XML 전자 서명에 기반한 이동 에이전트 시스템 설계

김만수°, 김환조, 정목동
부경대학교 컴퓨터공학과

Design of Mobile Agent System based on XML Digital Signature

Mansoo Kim, Hwanjo Kim, Mokdong Chung
Dept. of Computer Engineering, Pukyong National University.
E-mail : kmansoo@hitel.net, xxrcn11@lycos.co.kr, mdchung@pknu.ac.kr

요 약

Pmart(Pukyong-mart)는 지능형 멀티 에이전트에 바탕을 두고 가격, 상품의 특성, 보장 기간, 서비스 정책 등에 대해서 협상을 벌이는 에이전트 중재에 의한 전자상거래 프레임워크이다. Pmart는 협상 알고리즘, 에이전트 시스템, 웹 서버로 구성되어 판매자 및 구매자 모두 만족할만한 성공적인 거래를 제공하지만 단일 시스템 내에서의 Pmart 서비스는 다양한 거래자를 선택할 수 없다. 본 논문에서는 이러한 Pmart의 단점을 보완한 분산 Pmart 시스템을 제안하고, 이를 위하여 이동 에이전트의 보안 및 전자지불 기능이 추가된 확장 Pmart를 설계한다. 또한 분산된 Pmart 구성에 필요한 XML과 전자서명에 기반한 안전한 이동 에이전트 시스템을 제안한다.

1. 서론

Forrester Research에서 평가하기로는 인터넷을 통한 상품 판매는 1996년에 약 6억불, 1997년에 20억불을 넘어섰고, 2001년에는 170억불에 달할 것으로 전망하고 있다. 이처럼 전자 상거래는 전통적인 경제 행위의 지축을 흔들 정도로 우리의 일상생활에 깊숙이 파고들고 있는 실정이다. 하지만 인터넷 전자상거래의 성공을 위협하는 요소도 여러 가지 있는데 그 중 가장 큰 것은 보안에 관한 것을 것이다. PKI(Public Key Infrastructure)기반의 정보 보호 및 전자결제시스템은 분산된 전자상거래에 있어 안전한 거래와 전자지불시스템을 구현하는데 적합한 것이다. 이와 더불어 XML 기술이 인터넷 e-비즈니스 시스템 등에서 메시지 교환 형식으로 이용되면서 이들 XML 문서의 보안은 필수적 요구조건이 되고 있고, 안전한 전자상거래를 수행하기 위해서 XML 디지털 서명(Digital Signature)은 반드시 지원 되어야 한다 [1][2][3][4][5].

Pmart(Pukyong-mart)[6]는 지능형 멀티 에이전트에 바탕을 두고 가격, 상품의 특성, 보장 기간, 서비스 정책 등에 대해서 협상을 벌이는 에이전트 중재에 의한 전자 상거래 프레임워크이다. 현재 Pmart는 협상 알고리즘, 에이전트 시스템, 웹 서버로 구성되어 판매자 및 구매자 모두 만족할만한 성공적인 거래를 제공하지만, 단일 시스템 내에서의 Pmart 서비스는 다양한 거래자를 선택할 수 없기 때문에 Pmart를 분산된 구조로의 확장이 필수적이다. 이러한 분산 구조 Pmart의 구성은 Pmart간 자율적인 이동형 에이전트의 이동이 보장되어야 하지만 이런 이동형 에이전트는 이동에 따른 인증 및 보안과 더불어 매매 이후의 각 에이전트간의 안전한 전자 결제 기능이 요구된다. 따

라서 본 논문에서는 XML 전자서명에 기반한 이동 에이전트 시스템의 설계를 다룬다.

논문의 구성은 1장 서론에 이어서 2장 관련연구, 3장 시스템 설계, 4장 결론과 향후 연구에 대해서 논한다.

2. 관련연구

2.1 Pmart

Pmart[9]는 본 연구실에서 개발한 다중변수 기반 에이전트 중재 전자상거래 시스템이다. 이 시스템의 프레임워크는 객체지향기법과 소프트웨어 컴포넌트(software component)로 구성되어 소프트웨어 재사용(software reuse) 기능을 제공하고 있다.

