TTP 보안 서비스 레벨에서 효율성과 공정성을 고려한 부인봉쇄 프로토콜

학생회원 박 상 준*, 정회원 홍 충 선*, 이 대 영*

Non-repudiation Protocol for Efficiency and Fairness in TTP Security Service Level

Sang Jun Park* *Student Member,* Choong Seon Hong*, Dae Young Lee* *Regular Members*

요 약

최근 인터넷 등과 같은 전자적인 서비스에서 약속된 프로토콜에 위반한 송수신자 쌍방간의 행위에 대한 기술적인 증거를 제공하고, 논쟁 발생 시 법적 근거로 제공할 수 있게 해주는 서비스로 부인봉쇄 서비스가 있다. 본 논문에서는 부인봉쇄 서비스를 위해 필요한 제 3의 신뢰기관인 TTP (Trusted Third Party)의 기능을 확장시켜 부인봉쇄 서비스에서의 효율성을 향상시키고, 동시에 공정성을 제공하는 프로토콜을 제안한다. 본 논문에서는 TTP의 기능을 확장시키기 위하여 Time Check기능과 Alert Message를 적용하여 모의실험결과 기존에 연구되어진 부인봉쇄 프로토콜보다 효율성이 증가함을 알 수 있었다.

ABSTRACT

Recently, in the case that provides electronic services using Internet, we need the non-repudiation service that supplies a technological evidence about actions between a sender and a receiver that violate the promised protocol. Also, this service offers legal evidences while producing controversy. In this paper, we propose a protocol that improves the efficiency and offers the fairness of non-repudiation service by the extension of ability of TTP (Trusted Third Party). The proposed protocol adds a Time Check function and an Alert Message to extend the ability of TTP. Through the computer simulation, we prove that the proposed protocol has better efficiency than previous protocols.

I. 서 론

네트워크를 통해 전송되는 메시지 즉, 전자문서는 직접 만나서 전해주지 않기 때문에 송신자와 수신자 서로간에 메시지의 송수신 여부를 쉽게 확인하기 어려운 특성이 있다. 특히, 현 사회가 정보화 사회로 발전하고, 인터넷이 급속히 확산 및 상용화됨에 따라 정보보호 기술을 이용하여 지금까지는 메시지 기밀성, 사용자 인증, 정보의 무결성, 전자 서명 등의 다양한 보안 서비스를 제공해오고 있었으나, 송수신자의 상호 거래에 있어서 자신들의 거래 행위를 부인하여 원래의 요청과는 위배되는 불법행위가 발생할 때를 대비할 부인봉쇄라는 새로운 서비스가 필요하게 되었다. 따라서 부인봉쇄 서비스 (Non-repudiation service) [1]는 송수신자 쌍방간의 행위에 기술적인 증거를 제공하고, 논쟁 발생 시 법적 근거를 제공하여준다.

본 논문에서는 이러한 부인봉쇄서비스에 개입되는 제 3의 신뢰기관 (Trusted Third Party) [2,7]에 대한 의존성을 줄여 부인봉쇄 서비스의 효율성을 향상시키고, 동시에 공정성을 제공하는 프로토콜을 제시하고 기존의 연구들과 모의실험을 통하여 비교

* 경희대학교 전자정보학부 (sjpark@digital.kyunghee.ac.kr)
논문번호: 010118-0524, 접수일자: 2001년 5월 24일

하였다.

본 논문의 구성은 다음과 같다. 2장에서는 현재 제공되어지고 있는 부인봉쇄 메커니즘에 대해 살펴보고, 3장에서는 부인봉쇄 서비스에 대한 기존의 관련 연구들을 소개한다. 4장에서는 이 논문에서 제안하고자 하는 TTP의 기능을 확장한 프로토콜 제시한다.

5장에서는 제시된 프로토콜의 시뮬레이션 결과를 분석하고, 6장에서는 현재의 부인봉쇄 서비스에서의 문제점들과 제안한 프로토콜에서 기대할 수 있는 효과를 논의하며 결론을 맺고 향후 연구 방향을 제시한다.

Ⅱ. 부인봉쇄 서비스의 응용분야

최근 인터넷 등과 같은 통신로를 이용하여 전자적인 서비스의 제공이 확대되고 있다. 그러나 서비스를 제공하면서 약속된 프로토콜을 위반하는 행위를 하는 송. 수신자가 발생할 수 있고, 이런 경우를 대비한 송. 수신자 쌍방간의 행위에 대한 기술적이고 법적인 근거가 필요로 하게 된다. 이러한 부인 공격을 방지하기 위해서 다음과 같은 부인봉쇄 메커니즘 서비스가 제공되어져야한다.

