이동 애드혹 망을 위한 패스워드 기반의 그룹키 동의 프로토콜

최연이° 조인휘
신성대학° 한양대학교
yychoi@shinsung.ac.kr°, iwjoe@hanyang.ac.kr

A Password-based Group Key Agreement Protocol for Mobile Ad-Hoc Networks

Yeonyi Choi° Inwhee Joe
Shinsung College° Hanyang University

요 약

이동 애드혹 망은 기반구조가 없는, 즉, 고정된 라우터나 백본망 같은 기반구조가 없는 무선 이동 노드들로 구성된 망이다. 현재 이동 애드혹 망은 기반구조가 없어 보안이 가장 취약한 부분이다. 본 논문에서는 클러스터 구조 기반의 이동 애드혹 환경에서 안전하고 효율적인 방법으로 그룹의 세션키를 공유하는 패스워드 기반의 그룹키 동의 프로토콜을 제안한다. 그룹키 동의 프로토콜은 일련의 그룹을 형성하는 다수의 통신 참여자들이 공개된 통신망에서 안전하고 효율적인 방법으로 그룹의 세션키를 설정한다. 하지만 기존의 연구는 모두 상당한 양의 통신부하를 유발한다. 따라서 제안 프로토콜은 이동 애드혹 망에 적합한 대칭키 기반으로, 최적의 전송 메시지 복잡도와 2번의 통신 라운드를 요구하기 때문에 매우 효율적이다. 또한 그룹 구성원의 변경이 가능한 동적 특성과 전방향 안전성을 제공한다.

1. 서론

이동 애드혹 망(Mobile Ad-hoc Network)은 이동성을 가진 다수의 노드들에 의해 자율적으로 구성되는 네트워크 기반구조(Infrastructure)가 없거나 기반구조에 기초한 네트워크 구성이 어려운 지역에서 임시 네트워크 구성이 목적인 새로운 형태의 통신망이며, 다양한 형태로 발전하고 있다. 노드들의 이동으로 동적인 네트워크 토폴로지, 전송대역폭 및 전송거리상의 제약성, 중앙 집중적인 관리 노드의 부재, 에너지 사용상의 제약성, 또한 무선망 고유의 보안 취약성 등의 여러 문제점을 해결하기 위하여 다양한 연구가 진행되고 있다[1,2,3].

이동 애드혹 망 환경은 기존의 네트워크보다 보안 대책이 어려운 문제로 인식되어 기존의 방식이 아닌 새로운 개념의 검토가 이루어져야 한다. 따라서, 이동 애드혹 망 환경에서 보안 메커니즘은 매우 중요한 문제이며, 보안 연구는 크게 키관리 메카니즘과 라우팅 프로토콜 보안으로 나눌 수 있다. 그중에서 안전한 키 관리는 가장 중요하고 복잡한 일이다.

이동 애드혹 망 환경에서의 기존 보안 연구는 Threshold Cryptography를 이용한 비밀분산기법[1]을 사용하여 애드 혹 망내의 호스트들이 CA을 하고 각 노드들에게 인증서를 발급하는 공개키 암호시스템을 이용한 애드 혹 환경에 적용한 인증기법[4], 안전한 라우팅을 위한 보안기법[5,6]들이 있다. 그러나 이동 애드혹 망 환경에 적용하기에는 공개키 암호 방식은 즉 공개키기반구조(PKI)를 사용할 경우, 인증서 취소를 위한 폐기된 키의 리스트를 인증 서버를 통한 확인 문제와 또한 상대방 노드의 신뢰하는 공개키의 분배가 어렵다[7].

본 논문에서는 애드혹 망 특성에 의해 회의장과 같은 특정한 공간에서 소규모 그룹회의 환경을 위하여, 클러스터 구조의 이동 애드혹 망을 구성하여 안전하고 효율적인 방법으로 그룹의 세션키를 공유하는 패스워드 기반의 그룹키 동의 프로토콜을 제안한다. 본 논문의 구성은 다음과 같다. 2 장에서는 프로토콜 설계의 보안 요구사항을 분석하고, 3 장에서는 본 논문에서 제안하는 새로운 패스워드 기반 그룹키 동의 프로토콜을 제안한다. 4 장에서 제안한 프로토콜의 안전성과 효율성을 분석한다. 마지막으로 5 장에서 결론을 맺는다.

2. 패스워드 기반 그룹키 공유 프로토콜의 보안 요구사항

2.1 안전한 그룹통신을 위한 보안 요구사항

안전한 그룹통신의 핵심은 그룹키의 관리에 있으며 그룹키에 대한 안전성과 관리 시스템의 효율성 고려하여야 한다.

