대칭키 전자서명을 위한 Kailar책임 로직 (Accountability Logic)의 확장 및 전자지불 프로토콜의 책임분석

김 영 달† · 한 선 영††

요 약

전자 상거래를 위한 비대칭 키 전자서명 기법의 정보통신 프로토콜에서 거래 당사자들간에 전송된 메시지에 대한 책임 소재 증명의 분석을 위해 제안된 Kailar Accountability Logic을, 대칭키 암호화 기법의 전자 서명을 사용하는 프로토콜에 적용하기 위해 일부의 구성 요소를 변경 및 추가하여 확장하였다. 이 확장된 로직을 적용하여 대칭키 전자서명 기법을 사용하는 소액 상거래용 전자 지불 프로토콜을 분석해 봄으로써, 프로토콜의 책임 소재 증명 능력에 대한 프로토콜의 약점을 파악하고, 이를 보완하기 위한 프로토콜의 변경 사항을 제시함으로써 확장된 로직의 효용성을 설명하였다.

Extention of Kailar Accountability Logic for Symmetric Key Digital Signature and Accountability Analysis of an Electronic Payment Protocol

Young-Dal Kim† · Sun-Young Han††

ABSTRACT

Kailar Accountability Logic proposed for the accountability analysis of communication protocols that require accountability and use asymmetric key digital signature is extended for protocols that use symmetric key digital signature. A proposed electronic micropayment protocol that uses symmetric key digital signature is analyzed to illustrate the use of the extended logic in detecting its lack of accountability and suggesting changes to enhance its accountability.

1. 서 론

지금까지 사용해 온 메시지 전송 프로토콜의 분석 방법은 메시지를 주고 받는 당사자간에 세션의 보안을 위해 공유하는 세션키의 신선도(Freshness), 메시지의 기밀성, 및 메시지의 발신지 증명(Message Origin Authentication)등과 같은 메시지 자체의 특성에 주안점을 두고 있었다. 이러한 메시지 전송 프로토콜의 특성들을 분석하기 위해서 가장 보편적으로 사용된 방법은 BAN Logic[1]이다. 그러나 전자상거래의 발전과 함께 암호화 기법을 이용한 프로토콜들이 전자 상거래를 구현하는데 이용되게 됨으로써 거래 참여자들의 메시지에 대한 책임, 즉 참여자와 메시지간의 연관관계를 증명할 수 있는 분석 방법이 필요하게 되었다.

이러한 책임 소재를 분석하기 위한 방법으로는 Kailar

† 정 회 원 : 건국대학교 대학원 컴퓨터정보통신공학과
†† 정 회 원 : 건국대학교 컴퓨터정보통신공학과 교수
논문접수 : 1999년 7월 28일, 심사완료 : 1999년 9월 29일

Accountability Logic(KA 로직)[2]이 제안되어 있다. 이 방법에서는 지금까지의 분석 방법들과는 달리, 책임소재에 관련된 중요한 속성들을 분석할 수 있는 수단을 제공하고 있다. 그러나 이 로직은 비대칭키 전자서명을 가정하고 있기 때문에, 소액 상거래용 전자 지불 프로토콜과 같이 전산처리의 효율성 때문에, 비대칭키 암호화 기법보다는 대칭키 암호화 기법을 많이 사용하고 있는 프로토콜의 책임 소재 분석을 위해서는 적절한 분석 수단이 되지 못하고 있다. 이를 위해 본 논문에서는 대칭키 전자 서명에 관련된 특성을 KA 로직에 반영하여 변경 및 추가 요소를 정의함으로써 KA 로직을 확장하였으며, 이 확장된 로직을 이용하여 저자가 제안한, 대칭키 전자 서명을 이용하는 소액 상거래용 전자 지불 프로토콜을 분석해 봄으로써 확장된 KA 로직의 책임 소재 증명 능력을 검증하고자 한다.

2. 제안된 프로토콜의 분석을 위해 사용하는 Kailar Accountability Logic (KA 로직)[2]의 요소

2.1 분석 틀(Analysis Framework)

KA 로직에서는, 메시지 전송 프로토콜에서 메시지에 대한 책임이 있는 거래 당사자를 증명할 수 있는 능력에 대해 분석한다. 분석하고자 하는 시스템은 거래 당사자라고 불리는 일단의 사용자들로 구성되는데, 이 당사자들은 거래를 위해 서로간에 메시지를 주고받는다. 당사자들은 A, B, …로 표시한다. 서명이 된 메시지는 서명을 한 당사자가 거절할 수 없는 확실한 진술(Statement)로서의 역할을 한다. 각각의 메시지가 의미하는 사실은 메시지의 해석으로써, 프로토콜의 설계자가 정의하는 것으로 가정한다. 거래 당사자가 메시지를 통해 전하고자 하는 진술은 x, y, …로 표시한다. KA 로직에 정의된 기본 구문(Constructs) 중에서, 본 논문에서 사용하는 구문들은 다음과 같다.

- 강한 증명 : "A **CanProve** x"
  A가 임의의 당사자 B에게 어떠한 비밀, y(x와는 다른 진술임)도 밝히지 않고 일련의 작업을 거친 후에 확신을 줄 수 있다면, 당사자 A는 x를 증명할 수 있다는 것을 의미한다.
- 서명 인증 : "K **Authenticates** A"
  이 구문은, 비대칭 암호화 기법의 공개키 K를 당사자 A의 서명을 인증하는데 사용할 수 있다는 사실과 당사자 A는 비밀키 K^{-1}를 이용하여 암호화된 어떠한 x와도 연결되어 있음을 보이기 위해 사용할 수 있다는 것을 나타낸다.
- 메시지의 해석 : "x in m"
  진술 x는 메시지 m내의 일부 또는 전체에 대한 해석임을 의미한다. 이 해석은 프로토콜에 따라 달라지기 때문에 프로토콜의 설계자가 명시적으로 정의할 것으로 기대한다. 암호화된 메시지와 평문이 서명이 된 메시지의 일부로 함께 존재하지 않을 경우 복호화된 메시지는 해석으로 사용될 수 없다
- 진술 : "A **Says** x"
  당사자 A는 x를 말했다는 것과 x가 의미하는 모든 것에 대해 책임을 진다는 것을 의미한다.

2.2 분석을 위한 가정

KA 로직에서 제안하는 분석 틀을 사용하여 도출된 프로토콜의 약점은 프로토콜의 설계에 관련된 것이기 때문에 어떤 가정을 필요로 하지는 않는다. 즉 이 약점들은 가정들이 사실이든 아니든 여전히 약점으로 남는다. 그러나 이 분석 방법을 사용하여 도출한 책임의 증명은 다음의 가정들이 사실이라는 전제에 기반을 두고 있기 때문에 프로토콜을 운영하는 과정에서, 가정하였던 속성들에 대한 지원이 부족한 경우, 분석의 결과로 얻어진 책임에 대한 결론은 유효하지 않을 수도 있다. KA 로직에서 정의 된 가정들 중에 본 논문에서 사용하는 것들은 다음과 같다.

- 비대칭키 암호화 기법을 사용한 전자서명 알고리즘 :
  전자서명 알고리즘은 서명과 서명을 한 당사자를 아무런 이의 없이 연관 시킬 수 있을 정도로 안전한 것으로 가정한다. 또한 이 알고리즘은 충분히 오랜 동안 타인에 의해 파괴될 수 없는 것으로 가정한다. 전자서명은 메시지의 발신지 증명, 메시지 내용의 무결성 및 메시지 송신자에 의한 거부 불가성을 제공하는 것으로 가정한다.
- 신뢰 :
  어떠한 암호화 기법을 사용하든, 당사자들은 자신들의 비밀키(대칭키 암호화 기법에서 당사자간에 공유하는 키나, 비대칭키 암호화 기법에서의 비밀키를 의미함)에 대한 보안에 책임이 있기 때문에, 책임지지 않을 다른 당사자들과 이 비밀키를 공유하지 않을 것이라는 신뢰를 가정한다.

2.3 기본 명제(Postulates)

KA 로직에서 정의한 기본 명제 중에서, 본 논문에서 사용하는 것들은 다음과 같다. 이 명제들은 일반적인 속성들과 전자 상거래 프로토콜에서 메시지의 책임에 관련된 속성들로 구분된다.

2.3.1 증명가능성에 관한 일반적인 속성

이 기본 명제들의 표기 방법은 다음의 형식을 이용한다.

$$\frac{P\ ;\ Q}{R}$$

즉 이것은, P와 Q가 사실이라면, R은 사실이다라는 것을 의미한다. ";"는 결합을 의미하며, 시간상의 순서를 의미하지는 않는다.

