2001년 한국정보처리학회 춘계 학술발표논문집 제8권 제1호

WPAN에서 종단 사용자를 위한 상호 공정 계약 지원 서비스

장경아, 이병래, 김태윤
고려대학교 컴퓨터학과
e-mail : gypsy93@netlab.korea.ac.kr

Mutual Fair Contract Service for End-Users in WPAN

Kyung-Ah Chang, Byung-Rae Lee, Tai-Yun Kim
Dept. of Computer Science & Engineering, Korea University

요 약

본 논문에서는 WPAN(Wireless Personal Area Network)의 종단 사용자 기기의 한계적 계산 능력 및 무선 링크의 대역폭과 기존 외부 네트워크와의 연결을 고려하여 선택적 신뢰 기관(Trusted Third Party, TTP) 서비스를 수용한 상호 공정 계약 서비스 프로토콜을 제안하였다. 제안한 서비스는 종단 사용자 기기의 한계적 능력에 대해 해당 내부 네트워크의 TTP 와 공개키를 기반으로 인증 서비스를 수행하도록 하였으며, 이후 종단 사용자는 해당 인증 결과를 기반으로 외부 네트워크의 전자 상거래 주체와의 상호 메시지 교환을 위한 서비스 프로토콜을 수행하도록 하였다. 또한 사전에 외부 네트워크에 대한 전자 상거래 서비스 요청에 한하여 TTP 의 부분적 서비스를 수행하도록 허용하여 시스템의 대단위 계산 능력에 대한 효율성을 보장할 수 있다.

1. 서 론

인터넷의 확장은 가정 내의 가전 기기와 자동화 기기에 대해 자체적으로 내부 네트워크를 구성하여 정보 공유 및 외부의 제어가 가능한 홈 네트워크 형태로 발전하고 있으며, 이것은 근거리 무선 통신 기술의 실용화로 휴대 전화기를 기반으로 다종 기기간의 통신을 지원하는 네트워크(WPAN : Wireless Personal Area Network)를 구성하고 있다.

WPAN 환경에서 사용자는 자신의 휴대 정보기기와 다른 정보기기 대한 Bluetooth 등의 무선 서비스 접속을 통해 휴대 전화기를 게이트웨이로 하여 외부망의 인터넷 컨텐츠 사용을 가능하게 한다. 이에 따라 사용자는 이전의 통신 구조를 이용한 인터넷 전자 상거래 등의 서비스 뿐만 아니라 가정과 기존 외부망의 원활한 물리적 연결 및 가정 내의 다양한 기기에 대한 제어 및 업그레이 등에 필요한 상호 연결, 무오류(Fail-free) 서비스 지원 등이 요구하고 있다.

최근 Bluetooth 등 다양한 구조에 기반한 전자 상거래 참여가 증가하면서 이에 따른 안전성에 대한 많은 연구가 진행 중이다.

본 연구에서는 WPAN 의 종단 사용자 기기의 한계적 계산 능력 및 무선 링크의 대역폭과 기존 외부 네트워크와의 연결을 고려하여 선택적 신뢰 기관(Trusted Third Party, TTP) 서비스를 수용한 보안 관리 서비스 프로토콜을 제안하였다.

제안한 서비스는 종단 사용자 기기의 한계적 능력에 대해 해당 내부 네트워크의 TTP 와 공개키를 기반으로 인증 서비스를 수행하도록 하였으며, 이후 종단 사용자는 해당 인증 결과를 기반으로 외부 네트워크의 전자 상거래 주체와의 상호 메시지 교환을 위한 보안 관리 서비스 프로토콜을 수행하도록 하였다.

또한 사전에 외부 네트워크에 대한 전자 상거래 서비스 요청에 한하여 TTP 의 부분적 서비스를 수행하도록 허용하여 시스템의 대단위 계산 능력에 대한 효율성을 보장할 수 있다.

본 연구의 구성은 다음과 같다. 2 장에서 보안 관리 서비스 및 공개키 기반 인증 구조를 살펴본다. 3 장에서는 해당 내부 네트워크의 선택적 TTP 서비스 구

조를 수용하여 인증 수행 및 이후 인증 결과 정보를 기반으로 전자 상거래 지원 보안 관리 서비스 프로토콜을 제안한다. 마지막으로 4 장에서 결론을 내리고 향후 과제를 제시한다.