•그룹키 비밀성(Group Key Secrecy), 그룹키는 그룹 구성원들만이 공유하여야 한다. 가장 기본적인 성질로서, 어떤 악의적인 공격자가 그룹키의 도출이 계산상 불가능 하여야 한다.

•그룹키 독립성(Group Key Independence), 그룹키 집합 K의 적당한 부분집합 K'를 알고 있는 공격자가 그룹키의 다른 부분집합 $K \in (K-K')$를 계산 할 수 없어야 한다.

•완전한 전방향 안전성(Perfect Forward Secrecy), 공격자가 그룹 구성원의 개인키를 알더라도 과거에 사용된 그룹키를 알아낼 수 없다면 그룹키 설정 프로토콜은 완전한 전방향 안전성을 제공한다고 한다.

그룹키 관리의 효율성과 확장성 측면의 고려사항은 동

적 특성, 한 세션동안 사용자들의 그룹 가입(Join)과 탈퇴(Leave)가 발생하는 동적특성을 고려하여야 한다.

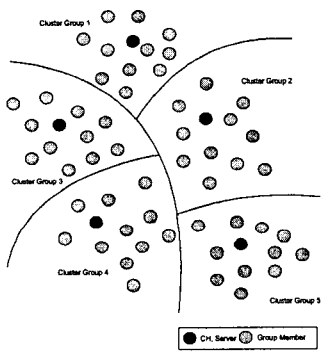
2.2 패스워드 기반 프로토콜의 보안 요구사항

•오프라인 사전 공격 (Off-line Password Dictionary Attack)에 대한 안전성

정당한 인증 프로토콜 실행 중에 공격자가 도청과 같은 수동적 공격으로 패스워드에 대한 어떠한 정보도 획득 불가능하여야 한다.

2.3 클러스터 기반 이동 애드혹 망 보안 요구사항

계산능력과 저장 공간의 제약과 낮은 대역폭의 무선채널, 노드의 이동성의 특성에 기인한 Hand-off허용 이 필요하다.



[그림1] Cluster-based Mobile Ad-Hoc Networks

3. 제안하는 효율적인 패스워드 기반의 그룹키 동의 프로토콜

다음은 본 논문에서 사용될 기호 표현에 대한 정의이다.

- U_i : i번째 사용자. 그룹원.
- U_n : 서버, CH(cluster head).
- p : $p=2q+1$, q는 큰 소수 - g : z_P^*상의 원시원소.
- r_i : 사용자 i가 선택한 랜덤 값.
- pwd : 프로토콜 참여자들이 소유한 공유 패스워드.
- $E_{pwd}(m)$: 패스워드 pwd를 사용하여 메시지 (m)을 암호화.
- $H(\ ):\{0,1\}^* \rightarrow \{0,1\}^r$ 인 해쉬함수.
- K : 세션 그룹 키.

제안하는 프로토콜은 올바른 그룹 구성원들은 회의장 입장 전에 안전한 방법으로 그룹 간에 공유된 패스워드를 공유하고, 항상 정직하게 행동한다. 또한 이동 애드혹 망 고유 특성으로 상호인증을 위한 인증서나 신뢰할 수 있는 KDC(Key Distribution Center)의 사용 불가능하고 그룹 내에는 회의주최 측의 무선 호스트가 서버(CH)로서 존재하며, 좀 더 강력한 계산능력을 갖는다.

3.1 그룹키 초기화 : [프로토콜 IKA]

그룹원 $U_1, U_2, \cdots, U_{n-1}$와 서버 U_n로 구성된 n명의 멀티캐스트 그룹 $MG=\{U_1, U_2, \ldots, U_n\}$은 프로토콜 IKA로부터의 세션 그룹 키 생성을 가정한다.

<라운드 1> $U_i \neq U_n$인 각 그룹원은 랜덤 수 $r_i \in Z_q$를 선택한 후 $z_i = g^{r_i}$를 계산한다. 그룹원들 간에 사전 공유한 패스워드(pwd)로 암호화하고, 이 값 $m_i = E_{pwd}(z_i)$을 서버에 전송한다. 서버 또한 $r, r_n \in Z_q$인 랜덤 수를 선택한 후 $z = g^r$과 $x_n = g^{rr_n}$을 계산한다.

<라운드 2> 서버는 그룹원이 전송한 메시지 m_i를 복호화하여 $x = z_i^r$를 구하고, $X = \Pi_{i\in[1,n]} x_i \bmod p$인 $X = x_1 \cdot x_2 \cdot \cdots \cdot x_n$와 $y_i = X \cdot x_i^{-1} \bmod p$ 집합 $Y = \{y_i \mid 1 \le i \le n-1\}$를 계산한다. 서버는 그룹원 모두에게 패스워드로 암호화한 $m_n = E_{pwd}(z) \| Y$을 브로드 캐스트 한다.