- 결합(Conjunction)

이 기본 명제는 증명들의 결합을 정의한다:

$$\textbf{Conj:}\ \frac{A\ \textbf{CanProve}\ x\ ;\ A\ \textbf{CanProve}\ y}{A\ \textbf{CanProve}\ (x \wedge y)}$$

즉, 만약에 A가 x가 유효함을 증명할 수 있고, y가 유효함을 증명할 수 있다면, A는 x와 y의 조합인 $(x \wedge y)$가 유효함을 증명할 수 있다.

- 추론(Inference)

이 기본 명제는 증명 가능성과 추론을 연관시키는데 사용한다.

$$\textbf{Inf:}\ \frac{A\ \textbf{CanProve}\ x\ ;\ x \rightarrow y}{A\ \textbf{CanProve}\ y}$$

즉, 당사자 A가 x가 유효함을 증명할 수 있고, 또 x는 y를 함축하고 있다면, 당사자 A는 y가 유효함을 증명할 수 있다.

2.3.2 전자 상거래 메시지의 책임에 관련된 속성들

아래의 기본 명제들은 전자 서명을 사용하는 시스템의 속성들을 요약하고 있으며, 또 특정 진술을 하는 당사자들에 대한 신뢰와 증명 가능성에 관련된 속성들을 서로 연관시킨다.

- 비대칭키 암호화 기법을 사용한 전자 서명의 책임 속성 : 전자 서명이 된 메시지는, 메시지에 서명을 한 당사자가 그 메시지에 대해 책임이 있다는 것을 나타내는 증거로써 작용한다. 이 책임은, 메시지에 있는 서명과 서명한 당사자간의 연관성을 증명할 수 있는 어느 누구에 의해서도 증명될 수 있다.

$$\frac{A\ \textbf{Receives}\ (m\ \textbf{SignedWith}\ K^{-1});\ x\ \text{in}\ m \quad \textbf{Sign;}\ A\ \textbf{CanProve}\ (K\ \textbf{Authenticates}\ B)}{A\ \textbf{CanProve}\ (B\ \textbf{Says}\ x)}$$

즉, A가 비밀키 K^{-1}로 서명이 된 메시지 m을 받고, m이 x를 포함하고 있다는 조건하에서 A가, 공개키 K는 당사자 B를 인증한다는 것을 증명할 수 있다면, A는 B가 x를 말했다는 것을 증명할 수 있다. 여기서의 암묵적인 가정은, 만약에 메시지가 비밀키 K^{-1}로 서명이 되었다면, A는 K^{-1}를 알지 못해도 메시지가 K^{-1}로 서명이 되었다는 것을 증명할 수 있다는 것이다. 서명을 검증하기 위해서 필요한 유일한 정보인 K는 공개되어 있기 때문에, 이것은 타당한 가정이다.

3. 대칭키 전자 서명을 위해 변경된 Kailar Accountability Logic (KA 로직)의 구성 요소

3.1 변경된 분석 틀

KA 로직은 비대칭키 암호화 기법을 이용한 전자 서명을 가정하고 있다. 그러나 소액 상거래용 전자지불 프로토콜의 경우, 전산처리 비용을 최소화하기 위해 대칭키 암호화 기법을 사용한 전자서명을 많이 사용하므로, 이러한 프로토콜들의 분석을 위해 KA 로직을 아래와 같이 수정 및 확장하여 정의한다.

대칭키 암호화 기법의 전자 서명을 사용하는 경우의 기본적인 가정은 다음과 같다.

1) 상거래의 직접적인 당사자들은 자신들 사이에서 이루어지는 모든 상거래의 중재자에 대해서 절대적인 신뢰를 가지고 있다. 이 가정이 불가능할 경우, 대칭키 암호화 기법의 전자 서명은 사용이 불가능하기 때문에 기본 가정으로 정의한다.
2) 거래 당사자와 중재자간의 메시지나 중재자의 중재가 필요한 메시지의 송신은 중재자가 작성하여 미리 배포한 마스터키를 사용하며, 거래 당사자간의 메시지 송신은 중재자가 작성하여 배포한 세션키를 사용한다.
3) 중재자는 좋은 마스터키와 세션키를 작성할 수 있는 능력이 있다.

- 약한 증명 : "A **CanProve** x with $K_{A,B}$"
  A는 B(거래의 중재자 포함)와 함께 공유하는 키 $K_{A,B}$(마스터키나 세션키)를 공개하지 않고는 x를 증명할 수 없다는 것을 의미한다. KA 로직에서 정의한 "강한 증명"에서는 x외의 다른 어떤 비밀도 공개하지 않은 상태에서 x를 증명할 수 있는 경우로 정의하고 있으나, 대칭키 암호화 기법의 전자 서명을 사용하는 경우에는, 일반 대중에게 공개되지 않은 키를 이용해서만 전자서명의 검증이 가능하기 때문에, 제 3자에게 거래관련 사실을 증명하기 위해서는 거래 당사자들만 공유하던 키를 공개해야 한다.
- 마스터키 서명 인증 :
  "**A**(or S) **IsAuthenticatedUsing** $K_{A,S}$ by S(or A)"
  이 구문은, 중재자 S(또는 당사자 A)는 당사자 A(또는 중재자 S)와 공유하는 키 $K_{A,S}$를 이용하여 당사자 A(또는 중재자 S)의 서명을 인증할 수 있다는 사실과, 키 $K_{A,S}$를 이용하여 암호화된 어떠한 x와도 A(또는 S)가 연결되어 있음을 보이기 위해 사용할 수 있다는 것을 나타낸다. 여기서 $K_{A,S}$는 대칭키 시스템에서 A가 지불 서버와 같은 신뢰를 받는 중재자 S와 공유하는 키로써 마스터키라고 정의한다.
- 세션키 서명 인증 :
  "A(or B) **IsAuthenticatedUsing** $K_{A,B}$ by B(or A) until T"
  이 구문은, 기간 T가 아직 경과하지 않았다면, 거래 당사자 B(또는 A)는 당사자 A(또는 B)와 공유하는 세션키 $K_{A,B}$를 이용하여 당사자 A(또는 B)의 서명을 인증할 수 있다는 사실과, 키 $K_{A,B}$를 이용하여 암호화된 어떠한 x와도 A(또는 B)가 연결되어 있음을 보이기 위해 사용할 수 있다는 것을 나타낸다. 여기서 키 $K_{A,B}$는 중재자 S가 작성하여 A와 B에게 전송한 것으로써 세션키라고 정의하며, T는 거래 당사자나 거래의 중재자가 아닌 제 3자가 $K_{A,B}$를 해독하는데 소요되는 시간보다 충분히 짧은 시간으로써 Timestamp에 의해 정의한 시간이나 Nonce를 이용한 Challenge/Response 프로토콜에서 응답이 돌아오는 시간, 또는 이와 유사한 기능을 이용하여 검증한다고 가정한다. 세션키 $K_{A,B}$는 중재자 S의 직접적인 개입이 없이 사용되므로 유효성이 마스터키보다 나쁠 수 있기 때문에 T를 이용한 유효성의 검증이 필요하다.
- 대칭키로 서명된 메시지의 수령 :
  1) "A **Receives** m **SignedWith** $K_{A,S}$"
     당사자 A는 자신과 신뢰 받고 있는 중재자 S가 공유하는 키 $K_{A,S}$를 이용하여 서명이 된 메시지 m을 받는다. 여기에서 m은 메시지와 관련된 모든 내용(예를 들어, S를 중재자로 하여 A와 거래를 하고자 하는 다른 당사자의 ID)과 서명을 포함한다. 이 경우의 전자 서명은 3.2절에서 설명한 방법을 이용하여 작성된 것으로 가정한다.
  2) "S **Receives** m **SignedWith** $K_{A,S}$"
     중재자 S가 자신과 당사자 A가 공유하는 키 $K_{A,S}$를 이용하여 암호화한 메시지 m을 받으면, 당사자 A가 m에 키 $K_{A,S}$를 이용하여 서명을 하여 보낸 것으로 가정한다는 것을 의미한다.
  3) "A(or B) **Receives** m **SignedWith** $K_{A,B}$"
     당사자 A(또는 B)가 자신과 당사자 B(또는 A)가 공유하는 키 $K_{A,B}$를 이용하여 암호화한 메시지 m을 받으면, 당사자 B(또는A)가 m에 키 $K_{A,B}$를 이용하여 서명을 하여 보낸 것으로 가정한다는 것을 의미한다. 이와 같이 세션키를 사용하는 경우는 중재자가 직접적으로 개입하지 않기 때문에 시간 T를 이용하여 세션키의 유효성을 검증해야 한다.

3.2 추가된 가정

추가된 속성들은 다음과 같다.

