通信情報保護學會論文誌
第 10 券 第 1 號, 2000. 3

페트리네트를 이용한 침입탐지 전자지불 프로토콜의 설계와 검증

유 은 진*, 전 문 석**, 이 철 희***

Design and Verification of Intrusion Detectioned Electronic Payment Protocol by Petri Net

Eun-Jin Yu*, Moon-Seog Jun**, Chul-Hee Lee***

요 약

본 논문은 인터넷 상에서 전자상거래가 이루어지는데 기본적으로 요구되는 보안성을 강화하기 위해 침입탐지 전자지불 프로토콜을 제안하였다. 여기서 침입탐지 기능이란 정보 전송이 이루어지는 순간마다 침입이 발생하였는지 탐지하도록 하므로써 신속한 탐지가 이루어지도록 하는 기능을 말한다. 제안된 침입탐지 전자지불 프로토콜의 타당성, 안정성을 분석하기 위해 페트리네트와 CPN(Coloured PetriNet)을 이용하여 모델링하였다. 또한 암호화 논리의 유용한 검증 도구로서 BAN(Burrows-Abadi-Needham) 논리 시스템과 Kailar 논리 시스템을 이용하여 프로토콜의 타당성과 안정성을 확인·검증하였다.

ABSTRACT

This paper suggestes on intrusion-detectioned electronic payment protocol to purpose of strengthen securicy for requiering at basically electronic commerce in the Internet. The intrusion-detectioned property is to detection for intrusion at the every time of making information transmission rather than to prevent intrusions. Petri Net and CPN(Coloured Petri Net) was used for analysis to validity and security of intrusion-detectioned electronic payment protocol. And as useful verification tools of encrypt logics, the paper verifies the authentication of intrusion-detectioned electronic payment protocols used for the BAN logic systems and Kailar logic systems.

keyword : *intrusion-detectioned electronic payment protocol, Petri Net, CPN*

Ⅰ. 서 론

인터넷을 사용하여 거래하는 것은 전통적인 거래 방식에 새로운 변화를 가져온다. 거래는 상인의 업무 장소나 소비자의 배달 장소가 쉽게 확인될 수 없는 가상의 장소에서 이루어지며 네트워크를 공유하는 제3의 서버에 의해 관찰된다. 또한 거래에 컴퓨터를 사용하는 것은 기록 유지가 보다 쉬워지는 대신 거래 데이터로부터 발생되는 개인정보 보호 및 금융상의 정보 노출 문제가 제기된다. 또한 가상의 공간에서 거래를 지원하는 것은 전자적인 분석이 요구되는데, 그들이 누구와 거래하려는지 알 필요가 있으며, 적

* 숭실대학교 정보과학대학 컴퓨터학부 (YEJ319@hotmail.com)
** 숭실대학교 정보과학대학 컴퓨터학부 (mjun@computing.soongsil.ac.kr)
*** 숭실대학교 정보과학대학 컴퓨터학부 (chlee@computing.soongsil.ac.kr)

어도 그들의 신용 가치를 검증할 필요가 있다. 이러한 전자거래의 가장 중요한 요구 사항은 안전하고 편리한 전자지불 시스템의 개발이다.

본 논문의 Ⅱ 장에서는 전자상거래와 전자지불시스템에 대해 알아보고, Ⅲ 장에서는 보안성이 강화된 침입탐지 전자지불 프로토콜을 제안한다. Ⅳ 장에서는 침입탐지 칼라 페트리네트를 정의하고 이를 통해 제안된 프로토콜을 분석한다. Ⅴ 장에서는 제안된 침입탐지 전자지불 프로토콜을 BAN 논리 시스템과 Kailar 논리 시스템을 이용하여 검증한다. Ⅵ 장에서는 기존의 전자지불 프로토콜과 제안한 프로토콜을 비교한 후, Ⅶ 장에서 결론을 제시한다.

Ⅱ. 전자상거래와 전자지불 시스템

1. 전자상거래

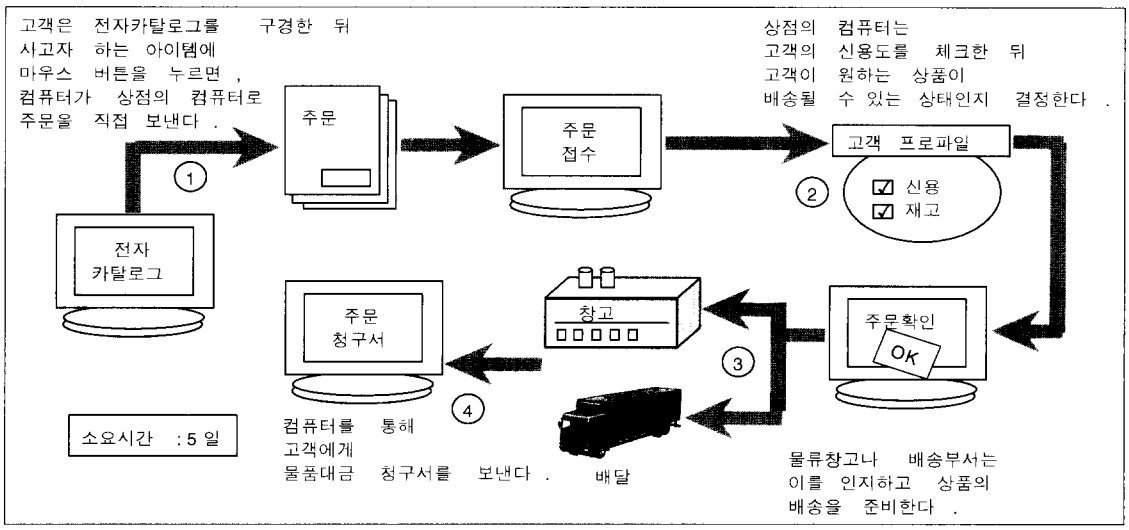
전자상거래(Electronic Commerce)는 미국의 국립 로렌스 리브모어 연구소(Lawrence Livemore National Laboratory)가 국방성의 프로젝트를 수행하면서 처음으로 사용한 용어로 거래가 시작되면서 끝날 때까지 종이서류가 사용되지 않는 기업환경을 정보통신 기술에 의해 추구하려는데 그 목적이 있었다. 이처럼 전자상거래는 인터넷과는 무관하게 제안되었지만 일반에게 전자상거래라는 개념이 부각되기 시작한 것은 인터넷이 대중화되기 시작하면서였다. 전자상거래에 대한 정의는 여러 가지 관점에서 다양하게 내려질 수 있으나, 미국 오스틴 대학의 윈스턴 교수는 '네트워크를 통한 상품의 구매와 판매'로 정의하고 있다.[15]

상거래(Commerce)의 원래 의미는 기업과 기업의 상거래를 의미하는데 상품과 서비스를 판매하고 반대로 금전적인 대가를 받는 것을 말한다. 컴퓨터 네트워크의 확산에 따라 거래 관계에 있는 기업과 기업 사이에 단지 상품과 서비스의 교환뿐만 아니라 그 이전 단계의 제품 개발과 수요자 요구의 발굴에 이르는 모든 정보를 서로 공유하면서 협력하는 새로운 형태의 거래가 형성되면서 '전자상거래(Electronic Commerce)'란 용어가 범용화되기 시작한 것이다.[16]

2. 전자상거래의 전제 조건

네트워크를 근간으로 한 전자거래에는 이를 형성하기 위한 기반 조건으로서 고려할 중요한 요소들이 있다. 이들은 네트워크 접속, 지불 방법, 소비자 서비스, 개인 정보 보호 등이 있다. 이들 요소들은 쉽고 편리하며 일관성있게 구성되어야 일반 사용자들이 많이 사용하며 성공적인 전자거래가 이루어질 수 있다.

네트워크 접속을 생각할 때 일반 컴퓨터 통신은 범용 에뮬레이터로 모뎀과 전화만으로01410/01420 혹은 고속모뎀 전화번호 등으로 접속하고 메뉴에서 서비스를 선택하면 되도록 비교적 쉽게 구성되어 있다.



〔그림 1〕 전자거래 방식
〔Fig. 1〕 Electronic commerce methode

그러나 범용 에뮬레이터에 각종 지불방식 등을 도입하기에는 불편함이 있다. 최근 국내의 통신 서비스(컴퓨터 통신/인터넷) 회사들은 이런 네트워크 접속을 쉽게 할 수 있도록 서비스하는 회사들이 있고, PPP 사용법도 많이 일반화되는 추세여서 네트워크 접속 문제는 상당 부분 해결되어 가는 전망이다.