<키 계산> 그룹원인 각 사용자 U_i 는 서버로부터 수신된 메시지 m_n을 이용하여 다음 $X = y_i \cdot z^{r_i} \bmod p$를 계산하고 그룹원과 서버 모두 세션 그룹 키 K를 다음과 같이 계산 한다.:

$$K = H(y_1 \mid \cdots \mid y_{n-1} \mid X).$$

3.2 그룹원 탈퇴 : [프로토콜 LP1]

그룹원 j가 탈퇴한 새로운 멀티캐스트 그룹 $MG = MG_p \setminus J$ 은 삭제된 그룹원을 제외한 모든 그룹원과의 새로운 세션 그룹 키를 생성한다.

<라운드 1> 그룹원 탈퇴의 경우 서버 U_n은 새로이 $r', r'_n \in Z_q$값을 선택하고 $z' = g^{r'}$과 $x'_n = g^{r'r_n}$를 계산 후, 기존의 r과 x_n대신 r'과 x'_n을 사용하여 IKA 프로토콜의 절차를 수행한다. X와 Y를 새로이 계산하고 패스워드로 암호화하여 탈퇴자를 제외한 그룹원 모두에게 $m'_n = E_{pwd}(z, z') \| Y$를 브로드 캐스트 한다.

<키 계산> 각 그룹원은 전송받은 메시지 m'_n를 복호화하여 $X = y_i \cdot z''^{r_i} \bmod p$를 구한 후 그룹원과 서버 모두 새로운 세션 그룹 키 K'를 다음과 같이 계산한다.

$$K' = H(y_1 \mid \cdots \mid y_{n-1} \mid X).$$

3.3 그룹원 가입 : [프로토콜 JP1]

새로운 그룹원인 j 가 가입된 새로운 멀티캐스트 그룹 $MG = MG_p \cup J$ 으로 가정한다. 기존의 프로토콜과 동일하나, 서버는 새로운 가입자와 기존 그룹원에게 가입 프로토콜을 수행하여 새로운 세션 그룹 키를 생성한다.

<라운드 1> 새로운 그룹원 $U_i \in J$ 는 랜덤 수 $r_i \in Z_q$를 선택한 후 $r_i \in Z_q z_i = g^{r_i}$를 사전 공유한 패스워드 ($pwd$)로 암호화하여 $m_i = E_{pwd}(z_i)$을 서버에 전송한다.

<라운드 2> 서버 U_n은 새로운 랜덤 수 $r', r'_n \in Z_q$를 생성한 후 $z' = g^{r'}$과 $x'_n = g^{r'r_n}$를 계산한 후 기존의 r과 x_n대신 r'과 x'_n을 사용하여 IKA 프로토콜의 절차를 수행한다. X와 Y를 새로이 계산 후 사전 공유 패스워드

로 암호화하여 각 그룹원 모두에게 $m'_n = E_{pwd}(z, z') \| Y$를 브로드 캐스트 한다.

<키 계산> 각 그룹원은 전송받은 메시지 m'_n를 복호화하여 $X = y_i \cdot z^{r'_i} \bmod p$를 구한 후 그룹원과 서버 모두 새로운 세션 그룹 키 K'를 다음과 같이 계산한다.

$$K' = H(y_1 \| \cdots \| y_{n-1} \| X).$$

4. 제안 프로토콜 평가

4.1 안전성 분석

4.1.1 오프라인 사전 공격 (Off-line Password Dictionary Attack)에 대한 안전성

선택된 패스워드 PWD'으로 $E_{pwd}(g^{r_1})$과 $E_{pwd}(g^{r_n})$을 복호화하여 g^{r_1}과 g^{r_n}을 구할 수 있지만, 올바른 값 여부 확인을 위해 다시 $g^{r_1 r_n}$을 구한 다음 세션키 K를 구해야 한다. 따라서 패스워드를 찾는 문제가 Diffie-Hellman 문제로 귀결되어 사전공격으로 실제 패스워드를 찾기 힘들다.

4.1.2 수동적 공격자에 대한 안전성 (Security Against Passive Attacker)

제안한 프로토콜의 수행 중 수동적 공격자에게 노출되는 정보는 <라운드 1과 2>에서의 $E_{pwd}(g^{r_n})$, $E_{pwd}(g^{r_1})$, Y 값이다. 이 정보로 세션 키를 획득하려면 $g^{r_n r_1}$값을 알아야한다. 이는 공격자가 $E_{pwd}(g^{r_1})$로부터 g^{r_1}값을 구해도 이산대수문제로 귀결된다.