- 송신부인봉쇄 (NRO:Non-Repudiation of Origin) : 송신자가 보낸 메시지에 대한 송신자의 부인을 방지한다.
- 수신부인봉쇄 (NRR:Non-Repudiation of Receipt) : 수신자가 메시지를 수신하고 이를 부인하는 것을 방지한다.
- 제출부인봉쇄 (NRS:Non-Repudiation of Submission) : 송신자가 제출한 메시지가 배달되기 위하여 배달기관에 제출되었다는 증거를 제공한다.
- 전달부인봉쇄 (NRD:Non-Repudiation of Delivery) : 메시지가 배달기관에 의해 수신자에게 전송되었다는 증거를 제공한다.

부인봉쇄 서비스의 적용 가능한 분야는 다음과 같은 것들이 있다[12].

- 전자상거래 : 최근 인터넷 쇼핑, 사이버 은행, 온라인 증권거래 등 전자상거래 시장이 크게 활성화되고 있다. 전자상거래에서는 이용자들에게 직접적으로 물품과 비용 등을 주고받기 때문에 공정한 전자상거래가 이루어지기 위해서는 부인봉쇄 서비스가 필수적이다.
- 전자계약 : 국내에서 전자서명법이 99년 하반기부터 발표되어 이에 따라 전자적인 수단으로 이루어지는 계약이 큰 비중을 차지하게 될 것으로 기대된다. 이러한 전자계약에서의 공정성을 위해 부인봉쇄 서비스가 반드시 필요하다.
- 이동통신 : 현재의 WAP이나 IMT-2000같은 차세대 이동통신서비스에서는 음성기능뿐만 아니라 데이터통신, 인터넷 서비스, 전자상거래 등의 다양한 기능을 제공할 것이다. 이동통신단말기를 통하여 전자상거래와 같은 서비스를 이용하기 위해서는 앞에서 기술한 바와 같이 부인봉쇄 서비스가 제공되어져야 한다.
- 전자우편 : 인터넷의 보급에 따라 컴퓨터를 이용한 메일이나 문서의 전달이 확산되고 있다. 우체국을 대신하는 이러한 서비스에서 우편물의 송. 수신 부인을 방지하고 배달을 증명할 수 있는 부인봉쇄 서비스를 활용할 수 있다.
- 온라인 요금납부 : 최근 인터넷을 이용한 통신매체가 발달하면서 기존의 요금 납부 방식이 온라인 방식으로 대체되는 추세에 있다. 온라인 지불에 대한 전자영수증을 받을 경우 이의 유효성을 위해 부인봉쇄 서비스의 활용이 기대된다.

Ⅲ. 관련 연구

3.1 연구동향

현재 부인봉쇄 메커니즘과 관련하여 표준화가 이루어져 있는 부분으로는 OSI 환경에서의 송. 수신 부인봉쇄 서비스를 규정하는 Open System Interconnection - Security Framework in Part 4 : Non-Repudiation 과 ISO/IEC 13888의 Part1,2,3이 있다[3,4,5].

최근에 부인봉쇄 메커니즘과 관련하여 많은 연구가 진행 중에 있다. 크게 나누어 국제 표준으로 제시된 메커니즘들이 충족시키고 있지 못한 부분을 보완하는 것과 효율성 개선이라는 두 가지 측면에서 접근하고 있다. 표준 메커니즘들이 만족하고 있지 못한 요소로는 수신자의 선택적 수신 (selective receipt) 문제와 공정성 (Fairness) 문제가 있다. 이러한 문제점들을 개선하기 위해 J. Zhou와 D. Gollmann등이 연구를 수행하였다[1,6,7]. 효율성 개선과 관련한 연구로는 기존의 부인봉쇄 메커니즘이 의존하는 제 3의 신뢰기관인 TTP의 의존도를 줄이는 방향으로 연구를 수행하고 있다. 또한 프로토콜 수행을 위한 통신량을 줄이는 방법에 대한 연구도 병행하여 이루어지고 있다[8,9].

관련 연구의 프로토콜을 이해하는데 필요한 기본

용어는 다음과 같다.

-X, Y : 두 메시지 X와 Y의 연결
-H(X) : 메시지 X의 해쉬 함수
-eK(X) and dK(X) : 키 K를 이용한 메시지 X의 암호화와 복호화
-sK(X) : 개인키 K를 이용한 메시지 X의 디지털 서명
-PA, SA : 주체 A의 공개키와 개인키
-A→B : 주체 A가 주체 B에게 메시지 X를 전달함
-fNRO : NRO를 나타내는 플래그 정보
-fNRR : NRR를 나타내는 플래그 정보
-fNRS : NRS를 나타내는 플래그 정보
-fNRD : NRD를 나타내는 플래그 정보

3.2 J. Zhou, D. Gollmann의 기법

[2]에서 제시한 ZG기법에서는 TTP의 개입을 줄이기 위하여 통신채널의 환경에 따라 부인봉쇄 프로토콜을 4가지로 분류하였으며, 비밀키를 적용하여 공정성 문제를 해결하려 하였다.