Pmart의 협상 모델은 영역 지식과 일반 지식을 동시에 사용할 수 있는데, 영역 지식은 MAUT (Multi-Attribute Utility Theory) [7]에 바탕을 두고 있고 일반 지식은 기존의 구매기록(purchase history)과 간결한 휴리스틱스(simple heuristics) [8]에 바탕을 두고 있다.

Pmart의 협상 모델은 다음과 같다. 상품의 전체 변수에 대해서 협상하는 방법으로 세 가지를 생각할 수 있는데, 첫 번째 접근 방법은 단지 MAUT만 의존하는 방법이다. 두 번째 방법은 MAUT를 먼저 사용하고 몇 번 실패 후에는, 기존의 구매기록과 간결한 휴리스틱스에 의존하는 방법이다. 마지막 방법은 MAUT를 사용하지 않고 바로 구매 기록과 휴리스틱스로 구성된 일반 지식만 사용하는 방법이다.

본 협상 모델에서는 세 가지 방법을 모두 쓸 수 있지만 이 중 두 번째 방법에 초점을 맞추는 이유는 다음과 같다. 첫째, 특수 지식에서 일반 지식으로 추론해 나가는 것은 일반적인 추론 기법에서 보았을 때도 타당성이 있다. 둘째, MAUT 기반 협상을 몇 번 사용 한 다음에도 계속 실패하면 기존의 구매기록과 휴리스틱스에 바탕을 두고 있는 일반 지식 기반 협상에 의존하는 것이 보다 우수해 보이기 때문이다.

2.2 XML 전자 서명(XML Digital Signature)

최근 XML[1]은 B2B와 B2C 등과 같은 기본적인 응용과 더불어 여러 분야에 적용할 수 있는 기술로 각광 받고 있다. 한편 전자상거래 상에서의 대부분의 서비스가 전자적으로 처리됨에 따라 그에 따른 보안의 중요성이 대두되고 있다. 특히, XML을 활용한 전자상거래상의 문서 교환시의 보안에 대한 표준화 작업이 활발히 진행되고 있는데, XML 전자서명은 IETF와 W3C의 XML-Signature Working Group에서 제정된 "XML-Signature Syntax and Processing" 명세서[3]에서 XML 디지털 서명의 구문과 처리 과정을 기술하고 있다.

XML 전자서명을 사용하기 위한 보안관련 고려사항은 다음과 같다.

- 기밀성(Confidentiality): 전송되는 자료의 일부 또는 전부를 제 3자가 볼 수 없도록 하는 기능.
- 인증(Authentication): 사용자 인증은 사용자가 정당한 사용자임을 증명하는 기능.
- 무결성(Integrity): 원격지에서 전송된 문서가 위, 변조되지 않음을 증명하는 기능.
- 승인(Authorization): 거래 요청에 대하여 상대방의 거래를 인증하고 이에 대한 처리 결과를 거래 요청자에게 통보하는 기능.
- 부인방지(Non-Repudiation): 문서를 송, 수신하는 경우 해당자가 송, 수신에 대한 행위를 부인할 수 없도록 하는 기능

SSL[11]은 Netscape사에서 처음으로 제안되었으며, 자사의 웹 어플리케이션에 처음으로 구현함으로써 현재 웹 보안의 대명사로 알려져 있는 보안 프로토콜이다. 그러나 SSL은 웹과 같은 특정 응용을 위한 보안 프로토콜이 아닌 일반적인 인터넷 보안 프로토콜로 사용되며 웹 보안은 HTTP프로토콜을 SSL로 암호화시킨 HTTPS가 사용된다.

SSL은 프로토콜 계층상에서 상호인증, 무결성을 위한 메시지 인증 코드, 기밀성을 위한 암호화 등을 제공함으로써 클라이언트와 서버 사이에 안전한 데이터 통신을 제공하는 반면에 부인방지에 대한 기능은 제공하지 못하고 있다. 반면 XML 전자서명은 이러한 SSL의 부인방지 문제점을 해결하고 있다.