소비자 서비스와 개인 정보 보호는 전자거래 서비스 회사들의 정책과 관련되는 문제이다. 전자거래에 있어서 가장 중요한 요소는 손쉽고 일관성있는 지불 방법으로 전자지불 프로토콜은 아직 연구·시험중에 있으며 발전의 여지가 많다. 그러나 외국에는 이런 지불 메커니즘은 전자거래의 핵심적인 요소임을 인식하고 이미 많은 연구가 이루어졌고 상용 서비스를 하는 회사들도 다수 생겨나고 있다.

3. 전자지불 시스템

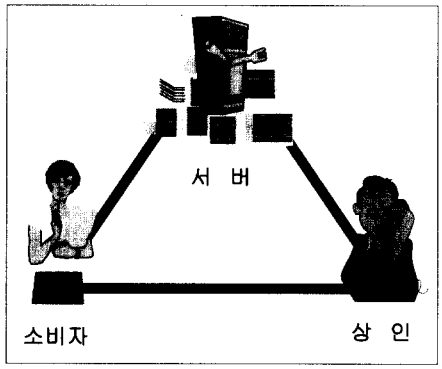
3.1 화폐기능의 변화

전자화폐의 등장 및 정보 네트워크의 발전은 앞으로 지급 결제의 방식이 유동성있는 교환 형태에서 부(Wealth)의 교환 혹은 부에 관한 정보의 교환 형태로 바뀌게 될 가능성이 있다.

이러한 관점에서 보면 화폐의 교환결제 기능은 종래 운송 및 우송에 의한 "오프라인 화폐"로부터 통신회선에 의한 "온라인 화폐"를 거쳐 앞으로는 네트워크의 고유 기능과 결합하여 새로운 부가가치를 창출하는 "네트워크 화폐"로 발전하게 된다고 볼 수 있다. 화폐의 가치저장 기능 측면에서 볼 때 화폐는 단순히 명목 가치를 표시하는 "상징 화폐"(symbol money)로부터 현금 흐름과 결합된 "알고리즘 화폐"(algorithm money)로, 나아가서는 자산의 포트폴리오화 과정에서 시장 환경에 적응하여 수익 추구 및 위험 회피를 목적으로 스스로 최적 자산으로의 가치 극대화를 도모한다는 의미에서의 "인텔리전트 화폐"(intelligent money)로 발전하고 있다고 볼 수 있다.

3.2 전자지불 시스템의 구성 요소

전자지불 시스템은 암호기술을 이용한 보안 시스템의 일종으로 일반적인 보안 시스템과는 몇 가지 다른 점이 있다. 우선 일반적인 보안 시스템은 두 컴퓨터 또는 당사자간의 보안, 즉 클라이언트 서버 간의 보안, 일대일 보안 등에 이용되는 반면, 전자지불 시스템 보안은 세 개 또는 네 개 부분이 하나의 트랜잭션을 가지고 일관성있게 처리되는 보안 시스



〔그림 2〕 전자지불 시스템의 구성요소
〔Fig. 2〕 The component of Electronic payment system

템이다. 즉, 사용자, 쇼핑몰, 전자지불 서버, 금융기관 등의 네 부분, 또는 소비자, 상인, 서버(금융기관의 기능을 포함)의 세 부분으로 구성되어 상품을 주문하고 대금을 지불하는 행위에 관여하는데 본 논문에서는 그림 2와 같이 세 구성 요소로 정의한다.

① 지불인(Payer) 또는 소비자(Consumer)
② 영수인(Payee) 또는 상인(Merchant)
③ 재정적 네트워크 또는 은행에 해당하는 서버 (Server)

Ⅲ. 침입탐지 전자지불 프로토콜

1. 침입탐지 전자지불 프로토콜의 개요

전자지불 프로토콜은 인터넷 상에서 소비자, 상인, 서버 간의 상품거래 과정을 표현한 규약으로, 소비자-상인간의 거래 과정에서 신용카드 번호, 은행계좌 번호 등의 개인 신상에 대한 비밀 정보가 노출될 위험이 크다. 따라서 전자상거래에서 전자지불 프로토콜은 무엇보다 보안에 대한 대비가 철저해야 한다. 본 논문에서 말하는 침입탐지 기능이란 침입이 발생하였을 때 신속하게 침입을 탐지해 낼 수 있는 기능을 말한다. 따라서 침입탐지 전자지불 프로토콜은 전자지불 프로토콜에 침입탐지 기능을 첨가한 프로토콜이다.

2. 표기법(Notation)

C : 소비자(Customer)
M : 상인(Merchant)

S : 서버(Server)
K_x : x의 공개키
K_x^{-1} : x의 비밀키
{text}K : 키 K로 "text"의 암호화
ID : identify
K_{CM} : 소비자와 상인간의 세션키
K_{MS} : 상인과 서버간의 세션키
K_{CS} : 소비자 서버간의 세션키
RN_N : 생성된 난수(난수의 구분을 위해 아래 첨자 N = 1, 2, 3 .... k로 표기)
PRD : 상품정보 요청 (Product Request Data)
EPO : 전자지불 주문(Electronic Payment Order), 전자상품 주문(Electronic Product Order)
EPREC : 전자지불 영수증(Electronic Payment Receipt)
표기법 "X → Y"는 X가 특정 메시지를 Y에게 보내는 것을 뜻한다.

3. 침입탐지 전자지불 프로토콜

가격 요청 단계와 상품 배달 단계의 프로토콜 내용은 지불 단계에서 중복·표현되므로 지불단계의 프로토콜에 대해서만 서술하고자 한다.

1) 소비자는 자신의 ID를 상인의 공개키로 암호화하여 소비자에게 보낸다.
2) 상인은 자신의 ID와 소비자-상인간의 세션키를 소비자의 공개키로 암호화하여 소비자에게 보낸다.
3) 소비자는 ((전자지불주문과 난수 RN_5)를 소비자의 비밀키로 암호화하고 상인의 공개키로 암호화한 것과 난수 RN_5)를 소비자-상인간의 세션키로 암호화하여 상인에게 보낸다.
4) 상인는 자신의 ID를 서버의 공개키로 암호화하여 서버에게 보낸다.
5) 서버는 자신의 ID와 상인-서버간의 세션키를 상인의 공개키로 암호화하여 상인에게 보낸다.
6) 상인은 ((소비자의 비밀키로 암호화한 전자지불 주문과 난수 RN_6)을 상인의 비밀키로 암호화하고 서버의 공개키로 암호화한 것과 난수 RN_6)을 상인-서버간의 세션키로 암호화하여 서버에게 보낸다.
7) 서버는 자신의 ID를 소비자의 공개키로 암호
8) 소비자는 자신의 ID와 소비자-서버간의 세션키를 서버의 공개키로 암호화하여 서버에게 보낸다.
9) 서버는 ((전자지불 영수증과 난수 RN_7)을 서버의 비밀키로 암호화하고 상인의 공개키로 암호화한 것과 난수 RN_7)을 상인-서버간의 세션키로 암호화하여 상인에게 보낸다.
10) 상인은 ((서버의 비밀키로 암호화한 전자지불 영수증과 난수 RN_8)을 상인의 비밀키로 암호화하고 소비자의 공개키로 암호화한 것과 난수 RN_8)을 다시 상인-소비자간의 세션키로 암호화하여 소비자에게 보낸다.

