이동 에이전트 기반 전자상거래 시스템에서의 안전한 이동 에이전트 전송 프로토콜

한 승 완† · 임 형 석††

요 약

이동 에이전트 기반 전자상거래 시스템은 기반 기술로 이동 에이전트를 사용하여 전자상거래의 중요한 기능인 상품에 대한 정보 수집, 가격 결정 및 지불, 구입한 상품의 배달 등을 효율적으로 수행할 수 있어 다양한 측면에서 기존의 전자상거래 시스템에 비하여 장점을 갖는다. 그러나 이동 에이전트의 이동성 때문에 이동 에이전트 기반 전자상거래 시스템에서는 부가적인 보안 문제가 나타난다. 그러므로 이동 에이전트 기반 전자상거래 시스템을 활용하여 안전한 전자상거래를 수행하기 위해서는 기반 기술인 이동 에이전트의 보안에 관한 연구가 선행되어야 한다.

본 논문에서는 이동 에이전트를 보호하기 위해 이동 중인 에이전트의 비밀성과 무결성을 제공하고 에이전트 전송에 참여하는 호스트들 간의 상호 인증을 수행하는 이동 에이전트 전송 프로토콜을 제안하고 여러 가지 가능한 공격에 대한 안전성을 증명한다. 또한, 에이전트 위치 발견에 투명성(transparency)을 제공하고 사용자들의 고의적인 이동 에이전트 불법 복제를 검출할 수 있도록 신뢰 센터 기반의 이동 에이전트 위치 관리 메커니즘을 제안한다.

A Secure Mobile Agent Transfer Protocol in Mobile Agents Based E-Commerce System

Seung-Wan Han† · Hyeong-Seok Lim††

ABSTRACT

Mobile agents based e-commerce system has many advantages than traditional e-commerce system because mobile agents can efficiently perform the core functions of e-commerce-information gathering on goods, price settlement and payment, delivery of the goods purchased, and so on. However, due to the security vulnerability that stems from mobile agent's mobility, mobile agents based e-commerce system has additional security problems. Therefore in order to do e-commerce securely in the system, first of all the security issues on mobile agents must be addressed.

In this paper, we propose a mobile agent transfer protocol that provides confidentiality and integrity of mobile agent in transit and mutual authentication for communicating hosts. We further show the security of the protocol against many possible attacks. Also, we suggest the location management mechanism of mobile agents based on the trust center. This mechanism is capable of finding their locations transparently and detecting mobile agent clones.

1. 서 론

인터넷의 사용 증가와 분산 처리 기술의 발달로 실생활의 상거래 환경을 전자적으로 구현한 전자상거래에 관한 기대와 관심이 고조되고 있다. 일반적으로 전자상거래는 기업, 개인, 정부 등 경제주체들이 인터넷과 같은 네트워크 환경에서 전자매체를 이용하여 수행하는 상품이나 서비스의 거래 뿐만 아니라 거래에 수반되는 제반 경제 활동으로 정의된다. 이러한 전자상거래는 기업내 또는 기업간 업무의 효율성과 투명성을

※ 본 논문은 한국과학재단의 특정기초연구(98-0102-11-01-3) 연구비의 지원과 1999년도 두뇌한국 21 사업 핵심분야 연구비의 지원에 의한 것임
† 준 회 원 : 진남대학교 대학원 전산통계학과
†† 정 회 원 : 진남대학교 전산학과 교수
논문접수 : 2000년 3월 29일, 심사완료 : 2000년 5월 1일

높일 뿐만 아니라 시간적, 공간적 제약을 극복할 수 있어 전세계적으로 기업, 개인, 정부 등 모든 경제주체의 주목을 받고 있다. 그러니 전자상거래는 기존의 상거래에 비하여 고객이나 상품 공급자에게 더 많은 능력을 요구하게 된다. 예를 들면, 고객은 전 세계에 연결된 상품 공급자로부터 물건을 구매할 수 있기 때문에 선택의 폭이 매우 커지지만 과거보다 많아진 공급자들과 어떻게 접촉해서 원하는 물건을 저렴하게 구입할 수 있는가 하는 문제에 부딪히게 되고 상품 공급자는 전 세계의 고객으로부터의 상품에 관한 다양한 형태의 문의나 요구에 대처해야 한다. 그러므로 전자상거래를 보다 효율적으로 수행하기 위해서는 고객이나 상품 공급자 모두 자신을 대신하여 전자상거래와 관련된 업무를 수행할 소프트웨어 에이전트가 요구된다[3, 8, 9]

소프트웨어 에이전트는 사용자를 대신하여 업무를 수행하는 소프트웨어라고 넓게 정의할 수 있고 그 특성으로 자율성(autonomy), 사회성(social ability), 반응성(reactivity), 주도적 능동성(pro-activeness) 등을 갖는다. 이러한 특성으로 인하여 에이전트를 사용한 전자상거래 시스템은 복잡한 직업이나 단순 반복적인 작업을 에이전트가 대행하게 하여 기존의 상거래시에 소요되는 시간과 비용을 줄일 수 있을 뿐만 아니라 편리성, 확장성 등을 갖는다. 특히 전자상거래 시스템에서 이동 에이전트를 사용하면 전자상거래의 중요한 기능인 상품에 대한 정보 수집, 가격 결정 및 지불, 구입한 상품의 배달 등을 효율적으로 수행할 수 있어 이동 에이전트 기반 전자상거래 시스템은 다양한 측면에서 보다 큰 잠재력을 갖는다[3, 8, 9].