- 대칭키 암호화 기법의 전자서명 알고리즘 :
  S는 신뢰를 받고 있는 강력한 중재자이며, 거래 당사자인A와 B 모두와 메시지를 교환할 수 있다. S는 A와 키 $K_{A,S}$를 공유하며, B와는 키 $K_{B,S}$를 공유한다. 이 키들은 프로토콜이 시작하기 전에 S에 의해 작성되어 A와 B에게 전송되었으며, 또 여러 번 사용할 수 있다.
  위에 기술한 가정하에서 대칭키 암호화 기법과 중재자(Arbitrator)를 통한 전자서명은 다음과 같이 작성되는 것으로 가정한다[3].
  1) A는 $K_{A,S}$로 메시지를 암호화하여 S에 보낸다.
  2) S는 이 메시지를 $K_{A,S}$로 복호화한다.
  3) S는 복호화된 메시지와 이 메시지를 A로부터 받았음을 나타내는 추가 메시지를 함께 $K_{B,S}$로 암호화한다.
  4) S는 이 암호화된 메시지를 B에게 보낸다.

5) B는 이 복합 메시지를 $K_{B,S}$로 복호화한다.

이제 B는 A가 보낸 메시지와 S가 이 메시지를 A로부터 받았음을 알려 주는 S의 인증을 판독할 수 있다.

이 방법의 특성은 다음과 같다.

1) 이 서명은 믿을 수 있다.
S는 신뢰할 수 있는 중재자이며 또, 그는 이 메시지를 A가 보냈다는 것을 알고 있기 때문에 S의 인증은 B를 위한 증거가 된다.
2) 이 서명은 위조할 수 없다.
A와 S만 $K_{A,S}$를 알고 있기 때문에 A만 S에게 이 키로 암호화된 메시지를 보낼 수 있다. 다른 사람이 A를 사칭하고자 했다면 S는 이 사실을 앞에서 기술한 알고리즘의 2)단계에서 즉시 확인할수 있었기 때문에 이 메시지가 믿을 수 있다는 것을 인증하지는 않았을 것이다.
3) 이 서명은 재사용할 수 없다. B가 S의 인증을 다른 메시지에 첨부하여 사용했다면, A는 이 서명이 잘못된 것임을 즉시 확인할 수 있다. 이 때 S는 B에게, 평문의 메시지와 A의 암호화된 메시지를 다시 만들어 보도록 요청할 수 있을 것이다. 중재자는 이 평문의 메시지를 $K_{A,S}$로 암호 화하여 B가 준 암호화된 메시지와 비교해 봄으로써 이 두개의 메시지가 서로 다르다는 것을 확인할 수 있다. B는 $K_{A,S}$를 모르기 때문에 S가 제시한 암호문과 일치하는 암호문을 만들 수 없기 때문이다.
4) 서명이 된 문서는 변조할 수 없다.
B가 A의 서명이 첨부된 메시지를 변조하였다면, S는 이 사실을 3)에서 설명한 조치를 이용하여 증명할 수 있다.
5) 문서에 서명한 사실을 거부할 수 없다.
비록 A가 후에 자신이 이 메시지를 보낸 사실을 거부한다고 할지라도, S가 B에게 보낸 인증은 이 것이 사실이 아님을 증명할 수 있다. S는 모든 사람에게 신뢰 받는 기관으로 가정하기 때문에, 그가 말한 진술은 모두 사실이기 때문이다.

이상의 전자서명 기법에서 사용하는 알고리즘은 서명과 서명을 한 당사자를 아무런 이의 없이 연관 시킬 수 있을 정도로 안전하며, 충분히 오랜 동안 타인에 의해 파괴될 수 없는 것으로 가정한다.

위에 설명한 바와 같이 대칭키 암호화 기법의 전자서명도 메시지의 발신지 증명, 메시지 내용의 무결성 및 메시지 송신자에 의한 거부 불가성을 제공하는 것으로 가정한다.

3.3 추가된 기본 명제

KA 로직에서 정의한 표기 방법을 사용하여, 전자상거래 메시지의 책임에 관련된 속성들을 추가한다.

- 대칭키 암호화 기법을 이용한 전자 서명의 책임 속성: 아래의 정의에서 M-Sign(Master Key Signature)은 마스터키를 사용하여 중재자 S가 직접적으로 개입하는 경우에 적용되며, S-Sign(Session Key Signature)는 중재자 S의 개입이 없이 세션키를 이용는 경우에 적용된다.

  M-Sign1은, 거래를 원하는 임의의 당사자가 신뢰할 수 있는 중재자를 통해 자신의 신원 정보와 함께 메시지를 보낸 경우, 이 당사자는 자신이 보낸 메시지에 대해 책임이 있다는 것을 증명하는데 사용한다.

  S **Receives** (x **SignedWith** $K_{B,S}$);
  A **Receives** (m **SignedWith** $K_{A,S}$); x in m
  S **CanProve** (B **IsAuthenticatedUsing** $K_{B,S}$ by S) With $K_{B,S}$
  M-Sign1; A **CanProve** (S **IsAuthenticatedUsing** $K_{A,S}$ by A) With $K_{A,S}$
  A **CanProve** (B **Says** x) With $K_{A,S}$ and $K_{B,S}$

  즉, S가 $K_{B,S}$로 서명이 된 메시지 x를 받고 A가 $K_{A,S}$로 서명이 된 메시지 m을 받은 상황에서, m이 x를 포함하고 있다는 조건일 경우, S가 $K_{B,S}$는 B를 인증한다는 것을 증명할 수 있고, A가 $K_{A,S}$는 S를 인증한다는 것을 증명할 수 있다면, A는 B가 x를 말했다는 것을 증명할 수 있다. 즉, A가 B의 서명이 된 메시지 x를 중재자 S를 통해서 받으면, B가 x를 말했다는 것을 A는 증명할 수 있다는 것을 의미한다. 아래에 정의한 M-Sign2와 M-Sign3는 중재자와 당사자간의 메시지 송신으로, 메시지를 서명하기 위해서 사용한 마스터키를 작성한 중재자와의 직접적인 메시지 통신이기 때문에, 직관적인 추론이 가능하나, 거래 당사자간의 통신에 중재자가 개입하는 형태와는 다르기 때문에 정의하기로 한다. M-Sign2와 M-Sign3가 동일한 메시지에 대해서 연속적으로 서로 다른 두명의 당사자들사이에서 수행되면 M-Sign1의 경우가 된다.

S Receives (m **SignedWith** $K_{A,S}$); x in m
M-Sign2;S CanProve (A **IsAuthenticatedUsing** $K_{A,S}$ by S) With $K_{A,S}$
S **CanProve** (A **Says** x) With $K_{A,S}$

A **Receives** (m SignedWith $K_{A,S}$); x in m
M-Sign3; ACanProve (S **IsAuthenticatedUsing** $K_{A,S}$ by A) With $K_{A,S}$
A **CanProve** (S **Says** x) With $K_{A,S}$

M-Sign2는, S가 자신이 작성하여 A에게 보낸 마스터키 $K_{A,S}$를 이용하여 서명한 메시지 m을 받고, 또 m이 x를 포함한다면, S는 A가 x를 말했다는 것을 증명할 수 있다는 것을 의미한다.
M-Sign3는, A가 마스터키 $K_{A,S}$를 이용하여 서명된 메시지 m을 받고, 또 m이 x를 포함한다면, A는 S가 x를 말했다는 것을 증명할 수 있다는 것을 의미한다.
S-Sign(세션키 서명)은 중재자 S의 직접적인 개입이 없이, 중재자가 작성하여 배포한 세션키 $K_{A,B}$를 이용하여 전자 서명이 된 메시지도 메시지에 서명을 한 당사자가 그 메시지에 대해 책임이 있다는 것을 나타내는 증거로써 사용할 수 있음을 의미한다.

A **Receives** (m **SignedWith** $K_{A,B}$); x in m
S-Sign; A CanProve (B **IsAuthenticatedUsing** $K_{A,B}$ by A until T) With $K_{A,B}$
A **CanProve** (B **Says** x) With $K_{A,B}$

즉, A가 B와 공유하는 키 $K_{A,B}$로 서명이 된 메시지 m을 B로부터 받고, m이 x를 포함하고 있다는 조건하에서 A가, T를 이용하여 키 $K_{A,B}$가 유효하다는 것을 증명할 수 있고, 또 이 키는 당사자 B를 인증한다는 것을 증명할 수 있다면, A는 B가 x를 말했다는 것을 증명할 수 있다는 것을 의미한다.

4. 분석을 위한 소액 상거래용 전자지불 시스템[4]

제안하는 시스템의 프로토콜에서 사용하는 표기방법은 다음과 같다.

