2001년 한국정보처리학회 추계 학술발표논문집 제8권 제2호

안전한 이동통신 환경을 위한 키 교환 프로토콜

홍주형* · 문준선* · 김종훈*
*동아대학교 컴퓨터공학과
e-mail : hongma@spring.donga.ac.kr

The Key Exchange Protocol of Secure Mobile Communication Environments

Joo-Hyung Hong* · Joon-Sun Moon* · Jong-Hoon Kim*
*Dept of Computer Engineering, Dong-A University

요약

안전한 이동통신 환경을 위해서는 이동통신 기기의 소형화로 인한 낮은 대역폭, 낮은 계산능력 등을 고려해야 하며 안전한 키 교환을 위해 기밀성, 무결성, 인증, 부인봉쇄와 같은 보안요건이 충족되어야 한다. 본 논문에서는 기존의 키 교환 프로토콜을 분석하여 이동통신의 특성을 만족하는 효율적인 연산의 End-to-End 키 교환 프로토콜을 설계하고, 이를 기존의 프로토콜과 비교·분석하였다.

1. 서론

이동통신의 가입자가 크게 늘면서 이동통신 기기의 사용의 폭이 많이 넓어지게 됐다. 이러한 이동통신이 무선 통신망을 사용함으로써 야기되는 도청, 추적, 다른 불법적인 사용 등의 범죄 행위가 전자 상거래와 같은 사용자에 더 밀접한 서비스를 제공하는데 큰 장애가 되고 있다.

이동통신의 채널 보안의 문제를 해결하기 위해 비밀키 알고리즘을 사용함으로써 계산량이 적다는 장점이 있으나, 인증과 키 교환에 있어서 TTP (Trusted Third Party)인 인증 센터를 필요로 하고 전자 서명을 하기 어렵다는 단점이 있다. 그러나 공개키 암호 알고리즘을 씀으로써, 인증센터를 가질 필요가 없으며, 전자 상거래와 같은 더 중요한 정보들을 교환하는 서비스제공에 편리하다. 암호 알고리즘의 이러한 장·단점들 때문에 키 교환 단계에서는 공개키 암호 방식, 메시지 교환 단계에서는 비밀키 암호 방식을 사용하는 하이브리드 방식을 많이 사용하고 있다.

본 논문에서 제안한 키 교환 프로토콜은 공개키 암호 알고리즘과 비밀키 암호 알고리즘의 혼합 방식인 하이브리드 방식을 이용하였으며, 이동국(Mobile Station)과 기지국(Base Station) 사이의 보안에 관련된 키 교환이 아니라 End-to-End, 즉 이동국 간의 암호/복호화 통신을 위한 키 교환을 위해 제안되었다. 제안하는 프로토콜은 이동통신 단말기가 가지는 특성을 고려하고, 기존의 키 교환 프로토콜을 분석한 뒤, 이러한 것들을 기반으로 차세대 무선인터넷에 적합한 키 교환 프로토콜을 제안 하고자 한다.

본 논문은 2절에서 이동통신 환경의 특성과 고려해야 할 보안 요소들에 대해 살펴보고, 3절에서는 기존의 키 교환 프로토콜의 특성을 분석하며, 4절에서는 효율적인 연산의 키 교환 프로토콜을 제안하여 기존의 키 교환 프로토콜과 비교 분석하고, 5절에서 결론을 내리도록 한다.

2. 이동통신 환경

2.1 특성

이동 통신기기의 소형화로 인한 낮은 대역폭, 낮은 계산능력과 사용자의 이동성을 큰 특성으로 들 수 있다. 이로 인하여 무선통신 프로토콜의 메시지 양과 통신 패스 수를 최소로 해야 하며, 기지국에서의 계산을 늘림으로써 이동통신 기기의 부하를 최소한으로 줄여야 한다. 그리고 한 도메인의 셀에서 다른

도메인의 셀로의 이동에 전혀 불편함 없이 정보들이 유지되어야 한다.

2.2 고려해야될 보안요소

이동통신 환경 이외에도 키 교환 프로토콜은 기밀성, 무결성, 인증, 부인봉쇄와 같은 보안 요건[6]을 만족해야 한다.