〔표 1〕 제안한 침입탐지 전자지불 프로토콜
〔Table 1〕 suggest on intrusion-detectioned electronic payment protocol

1. 가격요청 단계
 1) $C \rightarrow M : \{ ID_C \}K_M$
 2) $C \leftarrow M : \{ ID_M, K_{CM} \}K_C$
 3) $C \rightarrow M : \{\{ PRD, RN_1 \} K_C^{-1} \} K_M, RN_1 \} K_{CM}$
 4) $C \leftarrow M : \{\{ PRD, RN_2 \} K_M^{-1} \} K_C, RN_2 \} K_{CM}$
2. 상품배달 단계
 1) $C \rightarrow M : \{ ID_C \}K_M$
 2) $C \leftarrow M : \{ ID_M, K_{CM} \}K_C$
 3) $C \rightarrow M : \{\{ EPO, RN_3 \} K_C^{-1} \} K_M, RN_3 \} K_{CM}$
 4) $C \leftarrow M : \{\{ EPO, RN_4 \} K_M^{-1} \} K_C, RN_4 \} K_{CM}$
3. 지불 단계
 1) $C \rightarrow M : \{ ID_C \}K_M$
 2) $C \leftarrow M : \{ ID_M, K_{CM} \}K_C$
 3) $C \rightarrow M : \{\{ EPO, RN_5 \} K_C^{-1} \} K_M, RN_5 \} K_{CM}$
 4) $M \rightarrow S : \{ ID_M \}K_S$
 5) $M \leftarrow S : \{ ID_S, K_{MS} \}K_M$
 6) $M \rightarrow S : \{\{ EPO \}K_C^{-1}, RN_6 \} K_M^{-1} \} K_S, RN_6 \} K_{MS}$
 7) $C \leftarrow S : \{ ID_S \}K_C$
 8) $C \rightarrow S : \{ ID_C, K_{CS} \}K_S$
 9) $M \leftarrow S : \{\{ EPREC, RN_7 \} K_S^{-1} \} K_M, RN_7 \} K_{MS}$
 10) $C \leftarrow M: \{\{\{ EPREC \}K_S^{-1}, RN_8 \} K_M^{-1} \} K_C, RN_8 \} K_{CM}$

Ⅳ. 침입탐지 칼라 페트리 네트

1. 침입탐지 칼라 페트리네트의 정의

칼라 페트리 네트(CPN : Colour Petri Net)는 덴마크의 Hartmann Genrich와 Kurt Lautenbach에 의해 개발된 서술/전이(Predicate/Transition) 네트로부터 유래된 것으로, 시스템의 설계, 사양, 시뮬레이션, 검증을 위한 그래픽 기반 언어로서 특히, 통신과 동시성을 갖는 수많은 프로세스들로 구성되는 시스템에 적절하다. 대표적인 응용 영역으로는 통신 프로토콜, 분산 시스템, 자동화된 생산 시스템,

작업 흐름 분석, 그리고 VLSI 칩 등으로 다양하다.[8]

일반 페트리 네트는 유형도 없고, 모듈도 없이 단지 한 종류의 토큰만을 가지는 단조로운 형태임에 비해, 칼라 페트리 네트는 여러 데이터 유형과 복잡한 데이터 조작이 가능하다. 곧, 칼라 페트리 네트에서는 각 토큰이 토큰 칼라라 불리는 데이터 값을 접근할 수 있으며, 토큰 칼라는 발생되는 전이에 의해 조사될 수도 있고 변조될 수도 있다. 또한 CPN은 계층적 기술이 가능하여 거대한 모델은 서브 모델들의 집합을 결합하도록 할 수 있다.

본 논문에서 정의하고 제안한 침입탐지 칼라 페트리 네트는 칼라 페트리 네트에 침입탐지 기능을 첨가하여 정확히 침입을 탐지하여 순간 순간 경보를 발생할 수 있는 CPN을 말한다.

<정의 1>

침입탐지 칼라 페트리 네트(IDCPN: Intrusion Detectioned Colour Petri Net)는 다음 튜플로 구성된다.

IDCPN=(Σ, P, T, A, N, C, G, E, I, D)

- Σ : 칼라 집합으로 불리는 유한 집합
  Colour DATA=string
  Colour UE =K(DATA)
  Colour RE =K^{-1}(DATA)
  Colour URE =$K_1(K_2^{-1}$(DATA))
  Colour SURE=$K_S(K_1(K_2^{-1}$(DATA))
- P : place를 나타내며, 본 논문에서는 타원형과 원형으로 나타낸다.
- T : 전이(Transition)를 나타내며, 본 논문에서는 직사각형으로 나타낸다.
- A : arc는 전이의 흐름을 나타내는 것으로 → 표로 표현한다. [P∩T=P∩A=T∩A=∅]
- N : 노드 함수로서, A → P×T∪T×P
- C : 칼라 함수로서, P → Σ
- G : guard 함수로서, T → 수식 ∀t∈T : [Type(G(t))=Bool∧Type(Var(G(t)) ⊆Σ]
- E : arc 수식 함수로서, A → 수식 ∀a∈A : [Type(E(a))=C(p(a))$_{MS}$∧Type (Var(E(a))⊆Σ]
  여기서 p(a)는 N(a)의 place이며, C_{MS}의 MS는 C에 대한 모든 multiset의 집합을 말한다.
- I : 초기화 함수로서 P → 닫힌 수식, ∀p∈P : [Type(I(p))=C(p)$_{MS}$]
- D : T → ΣR_0, 전이 t의 점화할 때까지의 시간

2. 침입탐지 칼라 페트리네트의 전이 규칙

<정의 2>

한 전이 단계는 binding 요소들의 multi-set으로 정의한다. binding이란 각 전이의 변수에 칼라를 할당하는 것으로, binding 요소는 (t, b)의 쌍으로 표현한다. 여기서 t는 전이를, b는 t의 변수들에 대한 binding을 말하며, 예를 들면 (T_2,〈X=P, I=2〉)로 표현할 수 있다.

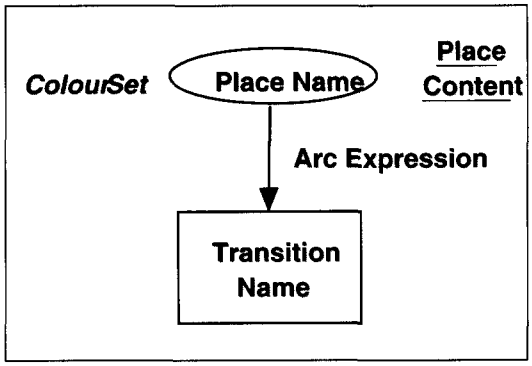
- 한 전이 단계 Y가 마킹 M에서 가능한 필요충분조건은 ∀p∈P : [$\sum_{(t,b)\in Y}$ E(p,t)〈b〉≤M(P)]
- 한 전이 단계 Y가 마킹 M_1으로 가능할 때, 마킹 M_1은 또다른 마킹 M_2로 바뀌면서 다음과 같이 정의된다.
  ∀p∈P : [$M_2(P)=M_1(P)-\sum_{(t,b)\in Y} E_{(p,t)}\langle b\rangle+\sum_{(t,b)\in Y} E(t,p)\langle b\rangle$]

여기서 첫 번째 합계는 제거된 토큰으로 불리며, 두 번째 합계는 추가된 토큰으로 불린다. 더욱이 M_2는 단계 Y의 발생으로 인해 M_1으로부터 직접 도달가능하다고 말할 수 있다 : $M_1[Y > M_2$.

- 전이의 발생 순서는 마킹과 단계의 순서이다.
  $M_1[Y > M_2\ [Y_2 > M_3 \ldots M_n[Y_n > M_{n+1}$.
  그러므로 모든 i∈1 ... n에 대해 $M_i[Y_i > M_{i+1}$으로 표현할 수 있다. 이 때 M_{n+1}은 M_1으로부터 도달가능하다고 말한다. 따라서 M[Y>는 M으로부터 도달가능한 마킹의 집합을 나타낸다.

3. 침입탐지 칼라 페트리 네트의 전이 규칙에 대한 정의

앞으로 침입탐지 칼라 페트리 네트에서 표현되는 place와 arc, 그리고 전이를 나타내는 표현은 다음과 같이 사용하도록 한다. 다음 그림 3에서 place 내용은 토큰 칼라의 내용을 말하며, colour set은 토큰의 유형을 말하는데 본 논문에서 제안된 침입탐지 칼라 페트리 네트에서는 〈정의 1〉에서와 같이

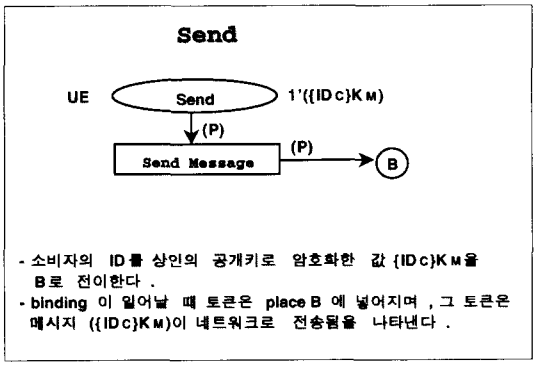


〔그림 3〕 침입탐지 칼라 페트리네트의 표현
〔Fig. 3〕 expression of intrusion-detectioned coloured petrinet

DATA, UE, RE, URE, SURE의 *colour*가 있다. Arc expression은 전이 흐름의 변화가 필요할 때 조건식으로 표현되며, Transition은 사건을 나타내는 전이로 Guard 함수로서 나타낸다.

<정의 3>

Send place에 있는 데이터가 Send Message 전이를 통해 버퍼로 전송됨을 정의한다.



