通信情報保護學會誌
第6卷 第1號, 1996. 3

컴퓨터 네트워크 시스템에서의 부인-봉쇄 서비스+

Non-Repudiation Service in Computer Network System

이 선 우*, 김 봉 한*, 이 재 광 *

요 약

ISO 7498-2 정보보호 구조에서는 컴퓨터 네트워크 구조에서의 안전성 문제를 해결하기 위하여 5가지의 기본적인 정보보호 서비스로 인증, 액세스 제어, 무결성, 기밀성, 부인-봉쇄를 정의하였다. 이 가운데 부인-봉쇄는 이미 발생한 통신 사실을 부인할 수 없도록 송수신자간의 통신 사실을 증명해 주는 서비스이다. 이 서비스에 대해 ISO/IEC JTC1/SC27에서는 현재 일반 모델에 대해서는 CD 13888-1로 대칭 암호화 알고리즘 이용에 대해서는 CD 13888-2로 규정 중에 있다. 본 고에서는 부인-봉쇄에 대한 개념을 살펴보고, 부인-봉쇄 메커니즘을 중심으로 부인-봉쇄 서비스에 대하여 고찰하였다.

1. 서 론

고도의 정보화 사회를 구축하기 위한 노력은 컴퓨터 보급의 확산과 정보통신 기술의 발전에 따라 계속 변화되어가고 있다. 정보통신 기술 분야가 일반화되어감에 따라 컴퓨터에서 생성, 저장, 관리되는 정보 자원과 통신망을 통하여 전송되는 정보 자원에 대한 보호는 그 중요성이 점점 더해가고 있다.

이러한 안전성 문제를 해결하기 위해 ISO/IEC JTC1/SC21에서는 OSI 정보보호 구조(ISO DIS 7898-2)를 발표하였는데, 대부분의 안전성 서비스를 OSI 응용계층, 표현계층 그리고 트랜스포트 계층에서 제공되도록 하였다. OSI 정보보호 구조에서 정의된 5가지 기본 정보보호 서비스에는 신분확인(Identification / Authentication) 서비스, 액세스 제어(Access Control) 서비스, 3) 데이터 무결성(Data Integrity) 서비스, 데이터 기밀성(Data Confidentiality) 서비스, 부인-봉쇄(Non-Repudiation) 서비스 등이 있다. 따라서 본 고에서는 이러한 안전성 서비스 가운데 이미 발생한 통신 사실을 부인할 수 없도록 하기 위해 발신자나 수신자의 통신 사실을 증명해주는 부인-봉쇄 서비스에 대하여 ISO/IEC CD 13888-1(General Model)과 ISO/IEC CD 13888-2(Using symmetric encipherment algorithms)를 중심으로 기술하였다.

* 한남대학교 공과대학 전자계산공학과
+ 본 연구는 1995년도 한남대학교 학술연구조성비 지원에 의하여 연구되었음

2. 부인-봉쇄 서비스의 기본 개념

컴퓨터 네트워크 시스템을 통하여 양 당사자간에 이루어진 통신 사실을 부인할 수 없도록 하는 것을 부인-봉쇄라고 하며, 이를 위해 제공되는 부인-봉쇄 서비스는 통신 당사자간에 메시지를 제출, 전송, 배달된 후 제 삼자에게 그 메시지의 제출, 전송, 수신한 사실에 대한 부인할 수 없는 증명을 제공한다. 이에 대한 실례를 살펴보면 은행에서 오퍼레이터가 계좌의 말소에 따른 잔금들을 임의의 통장으로 빼돌린 사건을 들 수 있는데, 이러한 문제가 발생했을 때 이러한 조작을 한 오퍼레이터를 찾아내고, 또한 그 사실을 부인할 수 없도록 하는 서비스를 제공하지 못한다면 큰 문제가 아닐 수 없다. 그리고 은행을 통한 대금의 송수신시 송신자가 거짓으로 보내지도 않은 금액을 보냈다고 한다거나, 수신자가 대금을 수신하고 그 사실을 부인하거나 또는 수신한 대금을 줄여서 원래의 금액만큼 받지 못했다고 송신자에게 주장할 수 있다. 이러한 경우에 발생할 수 있는 부당한 사실을 막기 위해 제공되어야 한다. 따라서 이를 위해서는 반박할 수 없는 증거를 입증하기 위하여 증거를 사용가능하도록 만들고, 수집하고 유지 관리해야 한다.

부인-봉쇄 서비스는 비단 은행을 포함한 모든 금융과 관련된 거래뿐만 아니라 군사적인 목적이나 전자문서교환(EDI)을 포함한 그 밖의 여러 가지 응용 통신 환경에서도 그 필요성과 중요성이 점점 커지고 있다. 따라서 컴퓨터 네트워크 시스템에서 이루어지는 정보통신 환경에서 부인-봉쇄 서비스는 앞으로 필수적인 요소가 될 것으로 기대된다.

부인(Repudiation)의 위협으로 부터 보호하기 위해서 제공되는 부인-봉쇄 서비스에서는 다음과 같은 4가지의 서비스가 제공된다. 이 서비스에 대해 발신처, 의뢰증명, 배달증명에 대한 부인-봉쇄는 그림 1과 같이 나타낼 수 있고, 수신처, 의뢰증명, 배달증명에 대한 부인-봉쇄는 그림 2와 같이 나타낼 수 있다.