2. 관련 연구

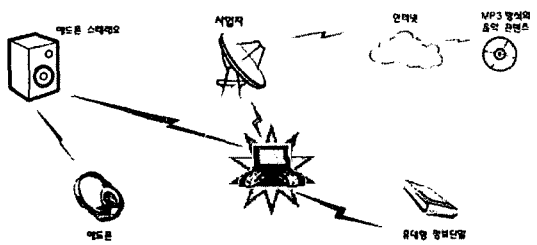
2.1 WPAN 지원 전자 상거래 보안 서비스

전자 상거래에서 종단 사용자 간의 계약 문서나 결제 정보 교환은 논리적 동시성 보장을 가정하고 있으나 실제 네트워크 환경에서는 불가능하므로 TTP 설치를 통해 메시지 교환에 대한 보안 관리 서비스를 중개하도록 한다.

그러나, 이것은 TTP 로의 병목 현상이 발생할 위험이 있으며, WPAN 과 같은 환경에서는 더욱이 기존 외부 네트워크의 TTP 와의 연결도 원활하지 못하므로 내부 네트워크의 홈 게이트웨이 서버에 대해 TTP 서비스를 수용할 수 있도록 하여 사전에 정의된 외부 네트워크와의 전자 상거래 서비스 요청에 한하여 TTP 를 이용하는 최적화 기법이 제안되었다.

일반적으로 서비스 초기화시 종단간 주체는 전자 상거래 메시지 교환 프로토콜에서 사용될 형식과 TTP 서비스에 대해 동의하도록 한다. 이때 종단 사용자는 자신의 모든 권한과 자신의 해당 정보를 내부 네트워크의 홈 게이트웨이 서버에 위임하고 이것으로 홈 게이트웨이 서버는 사전 정의된 전자 상거래 서비스 요청이 들어오면, 외부 네트워크 상거래 주체에게서 응답을 기대하는 해당 아이템을 전송하게 된다.

만약 내부 네트워크의 종단 사용자가 TTP 서비스를 통해 기대한 아이템에 대한 응답을 회수하게 되면 프로토콜을 성공적으로 종료하게 된다. 이외의 경우 종단 사용자는 공정 상호 교환 여부를 판단하기 위해 홈 게이트웨이 서버에게 TTP 서비스를 문의하기 위해 요청하게 된다. <그림 1>은 WPAN 과 같은 홈 네트워크 환경에서의 기본적인 구조를 나타내고 있다.



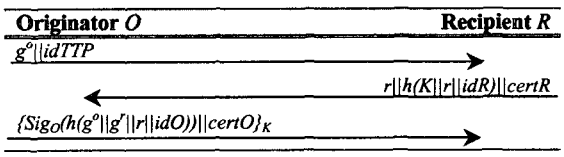
<그림 1> 홈네트워크 환경의 기본 구조

2.2 공개키 기반 인증 구조

WPAN 환경에서 대부분의 종단 사용자 기기의 한계적 계산 능력 및 무선 링크의 대역폭에 대한 한계는 전자 상거래 지원에 있어 비밀키 암호 방식 이상을 채택하기 어렵다.

본 논문에서 고려하고 있는 WPAN 환경에서는 종단 사용자의 전자 상거래 관련 정보에 대한 위탁으로 초기화 된다. 실제 서비스 프로토콜은 내부 네트워크의 홈 게이트웨이 서버에 대해 종단 사용자가 외부 네트워크의 전자 상거래 서비스 요청에 대한 초기화로 시작된다. 홈 게이트웨이 서버는 TTP 서비스를 실행하여 해당 외부 네트워크로의 관련 서비스를 수행하며 이에 대한 결과를 종단 사용자에게 통보하게 된다.

종단 사용자 기기의 한계적인 컴퓨팅 능력을 고려하였을 때, 선택적 TTP 서비스 수행은 효율적이다. 또한 종단 사용자와 홈 게이트웨이 서버는 세션키를 공유하므로, 전자 상거래 지원 서비스 프로토콜의 종료후, 단지 결과를 통보 받기만 하면 된다.