- B, S, IAP : 거래에 참여하는 당사자들로써, 각각 구매자, 판매자 및 구매자의 Internet Access Provider를 나타내며, IAP는 본 시스템의 비용 정산 서버 및 거래 중재자 역할을 수행.
- CR : B와 S의 신용 정보 및 B의 구매 한도에 대한 정보.
- S_{ACCT} : S가 B와 거래한 후의 정산을 위해, B가 등록되어 있는 IAP에 자신을 등록시키기 위해 필요한 정보.
- PO : S가 판매하고자 하는 상품의 번호와 가격을 자신의 비밀키를 이용하여 전자 서명을 한 후에 인터넷에 올린 정보를 이용하여, B가 S에게 보낸 구매 요청.
- PS : B가 S로부터 구매한 정보상품.
- TB : 현재의 PO를 제외하고, B가 S로부터 현재까지 구매한 총구매 요금중에서 아직 정산이 되지 않은 금액.
- TS : 현재의 PO를 제외하고, S가 B에게 판매한 총 판매 요금에서 아직 정산이 되지 않은 금액.
- PUB_X, PRI_X : 당사자 X의 상위 인증기관에 의해 인증된 X의 공개키와 비밀키.
- $K_{X,IAP}$, $K_{B,S}$, K_T : 당사자 X가 IAP와 교신하기 위한 마스터키와 당사자들간의 교신을 위한 세션키 및 현재의 인증세션만을 위한 임시 세션키.
- N_X, $N_{X'}$, $N_{X''}$: 당사자 X가 발행한 Nonce.
- T_X : 당사자 X의 시계를 기준으로 한 시간 표시로써 당사자 X가 세션키 인증서의 유효기간(또는, 세션키 인증서는 세션키를 포함하고 있으므로 세션키의 유효기간)을 제한하기 위한 목적으로 사용.
- {Message}PUB_S, {Message}$K_{X,IAP}$: PUB_S나 $K_{X,IAP}$를 이용하여 암호화된 메시지.
- [Message]$K_{X,IAP}$, [Message]$K_{B,S}$: Message에 단방향 해싱 함수를 적용하여 Message Digest를 계산하고, 여기에 $K_{X,IAP}$나 $K_{B,S}$를 적용하여 MIC(Message Integrity Check)를 계산한 뒤, 원래의 메시지에 첨부하여 작성한 메시지[5].
- {Message}PRI_S, {Message}PRI_{IAP} : S나 IAP의 비밀키를 적용하여 전자 서명이 된 메시지.
- X,Y,Z : X, Y, 및 Z의 결합.

본 시스템의 프로토콜에서 사용하는 대칭키 전자서명은 3.2절에서 기술한 방법으로 작성되는 것으로 가정한다. 제안하는 프로토콜은 설계의 특성상, 세션키에 의한 메시지의 발신지 증명 및 MIC에 의한 메시지 내용의 무결성 제공이 가능하다. 특히 MIC기법은, 암호화된 메시지와 함께 평문도 전송되어야 한다는 KA 로직의 기본 요건을 충족시켜 준다. 단, 상기한 기능들은 하나의 메시지에 대해서 위의 기법들이 함께 적용되었

을 경우에만 가능하다.

제안하는 시스템에서는 다음의 사항을 가정한다:

1) B와 S는 IAP에 대해 자신들 사이에서 이루어지는 모든 상거래의 중재자로써 절대적인 신뢰를 가지고 있다.
2) B와 S는 서로를 거래 당사자로 인증하기를 원하고 있으며 후속 되는 거래에서의 안전한 비용지불과 구매한 상품의 안전한 배달을 위해 필요한 양 당사자간에 공유하는 세션키를 IAP로부터 받기를 원한다.
3) 마스터키 $K_{B.IAP}$는 구매자가 자신의 IAP에 구좌를 개설할 때 IAP로부터 부여받은 것으로써, 안전한 절차를 통해 구매자에게 전달되어 이미 알고 있다.
4) S는 B가 사용한 유사한 방법을 사용하여 자신의 IAP에 미리 구좌를 개설한 것으로 간주한다.
5) 상품의 ID, 상품의 가격, IAP에 임시등록을 하기 위한 판매자의 정보 및 판매자의 PUBS은 판매자가 미리 전자 서명하여 판매하고자 하는 상품의 정보와 함께 웹에 공개되어 있기 때문에 구매자는 언제든지 이 정보를 이용하여 구매 요청을 작성할 수 있다.
6) 비용 정산 및 당사자 인증 서버 역할을 수행하는 구매자의 IAP는 좋은 세션키를 작성할 수 있는 능력이 있는 것으로 간주한다.

4.1 단계별 프로토콜 메시지

분석하고자 하는 소액 상거래용 전자 지불 시스템[4]의 당사자간 거래용 메시지는 다음과 같다. 아래에 설명한 프로토콜에서 구매자는, 판매자가 상품 정보와 함께 자신의 비밀키를 이용하여 서명한 가격정보를 인터넷에서 취득한 뒤에 PO를 이용하여 판매자에게 주문 요청을 한다. 즉 판매자가 서명을 하여 인터넷에 공표한 가격정보를 이용하여 구매자가 주문 요청을 할 경우이므로, 주문을 요청할 때 가격 협약은 동시에 수행되는 것으로 본다(메시지 F0, S0). 따라서 프로토콜의 일부는 아니나, 그에 상응하는 메시지이므로 함께 기술한다.

확장된 KA 로직을 적용하여 전자 지불 시스템을 분석하기 위해 가격의 보장, 서비스의 제공 및 청구서의 배달의 세 단계에 상응하는 메시지를 요약하여 정리하면 다음과 같다.

4.1.1 첫째 거래를 위한 메시지의 흐름(F)

이 프로토콜은 판매자와 IAP사이에 약속한 매 비용 정산 기간 내에서 구매자로부터 첫번째 주문이 있을 때마다 수행된다. 구매자의 신용상태에 따라 IAP와 판매자간에 약속한 비용정산 기간은 1일, 1주 또는 1개월이 될 수도 있다. 구매자는 판매자의 공개키를 IAP에게 보내고, IAP는 자신의 공개키를 판매자에게 보낸다. 판매자는 비용정산 프로토콜에서 IAP의 전자 서명을 검증하기 위해 IAP의 공개키를 사용한다. IAP가 판매자의 마스터키를 만들어서 판매자에게 보낼 때, IAP는 세션키, $K_{B.S}$와 임시 세션키 K_T를 판매자와 구매자에게 보내기 위해 판매자용 세션 인증서와 구매자용 세션 인증서를 작성하여 각자에게 보낸다. IAP는 구매자가 보낸 판매자의 공개키를 사용하여 판매자의 마스터키를 암호화한다. 구매자와 판매자는 정산기간 내에서 있을 수 있는 추가적인 주문의 처리를 위해 세션키 인증서라는 신용장을 만들어서 서로 교환한다. 추가적인 주문의 요청 시에, IAP의 중재를 받지 않고도 거래의 양 당사자간에 TS, CR 및 세션키를 안전하게 교환하기 위해서 세션키 인증서를 사용한다.

1) 가격의 보장

메시지 **F0;** S → B:

{price} PRI_S

2) 서비스의 요청

메시지 **F1;** B → IAP:

{price} PRI_S, PO,

[B, S, TS, N_B, PUB_S, S_{ACCT}]$K_{B.IAP}$

IAP는 이 메시지를 받으면, S_{ACCT}를 사용하여 판매자를 임시로 등록하고, 후에 이 판매자와 구매자사이의 거래금액에 대한 비용정산을 하기 위해 등록된 정보를 사용한다. IAP는, 가장 최근에 이루어진 정산과정에서 판매자가 보낸, 구매자가 서명한 정산용 누적지불 승인서를 이용하여 TS를 검증한다. TS가 이 정산용 누적지불 승인서의 금액과 같거나(즉 판매자가 정산 프로토콜을 이용하여 전번 비용정산 기간내의 모든 거래 금액의 정산을 완료한 경우), 크면(즉 판매자가 정산 프로토콜을 이용하여 전번 비용정산 기간내의 거래 금액중 일부만을 정산한 경우) 정상적인 메시지이기 때문에 IAP는 TS에서, 서명된 금액을 감액함으로써 TS를 갱신한다.