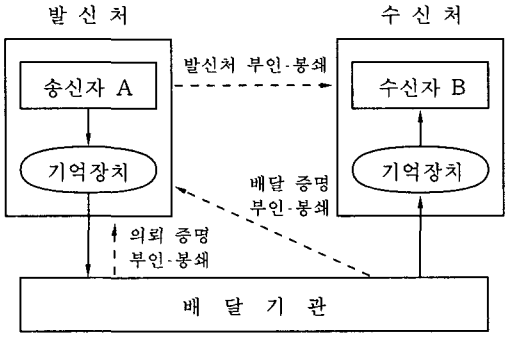

그림 1. 발신처, 의뢰증명, 배달증명 부인-봉쇄

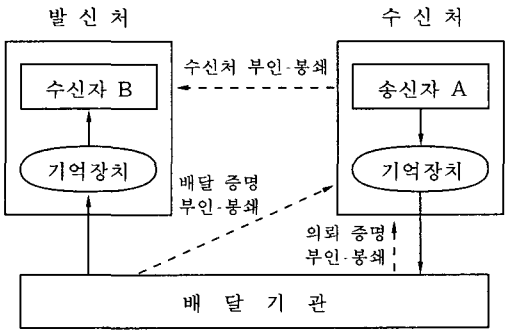

그림 2. 수신처, 의뢰증명, 배달증명 부인-봉쇄

1) 발신처 부인-봉쇄 (Non-repudiation of origin): 발신처 부인-봉쇄 서비스는 메시지나 메시지 내용을 송신한 송신자의 거짓 부인을 막기 위한 서비스.

2) 수신처 부인-봉쇄 (Non-repudiation of delivery): 수신처 부인-봉쇄 서비스는 메시지나 메시지 내용을 수신한 수신자의 거짓 부인을 막기 위한 서비스.

3) 의뢰증명 부인-봉쇄 (Non-repudiation of

submission): 의뢰증명 부인-봉쇄 서비스는 배달요구를 받은 메시지를 가진 배달기관의 거짓 부인을 막기 위한 서비스.

4) 배달증명 부인-봉쇄 (Non-repudiation of transport): 배달증명 부인-봉쇄 서비스는 배달된 메시지가 의도하는 수신자의 메시지 기억장소안에 들어 있는 배달기관의 거짓부인을 막기 위한 서비스.

3. 부인-봉쇄 서비스와 TTP 역할

믿을 수 있는 제 3자로서의 TTP(Trusted Third Party)는 사용된 메커니즘이나 효과적인 부인-봉쇄 정책에 의해 부인-봉쇄 안에 포함된다. 대칭 암호화 기법에서는 항상 온-라인 또는 인-라인 TTP가 요구되는 인증서를 생성하고 확인하는데 사용된다. 그리고 효과적인 부인-봉쇄 정책은 TTP에 의해서 부분적으로 또는 전체적으로 생성되는 증거가 요구된다. 부인-봉쇄 정책에서는 배달 기관(Delivery authority)에 의해 제공되는 의뢰증명 부인봉쇄(non-repudiation of submission)나 배달증명 부인봉쇄(non-repudiation of transport)가 요구된다. 또 보안시간 참조는 믿을 수 있는 타임 스탬프(time stamp) 발행기관에 의해 제공되는 것이 요구된다. 공증은 개체나 통신된 데이터의 특성을 증명하기 위해서 포함된다. 부인-봉쇄 서비스 제공에 있어서 TTP는 다음의 역할(부인-봉쇄 단계별)을 수행한다.

1) 증거 생성(Evidence Generation) 단계

증거는 TTP와 함께 협력해서 부인-봉쇄 초기자에 의해서나 초기자 단독에 의해서 TTP에 의해 제공되는 정보이다. 이 단계에서 TTP가 수행하는 기관(Authority)으로서의 역할은 다음과 같다.

① 증거 확인 기관 : 부인-봉쇄 초기자를 단독으로 대신하여 TTP가 생성하는 증거(발신과 배달 부인-봉쇄)로서 증명과 토큰의 온-라인 생성은 항상 증거 제공에 사용되는 대칭 암호화 기법이 요구된다.

② 인-라인 증거 생성 기관 : TTP가 생성하는 증거(발신과 배달 부인봉쇄)는 단독 또는 초기자와 협력하여 이루어진다. 배달기관(Delivery authority)으로써 증거는 의뢰와 배달 부인-봉쇄를 제공한다.

③ 오프-라인 증명서 발급 기관 : TTP는 부인-봉쇄를 위해 사용되는 공개키 쌍이 진짜인 것을 보증하기 위해 부인-봉쇄 초기자와 관계된 오프-라인 공개키 증명서를 제공한다.

④ 토큰 생성 기관 : TTP는 초기자 또는 하나 또는 그 이상에 신뢰 기관에 의해 제공되는 하나 또는 그 이상에 증명된 부인-봉쇄 토큰의 형태를 구성한다.

⑤ 타임 스탬프 발급 기관 : TTP는 문서의 작성시간 또는 증거 발생 시간과 같은 사건 또는 사실의 시간을 포함한 증거를 제공한다.

⑥ 공증 기관: TTP는 데이터의 무결성, 발신처, 목적지와 시간/날짜, 같은 둘 또는 그 이상의 엔티티간에 교환된 데이터 속성에 관한 보증을 제공하기 위해 정보를 교환한 개체들과 4자가 신뢰한다.

⑦ 디지털 서명 생성 기관: TTP는 발신자나 수령인 또는 수신 기관이든 부인-봉쇄 초기자의 요청으로 디지털 서명을 생성한다.

이상의 증거 생성 단계에서의 TTP가 수행하는 역할은 그림 3과 같다.