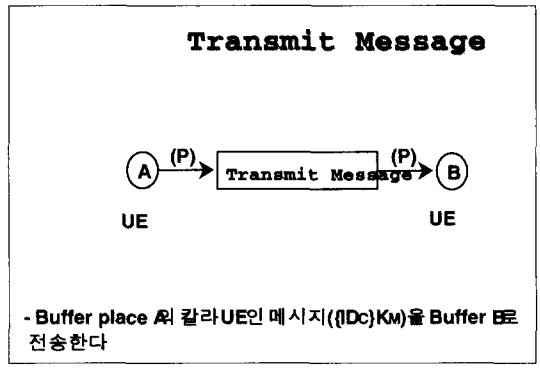
〔그림 4〕 Send Message 전이
〔Fig. 4〕 Send Message transition

<정의 4>

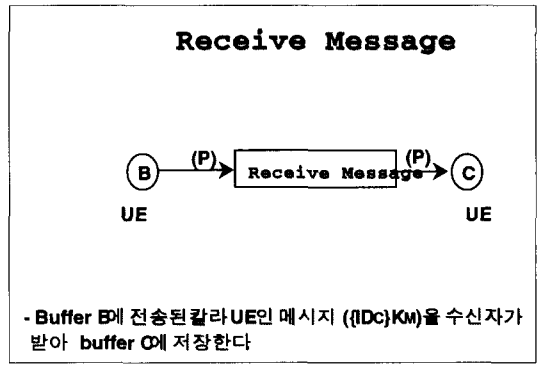
Transmit Message 전이는 버퍼에 저장되어 있는 데이터를 또다른 버퍼로 전송하는 사건으로 정의한다.

<정의 5>

Receive Message 전이는 버퍼에 전송된 데이터를 수신자가 받아서 버퍼에 저장하는 전이로 정의한다.



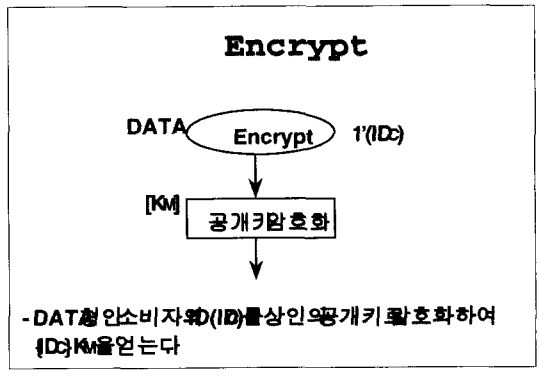
〔그림 5〕 Transmit Message 전이
〔Fig. 5〕 Transmit Message transition



〔그림 6〕 Receive Message 전이
〔Fig. 6〕 Receive Message transition

<정의 6>

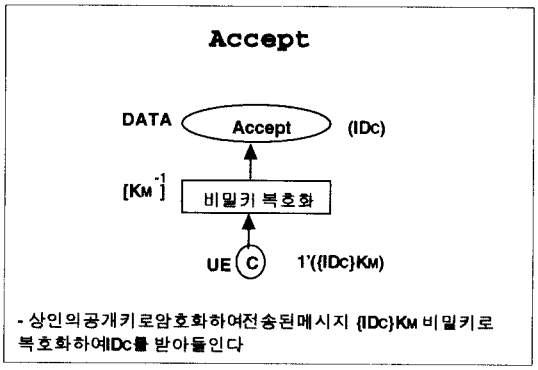
공개키 암호화 전이는 입력 데이터를 공개키로 암호화하는 전이로 정의한다.



〔그림 7〕 공개키 암호화 전이
〔Fig. 7〕 public-key encrypted transition

<정의 7>

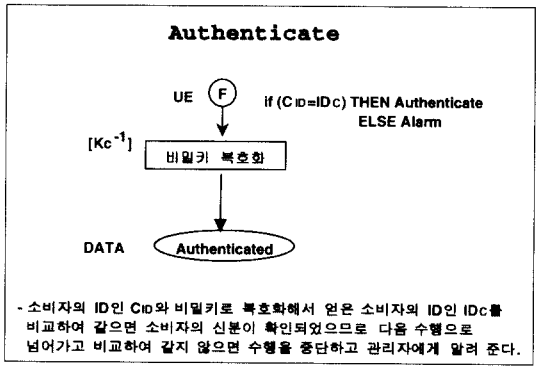
비밀키 복호화 전이는 입력되는 데이터를 비밀키로 복호화하는 전이로 정의하며, Accept는 복호화된 데이터를 받아들이는 것으로 정의한다.



(그림 8) 비밀키 복호화 전이와 accept
(Fig. 8) secret-key decrypted transition and accept

<정의 8>

Authenticate는 Authenticate 이전 arc 표현식에서 조건이 True이면 Authenticate place로 전이가 일어나고, False이면 Alarm으로 정의한다.



(그림 9) 인증
(Fig. 9) Authenticate

4. 침입탐지 칼라 페트리 네트를 이용한 침입탐지 전자지불 프로토콜의 분석

침입탐지 칼라 페트리 네트는 시스템의 설계, 사양, 시뮬레이션, 검증을 위한 그래픽 기반 언어인 칼라 페트리 네트에 침입탐지 기능을 첨가하므로써 순간 순간 침입이 일어날 때마다 침입을 탐지하여 경보를 발생할 수 있는 모델링 도구이다. 이 절에서는 칼라 페트리 네트를 이용하여 데이터 유형에 따라 다음과 같이 5 개의 칼라와 1 개의 변수를 사용하여 프로토콜을 분석하므로서 한 전이가 일어날 때마다 칼라의 변화를 통해 어떤 데이터 유형이 전이의 흐름에 따라 어떤 데이터 유형으로 변하는지 쉽게 분석·확인할 수 있다.

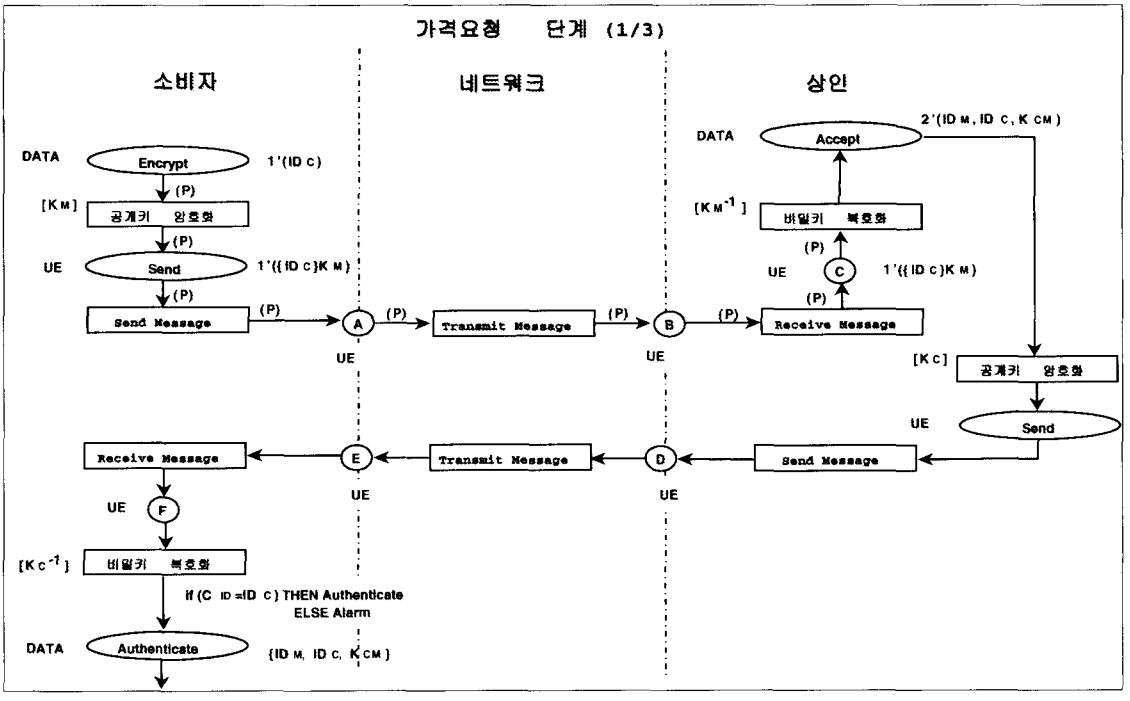
▶ 침입탐지 칼라 페트리 네트에서 정의된 칼라와 변수

Colour DATA =String;
Colour UE =K(DATA);
Colour RE =K^{-1}(DATA);
Colour URE =$K_1(K_2^{-1}(DATA))$;
Colour SURE=$K_S(K_1(K_2^{-1}(DATA)))$;
Var P : DATA;

칼라 페트리 네트의 이점을 살펴보면 다음과 같다.