이동 에이전트는 이질적인 망(heterogeneous network)에서 자신의 제어로 호스트들을 옮겨다니며 다른 호스트의 에이전트 서버나 에이전트와 상호 작용하거나 자원을 이용하면서 사용자의 작업을 수행하는 프로그램이다. 이동성과 자율성을 특징으로 하는 이동 에이전트는 네트워크 부하를 줄일 수 있고 불안정한 통신 환경에서 클라이언트와 서버 사이의 지속적인 연결을 유지할 필요가 없으며, 또한 클라이언트의 요구가 다양하고 수시로 변하는 환경에서도 장점을 갖는다[5, 7]. 이러한 특성을 갖는 이동 에이전트 시스템은 전자상거래의 기반 기술로써 적합하다. 그 이유는 전자상거래에서는 전 세계에 흩어져 있는 상품 공급자들로부터 수시로 변화하는 고객의 요구와 기호에 맞는 상품 정보를 획득해야 하고, 획득된 정보를 활용하여 고객과 상품 공급자는 반복적인 상호작용을 통한 거래 협상을 수행해야하기 때문이다. 지금까지 개발된 이동 에이전트 기반 전자상거래 시스템으로는 IBM의 Aglet을 기반으로 구현된 MAgNet[3], AgentSpace을 기반으로 구현된 CELIA와 VSM[13], D'Agents을 기반으로 구현된 Realtor Demo[14] 등이 있다.

이동 에이전트는 전자상거래의 많은 분야에서 장점을 갖지만 이동성 때문에 나타나는 보안 취약점들로 인하여 실제 응용에 적용하는데 제약성을 갖는다. 이러한 제약성을 제거하고 이동 에이전트를 보다 널리 활용하기 위해서는 이동 에이전트 보안에 관한 연구가 절실히 요구된다[4, 5, 7]

전자상거래의 기반 기술로써 사용될 수 있는 이동 에이전트 시스템은 이동 에이전트와 에이전트 서버(호스트)로 구성된다. 그러므로 이동 에이전트 시스템에 대한 보안 문제는 크게 두 가지로 나누어 고려할 수 있다.

첫째, 악성 이동 에이전트나 악성 호스트의 공격으로부터 호스트를 보호하는 문제이다. 이러한 보호는 이동 에이전트와 호스트의 인증, 그리고 호스트내에 적절한 접근 통제 메커니즘을 채택함으로써 비교적 쉽게 해결될 수 있다

둘째, 악성 이동 에이전트와 악성 호스트의 공격으로부터 이동 에이전트를 보호하는 문제이다. 사용자의 작업을 정확하게 수행하기 위해서는 이동 에이전트의 보호가 무엇보다도 우선적으로 해결되어야 한다. 에이전트 보호는 다시 이동 중인 에이전트 보호와 호스트 상에서 실행 중인 에이전트 보호로 나눌 수 있다. 이 중에서 호스트 상에서 실행 중인 에이전트를 보호하기 위해서는 에이전트를 실행하는 호스트로부터 에이전트의 코드나 자료를 감출 수 있는 효과적인 방법을 요구한다. 그러나 호스트에게 프로그램을 드러내지 않고 수행할 수 있는 현실적인 메커니즘이 없고 이러한 메커니즘을 구현한다하더라도 그 메커니즘은 첫 번째 문제인 호스트 보호 문제와 교환 관계(trade off)를 발생시킬 수 있다. 그 결과 호스트 상에서 실행 중인 에이전트의 보호는 해결 불가능한 문제로 분류된다[4]. 반면에 이동 중인 에이전트 보호는 이동시에 적절한 이동 에이전트 전송 프로토콜이 채택된다면 해결될 수 있다. 본 논문에서는 이동 에이전트의 이동시에 발생하는 보안 문제점에 대해서 다루고 해결 방안으로 신

뢰 센터 기반의 안전한 이동 에이전트 전송 프로토콜을 제안함으로써 이동 에이전트 시스템이 전자상거래의 기반 기술로 보다 널리 활용될 수 있도록 하고자한다.