XML 전자 서명 문법에 따른 종류는 다음과 같

이 세가지가 있다

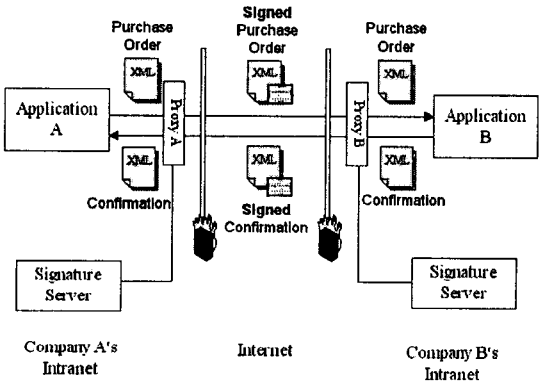
(1) Enveloping Signature: <Signature> 요소가 전송 문서의 최상위 요소에 위치

(2) Enveloped Signature: <Signature> 요소가 XML 문서 내부에 포함되어 하위 요소로 구성

(3) Detached Signature: XML 문서가 전자서명 된 문서와 따로 분리되어 전송

2.3 XML 전자 서명을 사용한 예

일본 IBM 연구소[10] 에서는 Signature/Verification Server를 기존의 두 전자상거래 애플리케이션 사이에 각각 두어 구매 요청서와 같은 XML 문서를 서명된 XML 문서로 변환 한 후에 송/수신 하는 시스템을 제안했다. 그림 1은 제안된 시스템 구성도이다.



[그림 1] 일본 IBM 연구소에서 제안된 애플리케이션들에 투명한 서명 XML 문서 교환 시스템

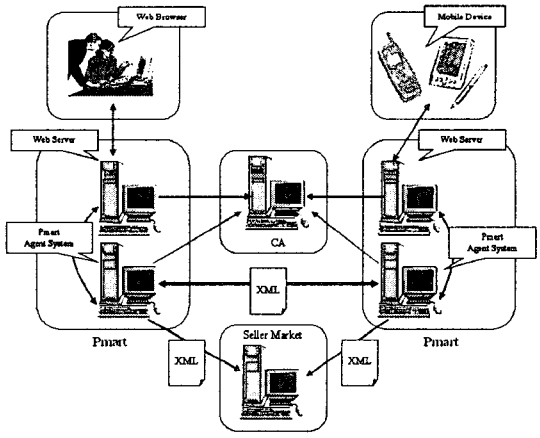
이 시스템은 XML 전자 서명과 SOAP을 사용한 웹 서비스로 구현함으로써 기존의 애플리케이션과 다양한 네트워크 환경에 유연한 구조가 되었고, 서명된 문서전달을 통해 신뢰된 거래를 수행할 수 있도록 하였다.

본 논문에서는 분산 Pmart 시스템에서 에이전트의 이동에 따른 보안 문제와 시스템간 부인방지의 문제를 해결하기 위하여 확장 Pmart에서 XML과 Enveloped Signature 방식의 전자서명을 이용한 안전한 이동 에이전트 시스템을 제안한다.

3. 시스템 설계

3.1 확장 Pmart

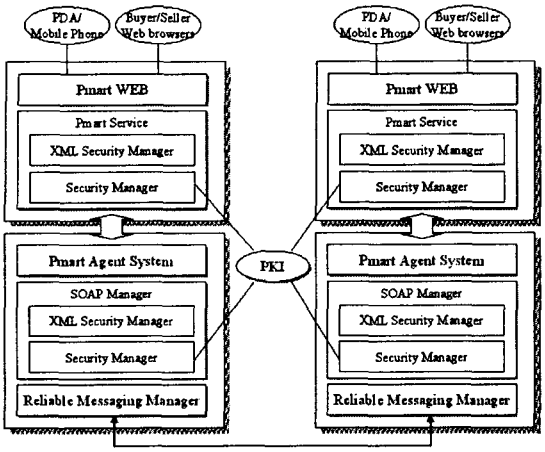
그림 2는 확장된 Pmart의 전체 시스템 구성도를 보여준다. 판매자/구매자는 웹 브라우저 또는 이동기기를 사용하여 분산된 Pmart에 연결할 수 있다. 하나의 Pmart 시스템은 웹 서버와 Pmart 에이전트 시스템으로 구분되어 있고, 웹 서버와 Pmart 시스템은 각각의 분리된 시스템일 수도 있고, 하나의 시스템으로 구성될 수 있지만, 웹 서버와 Pmart 에이전트 시스템은 반드시 방화벽이 있는 로컬 네트워크 안에 위치되어야 한다.