① 칼라 페트리 네트는 그래픽 표현이 가능하다.
② 칼라 페트리 네트는 각 행위를 명백하게 정의하는 잘 정의된 semantics이다.
③ 칼라 페트리 네트는 매우 일반적이며, 매우 다양한 여러 시스템을 설명하는데 사용할 수 있다.
④ 칼라 페트리 네트는 매우 적은 수의 강력한 프리미티브(primitive)를 지닌다.
⑤ 칼라 페트리 네트는 상태와 활동에 대해 명백한 설명을 해준다.
⑥ 칼라 페트리 네트는 삽입 대신 진정한 병행성에 기초한 semantics를 지닌다.
⑦ 칼라 페트리 네트는 계층적 서술이 가능하다.
⑧ 칼라 페트리 네트는 데이터 처리 과정과 제어, 동기화에 대한 모든 서술을 통합하여 서술한다.
⑨ 칼라 페트리 네트는 모델 시스템에 대한 미세한 변화에 대해 안정적이다.
⑩ 칼라 페트리 네트는 CPN 도형에 직접적으로 결과가 나타나므로 상호작용하는 시뮬레이션을 제공한다.
⑪ 칼라 페트리 네트는 칼라 페트리 네트의 속성이 증명될 수 있으므로 수많은 정형 분석 방법을 지닌다.
⑫ 칼라 페트리 네트는 그림과 시뮬레이션 및 정형 분석을 지원하는 컴퓨터 도구를 지닌다.[8]

이상과 같은 여러 이점들을 지닌 칼라 페트리 네트를 이용하여 제 Ⅲ 장에서 제안한 침입탐지 전자지불 프로토콜을 분석하여 보기로 한다.



〔그림 10〕 가격요청 단계(1/3)
〔Fig. 10〕 price request stage(1/3)

그림 10의 가격요청 단계(1/3)는 네트워크 상에서 소비자와 상인간의 상호인증 과정을 보여주는 침입탐지 칼라 페트리 네트이다. 앞에서 정의한대로 원형과 타원형 모양은 place를, →는 arc를, 직사각형은 전이를 나타낸다.

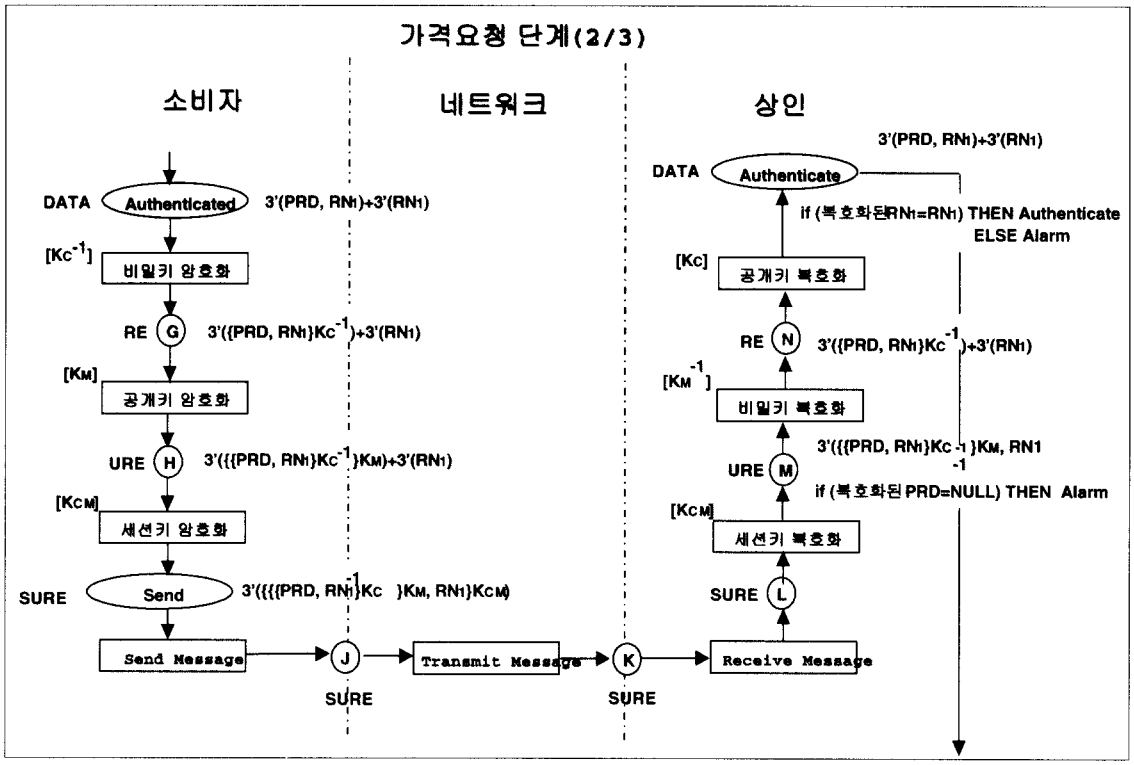
우선 place "Encrypt"로부터 →의 흐름에 따라 전이의 과정을 순서대로 검토해 보기로 하자. place "Encrypt"의 초기 데이터 내용은 ID_C로 소비자의 ID를 나타내며, 이는 string으로서 칼라를 DATA로 할당한다. 다음 공개키로 암호화하는 전이가 이루어지면, 데이터 내용은 $\{ID_C\}K_M$으로 칼라도 UE형으로 변화된다. 따라서 다음의 place "send"의 내용은 $\{ID_C\}K_M$이며, UE 칼라이다

"Send message" 전이는 공개키로 암호화된 데이터인 $\{ID_C\}K_M$을 버퍼 A로 보낸다. 따라서 버퍼 A의 칼라는 UE이며, 데이터 내용은 $\{ID_C\}K_M$이다.

"Transmit message" 전이는 공개키로 암호화된 데이터를 네트워크 상에서 전송하는 전이로 버퍼 A에서 버퍼 B로 전송된다. 따라서 place B의 데이터 내용은 $\{ID_C\}K_M$이고, 칼라는 UE 형이다. "Receive message" 전이가 수행되면 네트워크를 통해 전송된 데이터를 수신하며, place C의 데이터는 $\{ID_C\}K_M$이고 칼라도 UE 형이다.

다음 전이인 비밀키 복호화는 M의 공개키로 암호화된 ID_C를 M만이 알고 있는 M의 비밀키로 복호화하는 수행으로 소비자가 ID_C임을 인증한다. 따라서 이 전이를 수행하고 나면 데이터는 ID_C로 바뀌고, 데이터 칼라도 DATA 형으로 변한다. place "Accept"에서는 칼라가 DATA 형인 ID_M과 ID_C, KC_M을 가지고 있다. 공개키로 암호화하는 전이가 이루어지면 ID_M과 ID_C, 그리고 소비자-상인간의 세션키 KCM을 소비자의 공개키로 암호화한다. 따라서 Send에는 공개키로 암호화된 데이터 $\{ID_M, ID_C, K_{CM}\}K_C$가 저장되며, 칼라는 UE 형이다.

다음 전이 "Send message"는 Send의 데이터를 버퍼 D로 보내며, 칼라는 UE형이다. "Transmit message" 전이가 수행되면, 버퍼 D의 데이터가 버퍼 E로 전송되며 칼라는 그대로 UE 형이다. "Receive message" 전이가 수행되면, 전송된 버퍼 E의 데이터가 버퍼 F로 $\{ID_M, ID_C, K_{CM}\}K_C$가 저장되고 칼라는 그대로 UE 형이다. 비밀키 복호화 전이는 공개키로 암호화되어 전송된 데이터를 소비자의 비밀키로 복호화하는 수행을 말하며, 데이터 $\{ID_M, ID_C, K_{CM}\}$를 얻으며 다음 place의 칼라는 DATA 형이 된다.