각각의 통신채널에서의 부인봉쇄 프로토콜을 다음과 같다.

CASE 1 : 통신채널과 통신 상대자 모두를 신뢰할 수 있는 경우

1. A→B : fNRO, B, M, *sSA*(fNRO, B, M)
2. B→A : fNRR, A, M, *sSB*(fNRR, A, M)

CASE 2 : 통신채널은 신뢰할 수 있으나, 통신 상대자는 신뢰할 수 없는 경우

1. A→TTP : fNRO, TTP, B, M, *sSA*(fNRO, TTP, B, M)
2. TTP→B : fNRS, A, B, M, *sST*(fNRS, A, B, M)
3. TTP→A : fNRD, A, B, *sST*(fNRD, A, B, M)

CASE 3 : 통신채널은 신뢰할 수 없으나, 통신 상대자는 신뢰할 수 있는 경우

1. A→B : fNRO, B, M, *sSA*(fNRO, B, M)
2. B→A : fNRR, A, *sSB*(fNRR, A, M)
3. A→B : fACK, B, *sSA*(fACK, B, M)

CASE 4 : 통신채널도 신뢰할 수 없고, 통신 상대자도 신뢰할 수 없는 경우

1. A→B : fPOE, B, *e*K(M), *sSA*(fPOE, B, eK(M))
2. B→A : fACP, A, *sSB*(fACP, A, *e*K(M))
3. A→B : fNRO, B, K, *sSA*(fNRO, B, K)
4. B→A : fNRR, A, *sSB*(fNRR, A, K)

비밀키를 사용한 공정한 부인봉쇄 프로토콜의 구성은 아래의 그림 1과 같다.

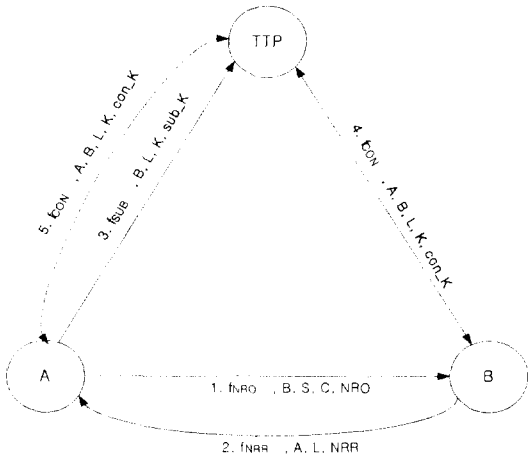


그림 1. 공정한 부인봉쇄 프로토콜

공정성을 위한 프로토콜 수행과정을 다음과 같다.

1. A→B : fNRO, B, L, C, NRO
2. B→A : fNRR, A, L, NRR
3. A→TTP : fSUB, B, L, K, *sub*_K
4. B→TTP : fCON, A, B, L, K, *con*_K
5. A→TTP : fCON, A, B, L, K, *con*_K

NRO : *SSA*(fNRO, B, L, C)
NRR : *SSB*(fNRR, A, L, C)
*sub*_K : *SSA*(fSUB, B, L, K)
*con*_K : *SST*(fCON, A, B, L, K)

3.3 K. Kim, S. Park, J. Baek의 기법

KPB기법 [6]에서는 J.Zhou와 D. Gollmann기법 [1]이 B가 A로부터 받은 암호문을 지워버려 A가 D로부터 키 확인 인증서를 받은 경우에도 B는 암호문을 복호화 할 길이 없는 경우를 방지하기 위하여 키 확인 인증서에 시간 제한 (time limit) T1(<T)를 두어 해결하였다. 이 프로토콜은 아래와 같다.

NRO : S(fNRO||B||L||T||C,*SA*)
NRR : S(fNRR||A||L||T||T1||C,*SB*)
*sub*_K : S(fSUB||B||L||T||K,*SA*)
*con*_K : S(fNRO||A||B||L||T||T0||K,*ST*)

1. A→B : fNRO, B, L, T, C, NRO
2. B→A : fNRR, A, L, T1, NRO
3. A→TTP : fSUB, B, L, T, K, *sub*_K
4. B↔TTP : fCON, A, B, L, T0, K, *con*_K
5. A↔TTP : fCON, A, B, L, T0, K, *con*_K

또한 ZG기법이 A와 B가 주고받는 메시지들에 대한 비밀성을 보장하지 못하는 단점을 보완한 기법을 제시하였다.

Ⅳ. TTP 기능 확장을 통한 부인봉쇄 메커니즘

4.1 기본 용어

본 논문에서 사용된 주요 기호의 의미는 다음과 같다.

