이동 컴퓨팅 환경에서의 익명성과 불추적성 지원 기법

(A Scheme for Providing Anonymity and Untraceability in Mobile Computing Environments)

최 선 영 † 박 상 윤 † 엄 영 익 ††

(Sun young Choi) (Sang Yun Park) (Young Ik Eom)

요 약 이동 네트워크 상에서의 인터넷 서비스가 활성화됨에 따라 이동 호스트에 대한 인증 및 비밀성이 요구되었고, 이동 호스트의 이동성에 따른 익명성 및 불추적성이 중요한 고려사항이 되었다. 본 논문에서는 이동 호스트가 도메인간을 이동하면서 노출될 수 있는 이동 호스트의 Identity의 보호를 위해 사용자 Alias를 사용하였으며, 원격 도메인에도 Alias를 사용함으로 익명성 보장 및 불추적성을 지원한 안전한 인증 프로토콜을 제시한다. 본 논문에서는 안전성을 높이기 위해서 Alias 생성시 공개키 암호 시스템을 이용하였다.

Abstract In recent years, Internet-based application services on the mobile environment have been activated, and the developments of mobile internet application for user authentication and privacy have been required. Especially, the research for preventing disclosure of identity caused by user mobility is on the progress. In this paper, we introduce the study of an authentication protocol for anonymity and untraceability supporting the protection of user identity and the authenticated secure association mechanism between mobile hosts and remote domains. In this protocol use public cryptography.

1. 서 론

이동 컴퓨팅 환경이 보편화되고 이동 컴퓨팅 환경에서의 인터넷 서비스가 활성화됨에 따라 이동 호스트 사용자에 대한 인증 및 비밀성이 중요한 고려 사항이 되었다[1]. 특히, 이동 호스트 사용자의 이동에 의해 노출될 수 있는 사용자의 Identity를 보호하기 위한 이동 호스트의 익명성(Anonymity)과 불추적성(Untraceability)은 이동 인터넷 서비스의 인증 및 비밀성 분야의 새로운 연구 과제가 되고 있다.

그러나 기존 GSM 및 CDPD 등의 이동 네트워크 프로토콜들의 인증 및 비밀성 기술은 단순한 인증 과정과 약한 비밀성을 제공하고, 인증 과정에 사용자의 익명성을 일부만 포함함으로서 사용자의 Identity가 노출될 수 있는 한계점을 내포하고 있는 실정이다.

본 논문에서는 기존 이동 네트워크 프로토콜들의 인증, 비밀성 및 익명성에 대한 기술을 분석하고 문제점을 진단하며, 이를 개선하여 설계한 익명성 지원을 위한 인증 프로토콜의 기능 및 동작 원리를 소개한다. 본 논문의 2장에서는 이동 네트워크 프로토콜들의 기술 현황을 소개하고 3장에서는 본 인증 프로토콜의 설계를 위한 원칙들을 정의한다. 4장에서는 본 인증 프로토콜의 기능 및 동작원리를 소개하고, 5장에서는 본 인증 프로토콜의 평가 및 증명에 대해 기술하고, 6장에서는 요약 및 향 후 연구과제를 제시한다[1, 2, 3].

† 비 회 원 : 성균관대학교 전기전자및컴퓨터공학부
SUN391@chollian.net
bronson@ece.skku.ac.kr
†† 종신회원 : 성균관대학교 전기전자및컴퓨터공학부 교수
yieom@ece.skku.ac.kr
논문접수 : 2001년 1월 3일
심사완료 : 2001년 6월 7일

2. 이동 네트워크의 익명성 기술

2.1 기존 이동 네트워크 프로토콜의 익명성 기술

GSM(Global System for Mobile)은 가입자들에게 비밀성을 제공하는 최초의 digital cellular 네트워크

로서 TMSI(Temporary Mobile Subscriber Identity)라는 Alias를 사용하여 익명성을 제공한다. GSM에서는 IMSI(International Mobile Subscriber Identity)라는 사용자 고유의 Identity와 TMSI간의 매핑을 통하여 원격 도메인에서 사용자의 Identity를 보호할 수 있는 익명성을 제공하지만, 도청자는 트래픽 분석을 통하여 IMSI와 TMSI간의 관계를 유추할 수 있다[1, 2, 3].

CDPD(Cellular Digital Packet Data)는 GSM에 비해 좀 더 강한 익명성을 제공하는데, 인증 과정 이전에 사용자와 원격 도메인간에 Diffe-Hellman 키 교환 프로토콜을 사용해 비밀 세션 키를 생성하여 사용자 Identity를 암호화해서 원격 도메인에게 전달함으로서 도청자가 사용자 Identity를 획득할 수 없다. 그러나 원격 도메인에게 사용자 Identity가 노출될 수 있고, Diffe-Hellman 키 교환 프로토콜의 특성상 도청자가 원격 도메인으로 가장할 수 있는 등의 단점을 내포하고 있다[1, 4, 5, 6, 7].

