P2P상에 전자서명 알고리즘 인증 설계

이정기* · 문정환* · 이준**
*조선대학교 컴퓨터공학과
**조선대학교 컴퓨터공학부

Authentication Design for Digital Signature Algorithm in P2P Base

Jeong-ki Lee* · Jung-hwan Moon* · Joon Lee**
* Dept. of Computer Engineering, Chosun University.
** School of Computer Engineering, Chosun University.
E-mail : sitdol@yahoo.co.kr

요 약

개방형 네트워크를 통한 전자거래는 무엇보다도 거래의 신뢰성 제고 측면에서 집중적으로 논의되고 있는데 이를 확보하기 위한 중요한 수단으로서 전자서명과 인증제도 방안이 가장 주목을 받고 있다. 전자서명은 기술적으로 암호기술을 이용하여 통신내용의 무결성과 기밀성을 보장받고, 법적으로는 근거법의 제정을 통하여 전자문서와 전자서명의 효력을 부여받아 그 신뢰성을 확보하게 되는 것이다. 특히 P2P기반의 개방형 시스템 환경에서 신뢰성, 무결성, 부인금지와 같은 각종 기술적 선결과제들을 해결하고 거래의 신뢰성을 제고하기 위한 여러 가지 전자서명 방안들 중에서도 현재까지 공개키 암호화방식과 일방적 해쉬함수의 요약추출물 알고리즘을 결합한 디지털서명이 가장 믿을 만한 전자서명 방안으로 인정받고 있는 실정이다. 본 연구는 P2P 전자서명 모델에 개인 간 전자서명모델 이론을 조명하고 P2P 전자문서를 안전하고 신뢰성 있게 이용 할 수 있는 여건을 조성 할 수 있도록 공개키 암호기술에 기반을 두었으며 P2P상에서 전자서명 프로그램이 원활히 작동하도록 설계하고 전자 서명된 문서가 변질되지 않고 상호간의 사용자에게 신뢰할 수 있도록 하였다.

Ⅰ. 서 론

전자서명은 기술적으로 암호기술을 이용하여 통신내용의 무결성과 기밀성을 보장받고, 법적으로는 근거법의 제정을 통하여 전자문서와 전자서명의 효력을 부여받아 그 진정성을 확보하게 되는 것이다. 특히 P2P에서의 개방형 시스템에서의 진정성, 무결성, 부인금지와 같은 각종 기술적 선결과제들을 해결하고 거래의 신뢰성을 제고하기 위한 여러 가지 전자서명 방안들 중에서도 현재까지 공개키 암호화 방식과 일방적 해쉬함수의 요약추출물 알고리즘을 결합한 디지털서명이 가장 믿을 만한 전자서명 방안으로 인정받고 있는 실정이다[1][2][3].

본 연구는 P2P 전자서명 모델에 관한 가능성에 대한 의견이 많으나 이론에 대한 것은 아직까지 미흡하다. 이러한 관점에서 개인 간 전자서명모델 이론을 조명하고 먼저 P2P의 개념 및 구성 방식과 P2P새로운 키워드 서비스와 P2P 전자문서를 안전하고 신뢰성 있게 이용 할 수 있는 여건을 조성 할 수 있도록 공개키 암호기술에 기반을 두는 방식을 사용하여 P2P에서 전자서명을 이용한 전자거래 보안에 대한 신뢰도를 향상시킬 수 있도록 하며, 최종적으로 결론을 내리고자 한다[4][8].

Ⅱ. Peer-to-Peer

P2P(Peer-to-Peer) 컴퓨팅은 공동 파일 서버에 전적으로 의존하지 않으면서 각 PC 간의 직접적인 리소스 교환을 지원하는 Application 및 Network 솔루션으로 정의할 수 있다[1][6]. 그러므로 모두 Client/Server 양쪽으로 활동할 수 있는 "Peer"가 되며 이는 다양한 신규 Application을 위한 기초가 될 뿐 아니라, 기존 인프라스트럭처에서 상당한 로드를 덜어냄으로써 값비싸고 성능에 방해가 되는 업그레이드의 필요성을 줄일 수 있는 장점을 가지고 있다.