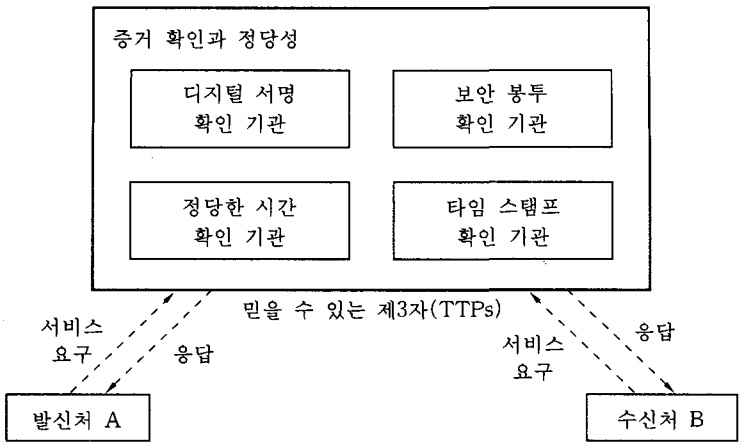

그림 3. 증거 생성 단계에서의 TTP 의 역할

2) 증거 전달, 저장과 검색(Evidence Transfer, Storage, and Retrieval) 단계

이 단계에서 증거는 당사자간이나 저장 장치로부터 또는 저장장치로 전송된다. 실제적으로 이 단계의 수행과정은 부인-봉쇄 서비스의 모든 경우에 항상 발생하지 않고 부인-봉쇄 정책에 따라 수행된다. 당사자간의 증거 전달은 부인-봉쇄 프로토콜에 의해 이루어지는데, 이 단계에서는 다음의 두 가지 과정이 TTP에 의해 수행될 수 도 있다.

① 부인-봉쇄 정책에 의해 요구된다면 TTP는 단지 수신 기관의 역할에서만 필요하다. 의뢰증명이나 배달증명 부인-봉쇄는 온-라인 배달 기관에 의해 제공되고 발신처 또는 수신처 부인-봉쇄는 인-라인 배달 기관에 의해 제공된다.

② 증거 기록 보관 기관: TTP는 증거 사용자 또는 판결관이 후에 검색할 수 있는 증거를 기록한다.

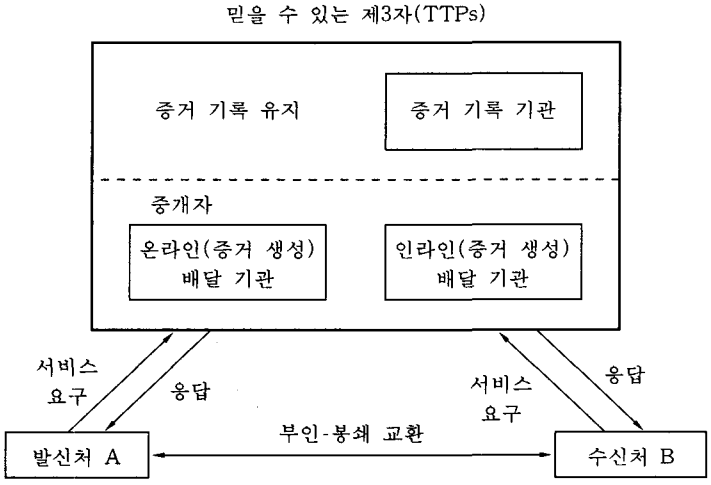

그림 4. 증거 전송, 저장과 검색 단계에서의 TTP 역할

3) 증거 확인(Evidence Verification) 단계

증거 확인 기관으로서 TTP는 부인-봉쇄 토큰에서 제공되는 부인-봉쇄의 유형을 확인하기 위해 증거 사용자가 신뢰하는 온-라인 기관으로서의 역할을 한다. 대칭 암호화 기술을 이용하여 생성된 증거인 경우는 TTP에 의해 확인만 할 수 있고, 그 밖의 경우에는 TTP의 역할은 선택사항이다. 이때는 부인-봉쇄 증명서는 사용된 기술에 따라 확인되는데, 보안 봉투는 TTP에 의해서만 확인되고, 디지털 서명과 사용된 공개키 증명서, 안전한 시간/날짜 스탬프, 그리고 증명서에 들어있는 증명서의 타당한 시간이다. 부가적인 부인-봉쇄 증명서는 공증에 의해 제공된다.

4) 분쟁 해결(Dispute Resolution) 단계

이 단계에서 증거 기록 기관은 판결관이나 분쟁 당사자의 요청에 따라 부인-봉쇄 정보를 이용할 수 있도록 온-라인 TTP의 역할을 한다. 부가적으로 TTP는 판결관이나 분쟁 당사