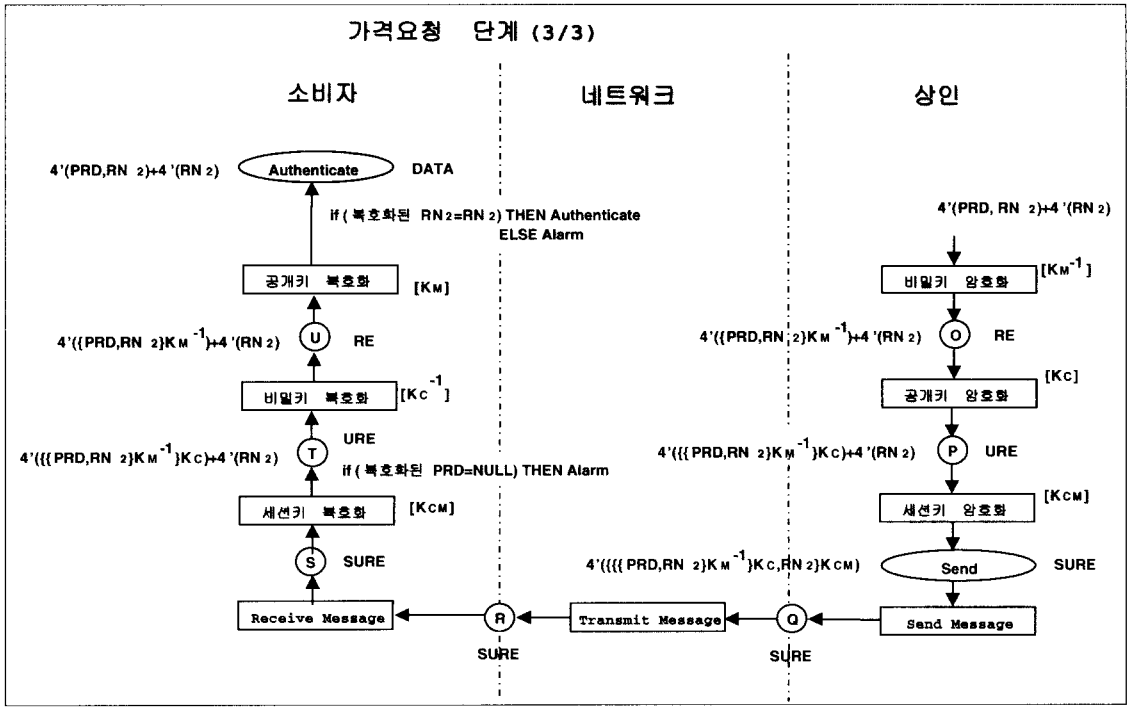


〔그림 11〕 가격요청 단계(2/3)
〔Fig. 11〕 price request stage(2/3)

arc 표현식 IF (C_{ID}=ID_C) THEN Authenticates ELSE Alarm은 소비자 자신의 ID인 C_{ID}와 복호화되어 보내진 ID인 ID_C를 비교하여 같으면, 상호간의 인증이 모두 끝나 다음 수행을 계속하고 같지 않으면 수행을 중단하고 관리자에게 침입이 일어났음을 경보해 준다. 여기서 우리가 주목해야 할 것은 각 전이가 일어날 때마다 데이터의 변화와 칼라의 변화를 명백히 알 수 있으므로 정확한 분석이 가능하다는 점이다.

그림 11의 가격요청 단계(2/3)는 네트워크 상에서 소비자가 상인에게 상품정보를 요청하는 과정을 보여주는 침입탐지 칼라 페트리 네트이다. 앞의 그림 10의 가격요청 단계(1/3)의 상호인증 과정이 끝난 후 Place는 "Authenticate"로서 칼라는 DATA 형이며, 데이터는 상품정보 요청을 나타내는 PRD와 임의로 발생하는 난수 RN_1이 있다. PRD와 RN_1을 소비자의 비밀키로 암호화하여 버퍼 G에 저장하면 칼라는 RE 형이 되고, 데이터는 $\{PRD, RN_1\}K_C^{-1}$과 난수 그대로인 RN_1이 있다. 이를 다시 상인의 공개키로 암호화하여 버퍼 H에 저장하면 칼라는 URE 형이 되고, 데이터는 $\{\{PRD, RN_1\}K_C^{-1}\}K_M$과 난수 그대로인 RN_1이 있다. 이들 두 값을 소비자-상인간 의 세션키로 암호화하여 저장하면 칼라는 SURE 형이고 데이터는 $\{\{\{PRD, RN_1\}K_C^{-1}\}K_M, RN_1\}K_{CM}$이 된다.

PRD와 RN_1이 비밀키로 암호화되고 공개키로 암호화된 후, 다시 RN_1과 함께 세션키로 암호화된 SURE 형의 데이터가 "Send Message" 전이에 의해 버퍼 J로, "Transmit Message" 전이에 의해 버퍼 J로부터 버퍼 K로 전송되고, "Receive Message" 전이에 의해 버퍼 L에서 수신한다. 이 SURE 형의 데이터를 세션키로 복호화하면 칼라는 URE 형이 되며, 데이터는 $\{\{PRD, RN_1\}K_C^{-1}\}K_M$과 RN_1이 된다. 이 때 복호화된 PRD의 값이 NULL이면 삭제 공격이 발생하였으므로 관리자에게 경고하고, 아니면 상인의 비밀키로 복호화하여 $\{PRD, RN_1\}K_C^{-1}$과 RN_1을 얻으며 칼라는 RE 형이 된다. 이를 다시 소비자의 공개키로 복호화하여 칼라가 DATA인 PRD와 RN_1을 얻게 되며, 이 복호화된 RN_1과 세션키로 복호화되었을 때 얻어진 RN_1과 비교하여 같으면 침



〔그림 12〕 가격요청 단계(3/3)
〔Fig. 12〕 price request stage(3/3)

입이 없는 것으로 판단하고, 같지 않으면 침입이 발생한 것으로 판단하여 관리자에게 경고한다. 이로서 가격요청 단계의 품정보 요청 과정이 이루어졌다. 이와 똑같은 방식으로 다음의 그림 12도 설명될 수 있으며, 이후 계속되는 상품배달 단계와 지불 단계는 생략하기로 한다.

V. 침입탐지 전자지불 프로토콜의 검증

본 장은 Ⅲ 장에서 제안된 침입탐지 전자지불 프로토콜을 BAN 논리 시스템과 Kailar 논리 시스템에 적용시켜 프로토콜의 정당성을 확인하고자 한다.

1. BAN 논리 시스템

BAN 논리에 사용하는 체계는 주어진 논리가 L이라고 가정하면, 논리 L에 몇 가지 제한을 가하게 된다. 우선 논리의 수식은 다음과 같은 최소한의 집합이다.

- V는 어떤 변수 V에 대한 논리식이며,
- F_1, ..., F_n이 논리식이고 S가 기능 부호라면, $S(F_1, ..., F_n)$도 하나의 논리식이다($n \geq 0$).
- 상수는 독립변수 없이 함수 기호로써 나타낼 수 있다.

다음은 BAN 논리의 추론 규칙을 세 가지 유형으로 분리하고자 한다.

1) S 규칙(Shrinking rule)

축소 규칙인 S 규칙은 $\{P_1, ..., P_n\}$이라는 전제(premise) 집합으로 구성된다. 또한, 결론 C도 유효한 논리식이다. 결론은 잘 정립된 척도에 의해 전제보다 작거나 똑같은 크기임에 틀림없다. 또한 결론에서 나타나는 각 변수는 하나 혹은 그 이상의 전제에 존재한다.

2) G 규칙(Growing rule)

확대 규칙인 G 규칙은 S 규칙과 형태가 같으나, 결론은 동일한 척도에 의하여 각 전제들에 비해 크다. 또, 전제에 존재하는 각 변수는 결론에도 존재한다.

3) 바꿔쓰기(Rewrites)

바꿔쓰기는 한 쌍의 논리식을 만들며, BAN 함수 중 일부의 함수가 수학에서 사용되는 교환법칙이나 결합법

칙을 사용하여 한 쌍의 논리식을 만들 수 있다. 한 쌍의 논리식은 똑같은 크기이며, 동일한 변수를 포함한다.

마지막으로, 모든 G 규칙의 결론과 대응하는 S 규칙의 전제들이 모두 삭제될 때 각각의 S 규칙이 자체 규칙의 기준을 충족시켜야 한다. BAN 이론에서는 이것을 S/G 한정이라고 부르고 있다. 왜냐하면, S, G 규칙이 서로 상호작용할 수 있는 방식을 포함하기 때문이다. 반면에 또 다른 한정 사항들은 개별적 규칙들의 독특한 특성이며, 따라서 각 규칙이 별개로 검사될 수 있다.[3]

2. Kailar 논리 시스템

최근에 Kailar는 전자 상거래 프로토콜의 계정성(accountability) 추론에 관한 단순 논리식을 제시했다.[3,10] 이 논리식의 주요 구성은 다음과 같다.

