이동 사용자의 익명성을 보장하는 안전한 종단간 프로토콜

김선형*, 이병래*, 강상승**, 김태윤*
*고려대학교 컴퓨터학과
**한국전자통신연구원
e-mail : shaklim@netlab.korea.ac.kr

A Secure End-to-End Protocol assuring Anonymity for Mobile Users

Sun-Hyoung Kim*, Byung-Rae Lee*, Sang-Seung Kang**,
Tai-Yun Kim*
*Dept of Computer Science and Engineering, Korea University
**Electronics and Telecommunications Research Institute

요약

무선 통신 시스템에서 이동 사용자들의 안전성 문제에 대한 논쟁은 끊임없이 이루어지고 있으며 무선 네트워크 환경에서 더 안전한 통신을 위한 연구들이 계속 진행되고 있다. 무선 네트워크 환경에서는 전달하고자 하는 메시지들이 공중파를 매체로 하여 전송되기 때문에 유선 네트워크 시스템에서보다 안전성의 문제가 더욱 철저히 고려되어야 한다. 본 논문에서는 무선 이동 네트워크 환경에서 인증서를 기반으로 한 안전한 통신 프로토콜을 제안하고자 한다. 특히 이동 사용자들이 각기 다른 도메인으로부터 서비스를 받고 있는 환경에서 종단간에 위치한 이동 사용자들이 다른 사용자와 외부 도메인으로부터 익명성을 보장받으며 서로를 인증하고 안전하게 통신을 위한 비밀키를 공유할 수 있는 프로토콜을 제안한다.

1. 서론

기존의 유선 네트워크에 무선 이동 네트워크를 접목시키는 작업은 단순히 유선 상에서의 기술들을 옮겨놓는 것만으로 끝나지 않는다. 무선 네트워크 기술은 새로운 기술력을 필요로 하는 독립적인 네트워크 시스템이라 할 수 있다. 대부분의 이동 사용자는 이동 단말기를 통해 자신이 원하는 서비스를 받기를 원하며 앞으로도 사용자들의 요구는 끊임없이 늘어날 것이다. 그러나 이러한 이동 사용자에 대한 서비스의 질과 양적인 측면을 논하기 이전에 이동 사용자들로 하여금 안전하고 신뢰성 있는 통신의 보장이 필수적으로 이루어져야 할 것이다.

오늘날의 노트북 컴퓨터와 개인용 보조 단말기(PDA)가 모든 기능을 스스로 해결하는 반면에 네트워크와 연동된 이동 컴퓨터들은 더 큰 컴퓨팅 기반구조의 한 부분이 된다. 이것은 정보 보호와 개인의 사생활 보장, 그리고 시스템 의존력과 가용성과 유효성에 대한 쟁점이 되고 있다.

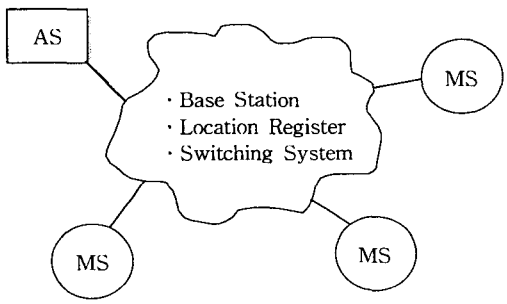
본 논문에서는 무선 이동 네트워크 환경에서 인증서를 기반으로 한 안전한 프로토콜을 제안하고자 한다. 특히 이동 사용자들이 각기 다른 도메인으로부터 서비스를 받고 있는 환경에서 종단간에 위치한 이동 사용자들이 다른 사용자와 외부 도메인으로부터 익명성을 보장받으며 서로를 인증하고 안전하게 통신을 위한 비밀키를 공유할 수 있는 프로토콜을 제안한다.

본 논문은 다음과 같이 구성되어 있다. 2절에서는 이동 네트워크 시스템의 환경에 대해 설명한다. 3절에서는 무선 네트워크 환경에서의 보안 요구사항을 알아본다. 4절에서는 종단간 이동 사용자 사이의 프로토콜에 대해 살펴보고 이 프로토콜의 취약점을 고찰한다. 5절에서는 두 사용자가 서로를 인증하고 공통의 비밀키를 확립할 수 있는 안전한 종단간 프로토콜을 제시하고 6절에서 이에 대한 성능 평가를 한다. 마지막으로 7절에서 본 논문의 결론을 맺는다.

