무선 단말기의 계산 효율성을 고려한 유·무선 통합 네트워크 환경에 적합한 그룹 키 동의 프로토콜*

장우석†, 김현주, 남정현, 조석향, 원동호, 김승주‡

성균대학교 정보통신공학부 정보보호연구소

Group Key Agreement Protocol Considering Computational Efficiency of Mobile Devices for Integrated Wired/Wireless Networks *

Woosuk Chang†, Hyunjue Kim, Junghyun Nam, Seokhyang Cho,

Dongho Won, Seungjoo Kim‡

Information Security Group, School of Information and Communication Engineering,

Sungkyunkwan University

요 약

그룹 키 동의 프로토콜에 관한 연구는 그동안 많은 연구자들에 의해 다양한 관점에서 진행되어 왔으며, 최근 Nam 등이 유·무선 통합 네트워크 환경에서 효율적이면서도 안전한 그룹 키 동의 프로토콜을 제안하였다. 유·무선 통합 네트워크 환경에 적합한 그룹 키 동의 프로토콜을 설계하기 위해서는 고성능 연산 능력을 가진 유선 단말기의 특성과 상대적으로 계산능력이 떨어지는 무선 단말기의 특성이 함께 고려되어야 한다. 특히, 시스템자원의 제한성을 갖는 무선 단말기에서의 계산량을 최소화하는 문제는 그룹 키 동의 프로토콜 설계에 있어서 무엇보다 중요하다. 따라서, 본 논문에서는 무선 단말기의 계산량을 최소화하면서 유·무선 통합 네트워크 환경에 적합한 효율적인 그룹 키 동의 프로토콜을 제안하고자 한다.

I. 서론

그룹 키 동의 프로토콜(group key agreement protocol)은 일련의 그룹을 형성하는 다수의 통신 참여자들이 공개된 통신망 상에서 세션키(session key)라 불리는 그룹의 공통 비밀키를 공유함으로써 그룹 내에서의 안전한 통신을 가능하게 하는 프로토콜이다.

다수의 사용자가 참여하는 다양한 응용프로그램(유료 영상 서비스, 원격 사이버 강의, 다중 사용자 게임, 커뮤니티 채팅 등)에서 이 세션키를 공유함으로써 인증(Authentication), 기밀성(Confidentiality), 그리고 메시지의 무결성(Message Integrity) 등과 같은 보안 서비스를 효과적으로 제공할 수 있다. 이와 같은 그룹 기반의 응용프로그램들이 현대 컴퓨팅 환경에서 급증하고 있는 반면에 미래의 네트워크 환경이라고 할 수 있는 유·무선 통합 네트워크 환경에서의 안전한 그룹 통신을 위한 그룹 키 동의 프로토콜에 대한 연구는 아직 시작 단계에 불과하다. 최근, Nam 등은 유·무선 통합 네트워크 환경에서 효율적이면서도 안전한 그룹 키 동의 프로토콜을 제안하였다[2]. 유·무선 통합 네트워크 환경에 적합한 그룹 키 동의 프로토콜을 설계하기 위해서는 무선 단말기 특성과 유선 단말기 특성이 함께 고려해야 한다. 특히, 무선 단말기의 이동성과 시스템 자원의 제한성 등으로 인하여 유·무선 통합 네트워크 환경에서의 그룹 키 동의 프로토콜은 무선 단말기에서의 계산량을 줄이는 데에 보다 초점을 맞추어 설계되어야 한다. 따라서, 본 논문에서는 무선 단말기에서의 계산량을 최소화하면서 유·무선 통합 네트워크 환경에 적합한 효율적인

* 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 육성·지원 사업의 연구결과로서 수행되었음.

