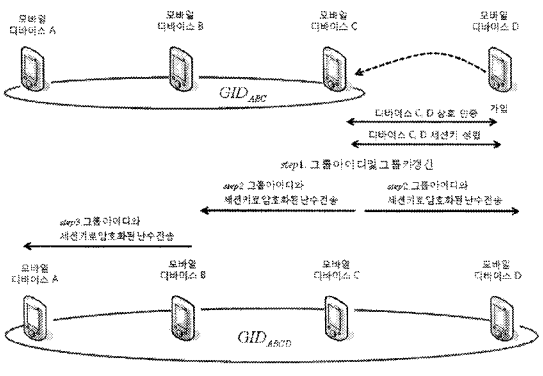


그림 9. 그룹 가입(모바일 디바이스 D)에 따른 그룹 키 생성 흐름도

step 2. 모바일 디바이스 C는 자신에 연접한 모바일 디바이스 B와 C에 각각 모바일 디바이스 B 데이터($GID_{ABCD}, MID_D, E_{SK_{BC}}[(MID_B)^{R_{C2}}, R_{C1}]$)와 모바일 디바이스 D 데이터($GID_{ABCD}, MID_A, MID_B, E_{SK_{CD}}[(MID_D)^{R_{C2}}, R_{C1}]$)를 전송한다.

step 3. 모바일 디바이스 B는 디바이스 A에 그룹 아이디(GID_{ABCD})와 그룹 키 갱신 데이터($MID_D, E_{SK_{AB}}[(MID_A)^{R_{C2}}, R_{C1}]$)를 전송한다.

전송 받은 데이터를 통해 3.4의 3단계처럼 역수를 지수승하여 그룹 키 생성 인자를 획득할 수 있게 된다.

3.4.2 그룹 탈퇴

그림 9를 보면 현재 4개의 모바일 디바이스가 그룹을 이루고 있다. 모바일 디바이스 A가 탈퇴를 하게 되면 그룹 키의 갱신이 필요하다(그림 10 참조). 그룹 키에 대한 전방향 안전성 제공으로 탈퇴한 멤버가 다음의 그룹 키를 유추할 수 없게 해야 한다. 모바일 디바이스 A가 탈퇴하면서 자신과 통신한 모바일 디바이스 B에게 탈퇴 메시지를 전송한다. 모바일 디바이스 B는 A를 제외한 새로운 그룹 아이디를 생성하게 되고, 이 내용을 자신과 통신하는 그룹 멤버에게 알려 주게 된다. 이때 모바일 디바이스 A의 탈퇴로 모바일 디바이스 B는 그룹 아이디 GID_{BCD}를 생성하고, 그룹 키 갱신의 주체가 된다.

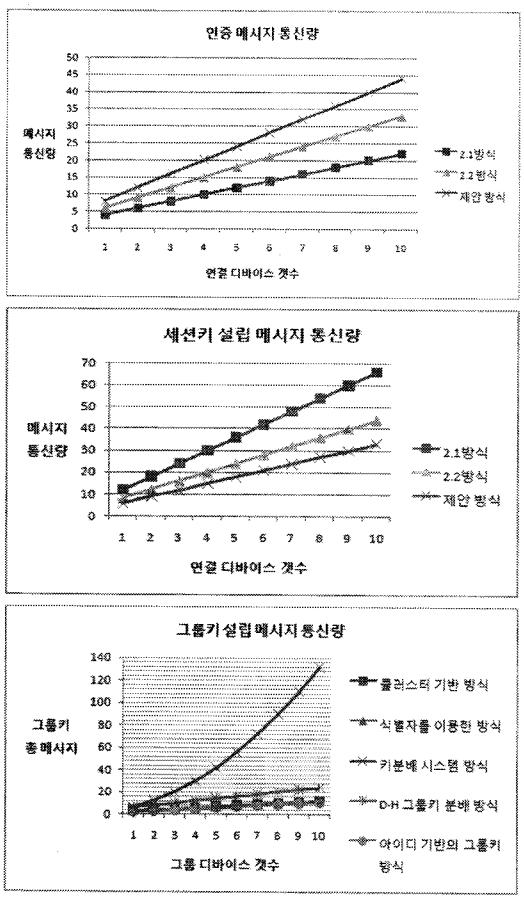


그림 10. 각 방식에 따른 통신량 그래프

step 1. 모바일 디바이스 B는 새로운 그룹 아이디(GID_{BCD})의 생성을 통해서 그룹 키 갱신을 알리고, 난수(R_B)를 생성하여 그룹 키 $GK_{BCD}(=h(g^{R_B}\|GID_{BCD}))$를 생성한다.