<그림 1> 기본 인증 프로토콜

본 논문에서 제안하는 보안 관리 서비스의 기본 인증 구조는 O 가 난수 o 를 생성하여 공개키 동의 키 (public key agreement key) g^o 와 함께 메시지를 교환하고자 하는 R 의 해당 인증 기관 정보 id_caR 를 R 에게 전송하면서 시작된다. <그림 1>은 기본 인증 프로토콜 구조를 나타내고 있다.

이 메시지로는 R 은 아직 통신 대상을 파악할 수 없으나 난수 r 을 생성하여 전송 받은 정보를 $(g^o)^r$ 로 연산하여 세션키 K 를 생성하여 해쉬화(h)한 후 R 의 인증서 $certR$ 와 함께 전송한다. O 는 $certR$ 를 통해 R 의 공개키 정보 등을 파악할 수 있으며 자신의 신분 정보 idO 와 함께 인증서 $certO$ 를 자신의 공개키로 서명한 후 다시 K 로 암호화하여 전송하게 된다. 이후 R 은 $certO$ 를 통해 O 의 서명을 검증하게 되고 이 정보는 차후 서비스에 반영하도록 한다.

3. 종단 사용자의 상호 공정 계약 서비스

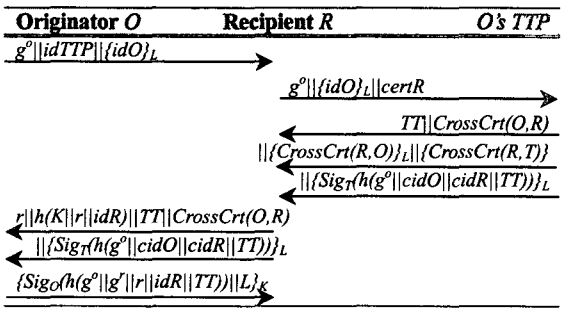
3.1 제안한 서비스 프로토콜의 개요

본 연구에서 제안하는 서비스 종단간 인증 및 메시지 교환 과정으로 구성된다. 선택적 TTP 서비스 수행을 기반으로 종단 사용자 기기의 컴퓨팅 능력 및 대역폭에 대한 오버헤드에 대한 대단위 계산의 효율

성을 증가시킨다.

3.2 종단 사용자의 상호 인증 프로토콜

종단간 인증 프로토콜은 주체 *O* 와 *R* 이 상대방의 인증서 검증을 위해 해당 TTP 의 공개키 보유 및 해당 TTP 에 자신의 공개키에 대한 인증서 식별 정보 (*cidO, cidR*)를 인지하고 있음을 가정한다. <그림 2>는 제안한 인증 프로토콜을 나타내고 있다.



<그림 2> 제안한 종단간 인증 프로토콜

종단간 인증 프로토콜은 내부 네트워크의 종단 사용자로부터 위탁 받은 정보를 통해 해당 홈 게이트웨이 서버 *O* 가 외부 네트워크 전자 상거래 주체 *R* 에게 자신의 네트워크 영역에 대한 TTP 식별 정보 및 TTP 과의 공유 비밀키 *L* 로 암호화된 자신의 신분 정보를 전송한다. 이 메시지를 *R* 은 자신의 인증서 (*certR*)와 함께 *O's TTP* 에게 전달(forwarding)한다. 이때 *O's TTP* 는 $\{idO\}_L$ 를 복호화하여 현재 유효한 사용자인지를 확인하고 *R* 의 인증서 적합성 역시 검증하여 종단간 인증을 수행하도록 한다.

인증서의 유용성이 검증된 경우, *O's TTP* 는 타임스탬프 *TT* 와 *O* 에 대한 범용 인증서(*CrossCrt*)들과 검증된 인증서에 대한 고유 식별 정보 *cidO, cidR* 를 서명하여 암호화한 후 *R* 에게 전송한다. *CrossCrt* 는 해당 네트워크의 TTP 가 그 인증서에 서명하여 일반 인증서를 확장한 형태이다.