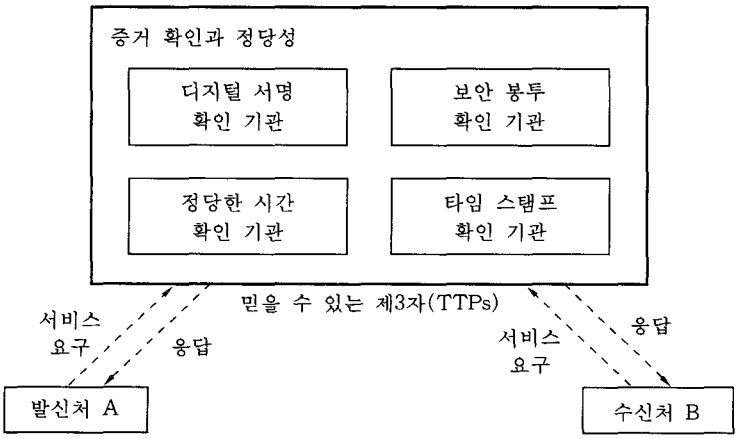

그림 5. 증거 확인 단계에서의 TTP 역할

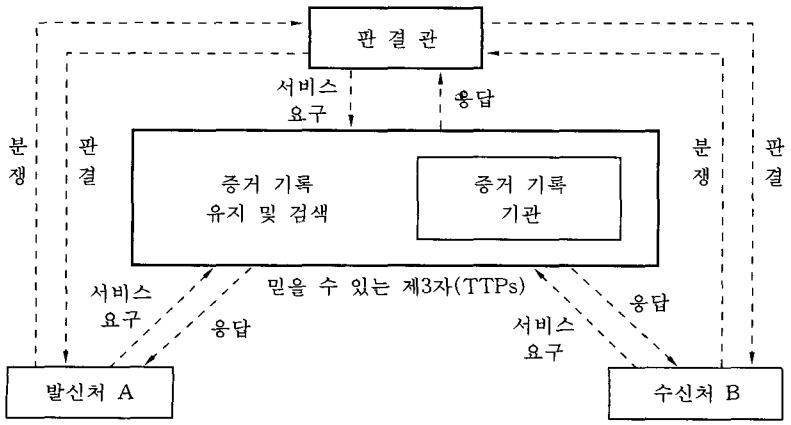

그림 6. 분쟁 해결 단계에서의 TTP 역할

자의 요구에 따라 부인-봉쇄 정보를 재 검색하기 위해 증거 확인 단계에서 수행된 기능을 수행할 수 도 있다.

4. 증거 생성과 확인 메커니즘

증거는 대칭 암호화 기법을 이용한 보안 봉투(SENV: Secure Envelopes)나 비대칭 암호화 기법을 이용한 디지털 서명(SIG: Digital Signature)으로 나타내는 부인-봉쇄 증명서에 의해 제공된다. 증명서-기반 서명을 이용하면 부인-봉쇄 증명서는 디지털 서명과 이에 사용되는 공개키 증명서로 구성된다. 일반적인 부인-봉쇄 증명서는 다음과 같다.

$$\mathrm{CERT}() = \begin{matrix}\mathrm{SENVS}\\ \mathrm{IG}\end{matrix}()$$

1) 보안 봉투

보안 봉투는 데이터 송신자를 인증하고, 데이터 수신한 수신자를 알아내기 위해 사용되는데 일반적으로 보안 봉투는 반박할 수 없는 증거의 한 부분이 되기 위해서 이것은 TTP만 알고있는 비밀키를 사용하여 TTP에 의해서 생성된다. 암호화를 이용하여 생성된 보안 봉투 SENV는 데이터를 비밀키 a로 암호화하여 생성한다. 메시지 y로 구성된 데이터는 비밀 파라메터를 이용하지 않고 y로부터 유도된 잉여 값인 RED와 연결된다. 이 RED는 MDC(Manipulation Dectection Code)일 수 도 있다. 이는 다음과 같이 나타낼 수 있다.

$$SENV_a(y) = {}_eK_a\ (y||RED)$$

또 보안 봉투 SENV는 비밀키 x를 이용하여 y로부터 유도된 잉여 값인 RED와 연결된 메시지 y로 구성된다. 이는 다음과 같이 나타낼 수 있다.

$$SENV_x(y) = y||RED_x(y)$$

보안 봉투를 대칭 암호화 알고리즘을 적용한 경우를 살펴보면, x1, x2, x3…, xm을 엔티티간에 전송되는 데이터 필드의 집합이라 하자. 이때 보안 봉투는 두 엔티티가 공유하는 비밀키 k를 이용하여 입력 데이터 x1, x2, x3, …,xm은 새로운 데이터인 y1, y2, y3, …, ym으로 변환할 수 있다. 이는 다음과 같이 나타낼 수 있다.

$$\mathrm{SENV}_k : \{x_1, x_2, x_3, \cdots, x_m\} \rightarrow \{y_1, y_2, y_3, \cdots, y_m\}$$

이때 $\{y_1, y_2, y_3, \cdots, y_m\}$과 비밀키 k가 주어지면 보안 봉투의 수령인은 $\{x_1, x_2, x_3, \cdots, x_m\}$을 알수 있고, 데이터의 인증성을 확인한다. 그리고 암호화를 이용한 보안 봉투는 기밀성과 무결성도 제공한다. 즉, $\mathrm{SENV}_K(y) = E_K(yr)$에서 yr은 데이터 필드 y에 추가된 필드 r인데, 이를 암호화 알고리즘 E와 암호화 키 k를 이용하여 보안 봉투를 생성한다. 이를 엔티티 A와 엔티티 B간에 송수신이 이루어진다면 엔티티 A는 보안 봉투 $\mathrm{SENV}_a(y) = E_a(yr)$를 TTP에게 보낸다. TTP는 보안 봉투를 비밀키 a를 이용하여 복호화하여 A로부터 온 것임을 확인하고 데이터 필드 y와 추가된 필드를 알아낸다. 그러면 TTP는 보안 봉투의 송신자가 A임을 보증하고 따라서, A는 비밀키 a를 알고 있는 유일한 엔티터가 된다. 마찬가지로 TTP와 엔티티 B는 비밀키 b를 이용하여 보안 봉투로 서로 통신이 가능하다.

2) 디지털 서명

디지털 서명 SIG는 서명자만 알고 있는 비

밀 키 s를 이용하여 메시지 y나 메시지의 해쉬코드 H(y)에 디지털 서명 알고리즘 S를 적용하여 생성된다. 이는 다음과 같이 나타낼 수 있다.

$$SIG = S_s(y)$$

디지털 서명이 반박할 수 없는 증거의 한 부분이 되기 위해서 서명은 증명서 발급 기관(CA: Certification authority)에 의해 발행된 공개키 증명서와 연관이 있어야 한다.

3) 확인 메커니즘

부인-봉쇄 증명서(CERT)의 확인 결과(pon: positive or negative)는 확인 알고리즘 V와 확인키 v를 적용하게 된다. 이는 다음과 같이 나타낼 수 있다.

$$V_v(CERT) = pon$$

보안 봉투는 보안-봉투 생성에 사용된 비밀키를 가지고 있는 TTP에 의해서만 확인된다. 디지털 서명은 서명자와 디지털 서명의 공개키 증명서를 발행한 TTP의 공개키를 가지고 있는 엔티티에 의해서만 확인된다.