혼합 시스템은 중앙 서버에 의존하는 방식으로

대부분의 작업이 서버에서 처리되며 직접적인 파일 전달만 개인 대 개인으로 이루어지는 방식이다. Hybrid 경우 각 Client간 통신 방식은 최초의 관계가 형성되기까지 서버의 존재를 필요로 하며, 이 관계가 형성된 후 Client 상호간 직접 정보를 전달하는 특성을 가진다[6]. 실제로 원하는 파일을 내려받기 할 때에는 중앙 서버를 거치지 않고 파일을 갖고 있는 사용자의 PC와 직접 연결하게 된다. P2P 파일공유서비스를 제공하게 되는 대부분의 컴퓨터프로그램이 냅스터와 같은 방식을 취하고 있으며, 중앙 서버가 공유 파일의 목록까지 유지하는가, 아니면 접속자의 유동IP 주소만을 유지하는가에 따라서 여러 가지로 나뉘게 된다.

순수 시스템은 Hybrid P2P 방식의 서비스가 중앙관리서버에 의해 검색 기능을 지원하는 것에 반해 Pure구조은 서버가 존재하지 않는 방식으로 구현된 기술이다[6]. 모든 Peer가 동등한 조건을 가지고 익명성이 보장된 형태로 자료나 리소스를 공유하는 구조이다. 모든 이용자들이 직접 상호관계를 맺고 디렉토리 정보를 릴레이식으로 중개하는 방식을 취하게 된다. Pure구조은 어느 단일 주체에 의하여 보급, 관리되는 소프트웨어가 아니라 그 소스코드가 공개되었고 자유로이 배포되어 누구라도 수정을 할 수 있다. 따라서 P2P서비스를 제공하는 업체를 대상으로 저작권침해를 추궁할 수 없다는 점에서 Hybrid P2P서비스의 경우보다 저작권이 실행될 수 있는 가능성은 현실적으로 희박하다. 분산된 모델에서도 기본적으로 새로운 호스트를 찾기 위한 모델로 중앙 집중식 방법을 쓰기도 한다. 중앙 집중식 모델을 제외한 다른 방법을 사용할 수도 있지만 대부부분의 분산 모델에서 중앙 집중식 방법을 체택하는 추세다. 또 분산된 모델에 대표적인 것은 라우팅 모델이다.

III. 전자서명과 위협행위

일반적으로 전자서명은 크게 두 가지 의미로 나뉘어 진다. 첫 번째는 Electronic Signature를 의미하는 것이며, 두 번째는 Digital Signature를 말하는 것이다.

전자의 가장 일반적인 예는 전자 펜을 이용 한 그래픽 기반의 서명 방식이다. 전자 서명된 문서를 수신한 수신자는 시각적으로 전자서명의 진위를 확인한 후 전자문서의 접수여부를 결정하게 된다[7].

후자는 공개키 암호 기술에 기반을 두는 방식으로서 사용자는 자신만이 알고있는 전자 서명 생성키를 이용하여 수학적인 연산을 통하여 자신만의 고유한 전자서명 값을 계산한 후, 그 결과를 수신자에게 송신한다[8]. 수신자는 송신자가 제공하는 전자서명 검증키를 사용하여 전자서명 값의 진위여부를 수학적인 연산으로 확인할 수 있으며, 올바른 결과 값이 나오는 경우에만 전자문서를 접수한다.

최근 선진 각국에서 시행 또는 제정 중에 있는 전자서명법은 일반적으로 후자의 개념을 법적으로 인정하고 있다.

3-1. 필요성

컴퓨터 네트웍을 통한 비 대면 방식의 전자적 거래는 기존 거래 방식에서 시간적·공간적 제약의 문제점을 해결해줌으로써 새로운 거래 문화로서 자리잡아 가고 있다. 이러한 전자적 거래는 많은 장점을 가지고 있음에도 불과하고, 보안 요구사항이 먼저 해결되어야만 전자적 거래의 활성화를 기대 할 수 있을 것이다. 대표적인 보안 선결 요구사항은 다음과 같다.

가. 무결성 : 메시지가 변조나 수정이 될 수 없게 하는 것을 말한다.
나. 비밀성 : 적법한 수신자를 제외한 제3자는 볼 수 없도록 하는 기능을 말한다.
다. 부인방지 : 부인방지는 메시지를 송·수신하는 경우 해당자가 송·수신에 대한 행위를 부인 못하도록 하는 기능을 말한다.

전자서명은 상기의 보안 요구사항 중 인증, 무결성, 부인방지에 대한 보안 기능을 제공해 주며, 이것은 결국 비 대면 방식의 전자적 거래 환경 구축이 전자서명 기술이 필요하다는 것을 의미한다.