2. 이동 네트워크 환경

무선 이동 통신 시스템은 단말기를 소유한 이동 스테이션(MS)과 이동 네트워크 시스템(MNS)의 두 가지로 분류할 수 있다. 이동 네트워크 시스템은 이러한 이동 스테이션의 제반 사항에 대한 기록을 관리하고 있으며 <그림 1>과 같이 기지국(BS), 위치 레지스터, 스위칭 시스템의 세 가지로

구분할 수 있다. 이동 스테이션은 기지국을 통하여 네트워크 시스템에 접속할 수 있고 하나의 기지국은 해당 네트워크의 위치 레지스터에 의해서 제어된다. 스위칭 시스템은 다른 모든 이동 네트워크 혹은 유선 네트워크와 연결되는 접속점의 역할을 하며 이동 스테이션의 이동 정보에 대한 데이터베이스를 수반하고 있다. 또한 각각의 네트워크에는 인증 서버(AS)가 존재하며 이는 위치 레지스터와 같은 도메인 상에 위치하고 있다. 인증 서버는 이동 사용자의 비밀키와 같은 보안 관련 정보를 저장하고 있으며 위치 레지스터는 자신의 네트워크에 등록된 이동 사용자의 현재 위치와 가입 정보를 저장하고 있다. 각각의 이동 사용자는 이동 네트워크에 가입할 때 자신의 홈 네트워크(HN)를 가지게 된다. 이동 사용자는 언제든지 다른 네트워크로 이동할 수 있으며 이를 방문 네트워크(VN)라 부른다. 이동 사용자가 다른 네트워크로 이동하기 위해서는 홈 네트워크와 방문 네트워크 사이에 일련의 합의가 있어야 하며 이들 네트워크간의 통신 합의가 수행된 후에야 다른 네트워크로부터 서비스를 받을 수 있게 된다[1].



<그림 1> 이동 네트워크 환경

3. 보안 요구사항

- 인증 : 인증 서비스는 통신에 참여하고 있는 사람에게 신뢰성을 제공해야 한다. 즉 종단 참여자 A와 B는 서로 안전한 통신을 하고 있다는 사실을 확신해야 한다. 이는 각각의 도메인에 속해 있는 인증 서버에 의해 달성될 수 있다. 사용자들은 자신의 도메인에 속한 인증 서버를 전적으로 신뢰하고 있으며 인증 서버는 통신 참여자에게 그들의 신원을 신뢰성 있게 인증할 수 있어야 한다. 도메인 서버들간의 인증은 공개키 암호 시스템을 사용하여 달성된다.
- 안전한 통신 : 통신이 안전하기 위해서는 다른 사용자나 도청자로부터의 공격을 받아서는 안 된다. 이는 통신을 위한 세션키를 확립함으로써 달성될 수 있으며, 이 세션키로 인해 종단간의 참여자들 사이에서의 통신이 안전해질 수 있다.
- 사용자 신원의 기밀성 : 실제로 사용자들은 다른 사용자들로부터 자신의 신원을 알리지 않길 원한다[6]. 예를 들면 이동 사용자는 다른 네트워크 사용자들에게는 익명성을 유지하면서 오직 인증 서버와 통신 상대에게만 알려지길 원할 수 있다. 또한 사용자는 방문 도메인의 인증 서버에 대해서도 익명성을 유지하길 바랄 수 있다. 원칙적으로는 방문 도메인의 인증 서버가 다른 도메인의 사용자의 실제 신원을 알 필요가 없으며 다만 사용자의 지불 능력과 홈 도메인에게 계산서를 올바르게 청구할 수 있는지에 대한 정보만이 요구된다.
- 서비스의 부인 방지 : 서비스 제공 업체는 이동 사용자로 하여금 서비스에 대한 계산 청구에 대해 부인할 수 없도록 해야 한다. 마찬가지로 이동 가입자는 네트워크 상에서 어떠한 청구 에러나 보안 결점으로 인해 잘못된 요금이 부과되어서는 안 된다. 이는 모두 전자 서명의 사용을 통해 달성될 수 있다. 이동 사용자가 실질적으로 복잡한 공개키 함수의 계산에 제약이 있다면 오직 제한된 서비스의 부인 방지만이 달성될 수 있다.
- 프로토콜 설계 원리 : 사용자의 장기적 비밀키와 같은 도메인의 비밀 정보는 홈 도메인으로부터 외부 도메인으로 전파되어서는 안 된다. 더욱이 도메인 사이의 거리가 멀 경우에 메시지 교환의 횟수가 최소화되도록 프로토콜을 설계하는 것이 중요하다[7].