5. 부인-봉쇄 토큰과 부인-봉쇄 메커니즘

5.1 부인-봉쇄 토큰

부인-봉쇄 토큰은 부인-봉쇄 교환에서 송신자 A로부터 수신자 B에게 전송되는 데이터 필드로서 토큰의 구성은 하나 또는 그 이상의 부인-봉쇄 증명서(CERT)와 키 식별자나 메시지 식별자와 같은 반드시 인증하지 않아도 되는 부가적인 정보가 들어있는 텍스트 필드로 구성된다. 일반적인 부인-봉쇄 토큰(NRT)은 다음과 같이 정의할 수 있다.

$$NRT = text||CERT(z)$$

여기서,

$$\mathrm{CERT}(z) = \frac{\mathrm{SENVS}}{\mathrm{IG}}(z)\text{이고}$$

$$z = f||A||B||T||H(m)\text{이다.}$$

데이터 필드 z는 부인-봉쇄 유형을 나타내는 플래그 f, 부인-봉쇄 교환의 초기자 A를 구분하는 식별자, 증거 수신자 B를 구분하는 식별자, 안전한 시간 참조값 T, 전달되는 메시지나 메시지 그 자체의 메시지 m의 해쉬코드 H(m), 그리고 선택적으로 배달 기관 D의 식별자로 구성된다. 토큰은 부인-봉쇄 교환의 초기자나 초기자의 요구에 따라 토큰 생성 기관에 의해 생성된다.

① 발신처 토큰 부인-봉쇄(NRO)

발신처 토큰 부인-봉쇄(NRO)는 발신자 또는 발신자의 요구에 따라 TTP에 의해 다음과 같이 생성된다.

$$NRO = text1||CERT(z1),$$
$$z1 = f1||A||B||T1||H(m)$$

NRO 토큰에서 필요한 부인-봉쇄 정보 Z1은 최소한 다음의 데이터 요소로 구성된다. f1 : 부인-봉쇄 증명서가 발신처 부인-봉쇄임을 가리키는 플래그, A : 송신자를 구분하는 식별자, B : 발신자를 구분하는 식별자, T1 : 데이터를 보낸 날짜와 시간, H(m) : 보낸 데이터나 데이터 자체의 해쉬코드이다.

② 수신처 토큰 부인-봉쇄

수신처(delivery) 토큰 부인-봉쇄(NRD)는 수령인(recipient) 또는 수령인의 요구에 따라 TPP에 의해 생성된다.

$$NRD = text2||CERT(z2),$$
$$z2 = f2||A||B||T2||H(m)$$

NRD 토큰에서 필요한 부인-봉쇄 정보 z2는 최소한 다음의 데이터 요소로 구성된다. f2 : 부인-봉쇄 증명서가 수신처(delivery) 부인-봉쇄임을 가리키는 플래그, A : 수신자를 구분하는 식별자, B : 발신자를 구분하는 식별자, T2 : 데이터를 보낸 날짜와 시간, H(m) : 보낸 데이터나 데이터 그 자체의 해쉬코드이다.

③ 의뢰증명 토큰의 부인봉쇄

의뢰증명 토큰 부인봉쇄(NRS)는 발신자의 요구에 따라 배달 기관에 의해 생성된다.

$$NRS = text3||CERT(z3),$$
$$z3 = f3||A||B||D||T3||H(m)$$

의뢰증명 토큰의 부인-봉쇄 정보 z3은 최소한 다음의 데이터 요소로 구성된다. f3 : 부인-봉쇄 증명서가 의뢰 증명임을 가리키는 플래그, A : 송신자를 구분하는 식별자, B : 수신자를 구분하는 식별자, D : 배달 기관 식별자, T3 : 데이터의 전송을 의뢰한 날짜와 시간, H(m) : 의뢰된 데이터나 데이터 자체의 해쉬코드이다.

④ 배달증명 토큰의 부인-봉쇄

배달증명 토큰 부인-봉쇄(NRT)는 발신자 요구에 따라 배달기관(delivery authority)에 의해 생성된다.

$$NRT = text4||CERT(z4),$$
$$z4 = f4||A||B||D||T4||H(m)$$

NRT 토큰에 필요한 부인봉쇄 정보 z4는 최소한 다음의 데이터 요소로 구성된다. f4 : 부인-봉쇄 증명서가 전송 부인-봉쇄임을 가리키는 플래그, A : 송신자를 구분하는 식별자, B : 수신자를 구분하는 식별자, D : 배달 기관 식별자, T4 : 배달 기관에 의해 데이터가 수신인에게 배달된 날짜와 시간, H(m) : 배달된 데이터나 데이터 그 자체의 해쉬코드이다.

5.2 부인-봉쇄 메커니즘

엔티티 A와 B간의 부인-봉쇄 교환에서의 발신처, 수신처, 의뢰증명, 배달전송의 부인-봉쇄 메커니즘은 다음과 같다.

① 발신처 부인-봉쇄 메커니즘

- 엔티티 A(발신자)에서 엔티티 B(수신인)로의 트랜젝션.
  a. 엔티티 A는 NRO 토큰을 생성한다.
  b. 엔티티 A는 직접 또는 배달 기관에 의해 NRO 토큰을 B에게 보낸다.
  c. 엔티티 B는 A로 부터 온 NRO 토큰을 확인하고, 만약 NRO 토큰이 타당하면, NRO 토큰을 증거로써 저장한다.

