2001년 한국정보처리학회 추계 학술발표논문집 제8권 제2호

WAP 환경에서의 안전한 키 분배 프로토콜 설계

서병기*, 김태연*
*서남대학교 컴퓨터영상정보통신학부
e-mail:tykim@tiger.seonam.ac.kr

Design of Secure Key Distribution Protocol in WAP Environment

Byung-Gi Seo*, Tae-Yeon Kim*
*Dept of Computer Image and Information Communication,
Seonam University

요약

사용자 망이 전 세계적으로 연결되고 이동 통신 서비스가 급속하게 확대되어 감에 따라 신뢰성과 보안 문제가 크게 대두되고 있다. 본 논문에서는 인터넷 환경에서 무선 이동호스트(단말)의 특성을 감안한 호스트의 인증과 안전한 키 분배 프로토콜을 제안한다. 또한 제안된 프로토콜은 중간 에이전트나 다른 이동 호스트로부터 자신의 ID와 위치를 감출 수 있는 프라이버시를 보장한다.

1. 서론

현재의 디지털 이동통신기술에 기존의 고속 인터넷 서비스 및 화상 통신과 같은 IP 기반 멀티미디어 통신 서비스를 실현하려는 연구에 많은 관심을 갖고 있다. 이러한 무선 이동시스템은 언제 어디서나 이동 호스트가 고정된 유선 망뿐만 아니라 무선 망 자원과 서비스를 사용할 수 있도록 하기 위함이다. 따라서 인터넷과 무선 이동호스트 간에 안전한 데이터 전송이 보장되는 연동 방법으로는 크게 두 가지가 있다.

첫째, 송신자가 전송한 데이터를 중간 노드에서 어떠한 변환 과정을 거치지 않고 그대로 수신자만이 받아볼 수 있도록 하는 구조이다. 이러한 구조를 위해서는 이동 단말과 무선망의 성능을 향상시켜 기존의 인터넷 서비스를 그대로 이동 단말까지 수용할 수 있도록 하는 방법과 이동 단말과 무선망의 성능을 고려하여 송신 측에서 기존의 유선 망에 연결된 단말과 무선망에 연결된 단말을 구분하여 서로 다른 방법으로 데이터를 처리할 수 있는 장치를 송신 측에 설치하는 방법을 고려해 볼 수 있다. 그렇지만 현재의 이동단말의 특성과 무선통신 환경에 발생할 수 있는 문제점을 완화하는 일이 쉽지 않다[9]. 무선망의 성능을 높일 수 있다고 하더라도 단말의 크기와 무게, 구입비가 기대이상으로 커질 수밖에 없다. 그리고 현재의 단말을 그대로 사용할 수 있는 방안으로는 유선 망 단말에 무선 인터넷 서비스와 이동전화 서비스를 지원할 수 있는 개발환경을 추가하는 문제도 쉽지 않다.

둘째, 송신자가 전송한 데이터를 에이전트로 하여금 중간에서 데이터를 유·무선망에 적합하도록 변경하여 수신자에게 전달하는 연결분리(split connection) 구조이다. 다시 말해서 WAP(Wireless Application Protocol)은 무선 인터넷 서비스를 지원하기 위한 개방 통신 규약으로 인터넷망과 이동통신망의 접속 점에 게이트웨이를 두어 원활한 상호연동이 가능하도록 하는 기능을 담당하게 한다. 즉, 무선 도메인과 웹 사이를 연결하기 위해 대리인(proxy) 기술을 이용한다[7,8]. 이 구조는 게이트웨이에서 유선 인터넷 서비스를 다양한 접속 방법, 다양한 단말 형태, 다양한 프로토콜 등을 수용하여 매우 유연한 형태로 사용자의 다양한 요구를 만족시킬 있도록 하는 것이다. 단말의 특성에서 오는 문제점을 완화하면서 인터넷 서비스

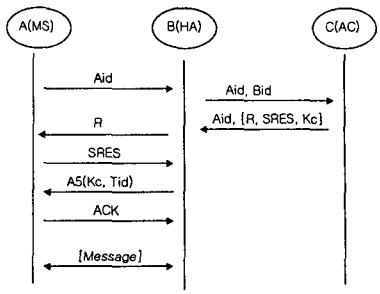
를 지원할 수 있도록 한다. 그렇지만 유·무선망 사이에 중간 게이트웨이가 필요할 뿐만 아니라 기존의 인터넷 서비스를 충분히 이용할 수 없으며, 게이트웨이의 신뢰도에 따라 보안 강도가 결정되는 구조이다. 따라서 중간 게이트웨이는 외부의 모든 공격으로부터 안전하고 내부에서 보안 위반 행위를 하지 않는다는 가정이 절대적으로 필요하다.