개방된 분산 환경에서 이동 에이전트가 호스트를 옮겨 다닐 때 이동 중인 에이전트는 불법적으로 도청 또는 변경될 수 있을 뿐만 아니라 송신 호스트는 고의적으로 변형된 악성 이동 에이전트를 전송함으로써 수신 호스트를 공격할 수 있다. 이러한 문제들을 해결하기 위해서 안전한 이동 에이전트 전송 프로토콜이 요구된다. 또한, 이동 에이전트는 쉽게 복제가 가능하므로 불법적인 복제를 통하여 이동 에이전트를 가장하거나 호스트의 서비스 거부 공격 등을 수행할 수 있다[1]. 그러므로 안전한 이동 에이전트 전송 프로토콜은 이동 에이전트의 불법적인 복제를 검출할 수 있는 메커니즘도 제공해야한다

본 논문에서는 이동 에이전트를 보호하기 위해 이동 중인 에이전트의 비밀성과 무결성을 제공하고 에이전트 전송에 참여하는 호스트들 간의 상호 인증을 수행하는 신뢰 센터 기반의 안전한 이동 에이전트 전송 프로토콜을 제안하고 여러 가지 가능한 공격에 대한 안전성을 증명한다. 제안된 프로토콜은 이동 중인 에이전트 보호 방법을 제공할 뿐만 아니라 에이전트 위치 발견에 투명성(transparency)을 제공하는 신뢰 센터 기반의 이동 에이전트 위치 관리 메커니즘을 활용하여 호스트의 고의적인 이동 에이전트 불법 복제를 검출할 수 있다. 또한, 송신 호스트가 고의적으로 변형된 악성 이동 에이전트를 전송하여 수신 호스트를 속이는 공격도 방지할 수 있다.

본 논문의 구성은 다음과 같다. 2장에서는 기존의 이동 에이전트 전송 프로토콜과 이동 에이전트 복제 검출에 대한 관련 연구를 살펴본다. 그리고 3장에서는 본 논문에서 제안한 이동 에이전트 기반 전자상거래에서의 안전한 이동 에이전트 전송 프로토콜을 설명한다. 4장에서는 제안한 프로토콜이 여러 가지 가능한 공격에 대해 안전함을 증명하고, 5장에서 결론을 기술한다.

2. 관련연구

전자상거래를 안전하게 실현하기 위해서는 인터넷과 웹 보안 기술, 암호 기술, 인증/PKI 기술, 전자우편 보안기술, 전자지불/전자화폐 보안 기술 및 방화벽 기술 등이 요구된다[12]. 이러한 전자상거래 보안 문제 이외에 이동 에이전트 기반 전자상거래 시스템은 기반 기술로 사용된 이동 에이전트에 관한 보안 문제가 추가적으로 해결되어야만 개방된 분산 환경에서 안전하게 실현될 수 있다

이동 에이전트 기술이 '90년대 중반에 등장한 까닭에 이동 에이전트 보안에 관한 연구는 전반적으로 미진하다. 그러나 최근의 분산 컴퓨팅 환경에서 이동 에이전트 기술이 두각을 나타냄에 따라서 이동 에이전트 보안에 대한 관심도 고조되고 있다.

[4]는 이동 에이전트 보안에 관한 일반적인 문제들과 요구 사항을 분석하고 보안 목표의 달성 가능성에 따라 해결 불가능한 문제, 쉽게 해결 가능한 문제, 해결 가능하지만 쉽지 않은 문제 등으로 분류하였다. [6]은 이동 에이전트 보안을 크게 4가지 측면으로 나누고 악의적인 호스트로부터 이동 에이전트를 보호하기 위한 메커니즘으로 시간 제약을 갖는 코드 혼합(code mess up) 기법을 제안하였다. 또한, [10]은 이동 에이전트의 보호를 위해 암호화된 함수를 평가하는 이동 암호화 시스템(mobile cryptography)을 이동 에이전트 시스템에 적용할 것을 제안하였다. 그러나 암호화된 함수를 평가하는 이동 암호 시스템은 함수의 대수적 준동형(algebraically homomorphic) 특성에 기반을 둔 것으로써 아직까지 일반적인 함수에 대해 적용할 수 없고 특수한 형태의 다항식과 유리 함수에 대해서만 적용 가능한 방법이 제안되었다. [2]에서는 이동 에이전트에 대한 인증과 권한 부여에 대해서 기술하였다.

호스트 사이의 에이전트 전송을 안전하게 수행하기 위해서 [7]은 Ajanta 시스템 구현에서 호스트 사이의 인증을 위해 질의-응답(challenge-response) 기반의 인증 프로토콜을 사용하고 암호화를 위해 ElGamal 공개키 암호화 시스템을 사용하였다. Ajanta 시스템이 채택한 질의-응답 방식의 인증 프로토콜은 간단하고 효율적이지만 man-in-the-middle 공격에 취약하다. 다른 이동 에이전트 시스템의 구현인 Telescript는 인증을 위해서 RSA를 사용하고 암호화를 위해서는 RC4를 사용하였다. 그 밖의 현재 구현된 대부분의 이동 에이전트 시스템들은 이동 에이전트의 안전한 전송을 위한 메커니즘을 제공하지 않고 있거나 단지 이동 중인 에이전트의 암호화만을 채택하고 있다[7].