• 기밀성(Confidentiality)

무선 네트워크를 통해서 전송되는 데이터들은 공격자들에게 노출이 되기 쉬우며, 이러한 노출은 사용자의 신분과 위치 정보가 드러남으로써 악의의 공격이 가능하게 된다.

• 무결성(Integrity)

무선 통신상에서 교환되는 데이터가 중간에 에러나 악의의 공격에 의해서 변조되었는지 검증할 수 있는 정보가 있어야 한다.

• 인증(Certification)

이동통신 환경에서의 키 교환에 있어서 인증은 사용자 인증과 키 인증으로 나눌 수 있다. 사용자 인증은 키 교환에 있어서 관계하는 개체들의 신분을 확인하는 과정이며, 키 인증은 통신에 참여하지 않은 다른 개체가 교환된 세션키를 알 수 없도록 하기 위해 서로 확인하는 과정이다.

• 부인봉쇄(non-repudiation)

무선 네트워크를 통한 중요한 정보의 근원지를 확인하는 과정으로써, 자신이 보낸 정보를 부인할 수 없도록 하는 것이다.

3. 기존의 이동통신 키 교환 프로토콜

본 절에서는 공개키 암호 시스템에 기반 한 기존의 키 교환 프로토콜을 분석한다. 각각의 키 교환 프로토콜에 관한 기술은 <표 1>을 사용한다.

<표 1> 기호의 정의

기호	정의
ID_x	x의 식별자
N_x	x가 생성한 난수
K_x	x가 생성한 최종 세션키 정보
K_{xy}	x, y가 비밀 통신을 하는데 사용된 세션키
h(x)	x의 메시지 다이제스트
PK_x	x의 공개키
PK_x^{-1}	x의 개인키
Cert(x)	x의 인증서
$E_x\{M\}$	키 x를 이용하여 M을 암호화
$Sig_x\{M\}$	키 x를 이용하여 M을 전자서명

3.1 MSR+DH 키 교환 프로토콜

MSR(Modular Square Root)+DH(Diffie-Hellman)는 Carlsen에 의해 제안된 키 교환 프로토콜[9]로 BCY 키 교환 프로토콜[10]을 개선한 것이다.

(1) B → M : B, N_B, PK_B, Cert(B)
(2) M → B : $E_{PK_B}\{x\}$, $E_x\{N_B, M, PK_M, Cert(M)\}$

이 키 교환프로토콜은 사용자 인증 및 기밀성 만을 만족시키며, 기지국와 이동국 사이의 Link Security [4] 범위에서의 보안을 지원한다.

3.2 BY(Beller and Yacobi) 키 교환 프로토콜

Beller와 Yacobi에 의해 제안된 Link Security 범위의 키 교환 프로토콜이며, 이후 Boyd와 Mathuria에 의해 취약점이 발견되면서 아래와 같은 개선된 BY 키 교환 프로토콜[3]이 나오게 되었다.

(1) B→M : B, N_B, PK_B, Cert(B)
(2) M→B : $E_{PK_B}\{x\}$, $E_x\{M, PK_M, Cert(M)\}$, $Sig_{PK_M^{-1}}\{h(B, M, N_B, x)\}$
(3) B→M : $E_x\{N_B\}$

(2)과정에서 이동국이 전송하는 데이터의 전자서명 값을 포함시키고, (3)과정에서 기지국이 검증함으로써 취약점을 해결 할 수 있다. 이 프로토콜은 MSR+DH 프로토콜에 비해 전자 서명이 추가됨으로써 부인봉쇄 및 무결성을 만족시키나, 키 인증을 만족시킬 수 없다.

3.3 AZ(Aziz-Diffie) 키 교환 프로토콜

Aziz와 Diffie에 의해 제안된 Link Security 범위의 키 교환 프로토콜[4]으로써 이동국과 기지국에서 각각 세션키 정보를 생성한 뒤, 최종 세션키를 교환된 정보로써 생성해 낸다. Boyd와 Mathuria에 의해 취약점이 발견되면서 아래와 같은 개선된 AD 키 교환 프로토콜[3]이 나오게 되었다.