step 2. 모바일 디바이스 B는 모바일 디바이스 C에 그룹 아이디(GID_{BCD})와 세션키(SK_{BC})를 이용하여 그룹 키 생성 인자를 암호화($E_{SK_{BC}}[(MID_C)^{R_B}, R_B]$)하여 전송한다.

step 3. 모바일 디바이스 C는 모바일 디바이스 D에 동일하게 그룹 아이디(GID_{BCD})와 세션키(SK_{CD})를 이용하여 그룹 키 생성 인자를 암호화($E_{SK_{CD}}[(MID_D)^{R_B}, R_B]$)하여 전송한다.

탈퇴에 따른 그룹 키 생성은 3.4의 3단계처럼 자신의 역수를 지수승하면 그룹 키의 생성인자를 획득할 수 있게 된다.

4. 제안 방식 분석

제안 방식의 안전성 분석으로 다음의 내용을 확인한다. 첫 번째는 메시지의 기밀성으로써 전체적인 메시지가 안전하게 당사자만이 확인 할 수 있는지 분석하고 두 번째는 상호 인증 단계에서 제 3자가 위장이 가능한지 분석한다. 세 번째에서는 세션키의 설립 과정에서는 중간자 공격(man-in-the-middle attack)이 가능한지 분석한다. 네 번째에서는 그룹키의 성립에서 전방향성과 후방향성에 대하여 알아본다. 그리고 마지막으로는 메시지의 통신량을 비교한다.

4.1 기밀성

제안 방식에서 기밀성이 필요한 메시지는 그룹 키의 난수이다. 모바일 디바이스 아이디는 공개되어 있기 때문에 기밀성을 제공할 필요가 없으며, 상호 인증 단계의 메시지는 상호 전송한 난수에 응답되는 메시지를 생성하고, 검증하므로 기밀성의 제공이 필요 없

다. 하지만 그룹 키 성립에서는 난수가 공개되면 키 노출의 문제가 발생하기 때문이 이전 단계의 세션키로 암호화 하여 전송하는 방식으로 메시지에 대한 기밀성을 제공할 수 있게 된다.

4.2 상호 인증의 위장

상호 인증에서 위장이 발생하면 악의적인 제 3자가 인증을 받을 수 있으므로 3.2방식에서 위장이 제공되어서는 안 된다. 3.2방식에서 메시지의 전송은 step2, 3과 6에서 이루어진다. step 6의 메시지는 step 2, 3에 응답하는 메시지이다. 만약 제 3자가 모바일 디바이스 A로 위장하여 step 2의 메시지를 전송하면, 모바일 디바이스 B는 step 3과 step 6의 메시지를 전송한다. 이때 위장한 제 3자는 $w_{A'}(g^{R_{A'}} \bmod n)$, $S_{A'}(a' - R_{A'}R_{B})$를 생성하여, 모바일 디바이스 B에 전송한다. 모바일 디바이스 B는 모바일 디바이스 A를 검증하기 위한 연산을 한다.

$$MID_A \stackrel{?}{=} g^{S_{A'}} w_{A'}^{R_{B}}$$
$$g^{S_{A'}} w_{A'}^{R_{B}} = g^{a' - R_{B}R_{A'}} g^{R_{B}R_{A'}} = g^{a'} \neq MID_A$$

이와 같이 MID_A의 검증을 할 수 없으므로 통신의 대상이 모바일 디바이스 A가 아님을 알 수 있고 제 3자는 위장을 할 수 없다.