-X||Y : 두 메시지 X와 Y의 연결
-*e*K(X) : 키 K를 이용하여 암호화한 메시지 X
-*d*K(X) : 키 K를 이용하여 복호화한 메시지 X
-*s*K(X) : 개인키 K를 이용한 메시지 X의 디지털 서명
-SA, PA : 주체 A의 개인키와 공개키
-M : A가 B로 보내거나, B가 A로 보내는 메시지
-MA : TTP가 A, B에게 보내는 경고 (Alert) 메시지
-C : 메시지 M의 암호문
C = eK(M)
-fNRO : NRO를 나타내는 플래그 정보
-fNRR : NRR를 나타내는 플래그 정보
-fNRS : NRS를 나타내는 플래그 정보
-fNRD : NRD를 나타내는 플래그 정보
-TC : 메시지가 보내진 시간 (Time Check)
-TS : 타임 스탬프 (Time Stamp)
-TTP : 제 3의 신뢰기관

4.2 TTP(Trusted Third Party)의 기능확장

본 논문에서는 부인봉쇄 서비스의 효율성을 개선시키기 위한 방법으로 부인봉쇄 메커니즘이 의존하고 있는 제 3의 신뢰기관인 TTP (Trusted Third Party) 의 기능을 확장하여 TTP의 의존도를 줄이는 프로토콜을 제안한다.

TTP를 사용자나 신뢰기관이 요구할 수 있는 로컬 보안정책에 따라 기존의 신뢰기관 (Trusted Third Party) 을 3 Level로 분류하여 TTP에 대해 차별화 된 기능을 부여한다. TTP의 기능이 확장되고 차별화됨에 따라 TTP를 이용하는 사용자나 신뢰기관은 보안 정책에 알맞은 TTP의 역할을 결정할 수 있다. 이로 인하여 TTP의 개입을 최소로 줄여줄 수 있어 현재 TTP에 대한 높은 의존률을 개선할 수 있다. TTP에 적용되는 Level은 High-Trust Level, Common-Trust Level, Low-Trust Level로 구분한다.

메시지 전달과정에서의 재전송 공격 방지(replay attack) [5]를 위해 타임 스탬프(Time Stamp, TS) [6]을 적용하였고, Common Level부터는 메시지의 전달시간을 확인하여 경고 메시지를 보내기 위해 Time Check (TC) 을 도입하여 메시지의 전달시간을 확인할 수 있다. 또한, 메시지의 신뢰성 보장을 위하여 Low-Trust Level에서는 원문을 암호화하여 전송하였다.

첫째, High-Trust Level에서는 통신망이나 상대방에 대한 보안을 신뢰할 수 있어 송. 수신 쌍방 간에 어떠한 Non-repudiation 증거자료들의 확인 과정 없이 단순히 메시지들을 전달해주는 기능을 하며, 필요시에만 TTP에 보관되고 있는 Non-repudiation의 증거자료들을 송. 수신자에게 전달하는 기능을 부여한다. 사설망의 경우 자체적인 프로토콜을 사용하는 경우가 많으므로, 통신망이나 상대방에 대한 외부의 보안에도 강한 장점이 있다. 따라서, 이러한 사설망의 경우에 High Trust Level을 적용할 수 있다.

이 과정에서 전달되어지는 메시지들은 다음과 같다.

1. A→B, TTP : fNRO, B, TTP, M, TS, NRO
2. B→A, TTP : fNRR, A, TTP, M, TS, NRR
NRO : *s*SA(fNRO||B||TTP||M||TS)
NRR : *s*SB(fNRR||A||TTP||M||TS)

A는 자신의 요구사항을 위 1번 메시지와 같이 생성하여 B와 TTP에게 동시에 전달한다. 전달되는 메시지 중에서 NRO는 A의 개인키로 서명되어 있기 때문에 B는 A를 인증 할 수 있다. A의 메시지를 받은 B는 A에게 응답에 대한 회신을 2번 메시지와 같이 생성하여 A와 TTP에게 보낸다. 이때, 전송되는 메시지 중에서 NRR은 B의 개인키로 서명되어 있기 때문에, A는 B를 인증을 할 수 있다.

둘째, Common-Trust Level에서는 High-Trust 환경에서보다는 덜 안전한 통신망이나 상대방에 대한 신뢰에서 적용된다. Common-Trust Level은 근거리 통신망 (LAN), 지역 통신망 (MAN), 광역 통신망 (WAN)에서 적용될 수 있으며, 일반 Internet 통신 환경에서도 TTP에서 Time Check와 Alert 기능으로