(1) M→B : Cert(M), N_M, alg_list
(2) B→M : Cert(B), N_B, $E_{PK_M}\{x_B\}$, sel_alg, $Sig_{PK_B^{-1}}\{h(x_B, M, N_M, sel\_alg)\}$
(3) M→B : $E_{PK_B}\{x_M\}$, $Sig_{PK_M^{-1}}\{h(x_M, B, N_B)\}$

*alg_list : 세션키 사용을 위한 비밀키 알고리즘 리스트
*sel_alg : alg_list에서 선택된 알고리즘

이 프로토콜은 앞의 프로토콜과 비교해서 사용자 인증 및 키 인증을 수행하지만, 이동국에서의 많은 공개키 암호알고리즘의 수행에 의해 큰 부하가 걸리게 된다.

3.4 VM(Varadharajan-Mu) 키 교환 프로토콜

Varadharajan과 Mu에 의해 제안된 End-to-End Security 범위의 키 교환 프로토콜[7][8]이다

· 단계 1 : M1 ↔ B

(1) M1 → B : ID_{M1}, B, Cert(M1), N_{M1}, K_{M1}, $E_{KM1}\{(h(ID_{M1}, B, N_{M1})\}$

(2) B → M1 : B, ID_{M1}, Cert(B), K_B, T_B, N_B, $E_{K_B}\{h(B, ID_{M1}, N_{M1}, N_B)\}$

(3) M1 → B : ID_{M1}, B, $E_{K_{MB}}\{h(ID_{M1}, M2, B, N_B)\}$, $E_{K_{MB}}\{M2\}$

· 단계 2 : B ↔ M2

(1) B → M2 : B, ID_{M2}, Cert(B), K_B, T_B, Cert(M1), K_{M1}, T_{M1}, N_B', N_{M1}, $E_{K_B}\{h(B, ID_B, N_B', N_{M1})\}$

(2) M2 → B : ID_{M2}, B, N_{M1}, N_B, $E_{K_{MB}}\{h(ID_{M2}, B, N_{M1}, N_{M2}, N_B')\}$, $E_{K_{MB}}\{h(M1, M2, N_{M1}, N_{M2})\}$

· 단계 3 : M1 ↔ M2

(1) B → M1 : B, ID_{M1}, Cert(M2), K_{M2}, T_{M2}, N_{M1}, N_{M2}, N_B'', $E_{K_{MB}}\{ID_{M1}'\}$, $E_{K_{M1B}}\{h(B, ID_{M1}, ID_{M1}', N_{M1}, N_{M2}, N_B'')\}$, $E_{K_{MB}}\{h(M1, M2, N_{M1}, N_{M2})\}$

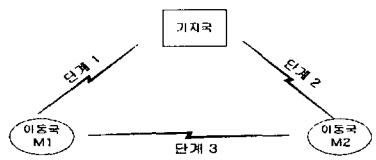
(2) M1 → M2 : N_B, $E_{K_{MM2}}\{M1, M2, N_B+1\}$

*T_x : x의 인증서 유효기간

이 프로토콜은 앞의 세가지 프로토콜과는 달리 이동통신 사용자간의 키 교환을 위해 설계된 프로토콜이다. 결점은 없지만 각각의 단계에 있어서의 보조 세션키 생성에 많은 연산을 하므로 실제 적용되기에는 불가능하다[3].

4. 제안한 키 교환 프로토콜

이번 절에서는 제시된 특성 및 요구사항을 고려하여, 이동통신 환경에 적합한 End-to-End 보안조건을 만족하는 효율적인 연산의 키 교환 프로토콜을 제안하고 분석한다. 제안하는 키 교환 프로토콜은 (그림 1)처럼 진행되며,



(그림 1) 키 교환을 위한 구성

아래와 같은 가정 하에 기술된다.

- 기지국의 인증정보(Cert(B))는 항상 Broadcast Channel을 통하여 전송되며, 통신을 원하는 이동국측에서는 기지국과 통신 가능한 곳에 속해 있을 때, 기지국의 인증서를 받고 이를 검증한다[5].
- 기지국은 M1, M2등 여러 이동국의 실제 이름과 ID를 매칭 시킬 수 있다.
- 이동국에서 생성하는 난수는 Off-Line 상태에서 생성이 되며, 직접적인 키 교환과정의 계산효율에는 영향을 주지 않는다.