4.1.3 완전한 전방향 안전성 (Perfect Forward Secrecy)

공격자는 획득한 패스워드로, 이전 세션에서 패스워드로 암호화된 메시지 $E_{pwd}(g^{r_1}), \ldots, E_{pwd}(g^{r_n})$로부터 $g^{r_1}, \ldots, g^{r_n}$은 알 수 있지만, 이산대수 문제에 의해서 $g^{r_1 r_n}, g^{r_2 r_n}$를 구할 수 없어 세션 키 정보 획득이 불가능 하여 전방향 안전성을 제공한다.

4.2 효율성 분석

제안한 논문을 통신량과 계산량 측면에서 기존 프로토콜과의 효율성 분석이다.

[표1] 기존 프로토콜과의 효율성 분석

효율성 / 프로토콜		통신량				계산량
		라운드	메시지	유니캐스트	브로드캐스트	모듈러
Asokan& Ginzboorg[8]		n+2	3	2n-2	n+1	$O(n)$Exp
Hwang& Lee [9]		2	2n	-	2n	$O(n)$Exp
제안 방식	IKA	2	1	n-1	1	$O(n)$Exp
	가입	2	1	j	1	$O(n)$Exp
	탈퇴	1	1	-	1	$O(n)$Exp

1) IKA : 초기 키 동의. 2) 모듈러 : 모듈러 연산.
3) n : 새롭게 갱신된 구성원의 수.
4) j : 가입자의 수.
5) Exp : 참여자 모두의 모듈러 지수승 총 수.
6) 라운드 : 프로토콜 수행에 필요한 총 수.
7) 메시지 : 사용자 한 명당 받는 메시지 수.

본 논문에서 제안한 프로토콜은 [표1]에서, 그룹원의 가입과 탈퇴에 따른 갱신의 동적특성과 확장성, 2 라운드 통신과 계산량 측면에서 효율적인 프로토콜이다.

5. 결론

본 논문은 이동 애드혹 망에 적합한 라운드 수와 메시지 수 측면에서 효율적인 패스워드 기반의 그룹키 동의 프로토콜을 제안하였다. 이 프로토콜은 최적의 메시지 복잡도와 2번 통신 라운드로 효율적이며, 그룹 구성원의 변경을 고려한 동적인 프로토콜이다. 또한 전방향 안전성을 제공한다. 이동 애드혹 망의 일반화된 환경에서는 탈퇴자와 내부 구성원과의 공모에 의한 안전성 침해 등 향후 연구가 필요하다.

[참고 문헌]

[1] L. Zhou and Z. J. Haas, "Securing Ad Hoc Networks", IEEE Network Magazine, Volume 13, Issue 6, 1999.

[2] H. Luo and S. Lu, "Ubiquitous and Robust Authentication Services for Ad Hoc Wireless Networks", Technical Report 200030, UCLA Computer Science Department 2000.

[3] J. Kong, P. Zerfos, H, Lu, S.Lu and L. Zhang, "Providing Robust and Ubiquitous Security Support for Mobile Ad-Hoc Network", Proceedings of the 9th Conference on Network Protocols(ICNP), pp.251-260, 2001.

[4] Srdjan Capkun, Levente Buttyan and Jean-Pierre Hubaux, "Self-Organized Public-Key Management for Mobile Ad Hoc Network", Swiss Federal Institute of Technology Lausanne(EPFL) Tech. Report, JUNE 2002.

[5] Panagiotis Papadimitratos and Zygmunt J. Hass, "Secure Routing Protocol for Ad hoc Networks", SCS Communication Networks and Distributed Systems Modeling and Simulation Conference(CNDS 2002), January 2002.

[6] Yih-Chun Hu, Adrian Perrig, and David B. Johnson. "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks", Technical Repor TR01-383, December 2001.

[7] J. Hubaux, L. Buttyan, and S. Capkun, "The Quest for Security in Mobile Ad Hoc Networks",ACM MobiHOC, pp.146-155, 2001.

[8] N.Asokan and Philp Ginzboorg. "Key Agreement in Ad-hoc Networks", Computer Communications, vol 23, pp.1627-1637, 2000.

[9] 황정현, 최규영, 이동훈, 백종명, "효율적인 패스워드 기반 그룹 키 교환 프로토콜" , 정보보호학회논문지, 제14권, 제1호, pp.59-69, 2004.2.