2.2 익명성 보장을 위한 인증 프로토콜

Didier Samfat, Refik Molva 및 N. Asokan은 IBM에서 개발한 인증 및 키 교환 서비스인 KryptoKnight 시스템의 단-방향 인증 프로토콜을 기반으로 하여 익명성을 제공하고 세션키를 통한 비밀 통신을 할 수 있는 인증 프로토콜을 제안하였다. 이들이 제안한 인증 프로토콜은 사용자 및 원격 도메인 Identity와 랜덤 넘버를 사용하여 사용자 Alias를 생성하고, Alias를 사용자, 원격 도메인 및 홈 도메인간에 교환하여 사용자를 인증하며 세션 키를 생성하여 비밀 통신을 한다. 이 인증 프로토콜은 제삼자에게 사용자의 익명

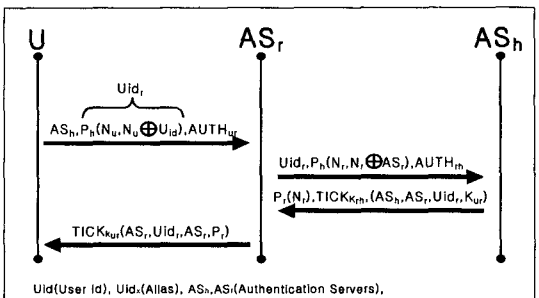

그림 1 Didier Samfat, Refik Molva 및 N. Asokan이 제안한 인증 프로토콜의 흐름도

성뿐 아니라 원격 도메인의 익명성도 보장하며, 인증 과정에 비밀 키 교환을 포함시킴으로서 인증과 키 교환 과정을 축약시키는 장점을 갖고 있다. 반면, 각 사이트의 메시지 인증 코드인 $AUTH_{ur}$와 $AUTH_{rh}$내의 Token 생성시 마다 3중의 암호화 과정을 수행해야 하는 오버헤드를 수반한다. 그림 1에서는 인증 프로토콜의 메시지 구조 및 흐름도를 예시한다[1, 2, 3, 4, 7].

2.3 인증 프로토콜 흐름도에 대한 설명

(1) 사용자로부터 원격 도메인 인증 서버에게 보내는 메시지

사용자는 원격 도메인에게 자신의 실제 Identity를 숨기기 위해서, Alias인 $\mathbf{Uid_r = P_h(N_u, N_u \oplus U_{id})}$를 사용하여 **홈 도메인 인증 서버($AS_h$)** 에게 $AUTH_{ur}$ 메시지를 보내게 된다. 사용된 인증 메시지 $\mathbf{AUTH_{ur} = [N_u, T_u, TokenK_{ur}(U_{id}, T_u, N_u)]}$이며, 여기서 $\mathbf{TokenK_{ur}(U_{id}, T_u, N_u)}$은 token chaining 기법[7]을 이용해 $\mathbf{E(U_{id} \oplus E(T_u \oplus E(N_u)))}$와 같이 삼중 암호화를 하였다. 여기서 E는 DES와 같은 암호화 함수로서 암호화 키 $\mathbf{K_{ur}}$로 암호화하여 나온 값을 표현한 것이다.

(2) 원격 도메인으로부터 홈 도메인에 보내는 메시지

원격 도메인 인증 서버는 사용자로부터 받은 메시지와 자신의 Alias인 $\mathbf{P_h(Nr, Nr \oplus ASr)}$를 생성하여 사용자의 홈 도메인 인증 서버에게 보낸다. $\mathbf{P_h(Nr, Nr \oplus ASr)}$는 도청자로부터 원격 도메인을 숨기기 위해 생성한 원격 도메인의 Alias이다. 원격 도메인 인증 서버가 생성한 랜덤 넘버 N_r를 원격 도메인의 실제 Identity와 배타적논리합(XOR)하여 홈 도메인 인증 서버의 공개키로 암호화한다. 원격 도메인 인증 서버의 인증을 위한 메시지로 token chaining 기법[7]을 이용한 $\mathbf{AUTH_{rh}}$를 생성하여 보낸다.

(3) 홈 도메인으로부터 원격 도메인에 보내는 메시지

홈 도메인의 인증 서버는 원격 도메인으로부터 받은 메시지를 통하여 원격 도메인과 사용자간의 세션키 K_{ur}를 계산하여 얻어낸다. 이를 원격 도메인 인증 서버에게 보내기 위해 티켓$\mathbf{TICK_{Krh}(AS_h, AS_r, Uid_r, K_{ur})}$과 $\mathbf{P_r(N_r)}$을 생성한다.

(4) 원격 도메인으로부터 사용자에게 보내는 메시지

홈 도메인 인증 서버로부터 받은 티켓으로부터 K_{ur}를 얻어내고, 이를 이용하여 사용자에게 보낼 새로운 티켓 $\mathbf{TICK_{Kur}(AS_h, Uid_r, AS_r, P_r)}$을 생성해 낸다.

(5) 사용자는 원격 도메인으로부터 티켓을 받고, 이를 K_{ur}로 복호화하여 상호 인증을 수립하게 된다.

2.4 Samfat, Refik Molva 및 N. Asokan가 제시한 프로토콜의 평가

Samfat, Refik Molva 및 N. Asokan가 제시한 프로토콜에서는 사용자가 Alias를 사용함으로 제삼자와 원격 도메인에게 사용자의 실제 Identity를 노출시키지 않기 때문에 사용자의 익명성을 보장한다. 또한, 원격 도메인의 Identity에도 Alias를 사용해 제삼자에게 사용자의 현재 위치를 추적할 없도록 불추적성을 지원한다. 그러나, 홈 도메인에게는 원격 도메인의 실제 Identity가 노출되므로 사용자의 현재 위치를 유추해 낼 수 있게 된다. 이는 위의 2.3절의 (2)에서 설명한 바와 같이 원격 도메인의 Alias가 홈 도메인의 공개키로 암호화한 값이므로, 이를 복호화 하여 원격 도메인의 실제 Identity를 알아 낼 수 있기 때문에 사용자의 위치 정보를 숨길 수 없다. 따라서 본 논문에서는 홈 도메인에게도 사용자의 위치 정보를 숨기기 위해 다음과 같은 프로토콜을 제시한다.