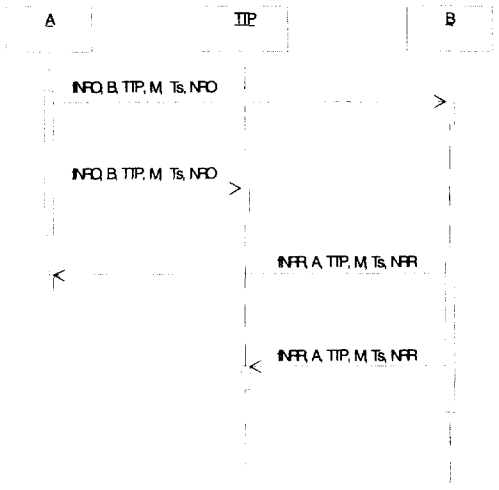


그림 2. High-Trust Level TTP의 동작

보안사항을 점검할 수 있기 때문에 적용할 수 있다. 이 경우에도 High-Trust Level에서와 마찬가지로 송. 수신 쌍방 간에 어떠한 Non-repudiation 증거자료 없이 메시지를 전달하지만, network delay를 고려한 message 전달시간을 측정하여 기대치 이상의 지연시간이 발생할 경우에 각각의 이용자들에게 경고 메시지를 보내고 각 이용자들이 요구하는 Non-repudiation 증거자료를 보내주는 기능을 한다.

만약, 메시지가 기대 이상의 지연시간이 발생할 경우 전달되어지는 메시지들은 다음과 같다.

1. A→B, TTP : fNRO, B, TTP, M, TC1, TS, NRO
2. B→A, TTP : fNRR, A, TTP, M, TC2, TC3, TS, NRR
3. TTP : Time Check
4. TTP→A, B : MA

NRO : *s*SA(fNRO||B||TTP||M||TC1||TS)
NRR : *s*SB(fNRO||A||TTP||M||TC2|| TC3||TS)

A는 High-Trust Level의 메시지에 자신이 메시지를 전송한 시간 TC1을 첨가하여 B와 TTP에게 메시지를 전송한다. B는 A의 메시지를 받고, A의 메시지를 전송 받은 시간 TC2와 자신이 응답메시지를 전송한 시간 TC3을 첨가한 메시지를 A와 TTP에게 전송한다. TTP에서는 TC1, TC2와 TC3의 정보를 비교하여 이상이 발견되거나, B의 메시지를 전달받지 못하였을 때 A와 B에게 경고메시지 MA를 전달한다.

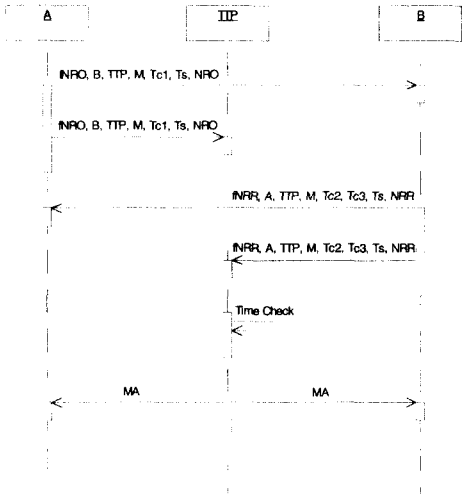


그림 3. Common-Trust Level TTP의 동작

셋째, Low-Trust Level에서는 통신망이나 상대방에 대해 신뢰할 수 없는 환경에서 적용된다. 이는 Internet 통신환경에서 적용되어질 수 있으나 보안이 많이 요구될 경우에 사용되어지며, 일반적인 Internet 통신은 Common-Trust Level로 대체할 수 있다. 여기서의 TTP는 철저히 부인봉쇄 기능을 수행하게 되며 각각의 이용자들에게 Non-repudiation 증거자료들을 전달하고 전달된 Non-repudiation 증거자료에 의해 행동하도록 유도한다.

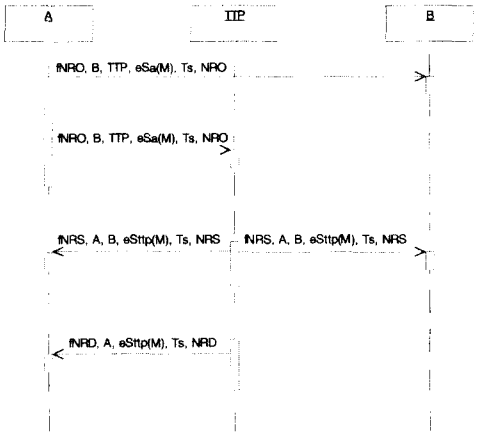


그림 4. Low-Trust Level TTP에서 Origin 동작

A가 보낸 메시지가 B에 전송되어 확인되어지기까지의 과정은 다음과 같다.

