韓國 컴퓨터情報學會 論文誌
第10卷 第2號, 2005. 5.

2005-10-2-2-5

통합 멀티캐스팅 환경에서 효율적인 그룹 통신에 관한 연구

김 현 주*, 남 정 현*, 김 승 주*, 원 동 호*

A Study on Efficient Group Communication in the Integrated Multicasting Environment

Hyun-jue Kim*, Jung-hyun Nam*, Seung-joo Kim*, Dong-ho Won*

요 약

최근 그룹 지향적 응용 서비스가 증가함에 따라 유·무선 네트워크상에서 사용 가능한 멀티캐스트 통신에 대한 연구가 활발히 진행되고 있다. 그러나 멀티캐스트 통신에 대한 안전성과 효율성에 대한 해결책은 아직 미비한 상태이다. 본 논문에서는 유·무선 통합 멀티캐스트 서비스 지원을 위해, 인증을 제공하는 안전한 멀티캐스팅 프로토콜을 제안한다. 제안하는 프로토콜은 개인 휴대단말기 등과 같은 낮은 연산 처리 능력을 가지는 시스템에서 사용 가능한 효율적인 프로토콜이다.

Abstract

Through the increment of group oriented application services, the multicast communication in wire/wireless network has become a widely discussed researching topic. However solution for security, efficiency and scaleability of a multicast communications are not enough to be satisfactory. In this paper, we propose a new secure, efficient and scalable multicasting protocols to provide a integrated multicast service. Our protocol is an authenticated key establishment protocol which has been designed specifically for use with low powered computationally weak equipment such as Cellular phone and PDA(Personal Digital Assistant).

▸ Keyword : Wire/Wireless Network, Multicast, Key Establishment

• 제1저자 : 김현주
• 접수일 : 2005.04.11, 심사완료일 : 2005.05.18
* 성균관대학교 정보통신공학부
※본 연구는 정보통신부 지원 대학 IT 연구센터 육성지원사업(C1090-0403-0005)으로 수행되었음

Ⅰ. 서 론

멀티캐스트이란 특정한 그룹에 속한 수신자들에게 동시에 데이터를 전송하는 일 대 다 방식으로 브로드캐스트에서 발생하는 네트웍 자원의 낭비를 막을 수 있고 이러한 장점 때문에 여러 인터넷 서비스에 유용하게 사용될 수 있다. 이에 인터넷 환경도 기존의 유니캐스트 모드와 더불어 다수의 수신자들에게 전송되는 멀티캐스트 모드를 지원하고 있다. 그리고 인터넷의 상업적인 목적으로의 이용이 증가함에 따라, 멀티캐스팅을 이용한 송신자측의 자원과 네트웍 자원의 효율적 활용을 필요로 하는 많은 응용분야들이 생겨나고 있다. 이러한 응용분야에는 pay-per-view TV와 같은 방송 서비스, 신문이나 주식 시세와 같은 각종 정보 배포, 소프트웨어 업데이트, 가상대학과 같은 원격교육시스템들이 있다.

이와 같이 멀티캐스트는 특정 그룹을 대상으로 하는 서비스에 유용하게 사용되고 있지만, 다수의 그룹 구성원들이 넓은 네트워크 영역에 걸쳐 데이터를 주고받기 때문에 유니캐스트보다 더 많은 보안 취약 요소를 가진다. 즉, 더 많은 통신 링크를 경유하게 되어 도청, 정보의 위·변조 및 파괴 등의 공격을 받게 된다. 이로 인해 비인가된 사용자가 데이터를 불법적으로 사용하거나 또는 기밀 정보의 노출로 위험한 상황에 노출될 수도 있게 된다. 따라서 단순한 멀티캐스트 만으로는 안전한 서비스를 보장하지는 못한다. 이에 네트웍 상에 전송되는 디지털 정보의 안전성과 관련된 여러 가지 문제를 효율적으로 대처할 수 있는 암호 시스템의 사용이 요구되고 있다.

인터넷과 같이 공개된 네트워크상에서 안전하게 그룹 통신을 하기 위해서는 우선 그룹의 모든 구성원이 하나의 그룹키를 공유하도록 키 설정(key establishment)을 해야 한다. 이것은 안전한 그룹 통신을 하기 위한 가장 기본적인 사항으로, 그룹 멤버들은 그룹 구성원들만이 아는 그룹키를 생성할 수 있고 생성된 키를 서로 공유해야 한다. 이러한 목적으로 설계되는 프로토콜을 그룹키 설정 프로토콜이라고 한다.