3. 설계 원칙

본 논문은 익명성과 불추적성을 위한 인증 프로토콜을 위해 다음과 같은 가정을 한다.

사용자는 홈 도메인으로부터 지속적으로 유지되는 유일한 Identity를 할당받는다. 사용자가 원격 도메인으로 이동하였을 때, 원격 도메인의 인증 서버는 사용자 인증을 위하여 서버 기반의 인증 시스템인 Kerberos 또는 KryptoKnight 등을 사용할 수 있다. 인증 서버들간의 인증을 위해서는 PKI(Public Key Infrastructure) 구조를 이용하는데, 이 때 인증 서버들은 Alias를 통한 상호인증을 전제로 한다. 다음 시나리오는 인증 서버간의 세션수립 과정을 예시한다[1, 7, 8].

(1) 이동 컴퓨팅 환경을 지원하는 인증 서버들은 PKI 구조내의 상위 인증 서버에게 각 인증 서버의 Alias를 등록하고 Alias에 대한 인증서를 획득한다. 획득된 인증서와 Alias는 공개되므로, 인증 서버들은 Alias에 대한 상호 인증을 수립할 수 있다. 따라서 각 인증 서버의 Identity는 도청자들 뿐 아니라 인증 서버들간에도 보호될 수 있다.

(2) 각 인증 서버들은 Alias를 갱신시 마다 상위 인증 서버에게 Alias를 등록하고, 새로운 인증서를 획득하며 이를 재공개한다.

(3) 인증 서버들 간에는 정기적으로 또는 필요시에 인증서를 교환하여 Alias에 대한 상호 인증을 수행하고 임시키를 공유하여 이동 호스트의 인증 요구 발생시에 사전에 수립된 임시키를 사용하여 비밀 통신을 하도록 한다.

4. 익명성과 불추적성을 위한 인증 프로토콜

4.1 익명성과 불추적성을 위한 인증 알고리즘

(1) Alias의 생성

① 사용자 Alias ($U_{alias} = P_h(N_u, N_u \oplus U_{id})$) : 사용자가 생성한 랜덤 넘버와 사용자의 실제 Identity를 랜덤 넘버와 배타적논리합(XOR)한 결과를 홈도메인 인증 서버의 공개키로 암호화한 Alias로 홈 도메인 서버만이 사용자의 Identity를 확인하여 인증할 수 있다.

② 원격 도메인 인증 서버의 Alias ($R_{alias} = P_{as}(N_r, N_r \oplus R_{id})$) : 원격 도메인 인증 서버가 생성한 랜덤 넘버와 원격 도메인 인증 서버의 Identity를 배타적논리합(XOR)한 결과를 상위 인증 서버의 공개키로 암호화한 Alias로 상위 인증 서버만이 원격 도메인의 실제 Identity를 확인할 수 있다.

(2) 전자 서명의 생성

① 사용자 전자 서명 ($SIG_{ur} = [N_u, T_u, ESk_{ur}(U_{alias}, N_u, T_u)]$) : 사용자의 Alias와 랜덤 넘버 및 타임 스탬프로 구성된 메시지를 메시지 다이제스트하고 랜덤 넘버와 타임 스탬프와 사용자와 원격 도메인간의 세션 키로 암호화된 메시지 다이제스트 코드를 조합하여 전자 서명을 구성한다.

② 원격 도메인 인증 서버의 전자 서명 ($SIG_{rh} = [N_r, T_r, ESk_{rh}(R_{alias}, N_r, T_r)]$) : 원격 도메인 인증 서버의 Alias와 랜덤 넘버 및 타임 스탬프로 구성된 메시지를 메시지 다이제스트하고 랜덤 넘버와 타임 스탬프와 원격 도메인과 홈 도메인간의 세션 키로 암호화된 메시지 다이제스트 코드를 조합하여 전자 서명을 구성한다.

③ 홈 도메인 인증 서버의 전자 서명 ($ASIG_{rh}=[N_r, N_h, T_h, Ek_{rh}(K_{ur}, N_r, N_h, T_h)]$) : 홈 도메인 인증 서버가 생성한, 사용자와 원격 도메인 인증 서버간의 세션 키와 원격 도메인과 홈 도메인의 랜덤 넘버 및 홈 도메인 인증 서버의 타임 스탬프를 원격 도메인과 홈 도메인간의 세션 키로 암호화한다. 원격 도메인과 홈 도메인의 랜덤 넘버, 홈 도메인의 타임 스탬프 및 암호화된 코드를 조합하여 전자 서명을 구성한다.

④ 원격 도메인 인증 서버의 전자 서명 ($ASIG_{ur} = [N_u, N_r, T_r, Ek_{ur}(AS_h, N_u, N_r, T_r)]$) : 원격 도메인 인증 서버가 이전 단계에서 수신하여 적재한 홈 도메인 인증 서버의 Identity, 사용자와 원격 도메인의 랜덤 넘버 및 타임 스탬프를 사용자와 원격 도메인의 세션키 K_{ur}로 암호화한다. 사용자와 원격 도메인의 랜덤 넘버와 타임 스탬프 및 암호화 코드를 조합하여 전자 서명을 구성한다.

(3) 세션 키의 생성

① 원격 도메인과 홈 도메인간의 세션 키 (K_{rh}) : 원격 도메인과 홈 도메인은 3장의 가정에서 언급한 바와 같이 Alias를 수반하는 PKI 구조를 통하여 인증 서버들 간에 인증을 수립하고 인증된 서버들간에 정기적인 세션 키를 관리함으로서 사용자의 이동에 따른 인증 서버간의 안전한 동적 통신을 지원하도록 한다.