1. A→B, TTP : fNRO, B, TTP, *e*SA(M), TS, NRO
2. TTP→A, B : fNRS, A, B, *e*STTP(M), TS, NRS
3. TTP→A : fNRD, A, *e*STTP(M), TS, NRD

NRO : *s*SA(fNRO||B||TTP||*e*SA(M)||TS)
NRS : *s*STTP(fNRS||A||B||*e*STTP(M)||TS)
NRD : *s*STTP(fNRD||A||B||*e*STTP(M)||TS)

이 NRS를 전송함으로서 A가 제출한 메시지가 TTP에게 전달되었다는 증거를 제시할 수 있고, B는 전달받은 NRS를 TTP의 공개키로 복호화하여 A가 보낸 메시지와 비교한 후 A가 보낸 메시지가 정당한지를 확인할 수 있다[11]. TTP가 NRS 메시지를 전달한 후 A에게 NRD를 전송하여 A의 메시지가 B에게 전송되었다는 증거를 제시한다.

4. B→A, TTP : fNRR, A, TTP, *e*SB(M), TS, NRR
5. TTP→A, B : fNRS, A, B, *e*STTP(M), TS, NRS
6. TTP→B : fNRD, B, *e*STTP(M), TS, NRD

NRR : *s*SB(fNRR||A||TTP||*e*SB(M)||TS)

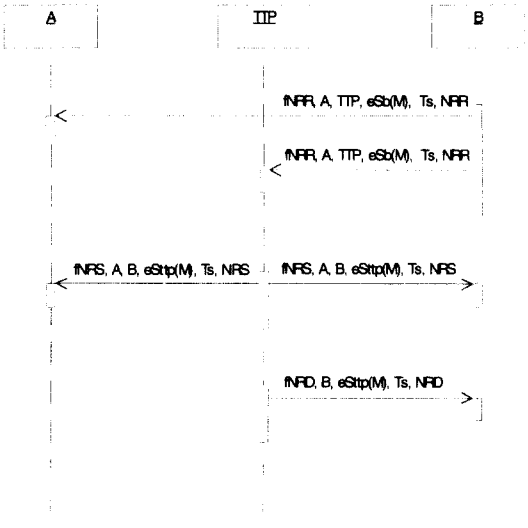


그림 5. Low-Trust Level TTP에서 Receipt 동작

4.2 공정성 (Fairness) 제공

공정성 문제는 부인봉쇄 메커니즘의 프로토콜을 수행하는 도중 임의의 단계에서 프로토콜이 중단되는 경우 프로토콜 참여자의 정보획득 양이 동등해야하며 어느 한쪽도 유리하지 않아야 한다는 점이다.

본 논문에서는 TTP의 기능에 Time Check기능을 추가하였다. 따라서, 송수신자는 중간에 프로토콜이 중단되더라도, TTP에 의한 경고 메시지 (MA) 를 송수신자가 동등하게 전송 받기 때문에 송신 메시지나 수신 메시지를 폐기할 수 있다. 또한 제 3자의 부정한 행위로 참여자의 공정성이 침해되었을 경우도 TTP에서 Time Check 기능에 의해 인지되므로 제 3자의 부정에 대한 신뢰성을 높였다.

만약, 수신자 B가 T2시간을 조작하였을 경우를 가정해 볼 수 있다. 곧, B가 T2시간을 실제 받은 시간보다 빨리 받은 것처럼 조작할 경우 TTP에서는 공정한 Time Check기능을 수행할 수 없게 된다. 이를 방지하기 위하여 송신자 A는 메시지는 송신하고 나서 수신자 B로부터 NRR을 수신할 때까지의 유효한 시간 T를 설정한다. 따라서, 송신자 A는 B로부터 받은 NRR 수신 시간이 유효 시간 T보다 크거나, 메시지를 수신 받지 못할 경우 자신이 보낸 메시지를 폐기할 수 있다.

1. A→B : fNRO, B, TTP, M, TC1, TS, NRO **IF** sended **THEN**
2. B→A : fNRR, A, TTP, M, TC2, TC3, TS, NRR **IF** sended **THEN**
3. A : Time Check **IF** T<NRR도착시간 **THEN** discard NRO **ELSE**
4. A : *d*PB(NRR)

B는 A가 보낸 메시지에 대한 응답 메시지를 A에게 보내주게 되는데 이때 적용되는 부인봉쇄 서비스 메커니즘은 위의 과정을 역행하면 된다.

V. 시뮬레이션 결과

그림 6은 TTP의 각 Level별 메시지의 전달시간을 비교한 시뮬레이션 결과이다. 서버와 통신을 하는 가입자가 증가할 때, 메시지의 전송지연시간을 측정한 것이다.