이동 에이전트의 복제 검출에 관한 연구로는 [1]에서 이동 에이전트의 상태 토큰을 이용하여 신뢰받는

조정자(coordinator)가 복제된 에이전트 검출하는 방법을 제안하였다. 그러나 이동 에이전트의 이동시에 발생할 수 있는 다른 보안 문제들에 대한 대응책은 제공하지 않는다.

3. 안전한 이동 에이전트 전송 프로토콜

이동 에이전트는 자신의 제어에 의해서 네트워크의 호스트들을 옮겨 다니며 실행된다. 이때 이동 중인 에이전트의 노출, 훼손 또는 탈취는 이동 에이전트 시스템의 보안을 침해한다. 그러므로 안전하게 이동 에이전트를 전송할 수 있는 메커니즘이 요구된다. 또한, 이동 에이전트 시스템에서는 홈 플레이스(home place)와 이동 에이전트간의 통신이나 이동 에이전트들 사이의 통신을 위해서 이동 에이전트의 현재 위치를 발견하기 위한 효율적이고 투명성을 갖는 방법이 요구된다. 그리고 이동 에이전트는 어디에서나 쉽게 복제될 수 있는 프로그램이므로 전송되는 에이전트가 불법적인 복제가 아님을 보장할 수 있어야 한다. 이러한 문제들은 이동 에이전트가 갖는 이동성으로부터 발생되기 때문에 이동 에이전트가 호스트 사이를 옮겨다닐 때 적절한 조치가 취해진다면 제기된 문제들은 해결될 수 있다.

본 논문에서는 이동 에이전트를 안전하게 전송하고 에이전트의 위치 유지와 복제 검출을 제공할 수 있는 신뢰 센터 기반의 안전한 이동 에이전트 전송 프로토콜을 제안함으로써 이동 에이전트의 이동성으로부터 제기되는 몇 가지 보안 문제들을 해결하고자 한다.

이동 에이전트가 호스트 사이를 옮겨 다닐 때 두 호스트들은 상호 인증과 키 분배 프로토콜을 통해서 안전한 통신 채널을 형성할 수 있다 그러므로 제3의 호스트가 정당한 상대 호스트로 위장(masquerade)함으로써 변형된 악성 에이전트의 전송을 시도하거나 이동 에이전트의 탈취를 시도하는 것은 호스트의 상호 인증을 통해서 방지할 수 있다. 그리고 다른 호스트에 의해 시도되는 이동 에이전트 도청은 분배된 키를 사용한 암호화 기술을 통해서 막을 수 있다.

이동 에이전트의 현재 위치는 에이전트가 움직일 때마다 위치 변화를 에이전트 이름 저장소에 반영시킴으로써 유지할 수 있다. 에이전트 이름 저장소의 일관성을 유지하기 위해서는 이동 에이전트의 전송이 완료될 때만 위치 정보가 변경되도록 해야한다. 이것은 이동 에이전트를 전송하는 프로토콜이 정상적으로 완료되었을 때 이동 에이전트의 변경된 위치 정보를 에이전트 이름 저장소에 반영함으로써 얻을 수 있다.

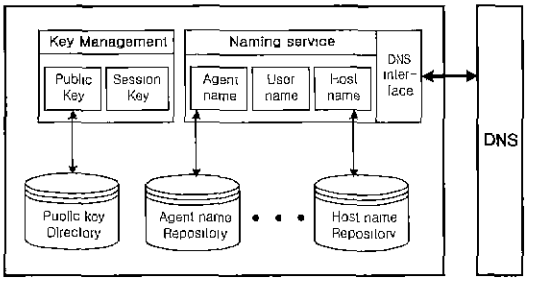
전송 호스트는 수신 호스트와 상호 인증 단계에서 보내기로 약속한 이동 에이전트를 보내지 않고 다른 이동 에이전트나 변형된 에이전트를 보내는 공격을 할 수 있다. 이러한 공격은 상호 인증 단계에서 전송 호스트가 수신 호스트의 공개키를 신뢰 센터에게 요청할 때 자신이 전송할 이동 에이전트의 현재 상태에 대한 서명값을 위탁하게 하고 수신 호스트가 이동 에이전트를 받은 후에 이동 에이전트의 위치 변경을 신뢰 센터에 요청할 때 수신한 이동 에이전트의 현재 상태에 대한 서명값을 신뢰 센터에 보내서 전송 호스트가 위탁한 서명값과 그 값을 비교하는 단계를 추가함으로써 방지할 수 있다

이동 에이전트는 사용자를 위하여 자율적으로 이동하며 수행되는 프로그램이므로 이동 에이전트를 실행하는 모든 호스트들은 이동 에이전트를 쉽게 복제할 수 있다. 그러므로, 이동 에이전트의 복제를 사전에 방지할 수 있는 현실적인 방법은 없고 다만 복제된 에이전트가 불법적으로 호스트 사이를 옮겨 다닐 때 이를 검출할 수 있다 이동 에이전트 복제 문제는 이동 에이전트를 가지고 있는 호스트가 반복 전송을 시도하는 경우와 이동 에이전트가 지나온 호스트가 재전송을 시도하는 경우로 축소해서 고려할 수 있다. 이러한 에이전트의 복제 문제는 이동 에이전트의 현재 위치를 유지하는 신뢰 센터 기반의 안전한 이동 에이전트 전송 프로토콜을 통하여 해결할 수 있다.