4.1 제안된 키 교환 프로토콜

본 논문에서 제안하는 프로토콜은 다음과 같이 3단계로 이루어진다.

· 단계 1 : M1 ↔ B

(1) M1 → B : $E_{PK_B}\{ID_{M1}, N_{M1}\}$

초기 요청으로 M1이 생성한 난수와 자신의 ID를 B에게 보내며, 전송되어지는 정보는 가정에 의해서 Off-Line에서 계산되어진다.

(2) B → M1 : $E_{N_{M1}}\{N_B, h(K_{M1B})\}$

B는 받은 데이터를 자신의 개인키로 복호화한 뒤 자신이 생성한 난수와 보내온 N_{M1}을 결합하여 단계 1의 부분 세션키를 만들어 M1에게 그것의 해쉬 값을 전송한다.

(3) M1 → B : $E_{K_{MB}}\{Cert(M1), ID_{M2}, K_{M1}, Sig_{PK_{M1}^{-1}}\{h(ID_{M1}, ID_{M2}, ID_B, N_{M1}, N_B, K_{M1})\}$

M1은 생성된 부분 세션키를 확인하고 자신이 통신하고자 하는 대상의 ID와 키정보를 포함시킨 데이터와 전자서명 값을 B에게 보내준다.

· 단계 2 : B ↔ M2

(1) B → M2 : $E_{PK_{M2}}\{N_B'\}$, $E_{N_B'}\{Cert(B), Cert(M1), N_B, N_{M1}, K_{M1}, h(N_B', K_{M1})\}$

M1에게 받은 데이터를 검증한 후 M1이 통신하고자 하는 사용자를 찾아서 각각의 인증서 및 키정보를 전송해 준다. 단계 2의 부분 세션키를 생성하기 위한 정보로서 N_B'을 포함 시킨다.

(2) M2 → B : $E_{PK_B}\{ID_B, N_{M2}\}$, $E_{K_{BM2}}\{N_B', Cert(M2), Sig_{PK_{M2}^{-1}}\{K_{M2}, E_{K_{M1M2}}\{h(K_{M1}, K_{M2})\}\}\}$

B에게서 받은 정보를 확인 후 M2는 자신의 키정보와 난수, 그리고 최종 세션키의 해쉬 값을 생성해서 자신의 개인키로 서명한 뒤 B로 보낸다.

· 단계 3 : M1 ↔ M2

(1) B → M1 : $E_{K_{MB}}\{K_{M2}\}$, $E_{K_{MBM}}\{h(K_{M1}, K_{M2})\}$

단계 1의 세션키(K_{BM1})을 이용해서 최종 세션키 정보와 무결성 검증을 위해 각각의 세션키 정보의 해쉬값을 최종 세션키로 암호화해서 M1에게 보낸다.

(2) M1 → M2 : SessionKey Validation (Succ/Fail)

M1은 마지막으로 최종세션키의 보내온 해쉬값과 생성한 해쉬값을 비교한 뒤 세션키 확인 메시지를

M2에게 보낸다.

4.2 제안된 키 교환 프로토콜의 분석

제안된 키 교환 프로토콜의 각 단계를 분석하면 각 보안요소에 대해 다음과 같은 결과를 얻을 수 있다.

• 기밀성

단계 1, 단계 2에서 각 과정에 대한 부분 세션키 K_{M1B}, K_{M2B}를 생성함으로써 전송되어지는 정보를 보호 할 수 있다.

• 무결성

단계 1, 단계 2, 단계 3에서 키 교환을 위해 전송된 데이터에는 그 데이터의 무결성을 검증할 수 있는 해쉬 값이 포함되어 있다.

• 인증

사용자 인증은 기 교환에 사용되는 인증서 및 개인키를 이용한 전자 서명으로 가능하며, K_A 및 K_B와 같은 키 정보를 서로 교환, 확인, 생성(단계 2, 단계 3) 과정에 의해서 키 인증을 할 수 있다.