그룹키 설정에 관한 연구는 1982년 Ingemarsson, Tang와 Wong[1]에 의해서 처음으로 시작되었다. 이후 많은 프로토콜들이 발표되었으며[2~9], 안전성이 증명 가능한 그룹키 설정 프로토콜에 관한 연구는 2001년 Bresson[10~12]에 의해 이루어졌다. 그러나 Bresson이 제안한 프로토콜은 라운드 복잡도가 그룹 구성원들의 수에 관하여 선형(linear)이 된다는 문제점이 있기 때문에 그룹 사이즈가 커지면 현실적으로 실용화되기 어렵다. 2003년 Boyd와 Bresson[13]은 이러한 문제점을 해결한 안전성이 증명 가능한 효율적인 프로토콜을 제안하였다. 그러나 이들의 프로토콜들은 완전 전방향 안전성 (PFS: Perfect Forward Secrecy)를 만족하지 못한다. PFS를 만족하면서 상수 라운드를 갖는 프로토콜은 2003년 Katz와 Yung[14]에 의하여 제안되었다. 이들은 또한 Burmester[3]의 2라운드 프로토콜에 대한 안전성을 증명하였다. Burmester[3]은 가장 잘 알려진 대표적인 그룹키 설정 프로토콜이다. 그리고 최근 2004년 Choi[15]가 Burmester[3]의 프로토콜을 타원곡선 암호 시스템에 적용시켜, Pairing을 이용한 ID 기반 그룹키 설정 프로토콜을 제안하였다.

Pairing은 처음 타원곡선상에서의 이산대수문제의 공격에 사용되었으며, 2000년 Joux[16]에 의해 3자간 Diffie-Hellman 프로토콜 설계 시 이용 될 수 있음이 제안되어졌다. 그 후, 2001년, Boneh[17,18]은 실제로 구현 가능한 새로운 암호방식과 서명방식을 제안하였다. 이 제안이 이루어진 이후, Pairing을 이용한 새로운 형태의 암호 방식들이 활발히 연구되고 있다.[15,19~24]

본 논문에서는 최근 이슈가 되고있는 Pairing을 사용하여 사용자 인증이 가능한 그룹키 설정 프로토콜을 제안한다. 제안하는 프로토콜은 대부분의 그룹 지향적 서비스와 같이 특정 센터(Server)가 서비스를 하는 응용분야에 효율적으로 적용할 수 있도록 설계하였다. 특히 사용자(Client)측의 연산량을 줄임으로서 휴대폰, 개인 휴대단말기등과 같은 낮은 연산 처리 능력을 가지는 시스템에 적합하도록 설계하였다.

본 논문의 구성은 다음과 같다. 1장의 서론에 이어 2장에서는 본 논문에서 제안하는 프로토콜에 사용된 안전성 기반 문제에 대하여 설명하고, 3장에서는 본 논문에서 제안하는 그룹키 설정 프로토콜과 ID 기반 그룹키 설정 프로토콜을 소개한다. 그리고 4장에서는 제안한 방식의 안전성과 효율성을 살펴보고 마지막으로 5장에서 결론을 도출한다.

II. 안전성 기반 문제

이 장에서는 본 논문에서 사용된 안전성 기반 문제들을 살펴본다. 본 논문에서 제안하는 프로코콜의 안전성은 계산적 Diffie-Hellman (CDH) 문제와 Bilinear 결정적 Diffie-Hellman (BDDH) 문제의 어려움에 기반을 두었으며, 이 문제들에 대한 정의는 다음과 같다.

G_1과 G_2는 위수가 임의의 k-bit의 큰 소수 p인 순환군으로, G_1은 타원곡선 $E(F_p)$위의 점들로 이루어진 덧셈군이고, G_2는 F_{p^2}의 부분군으로 곱셈군이다. 이때 k는 안전성 파라미터이다. 그리고 P는 G_1의 생성원이다.

▸CDH(Computational Diffie-Hellman) 문제: 임의의 $a, b \in Z_p$ 에 대하여, P, aP와 bP로부터 abP를 구하는 문제

▸CDH 가정: 임의의 확률적 다항식 시간(polynomial-time) 알고리즘 A에 대하여, 만일 아래의 정의된 A의 이점(advantage)이 무시할 수 있을 만큼(negligible) 아주 작다면 CDH 생성자 IG_{CDH}는 CDH 가정을 만족한다고 말한다.

$$\mathrm{Adv}_{G_1}^{CDH}(A) = \left| \Pr\left[A(G_1, P, aP, bP) = abP \;\middle|\; \begin{array}{l} G_1 \leftarrow IG_{CDH}(1^k); \\ P \leftarrow G_1; \\ a, b \leftarrow Z_p^* \end{array} \right] \right|$$

이때, t 수행시간내에서 실행되는 모든 확률적 다항식 시간 알고리즘 A의 이점 $\mathrm{Adv}_{G_1}^{CDH}(A)$의 최대값은 $\mathrm{Adv}_{G_1}^{CDH}(t)$로 표시한다.

▸Bilinear-pairing: 임의의 $Q, R \in G_1$와 $a, b \in Z/\ell$ 에 대하여, 함수 $e: G_1 \times G_1 \rightarrow G_2$가 다음의 조건들을 만족하면 e를 bilinear-pairing이라고 한다.

- Bilinearity
  : $e(aP, bQ) = e(P, Q)^{ab}$ 또는
  $e(P+Q, R) = e(P, R) \cdot e(Q, R)$,
  $e(P, Q+R) = e(P, Q) \cdot e(P, R)$를 만족한다.
- Non-degeneracy
  : $e(P, Q) = 1$ 이면 P는 무한원점 (O)이다.
- Efficiency
  : $e(P, Q)$의 계산이 효율적인 알고리즘이 존재한다.