† 주저자 : wschang@security.re.kr

‡ 교신저자 : skim@security.re.kr

그룹 키 동의 프로토콜을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 네트워크 환경에 따른 기존의 contributory 그룹 키 동의 프로토콜에 대해 살펴보고, 3장에서는 무선 단말기의 계산 효율성을 고려한 유·무선 통합 네트워크 환경에 적합한 그룹 키 동의 프로토콜을 제안한다. 그리고 4장에서는 제안한 프로토콜의 효율성을 분석하며, 마지막으로 5장에서는 결론을 맺는다.

II. 관련 연구

본 장에서는 이제까지 연구되었던 contributory 그룹 키 동의 프로토콜을 유선 네트워크 환경, 무선 네트워크 환경, 유·무선 통합 네트워크 환경에 따라 살펴보기로 한다.

1.1 유선 네트워크 환경

유선 네트워크 환경에 적합한 가장 대표적인 그룹 키 동의 프로토콜로는 1994년 Burmester와 Desmedt[3]에 의해 제안된 BD 프로토콜과 1996년 Steiner, Tsudik와 Waidner[4]에 의해 제안된 GDH.2 프로토콜이 있다. BD 프로토콜은 완전한 전방향 안전성을 만족한다. 그러나 GDH.2 프로토콜은 $O(n)$번의 모듈러 멱승 연산과 통신 라운드를 요구하는 단점이 있으며, BD 프로토콜은 그룹 크기에 따라 브로드캐스트되는 메시지의 수가 선형적으로 변한다는 단점이 있다.

1.2 무선 네트워크 환경

무선 네트워크 환경에 적합한 가장 대표적인 그룹키 동의 프로토콜로는 2003년도에 Bresson 등[5]이 제안한 프로토콜 있다. [5]은 저전력 모바일 단말기와 게이트웨이 사이에서의 효율적인 그룹 키 동의에 관한 방법을 제안하였다.

최근, 2005년도에 Cho 등[6]은 모바일 환경에 적합한 그룹 키 동의 프로토콜을 제안하였다. 그러나, [6]는 [5]과 마찬가지로 고성능 연산 능력을 가진 한 명의 사용자(서비스 제공자)가 그룹의 세션키를 계산하기 위해서 $O(n)$의 연산을 수행하는데 비해 그룹에 참여하는 나머지 사용자들(모바일 사용자들)은 단지 $O(1)$의 연산만을 수행하는 비대칭적 구조의 문제점을 안고 있다.

1.3 유·무선 통합 네트워크 환경

최근 Nam 등은 유·무선 통합 네트워크 환경에서의 효율적이고도 안전한 그룹 키 동의 프로토콜을 제안하였다[2]. 이 논문에서는 유선 사용자 그룹과 무선 사용자 그룹을 높이가 2인 트리구조를 이용하여 네트워크를 구성하였으며, DDH (Decisional Diffie-Hellman)문제에 기반하여 수동적 공격자에 대한 안전함을 증명하였다. 하지만, 제안된 프로토콜은 무선 사용자 그룹에서 3번의 모듈러 멱승 연산과 2번의 모듈러 곱셈 연산을 수행해야 하므로 제한된 시스템 자원을 보유한 무선 단말기에서의 계산량을 최소화할 필요성이 있다.

III. 제안하는 그룹 키 동의 프로토콜

본 장에서는 무선 단말기에서의 계산량을 최소화하면서 유·무선 통합 네트워크 환경에 적합한 효율적인 새로운 contributory 그룹 키 동의 프로토콜을 제안한다.

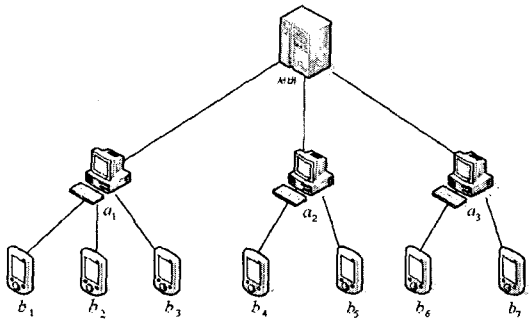
본 논문에서 제안하는 그룹 키 동의 프로토콜에서 사용될 시스템 파라미터의 정의는 [표1]과 같다.