② 사용자와 원격 도메인간의 세션 키 ($K_{ur} = H(U_{id} \oplus R_{alias})$) : 사용자의 Identy와 원격 도메인의 Alias를 H 해쉬 함수의 입력으로 하여 생성된 고정 길이 해쉬 코드를 세션 키로 한다.

4.2 익명성과 불추적성을 위한 인증 시나리오

(1) 1단계 (사용자 ⇒ 원격 도메인 인증 서버)

사용자가 홈 도메인을 벗어나 외부 영역에 진입한 경우 먼저 원격 도메인 인증 서버와의 통신을 위해 사용자 인증이 필요하게 된다. 사용자는 먼저 Alias 등록과 사용자 인증을 위해 홈 도메인 인증 서버에 메시지를 보내게 된다. 이 때, Alias를 이용하여 메시지를 보냄으로써, 제 삼자와 원격 도메인 인증 서버에게 사용자의 실제 Identity는 숨길 수 있다. 메시지 인증을 위해서 사용자와 원격 도메인 인증 서버간의 세션 키로 암호화한 SIG_{ur}을 원격 도메인 인증 서버에게 보낸다.

(2) 2단계 (원격 도메인 인증 서버 ⇒ 홈 도메인 인증 서버)

메시지를 받은 원격 도메인 인증 서버는 사용자의 $Alias(U_{alias})$, 원격 도메인의 $Alias(R_{alias})$ 및 SIG_{rh}를 조합한 메시지를 홈 도메인 인증 서버에게 보낸 후에 향 후 사용자 인증과 메시지 인증을 위해 SIG_{ur}를 저장한다. 이때, 원격 도메인의 Alias를 사용함으로 도청자와 홈 도메인으로부터 원격 도메인의 실제 Identity를 숨길 수 있다.

(3) 3단계 (홈 도메인 인증 서버 ⇒ 원격 도메인 인증 서버)

① 메시지를 받은 홈 도메인 인증 서버는 SIG_{rh}를 세션 키(K_{rh})로 복호화하여 메시지 인증을 하고 사용자의 $Alias(U_{alias})$를 홈 도메인의 비밀키로 복호화하여 사용자의 Identity를 획득한다.

② 홈 도메인 인증 서버는 사용자의 Identity와 원격 도메인 인증 서버의 $Alias(R_{alias})$를 이용해 K_{ur}를 생성한다. 이 단계에서 홈 도메인 인증 서버는 원격 도메인의 실제 Identity를 알 수 없기 때문에 현재 사용자의 위치를 유추할 수 없게 되고, 제 삼자에게도 완전한 익명성을 보장하게 된다.

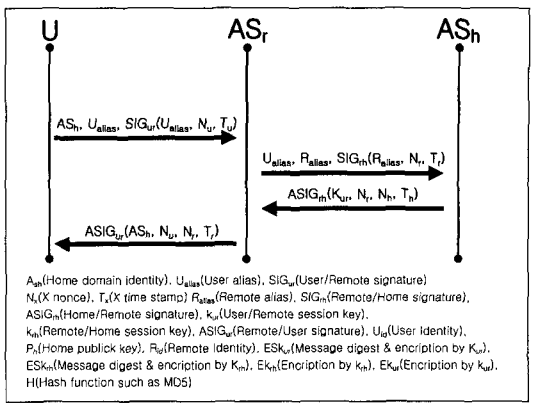

그림 2 익명성과 불추적성을 지원하는 인증 프로토콜의 동작 시나리오

③ 홈 도메인 인증 서버는 $ASIG_{rh}(K_{ur}, N_r, N_h, T_h)$를 원격 도메인 인증 서버에게 보낸다.

④ 원격 도메인 인증 서버는 $ASIG_{rh}$를 세션키(K_{rh})로 복호화하여 K_{ur}를 얻는다. K_{ur}로 저장해 두었던 SIG_{ur}를 복호화하여 사용자 인증과 사용자가 보낸 메시지 인증을 하게 된다.

(4) 4단계 (원격 도메인 인증 서버 ⇒ 사용자)

① 원격 도메인 인증 서버는 사용자에게 $ASIG_{ur}$를 생성하여 보낸다.

② 사용자는 $ASIG_{ur}$를 K_{ur}로 복호화하여, 원격 도메인 인증 서버의 인증과 메시지 인증을 하게된다. 따라서, 이 단계에서 최종적으로 상호 인증이 수립된다. 그림 2는 본 프로토콜의 인증 시나리오를 예시한다.

5. 프로토콜 평가 및 증명

5.1 프로토콜 평가

5.1.1 프로토콜 간소화

Didier Samfat, Refik Molva 및 N. Asokan이 제안한 익명성 및 불추적성을 지원하는 인증 프로토콜에서 사용한 메시지 인증 코드를 비교해보면 다음과 같다. 즉, $AUTH_{ur}$, $AUTH_{rh}$ 생성시 각각 삼중 암호화 과정을 거치게 되며, 본 논문에서 제시한 메시지 인증 코드인 SIG_{ur}과 SIG_{rh}는 다중 암호화 과정의 오버헤드를 줄이기 위해 단일 암호화 과정으로 간소화하였다. 따라서 Didier Samfat, Refik Molva 및 N. Asokan가 제안한 프로토콜에서는 사용자의 Alias 생성시 한번의 공개키 암호화, $AUTH_{ur}$ 생성시 삼중 암호화, 원격 도메인의 Alias 생성시 한 번의 공캐키 암호화, $AUTH_{rh}$ 생성시 삼중 암호화 과정을 거쳐,