▸BDDH(Bilinear Decisional Diffie-Hellman) 문제
: 임의의 $a, b, c, d \in Z_p$ 에 대하여, P, aP, bP, cP와 $e(P, P)^d$로부터 $d = abc$인지를 결정하는 문제

▸BDDH 가정: 임의의 확률적 다항식 시간 알고리즘 A에 대하여, 만일 아래의 정의된 A의 이점(advantage)이 무시할 수 있을 만큼(negligible) 아주 작다면 BDDH 파라미터 생성자 IG_{BDDH}는 BDDH 가정을 만족한다고 말한다.

$$\mathrm{Adv}_{(e, G_1, G_2)}^{BDDH}(A) = \left| \Pr\left[A\begin{pmatrix} e, G_1, G_2, P, \\ aP, bP, cP, \\ e(P,P)^{abc} \end{pmatrix} = 1 \;\middle|\; \begin{array}{l} \langle G_1, G_2, e \rangle \\ \quad \leftarrow IG_{BDH}(1^k); \\ |G_1| = |G_2| = p; \\ P \leftarrow G_1^*; \\ a, b, c \leftarrow Z_P \end{array} \right] - \Pr\left[A\begin{pmatrix} e, G_1, G_2, P, \\ aP, bP, cP, \\ e(P,P)^{d} \end{pmatrix} = 1 \;\middle|\; \begin{array}{l} \langle G_1, G_2, e \rangle \\ \quad \leftarrow IG_{BDH}(1^k); \\ |G_1| = |G_2| = p; \\ P \leftarrow G_1^*; \\ a, b, c, d \leftarrow Z_P \end{array} \right] \right|$$

이때, t 수행시간내에서 실행되는 모든 확률적 다항식 시간 알고리즘 A의 이점 $\mathrm{Adv}_{(e, G_1, G_2)}^{BDDH}(A)$의 최대값은 $\mathrm{Adv}_{(e, G_1, G_2)}^{BDDH}(t)$로 표시한다.

III. 제안 프로토콜

그룹키 설정 솔루션은 멀티캐스트 그룹을 구성하는 사용자들의 능력에 따라 달라진다. 원격회의 시스템과 같이 모든 사용자들이 동일한 컴퓨팅파워를 가지는지 아니면 특정

사용자가 다른 사용자들 보다 우수한 컴퓨팅 파워를 가지고 있어 더 많은 작업을 수행할 수 있는 능력을 소유하였는지에 따라서도 달라진다.

차세대 네트워크 환경인 유·무선 통합 네트워크에서는 특히 그룹 구성원의 능력을 고려해서 설계해야 한다. 무선 인터넷 환경에서 사용되는 무선 단말기는 이동성에 귀결되는 단말기의 소형화 경향으로 인해 제한된 시스템 자원을 보유하게 되고, 반대로 유선 인터넷 환경에서 사용되는 개인용 PC와 같은 유선단말기는 무선단말기에 비해 상대적으로 이동성이 적고 연산능력과 메모리와 같은 시스템 자원이 풍부하다. 그렇기 때문에 서로 다른 특성을 지니는 유·무선 통합 네트워크 환경에서는 구성원 각자의 자원을 고려해야 할 필요가 있다. 본 장에서는 Bilinear-pairing을 이용하여 특정 센터가 다수의 사용자들에게 서비스를 하는 응용분야에 적합한 그룹키 설정 프로토콜들을 제안한다.

3.1 그룹키 설정 프로토콜(GKA)

$\bigcup = \{U_1, U_2, \cdots, U_{p_u(k)}\}$를 그룹키 설정 프로토콜에 참가하는 모든 참가자들의 집합이라고 놓는다. 여기에서 $p_u(k)$ 는 안전성 파라미터 k의 다항식 함수이다. 그리고 GKA 프로토콜에 참가하는 n명의 사용자 U_i ($i=[1,n]$)들로 이루어진 멀티캐스트 그룹을 $MG=\{U_1, U_2, \cdots, U_n\} \subseteq \bigcup$ 라고 정의한다. 그리고 그룹의 구성원 중의 한 사용자 $U_C \in MG$가 멀티캐스트 그룹 MG에서의 특별한 역할을 담당하는 관리자(Controller)라고 정의한다. 본 논문에서는 편의상 그룹 관리자가 $U_C = U_n$ 이라고 가정한다.

GKA 프로토콜은 Setup, GKeyEst의 두 개의 알고리즘으로 구성되어 있으며 각 과정은 다음과 같다.

① Setup: 시스템파라미터를 생성하기 위하여 다음의 알고리즘을 수행한다.
시스템 파라미터는 $\langle G_1, G_2, e, p, P, H, H_Q \rangle$ 이다. 여기서 G_1, G_2, e, p와 P는 2장에서 정의한 값들이며, $H : \{0,1\}^* \rightarrow Z_p^*$와 $H_Q : \{0,1\}^* \rightarrow G_1$는 암호 해쉬 함수들이다.

② GKeyEst: 멀티캐스트 그룹 MG에서의 그룹키를 생성하기 위하여 다음의 알고리즘을 수행한다.