• 부인봉쇄

공개키 암호 알고리즘에 사용되는 키 쌍의 인증서를 발급 받고 그 인증서에 포함된 개인키를 사용하여 전자 서명(단계 1, 단계 2)을 함으로써 전송된 데이터의 부인 봉쇄를 가능하게 한다.

4.3 기존의 프로토콜과 비교 분석

제안된 프로토콜 전체의 이동국에서 공개키 암호 알고리즘의 연산은 단계 1에서 1회, 단계 2에서 2회가 수행된다. <표 2>에서 보듯이, 이것은 기존에 제안된 Link Security 범위를 가지는 키 교환 프로토콜과 비슷하거나 조금 더 많은 연산량을 보인다. 제안된 프로토콜은 End-to-End Security 범위의 키 교환 프로토콜이며 VM 프로토콜보다는 더 효율적인 연산을 가능하게 한다.

<표 2> 키 교환 프로토콜의 비교

키 교환 프로토콜	보안 범위	기밀성	무결성	인증	부인 봉쇄	공개키 연산량
MSR+DH	Link	△	×	△	×	암:1
BY	Link	△	○	△	△	암:1, 서:1
AD	Link	○	○	△	○	암:1, 복:1 서:1, 검:1
VM	EtoE	○	○	○	○	지:4, 서:1 검:2
제안된 프로토콜	EtoE	○	○	△	○	서:2, 암:1

*암→암호화, 복→복호화, 서→서명, 검→검증, 지→큰수의 지수승
*○→둘다 만족, △→부분 만족, ×→불만족

5 결론 및 향후 연구방향

본 논문에서는 이동 통신의 특성, 보안 요구사항을 고려하고 기존에 제안된 프로토콜을 분석한 뒤, 이동통신 사용자간의 End-to-End 통신을 위한 효율적인 연산의 키 교환 프로토콜을 제안하였다. 앞으로의 이동통신 환경에서의 사용자간의 중요한 정보를 기지국에 정보의 위탁 없이 바로 교환 할 수 있으며, 이동통신을 위한 개인 전자 상거래에 적용이 가능할 것이라고 본다.

향후 연구 과제로 본 논문의 Hybrid 방식이 아닌 ECC를 적용하여 더 효율적인 키 교환 프로토콜이 연구되어야 하겠다.

참고문헌

[1] D.G.Park, C. Boyd, S.J. Moon, "Forward Secrecy and Its Application to Future Mobile Communications Security", Public Key Cryptography 2000, pp.433-445, 2000

[2] Colin Boyd and Dong-Gook Park, "Public Key Protocols for Wireless Communications", Proceedings of ICISC '98, pp. 47-57, 1998

[3] C. Boyd and A. Mathuria, "Key Establishment Protocols for Secure Mobile Communications: A Selective Survey", Information Security and Privacy, LNCS 1438, Springer-Verlag,1998, pp.344-355.

[4] A. Aziz and W. Diffie. "Privacy and Authentication in Wireless Local Area Networks", IEEE Personal Communications, First Quarter, 1994.

[5] Y. Zheng, "An Authentication and Security Protocol for Mobile Computing", In Proc. of the IFIP World Conference on Mobile Communications , Canberra, 1996.

[6] N. Asokan, "Security Issues in Mobile Computing", CS 690B-Research Proposal, 1995.

[7] V. Varadharajan, Y. Mu, "Design of Secure End-to-End Protocols for Mobile Systems", In Proc. of the IFIP World Conference on Mobile Communications, Canberra, 1996.

[8] V. Varadharajan and Y. Mu, "On the Design of Security Protocols for Mobile Communications", ACISP'96 Conference, Springer-Verlag, pp. 134-145. 1996,

[9] U. Carlsen,"Optimal Privacy and Authentication on a Portable Communication System", ACM Operation System Review, 28(3), pp.16-23, 1994.

[10] M. Beller, L. Chang, and Y. Yacobi. "Privacy and authentication on a portable communications system", IEEE J. Selected Areas in Communications, 11(6), pp.821-829, 1993.