4. 관련 연구

여기서는 Yacobi-Shmuely[2]가 제시했던 인증 프로토콜을 수정한 Park의 프로토콜[3]을 이용한 종단간의 프로토콜을 살펴본다. 아울러 제시된 프로토콜에 대한 공격 가능성의 여부를 고찰해 봄으로써 안전성이 보장되는 새로운 종단간의 프로토콜의 필요성을 논한다.

4.1. 이동 사용자간의 통신 프로토콜

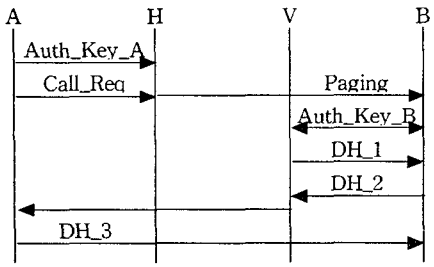
다음의 <그림 2>에서 두 이동 사용자 A와 B는 서로 구분된 두 개의 네트워크에 존재하고 있다. 즉 A의 홈 네트워크 서버는 H이고 B의 홈 네트워크 서버는 V이며 각각 이동 사용자는 자신의 도메인에 속한 서버로부터 서비스를 받고 있다. 이제 두 이동 사용자 A와 B는 서로를 인증하고 공통의 세션키를 공유하기를 원한다. 프로토콜에서 사용되는 기호는 다음과 같은 의미를 지닌다.

$$cert_A = \{ID_A, y_A, date_A, [h(ID_A, y_A, date_A)]_{s_{CA}}\}$$

$$DH(A) = g^{r_A + x_A} \bmod N, \quad DH(B) = g^{r_B + x_B} \bmod N$$

$$Res(A) = [ID_A, ID_B]_{k_s}, \quad Res(B) = [ID_B, ID_A]_{k_s}$$

$$k_s = \left(y_B \cdot g^{r_B + x_B}\right)^{r_A} \bmod N$$
$$= \left(y_A \cdot g^{r_A + x_A}\right)^{r_B} \bmod N = g^{r_A r_B} \bmod N$$



<그림 2> 이동 사용자간의 통신 프로토콜

[프로토콜 I]

1. Auth_Key_A : 위의 프로토콜을 이용하여 이동 사용자 A와 홈 네트워크 H 사이의 상호 인증을 수행한다. H는 A로부터 수신한 r_A+x_A을 이용하여 $DH(A)$을 계산한다.
2. Call_Req : 이동 사용자 A는 다른 네트워크에 속해 있는 이동 사용자 B를 호출하고 B의 네트워크 서버인 V에게 $cert_A$와 $DH(A)$를 전송한다.
3. Paging and Auth_Key_B : B를 페이징 한 후 V와 B 사이에 프로토콜이 수행된다. V는 $DH(B)$을 계산한다.
4. DH_1 : V는 B에게 A의 인증서 $cert_A$과 $DH(A)$를 전송한다. B는 k_s과 $Res(B)$를 계산한다.
5. DH_2 : B는 V에게 $Res(B)$를 전송하고 V는 $Res(B)$를 $DH(B)$, $cert_B$와 함께 A에게 전달한다.
6. DH_3 : B와의 세션키 k_s를 계산한 후 $Res(B)$를 이용하여 B를 인증한다. 그리고 $Res(A)$를 계산하여 B에게 전송하면 B는 이를 통해 A를 인증하게 된다.

4.2. 프로토콜 분석

Yacobi-Shmuely에 의해 제안된 키 교환 프로토콜에서는 x_B+r_B가 B에 의해 전송되고 누구든지 g^{r_B}를 알아낼 수 있다 하더라도 x_B는 오직 B만이 알고 있기 때문에 x_B+r_B를 만들어낼 수 없다. 그렇지만 위의 프로토콜에서 $g^{x_B+r_B}$은 공격자 스스로가 r_B를 임의로 선택함으로써 $y_B^{-1}g^{r_B}=g^{x_B+r_B}$를 만들어낼 수 있다. 즉 B의 개인키 값 x_B를 알지 못하더라도 누구든지 A와 B의 세션키인 $K_{AB}=\left(y_A g^{x_A+r_A}\right)^{r_B}=g^{r_A r_B}$를 계산할 수 있으므로 A와의 통신이 가능하게 된다[4].