기존의 고속 인터넷과 이동 통신 망이 연동하는 환경에서는 야기될 수 있는 보안문제는 외적인 통신 자원을 파괴와 정당한 가입자의 번호를 도용하거나, 도난·분실된 단말을 불법으로 사용하여 부당한 사용료 부과, 무선 통신의 본질적인 취약성과 암호화가 되었을 경우에도 암호화 알고리즘의 안전성에 문제로 인한 불법 도청, 프라이버시의 침해를 할 수 있는 사용자 정보나 위치 정보의 노출, 정보의 송신 부인이나 수신 부인, 내부적으로는 인증 서버나 이동 에이전트 역할을 담당하는 기지국 등이 결탁하여 불법행위를 하는 경우 등이 있다.

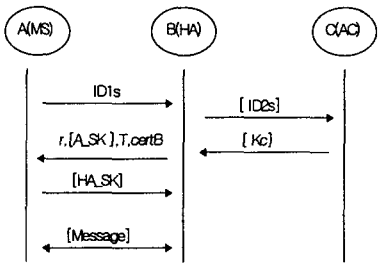
따라서 본 논문에서는 중간 에이전트를 두는 WAP 환경에서 사용자 인증과 안전한 키 분배, 프라이버시를 보장하는 프로토콜을 제안한다.

2. 기존의 연구

기존의 무선 통신망과 인터넷을 안전한 연동을 실현하기 위해서는 사용자와 데이터의 인증과 비밀성, 무결성, 부인봉쇄, 사용자의 프라이버시 등의 보장뿐만 아니라 웹 보안 기술, 암호 기술, 방화벽 기술, 침입 탐지 기술 등이 요구된다. 이 장에서 기술된 연구들을 대표적인 보안 서비스에 이동 통신 가입자의 프라이버시를 고려한 인증 프로토콜이다. 각 그림에서 A는 사용자 데이터를 송·수신하는 이동 호스트(MH), 사용자 데이터를 송·수신하는 고정 호스트(FH : Fixed Host), B는 이동 호스트와 유선 망간의 게이트웨이 역할을 담당하는 기지국인 호스트 에이전트(HA), 이동 단말이 현재 속해있는 셀의 에이전트가 아닌 다른 셀들의 외래 에이전트(FA : Foreign Agent), C(AC)는 인증 서버의 역할을 담당하는 노드를 가정하고 있다. 여기에서 C는 인증 기능을 수행하는 스테이션(station)으로서 3가지 경우를 고려할 수 있다. MH와 HA, FH의 관계에 있어서 C는 각각에 대해서 인증과 키 분배를 담당하는 제 3자인 인증 서버가 되고, MH이 다른 셀로 이동하여 MH와 HA, FA의 관계가 되어 HA로부터 인증을 받는 경우는 C는 HA가 되며, MH와 FA, FH의 관계인 경우에 인증을 HA로부터 받지 않는다면 제 3자인 인증 서버가 된다.



(그림 1) GSM 인증 프로토콜



(그림 2) Hom & Preneel 인증 프로토콜

2.1 비밀키 방식에 의한 인증 프로토콜[5]

2.1.1 GSM에서의 인증 및 세션 키 생성(그림1)

이동 통신의 에이전트는 인증서버(MSC/AC)와 공유하는 비밀키(K_i)를 스마트카드에 저장하고 있다는 가정에서 프로토콜이 수행된다.