마지막으로 *O* 가 받은 메시지의 서명을 검증하여 올바르다고 판단되었다면 *O* 는 *R* 에게 비밀키 *L* 을 포함한 메시지를 세션키 *K* 로 암호화하여 전송한다. *R* 은 비밀키 *L* 을 사용하여 *O* 의 마지막 전송 단계 이후 TTP 로부터 받은 메시지를 복호화하고 그 서명을 검증할 수 있다.

3.3 계약 메시지 교환 프로토콜

인증 프로토콜 수행 이후 메시지 교환 프로토콜은 *Exchange, Abort, Resolve* 단계로 구성하였다. 정상적인 메시지 교환시 양자간 프로토콜로 구성된 *Exchange* 프로토콜만 실행되며, 종단간 주체 간의 프로토콜 수행에 대한 오류 판단으로 강제적 종료 및 검증을 요청할 경우, 홈 게이트웨이 서버의 TTP 서비스를 실행하도록 하여 상대 주체의 정당성 여부를 결정한 후 프로토콜의 진행 여부를 결정하도록 하였다.

4. 결론 및 향후 과제

본 연구에서는 WPAN 의 종단 사용자 기기의 한계적 계산 능력 및 무선 링크의 대역폭과 기존 외부 네트워크와의 연결을 고려하여 선택적 신뢰 기관 (Trusted Third Party, TTP) 서비스를 수용한 상호 공종 계약 서비스 프로토콜을 제안하였다.

제안한 서비스는 종단 사용자 기기의 한계적 능력에 대해 해당 내부 네트워크의 TTP 와 공개키를 기반으로 인증 서비스를 수행하도록 하였으며, 이후 종단 사용자는 해당 인증 결과를 기반으로 외부 네트워크의 전자 상거래 주체와의 상호 메시지 교환을 위한 서비스 프로토콜을 수행하도록 하였다.

또한 사전에 외부 네트워크에 대한 전자 상거래 서비스 요청에 한하여 TTP 의 부분적 서비스를 수행하도록 허용하여 시스템의 대단위 계산 능력에 대한 효율성을 보장할 수 있다. 향후 본 논문에서 제안한 보안 관리 서비스의 WPAN 에 대한 안전성 검증과 이를 바탕으로 비동기적 메시지 교환 메커니즘에 대한 연구 및 분석이 진행되어야 할 것이다.

참 고 문 헌

[1] N. Asokan and Victor Shoup, "Optimistic fair exchange of digital signatures",*EUROCRYPT '98, Springer-Verlag*, 1998.

[2] P. A. Kearns, et al., "Wireless Personal Area Network Standards: Consumer in Mind?", Research Report RZ 2975(#93022), 2000.

[3] http://www.ieee802.org/, IEEE 802.15 Working Group for Wireless Personal Area Networks (WPANs)

[4] N. Asokan and Victor Shoup, "Optimistic fair exchange of digital signatures", *Advances in Cryptology – EUROCRYPT '98, Springer-Verlag*, 1998.

[5] N. Asokan, Victor Shoup, Michael Waidner, "Asynchronous protocols for optimistic fair exchange", Research Report RZ 2976(#93022), IBM Research, 1997.

[6] M. Ben-Or, O. Goldreich, S. Micali, R. L. Rivest, "A fair protocol for signing contracts", *IEEE Transactions on Information Theory*, Vol. 36 No.1, pp.40-46, 1990.

[7] Holger Burk, Andresas Pfitzmann, "Value exchange systems enabling security and unobservability", Computers & Security, Vol. 9 No. 8, pp.715-721, 1990.

[8] Benjamin Cox, J. D. Tygar, Marvin Sirbu, "NetBill security and transaction protocol", *USENIX Workshop on Electronic Commerce*, USENIX, 1995.

[9] Reboert H. Deng, Li Gong, Aurel A. Lazar, Weiguo Wang, "Practical protocols for certified electronic mail", *Journal of Network and System Managemnet*, Vol. 4 No. 3, 1996.

[10] Mattew K. Franklin, Michael K. Reiter, "Fair Exchange

with a semi-trusted third party", *ACM Conference on Computer and Communications Security*, pp1-7, 1997.

[11] N. Asokan, M. Schunter, M. Waidner, "Optimistic protocols for fair exchange", *ACM Conference on Computer and Communications Security*, pp. 8-17, 1997.