[그림 2] 확장 Pmart 전체 시스템 구성

웹 서버와 Pmart 에이전트 시스템은 SOAP을 사용하여 XML 기반 문서를 주고 받는다. 각 사용자들은 Pmart 웹 서버에서 사용 하기 전에는 인증서를 발급 받아야 하며, 이 인증서는 이동 에이전트에게 전송되어 모든 Pmart 시스템에서 검증을 받게 된다. 확장 Pmart에서는 XML 전자서명과 XML 엘리먼트 형식의 암호화 기술이 포함되어 있다.

그림 3은 제안된 확장 Pmart 시스템 아키텍처이다. 이 시스템은 위에서 설명한 것처럼 크게 Pmart 웹 서버와 에이전트 시스템으로 구성되어 있고, 주요한 컴포넌트들은 다음과 같다



[그림 3] 시스템 아키텍처

가) Pmart WEB

구매자 또는 판매자를 위한 일반적인 웹 브라우저를 위한 웹 서버와 이동기기를 지원하기 위한 SOAP기반의 웹 서비스로 이뤄져 있다. Pmart WEB은 안전한 거래 정보를 교환하고 보안 관련한 이동기기의 성능을 향상시키기 위한 Signcrytion[12]을 사용한 개량된 SSL을 사용한다.

나) Pmart Service

SOAP(Simple Object Access Protocol)[13][14] 기반의 웹 서비스로서 일반적인 웹 브라우저나 모바일 기기를 이용하는 구매자 또는 판매자를 위한 서비스로 이뤄져 있다

다) XML Security Manager

이 컴포넌트는 XML 전자인증 또는 엘리먼트 형식의 암호화와 같은 XML 보안 기술들을 구현한 것으로 CA로부터 전자인증서를 발급 받거나 인증서를 검증하는 여러 기능들을 가지고 있다.

라) Security Manager

PKI 기반의 암호화 알고리즘에 대한 기능을 가지고 있으며, 시스템 전반적인 암호기술은 JCE(Java Encryption Extension)를 사용하여 구현한다.

마) Pmart Agent System

사용자의 구매 선호도를 가진 구매에이전트가 판매에이전트와 협상을 하기 위하여 분산된 Pmart로 이동하여 활동하게 하는 시스템이다. 각 에이전트는 특정 Pmart에서 다른 Pmart로 이동 시에는 자신의 전자인증서를 사용하고, 현재 자신이 보유하고 있는 정보를 암호화 하여 모든 정보를 XML로 구성한 후 다른 Pmart 에이전트 시스템으로 보내진다. 이동 에이전트의 정보를 받은 Pmart 에이전트 시스템에서는 해당 정보를 토대로 하나의 에이전트를 구성하고 활성화시킨다.

바) SOAP Manager

Pmart 에이전트 시스템의 정보교환은 XML 기반의 문서를 교환한다. 이때 플랫폼 및 애플리케이션의 독립성을 유지하기 위하여 SOAP를 사용하여 문서를 주고받게 된다. 각 문서에는 XML 전자 서명이 첨부되어 있고, 이러한 요청에 대한 서비스를 제공한다.

사) Reliable Messaging Manager

Pmart 에이전트 시스템간의 문서 교환을 신뢰성 있으면서, 보안을 가지는 채널로 보내게 된다. 네트워크는 SSL 기반으로 신뢰성 있는 채널을 구성한 후 안전하게 문서를 교환하게 한다.

3.2 Pmart 에이전트 시스템

Pmart 에이전트 시스템은 자바로 설계되고 구현된다. 이 시스템에서의 에이전트 모델은 자바빈즈 형태이고, 이 에이전트를 이동시키기 위하여 다음과 같은 과정을 거친다.

(1) 에이전트 정보를 XML로 변환.
(2) 에이전트 정보들을 수신 측 Pmart 에이전트 시스템의 공개키로 암호화 수행.
(3) 이 에이전트를 생성한 사용자의 디지털 서명을 첨부.
(4) 수신 측 Pmart 에이전트 시스템의 SOAP을 통해 XML 문서를 전송하고, 이에 대한 확인 메시지 정보를 데이터베이스에 저장. 이것은 수신 측의 에이전트 정보 수신의 부인 방지

를 위한 것이다.