4.3 세션키 중간자 공격

세션키 생성에서 중간자(man-in-the-middle attack) 공격은 3.3방식에서 step 1의 메시지를 수정하여 공격한다. 제 3자는 step 1의 난수를 변경하여 $(MID_B)^{R_{A'}}$를 전송한다. 모바일 디바이스 B는 연산을 통해서 세션키($SK_{AB} = g^{R_{A'}R_{B}} \bmod n$)를 만들고 응답 메시지($(MID_A)^{R_{B}}, E_{SK_{AB}}[GID]$)를 생성하여 모바일 디바이스 A에 전송한다. 이때 제 3자는 메시지 $((MID_A)^{R_{B}}, E_{SK_{AB}}[GID])$를 가로채기 하여 세션키($SK_{AB}$)를 생성하여야 한다. 그러나 $MID_A(g^a \bmod n)$의 a에 대한 역수(a^{-1})를 제 3자가 알 수 없다는 것이다. 그러므로 제 3자는 모바일 디바이스 B가 보내는 난수(R_{B3})를 추출 할 수 없으며, $SK_{AB'}$를 동일하게 생성할 수 없다. 그리고 제 3자가 모바일 디바이스 B의 응답 메시지를 임의로 생성하여 전송하는 경우 모바일 디바이스 A가 전송한 $(MID_B)^{R_{A3}}$에서 R_{A3}를 알 수 없다. 이유는 b에 대한 역수(b^{-1})를 모르기 때문이다. 그러므로 제 3자는 중간에서 세션키를 생성할 수 없는 상황이 발생하게 된다. 그러므로 중간자 공격은 성공할 수 없다.

4.4 그룹 키의 전방향과 후방향 안전성 분석

전방향과 후방향 안전성은 그룹키의 보안 요구 사항이다. 본 제안 방식의 3.4.1방식에서 그룹 가입의 경우 가입된 멤버를 위해서 난수를 이용하여 키를 갱신하므로, 이전 키와 연관성이 없이 생성된다. 그러므로 후방향 안전성이 제공된다. 또한 3.4.2방식에서 탈퇴를 하면 그 사실을 인지한 모바일 디바이스가 그룹 모바일 디바이스 아이디와 키를 갱신하여 그룹에 제공한다. 이 또한 난수를 이용하는 것으로 이전의 키와 연관성이 없다.

4.5 메시지의 통신량 비교

메시지의 통신량을 비교는 모바일 디바이스가 인증 및 세션키 그리고 그룹 키를 이용하기 위해서 통신하는 메시지의 수를 비교하도록 한다. 표 2는 각 방식의 메시지량 계산 방법이다. 2.3.1과 2.3.2의 방식은 인증과 세션키를 생성하는 방안을 제외하는 이유는 논문에서 인증과 세션+키에 대한 언급을 일반적인 사항으로 기술함으로써 기존의 방식과 동일하기 때문에 비교에서 제외된다. 즉 비교 부분은 연구의 논문의 목적을 적용하여 메시지량을 비교한다. n은

표 2. 각 방식의 메시지량 계산식

	2.1 클러스터 기반 방식[6]	2.2 식별자를 이용한 클러스터 기반 방식[7]	2.3.1 키 분배 시스템 방식[1]	2.3.2 D-H 그룹 키 분배 방식[8]	제안 방식
인증	2n	3n	비교 제외	비교 제외	4n
세션키	6n	4n	비교 제외	비교 제외	3n
그룹키 총 전송메시지	m	m	m(m-1)	2m	m-1

디바이스가 중앙 클러스와 통신하는 횟수가 되며, m은 전체 네트워크의 모바일 디바이스 개수이다. 제안 방식의 메시지량의 비교를 보면 인증에서 상호 인증을 제공하기 때문에 다른 방식보다 증가하나 세션키 및 그룹 키 설립 방식에서는 메시지량이 적어지는 것을 확인 할 수 있다. 통신량은 통신 횟수를 측정하는 것으로 통신 횟수의 증가는 그래프의 증가를 가지고 온다(그림 10 참조).