5. 제안한 종단간의 안전한 통신 프로토콜

두 이동 사용자 사이에서의 통신은 네트워크의 외부 공격자뿐만 아니라 내부의 공격자에 대해서도 보호될 수 있어야 한다. 즉 두 이동 사용자 사이에 교환된 세션키에 대한 정보는 자신의 홈 네트워크에게조차 노출되어서는 안 된다. 따라서 종단간에 상호 인증과 세션키를 확립하기 위해서는 두 이동 사용자 사이에서의 보안뿐만 아니라 이동 사용자와 네트워크 사이에서의 보안 또한 철저히 이루어져야 한다. 즉 사용자의 신원은 자신이 속한 도메인의 인증 서버와 통신 상대방에게만 알려져야 하고 외부 네트워크와 네트워크 상의 다른 사용자들로부터는 익명성을 보장받을 필요가 있다. 본 절에서는 여러 개로 분리된 서로 다른 네트워크 상에서 사용자의 익명성을 보장하면서 종단간의 인증된 세션키를 확립하는 안전한 통신 프로토콜을 제안한다.

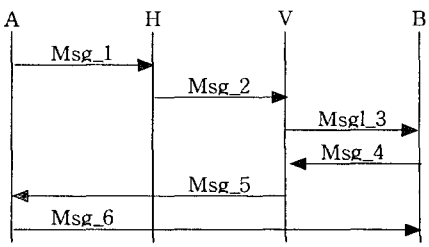
5.1. 가정 및 기호

- 이동 사용자 A, B
  - 각각의 사용자는 CA로부터 서명된 공개키 인증서를 가지고 있다.
  - 각 사용자는 자신이 속한 네트워크와 공통의 비밀키를 공유하고 있다.
  - 각 사용자는 자신이 속한 도메인의 인증 서버로부터 발급 받은 임시 신원을 가지고 있다.
- 이동 네트워크 H, V
  - 각각의 네트워크는 CA로부터 서명된 공개키 인증서를 가지고 있다.
  - 각 네트워크는 자신의 도메인에 속한 사용자에게 임시 신원을 발급하며 이를 실제 신원과 매핑할 수 있다.
  - 각 네트워크는 다른 네트워크와 공통의 비밀키를 공유하고 있다.

다음은 프로토콜에 사용되는 기호들이다.

h_1, h_2, h_3 : 일방향 해쉬 함수([5] 참조)
$Sig_A\{X\}$: 메시지 X에 대한 A의 서명
$cert_A$: 이동 사용자 A의 인증된 공개 서명키
$cert_B$: 이동 사용자 B의 인증된 공개키 (g^{x_B})
K_{AB} : A와 B 사이의 공통의 비밀 세션키
TID_X : 이동 사용자 X의 임시 신원

5.2. 제안한 새로운 종단간 인증 프로토콜



<그림 3> 새로운 종단간 인증 프로토콜

[프로토콜 II]

Msg_1 : $\left[TID_A, ID_B, g^{r_A}, ID_{CA}\right]_{K_{AH}}$

Msg_2 : $\left[g^{r_A}, ID_H, ID_{CA}\right]_{K_{HV}}$

Msg_3 : $\left[g^{r_A}, ID_V, ID_{CA}, TID_B\right]_{K_{HV}}$

Msg_4 : $\left[r_B, h_2(K_{AB}, r_B, ID_B), TID_B, T_B, cert_B\right]_{K_{HV}}$

Msg_5 : $r_B, h_2(K_{AB}, r_B, ID_B), TID_B, T_B, cert_B$

Msg_6 : $\left[Sig_A\left(h_3\left(g^{r_A}, g^{x_B}, r_B, ID_B, T_A\right), cert_A\right]_{K_{AH}}\right.$