② 수신처 부인-봉쇄를 위한 메커니즘

- 엔티티 B에서 엔티티 A로의 트랜젝션
  a. 엔티티 B는 NRD 토큰을 생성한다.
  b. 엔티티 B는 직접 또는 배달 기관에 의해 NRD 토큰을 A에게 보낸다.

c. 엔티티 A는 엔티티 B로부터 온 NRD 토큰을 확인하여, NRD 토큰이 타당하면 이것을 증거로써 저장한다.

③ 전송의뢰 부인-봉쇄 메커니즘
- 배달 기관에서 엔티티 A로의 트랜젝션
  a. 배달 기관은 NRS 토큰을 생성한다.
  b. 배달 기관은 A에게 NRS 토큰을 보낸다.
  c. 엔티티 A는 배달 기관으로부터 온 NRS 토큰을 확인한다.
  만약, NRS 토큰이 타당하면 이것을 증거로써 저장한다.

④ 배달증명 부인-봉쇄 메커니즘
- 배달 기관에서 엔티티 A로의 트랜젝션
  a. 배달 기관은 NRT 토큰을 생성한다.
  b. 배달 기관은 A에게 NRT 토큰을 송신한다.
  c. 엔티티 A는 배달 기관으로부터 온 NRT 토큰을 확인한다.
  만약, NRT 토큰이 타당하면 이것을 증거로써 저장한다.

5.3 온-라인 TTP를 이용한 부인-봉쇄 메커니즘

TTP는 공증인(notary)으로서 서명 생성 서비스를 수행하는데, 서명은 기록에 대한 무결성과 기밀성을 관리하기 위해 위탁하고, 분쟁을 해결하는데 사용된다. 온-라인 TTP를 이용한 부인-봉쇄 메커니즘에 이용되는 데이터 필드의 구성은 다음과 같다. z는 플래그 f1과 발신인 식별자, 수령인 식별자, 메시지에 해쉬함수 h를 적용해서 얻어진 결과의 연결로서 f1 ‖ originator id ‖ Recipient id ‖ h(message)가 된다. 그리고 z': 플래그 f2와 발신인 식별자, 수령인 식별자, 메시지에 해쉬함수 h를 적용한 결과의 연결로서 f2 ‖ originator id ‖ Recipient id ‖ h(message)가 된다.

TTP는 부인-봉쇄를 위해 토큰 생성하는데, 메시지로 지정된 데이터에 비밀키를 이용하여 TTP에 의해 만들어진 보안 봉투이다. 발신처 증명 토큰(POO: Proof of Origin)은 보안 봉투를 기반으로 POO = [key id] ‖ [msg id] ‖ SENVx(z')이다. 여기서 key id는 보안 봉투를 생성하는데 사용된 키의 식별자이고, msg id는 메시지 식별자로서 수신자가 메시지를 식별할 수 있는 유일한 데이터 스트림이다. 또 수신처 증명 토큰(POR: Proof of Receipt)은 [key id] ‖ [msg id] ‖ SENVx(z')이다. TTP가 생성한 토큰은 TTP에 의해 인증되어야 하는데, 먼저 key id를 이용하여 비밀키 x를 알아낸 다음 이를 이용하여 토큰을 재계산한 후에 데이터 필드(z나 z')를 이용하여 표현된 토큰이 대응되면 인증된다. 따라서 TTP에 의해 발행된 모든 토큰은 토큰 표로 저장하는데, TTP는 생성된 각 토큰에 대하여 key id와 데이터 필드(z나 z')를 연관하여 기록한다. 그리고 난 다음 인증을 위해서 토큰 표의 인덱스를 이용한다. 온-라인 TTP를 이용한 부인-봉쇄 메커니즘은 다음과 같이 세 가지로 구분할 수 있다.

① 부인-봉쇄 메커니즘(M1): 필수 POO, 선택사항 POR(그림 7)
발신지 엔티티 A는 TTP에게 $SENV_a(z)$를 보내서 POO 토큰을 요구한다. 그러면 TTP는 보안 봉투가 엔티티 A로부터 온 것임을 검사하여 맞으면 POO 토큰을 계산하여 $SENV_a(POO)$를 되돌려 보낸다. 엔티티 A는 $SENV_a(POO)$가 TTP로부터 온 것임을 검사한 다음 m||z||POO를 엔티티 B에게 보낸다. 엔티티 B는 z에 들어있는 h(m)값을 검사하고 $SENV_b(POO)$를 생성하며, A로부터 수신된 POO 토큰 확인하기 위해 TTP에게

송신한다. TTP는 $SENV_b$(POO)가 B로부터 온 것인지를 검사하고 POO 토큰의 인증성을 검사한다. SENV와 POO가 타당하면, TTP는 POR 토큰을 생성하고 PON이 양수인 $SENV_b$(PON||POO||POR)를 보내고, 타당치 않으면, PON이 음수인 $SENV_b$(PON||POO||POR)를 B에게 보낸다. 엔티티 B는 $SENV_b$(PON||POO||POR)이 TTP로부터 온 것인지 검사하여 타당하고 검증이 양수이면 발신처 증명이 확립된다. 그러면 POO 토큰은 발신처 증명을 위해 보관한다. 그리고 나서 엔티티 B는 A에게 POR 토큰을 보낸다.

엔티티 A는 TTP에게 POR을 보내서 POR 검증을 요구한다. TTP는 POR 토큰의 인증성을 검사하고, TTP는 $SENV_a$(PON||POO||POR)를 생성하여 A에게 보낸다. 엔티티 A는 SENV가 TTP로부터 온 것임을 검사하고 검증이 양이면 수신처 증명이 확립된다. 그러면 POR 토큰은 나중에 수신처 증명을 위해 저장한다.