표 1 프로토콜 암호화 회수 비교

Samfat, Refik Molva 및 N. Asokan가 제시한 프로토콜	본 논문에서 제시한 프로토콜
U-->AS_r : AS_h, Uid_r, $AUTH_{ur}$ 암호화 회수 $Uid_r = P_h(N_u, N_u \oplus U_{id})$, -->공개키로 한번 암호화 $AUTH_{ur} = [N_u, T_u, TokenK_{ur}(U_{id}, T_u, N_u)]$ $TokenK_{ur}(U_{id}, T_u, N_u) = E(U_{id} \oplus E(T_u \oplus E(N_u)))$ -->삼중 암호화 P_h: 홈 도메인 인증 서버의 공개키로 암호화 E: 암호화 키 K_{ur}로 DES와 같은 암호화 함수로 암호화한 것	U-->AS_r : AS_h, U_{alias}, $SIG_{ur}(U_{alias}, N_u, T_u)$ 암호화 회수 $U_{alias} = P_h(N_u, N_u \oplus U_{id})$ -->공개키로 한번 암호화 $SIG_{ur} = [N_u, T_u, ESk_{ur}(U_{alias}, N_u, T_u)]$ -->단일 암호화 P_h: 홈 도메인 인증 서버의 공개키로 암호화 ESk_{ur} : k_{ur}로 암호화
AS_r-->AS_h : Uid_r, $P_h(N_r, N_r \oplus AS_r)$, $AUTH_{rh}$ 암호화 회수 $P_h(N_r, N_r \oplus AS_r)$ -->홈 도메인의 공개키로 한번 암호화 $AUTH_{rh} = [N_r, T_r, TokenK_{rh}(R_{id}, T_r, N_r)]$ $TokenK_{rh}(R_{id}, T_r, N_r)] = E(R_{id} \oplus E(T_r \oplus E(N_r)))$ -->삼중 암호화	AS_r-->AS_h : U_{alias}, R_{alias}, $SIG_{rh}(R_{alias}, N_r, T_r)$ 암호화 회수 $R_{alias} = P_{as}(Nr, Nr \oplus ASr)$ -->상위 인증 서버의 공개키로 한번 암호화 $SIG_{rh} = [N_r, T_r, ESk_{rh}(R_{alias}, N_r, T_r)]$ -->단일 암호화

사용자로부터 홈 도메인까지 메시지를 보내는데 8번의 암호화 과정을 거치게 된다. 반면, 본 논문에서 제시한 프로토콜은 사용자의 Alias 생성시 한번의 공개키 암호화, SIGur 생성시 한번의 암호화, 원격도메인의 Alias 생성시 한번의 공개키 암호화, SIG_{rh} 생성시 한번의 암호화 과정을 거치므로 사용자로부터 홈 도메인까지 메시지를 보내는데, 4번의 암호화 과정을 거치게 된다. 따라서, 사용자로부터 홈 도메인까지 메시지를 보낼 때 총 암호화 회수가 반으로 감소하는 것을 볼 수 있으며, 비교표는 표 1과 같다.

5.1.2 강화된 익명성과 불추적성

기존 이동 컴퓨팅을 위한 인증 프로토콜들은 사용자 Identity를 도청자로부터 보호하거나 원격 도메인에게 숨기는 정도에 그치고, Didier Samfat, Refik Molva 및 N. Asokan에 의해 제안된 인증 프로토콜도 홈 도메인에게 사용자의 위치 정보를 완전히 숨기지는 못하게 된다. Didier Samfat, Refik Molva 및 N. Asokan가 제시한 프로토콜에서 사용한 Ralias는 원격 도메인의 실제 Identity와 랜덤 넘버를 배타적논리합(XOR)한 값을 홈 도메인 인증 서버의 공개키로 암호화하여, 랜덤 넘버와 함께 보내기 때문에 이 메시지를 받은 홈 도메인 인증 서버는 자신의 비밀키로 메시지를 복호화하여 나온 값을 랜덤 넘버로 배타적 논리합(XOR)하여 원격도메인의 실제 Identity를 얻어낼 수 있다.

이에 반해 본 논문에서 제시한 Ralias는 상위 인증 서버의 공개키로 원격 도메인의 실제 Identity와 랜덤 넘버를 배타적논리합(XOR)한 값을 암호화하였기 때문에, 메시지를 받은 홈 도메인은 원격 도메인의 실제 Identity를 유추해 낼 수 없다. 따라서, 도청자들뿐 아니라, 사용자의 홈 도메인에게도 사용자의 위치 정보를 숨길 수 있게 된다.

Didier Samfat, Refik Molva 및 N. Asokan에서 사용한 R_{alias}
$R_{alias} = P_h(Nr, Nr \oplus ASr)$
본 논문에서 제시한 R_{alias}
$R_{alias} = P_{as}(N_r, N_r \oplus R_{id})$

5.2 프로토콜 증명

본 논문에서 제시된 인증 프로토콜의 증명을 위하여 Michael Burrows가 제안한 증명 방법[9]을 사용하였다. Michael Burrows가 제안한 증명 방법에 사용되는 기본 용어는 표 2와 같다.