1. Msg_1 : A는 B를 호출하기 위해 H로부터 이미 발급받은 임시 신원과 B의 신원을 포함시킨 메시지를 H에게 전송한다.
2. Msg_2 : H는 V에게 B가 A와의 세션키를 만들 수 있는 정보를 포함한 메시지를 전송한다. 또한 A의 인증서를 인증할 수 있는 CA의 식별자를 같이 보낸다.
3. Msg_3 : H와 V는 B에게 A의 정보를 전달하고, B는 자신의 비밀키 x_B와 A의 임시 비밀키 r_A를 기반으로 공통의 비밀키 $K_{AB}=h_1\left(r_B, g^{x_B r_A}\right)$를 확립한다.
4. Msg_4 : V는 받은 메시지를 복호화하여 B를 인증한다. 그리고 A에게 B와 세션키를 확립할 수 있는 정보를 포함한 메시지를 전송한다.
5. Msg_5 : A는 V로부터 받은 정보들을 이용하여 세션키를 확립할 수 있으며 이로써 B를 인증할 수 있다.
6. Msg_6 : B는 A로부터 비밀 세션키 K_{AB}로 암호화한 메시지를 해독함으로써 A를 인증할 수 있다.

6. 성능 평가

본 논문에서 제시한 프로토콜은 종단간의 사용자의 익명성을 보장하면서 이들 사이에서 인증과 공통의 세션키의 확립을 주요 목표로 하고 있다. 여기서는 앞서 제시한 두 개의 프로토콜을 비교한다.

<표 1> 프로토콜의 안전성 비교

	프로토콜 I	프로토콜 II
상호 실체 인증	×	○
상호 키 합의	○	○
상호 함축적 키 인증	×	○
상호 키 확증	×	○
사용자 신원의 기밀성	○	○
익명성 제공	×	○

[○ : 만족, × : 불만족]

프로토콜 I 은 이동 사용자와 네트워크 사이에서 서로에 대한 인증을 못하기 때문에 공격자는 자신의 실체를 드러내지 않고서도 다른 실체의 역할을 할 수 있다.

제안한 프로토콜 II는 서명의 암호화를 통해 서명자 인증 공격과 컨텐트 인증 공격을 방지하고 있으며 메시지의 해쉬 함수에 네트워크 식별자와 난수를 포함함으로써 근원지 대체 공격과 타임-메모리 교환 공격을 방지할 수 있다. 또한 두 개의 서로 다른 프로토콜의 세션키 K값이 같을 때, 이를 찾기 위한 코드북 공격을 방지할 수 있다[5].

도메인에 속한 네트워크 서버는 사용자에 대한 임시 신원을 발급하여 외부 도청자 혹은 공격자로부터 익명성을 제공받는다.

7. 결론

본 논문에 제시된 종단간의 인증 프로토콜에서는 이동 사용자의 어떠한 비밀 정보도 다른 네트워크 상으로 전송되지 않으며, 이는 어느 누구도 이동 사용자로 위장할 수 없음을 의미한다. 따라서 두 이동 사용자의 비밀 통신이 보장될 수 있다. 또한 안전한 통신 채널이 사용자와 네트워크 사이에 설정되면 어떠한 암호학적 동작도 수행되지 않기 때문에 네트워크에서의 작업량이 경감될 수 있다. 본 논문에서는 사용자의 임시 신원을 사용함으로써 네트워크 상의 다른 사용자 혹은 다른 네트워크로부터 익명성을 보장받을 수 있다.

참고 문헌

[1] R. Molva, D. Samfat, G. Tsudik, "Authentication of Mobile Users," IEEE Network, pp. 26-34, 1994.

[2] Y. Yacobi, Z. Shmuley, "On Key Distribution Systems," in Advances in Cryptology - Crypto'89, LNCS 435, pp. 344-355, Springer Verlag, 1989.

[3] C. Park, "On Certificate-Based Security Protocols for Wireless Mobile Communication Systems," IEEE Network, pp. 50-55, September/October 1997.

[4] C. Boyd, D.-G. Park, "Public Key Protocols for Wireless Communications," in The 1st International Conference on Information Security and Cryptology(ICISC'98), pp. 47-57, 1998.

[5] G. Horn, B. Preneel, "Authentication and Payment in Future Mobile Systems," In Computer Security - ESORICS '98 Proceedings, pp. 277-293, Lecture Notes in Computer Science Vol. 1485, Springer Verlag, Berlin, 1998.

[6] N. Asokan, "Anonymity in a Mobile Computing Environment," in Proceedings of 1994 IEEE Workshop on Mobile Computing Systems and Applications, 1994.

[7] V. Varadharajan, Yi Mu, "Preserving Privacy in Mobile communications: A Hybrid Method" Persona Wireless Communications, 1997 IEEE International Conference on, pp. 532-536 1997.