가입자가 홈이 아닌 방문 지역으로 이동하여 서비스를 받기 위해서는 그림1과 같이 자신의 ID인 Aid를 에이전트 HA(FA)에게 전달한다. 에이전트는 인증 서버인 AC에게 Aid, Bid를 암호화하지 않는 상태로 전달한다. 인증서버는 임의의 난수(R)와 인증 정보(SRES), 이동 단말과 에이전트간의 세션 키를 에이전트로 암호화하여 전송하면 에이전트는 수신된 정보를 복호화하여 이동 단말의 신원을 확인하기 위해 난수만을 전송한다. 단말로부터 전송되어 온 SRES와 자신이 가지고 있는 SRES를 비교하여 정당한 사용자인지를 확인하고 에이전트는 A5 암호화 알고리즘에 의해서 세션 키와 임시적으로 사용할 가명 ID를 암호화하여 전송한다. 이동 단말 측에서는 가명을 사용하여 에이전트와 데이터를 교환한다.

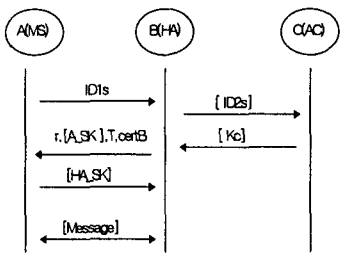
2.1.2 Hom & Preneel(H-P)의 인증 및 세션 키 생성(그림2)[3]

이동 단말은 u를 생성하여 gu ‖ Aid를 전송한다. 에이전트인 기지국은 자신이 생성한 v와 r을 사용하여 세션 키 K(= h1((gu)v ‖ r))를 생성한다. 그 다음 단계로 기지국 B는 random 값(r)과 [A_SK], TimeStamp T, 기지국의 인증서를 전송한다. 단말에서는 수신된 정보를

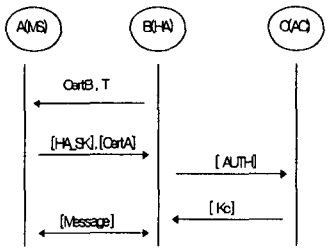
사용하여 세션 키 K'(= h1((gu)v ‖ r))를 생성한 다음 기지국이 가지고 있는 세션 키와 일치하는지를 확인하기 위해 [A_SK]'(= h2(K' ‖ r ‖ Bid)를 생성하여 [A_SK]와 비교한다. 수신된 키와 일치하면 사용자는 수신된 정보와 자신의 공개키, 해쉬 함수의 번호를 해쉬 함수에 적용한 다음 다시 서명한 결과와 단말의 공개 정보와 해쉬 함수 번호를 세션 키로 암호화한 결과를 기지국 B에 전송한다.

2.2 공개키 방식에 의한 인증 프로토콜

2.2.1 PACS 방식의 인증 및 세션 키 생성(그림3)[4]



(그림 3) PACS 인증 프로토콜



(그림 4) S-M-A 인증 프로토콜

기지국 B는 다른 그룹으로부터 자신의 그룹으로 이동한 단말을 위해 자신의 공개 인증서와 TimeStamp를 방송한다. 단말은 수신된 시간과 기지국의 ID, 단말의 가명 ID, 단말 번호를 사용하여 세션 키(K)를 생성한 다음 다시 세션 키와 단말 번호, 가명 ID, TimeStamp를 기지국의 공개키로 암호화한 결과([HA_SK])와 자신의 공개 인증서를 세션 키로 암호화([CertA])하여 기지국 B에 전송한다. 기지국에서는 자신의 개인 키로 복호화하고 단말의 인증서를 통해 이동 단말을 인증한다.

2.2.3 Samfat, Molva, Asokan의 인증 및 세션 키 생성(그림4)[2]

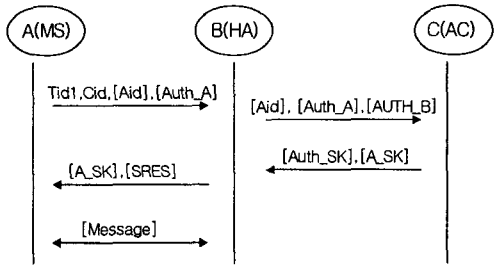
이 프로토콜에서 사용자 단말은 인증 서버의 ID와 자신의 ID를 숨기기 위해서 인증 서버의 공개키로 자신의 ID를 암호화하여 자신을 인증할 수 있는 인증 정보와 함께 전송한다. 기지국은 복호화 키를 알 수 없기 때문에 인증 서버 C에게 암호화된 단말 ID와 자신의 ID, 자신을 인증할 수 있는 정보를 함께 보낸다. 인증 서버가 개인 키를 사용하여 단말과 기지국을 인증한 다음 Auth1을 복호화할 수 있는 키를 기지국 B에게 전송하면 B는 단말을 인증하게 된다.