먼저 메시지 의미 규칙을 이용하여 메시지 인증 코드를 증명한다. 만일 수신자 A가 B로부터 메시지 $\langle X \rangle_K$를 수신하고 B와 공유하는 비밀키 K를 신뢰하면 A는 B가 메시지 X를 생성했다고 믿는다. 여기서 $\langle X \rangle_K$는 메시지 X를 비밀키 K로 암호화한 메시지이다. 공식화하면 다음과 같다.

$$\frac{A \text{ believes } A \overset{K}{\Longleftrightarrow} B,\ A \text{ sees } \langle X \rangle_K}{A \text{ beleieves } B \text{ once said } X}$$

용어 $\{M\}_K$는 K로 암호화된 메시지로 확장해서 생

표 2 기본 용어

Basic Notation

P believes X: P가 X를 신뢰한다.

P sees X: P가 X를 본다. 누군가 P에게 X를 포함한 메시지를 보내고, P는 이를 읽을 수 있다.

P said X: P가 X를 말한다. 즉, P가 X를 포함하는 메시지를 언젠가 보낸다.

P controls X: P는 X를 인증하고, 믿는다.

fresh(X): X는 fresh하다. 즉, X는 time stamp나 number를 포함하며, 오직 한번 사용된다.

$P \overset{K}{\Longleftrightarrow} Q$: P와 Q는 공유키 K를 사용한다.

$\overset{K}{\Longrightarrow} P$:P는 공개키로서 K를 갖는다.(비밀키 K^{-1})

$\{X\}_K$: X는 K에 의해 암호화 된다.

$\langle X \rangle_Y$: X는 formula Y와 함께 combine된다. 즉, X는 비밀키 Y함께 combine된다. X를 증명하기 위한 암호화키와 같은 방법이다.

각하면, "M은 K에 의해 보호된다."고 말할 수 있으며, 이는 수신자가 메시지 M을 복호화하기 위해 K를 알아야한다.

표현 방식을 증명방법에 맞추기 위해 다음과 같이 단순화시킨다.

$$ES_K(A,B,C) = \langle A,B,C \rangle_K$$

$$U_{alias} = \{U,N_u\}_{P_h}$$

$$R_{alias} = \{R,N_r\}_{P_{as}}$$

$$SIG_{ur} = N_u,\ T_u,\ ESk_{ur}\langle U_{alias},\ N_u,\ T_u\rangle_{K_{ur}}$$
$$= N_u,\ T_u,\langle U_{alias},\ N_u,\ T_u\rangle_{K_{ur}}$$

$$SIG_{rh} = N_r,\ T_r,\ ESk_{rh}\langle R_{alias},\ N_r,\ T_r\rangle_{K_{rh}}$$
$$= N_r,\ T_r,\langle R_{alias},\ N_r,\ T_r\rangle_{K_{rh}}$$

$$ASIG_{rh} = N_r,\ N_h,\ T_h,\ ESk_{rh}\langle K_{ur},\ N_r,\ N_h,\ T_h\rangle$$
$$= N_r,\ N_h,\ T_h,\langle K_{ur},\ N_r,\ N_h,\ T_h\rangle_{K_{rh}}$$

$$ASIG_{ur} = N_u,\ N_r,\ T_r,\ ESk_{ur}\langle AS_h,\ N_u,\ N_r,\ T_r\rangle$$
$$= N_u,\ N_r,\ T_r,\langle AS_h,\ N_u,\ N_r,\ T_r\rangle_{K_{ur}}$$

위의 기술된 사항에 따라 증명에 맞게 프로토콜을 단순화시키면 아래와 같다.

$$M1 : U \Rightarrow AS_r : \{U,N_u\}_{P_h},\ N_u,\ T_u,$$
$$\langle \{U,N_u\}_{P_h},\ N_u,\ T_u\rangle_{K_{ur}}$$

$$M2 : AS_r \Rightarrow AS_h : \{U,N_u\}_{P_h},\ \{R,N_r\}_{P_{as}},\ N_u,\ T_u,$$
$$\langle \{U,N_u\}_{P_h},\ N_u,\ T_u\rangle_{K_{ur}},\ N_r,\ T_r,$$
$$\langle \{R,N_r\}_{P_{as}},\ N_r,T_r\rangle_{K_{rh}}$$

$$M3 : AS_h \Rightarrow AS_r : \langle K_{ur},\ N_r,\ N_h,\ T_h\rangle_{K_{rh}}$$

$$M4 : AS_r \Rightarrow U : \langle AS_h,\ N_u,\ N_r,\ T_r,\ U \overset{K_{ur}}{\Longleftrightarrow} AS_r\rangle$$

위의 프로토콜은 실제 프로토콜(real protocol)을 나타내며, BAN logic 증명절차를 따르면 위의 실제 프로토콜과 증명을 위한 가정을 통하여 다음과 같은 이상적인 프로토콜(idealized protocol)을 유추해 낼 수 있다. 이 프로토콜은 상호 인증을 통하여 신뢰성을 얻고, 사용자와 원격 도메인의 Identity를 위해 Alias를 사용하였으므로 익명성과 불추적성을 제공하게 된다.

$$M1 : U \Rightarrow AS_r : \{U,N_u\}_{P_h}$$
$$\langle \{U,N_u\}_{P_h},\ N_u,T_u,\ U \overset{K_{ur}}{\Longleftrightarrow} AS_r\rangle_{K_{ur}},$$

$$M2 : AS_r \Rightarrow AS_h : \{U,N_u\}_{P_h}\ \{R,N_r\}_{P_{as}},$$
$$\langle \{U,N_u\}_{P_h},\ N_u,T_u,\ U \overset{K_{ur}}{\Longleftrightarrow} AS_r\rangle_{K_{ur}},$$
$$\langle \{R,N_r\}_{P_{as}},\ N_r,T_r\rangle_{K_{rh}}$$

$$M3 : AS_h \Rightarrow AS_r : \langle K_{ur},\ N_r,\ N_h,\ T_h\rangle_{K_{rh}}$$

$$M4 : AS_r \Rightarrow U : \langle AS_h,\ N_u,\ N_r,\ T_r,\ U \overset{K_{ur}}{\Longleftrightarrow} AS_r\rangle$$

위의 이상적인 프로토콜 증명을 위하여 다음과 같은 가정을 한다.