3-2. 전자서명의 요구 사항

전자서명 알고리즘은 안전·신뢰성 보장을 위해 기본적인 요구사항을 만족해야만 한다. 전자서명 알고리즘은 전자서명 검증키로부터 전자서명 생성키가 계산되는 것이 실행 불가능해야 하며, 전자서명은 메시지 내용, 서명자의 전자서명 생성키, 그리고 사용자 정보에 의존되어 생성되어야만 한다. 전자서명의 요구사항들은 다음과 같다[4][5].

가. 위조 불가 : 합법적인 서명자만이 전자서명을 생성할 수 있어야 한다.
나. 서명자 인증 : 서명자를 불특정 다수가 검증할 수 있어야 한다.
다. 부인방지 : 서명자는 서명한 후에 서명한 사실을 부인할 수 없어야 한다.
라. 변경 불가 : 서명한 문서의 내용을 변경할 수 없어야 한다.
마. 재사용 불가 : 전자서명을 다른 전자문서의 서명으로 사용할 수 없어야 한다.

IV. 공개키 암호시스템을 이용한 전자서명

전자서명기술은 공개키 암호 알고리즘으로 비밀키와 공개키가 사용된다. 공개키를 공개해도 그 공개키에 대응하는 비밀키를 알아내는 것은 계산상 불가능하다. 또한 공개키 암호 알고리즘에서 사용

되는 비밀키가 전자서명을 새성하는 생성키가 되고 공개키가 전자서명을 검증하는 검증키 역할을 한다[5]. 그러므로 전자서명기술의 안전한 운영은 서명키(공개키 암호알고리즘의 비밀키)와 검증키(공개키 암호알고리즘의 공개키)의 안전한 운영에 달려 있으며 서명키의 안전한 운영은 비밀키의 안전한 보관을 말하며 검증키의 안전한 운영은 공개키의 안전한 관리를 의미한다.

공개키는 공개된 정보이므로 어떻게 공개키 위·변조 문제를 해결하는가 하는 공개키 인증 문제를 귀착하게 된다[3].

그림 1는 이러한 키의 운영과 서명 및 암호화에 대한 내용을 설명하고 있다.

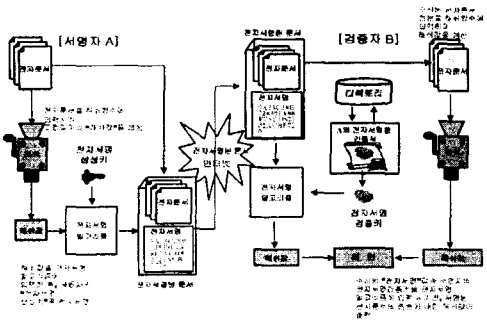

그림 4. 전자서명 생성·검증 과정
Fig 1. Digital Signature Generation · Verify Process

V. P2P기반에 전자서명 설계

수신자가 서명자로부터 디지털서명이 첨부된 전자문서를 전달받아 진정성, 무결성 등을 확인하기 위하여는 서명자의 공개키를 획득할 수 있어야 하는데, 원칙적으로 그 획득방법에는 제한이 없다. 즉, 수신자는 서명자로부터 서명자의 공개키를 건네 받은 서명자의 지인 을 통하여 디스켓에 담겨진 형태의 공개키를 전달받을 수도 있고, P2P서비스를 통하여 서명자로부터 그의 공개키를 직접 전달받는다.

그러나 어떠한 경우이든 서명자의 공개키가 서명자 자신의 것임이 객관적으로 보장되어 있는 않는 상황에서는 수신자가 서명자의 공개키를 이용하여 확인과정을 밟고 무작정 그 결과를 믿는다는 것은 매우 위험한 일이다.

왜냐하면 진정한 서명자가 아닌 다른 이가 자신이 진정한 서명자인 양 행동하면서 서명자의 공개키라고 주장하며 제공한 공개키를 다른 사용자의 진정한 공개키라고 언제나 신뢰할 수는 없기 때문이다. 그러므로 전자서명이 서명방법으로서 진정성과 무결성 등을 확실히 보장하기 위해서는 결국 서명자의 공개키가 진정한 서명자 자신에게 귀속되는 것임이 전제되어야 하며, 이러한 견지에서 디지털서명이 제 기능을 하는데는 서명자와 수신자 양자 모두가 신뢰 할 수 있는 제3자의 개념이 인증기관이다.