[round 1]

step 1:

그룹 관리자 U_n는 임의의 정수 $r_n \in Z_p^*$를 선택하고 해쉬값 $s \in Z_p^*$와 $v \in Z_p^*$을 구한 후, 부분키 $P_n = r_n P$, $P_S = sP$와 $P_V = vP$를 계산한다. 해쉬값 s, v 와 r_n는 관리자 U_n이 비밀로 간직한다. 그룹 관리자 U_n을 제외한 나머지 $n-1$명의 사용자 U_i는 임의의 정수 $r_i \in Z_p^*$를 선택하여 부분키 $P_i = r_i P$를 계산하고, $M_i = U_i \| P_i$를 멀티캐스트 그룹 관리자 U_n에게 전송한다. 임의의 정수 $r_i \in Z_p$는 각 사용자 U_i가 비밀로 간직한다.

[round 2]

step 2:

$n-1$ 개의 메시지 M_i를 모두 전달받은 관리자 U_n는 멀티캐스트 그룹 MG에서의 그룹키

$K = e\left(\sum_{i=[1,n]} P_i,\ svP\right) = e(P,P)^{sv\left(\sum_{i=[1,n]} r_i\right)}$

를 생성한다. 그리고 각 사용자 U_i들이 그룹키 K를 생성하도록 하기 위하여, 관리자 U_n는 집합

$\Xi = \{P_i, P_S, P_V \mid i \in [1, n-1]\}$를 생성하고

$T_i = e\left(\sum_{t=[1,n]\setminus\{i\}} P_t,\ svP\right)$를 계산하여 집합

$\Gamma = \{T_i \mid i \in [1, n-1]\}$를 생성한다.

그리고 $M_n = MG \| \Xi \| \Gamma$를 그룹내의 모든 사용자에게 브로드캐스트를 한다. (여기서 브로드캐스트의 의미는 단지 개별적인 링크를 통하여 그룹 관리자가 그룹의 모든 구성원에게 같은 메시지를 보내는 것을 의미한다.)

step 3:

각 사용자 $U_i \neq U_n$는

$K = T_i \cdot e(P_S, P_V)^{r_i} = e(P,P)^{sv\left(\sum_{i=[1,n]} r_i\right)}$

를 계산하여 멀티캐스트 그룹 MG에서의 그룹키 K를 생성한다. 그룹 MG에서의 모든 사용자 U_i는 첫 번째 라운드에서 선택했던 정수 $r_i \in Z_p^*$와

$Z = \Xi \setminus \{P_V\}$를 저장한다.

위 프로토콜에 의하여 멀티캐스트 그룹 $MG=\{U_1, U_2, \cdots, U_n\}$에 속하는 모든 사용자는 MG에서의 그룹키 $K = e(P,P)^{sv\left(\sum_{i=[1,n]} r_i\right)}$를 생성할 수 있다. 그러므로 그룹 MG의 모든 구성원은 그룹 구성원들만이 아는 그룹 세션키 $SK = H(K \| \Gamma)$를 이용하여 그

룹에서의 안전한 비밀 통신이나 유료 서비스를 할 수 있다.

GKA 프로토콜의 마지막 단계에서 저장된 정수 $r_i \in Z_p^*$와 Z는 차후 그룹 멤버의 가입이나 탈퇴와 같이 그룹 멤버가 변화할 때 그룹키를 갱신시키기 위한 정보로 사용된다. 그룹 멤버쉽의 변화로 새롭게 형성된 멀티캐스트 그룹의 그룹키를 갱신시킬 때, 기존에 남아있던 사용자는 누구나 새로운 멀티캐스트 그룹에서 그룹 관리자가 될 수 있다.

3.2 그룹키 설정 프로토콜(ID-AGKA)

이 절에서 제안하는 프로토콜은 앞 절에서 제안한 GKA 프로토콜을 개인식별 방식[25]에 적용시킨 인증 가능한 그룹키 설정 프로토콜이다.

GKA 프로토콜에서와 같이,

$\bigcup = \{U_1, U_2, \cdots, U_{p_n(k)}\}$는 그룹키 설정 프로토콜에 참가하는 모든 참가자들의 집합이며,

$MG = \{U_1, U_2, \cdots, U_n\} \subseteq \bigcup$는 ID-AGKA 프로토콜에 참가하는 n명의 사용자 U_i ($i = [1, n]$)들로 이루어진 멀티캐스트 그룹이고 사용자 $U_C = U_n \in MG$가 멀티캐스트 그룹 MG에서의 관리자이다.

ID-AGKA 프로토콜은 Setup, Extract, GKeyEst의 세 개의 알고리즘으로 구성되어 있으며 각 과정은 다음과 같다.

① Setup: GKA 프로토콜과 같다.

② Extract: 프로토콜의 초기 단계에서, 각 사용자 $U_i \in \bigcup$는 키 생성 알고리즘에 의해 각자의 개인식별 정보 ID_i에 대응되는 공개키와 비밀키 쌍 (Q_i, D_i)을 얻는다. 주어진 임의의 string ID_i에 관하여 Extract 알고리즘은 그에 해당하는 비밀키를 다음의 절차에 의하여 생성해준다.

step1: $Q_i = H_Q(ID_i)$를 계산한다.

step2: $D_i = wQ_i$를 계산한다.