전체 네트워크는 [그림1]과 같이 $L_0 = \{서버\}$, $L_1 = \{a_1, \cdots, a_m\}$, $L_2 = \{b_1, \cdots, b_n\}$으로 구성되어

[표1] 시스템 파라미터 정의

파라미터	정의
L_0	트리구조의 최상위 레벨에 속한 서버
L_1	트리구조의 레벨1에 속한 유선 사용자들의 집합
L_2	트리구조의 레벨2에 속한 무선 사용자들의 집합
I_{a_j}	그룹멤버 a_j의 자식 그룹 멤버들 index 집합
$p=k \cdot q+1$	큰 소수(k는 정수, q는 소수)
G	모듈러 p상에서 위수 q를 갖는 순환 부분군
g	모듈러 p상에서 위수 q를 갖는 순환 부분군의 원시 원소
$sign$	서명 알고리즘
$verify$	검증 알고리즘
E	암호화 알고리즘
D	복호화 알고리즘
$H()$	일방향 해쉬함수
K_j	그룹멤버 a_j와 그 자식 그룹멤버들 I_{a_j}간의 서브그룹키
SK	전체 그룹의 세션키

있다고 가정한다. 다음은 제안한 프로토콜의 자세한 실행 과정을 나타낸다.



[그림1] 유·무선 통합 네트워크 구성

(라운드 1.) 각각의 그룹 멤버 $b_i \in L_2$는 임의의 $r_{b_i} \in Z_q$를 선택하여 $z_{b_i} = g^{r_{b_i}}$를 계산한 다음, 각각의 개인키 sk_{b_i}로 z_{b_i}를 서명하여 $\sigma_{b_i} = sign_{sk_{b_i}}(z_{b_i})$를 얻는다. 그런 다음, (z_{b_i}, σ_{b_i})를 트리상의 부모 노드인 그룹 멤버 $a_j \in L_1$에게 전송한다. 그리고, 서버는 임의의 $s_s, r_s \in Z_q$를 선택하여 $z_s = g^{r_s}$, $w_s = g^{s_s}$와 $\hat{x}_s = w_s^{r_s} = g^{s_s r_s}$을 계산한 다음, 서버의 개인키 sk_s로 z_s를 서명하여 $\sigma_s = sign_{sk_s}(z_s)$를 얻는다. 그런 다음, (z_s, σ_s)를 트리상의 자식 노드인 그룹 멤버 $a_j \in L_1$에게 브로드캐스트 한다. 한편, $a_j \in L_1$는 임의의 $s_j, r_{a_j} \in Z_q$를 선택하여 $w_j = g^{s_j}$와 $x_{a_j} = (w_j)^{r_{a_j}} = g^{s_j r_{a_j}}$를 계산한다.

(라운드 2.) $a_j \in L_1$는 각각의 자식 그룹멤버 b_i로부터 (z_{b_i}, σ_{b_i})를 수신한 뒤 b_i의 공개키 pk_{b_i}를 이용하여 서명값 σ_{b_i}를 검증한 다음, 서명값이 모두 옳다면

$$x_{b_i} = (z_{b_i})^{s_j} = g^{s_j r_{b_i}}$$

를 계산한다. 또한, $a_j \in L_1$는 서버로부터 (z_s, σ_s)를 수신한 뒤 서버의 공개키 pk_s를 이용하여 서명값 σ_s를 검증한 다음, 서명값이 옳다면

$$x_s = (z_s)^{s_j} = g^{s_j r_s}$$

를 계산한다. 그리고, a_j는 안전성 파라미터로 일회용의 l비트, $\delta_{a_j} \in \{0,1\}^l$를 선택하여

$$X_j = \oplus_{i \in I_{a_j}} H(\delta_{a_j} \| x_{b_i}) \oplus H(\delta_{a_j} \| x_{a_j}),$$
$$Y_j = \{y_{b_i} | i \in I_{a_j}\}$$