(1) 키에 대한 가정

$$A1 : U\ believes\ U \overset{K_{ur}}{\Longleftrightarrow} AS_r$$
$$A2 : AS_h\ believes\ U \overset{K_{uh}}{\Longleftrightarrow} AS_h$$
$$A3 : AS_h\ believes\ AS_r \overset{K_{rh}}{\Longleftrightarrow} AS_h$$
$$A4 : AS_r\ believes\ AS_r \overset{K_{rh}}{\Longleftrightarrow} AS_{rh}$$
$$A5 : AS_r\ believes\ AS_h\ controls\ AS_r \overset{K}{\Longleftrightarrow} U$$
$$A6 : AS_r\ believes \overset{P_{as}}{\Longrightarrow} AS$$
$$A6' : AS\ believes \overset{P_{as}}{\Longrightarrow} AS$$
$$A7 : AS_h\ believes \overset{P_{as}}{\Longrightarrow} AS$$
$$A7' : AS\ believes \overset{P_{as}}{\Longrightarrow} AS$$

(2) 임의 수와 타임 스탬프에 대한 가정

$$A8 : U\ believes \overset{P_h}{\Longrightarrow} AS_h$$
$$A9 : U\ believes\ T_u\ is\ fresh$$
$$A10 : AS_h\ believes\ T_u\ is\ fresh$$
$$A11 : AS_r\ believes\ T_u\ is\ fresh$$
$$A12 : U\ believes\ N_u\ is\ fresh$$
$$A13 : AS_r\ believes\ N_r\ is\ fresh$$

(3) 증명은 다음과 같다.

① M1은 사용자가 원격도메인 서버로 메시지를 보내는 것으로 다음과 같은 R1이 나온다. R1은 "누군가 AS_r에게 보낸 K_{ur}로 암호화된 메시지를 AS_r이 볼 수 있다."는 의미이다.

$$R1 : AS_r\ sees \langle \{U,N_u\}_{P_h},\ N_u,T_u,\ U \overset{K_{ur}}{\Longleftrightarrow} AS_r\rangle_{K_{ur}}$$

② M2는 원격 도메인이 홈 도메인으로 보내는 메시지로 가정 A7, A7′ 와 Component Visitibility Rule을 적용하면 "AS_h 는 U와 AS_r를 포함한 메시지를 볼 수 있다."는 R2가 나온다.

$$R2 : AS_h\ sees\ U, AS_r$$

③ R2에서 AS_h는 메시지를 발생시킨 사용자의 실제 Identity 알기 때문에 이로부터 ASr과 배타적논리

합(XOR)하여 K_{ur}를 계산해 낼 수 있다. 이때, AS_h는 AS_r을 볼 수 있지만, 이는 AS_r이 Alias로 사용하였기 때문에 실제 AS_r의 Identity는 알지 못한다. 이에 대한 실제 Identity는 상위 인증 서버인 AS 만이 알 수 있다. 따라서, 다음과 같은 "AS_h는 U와 AS_r이 공유하는 키 K_{ur}를 신뢰한다."는 R3가 나온다.

$$R3 : AS_h \text{ believes } U \overset{K_{ur}}{\Longleftrightarrow} AS_r$$

③′ M2와 R3, 가설 A10를 이용해 the Message Meaning Rule과 Nonce Verification Rule을 적용시키면 다음과 같은 "AS_h는 U를 믿고, U는 U와 AS_r이 공유하는 키 K_{ur}를 신뢰한다."는 법칙이 나온다.

$$R3 : AS_h \text{ believes } U \text{ believes } U \overset{K_{ur}}{\Longleftrightarrow} AS_r$$

④ M2에서는 "AS_h는 N_r은 fresh하다는 것을 믿는다."는 R4에 도달할 수 있다.

$$R4 : AS_h \text{ believes } N_r \text{ is fresh}$$

⑤ M2, A3, R4를 이용해 the Message Meaning Rule과 Nonce Verification Rule을 적용하면 "AS_h는 AS_r을 믿고, AS_r은 N_r을 신뢰한다." R5가 나온다.

$$R5 : AS_h \text{ believes } AS_r \text{ believes } N_r$$

⑥ M3, A4, A13를 이용해 Message Meaning Rule과 Nonce Verification Rule을 적용하면 다음과 같은 "AS_r은 AS_h를 믿고, AS_h는 U와 AS_r이 공유하는 키 K_{ur}를 신뢰한다."는 R6에 도달한다.

$$R6 : AS_r \text{ believes } AS_h \text{ believes } U \overset{K_{ur}}{\Longleftrightarrow} AS_r$$

⑦ R6, A5를 이용해 the Jurisdiction Rule을 적용하면 다음과 같은 "AS_r은 U와 AS_r이 공유하는 키 K_{ur}를 사용하며 이를 신뢰한다."는 R7에 도달한다.

$$R7 : AS_r \text{ believes } U \overset{K_{ur}}{\Longleftrightarrow} AS_r$$

⑦′ R7, R1, A11을 이용해 the Message Meaning Rule과 Nonce Verification Rule을 적용하면 다음과 같은 "AS_r은 U를 믿으며, U는 U와 AS_r간에 사용하는 공유키 K_{ur}를 신뢰한다."는 R7에 도달한다.