본 논문에서 제안된 신뢰 센터 기반의 안전한 이동 에이전트 전송 프로토콜은 다음과 같은 시스템에 대한 가정을 갖는다.

- 신뢰 센터는 믿을 수 있고, 외부의 모든 공격으로부터 안전하다.
- 신뢰 센터는 호스트와 사용자의 공개키에 대한 인증 및 안전한 통신에 사용할 세션키를 생성 분배한다
- 신뢰 센터는 각 객체들의 위치 정보를 관리하고 이를 서비스를 제공한다.
- 신뢰 센터를 제외한 모든 호스트들은 신뢰할 수 없다.
- 부정을 저지른 호스트나 사용자에게 조직적 혹은 법적인 책임을 부가할 수 있다.

이러한 가정을 바탕으로 본 논문에서 제안하는 신뢰 센터의 구조는 (그림 1)과 같이 크게 키 관리 부분과 이름 서비스 부분으로 나눌 수 있다.



(그림 1) 신뢰 센터의 구조

신뢰 센터의 키 관리 부분은 공개키 디렉토리 관리, 공개키 인증 등과 같은 공개키 기반 구조(PKI)의 기능과 안전한 통신 채널 형성을 위해서 사용될 세션키를 생성 분배하는 기능을 수행한다. 이때, 세션키를 사용하여 생성된 채널의 안전성을 위해서 신뢰 센터는 모든 세션마다 새로운 임의의 세션키를 생성 분배해야 한다.

신뢰 센터의 이름 서비스 부분은 호스트의 이름 서비스를 손쉽게 제공하기 위해서 기존의 DNS를 이용하고 호스트 이름 저장소에 각각의 등록된 호스트들에 대해서 이동 에이전트 전송 요청 또는 수신 확인 메시지의 순서를 기록하기 위한 요청 계수기를 갖는다. 그리고 사용자, 에이전트, 자원의 이름 서비스를 위해서 각각 별도의 이름 저장소를 활용한다. 에이전트의 이름 서비스를 위한 에이전트 이름 저장소의 레코드 구조는 (그림 2)와 같다.

ID	소유자	소유자의 서명	현재 위치	목적지	이동 요청 플래그	현재 MA의 해쉬값
MA_{id}	O	S_O(SHA(MA))	A	B	On/Off	SHA(MA)
...	...	...	...	...	...	...

(그림 2) 에이전트 이름 저장소의 레코드 구조

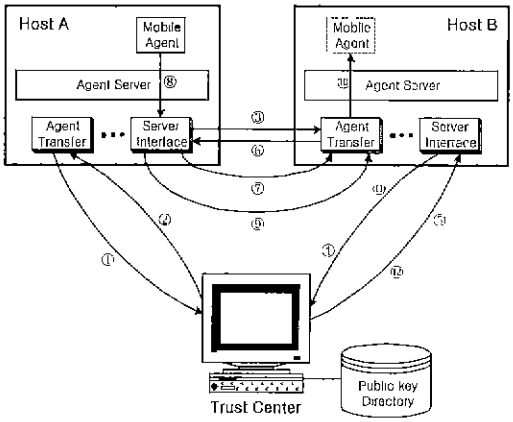
(그림 2)에서 ID 필드는 이동 에이전트 식별자로써 이동 에이전트가 등록될 때마다 신뢰 센터에 의해서 유일하게 부여된다. 소유자 필드는 이동 에이전트의 소유자를 나타낸다. 소유자의 서명 필드는 생성 당시의 이동 에이전트 코드의 해쉬값에 소유자가 서명한 값으로 이동 에이전트가 폐기될 때까지 변하지 않는다. 이 필드는 이동 에이전트의 코드가 이동 중에 변경되었는지를 검사하기 위해서 사용된다. 소유자 필드와 소유자의 서명 필드값은 새로운 이동 에이전트가 생성될 때 이동 에이전트의 소유자가 신뢰 센터에 등록한다. 현재 위치 필드는 이동 에이전트의 현재 위치를 나타내고 이동 에이전트의 이름 서비스를 제공하기 위해서 사용된다. 현재 위치에 해당하는 전송 호스트가 이동 에이전트를 전송하고자할 때 상대가 되는 수신 호스트는 목적지 필드에 기록되고 이동 요청 플래그 필드의 상태가 "On"으로 바뀌어 해당하는 이동 에이전트가 이동 중임을 나타내도록 한다. 이동 에이전트의 이동이 완료되면 목적지 필드값이 현재 위치 필드값으로 복사되고 이동 요청 플래그 필드는 "Off"로 변경된다. 현재 위치, 목적지, 이동 요청 플래그 필드는 이동 에이전트의 현재 위치를 유지하고 이동 에이전트의 복제를 검출하기 위해서 사용된다. 마지막 필드인 현재 이동 에이전트의 해쉬값은 이동 에이전트의 코드와 자료, 그리고 실행 상태 등을 포함하는 현재 상태에 대한 해쉬값으로써 이동 에이전트를 전송하는 호스트가 전송 요청 후 전송하기로 한 이동 에이전트를 변경하지 않고 전송하였는지를 확인하기 위한 필드이다