주어진 ID_i에 해당하는 사용자들의 공개키와 비밀키는 각각 Q_i와 D_i이다. 그리고 $w \in Z_p^*$는 마스터키이고, $P_{pub} = wP$는 키 발급 기관의 공개키이다.

③ GKeyEst: 멀티캐스트 그룹 MG에서의 그룹키를 생성하기 위하여 다음의 알고리즘을 수행한다.

[round 1]

step 1:

GKA 프로토콜에서와 같이 그룹 관리자 U_n는 $P_n = r_n P$, $P_S = sP$와 $P_V = vP$를 계산하고 그룹 관리자 U_n을 제외한 나머지 $n-1$명의 사용자 U_i는 $P_i = r_i P$를 생성한다. 그리고 사용자 U_i는 키 발급 기관의 공개키 P_{pub}와 자신의 비밀키 D_i를 사용하여 $O_i = h(P_i)D_i + r_i P_{pub}$를 계산하고 $M_i = U_i \| P_i \| O_i$를 멀티캐스트 그룹 관리자 U_n에게 전송함으로써 각 사용자 U_i는 그룹 관리자 U_n에게 자신을 인증한다. 임의의 정수 $r_i \in Z_p^*$는 각 사용자 U_i가 비밀로 간직한다.

[round 2]

step 2:

$n-1$개의 메시지 M_i를 모두 전달받은 관리자 U_n는 사용자 U_i로부터 전달받은 P_i가 정당한지를 확인하기 위하여 다음 방정식이 성립하는지를 체크한다.

$$\prod_{i=1}^{n-1} e(O_i, P) = \prod_{i=1}^{n-1} e(Q_i, H(P_i)P_{pub} + P_i)$$

만약 위의 방정식이 성립하지 않는다면 관리자 U_n는 P_i를 거부한다. P_i의 정당성 유무를 모두 확인한 후, 관리자 U_n는 GKA 프로토콜에서와 같이 집합 Ξ와 Γ를 생성하여 $M_n = MG \| \Xi \| \Gamma$를 그룹내의 모든 사용자에게 브로드캐스트를 한다.

step 3:

GKA 프로토콜의 step 3를 그대로 수행한다.

Ⅳ. 제안 프로토콜의 안전성

이 장에서는 랜덤 오라클 모델 아래에서 GKA 프로토콜과 ID-AGKA 프로토콜의 안전성에 대하여 살펴본다. 본 논문에서 사용한 안전성 모델은 [15,26]에서와 같다.

4.1 GKA 프로토콜의 안전성

제안하는 GKA 프로토콜은 BDDH 가정에 기반한 안전한 그룹 키 설정 프로토콜이다. 본 프로토콜에서의 공격자는

브로드캐스트상의 메시지를 볼 수 있는 수동적 공격자이며, 다양한 쿼리(*Send*, *Execute*, *Reveal*, *Corrupt*, *Test*)를 통해 GKA 프로토콜 참가자들과 상호 작용하여 $b \in \{0,1\}$의 값을 정확히 추측하는 것이다.

〔정리 1〕 q_{ex}를 공격자 A가 요구할 수 있는 *Execute*에 대한 최대 쿼리수라고 가정하자. 그러면 t의 수행시간을 갖는 모든 수동적 공격자 A가 프로토콜 GKA에 대하여 가질 수 있는 최대 이익 $\mathrm{Adv}_{GKA}(t, q_{ex})$은 다음과 같다.

$$\mathrm{Adv}_{GKA}(t, q_{ex}) \le 2q_{ex}\mathrm{Adv}^{BDDH}_{(e, G_1, G_2)}(t)$$

4.2 ID-AGKA 프로토콜의 안전성

제안하는 ID-AGKA 프로토콜은 CDH 가정과 BDDH 가정에 기반한 안전한 그룹 키 설정 프로토콜이다. 본 프로토콜에서의 공격자는 브로드캐스트상의 메시지를 볼 수 있고 위조 할 수 있는 능력을 가지고 있는 능동적 공격자이며, 다양한 쿼리(*Send*, *Execute*, *Reveal*, *Corrupt*, *Test*)를 통해 ID-AGKA 프로토콜 참가자들과 상호 작용하여 $b \in \{0,1\}$의 값을 정확히 추측하는 것이다.

〔정리 2〕 q_{ex}와 q_s를 공격자 A가 요구할 수 있는 *Execute*와 *Send*에 대한 각각의 최대 쿼리수라고 가정하자. 그러면 t의 수행시간을 갖는 모든 능동적 공격자 A가 프로토콜 ID-AGKA에 대하여 가질 수 있는 최대 이익 $\mathrm{Adv}_{ID-AGKA}(t, q_{ex}, q_s)$은 다음과 같다.

$$\mathrm{Adv}_{ID-AGKA}(t, q_{ex}, q_s) \le$$
$$2q_{ex}\mathrm{Adv}^{BDDH}_{(e, G_1, G_2)}(t) + (n-1)\mathrm{Adv}_{\Lambda}(t)$$

〔정리 2〕에서의 Λ는 ID-AGKA 프로토콜에서 사용된 ID 기반의 인증 방식을 나타낸 것이다. 제안하는 ID 기반의 인증 방식 Λ는 다음과 같다.