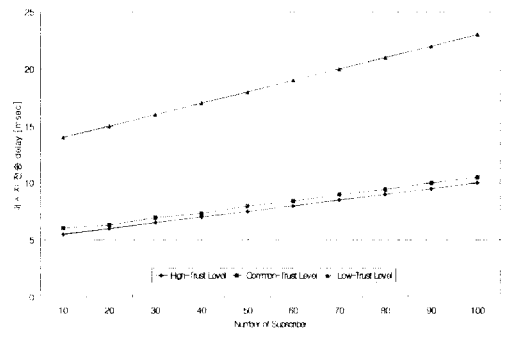


그림 6. 각 Level별 메시지 전송 지연시간 비교

그림에서 알 수 있듯이 High-Trust Level 환경에서의 메시지 전송지연시간이 가장 낮게 나왔고, Low-Trust Level에서의 메시지 전송지연이 훨씬 높은 것으로 나왔다.

Common-Trust Level에서의 통신은 network delay를 고려한 message 전달시간을 측정하여 기대치 이상의 지연시간이 발생할 경우에 각각의 이용자들에게 경고 메시지를 보내고 각 이용자들이 요구하는 Non-repudiation 증거자료를 보내주기 때문에 High-Trust Level의 통신속도보다 많은 지연시간을 가지고 있다. Low-Trust Level에서는 부인봉쇄 서비스가 전적으로 TTP에게 의존하기 때문에 다른 두 Level에서의 속도와 비교했을 경우 크게 차이가 남을 알 수 있다.

Telecom Non-Repudiation Inter-ORB Protocol (TeNoRIOP) [13]에서는 단일 ORB 도메인이나 ORB 도메인들 사이에서의 부인봉쇄 서비스 제공을 위한 메커니즘을 제시하여 주고 있다. 인증, 기밀성, 무결성과 같은 여러 보안 기능들은 **CORBA/SSL3 Security [14]에서 제시되어있기 때문에, TeNoRIOP에서는 부인봉쇄 메커니즘을 주요하게 다루었다. 이 문서에 의하면, 송신자나 수신자가 부인봉쇄 증거자료를 요구하고 이 증거자료를 받는데 소요되는 시간은 보통 1분 이내이며, network delay를 고려하였을 경우 2분을 threshold 값으로 정하고 있다. 이는 본 논문에서 제안하는 Time Check 기능의 수행과 같은 맥락을 취하고 있으며, 본 논문에서는 평균 메시지 전달시간보다 2배 이상의 delay가 발생하였을 경우를 threshold값이 초과하는 경우로 하였다. 예를 들어, 가입자가 10명일 경우 시뮬레이션 결과 평균 메시지 전송 지연시간은 5.5 msec 로 측정되었으며, 11 msec를 threshold값으로 정하였다.

결과에서 알 수 있듯이 TTP의 개입이 클수록 부인봉쇄 서비스의 효율성은 감소함을 알 수 있다. 따라서 이러한 문제점들은 본 논문에서 제시한 바와 같이 자신의 환경에 알맞는 TTP의 Level을 선택하여 해결할 수 있다.

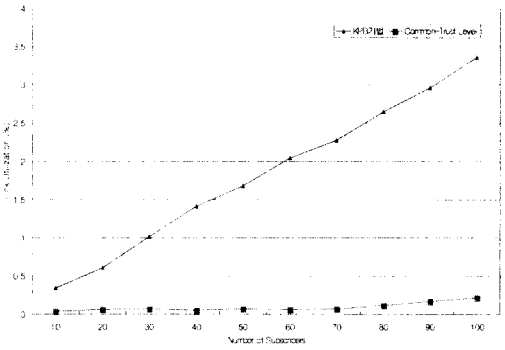


그림 7. KPB기법과 Common-Trust Level의 Link Utilization 비교

그림 7은 KPB기법과 Common-Trust Level에서의 Server와 TTP간의 Link Utilization을 비교한 시뮬레이션 결과이다. 가입자의 10%가 전송 중 기준치 이상의 전송지연이 발생할 경우를 고려한 결과이다.

결과에서 알 수 있듯이 KPB기법은 Server와 TTP간, Client와 TTP간에 항상 부인봉쇄 서비스를 위하여 TTP가 개입하게 된다. 그러나 제안한 Common-Trust Level에서는 TTP의 개입을 최소화하기 위하여 TTP는 송.수신자간의 메시지 전송시간을 검사하여 이상이 발생할 경우에만 송.수신자에게 경고 메시지를 보내주는 역할을 하기 때문에 그만큼 TTP의 개입이 줄어들게 된다. 따라서 결과에서 알 수 있듯이 Server와 TTP간의 Link Utilization을 비교해 보면 제안한 프로토콜의 효율성이 더 좋음을 알 수 있다.