메시지 **F2;** IAP → S:

[B, S, TS, {price} PRIs, PO, CR, PUB_{IAP}]$K_{S.IAP}$,
{S, $K_{S.IAP}$}PUB_S,
{B, S, N_B, K_T, $K_{B.S}$}$K_{S.IAP}$, : 판매자용 세션인증서
{B, S, N_B, K_T, $K_{B.S}$}$K_{B.IAP}$: 구매자용 세션인증서

IAP는 판매자(S)의 마스터키 $K_{S.IAP}$를 만들어 판매자의 공개키를 이용하여 암호화한 뒤에 판매자에게 보낸다. IAP는 이 마스터키를 이용하여 자신의 공개키와 구매자가 보낸 구매 요청에 관련된 메시지의 MIC를 작성하여 보낸다. 또 IAP는 판매자와 구매자가 상호간의 메시지 교환을 위해 사용할 세션키 $K_{B.S}$와 임시 세션키 K_T를 포함하는 구매자가 사용할 세션 인증서 {B, S, N_B, K_T, $K_{B.S}$}$K_{B.IAP}$와 판매자가 사용할 세션 인증서 {B, S, N_B, K_T, $K_{B.S}$}$K_{S.IAP}$를 작성하여 판매자에게 전송한다.

판매자는 IAP로부터 이 메시지를 받으면 마스터키를 복호화하고, 이 마스터키를 사용하여 임시 세션키 K_T와 세션키 $K_{B.S}$를 복호화한다. 판매자는 마스터키를 사용하여 구매 요청에 관련된 메시지의 MIC가 유효한지 검증한 뒤에 PO를 이용하여 TS를 갱신한다. 이 때 갱신된 TS는 추가 주문 시에 사용하기 위한 세션키 인증서에도 동일하게 반영하여 한 정산기간 내에서의 총구매액이 정산되기까지 누적될 수 있도록 한다. 판매자는 구매자가 서명하여 보낸 상품의 ID와 가격, PO 등을 자신의 기억장치에 기록하여 다음 정산 과정에서 사용할 수 있도록 한다.

3) 서비스의 제공
메시지 **F3;** S → B:
[B, S, TS, CR, {B, PS}$K_{B.S}$]$K_{B.S}$,
{B, S, N_B, K_T, $K_{B.S}$}$K_{B.IAP}$, : 구매자용 세션인증서
{B, N_B, $K_{B.S}$}K_T, N_S, : 세션 확인서
{B, S, TS, CR, T_S, $K_{B.S}$}$K_{S.IAP}$: 판매자 세션키 인증서

판매자는 메시지 F3에서 구매자가 요청한 상품을 구매자와 공유하는 세션키를 이용하여 MIC를 작성한 뒤에, 구매자의 신원, 자신의 신원, 이 구매자에 대한 총 판매 금액(TS) 및 IAP로부터 받은 이 구매자의 신용등급(CR)과 함께 암호화하여 구매자에게 보낸다.

판매자는 구매자(B)가 보낸 Challenge인 Nonce N_B에 대한 Response로써, 구매자의 Nonce N_B와 세션키 $K_{B.S}$를 암호화하여 구매자에게 전송한다. 판매자는 이 두 키를 임시적으로 신뢰하고 있음을 구매자에게 알리기 위해 임시 세션키 K_T를 이용하여 암호화한다. 구매자(B)는 자신의 Challenge에 대한 판매자의 Response인 세션 확인서 {B, N_B, $K_{B.S}$}K_T내에 자신이 구매 요청과 함께 보냈던 Nonce N_B가 있는지를 확인함으로써 이들 두 키에 대한 판매자의 임시적인 신뢰를 확인한다. 판매자는 자신의 마스터키를 사용하여 암호화한 세션키 인증서인 {B, S, TS, CR, T_S, $K_{B.S}$}$K_{S.IAP}$를 구매자에게 보내어 같은 정산기간 내에서의 추가 주문 요청 시에 사용할 수 있도록 한다.

4) 청구서의 요청
메시지 **F4;** B → S:
[B, S, TS, TB]$K_{B.S}$, : 누적 지불 승인서(검증용)
[B, S, TS, TB, N_S]$K_{B.IAP}$, : 누적 지불 승인서(정산용)
{S, N_S, $K_{B.S}$}K_T, : 세션 확인서
{B, S, T_B, $K_{B.S}$}$K_{B.IAP}$: 구매자 세션키 인증서

구매자는 판매자의 Challenge인 Nonce N_S에 대한 Response로써 Nonce N_S와 세션키 $K_{B.S}$를 임시 세션키 K_T로 암호화한 세션 확인서인 {S, N_S, $K_{B.S}$}K_T를 판매자에게 보낸다. 판매자는 이 메시지를 받으면 구매자의 신원과 K_T 및 $K_{B.S}$에 대한 자신의 임시적인 신뢰를 확인할 수 있게 된다. 구매자는 자신이 서명한 정산용 누적 지불 승인서를 이용하여 TB가 정확하며, 다음 번 정산과정에서 TS에 해당하는 금액을 판매자에게 지불할 것을 약속한다. 판매자는 세션키를 이용하여 서명된 검증용 누적 지불 승인서를 사용하여 정산용 누적 지불 승인서의 내용을 검증한다. 구매자는 메시지 F3의 유효성을 점검한 뒤에 자신의 마스터키로 암호화한 세션키 인증서인 {B, S, T_B, $K_{B.S}$} $K_{B.IAP}$를 추가적인 주문 요청의 처리를 위해 사용할 수 있도록 판매자에게 보낸다. 첫 번째 주문을 처리한 뒤에 구매자는 TS와 TB를 자신의 저장장치에 보관하였다가 추가적인 주문의 처리나, 다음 번 정산기간의 첫 번째 주문 시에 사용한다.

4.1.2 둘째 이후의 거래를 위한 메시지의 흐름(S)

첫번째 주문의 처리를 완료한 후에 구매자와 판매자는 각각 상대방의 세션키 인증서를 가지고 있게 된다. 이 인증서는 이 두 거래 당사자가 추가적인 거래를 하기 위해서 필요한 세션키를 포함하므로 각자의 기억장치에 보관했던 세션키를 지움으로써 이 시스템을 더 안전하게 만들 수 있다. 같은 정산기간 내에서 구매자

가 이 판매자로부터 추가적인 주문을 하고자 할 경우, 첫번째 주문을 처리하는 과정에서 판매자가 보냈던 세션키 인증서를 이용하여 판매자에게 주문 요청을 보내고, 판매자는 구매자가 보냈던 세션키 인증서를 이용하여 구매자가 주문한 상품을 보냄으로써, IAP의 중재를 받지 않고서도 첫번째 주문과 동일하게 상대방의 인증과 아울러 안전한 거래를 수행할 수 있게 된다.

1) 가격의 보장
메시지 **S0;** S → B:
{price} PRI_S

2) 서비스의 요청
메시지 **S1;** B → S:
{price} PRI_S, PO, $N_{B'}$,
{B, S, TS, CR, T_S, $K_{B.S}$}$K_{S.IAP}$: 판매자 세션키인증서

구매자(B)는 추가주문 요청을 판매자(S)가 보내 준 세션키 인증서 및 판매자에 대한 Challenge인 Nonce $N_{B'}$와 함께 판매자에게 보낸다. 구매자는 판매자가 서명하여 웹에 올려놓은 상품의 가격을 세션키를 이용하여 암호화하여 보냄으로써 자신이 가격에 동의함을 표시하게 된다. 판매자는 구매자가 보낸 자신의 세션키 인증서를 검증하여 유효함을 확인한 뒤에 구매자가 사용한 세션키 $K_{B.S}$를 임시적으로 신뢰하게 된다.

3) 서비스의 제공
메시지 **S2;** S → B:
[B, S, TS, {B, PS}$K_{B.S}$, $N_{B'}$]$K_{B.S}$, $N_{S'}$,
{B, S, T_B, $K_{B.S}$}$K_{B.IAP}$, : 구매자 세션키 인증서
{B, S, TS, CR, T_S, $K_{B.S}$}$K_{S.IAP}$: 판매자 세션키 인증서

판매자(S)는 구매자로부터 받은 구매 요청 메시지가 유효한지를 검증한 뒤에, 구매자와 공유하는 세션키를 적용하여 구매 요청한 상품을 암호화한다. 판매자는 구매요청 메시지에 있는 가격정보를 이용하여 이 구매자에 대한 총 판매액(TS)을 갱신한 뒤에 암호화한 상품, 구매자의 신원, 자신의 신원, 구매자에 대한 총 판매액 및 구매자의 Challenge에 대한 Response역할을 하는 Nonce $N_{B'}$의 MIC를 작성하여 구매자에게 보낸다. 판매자는 원래의 메시지, 자신이 작성한 구매자에 대한 Challenge인 Nonce $N_{S'}$ 및 구매자로부터 받은 세션키 인증서와 함께, 다음 번 거래를 위해 자신의 세션키 인증서에 있는 TS를 갱신한 뒤에 이 인증서도 구매자에게 보낸다. 판매자는 구매자가 서명하여 보낸 상품의 ID와 가격을 자신의 기억장치에 기록하여 다음 정산 과정에서 사용할 수 있도록 한다.