① 생성: 임의의 정수 $r \in {}_RZ_p^*$를 선택하여 $R = rP$를 계산한다. 그리고 $O = H(R)D_{ID} + rQ_{ID}$를 계산하여 R에 대한 인증정보 $Auth = \langle R, O \rangle$를 생성한다.

② 검증: R에 대한 인증정보 $Auth = \langle R, O \rangle$가 정당한지를 확인하기 위하여, $U = H(R)P_{pub} + R$을 계산하여 방정식 $e(O, P) = e(Q_{ID}, U)$이 성립하는지 확인한다.

Λ은 〔27〕의 ID 기반 서명 방식을 토대로 제안한 방식으로, CDH 문제가 어렵다면, 제안하는 ID 기반의 인증 방식 Λ은 적응적 선택 ID에서의 존재 위조 공격(Existential forgery on adaptive chosen ID attack)에 대하여 안전하다.〔27〕 다시 말하면, t의 수행시간을 갖는 모든 능동적 공격자 A가 Λ에 대하여 가질 수 있는 최대 이익 $Adv_{\Lambda}(t)$은 무시할 수 있을 만큼(negligible) 아주 작게 된다.

V. 제안 프로토콜의 효율성

본 논문에서 제안한 그룹키 설정 프로토콜들은 최근에 이슈가 되고 있는 Bilinear-pairing을 사용한 타원곡선 암호 시스템 상에서 설계하였다. Bilinear-pairing을 사용한 그룹키 설정 프로토콜은 2002년과 2003년에 각각 Nalla〔19〕와 Barua〔24〕에 의해서 제안되었다. 그러나 이들은 프로토콜의 안전성에 대한 증명을 하지 못하였고, 프로토콜의 라운드 수가 사용자 수에 의존하여 선형적으로 증가한다는 단점이 있다. 이후 2004년 Choi〔15〕가 랜덤 오라클 아래에서 안전성이 증명된 2라운드의 효율적인 그룹키 설정 프로토콜을 제안하였다. 그러나 Choi의 프로토콜은 완전 대칭적(Symmetry)인 특징을 지니기 있어 그룹내의 모든 사용자들에게 동일한 연산량을 부과한다. 뿐만 아니라 Choi의 프로토콜은 그룹 크기에 따라 브로드캐스트되는 메시지의 수가 선형적으로 증가한다는 단점을 가지고 있다. 그러므로 Choi의 프로토콜은, 그룹 사이즈가 커지면 그룹 구성원들의 통신량과 연산량도 함께 증가되기 때문에, 이동단말기의 소형화 경향으로 인해 제한된 시스템자원을 보유하는 차세대 네트워크 환경에는 적합하지 않다. 반면에 본 논문에서 제안하는 ID-AGKA 프로토콜은 사용자들이 보유하고 있는 제한된 시스템 자원을 고려하여 설계된 효율적인 2라운드의 그룹키 설정 프로토콜이다.

제안한 ID-AGKA 프로토콜은 Choi의 프로토콜과는 달리 사전계산(Pre-computation)이 가능하며, 특히, 프로토

표 1. Choi의 프로토콜과 제안하는 ID-AGKA 프로토콜과의 비교
Table 1. A Comparison with the Protocol of Choi[15]

		Choi의 프로토콜		ID-AGKA 프로토콜	
		사용자 (그룹관리자)	사용자 (Client)	사용자 (그룹관리자)	사용자 (Client)
유니캐스트					1 번
브로드캐스트		2 번	2 번	1 번	
서명 생성		1 번	1 번	1 번	1 번
서명 검증		$n-1$ 번	$n-1$ 번	1 번	1 번
연산량	사용자의 연산량	$3Ha+Inv+7Ad$ $+4Pa+5Smu$ $+(n-1)Mu$ $+(n-1)Exp$	$3Ha+Inv+7Ad$ $+4Pa+5Smu$ $+(n-1)Mu$ $+(n-1)Exp$	$(n-1)Ha$ $+(n-1)Inv$ $+(3n-2)Ad$ $+(n+2)Pa+Smu$	$Mu+Exp$
		$\Rightarrow O(n)$	$\Rightarrow O(n)$	$\Rightarrow O(n)$	$\Rightarrow O(1)$
	모든 사용자들의 연산량의 합 (그룹관리자 1명) (Client n-1명)	$3Ha+Inv+7Ad$ $+4Pa+5Smu$ $+(n-1)Mu$ $+(n-1)Exp$	$3(n-1)Ha$ $+(n-1)Inv$ $+7(n-1)Ad$ $+4(n-1)Pa$ $+5(n-1)Smu$ $+(n-1)^2Mu$ $+(n-1)^2Exp$	$(n-1)Ha$ $+(n-1)Inv$ $+(3n-2)Ad$ $+(n+2)Pa+Smu$	$(n-1)Mu$ $+(n-1)Exp$
		$\Rightarrow O(n)$	$\Rightarrow O(n^2)$	$\Rightarrow O(n)$	$\Rightarrow O(n)$