제안된 안전한 이동 에이전트 전송 프로토콜에서 사용된 암호화 기술 및 메커니즘은 <표 1>과 같다.

<표 1> 사용된 암호화 기술 및 메커니즘

요 소	기술 및 메커니즘[11]	에이전트 전송 프로토콜에 사용된 기호
공개키 암호화	RSA (1024비트 키)	E_{KA}(Mes) : A의 공개키로 Mes를 암호화
대칭키 암호화	IDEA (128비트 키)	E_K(Mes) 세션키(공유키)로 Mes를 암호화
해쉬 함수	SHA (160비트 해쉬)	SHA(Mes) : Mes에 대한 해쉬
디지털 서명	DSS (320비트 서명)	S_A(Mes) : A의 서명키로 Mes를 서명
호스트 상호 인증 및 키분배	공개키 기반의 Woo-Lam 프로토콜에 몇 개의 메시지 추가	

이동 에이전트를 안전하게 전송하고 에이전트의 위치 유지와 복제 검출을 위해서 본 논문에서 제안하는 프로토콜의 동작에 대한 개요는 (그림 3)과 같다.



(그림 3) 안전한 에이전트 전송 프로토콜의 동작 개요

에이전트 전송 요청 단계(①)에서 송신 호스트는 자신의 식별자, 수신 호스트의 식별자, 이동 에이전트의 식별자, 현재 이동 에이전트의 해쉬값, 요청 계수기를 포함하는 전송 요청 메시지를 신뢰 센터에 보내고 신뢰 센터는 에이전트 이름 저장소의 해당 에이전트의 레코드를 찾아 이동 요청 플래그를 "On"으로 변경하고 전송 호스트의 요청 계수기의 값을 1 증가시킴으로써 에이전트 상태를 이동 중으로 변경한다. 그리고 신뢰 센터는 수신 호스트에 대한 인증된 공개키를 포함하는 메시지를 전송 호스트에게 보냄으로써 그 다음 단계인 호스트 상호 인증 및 키 분배 단계(②~⑦)를 수행한다. 이 단계에서 두 호스트들은 상호간의 인증을 수행하고 신뢰 센터에 의해서 생성 분배된 세션키를 사용하여 안전한 통신 채널을 형성한다. 안전한 통신 채널이 형성되면 에이전트 전송 단계(⑧~⑩)에서는 자바의 객체 직렬화 기법과 암호화 기법을 사용하여 에이전트를 안전하게 전송한다. 그리고 에이전트의 전송이 끝나면 에이전트 수신 확인 및 위치 변경 단계(⑪~⑫)에서는 수신 호스트는 송신 호스트로부터 받은 에이전트의 해쉬값을 포함한 수신 확인 메시지를 신뢰 센터에게 보내고 신뢰 센터는 수신 호스트의 요청 계수기의 값을 1 증가시키고 수신 호스트가 수신한 에이전트가 송신 호스트가 전송하기로 한 에이전트인지를 확인하여 맞을 경우에만 에이전트 전송 프로토콜의 수행이 올바르게 완료된 것으로 간주하고 에이전트 이름 저장소의 해당 에이전트의 위치 정보를 변경한다. 그리고 수신 호스트에게 에이전트 전송 프로토콜이 올바르게 완료되었음을 나타내는 메시지를 보낸다

본 논문에서 제안하는 프로토콜의 완전한 명세는 (그림 4)와 같다.

[단계 1] 에이전트 전송 요청
① A→T : S_A(A, B, MA_{id}, E_T(SHA(MA)), $ReqCnt_A$)

[단계 2] 호스트 상호 인증 및 키 분배
② T→A : $S_T(K_B)$
③ A→B : E_{K_B}(A, R_A)
④ B→T : B, A, $E_{K_T}(R_A)$
⑤ T→B : $S_T(K_A)$, $E_{K_B}(S_T(R_A, K, A, B))$
⑥ B→A : $E_{K_A}(S_T(R_A, K, A, B), R_B)$
⑦ A→B : $E_K(R_B)$

[단계 3] 에이전트 전송
⑧ Object Serialization 후 IDEA를 사용하여 암호화 E_K(MA)
⑨ A→B E_K(MA)
⑩ IDEA를 사용하여 복호화 후 Object Deserialization하여 에이전트로부터 다음 값을 얻을 수 있다.
: MA, MA_{id}, S_O(SHA(MA)), SHA(MA)