4) 청구서의 요청
메시지 **S3;** B → S:
[B, S, TS, TB, $N_{S'}$]$K_{B.IAP}$, :누적 지불 승인서(정산용)
[B, S, TS, TB, $N_{B'}$, $N_{S'}$]$K_{B.S}$:누적 지불 승인서(검증용)
{B, S, TB, $K_{B.S}$}$K_{B.IAP}$, : 구매자 세션키 인증서

구매자(B)는 이 메시지를 이용하여, 자신이 판매자(S)의 신원을 확인하였으며 또 세션키 $K_{B.S}$를 신뢰하고 있음을 판매자에게 알려 준다. 구매자는 새로운 세션키 인증서 {B, S, $T_{B'}$, $K_{B.S}$}$K_{B.IAP}$를 보내어 추가 거래시에 사용할 수 있도록 한다. 판매자는 이 메시지를 수령한 뒤, 구매자의 신원과 세션키에 대한 자신의 신뢰를 확인한다. 구매자는 자신이 서명한 정산용 누적 지불 승인서를 이용하여 TB가 정확하며, 다음 번 정산 과정에서 TS에 해당하는 금액을 판매자에게 지불할 것을 약속한다. 판매자는 세션키를 이용하여 서명된 검증용 누적 지불 승인서를 사용하여 정산용 누적 지불 승인서의 내용을 검증한다. 판매자는 구매자가 서명하여 보낸 상품의 ID와 가격을 자신의 기억장치에 기록하여 다음 정산 과정에서 사용할 수 있도록 한다.

4.1.3 비용 정산을 위한 메시지의 흐름(C)

판매자는 필요할 경우, IAP와 협약한 매 정산기간 내에서 시스템이 한가한 시간을 이용하여 언제든지 정산 프로토콜을 시작할 수 있으며, 구매자가 한도를 초과하여 상품을 구매하는 것을 방지하기 위해 최소한 한번은 정산기간의 마지막에 이 정산 프로토콜을 시작한다. 판매자는 구매자가 서명한 정산용 누적 지불 승인서를 이용하여 현재까지의 총 구매액 (TS)을 정산해 주도록 IAP에게 요청한다

1) 청구서의 처리
메시지 **C1;** S → IAP: [CR, $N_{S''}$, PO1, PO2, …, POn, B's Signed Payment Order]$K_{S.IAP}$: B는 $K_{B.IAP}$를 이용하여 정산용 누적 지불 승인서(Signed Payment Order)를 서명하였음.

판매자(S)는 지난번 정산처리 후부터 현재까지 축적

된 구매자로부터의 모든 구매 요청과 마지막 구매요청과 함께 서명하여 보낸 정산용 누적 지불 승인서, 자신이 작성한 Nonce $N_{S''}$ 및 자신이 생각하는 새로운 신용등급을 포함하는 메시지의 MIC를 마스터키 $K_{S,IAP}$를 이용하여 만들어 IAP에게 보냄으로써 정산처리를 요청한다. IAP는 이 정산 요청을 받으면, TS에 해당하는 금액을 구매자의 구좌로부터 판매자의 임시구좌에 입금하고, 다음 번 구매자에 대한 청구서를 통해 같은 금액을 지불하도록 요청하게 된다. IAP는 TS와 TB를 갱신한 뒤에 이 것을 판매자가 보낸 Nonce $N_{S''}$와 함께 암호화하여 메시지 C2를 이용하여 판매자에게 보낸다. IAP는 자신의 경험이나 판매자의 의견을 이용하여 구매자의 신용등급을 조정할 수 있다. IAP는 구매자의 서명이 된 누적지불 승인서를 자신의 저장 장치에 보관하였다가 다음 번 정산기간내의 최초 주문처리 시에 구매자가 보내 오는 총구매액과 비교하여 아직 정산되지 않은 금액의 정산처리 시에 사용할 수 있도록 한다.

메시지 **C2;** IAP → S:
$\{B, S, TS, TB, CR, N_{S''}\}PRI_{IAP}$

IAP는 자신이 서명한 이 메시지를 통해 판매자(S)가 보낸 정산 요청이 완료되었음을 확인해 준다. 판매자는 이 메시지를 받으면, IAP의 공개키를 이용하여 IAP의 전자 서명을 검증한 뒤에, 장래에 있을 지도 모르는 판매자와 구매자간의 분쟁을 위해 자신의 저장 장소에 보관한다.

4.2 분석 단계[2]

여기서는 앞에서 정의한 KA 로직을 확장한 새로운 로직을 적용하여 프로토콜을 분석하기 위해서, Kailar가 정의한 분석단계를 사용한다. 이 분석 방법은 다음과 같은 단계로 구성된다.

1) 책임에 대한 프로토콜의 목표를 정의한다(전자 상거래를 위한 프로토콜의 경우, 이 것은 경험에 근거한 실제 상거래의 목표에서 도출한다)
2) 프로토콜의 메시지를 해석한다
3) 초기 상태에 대한 가정을 명확히 한다.
4) 책임 속성에 대해 메시지를 분석하고
5) 프로토콜에 참여하는 당사자들이 얻은 증명 가능성의 결과와 프로토콜의 목표를 비교한다. 목표 달성을 하지 못했다는 것은 프로토콜의 약점을 나타낸다.

다음에 설명하는 각 목표의 증명(CanProve구문)과정에서 비대칭키 전자 서명을 사용한 메시지에는 KA 로직에서 정의한 강한 증명을 적용하며, 대칭키 전자서명을 사용한 경우는 확장된 KA 로직에서 정의한 약한 증명을 적용한다.

4.3 전자 상거래 프로토콜의 목표[2]

전자 상거래용 프로토콜의 중요 목표는, 판매자는 전에 합의한 가격이 아닌 상품에 대해서 구매자에게 청구서를 보낼 수 없으며, 합의된 가격으로 상품이 제공되었을 경우 구매자는 상품 대금의 지불을 거절할 수 없다는 것을 확인하는 것이다. 전자 상거래용 프로토콜은 보통 다음과 같은 단계와 목표를 가지고 있다.

- 가격의 보장
  이 것은 구매자(B)와 판매자(S)사이에, 합의된 가격으로 상품을 제공하겠다는 계약이다. 완전한 책임의 증명이 가능함을 보이기 위해서, 이 프로토콜은 다음의 목표를 달성 해야만 한다.
  G1: B **CanProve** (S agreed on price/item)
  G2: S **CanProve** (B agreed on price/item)
- 상품의 제공
  이 것은 판매자가 구매자에게 상품을 제공하는 단계로써 완전한 책임의 증명은 다음의 목표가 달성될 때 가능하다.
  G3: B **CanProve** (S rendered k items of services)
  G4: S **CanProve** (B received k items of services)
  이 목표들은 B(S)가, S(B)가 정확하게 k개의 서비스를 제공했다(또는 B가 K개의 서비스를 받았다)는 것을 도출해 낼 방법을 필요로 한다. 구현과정에서 이것은 상품의 제공과 수령에 관련된 명확한 시작과 끝이 필요하다. 즉, 증명의 수령자들이, 증명자가 그들에게 모든 필요한 메시지를 보여 주고 있음을 알 수 있도록 모든 중간과정의 메시지는 일련 번호(Sequence Number) 부여하거나 Timestamp 또는 Challenge/Response프로토콜을 사용함으로써 가능하다[6].
- 청구서의 배달
  청구 서버가, 구매자에게는 상품 대금만큼 구매자 구좌에서 출금되었으며, 판매자의 구좌에는 상품 대금만큼 입금되었음을 통보하는 과정이다. 완전한 책임을 증명하기 위해서는 다음의 목표가 달성되어야 한다.

G5: B **CanProve** ($X transferred from B to S)
G6: S **CanProve** ($X transferred from B to S)

4.4 프로토콜의 해석

책임 분석에서는 서명과 함께 B(구매자)와 S(판매자)의 신뢰를 받는 IAP가 이해할 수 있는 평문이 있는 메시지만 유용하기 때문에, 상기의 프로토콜에서 그러한 것들만 아래에 해석하여 나열하였다.

분석하는 프로토콜에서 평문과 암호문이 함께 있는 경우는 비대칭키의 전자서명을 사용한 메시지나, 대칭키 전자 서명의 경우 MIC(Message Integrity Check)를 생성하여 평문과 함께 전송한 메시지로써 [message]$K_{A,B}$의 형태로 표현되어 있다. {message}$K_{A,B}$는 암호문만 있는 메시지이다. 앞에서 설명한 프로토콜의 첫째 거래(F) 및 정산(C)을 위한 메시지에서 이에 해당한 메시지들은 다음과 같은 해석이 가능하다.