를 계산하고,

$$X_{js} = H(\delta_{a_j} \| x_{a_j}) \oplus H(\delta_{a_j} \| x_s),$$
$$Y_{js} = \{y_{js} | j \in [1,n]\}$$

를 계산한다. 이 때, $y_{b_i} = X_j \oplus H(\delta_{a_j} \| x_{b_i})$, $y_{js} = X_{js} \oplus H(\delta_{a_j} \| x_s)$이다. 그런 다음, 각각의 $a_j \in L_1$와 그 자식 그룹 멤버들간의 서브그룹키 $K_j = H(Y_j \| X_j)$를 계산하고, 서버와 각각의 $a_j \in L_1$간의 비밀키 $K_{js} = H(Y_{js} \| X_{js})$를 계산하여 K_j를 다음과 같이 암호화 한다:

$$\hat{z}_{a_j} = E_{K_{js}}(K_j).$$

마지막으로, $a_j \in L_1$는 자신의 개인키 sk_{a_j}를 이용하여 메시지 $\delta_{a_j} \| w_j \| \hat{z}_{a_j} \| Y_j \| Y_{js}$에 대해서 서명 $\sigma_{a_j} = sign_{sk_{a_j}}(\delta_{a_j} \| w_j \| \hat{z}_{a_j} \| Y_j \| Y_{js})$를 생성하고, $(\delta_{a_j}, w_j, \hat{z}_{a_j}, Y_j, Y_{js}, \sigma_{a_j})$를 자신의 자식 그룹 멤버들과 서버에게 브로드캐스트 한다.

(라운드 3.) 서버는 각 자식 그룹멤버 a_j로부터 $(\delta_{a_j}, w_j, \hat{z}_{a_j}, Y_j, Y_{js}, \sigma_{a_j})$를 수신한 뒤 a_j의 공개키 pk_{a_j}를 이용하여 서명값 σ_{a_j}를 검증하여 서명값이 옳다면, 서버와 $a_j \in L_1$간의 공통 비밀값 X_{js}와 비밀키 K_{js}를 다음과 같이 계산한다:

$$X_{js} = y_{js} \oplus H(\delta_{a_j} \| (w_j)^{r_s}) = y_{js} \oplus H(\delta_{a_j} \| g^{s_j r_s}),$$
$$K_{js} = H(Y_{js} \| X_{js}).$$

그리고, K_{js}를 이용하여 $\hat{z}_{a_j}$를 다음과 같이 복호화 한다:

$$K_j = D_{K_{js}}(E_{K_{js}}(K_j)).$$

그런 다음, 서버는 안전성 파라미터로 일회용의 l비트, $\delta_s, K_{sr} \in \{0,1\}^l$을 선택하여

$$X = \oplus_{j=1}^{m} H(\delta_s \| K_j) \oplus H(\delta_s \| K_{sr})$$

를 계산하고, $Y = \{\hat{y_j} | j \in [1,m]\}$를 계산한다. 이 때, $\hat{y_j} = X \oplus H(\delta_s \| K_j)$이다. 마지막으로, 서버의 개인키 sk_s를 이용하여 메시지 $\delta_s \| Y$에 대해서 서명 $\sigma_s = sign_{pk_s}(\delta_s \| Y)$를 생성하고, $(\delta_s \| Y \| \sigma_s)$