3. 제안된 WAP 환경에서의 인증 프로토콜

이 장에서는 WAP 환경에서 이동 사용자의 프라이버시와 단말의 성능을 고려한 인증 프로토콜을 제안한다.

3.2.3.1 시스템 계수(그림5)

- Aid, Bid, Cid : 사용자 단말과 에이전트인 기지국, 인증 서버의 ID
- Tid, Sid,: 사용자 A와 인증서버의 가명 ID
- $K_{A,C}$: 사용자와 인증 서버간의 대칭 키
- $K_{A,B}$ = h(Aid, Tid, $K_{A,C}$), h는 일 방향 해쉬 함수
- P_X, S_X : X(=A, B, C)의 공개키와 개인 키
- T, N_A, N_B : TimeStamp와 random 값
- [Aid] = [Aid, [N, N⊕Aid]S_A]PC
- [Auth_A] = [Aid, Bid, Tid, T, N_A]$K_{A,C}$
- [Auth_B] = [Bid, [Bid]S_B, Tid, N_B]P_C
- [Auth_SK] = [Sid, N_A, N_B, $K_{A,B}$]P_B
- [A_SK] = [Sid, Tid, N_A, N_B]$K_{A,C}$
- [RES] = [N_A]$K_{A,B}$



(그림 5) 제안된 인증 프로토콜

3.2.3.2 프로토콜 분석

이동 단말은 인증 서버(MSC/AC)와 공유하는 비밀키(Ki)와 자신의 식별자를 자신의 비밀키와 서버의 공개키로 암호화된 내용이 스마트 카드에 저장하고 있다는 가정에서 프로토콜이 수행된다. 이와 같이 식별자를 암호화한 이유는 단말 사용자와 인증 서버 이외의 제 3자에 의해서 생성되거나 복호화할 수 없는 정보로 사용하기 위함이다. 따라서 단말에서는 공개키나 비밀키로 암호화하는 알고리즘을 사용하지 않지만 대칭키를 사용하여 메시지를 암호화하는 알고리즘을 수행한다.

[단계1] 연결 설정 요청

MH → HA : [Aid], Cid, [Aid, [N, N⊕Aid]S_A]P_C, [Aid, Bid, Tid, T, N_A]$K_{A,C}$

이동 단말의 ID(Tid)와 서버의 ID(Cid), 스마트 카드에

저장되어 있는 [Aid], ID와 TimeStamp, 난수 등을 대칭키로 암호화하여 기지국에 전송한다. 여기에서 단말의 ID인 Aid를 사용하지 않고 Tid를 사용하는 것은 단말 사용자의 위치 정보나 통화 당사자에 대한 정보가 제 3자에게 노출되는 것을 방지하기 위함이다.

[단계2] 이동 단말과 에이전트 인증 요청

HA → MSC/AC : [Aid], [Auth_A], [Bid, [Bid]S_H, Tid, N_B]P_C

메시지 [Aid]와 [Auth_A]의 내용은 에이전트에 의해서 복호화할 수 없는 부분으로서 인증서버와 자신의 식별자와 단말의 가명, 난수를 서버의 공개키로 암호화하여 전송한다. 마지막 부분의 내용을 공개키로 암호화함으로써 서버이외의 제 3자가 이 내용을 받아볼 수 없게 된다.