F0) B Receives (Price) SignedWith PRI_S
F1) IAP Receives (Price) SignedWith PRI_S
F2) S Receives (Price) SignedWith $K_{S.IAP}$
F4) S Receives (Payment Order) SignedWith $K_{B.S}$
C1) IAP Receives (Payment Order) SignedWith $K_{B.IAP}$
: B가 S에게 보내는 지급 승인 메시지는 자신의 마스터키 $K_{B.IAP}$로 서명되어 있다.
C2) S Receives (Payment) SignedWith PRI_{IAP}

둘째 이후의 거래(S)와 정산(C)을 위한 메시지에서 이에 해당한 메시지들은 다음과 같은 해석이 가능하다.

S0) B Receives (Price) SignedWith PRI_S
S1) S Receives (Price) SignedWith PRI_S
S3) S Receives (Payment Order) SignedWith $K_{B.S}$
C1) IAP Receives (Payment Order) SignedWith $K_{B.IAP}$
C2) S Receives (Payment) SignedWith PRI_{IAP}

4.5 초기 상태의 가정

앞에서 설명한 프로토콜의 설명과 프로토콜의 기본 가정에서 추출할 수 있는 초기 상태에 대한 가정은 다음과 같다. 다음의 가정에서 대칭키 전자 서명을 사용한 경우에는 약한 증명의 정의를 적용한다. 즉, 사실의 증명을 위해서 증명자는 증명의 수령자에게 거래 당사자들만 공유하던 키(마스터키나 세션키)를 공개함으로써 거래의 내역을 증명할 수 있는 경우이다.

A1 : S **CanProve** (IAP IsAuthenticatedUsing $K_{S.IAP}$ by S) With $K_{S.IAP}$
A2 : B **CanProve** (PRI_S Authenticates S)
A3 : IAP **CanProve** (PRI_S Authenticates S)
A4 : S **CanProve** (PRI_{IAP} Authenticates IAP)
A5 : S **CanProve** (B IsAuthenticatedUsing $K_{B.IAP}$ by S) With $K_{B.IAP}$
A6 : IAP **CanProve** (B IsAuthenticatedUsing $K_{B.IAP}$ by IAP) With $K_{B.IAP}$
A7 : S **CanProve** (B IsAuthenticatedUsing $K_{B.S}$ by S until T) With $K_{B.S}$
A8 : B **CanProve** (A IsAuthenticatedUsing $K_{B.S}$ by B until T) With $K_{B.S}$
A9 : (S **Says** Price) → (S agrees on price of item)
A10 : (B **Says** Price) → (B agrees on price of item)
A11 : (S **Says** Service) → (S renders one service item)
A12 : (B **Says** Payment Order) → (B agrees to pay $ of Invoice)
A13 : (IAP **Says** Payment) → ($ of invoice transferred from B to S by IAP)
A14 : (S **Says** Invoice) → (S requests B to pay $ of Invoice)
A15 : (IAP **Says** Price) → (IAP arbitrates agreement on price of item)

A1은, S(판매자)는 IAP가 키 $K_{S.IAP}$를 이용하여 인증될 수 있다는 것을 증명할 수 있음을 나타내며, A2는, B(구매자)는 S가 키 PRI_S를 이용하여 인증될 수 있다는 것을 증명할 수 있음을 나타낸다. A3부터 A8까지는 위와 같은 방법으로 설명이 되므로 생략한다. A9부터 A15까지는 각각의 당사자가 이 프로토콜에서 서명한 진술의 해석에 관한 것이다.

4.6 분석

4.6.1 첫째 거래를 위한 메시지의 분석(F)

1) 메시지 **F0**

B(구매자)는 F0를 웹 브라우저를 통해 받았을 때, B는 **A2**와 **Sign** 구문을 이용하여

B CanProve (S Says Price)

가 가능하다. 이 것은 가정 **A9**와 **Inf** 구문을 이용하여

B CanProve (S agrees on price of item) **[G1]**

이기 때문에 **G1**의 증명이 가능하다.

2) 메시지 **F1**

IAP가 F1을 받으면, 가정 **A3**와 **Sign** 구문을 이용하여

IAP CanProve (S Says Price)

가 가능하다. 그러나 이 메시지에는 B(구매자)의 서명이 없으므로 B가 S(판매자)의 가격에 동의했는지는 알 수 없다.

3) 메시지 **F2**

S(판매자)가 F2를 받으면, 가정 **A1**과 **M-Sign3** 구문을 이용하여

S CanProve (IAP Says Price) With $K_{S.IAP}$

가 가능하다. 이 것은 가정 **A15**와 **Inf** 구문을 이용하여 다음과 같이 세분화 할 수 있다.

S CanProve (IAP arbitrates agreement on price of item) With $K_{S.IAP}$

그러나 이것은 누군가가 IAP의 중재를 통해 S의 가격에 동의했다는 것만 알 수 있을 뿐 누구인지는 알 수 없기 때문에 **G2**의 증명은 불가능하다.

G2의 증명이 가능하기 위해서는 메시지 F1을 다음과 같이 변경해야 한다. 즉 S(판매자)의 가격에 동의한다는 표시로 B(구매자)가 자신이 IAP와 공유하는 키 $K_{B.IAP}$로 서명하여 보낸다.

메시지 **F1**; B → IAP:
[B, S, TS, N_B, PUB_S, ***{price} PRI***$_S$, S_{ACCT}]$K_{B.IAP}$

이 경우에 메시지 F1의 해석은

F1) IAP Receives (Price) SignedWith $K_{B.IAP}$

가 된다. IAP는 메시지 F2의 해석과 상기한 메시지 F1의 새로운 해석, 가정 **A1**과 **A6** 및 구문 **M-Sign1** 구문을 이용하여

S CanProve (B Says Price) With $K_{B.IAP}$ and $K_{S.IAP}$

가 가능하다. 이 것은 가정 **A10**과 **Inf** 구문을 이용하여 다음과 같이 세분화하여

S CanProve (B agrees on price of item) With $K_{B.IAP}$ and $K_{S.IAP}$ **[G2]**

이므로 **G2**의 증명이 가능하다.

4) 메시지 **F3**

메시지 F3에는 B(구매자)가 받은 상품(PS)의 평문이 없기 때문에 가정에 의해 증명이 불가능하다. 메시지 F3을 다음과 같이 변경하면 증명이 가능하다.

메시지 **F3**; → S B:
{B, S, TS, CR, ***[B, PS]K***$_{B.S}$}$K_{B.S}$,
{B, S, N_B, K_T, $K_{B.S}$}$K_{B.IAP}$,
{B, N_B, $K_{B.S}$}K_T, N_S,
{B, S, TS, CR, T_S, $K_{B.S}$}$K_{S.IAP}$

이 메시지에서 상품 PS는 MIC기법을 적용하여 전송하기 때문에 암호화된 상품과 아울러 평문도 함께 포함된다. 메시지 F3에서, S(판매자)는 B(구매자)가 구매한 상품을 보내기 전에 B와 S가 공유하도록 IAP가 작성하여 S에게 보낸 세션키 $K_{B.S}$를 이용하여 암호화하고, 이 세션키는 IAP가 S의 마스터키 $K_{B.IAP}$로 암호화하여 S를 통해 상품과 함께 B에게 보내기 때문에, B는 IAP와 공유하는 마스터키 $K_{B.IAP}$를 알지 못할 경우 상품을 복호화 할 수 없다. 메시지 F3의 해석은 다음과 같다.

F3) B Receives (Invoice) SignedWith $K_{B.S}$

B가 F3을 받으면, B는 가정 **A8**과 **S-Sign** 구문을 이용하여

B CanProve (S says Invoice) With $K_{B.S}$

가 가능하다. 이 것은 가정 **A14**와 **Inf** 구문을 이용하여

B CanProve (S requests B to pay $ Invoice) With $K_{B.S}$

으로 세밀하게 추론할 수 있다. 메시지 F3은 현재까지의 모든 주문에 대한 총 구매액을 포함하기 때문에 현재까지의 총 구매량인 K개의 서비스가 제공되었음을 의미하므로 **Conj**를 이용하여

B CanProve (S rendered k service item) With $K_{B.S}$ **[G3]**

이 되므로 **G3**의 증명이 가능하다.