[단계 4] 에이전트 수신 확인 및 위치 변경
⑪ B→T : S_B(A, B, MA_{id}, S_O(SHA(MA)), SHA(MA), $ReqCnt_B$)
⑫ T→B : S_T(SHA(⑪), Good/Bad)

T : 신뢰 센터 O : 에이전트의 소유자
A : 송신 호스트 B : 수신 호스트

(그림 4) 안전한 에이전트 전송 프로토콜

4. 프로토콜의 안전성

본 논문에서 제안된 프로토콜은 공격을 시도하는 호스트의 유형에 따라 송신 호스트의 공격, 수신 호스트의 공격, 제3의 호스트의 공격 등의 세 가지 공격에 대해 위협받을 수 있다. 그러므로 제안된 프로토콜이 세 가지 공격 유형에 대해 안전함을 보임으로써 제안된 프로토콜의 안전성을 증명할 수 있다.

프로토콜의 안전성 증명 과정에서 신뢰 센터는 절대적으로 믿을 수 있고 안전하며 프로토콜에 사용된 <표 1>의 암호화 기술 및 메커니즘들은 안전한 것으로 가정한다. 또한, 호스트 사이의 전송 오류는 발생하지 않는다고 가정한다. 그리고 증명에서는 편의성을 위하여 송신 호스트는 A, 수신 호스트는 B, 제3의 호스트는 C, 신뢰 센터는 T, 이동 에이전트는 MA라고 한다.

4.1 송신 호스트로부터의 공격에 대한 안전성

송신 호스트로부터의 제안된 프로토콜에 대한 공격

은 에이전트 복제를 전송하는 경우와 전송 요청시에 약속한 에이전트와 다른 변형된 에이전트를 전송하는 경우로 나눌 수 있다.

[보조 정리 1] 제안된 프로토콜은 송신 호스트의 에이전트 복제 공격에 대해서 안전하다

(증명) 송신 호스트의 에이전트 복제 공격은 자신을 지나갔고 실제 호스트 C에 존재하는 에이전트를 재전송하거나 자신이 갖고 있는 에이전트를 시간차를 두고 재전송하는 경우로 나누어서 고려할 수 있다.

먼저 송신 호스트가 자신을 지나간 에이전트를 재전송하는 경우를 고려해 보자. 송신 호스트를 지나간 에이전트를 MA_f라하면 송신 호스트 A는 제안된 프로토콜의 메시지 ①을 S_A(A, B, MA_f, E_I(SHA(MA_f)), $ReqCnt_A$)로 만들어 신뢰 센터에게 전송한다. 그런데 MA_f는 실제로 호스트 C에 존재하기 때문에 신뢰 센터의 현재 위치 비교에 있어서 A≠C가 되어 신뢰 센터는 쉽게 에이전트 복제 전송임을 감지할 수 있다.

다음으로 송신 호스트가 자신이 갖고 있는 에이전트(MA)를 시간차를 두고 재전송하는 경우를 고려해 보자. 송신 호스트는 에이전트 전송의 첫 번째 시도로써 S_A(A. B, MA, E_T(SHA(MA)), $ReqCnt_A$)를 메시지 ①로 만들어 한 프로토콜 과정을 수행 중에 있고 같은 에이전트에 대한 재전송의 시도로써 S_A(A. C, MA, E_T(SHA(MA)), $ReqCnt_A$+1)의 새로운 메시지 ①'를 생성하여 신뢰 센터로 진송할 수 있다. 그러나 첫 번째 전송 시도에서 신뢰 센터는 해당 에이전트 MA의 이동 요청 플레그를 "On"으로 변경하여 MA가 이동 중에 있음을 가리키고 있으므로 새로운 메시지 ①'는 에이진트 복제 전송 요청으로 판명할 수 있다.

그러므로 제안된 프로토콜은 송신 호스트의 에이진트 복제 공격에 대해서 안전하다. □

[정리 2] 제안된 프로토콜은 송신 호스트의 공격에 대해서 안전하다.

(증명) 송신 호스트로부터 에이전트 복제 공격에 대한 안전성은 보조 정리 1에 살펴본 것과 같이 증명할 수 있다

이제 전송 요청시에 약속한 에이전트와 다른 변형된 에이전트를 전송하는 공격에 대해서 살펴보자. 송신 호스트 A는 프로토콜의 메시지 ①로써 S_A(A. B, MA, E_T(SHA(MA)), $ReqCnt_A$)를 신뢰 센터에 보낸 후 메시지 ⑨에서 변형된 에이전트 MA_f를 수신 호스트 B에게 보냄으로써 프로토콜을 공격할 수 있다. 수신 호스트 B는 프로토콜의 에이전트 수신 확인 및 위치 변경 단계에서 송신 호스트가 보낸 변형된 에이전트의 해쉬값을 포함하는 메시지 ⑪ S_B(A, B, MA, S_O(SHA(MA)), SHA(MA_f), $ReqCnt_B$)를 신뢰 센터에게 전송한다. 신뢰 센터는 송신 호스트 A의 SHA(MA) ≠ 수신 호스트 B의 SHA(MA_f)임으로 송신 호스트의 변형된 에이전트 전송 공격을 발견할 수 있다.