P CanProve X

이는 당사자 P가 X 이외의 다른 비밀을 누설하지 않은채 X가 보유하는 전제 집합을 공유하려고 하는 청중 가운데 누군가를 확인할 수 있다는 뜻이다. Kailar의 논리식에는 CanProve, IsTrustedOn, Implies, Authenticates, Says, Receives, SignedWith, comma, inv 등의 함수를 사용했다. Kailar 논리식의 네 가지 주요 규칙은 다음과 같다

1) Conjunction

$$\text{Conj: } \frac{\text{CanProve}(P, X),\ \text{CanProve}(P, Y)}{\text{CanProve}(P, \text{comma}(X, Y))}$$

P가 X를 증명할 수 있고, 그리고 P가 Y를 증명할 수 있다.

⇒ P가 X와 Y의 관련체를 증명할 수 있다.

2) Inference

$$\text{Inf: } \frac{\text{CanProve}(P, X),\ \text{Implies}(X, Y)}{\text{CanProve}(P, Y)}$$

P가 X를 증명할 수 있고 , X가 Y를 포함한다.

⇒ P가 Y를 증명할 수 있다.(∵ Y가 X에 포함되므로)

3) 디지털 서명의 계정성 속성

$$\frac{\text{Receives}(P, \text{SignedWith}(M, K^{-1}))}{\text{CanProve}(P, \text{Authenticates}(K, Q))}$$

$$\text{Sign : } \frac{\text{Inv}(K, K^{-1})}{\text{CanProve}(P, \text{Says}(Q, M))}$$

전문 M을 비밀키 K^{-1}을 사용하여 서명한 것을 P가 받아들인다.

키 K를 사용한 것을 Q가 인증하고 이것을 P가 증명할 수 있다.

K와 K^{-1}는 공개키와 비밀키의 쌍이다.

⇒ Q는 전문 M을 전송한다고 P가 증명할 수 있다.

4) 신뢰 관계

$$\frac{\text{CanProve}(P, \text{Says}(Q, X))}{\text{CanProve}(P, X)}$$

$$\text{Trust : } \frac{\text{CanProve}(P, \text{IsTrustedOn}(Q, X))}{\text{CanProve}(P, X)}$$

Q가 전문 X를 송신하고 있다고 P가 증명할 수 있다.

Q가 X를 신뢰하고 있다고 P가 증명할 수 있다.

⇒ P는 전문 X의 내용을 증명할 수 있다.

Conj와 Inf 규칙은 결합 관계와 처음부터 제시한 암시를 사용하도록 허용한다. Sign과 Trust 규칙은 대략적으로 BAN 논리식의 공개키 메시지 의미와 지배 규칙에 상응한다. 또한, 논리식에서 콤마의 교환 법칙과 결합 법칙을 이용한 바꿔쓰기를 활용한다. 이러한 암호화는 어떤 G 규칙도 필요로 하지 않는다.

3. BAN논리를 이용한 제안된 프로토콜의 검증

앞의 표에 제시된 프로토콜의 메시지 중에서 검증의 대상이 되는 메시지는 다음과 같은 4 개의 메시지로 제한한다. 상품배달 단계는 가격요청 단계와 거의 유사한 메시지가 반복되므로 검증 대상에서 제외하였으며, 지불 단계 중에서도 메시지 유형이 다른 메시지 ⑥만을 검증하기로 한다.

<메세지>

① $C \rightarrow M : \{ID_C\ K_M$

Receives(M, SignedWith(ID_C, K_M))

② $C \leftarrow M : \{\ ID_M, K_{CM}\ \}K_C$

Receives(C, SignedWith(Comma(ID_M,

K_{CM}), K_C))

③ C → M : {{PRD, RN_1}K_C^{-1}} K_M, RN_1} K_{CM}
Receives(M, SignedWith (Comma (SignedWith (SignedWith (Comma (PRD, RN_1), K_C^{-1}), K_M), RN_1), K_{CM}))

⑥ M → S : {{{{EPO}K_C^{-1}, RN_6}K_M^{-1}} Ks, RN_6} K_{MS}
Receives(S, SignedWith (Comma (SignedWith (SignedWith (Comma(SignedWith (EPO, K_C^{-1}), RN_6), K_M^{-1}), Ks), RN_6), K_{MS}))

검증의 타당성을 확인하기 전에 다음과 같은 초기 가정을 둔다.

ⓐ CanProve (M, ID_C)
ⓑ CanProve (M, ID_S)
ⓒ CanProve (C, ID_M)
ⓓ CanProve (C, ID_S)
ⓔ CanProve (C, K_{CM})
ⓕ CanProve (M, RN_1)
ⓖ CanProve (M, PRD)
ⓗ CanProve (S, EPO)
ⓘ CanProve (M, EPO)
ⓙ CanProve (S, RN_6)

<메시지 ⑥의 검증>

⑥ Receives (S, ignedWith (Comma (Signed With (SignedWith (Comma(SignedWith(EPO, K_C^{-1}), RN_6), K_M^{-1}), Ks), RN_6), K_{MS}))

(소비자 C의 비밀키로 암호화한 전자지불주문 EPO와 난수 RN_6)을 상인 M의 비밀키로 암호화하고 다시 서버 S의 공개키로 암호화한 것과 난수 RN_6을 상인-서버간의 세션키 K_{MS}로 암호화하여 서버 S에게 보낸다.

→ Kailar의 Sign 규칙에 적용하여 보면 다음과 같이 표현할 수 있다.

SignedWith (EPO ,K_C^{-1}),RN_6)
Receives(P, SignedWith (M , K^{-1}))
CanProve(P, Authenticates(K, Q))
Sign : Inv(K, K^{-1})
CanProve(P, Says(Q, M))

⬇

Receives (S, SignedWith (Comma (SignedWith (EPO, K_{C-1}),RN_6),K_M^{-1}))
CanProve(S, Authenticates(K_M, M))
Sign : Inv(K_M, K_M^{-1})
CanProve(S, Says (M, Comma (SignedWith (EPO,K_C^{-1}),RN_6)))

→ Kailar의 Sign 규칙에 적용한 결과 다음식 ⑥^{1}을 얻는다.

⑥^1 CanProve(S, Says (M, Comma (SignedWith (EPO, K_C^{-1}), RN_6)))

소비자 C의 비밀키로 암호화된 EPO와 RN_6을 M이 전송하고 있다고 S가 확인할 수 있다.

→ 식 ⑥^{1}에 Kailar의 Trust 규칙을 다음과 같이 적용하면 식 ⑥^{2}를 얻을 수 있다.

CanProve(P, Says(Q, X))
Trust : CanProve(P, IsTrustedOn(Q, X)
CanProve(P, X)

⬇

CanProve(S, Says (M, Comma (SignedWith (EPO, K_C^{-1}),RN_6)))
Trust : CanProve (S, IsTrustedOn (M, Comma (SignedWith (EPO, K_C^{-1}), RN_6)))
CanProve(S, Comma (SignedWith (EPO, K_C^{-1}), RN_6))

⑥^2 CanProve(S, Comma(SignedWith(EPO, K_C^{-1}), RN_6))

S는 C의 비밀키로 암호화된 EPO와 RN_6을 확인할 수 있다(왜냐하면, M이 자신만이 아는 비밀키로 암호화하였으므로 C의 비밀키로 암호화된 EPO와 RN_6을 신뢰하고 있다고 S가 증명할 수 있기 때문이다.).

→ 식 ⑥^{2}에 BAN 논리의 메시지 요소 추출을 위한 S 규칙 ③을 다음과 같이 적용하면 식 ⑥^{3}을 얻을 수 있다.

believes(P, public_key(K, Q))
sees(P, encrypt(X, K_{-1}, R))
inv(K, K^{-1})
distinct(P, R)

sees(P, X)
⬇
believes(S, public_key(Kc, C))
sees(S, encrypt(EPO, Kc^{-1}, M))
inv(Kc, Kc^{-1})
distinct(S,M)
Sees(S, EPO)

식 ⑥^3 CanProve(S,Comma(EPO,RN_6))
EPO와 RN_6를 전송한다고 S가 증명할 수 있다.

- BAN 논리의 메시지 요소 추출을 위한 S 규칙 ⑤를 식 ⑥^{3}에 다음과 같이 다시 적용하면 두 식 ⑥^{4}와 ⑥^{5}를 얻을 수 있다.

sees(P,comma(X,Y))
Sees(P,X)
↙
CanProve(S, Comma(EPO, RN6))
CanProve(S, EPO)
↘
CanProve(S, Comma(EPO, RN_6))
CanProve(S, RN_6)

⑥^4 CanProve(S, EPO)

서버 S는 전자지불 주문인 EPO를 확인할 수 있다. 이는 초기 가정 ⓗ와 일치하므로 검증되었음을 알 수 있다.