5) 메시지 **F4**

S(판매자)가 F4를 받으면, S는 가정 **A7**과 **S-Sign** 구문을 이용하여

S CanProve (B Says Payment Order) With $K_{B,S}$

가 가능하다. 이것은 가정 **A12**와 **Inf**를 적용하여

S CanProve (B agrees to pay $ of Invoice) With $K_{B,S}$ **[P1]**

가 된다. 그런데, 메시지 F3에서 B(구매자)는 상품과 이 상품을 포함한 총구매액에 대한 청구서를 함께 받으므로 **P1**에 **Inf**를 적용하여

S CanProve (B receives one service item) With $K_{B,S}$

으로 세밀하게 추론할 수 있다. 메시지 F3은 현재까지의 모든 주문에 대한 총 구매액을 포함하기 때문에 현재까지의 총 구매량인 K개의 서비스가 제공되었음을 의미하므로 **Conj**를 이용하여

S CanProve (B received k service item) With $K_{B,S}$ **[G4]**

이므로 **G4**의 증명이 가능하다.

6) 메시지 **C1**

메시지 C1에 포함된 누적 지불 승인서(Signed Payment Order)는 B(구매자)가 $K_{B,IAP}$를 이용하여 서명한 것이므로, IAP는 가정 **A6**과 **M-Sign2** 구문을 이용하여

IAP CanProve (B Says Payment Order) With $K_{B,IAP}$

가 가능하다. 이 것은 가정 **A12**와 **Inf** 구문을 이용하여 다음과 같이 세분화 할 수 있다.

IAP CanProve (B agrees to pay $ of invoice) With $K_{B,IAP}$

그러나 실제로 B의 구좌에서 S(판매자)의 구좌로 입금이 되었는지는 알 수 없기 때문에, 이 것만으로 G5나 G6의 증명은 불가능하다.

7) 메시지 **C2**

S(판매자)가 C2를 받으면, S는 가정 **A4**와 **Sign** 구문을 이용하여

S CanProve (IAP Says Payment)

가 가능하다. 이 것은 가정 **A13**과 **Inf** 구문을 이용하여 다음과 같이 세분화 할 수 있다.

S CanProve ($ of Invoice transferred from B to S by IAP) **[P2]**

P2에 **Inf** 구문을 적용하여

S CanProve ($ amount transferred from B to S) **[G6]**

이 되므로 **G6**의 증명이 가능하다.

8) **G5**의 증명

메시지 C1이나 C2에서는 B(구매자)에게 정산의 완료에 대한 아무런 메시지도 보내지 않기 때문에 **G5**의 증명은 불가능하다. 그러나 첫째 구매의 메시지 F3나 둘째 구매의 메시지 S2를 통하여 S(판매자)가 B에게 보내는 내용에는 B가 S로부터 구매한 총구매액 중에서 S가 IAP를 통해 정산한 금액을 감산한 뒤에 현재의 구매액이 추가된 금액이 포함되어 있다. B는 S가 보낸 이 금액과 자신이 가장 최근에 서명하여 보낸 청구금액을 비교하여, 그 차액이 S에게 지급되었음을 알 수 있다. 위에서 설명한 확장된 KA 로직을 적용하여 **G5**를 증명하기 위해서는 S의 요청에 의한 정산이 이루어 질 때마다 IAP가 B에게 정산 완료 메시지를 보내야 하나, 소액 상거래용 전자 지불 시스템에서 전산처리 비용을 최소화해야 하는 요건을 충족시키기 위해서 메시지 수를 줄여야 할 필요가 있으므로, 위에서 설명한 간접적인 방법으로 증명할 수 있는 것으로 가정한다.

4.6.2 둘째 이후의 거래를 위한 메시지의 분석(S)

둘째 거래 이후의 메시지인 S0부터 C2까지의 분석은 첫째 거래와 거의 유사함으로 생략하기로 한다. 그러나 첫째 거래의 분석 결과로 제안된 프로토콜의 변경 요건은 둘째 거래를 위한 프로토콜에도 동일하게 적용하여 수정된 프로토콜은 다음과 같다.

메시지 S1; B → S:
$\{B, S, TS, CR, T_S, K_{B,S}\}K_{S,IAP}, N_{B'}$
$\{PO, \{price\}PRI_S\}K_{B,S}$

메시지 S2; S → B:
$[B, S, TS, \{B, PS\}K_{B,S}, N_{B'}]K_{B,S}$,
$\{B, S, T_B, K_{B,S}\}K_{B,IAP}, N_{S'}$,

{B, S, TS, CR, T_S, $K_{B,S}$}$K_{S,IAP}$

5. 결 론

정보통신 프로토콜에서 전송되는 메시지의 책임 소재에 대한 증명이 필요한 경우, 이 책임 소재의 증명 가능성을 검증하기 위해 적용할 수 있는 KA 로직(Kailar Accountability Logic)은 비대칭키 전자서명을 가정하고 있다. 그러나 소액 상거래용 전자 지불 프로토콜의 경우, 전산처리의 효율성 때문에, 비대칭키 암호화 기법보다는 대칭키 암호화 기법을 많이 사용하고 있다. 이를 위해 본 논문에서는 대칭키 전자 서명에 관련된 특성을 KA 로직에 반영하여 변경 및 추가 요소를 정의함으로써 KA 로직을 확장하였으며, 이 확장된 로직을 이용하여 저자가 제안한, 대칭키 전자 서명을 이용하는 소액 상거래용 전자 지불 프로토콜을 분석하였다. 이 로직의 적용을 통해서, 프로토콜의 책임 소재 증명 가능성에 대한 약점을 파악하고, 그 해결 방안을 제시할 수 있음을 보임으로써 대칭키 암호화 기법의 전자 서명을 위해 확장된 Kailar Accountability Logic의 효용성을 증명하였다.

참 고 문 헌

[1] M. Burrows, M. Abadi, and R. Needham, "A Logic of Authentication," ACM Trans, Computer Systems, Vol.8, No.1, Feb. 1990.

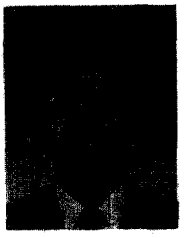
[2] Rajashekar Kailar, "Accountability in Electronic Commerce Protocols," IEEE Trans. on Software Engineering, Vol.22, No.5, pp.313-328, May 1996.

[3] Bruce Schneier, Applied Cryptography Second Edition, John Wiley & Sons, 1996.

[4] Youngdal Kim, Kwanho Song, Sunyoung Han, An Efficient and Secure Electronic Micropayment System Using Nonce-based Authentication Protocol, Proceedings of International Conference on Parallel and Distributed Processing Techniques and Applications, CSREA Press, pp.193-199, 1999.

[5] Donal O'Mahony, Michael Peirce, and Hitesh Tewari, Electronic Payment System, Artech House, 1997.

[6] I-Lung Kao and Randy Chow, An Efficient and Secure Authentication Protocol Using Uncertified Keys, Operating Systems Review Vol.29 No.3, 1995.



김 영 달

e-mail : ydkim@att.co.kr

1977년 서울대학교 자연대학 계산통계학과(이학사)

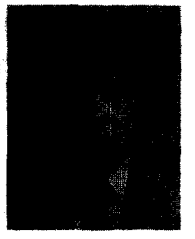
1991년 서강대학교 공공정책대학원 정보처리학과(이학석사)

1976년~현재 한국 IBM 컨설팅 사업부 전문 위원

1992년~현재 한국 정보처리 전문가 협회 회원

1994년~현재 건국대학교 컴퓨터공학과 박사과정

관심분야 : WWW 보안, 전자 상거래, 전자지불 시스템



한 선 영

e-mail : syhan@cclab.konkuk.ac.kr

1977년 서울대학교 계산통계학과(학사)

1979년 한국과학기술원 전산학 석사

1988년 한국과학기술원 전산학 박사

1981년~현재 건국대학교 컴퓨터정보통신공학과 교수

1989년~1990년 미국 Maryland대 컴퓨터 과학과 객원부교수

1991년~1997년 금융결재원 자문교수

1990년~1997년 한국과학기술원 인공지능 연구센터 참여교수

1992년~1997년 개방형 컴퓨터 통신 연구회 TG-VT 의장

1991년~1993년 한국정보과학회 정보통신연구회 부위원장

1990년~1997년 ISO/IEC JIC1/SC21 WG8 위원장(국내 위원회)

1995년~1997년 개방형 컴퓨터 통신 연구회 TG-Web의장

1995년~1997년 건국대학교 산업기술연구소 정보통신연구센타 소장

1996년~1998년 개방형 컴퓨터 통신 연구회 총무이사

1997년~현재 한국 인터넷 협회 기술위원회 위원

1997년~1998년 건국대학교 정보통신원 교육지원 센터 소장

1998년~1999년 미국 Maryland 대학교 컴퓨터 과학과 객원교수

1998년~현재 개방형 컴퓨터 통신 연구회 이사

관심분야 : Real-Time CORBA, Internet Caching, 차세대 인터넷 프로토콜, Mobile IP