5. 결론 및 향후 연구

제안 방식은 Ad-hoc 네트워크에서 모바일 디바이스간의 상호 인증 및 세션키 설립과 그룹 키를 통한 서비스 방안에 대하여 제시하였다. 메시지량에서 상호 인증 제공으로 통신량이 증가하나 세션키 및 그룹 키의 생성에 있어서는 다른 방식에 비해 적어도 1회의 메시지량이 감소하는 것을 확인 할 수 있다. 또한 인증의 경우 모바일 디바이스 아이디를 이용하며, 사전 정보를 공유하지 않는 상태에서 적용 가능하다. 또한 중간의 클러스터나 베이스 역할의 모바일 디바이스가 필요 없으므로 중간의 메시지가 서버나 클러스터에 노출되는 것을 막을 수 있다. 본 방식에서의 모바일 디바이스 아이디 기반의 암호 기술은 모바일 디바이스 아이디에 대한 신뢰성이 기반되며, 그룹 키 분배의 경우 상호 동의가 아닌 모바일 디바이스가 분배하는 방식을 이용하고 있다. 그러므로 다른 지수승 그룹 키 분배 방식 보다 메시지량이 감소한다. 본 제안 방식은 Ad-hoc 네트워크의 동적인 경우에도 적용하기 쉬운 방식이 될 것으로 사료된다. 그러나 향후 연구를 위해서는 상호 인증에서의 메시지량을 줄일 수 있는 방안이 필요하며, Ad-hoc 네트워크와 다른 네트워크망의 연동에 대한 연구도 지속적으로 진행되어야 한다.

참 고 문 헌

[1] Ingemar ingemarsson, Donald T.Tang and C.K. Wong, "A Conference key Distribution System," *IEEE TRANSACTIONS on INFORMATION THEORY*, Vol.28, No.5, pp. 714~721, 1982. 02.

[2] Laurent Eschenauer and Virgil D.Gligor, "A key-Management Scheme for Distributed Sensor Networks," *CCS'02*, pp. 18-22, 2002.

[3] Wang changda and Ju shiguang, "Multilevel security model for ad hoc networks," *Journal of systems engineering and electronics*, Vol.19, No.2, pp. 391-397, 2008.

[4] Lijun Liao and Mark Manulis, "Tree-based group key agreement framework for mobile ad-hoc networks," *FGCS*, pp. 787-803, 2007

[5] Michael Steiner, Gene Tsudik and Michael Waidner, "Diffie-Hellman key Distribution Extended to Group communication," *Procecdings of the 3rd ACM conference on computer and communications security*, pp. 31-37, 1996

[6] Varadharajan et al. "Security for cluster based ad hoc networks," *comput commun*, Vol.27, pp. 488-501, 2005.

[7] 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, 2007.

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

[9] Dijiang Huang and deep Medhi, "A secure group key management scheme for hierarchical mobile ad hoc networks," *Ad Hoc Networks2008*, pp. 560-577, 2008

[10] Eric Ricardo Anton and Otto Carlos Muniz Bandeira Duarte, "Group Key Establishment in Wireless Ad Hoc Networks," *Workshop on quality of service and mobility*, 2002.

[11] N.Asokan and P.Ginzboorg, "Key agreement in ad hoc networks," *computer communications 2000*, pp. 1627-1637, 2000.

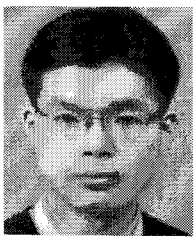
[12] Nen-chung wang and shian-Zhang fang, "A hierarchical key management scheme for secure group communications in mobile ad hoc networks," *the journal of systems and software*, pp. 1667-1677, 2007.

[13] Tzu-chiang Chiang and Yueh-Min Huang, "Group Keys and the Multicast security in Ad Hoc Networks," *ICPPW'03*, 2003.

강 서 일

2003년 2월 순천향대학교 정보기술 공학부 학사
2005년 2월 순천향대학교 전산학과 석사
2005년 3월~현재 순천향대학교 전산학과 박사 과정

관심분야 : 무선 네트워크 보안, 전자 투표, 전자 화폐



이 남 훈

1995년~1999년 홍익대학교 컴퓨터 공학과 학사
1999년~2001년 홍익대학교 전자계산학과 석사
2001년~현재 전자통신연구원 부설연구소

관심분야 : 분산 네트워크 및 네트워크 시스템 보안, 모바일 시스템 보안

이 임 영

1981년 홍익대학교 전자공학과 졸업
1986년 오사카대학 통신공학전공 석사
1989년 오사카대학 통신공학전공 박사
1989년~1994년 한국전자통신연구원 선임연구원
1994년~현재 순천향대학교 컴퓨터 학부 교수
관심분야 : 암호이론, 정보이론, 컴퓨터 보안