를 그룹의 모든 멤버들에게 브로드캐스트 한다. (키 계산.) 모든 $a_j(j\in[1,m])$와 그 자식 멤버인 $b_i(i\in I_{a_j})$에 대하여, $b_i\in L_2$는 $a_j\in L_1$로부터 받은 브로드캐스트 메시지에 대해 $a_j\in L_1$의 공개키 pk_{a_j}를 이용하여 서명값 σ_{a_j}를 검증한 뒤 서명값이 옳다면, 서브그룹 공통 비밀값 X_j와 서브그룹키 K_j를 다음과 같이 계산한다:

$$X_j = y_{b_i}\oplus H\left(\delta_{a_j}\parallel (w_j)^{r_{b_i}}\right)= y_{b_i}\oplus H\left(\delta_{a_j}\parallel g^{s_j r_{b_i}}\right),$$

$$K_j = H(Y_j\|X_j).$$

마지막으로, 모든 $a_j(j\in[1,m])$와 $b_i(i\in[1,n])$는 서버로부터 받은 브로드캐스트 메시지를 서버의 공개키 pk_s를 이용하여 서명값 σ_s를 검증한 뒤 서명값이 옳다면, 전체 그룹의 공통 비밀값 X와 전체 그룹의 세션키 SK를 다음과 같이 계산한다:

$$X=\hat{y}_j\oplus H(\delta_s\parallel K_j),\ SK=H(Y\|X).$$

IV. 효율성 분석

3장에서 제안한 프로토콜은 [표2]에서와 같이, 사용 가능한 전력이 극히 제한적인 무선 단말기 사용자의 계산량 측면에 있어서 매우 효율적이다. Nam 등의 프로토콜은 3번의 모듈러 멱승 연산을 필요로 하는데 비해 본 논문에서 제안한 프로토콜의 경우는 2번의 모듈러 멱승 연산만을 필요로 한다. 또한, 본 논문에서는 Nam 등의 프로토콜에서 사용된 모듈러 곱셈 연산 대신 해쉬 함수와 XOR 연산을 사용하여 계산 효율성을 보다 높였다.

[표2] 제안된 프로토콜의 효율성 비교

비교 \ 스킴		Nam 등의 프로토콜	제안하는 프로토콜
계산량	무선단말기	$3E+2M$	$2E+2H$
통신량	라운드	3	3
	유니캐스트	$t-m-1$	$t-m$
	브로드캐스트	$m+1$	$m+2$

E:모듈러 멱승 M:모듈러 곱셈 H:해쉬함수
t:그룹전체 수 m:유선사용자 그룹의 수

V. 결론

본 논문에서는 무선 단말기에서의 계산량을 최소화하면서도 유·무선 통합 네트워크 환경에 적합한 효율적이고 안전한 그룹 키 동의 프로토콜을 제안하였다. 제안하는 프로토콜은 무선 단말기에서의 계산 효율성이 뛰어나 차세대 유·무선 통합 네트워크 환경에서의 다양한 멀티미디어 서비스는 물론 여러 가지 그룹 응용 서비스에 활용될 수 있을 것으로 기대된다.

[참고문헌]

[1] I. Ingemarsson, D. Tang, and C. Wong, "A Conference Key Distribution System", IEEE Transactions on Information Theory, September, 1982.

[2] J. Nam, S. Kim, D. Won, "Secure Group Communications over Combined Wired and Wireless Networks", Proc. of TrustBus 2005, International Conference on Trust, Privacy, and Security in Digital Business (in conjunction with DEXA 2005), Springer-Verlag, LNCS 3592, pp. 90-99, 2005.

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

[4] M. Steiner, G. Tsudik and M. Waidner, "Diffie-Hellman Key Distribution Extended to Group Communication", Proceedings of the 3rd ACM Conference on Computer and Communications Security (CSS'96), pp.31-37, 1996.

[5] E. Bresson, O. Chevassut, A. Essiari, and D. Pointcheval, "Mutual authentication and group key agreement for low-power mobile devices", In Proc. of the 5th IFIP-TC6/IEEE International Conference on Mobile and Wireless Communications Networks (MWCN'03), pp. 59-62, 2003.

[6] S. Cho, J. Nam, S. Kim, and D. Won, "An Efficient Dynamic Group Key Agreement for Low-Power Mobile Devices", Proceedings of ICCSA 2005, International Conference on Computational Science and Applications, Springer-Verlag, LNCS 3480, Singapore, pp. 498-507, 2005.