⑥^5 CanProve(S, RN_6)

서버 S는 난수 RN_6을 확인할 수 있다.

이상으로 침입탐지 전자지불 프로토콜 중 메시지 ⑥에 대해 BAN 논리와 Kailar 논리의 규칙 적용을 통하여 검증하였다. 각 메시지의 최종 식에서 얻은 결론은 Kailar 논리가 초기 가정에서 제시하는 식과 일치하므로, 이것을 통하여 제안한 프로토콜에 대한 검증이 정확히 이루어졌음을 알 수 있다.

〔표 2〕 NetBill 프로토콜
〔Table 2〕 NetBill protocol

1. 가격요청 단계
1) C ⇒ M : T_{CM}(Identity), E_{CM}(Credentials, PRD, Bid, RequestFlags, TID)
2) M ⇒ C : E_{CM}(ProductID, Price, RequestFlags, TID)
2. 상품배달 단계
3) C ⇒ M : T_{CM}(Identity), E_{CM}(TID)
4) M ⇒ C : E_K(Goods), E_{CM}(CC(E_K(Goods)),EPOID)
3. 지불 단계
5) C ⇒ M : T_{CM}(Identity), E_{CM}([EPO]C)
6) M ⇒ N : TMN(M), EMN([[EPO]C, MAcct, MMemo, K]M)
7) N ⇒ M : EMN([Receipt]N-DSA, ECN(EPOID, CAcct, Bal, Flags))
8) M ⇒ C : ECM ([Receipt]N-DSA, ECN(EPOID, CAcct, Bal, Flags))

Ⅵ. 기존의 전자지불 프로토콜과 제안한 프로토콜의 비교

기존의 전자지불 프로토콜과 본 논문에서 제안하는 침입탐지 전자지불 프로토콜에 대한 보안성을 비교하고자 한다. 기존의 전자지불 프로토콜의 대표적인 것으로는 NetBill 프로토콜로서 1996년 카네기 멜론 대학에서 개발하여 상용화를 위해 테스트 중이다.

전자지불 프로토콜에 요구되는 보안 요구 사항은 정당한 사용자인지의 여부를 판단하는 신분확인 기능과 각 사용자의 키 분배에 대한 보안성을 높이기 위해 사용자를 인증할 때 사용자의 비밀 정보가 노

〔표 3〕 Netbill과 제안한 프로토콜의 비교
〔Table 3〕 comparison of Netbill and suggested protocol

항목	NetBill	제안한 프로토콜
인증 방식	커버러스 방식	공개키 방식
침입 탐지	상호인증에 의해 세션키를 공유한 이후 특별한 방법을 사용하지 않음.	- 상호인증에 의해 세션 키를 공유한 이후에도 난수를 발생시켜 침입의 여부를 판정한다. - 송신자의 비밀키로 암호화한 난수와 암호화하지 않은 난수를 동시에 전송한다. - 수신자는 송신자의 비밀키로 암호화한 난수를 송신자의 공개키로 복호화하고 그 결과와 암호화하지 않고 보낸 자료를 비교한다. - 비교 결과가 틀리면 침입으로 판정한다.

출되지 않는 인증 방식을 키 분배 프로토콜에 적용시키고자 하는 키 분배 기능과 불법 공격자로부터 침입이 발생하였을 때 이를 탐지해 낼 수 있는 기능이 있다.

표 2는 NetBill 프로토콜을 나타낸 것이며, 표 3은 NetBill과 제안한 프로토콜을 비교한 결과이다. NetBill은 커버러스 인증 방식을 사용하는데 비해 제안한 프로토콜은 공개키 방식을 사용한다. 또한 NetBill은 침입 여부의 판정 기능이 없지만 제안한 프로토콜은 침입의 여부를 판정하는 기능을 갖는다.

Ⅶ. 결 론

본 논문은 인터넷 상에서 전자상거래가 이루어지는데 필수적으로 요구되는 보안성을 강화하기 위해 침입탐지 전자지불 프로토콜을 제안하였다. 제안한 침입탐지 기능이란 정보 전송이 이루어지는 매 순간마다 침입이 발생하였는지 탐지하여 관리자에게 알려주도록 하므로써 신속한 탐지가 이루어지도록 하는 기능을 말한다. 제안된 침입탐지 전자지불 프로토콜의 정확성, 타당성, 안전성 등을 분석하기 위해 페트리네트와 CPN(Coloured Petri Net)을 이용하여 모델링하였으며, BAN 논리 시스템과 Kailar 논리 시스템을 이용하여 제안된 프로토콜을 검증하였다.

참 고 문 헌

[1] Bell, D.E., and LaPadula, L.J., "Secure Computer Systems: A Mathematical Model", MTR-2547, Vol. II, The MITRE Corporation, Bedford, Massachusetts, 31 May 1973.

[2] Benjamin Cox, J.D. Tygar, Marvin Sirbu, "NetBil Security and Transaction Protocol", In Proceedings of the First USENIX Workshop in Electronic Commerce, July 1995.

[3] D. Kindred and J. M. Wing, "Fast, Automatic Checking of Security Protocol", Carnegie Mellon University, 1996.

[4] Dorothy E. Denning, "An Intrusion Detection Model", In IEEE Transactions on Software Engineering, Number 2, Feburary 1987.

[5] E. Gabber and Abraham Silberschatz, "Agora : A Minimal Distributed Protocol for Electronic Commerce", Proceedings of the Second USENIX Workshop on Electronic Commerce, Oakland, California, November, 1996.

[6] J. D. Tygar, J. Wing, H. Chi Wong, "Model Checking Electronic Commerce Protocols", Neivin Heintze, Bell Labs, Carnegie Mellon University, 1996.

[7] K. Jensen, G. Rozenberg, "High-level Petri net : Theory and Application", Springer-Verlag, 1991.

[8] K Jensen, "Coloured Petri Nets : Basic Concepts, Analysis Methods and Practical Use", Volume 1, Springer, 1997.

[9] N. Heintze, J. D. Tygar, J. Wing, H. C.Wong, "Model Checking Electronic Commerce Protocols", This work was supported in part by Defence Advanced Research Project Agency (ARPA), the National Science Foundation(NSF), and by the US Postal Service, 1996.

[10] Rajashekar Kailar, "Accountability in electronic commerce protocols" , IEEE Transactions on Software Engineering, 22(5) : pp.313-328, May ,1996.

[11] R. A. Kemmerer and S. T. Eckmann, "A User's Manual for the UNISEX System", Dept. of Computer Science, UCSB, 1983.

[12] R. S. Rivest, A. Shamir, "Payword and Micromint: Two Simple Micropayment Schemes", MIT Lab. for Computer Science, & Weizemann Institute of Science, Applied Mathematics Dep. Rehovot, Israel, International Workshop Cambridge, United Kingdom, April 10-12, 1996.

[13] Sandeep Kumar Eugene H. Spafford, "An Application of Pattern Matching in Intrusion Detection" June 7, 1994.

[14] T. P. Pedersen, "Electronic Payments of Small Amounts", Cryptomathic, Den-

mark, International Workshop Cambridge, United Kingdom, April 10-12, 1996.
〔15〕 이와사키 가즈오, 사토 모토노리 공저, 김현일 옮김, "전자화폐 전쟁", 전자신문사, 1995. 11.
〔16〕 탁승호, "전자화폐와 결제 시스템", 더뱅커사, 1996.2.

〈著者紹介〉

유 은 진 (Eun-Jin Yu) 정회원
1977년 2월 : 숭실대학교 전자계산학과 졸업
1980년 2월 : 숭실대학교 전자계산학과 석사
1998년 2월 : 숭실대학교 전자계산학과 박사
1998년 3월 ~ 현재 : 숭실대학교, 서울산업대학교 강사
〈관심분야〉 정보 이론, 인터넷 보안, 침입탐지

전 문 석 (Moon-Seog Jun) 종신회원
1980년 2월 : 숭실대학교 전자계산학과 졸업
1986년 2월 : University of Maryland, Computer Science 석사
1989년 2월 : University of Maryland, Computer Science 박사
1989년 3월 ~ 현재 : 숭실대학교 정보과학대학, 컴퓨터학부 부교수
〈관심분야〉 정보 보안, 인터넷 보안, 침입탐지, 방화벽, 암호화 알고리즘

이 철 희 (Chul-Hee Lee)
1958년 2월 : 육군사관학교 졸업
1962년 2월 : Purdue University 석사
1988년 2월 : 중앙대학교 박사
1988년 3월 ~ 현재 : 숭실대학교 정보과학대학, 컴퓨터학부 명예교수