- Ha: 해쉬(hash)에 대한 평균 연산량
- Inv: G_1에서의 역(inverse)에 대한 평균 연산량
- Ad: G_1에서의 덧셈(addition)에 대한 평균 연산량
- Pa: Bilinear-pairing 평균 연산량
- Smu: G_1에서의 스칼라 곱(scalar multiplication)에 대한 평균 연산량
- Mu: G_2에서의 곱(multiplication)에 대한 평균 연산량
- Exp: G_2에서의 지수(exponentiation)에 대한 평균 연산량

콜 안전성의 변화 없이, 관리자 U_n이 $g=e(P, svP)$를 계산하는 것이 가능하므로 사용자측의 연산량에 대한 효율성을 더욱 증가시킬 수 있다. 〈표 1〉은 Choi의 프로토콜과 본 논문에서 제안한 ID-AGKA 프로토콜을 서로 비교하여 나타낸 것이며, 프로토콜의 안전성을 위하여 전송되는 그룹키 생성정보 메시지에 대해서도 인증을 실행하였다. 〈표 1〉에서 보듯이, 제안한 ID-AGKA 프로토콜은 그룹 사이즈와는 상관없이 단지 단 한번의 지수(Exponentiation)와 곱(Multiplication) 연산만으로 그룹키를 생성한다. 그러므로 본 논문에서 제안한 ID-AGKA 프로토콜은 특정 센터가 저전력 모바일 장치(Low-power mobile devices)를 보유하는 다수의 사용자들에게 서비스를 하는 응용분야에 적합하다.

Ⅵ. 결 론

유·무선 통합 네트워크에서의 보안은 무선 네트워크 환경을 충분히 고려해 이루어져야 하며, 단순히 무선 네트워크에만 그치는 것이 아니라 유선 네트워크와의 연동을 반드시 고려해야한다. 즉, 무선 단말기 고유의 이동성, 시스템 자원의 제한성 등과 유선 단말기의 비 이동성, 고성능 연산 능력 등이 함께 고려되어야한다.

본 논문에 제안하는 프로토콜은 그룹 지향적 서비스와 같이 특정 센터가 서비스를 하는 응용분야에 효율적으로 적용할 수 있도록 설계하였다. 특히 통합 환경에 능동적으로 대처할 수 있도록 사용자측의 연산량을 줄임으로서 낮은 연산 처리 능력을 가지는 시스템에 적합하도록 설계된 효율적

인 구조로 이루어져 잇다. 제안한 프로토콜은 향후 더욱 다양해지는 멀티캐스트 관련 서비스 분야에서 적극적으로 대처할 수 있을 것으로 기대된다.

참고문헌

[1] I. Ingemarsson, D. Tang, and C. Wong, "A Conference Key Distribution System", IEEE Transactions on Information Theory, 28(5): 714-720, 1982.

[2] G.H. Chiou and W.-T. Chen, "Secure Broadcasting Using the Secure Lock," IEEE Transactions on Software Engineering, 15(8):929-934, 1989.

[3] M. Burmester and Y. Desmedt, "A Secure and Efficient Conference Key Distribution System", Advances in Cryptology-Eurocrypt'94, LNCS 950, pp. 275-286, Springer-Verlag, 1994.

[4] M. Just and S. Vaudenay, "Authenticated Multi-party Key Agreement", Advances in Cryptology-Asiacrypt'96, LNCS 1163, pp. 36-49, Springer-Verlag, 1996.

[5] K. Becker and U. Wille, "Communication Complexity of Group Key Distribution", Proc. of 5th ACM Conference on Computer and Communications Security, pp. 1-6, Springer-Verlag, 1998.

[6] Y. Kim, A. Perrig, and G. Tsudik, "Simple and Fault-tolerant Key Agreement for Dynamic Collaborative Groups", Proc. of 7st ACM Conference on Computer and Communications Security, pp. 235-244, Springer-Verlag, 2000.

[7] M. Steiner, G. Tsudik, and M. Waidner, "Key Agreement in Dynamic Peer Groups", IEEE Transactions on Parallel and Distributed Systems, 11(8):769-780, 2000.

[8] W.G. Tzeng and Z.J. Tzeng, "Round-efficient Conference Key Agreement Protocols with Provable Security", Advances in Cryptology-Asiacrypt'00, LNCS 1976, pp. 614-627, Springer-Verlag, 2000.

[9] Y. Kim, A. Perrig, and G. Tsudik, "Communication-efficient Group Key Agreement", Proc. of International Federation for Information Processing, LNCS 1163, pp. 229-244, Springer-Verlag, 2001.

[10] E. Bresson, O. Chevassut, D. Pointcheval, and J.-J. Quisquater, "Provably Authenticated Group Diffie-Hellman Key Exchange", Proc. of the 8st ACM Conference on Computer and Communications Security, pp. 255-264, Springer-Verlag, 2001.

[11] E. Bresson, O. Chevassut, and D. Pointcheval, "Provably Authenticated Group Diffie-Hellman Key Exchange the Dynamic Case", Advances in Cryptology-Asiacrypt'01, LNCS 2248, pp. 290-309, Springer-Verlag, 2001.