② 부인-봉쇄 메커니즘 2(M2): 필수 POO, 필수 POR(그림 8)

발신자 엔티티 A는 TTP에게 $SENV_a$(z)를 보내서 POO 토큰 요구한다. 그러면 TTP는 보안 봉투가 엔티티 A로부터 온 것임을 검사하여 맞으면 POO 토큰을 계산하여 $SENV_a$(POO)를 되돌려 보낸다. 엔티티 A는 $SENV_a$(POO)가 TTP로부터 온 것임을 검사한 다음 m||z||POO를 엔티티 B에게 보낸다.

엔티티 B는 z에 들어있는 h(m)값을 검사하고 $SENV_b$(POO)를 생성하며, A로부터 수신된 POO 토큰을 확인하기 위해 TTP에게 송신한다. TTP는 $SENV_b$(POO)가 B로부터 온 것인지를 검사하고 POO 토큰의 인증성을 검사한다. SENV와 POO가 타당하면, TTP는 POR 토큰을 생성하고 PON이 양수인 $SENV_b$(PON||POO||POR)를, 타당치 않으면, PON이 음수인 $SENV_b$(PON||POO||POR)를 B에게 보낸다. 엔티티 B는 $SENV_b$(PON||POO||POR)이 TTP로부터 온 것인지 검사하여 타당하고 검증이 양수

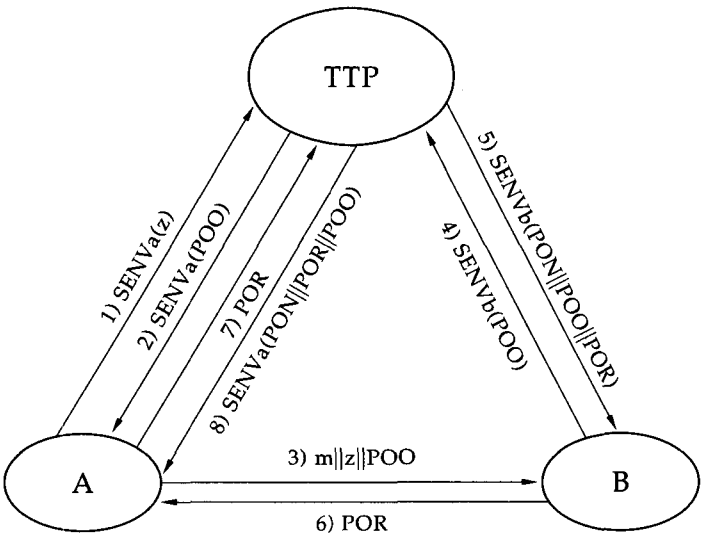

그림 7. 부인-봉쇄 메커니즘(M1): 필수 POO, 선택사항 POR

이면 발신처가 증명이 확립된다. 그러면 POO 토큰은 발신처 증명을 위해 보관한다. 앞서 TTP가 POR 토큰을 B에게 보낸 다음 TTP는 즉시 A에게 $SENV_a(POR)$를 보낸다. 엔티티 A는 $SENV_a(POR)$가 TTP로부터 온 것임을 확인하여 검증이 양이면 수신처가 증명이 확립된다. 그러면 POR 토큰은 나중에 수신처 증명을 위해 저장한다.