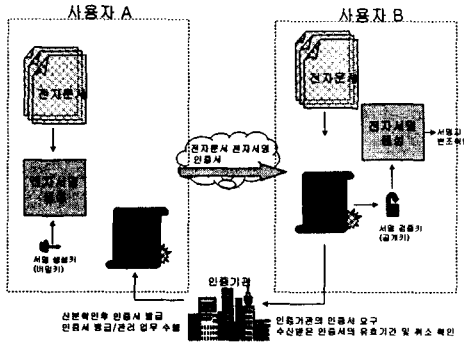

그림 5. P2P 전자서명 인증 센터
Fig 2. P2P Digital Signature Certification Center

그림 2는 서명자와 서명자로부터 전자문서를 받는 검증자의 경우를 나타낸 것이다. 서명자는 먼저 스스로 자신의 개인키와 공개키의 키조합을 생성한 다음, 개인키는 자신의 디지털서명을 위하여 보관하고 자신의 공개키는 각종 신상정보와 함께 인증기관에 제공하게 된다. 이때 인증기관은 서명자가 제공한 신상정보 등을 확인함과 동시에 제공받은 공개키가 서명자의 것인지를 확인하고 서명자의 공개키와 인증기관 자신의 디지털서명이 포함된 인증서를 서명자에게 발행하다. 이후 인증기관으로부터 인증서를 발급 받은 서명자는 상대방에게 전자문서에 디지털서명하고 그 주문서를 그의 공개키가 포함된 인증서와 함께 상대방에게 송신한다. 서명자로부터 디지털 서명된 전자문서를 수신한 상대방은 디지털서명에 관한 확인절차를 거치기 전에 인증기관이 제공하는 인증취소목록 등을 통하여 인증서의 유효 여부를 확인한 다음, 유효함이 인증서에 포함된 공개키를 가지고 전자문서의 진정성립과 무결성 등을 확인하면 된다.

VI. 결 론

컴퓨터와 정보 통신의 발달로 정보를 처리하고 저장하며 분배하는 능력이 향상되게 되었고 이로 인하여 P2P서비스와 전자서명은 정보화 시대에 제외 할 수 없는 분야가 되었다.

그러나 이러한 인터넷을 이용한 전자거래가 우리에게 커다란 편익을 주는 것은 사실이지만 전자문서를 이용한 전자거래는 여러 가지 문제점을 안고 있다. 거래 당사자들 간의 법적 분쟁이 방생했을 경우, 디지털 서명을 통한 신원 인증 및 메시지 인증은 부인 방지, 신분 인증에 대한 정확성과 신뢰성에 취약하다. 이러한 위협을 제거하기 위해 본 논문에서는 알려진 공개키 암호화 기법을 이용하여 공개키 기반 구조로 이루어진 인증센터를 설계하고 정당한 사용자에게 인증기관이 인증서를 발

급해 주도록 하였다. 앞으로 P2P서비스에서 전자거래 발전은 지속적으로 발전할 것이다. 이를 위해 안전한 인증 시스템에 관한 연구가 지속적으로 이루어지고 있다. 그러나 시스템의 안정성과 프라이버시를 보호하기 위해서는 상대적으로 계산 량과 저장량은 많아지고 처리속도와 효율성은 떨어질 것이다. 따라서 안전성과 효율성 등을 보장할 수 있는 방법에 대한 계속적인 연구가 진행되어야 할 것이다.

참고 문헌

[1] Kan. G., "Gnutella", in Andy Oram(ed), Peer-to-Peer: Harnessing the Power of Disruptive Technologies, 2001,

[2] Merrill Lynch, The Decentralized Web-Peer to Peer Internetworking Joins Browser -Based Computing". 2000. 6.

[3] ITU-T Recommandation X.509 (1997) ISO IEC 9594-8 1997, Information-The Directory; Authectication Framework, 1997.

[4] PKCS#1 V2.0, RSA Cryptography Standard", Oct., 1998.

[5] "Digital Signature Trust Co." Http://www.arcanvs.com/arcanvsCPD.html",1999.

[6] http://www.openp2p.com/topics/p2p/security/

[7] 이대기, 김희선, 조영섭, 진승현, 정교일, 조현숙 "국내외 전자서명 및 인증제도 동향 분석' 정보보증학회 2001.08.

[8] 이경석, 최도순, 이종근, "정보통신 보호를 위한 전자서명과 접근제어", 창원대학교, Vol.2 No.1[1998]