(5) 수신 측 Pmart 에이전트 시스템은 XML 문서에 있는 디지털 서명을 CA로 부터 확인하고, 에이전트 활성화에 대해 승인 결정.

(6) 수신 측 Pmart 에이전트 시스템의 비밀키로 에이전트 정보를 복호화 한 후 에이전트를 생성하고 활성화 시킴.

자바빈즈는 메쏘드의 특정 패턴을 포함하고 있는 클래스이다. 하지만 그렇게 간단한 클래스가 아니며, 컴포넌트 개념으로 구성된다. 컴포넌트는 다음과 같은 특징을 가진다. ① 재사용이 가능하다. ② 애플리케이션 개발자가 사용하는데 있어 최소한의 노력만을 필요로 하게 한다. ③ 보다 빠른 개발 속도를 가지게 한다. ④ 시각적인 프로그래밍 환경을 제공한다.

자바빈즈는 이러한 컴포넌트 특징 이외도 여러 가지 장점과 더불어 이식성, 개체지향개념, 개발의 용이성 등의 이점을 가지고 있다. 본 논문의 Pmart 에이전트 시스템에서는 이러한 자바빈즈의 특성을 가진 에이전트를 XML로 정의한 후 전자 서명을 통해 분산된 Pmart에 전송하는 이동 에이전트를 설계한다.

```
<!DOCTYPE JavaBean [
<!ELEMENT JavaBean (Properties)>
<!ELEMENT JavaBean ClassName CDATA # REQUEST>
<!ATTLIST Properties (Property *)>
<!ELEMENT Property (#PCDATA | JavaBean)*>
<!ATTLIST Property Name CDATA #REQUEST>
]>
```

[표 1] 자바빈즈를 위한 DTD

이동 에이전트 객체를 XML을 통해서 지속성(Persistence)을 유지할 수 있기 위해서는 이동 에이전트 모체인 자바빈즈를 표현하기 위한 DTD가 필요하다. 자바빈즈를 개념적인 수준에서 검사를 하고, 어떤 구조를 가지고 있는지 분석하여 표1과 같은 DTD를 설계한다.

가) 에이전트 정보를 XML로 변환

XML로부터 자바빈즈 상태를 복원하는 방법은 리플렉션(Reflection)과 인트로스펙션(Introspection) 두 자바 패키지를 사용하여 자바 클래스 정보인 클래스의 필드정보, 필드의 속성, 포함하고 있는 메쏘드 등을 분석할 수 있다. 리플렉션을 사용하면 클래스의 상태를 확인할 수 있을 뿐만 아니라 인자 목록을 생성하고 클래스의 메쏘드를 호출할 수 있다.

Pmart의 이동 에이전트를 XML문서로 만들기 위해서는 다음과 같은 단계를 가진다.

(1) 빈즈의 내용을 분석하기 위해 인스트로스펙션 엔진을 사용.

(2) 자바빈즈 안에 어떠한 필드가 존재하는지를 확인.

(3) 각 필드를 확인한 후에 자바빈즈 안에 있는 기본 타입 객체를 위한 getter 메쏘드의 레퍼런스를 획득하여 각 필드의 값과 타입 정보를 가지고 온다. 정적 필드나 휘발성 필드의 경우는 따로 저장할 필요가 없으므로 생략.

(4) 만약 주어진 필드가 기본 타입이 아닐 경우 그 내용을 저장하기 위한 메쏘드를 반복적으로 호출 가능.

위와 같은 단계를 거친 이동 에이전트의 XML 정보는 PKI 기반의 암호화를 통해 암호화 된다. 그러나 해당 에이전트의 활동을 요구 받은 Pmart는 에이전트의 유해성 및 향후에 발생할 결제 등의 보안을 위해 에이전트 인증이 요구된다. 이를 해결하기 위해 이동 에이전트는 에이전트의 정보를 암호화 하는 동시에 자신의 신원을 증명하는 전자 서명 내용을 XML 문서에 첨가하여 전송을 한다.

나) 전자 서명된 XML문서에서 에이전트 복원

그림 4처럼 특정 Pmart 에이전트 시스템으로부터 받은 이동 에이전트 XML 정보는 먼저 인증서 내용을 토대로 CA로부터 허가된 사용자인지를 확인 한 후 XML 내 암호화된 에이전트 정보를 복호화 하여 에이전트 상태를 복원한다. 에이전트 복원 단계는 다

음과 같다.