③ 부인-봉쇄 메커니즘 3(M3) : 중재인 TTP를 이용한 POO와 POR 필수(그림 9)
이 메커니즘은 TTP가 발신자와 수신자간에

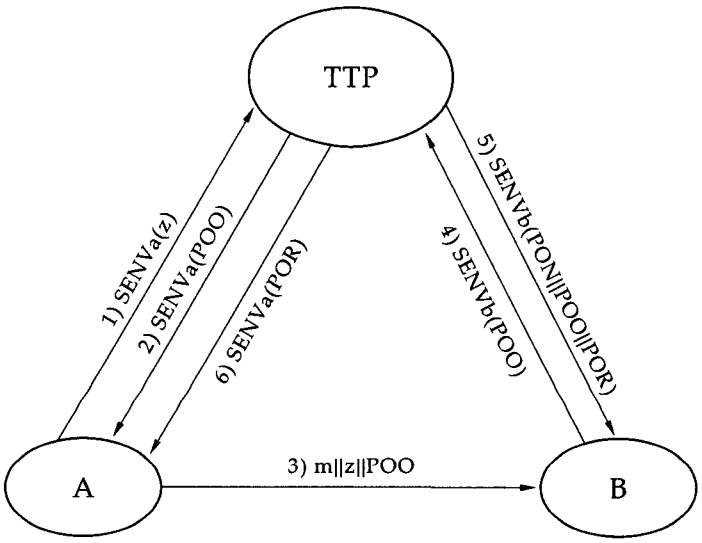

그림 8. 부인-봉쇄 메커니즘 2(M2): 필수 POO, 필수 POR

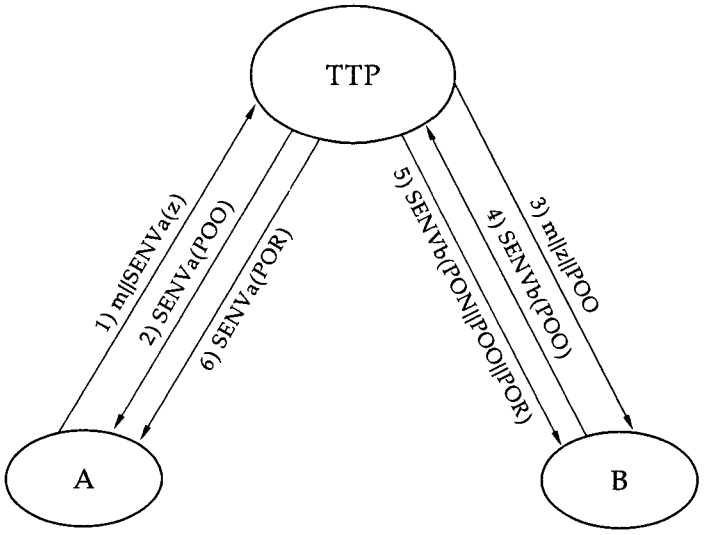

그림 9. 부인-봉쇄 메커니즘 3(M3) : 중재인 TTP를 이용한 POO와 POR 필수

중재인 역할을 하므로 양 당사자간에 직접적인 대화는 없다. 엔티티 A는 TTP에게 메시지 m과 $SENV_a(z)$를 보내고, TTP는 A에게 $SENV_a(POO)$를 보낸다. 그리고 나면 TTP는 B에게 z, m과 POO 토큰을 보낸다. 그 다음 B는 POO 토큰을 보안 봉투로 받지 못하면 TTP를 이용하여 확인하기 위해서 TTP에게 h(m)와$SENV_b(POO)$를 보낸다. TTP는 $SENV_b(POO)$가 B로 부터 온 것임을 확인하고, POO 토큰의 인증성을 확인하여 SENV와 POO가 타당하면, POR 토큰을 생성하여 B에게 $SENV_b(PON||POO||POR)$를 보냄으로서 PON 양수를 응답한다. 그렇지만 SENV가 타당하지만, POO 토큰이 타당하지 않으면 PON이 음수 검증이라는 것을 B에게 $SENV_b(PON||POO)$으로 보낸다. B는 SENV가 TTP로부터 온 것임을 검사하고, 확인되면 검증은 양수가 되고 POR이 이루어진다. 그러면 POO 토큰은 발신처 증명을 위해 저장한다.

TTP는 앞에서 B에게 POR 토큰을 보낸 후에 A에게 $SENV_a(POR)$를 보낸다. 그러면 A는 $SENV_a(POR)$을 확인하고 수신처 증명이 확립된다. POR 토큰은 수신처 증명을 위해 저장한다. 여기서 발신처나 수신처의 증명(재검증)은TTP가 이용한 키의 표와 TTP가 발행한 토큰 표를 사용하여 POO와 POR 토큰을 재검증 할 수 있다.

6. 결 론

컴퓨터 네트워크를 이용한 정보통신이 일반화되면서 중요 정보 자원의 불법적인 유출이나 권한을 가지지 않은 자의 불법적인 액세스, 그리고 불법적인 사용자에 의한 내용과 순서 변경 등과 같은 안전성이 중요한 문제로 대두되고 있다. 이러한 안전성 문제는 컴퓨터 네트워크를 이용한 통신 응용 및 서비스 등에서 이미 이루어진 통신 사실에 대해 거짓 부인을 봉쇄하기 위한 부인-봉쇄 서비스는 매우 중요한 서비스 중에 하나이다.

본 연구에서는 ISO/IEC JTC1/SC21에서 정의한 부인-봉쇄 서비스를 제공하기 위한 메커니즘을 ISO/IEC CD 13888-1과 ISO/IEC CD 13888-2를 중심으로 하여 살펴보았다. 송신자와 수신자, 배달 기관의 의뢰증명과 배달 증명을 위해서는 보안 봉투와 토큰, 그리고 신뢰할 수 있는 제3자를 이용, 부인-봉쇄 메커니즘을 적용하면 필요한 부인-봉쇄 서비스를 제공할 수 있다. 이러한 부인-봉쇄 메커니즘을 실제 통신 응용 서비스에 적용하는 것이 앞으로의 연구 과제가 될 것이다.

참 고 문 헌

1. 임채호, 정진욱, "OSI 시큐리티 연구 동향", 정보 통신 기술, pp.89-102, vol.4, no. 1, Jun. 1990.

2. 아주대학교, "OSI 통신망 구조에서의 네트워크 안전체제 연구", 과기처 최종 연구 보고서, May. 1989.

3. 한국 과학 기술원 시스템 공학 센터, "컴퓨터 망에서의 데이터 암호화 기법 적용에 관한 연구", Mar. 1988.

4. 차경돈, 김동규, "OSI 환경에서 부인봉쇄 서비스에 관한 연구", 한국정보과학회, Vol.18, No.1, 1991.

5. "OSI 상위계층에서의 안전성 프레임워크에 관한 연구", 한국 전자통신 연구소 최종보고서, 아주대, 1992.12.

6. Branstad, D. K., "Considerations for security in the OSI architecture", IEEE Network Magazine, 1987.

7. ISO 7498 Information Processing System-Open Systems Interconnection-Basic Reference Model.

8. ISO 7498-2 Information Processing System-Open Systems Interconnection-Security Architecture.

9. Pfleeger, C. P., "Security in Computing , Prentice Hall, 1989.

10. "Information technology - Security technique - Non-repudiation Part1 : General Mode" ISO / IEC CD 13888-1.

11. "Non-repudiation - Part2 : Using symmetric encipherment algorithms", ISO / IEC CD 13888-2.

□ 著者紹介

이 선 우

1995년 2월 한남대학교 전자계산공학과 졸업(학사)
1995년 2월~현재 한남대학교 대학원 전자계산공학과 석사과정

김 봉 한

1994년 2월 청주대학교 전자계산공학과 졸업(학사)
1994년 2월 ~ 현재 한남대학교 대학원 전자계산공학과 석사과정

이 재 광

1984년 광운대학교 전자계산학과 졸업(이학사)
1986년 광운대학교 대학원 전자계산학과 졸업(이학석사)
1993년 광운대학교 대학원 전자계산학과 졸업(이학박사)
1986년 ~ 1993년 군산전문대학 전자계산과 교수
1993년 ~ 현재 한남대학교 전자계산공학과 조교수

※ 관심분야 : 컴퓨터 네트워크, 정보통신 정보보호