[12] E. Bresson, O. Chevassut, and D. Pointcheval, "Dynamic Group Diffie-Hellman Key Exchange under Standard Assumptions", Advances in Cryptology-Eurocrypt'02, LNCS 2332, pp. 321-336, Springer-Verlag, 2002.

[13] C. Boyd and J.M.G. Nieto, "Round-optimal Contributory Conference Key Agreement", Proc. of the 6th International Workshop on Practice and Theory in Public Key Cryptography, LNCS 2567, pp. 161-174, 2003.

[14] J. Katze and M. Yung, "Scalable Protocols for Authenticated Group Key Exchange", Advances in Cryptology-Crypto'03, LNCS 2729, pp. 110-125, Springer-Verlag, 2003.

[15] K.Y. Choi, J.Y. Hwang, and D.H. Lee, "Efficient ID-based Group Key Agreement with Bilinear Maps", Proc. of the 7th International Workshop on Practice and Theory in Public Key Cryptography, LNCS 2947, pp. 130-134, Springer-Verlag, 2004.

[16] A. Joux, "A One Round Protocol for Tripartite Diffie-Hellman", In W. Bosma, editor, Proc. of Algorithmic Number Theory Symposium, LNCS 1838, pp. 385-394, Springer-Verlag, 2000.

[17] D. Boneh and D. Franklin, "Identity-Based Encryption from the Weil Pairing", Proc. of Crypto'01, LNCS 2139, pp. 213-229, Springer-Verlag, 2001.

[18] D. Bonech, B. Lynn, H. Shacham, "Short Signatures from the Weil Pairing", Advances in Cryptology-Asiacrypt'01, Springer-Verlag, 2001.
[19] D. Nalla and K.C. Reddy, "Identity Based Authenticated Group Key Agreement Protocol", Proc. of Indocrypt'02, LNCS 2551, pp. 215-233, Springer-Verlag, 2002.
[20] N.P. Smart. "An Identity-based Authenticated Key Agreement Protocol based on the Weil Pairing", Electronics Letters, 38(13):630-632, 2002.
[21] F. Zhang, S. Liu and K. Kim, "ID-based One Round Authenticated Tripartite Key Agreement Protocols with Pairings", Cryptology ePrint Archive, Report 2002/122, available at iacr.org /2002/122/.
[22] H. Kim, S. Kim, D. Won, "ID-Based Partially Blind Signatre under GDH Group", Proc. of the International Conference on Number Theory for Secure Communications 20th, pp. 159, 2003.
[23] S.S. Al-Riyami, K.G. Paterson, "Certificateless Public Key Cryptography", Advances in Cryptology -Asiacrypt'03, LNCS 2784, Springer Verlag, 2003.
[24] R. Barua, R. Dutta and P. Sarker, "Extending Joux's Protocol to Multi Party Key Agreement", Proc. of Indocrypt'03, LNCS 2904, pp. 205-217, Springer-Verlag, 2003.
[25] A. Shamir, "Identity-based Cryptosystems and Signature Schemes", Advances in Cryptology -Crypto'84, LNCS 196, pp. 47-53, Springer -Verlag, 1984.
[26] J. Nam, J. Lee, S. Kim, and D. Won, "DDH -based Group Key Agreement for Mobile Computing", Cryptology ePrint Archive, Report 2004/127, available at iacr.org/2004/127/.
[27] J. Cheon, Y. Kim, and H. Yoon, "A New ID -based Signature with Batch Verification", Cryptology ePrint Archive, Report 2004/131, available at iacr.org/2004/131/.

저 자 소 개

김 현 주

1995년 세명대학교 수학과(이학사)
1997년 서강대학교 대학원 수학과 (이학석사)
2005년 성균관대학교 전기전자 및 컴퓨터공학과(공학박사)
현재 성균관대학교 정보통신공학부 연구전임강사
〈관심분야〉 암호이론, 이동통신보안

남 정 현

1997년 성균관대학교 정보공학과 (공학사)
2002년 Computer Science, University of Louisiana, Lafayette(M.S.)
현재 성균관대학교 대학원 정보통신 공학부 박사과정
〈관심분야〉 암호이론, 이동통신보안, 네트워크 보안

김 승 주

1994년 성균관대학교 정보공학과 (공학사)
1996년 성균관대학교 대학원 정보 공학과(공학석사)
1999년 성균관대학교 대학원 정보 공학과(공학박사)
현재 한국정보보호학회 논문지 편집위원
현재 한국정보통신기술협회(TTA) IT 국제표준화 전문가
현재 성균관대학교 정보통신공학부 교수
현재 한국정보과학회 논문지 편집위원
〈관심분야〉 암호이론, 정보보호제품 및 스마트카드 보안성평가

원 동 호

성균관대학교 전자공학과(학사, 석사, 박사)
1988년~1999년 성균관대학교 교학처장, 전기전자 및 컴퓨터공학부장, 정보통신대학원장, 정보통신기술연구소장
1996년~1998년 국무총리실 정보화추진위원회 자문위원
2002년~2003년 한국정보보호학회장
2003년~2004년 성균관대학교 연구처장
1982년~현재 성균관대학교 정보통신공학부 교수
2000년~현재 정보보호인증기술연구소장
〈관심분야〉 암호이론, 정보시스템보안 등