[단계3] 인증 및 세션 키 전송

MSC/ACH → HA : [Sid, N_A, N_B, $K_{A,B}$]P_B, [Sid, Tid, N_A, N_B]$K_{A,C}$

서버는 [Aid]와 [Auth_A], [Bid]S_H를 통해 이동 단말과 에이전트를 인증할 수 있는데, 인증 서버는 여러 이동 단말과의 대칭키를 유지하고 있기 때문에 [Aid]는 [Auth_A]를 복호화하는 사용되는 대칭키를 검색하는 키로 사용된다. 따라서 서버와의 대칭키를 모르는 불법 사용자가 정당한 사용자 [Aid]와 자신이 만들어낸 [Auth_A]'를 전송하게 되면 복호화 키가 맞지 않아 인증을 받을 수 없게 된다. 서버 자신의 가명 식별자 Sid와 난수(N_A, N_B), 세션 키($K_{A,B}$)를 에이전트의 공개키로 암호화하여 자신과 이동 단말을 인증할 수 있도록 한다. 이동 단말에 전송할 부분도 자신의 가명 식별자와 난수를 대칭키로 암호화하여 함께 보낸다. 연결 설정 이후에 이동 단말과 에이전트가 메시지를 교환하는 경우에 실제 서버의 ID를 사용하지 않고 Sid를 사용한다. 여기에서 Sid를 사용하는 이유는 단말 사용자의 위치 정보나 통화 당사자에 대한 정보가 제 3자에게 노출되는 것을 방지하기 위해 Tid를 사용했듯이 서버 식별자를 그룹내의 다른 단말에 노출되는 것을 막기 위함이다..

[단계4] 인증 및 세션 키 확인

HA → MH : [Sid, Tid, NA, N_B]$K_{A,C}$, [N_B] $K_{A,B}$

이동 단말은 인증 서버와 에이전트로부터 수신된 N_B를 비교하여 일치하면 에이전트의 정당성과 세션 키의 안정성이 보장되기 때문에 메시지를 교환하겠지만 일치하지 않으면 불법 에이전트이거나 세션 키의 불일치로 인정하고 다시 연결설정을 시도한다. 실제 메시지를 교환하는 경우에 송신자와 수신자의 실제 ID를 사용하지 않고 가명 ID를 사용한다.

4. 결 론

인터넷의 사용이 보편화되고 이동 컴퓨터 서비스의 팽창이 가속화됨에 따라 신뢰성과 보안문제가 크게 대두되고 있다. 따라서 본 논문에서는 인터넷 멀티캐스트 환경에서 이동 호스를 위한 인증 프로토콜을 제안하였다. 인증 프로토콜은 그룹내의 다른 이동 단말에 대해 송·수신 호스트의 익명성이 보장하고, 이동 단말의 계산 능력을 감안해 대칭 키를 사용하였다. 그리고 호스트 에이전트에 이동 호스트의 ID를 감출 수 있으며, 같은 그룹에 반복 진입한 경우에 같은 대칭 키를 사용하지 않아도 된다. 유선 망에서는 기존의 통신방법을 그대로 사용할 수 있도록 하였다.

[참고문헌]

[1] A. Myles, D. B. Jhonson, and C. Perkins, "A mobile host protocol supporting route optimization and Authentication," IEEE Journal on Selected Areas in Communications, Vol.13, No.5, pp.839-849, June 1995.

[2] D. Samfat, R. Molva, N.Asokan, "Anonymity and Untraceability in Mobile networks," Proceedings of the ACM International Conference on Mobile Computing and Networking, Nov. 1995.

[3] G. Hom and B. Preneel, "Authentication and Payment in Future Mobile Systems," Proceedings ESORICS '98, LNCS 1485, pp.277-293.

[4] JTC(air)/94.12.15-119Rc, "Personal Communications Services," PACS Air Interface Specification, PN3418.

[5] M. Rahnema, "Overview of the GSM System and Protocol Architecture," IEEE Communications Magazine, April 1993.

[6] R. Molva, D.Samfat, G. tsudik, "Authentication of Mobile Users," IEEE Network Magagine, Special Issue on Mobile Communications, March/April 1994.

[7] "Wireless Application Protocol Architecture Specification," WAP Forum, Nov. 8, 1999. URL: http://www.wapForum.org.

[8] "Wireless Transport Layer Security Protocol Specification," WAP Forum, Nov. 8, 1999. URL: http://www.wapForum.org.

[9] 김기조, 최윤석, 최은정, 임경식, "무선 응용 프로토콜 기술," 한국정보처리학회지, 제7권 3호, 2000, pp.44-55.