Ⅵ. 결과 및 향후 연구과제

정보통신과 컴퓨터기술의 발전으로 인하여 전자상거래, 인터넷 통신, 전자우편 등과 같은 분야에서 보안 기술의 중요성이 날로 중요시되고 있다. 그러나 안전한 통신과 정보교환을 위해서는 사용자 인증, 메시지 암호화, 부인봉쇄 서비스 등과 같은 기반구조가 갖추어져야 한다. 그러나 기존의 부인봉쇄 메커니즘이 가지고 있는 보완해야할 문제점들로는 선택적 수신 (selecrive receipt), 공정성 (fairness)

의 제공, 효율성의 개선, 사용자 시스템의 내장애성, 다른 기반구조와의 통합 운용성, 이종의 환경에서도 상호 호환 운영될 수 있게 해주는 문제들이 남아있다. 본 논문에서 제시한 TTP의 기능을 확장하는 프로토콜의 사용으로 제 3의 신뢰기관의 개입을 줄일 수 있어 부인봉쇄 서비스에서의 효율성을 개선할 수 있고, 동시에 공정성도 보장이 된다.

향후, 제시된 TTP 프로토콜 구현을 위한 구체적인 메시지 다이제스트 구현 [7]과 TTP의 신뢰성을 높일 수 있는 TTP의 인증에 관한 연구를 고려해야 할 것이다.

참 고 문 헌

[1] J. Zhou and D. Gollmann, "Observations on Non-repudiation" .Proc. of ASIACRYPT '96, LNCS 1163, Springer-Verlag, pp. 133-144, Springer-Verlag, 1996

[2] J. Zhou and D. Gollmann. "A fair non-repudiation protocol", Proc. of 1996 IEEE Symposium on Security and Privacy, pp. 55-61, May 6-8, 1996

[3] ISO/IEC 13888-1:1997(E) Information techn ology-Security techniques-Non-repudiation Par t 1:General

[4] ISO/IEC 13888-1:1997(E) Information tech nology-Security technique s-Non-repudiation Part 2:Mechani sms using symmetric techni-ques

[5] ISO/IEC 13888-1:1997(E) Informa tion technology-Security techniques-Non-repudiatio n Part 3:Mechani sms using asymmetric techniques

[6] Kwangjo Kim, Sangjoon Park, Joonsang Baek, "Improving fairness and privacy of Zhou-Gollman's Non-repudiation Protocol", IEEE International Workshop on Security, Aizu, Sep.23-24, 1999

[7] J. Zhou, Non-repudiation, Ph.D Thesis, University of London, December 1996.

[8] N.Asokan, Fairness in Electronic Commerce, Ph.D thesis, University of Waterloo, 1998

[9] J. Zhou, R. Deng, F. Bao, "Some Remarks on a Fair Exchange Protocol", PKC2000, Jan. 2000

[10] S. William, "Network security essentials: applications and standards", Prentice Hall, 1999

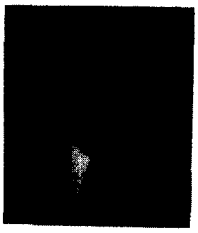
[11] A.. Salomaa, "Public-Key Cryptography". New York : Springer- Verlag, 1996

[12] M. Seo, B. Lee, J. Baek, K. Kim, S. Kim, K. Lee, On the Standard Mechanism for Non-repudiation Service , CISC99, Vol.9, No.1, pp.228-240, 1999

[13] Telecommunications Industry Forum, Telecom Non-Repudiation Inter-ORB Protocol, TCIF-99-008, Guideline, June, 1999

[14] Object Management Group, OMG Document orbos/97-02-04, Secure Socket Layer / CORBA Security, adopted June 24, 1997

박 상 준(Sang Jun Park) 학생회원

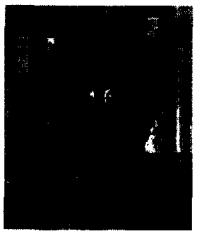


2000년 : 경희대학교 전자공학과 졸업(학사)

2000년~현재 : 경희대학교 전자공학과 석사과정

<주관심 분야> 네트워크 보안, 무선인터넷 보안

홍 충 선(Choong Seon Hong) 정회원



1983년 : 경희대학교 전자공학과 졸업 (학사)

1985년 : 경희대학교 전자공학과 (공학석사)

1997년 : Keio University, Department of Information and Computer Science (공학박사)

1988년~1999년 : 한국통신 통신망 연구소 선임연구원/ 네트워킹연구실장

1999년~현재 : 경희대학교 전자정보학부 조교수

<주관심 분야> 인터넷 서비스 및 망 관리 구조, 분산 컴포넌트관리, IP 프로토콜, 멀티미디어 스트리밍 등

이 대 영(Dae Young Lee) 정회원

1964년 : 서울대 물리학과 졸업 (학사)
1971년 : 캘리포니아 주립대학원 컴퓨터학과 (공학석사)
1979년 : 연세대학교 전자공학과 (공학박사)
1971년~현재 : 경희대학교 전자정보학부 교수
1990년~1993년 : 경희대학교 산업정보대학원 대학원장
1999년~2000년 : 한국통신학회 회장
<주관심 분야> 영상처리, 컴퓨터 네트워크, 컴퓨터 시스템