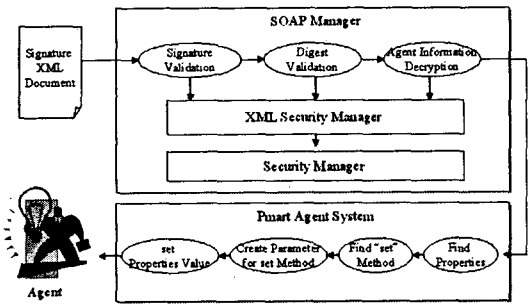
(1) 문서를 열고 루트 노드를 검색.

(2) Properties 노드를 검색하여 Property 원소에 대하여 반복.

(3) 각 Property 원소에 알맞은 set 메쏘드를 검색.

(4) set 메쏘드를 위하여 적절한 인자를 생성.

(5) (4)단계에서 만들어진 인자를 사용하여 Property의 값을 자바빈즈에 저장.



[그림 4] 이동 에이전트의 보안과 생성

4. 결론 및 향후 과제

본 논문에서는 다중변수기반 에이전트 중재 상거래 시스템 Pmart가 단일 시스템 구성으로 다양한 거래자를 선택할 수 없는 단점을 보완하기 위해 확장 Pmart를 설계하였다. 설계된 확장 Pmart의 구성은 Pmart간 자율적인 에이전트의 이동이 보장되어야 하고, 에이전트의 이동에 따른 인증 및 보안 기능이 필요 해진다. 따라서 에이전트의 안전한 이동과 협상에 필요한 정보의 전달을 위해 에이전트를 XML로 구성함과 동시에 이를 암호화 하고, 전자서명을 추가 함으로써 XML 보안 요구 사항을 만족하는 이동 에이전트 시스템을 설계하고 제안하였다.

향후 연구계획으로는 확장 Pmart 및 Pmart 에이전트 시스템의 구현과 이동에이전트간 전자결제를 위한 보안 설계, 구현과 부인방지에 대한 연구가 필요하다.

[참고문헌]

[1] W3C, Extensible Markup Language (XML), http://www.w3c.org/XML.

[2] www.w3.org "XML Signature Requirements WD," W3C Working Draft, 14 October 1999.

[3] www.w3c.org "XML-Signature Syntax and Processing" W3C Recommendation, 12 February 2002.

[4] www.w3c.org "XML Encryption Syntax and Processing," W3C Working Draft, 18 October 2001.

[5] www.w3c.org "Decryption Transform for XML Signature," W3C Working Draft, 18 October 2001.

[6] Mokdong Chung and Vasant Honavar, "A Negotiation Model in Agent-mediated Electronic Commerce," *Proceedings of the IEEE International Symposium on Multimedia Software Engineering*, Taipei, Dec. 2000 pp. 403-410.

[7] R.L.Keeney and H.Raiffa, Decisions with Multiple Objectives: Preferences and Value Tradeoffs, John Wiley & Sons, New York, NY, 1976.

[8] G.Gigerenzer et al., Simple Hueristics That Make Us Smart, Oxford University Press, New York, 1999.

[9]. 정목동, "다중변수 기반 에이전트 중재 전자상거래 협상 모델 및 프레임워크 설계," *정보과학회 논문지 : 소프트웨어 및 응용*, 28권, 11호, 2001, pp.842-854.

[10] T.Takase and N.Uramoto, "XML digital signature system independent of existing applications," *In proceedings of Applications and the Internet (SAINT) Workshops*, Nara City, JAPAN, 2002, pp. 150 -157.

[11] A. O. Freier, P. Karlton, and P. C. Kocher, "The SSL protocol version 3.0," November 18, 1996.

[12] Y. Zheng, "Digital Signcryption or How to Achieve Cost (Signature & Encryption) << Cost (Signature) + Cost (Encryption)," *Advances in Cryptology -- Crypto'97*, Springer-Verlag, 1997.

[13] W3C, "Simple Object Access Protocol (SOAP) 1.1," W3C Note, http://www.w3c.org/TR/SOAP.

[14] Apache, "Apache SOAP," http://xml.apache.org.