$$R7 : AS_r \text{ believes } U \text{ believes } U \overset{K_{ur}}{\Longleftrightarrow} AS_r$$

⑧ M4, A1, A12를 이용해 the Message Meaning Rule과 Nonce Verification Rule을 적용하면 "U는 AS_r을 믿으며, AS_r는 U와 AS_r간에 사용하는 공유키 K_{ur}를 신뢰한다."는 R8에 도달한다.

$$R8 : U \text{ believes } AS_r \text{ believes } U \overset{K_{ur}}{\Longleftrightarrow} AS_r$$

R7과 R8은 프로토콜의 결과로서, U와 AS_r간의 세션키인 K_{ur}이 생성되어 상호 인증을 수립하게 된다. 이 과정에서 사용자와 원격 도메인 AS_r은 Alias를 사용함으로 제 삼자에게 사용자의 실제 Identity와 위치 정보를 숨길 수 있게 된다. 또한, AS_r은 상위 인증 서버의 공개키로 암호화한 Alias를 사용하였으므로 AS_h는 원격 도메인의 실제 Identity를 알지 못하므로 홈 도메인 인증 서버에게도 사용자의 위치 정보가 노출되지 않게 된다.

6. 결 론

이동 컴퓨팅 환경에서의 인터넷 서비스가 활성화되고, 인증 및 비밀성이 요구되는 이동 인터넷 응용의 개발이 급속히 확산되고 있다. 특히, 이동 인터넷 서비스의 인증 및 비밀성 분야 중에서 이동 호스트 사용자의 이동에 의해 야기되는 사용자 Identity의 노출을 보호하기 위한 연구가 진행 중에 있다.

본 논문에서 제시한 프로토콜은 이동 컴퓨팅 환경에서 사용자의 이동에 따라 노출될 수 있는 사용자의 Identity와 원격 도메인의 Identity를 숨겨 사용자의 익명성 및 불추적성을 보장하였다. 이를 위해서 사용자의 실제 Identity 대신 사용자의 Alias를 사용하였으며, 원격 도메인 인증 서버도 Alias를 사용함으로서 도청자 뿐 아니라 홈 도메인에게도 사용자의 익명성을 보장할 수 있도록 하였다. 따라서, 이동 호스트의 사용자 증가되고 사용자의 프라이버시 보호의 요구가 증가됨에 따라 사용자 익명성과 불추적성을 지원하는 본 인증 프로토콜은 제삼자로부터 사용자의 Identity와 이동성 보호를 위해 유용하게 사용될 수 있다.

참 고 문 헌

[1] D. Samfat, R. Molva and N. Asokan, "Untraceablibity in Mobile Networks," MobiCom '95, November, 1995.

[2] Willian Stallings, CRYPTOGRAPYH AND NETWORK SECURITY: Principles and Practice, 2nd ed. Prentice-Hall, 1999.

[3] Jungjoon Kim, Mina Oh, and Taegun Kim, "Security Requirements of Next Generation Wireless Communications," Communication Technology Proceedings, 1998.

[4] Y. Frankel, A. Herzberg, P. A. Karger, H. Krawczyk, C. A. Kunzinger, M. Yung, "Security Issues in a CDPD Wireless Network," IEEE Personal Communications, Vol. 2, No. 4, Aug. 1995.

[5] G. Pierce and C. Paar, "Recent Developments in Digital Wireless Network Security," Technical

conference on Telecommunications Research and Development in Massachusetts, Lowell, March 12, 1996.
[6] Min-Shiang H., Yuan-Liang Tang and Heng-Chi Lee, "An efficient authentication protocol for GSM networks," UROCOMM 2000. Inforamation Systems for Inhanced Public Safety and Securi IEEE/AFCEA, 2000.
[7] Refik Molva Didier Smafat, Gene Tsudik, "Authentication of Mobile Users," IEEE Network, Social Issue on Mobile Communication Technologies, Vol. 8, No. w, March/April 1994.
[8] R. Molva, G. Tsudik, E. Van Herreweghen, S. Zatti, "KryptoKnight Authentication and Key Distribution System," Proceedings of ESORICS'92, November 1992.
[9] Michael Burrows et al., "A Logic of Authentication," Digital System Research Center, Tchinical Report 39, February 1990, May 1994.

최 선 영
1995년 2월 강원대 학사. 1998년 8월 성균관대 전기전자컴퓨터공학부 석사. 2001년 2월 성균관대 전기전자컴퓨터공학부 박사과정 수료. 관심분야는 이동 컴퓨팅 시스템, 이동 컴퓨팅 보안, 분산 시스템

박 상 윤
1997년 2월 동국대학교 전자계산학과 학사. 1999년 2월 성균관대학교 전기전자 및 컴퓨터공학부 석사. 2001년 2월 성균관대학교 전기전자 및 컴퓨터공학부 박사과정 수료. 관심분야는 이동 컴퓨팅 시스템, 시스템/이동 컴퓨팅 보안, 분산 시스템

엄 영 익
1983년 2월 서울대학교 계산통계학과 학사. 1985년 2월 서울대학교 대학원 전산과학전공 석사. 1991년 8월 서울대학교 대학원 전산과학전공 박사. 현재 성균관대학교 전기전자 및 컴퓨터공학부 교수. 2000년 8월 ~ 2001년 8월 미국 Univ. of California, Irvine에서 Visiting Scholar. 관심분야는 분산 시스템, 이동 컴퓨팅 시스템, 분산 객체 시스템