그러므로 제안된 프로토콜은 송신 호스트의 공격으로부터 안전하다. □

4.2 수신 호스트로부터의 공격에 대한 안전성

수신 호스트로부터의 제안된 프로토콜에 대한 공격으로는 전송 받은 에이전트의 수신 확인 부인과 전송 받지 않은 에이전트에 대한 수신 확인 시도가 있을 수 있다.

[보조 정리 3] 제안된 프로토콜은 수신 호스트의 에이전트 전송 확인 부인 공격에 대해서 안전하다.

(증명) 수신 호스트 B는 프로토콜의 메시지 ⑪을 신뢰 센터에 보내지 않거나 올바르지 않는 값으로 구성된 메시지 ⑪을 신뢰 센터에 보낼 수 있다. 두 경우 모두 신뢰 센터는 에이전트의 위치 정보를 변경하지 않고 에이전트 MA의 현재 위치를 송신 호스트 A, 목적지는 수신 호스트 B, 그리고 이동 요청 플래그는 "Off"인 채로 남겨둔다. 이 후에 수신 호스트 B가 MA를 전송하려고 시도한다면 에이전트 복제 공격으로 간주된다 또한, 송신 에이전트의 재전송 시도도 역시 탐지할 수 있다.

그러므로 제안된 프로토콜은 수신 호스트의 에이전트 전송 확인 부인 공격으로부터 안전하다. □

[정리 4] 제안된 프로토콜은 수신 호스트의 공격에 대해서 안전하다

(증명) 수신 호스트 B는 전송 받지 않은 에이전트에 대한 수신 확인을 시도하기 위해서는 프로토콜의 메시지 ⑪을 구성해야한다. 그러나 수신 호스트 B는 MA, S_O(SHA(MA)), SHA(MA) 등을 알 수 없으므로 메시지 ⑪을 구성할 수 없다. 만약 호스트 B가 가로챈 메시지를 이용하여 위조된 메시지 ⑪을 구성하더라도 신뢰 센터가 유지하고 있는 해당 MA의 목적지 위치가 B가 아님으로 신뢰 센터는 호스트 B의 공격을 탐지할 수 있다. 위의 결과와 보조 정리 3의 결과로부터

제안된 프로토콜은 수신 호스트의 공격으로부터 안전하다. □

4.3 제3의 호스트로부터의 공격에 대한 안전성

제3의 호스트로부터의 제안된 프로토콜에 대한 공격으로는 메시지 재사용 공격과 정당한 상대 호스트로 위장하는 공격이 있다.

[보조 정리 5] 제안된 프로토콜은 제3의 호스트로부터의 메시지 재사용 공격에 대해서 안전하다.

(증명) 제3의 호스트는 제안된 프로토콜이 기반을 두고 있는 Woo-Lam 프로토콜의 메시지와 새로 추가된 메시지 ⑩, ⑪에 대하여 재사용 공격을 시도할 수 있다. Woo-Lam 프로토콜에 포함된 메시지들의 재사용 공격에 대해서는 제안된 프로토콜에서 사용하는 암호화 기술과 메커니즘의 안전성 가정으로부터 안전하다고 할 수 있다 그러므로 제3의 호스트에 의한 메시지 재사용 공격에 대한 안전성을 검증하기 위해서는 새로 추가된 메시지 ⑩, ⑪에 대한 재사용 공격에 대한 안전성을 검증하면 된다.

메시지 ⑩, ⑪이 서명만 되어 있으므로 제3의 호스트는 메시지 ⑩, ⑪의 내용을 알 수 있고 해당 호스트의 다음 요청 계수기 값을 예측할 수 있다. 그러나 제3의 호스트는 가장하고자 하는 호스트 A의 서명키를 알 수 없으므로 예측된 요청 계수기를 포함하는 새로운 메시지 ⑩, ⑪을 생성할 수 없다 그러므로 제3의 호스트는 임의로 생성한 에이전트 전송 요청이나 에이전트 수신 확인 메시지를 성공적으로 신뢰 센터에 보낼 수 없다. 만약 메시지 ⑩, ⑪을 단지 재전송한다면 그 때의 요청 계수기 값은 신뢰 센터의 저장된 요청 계수기 값보다 작아서 신뢰 센터는 재전송된 메시지가 지난 메시지임을 쉽게 확인할 수 있고 그 메시지를 무시할 수 있다.

그러므로 제안된 프로토콜은 제3의 호스트로부터의 메시지 재사용 공격에 대하여 안전하다 □

[정리 6] 제안된 프로토콜은 제3의 호스트로부터의 공격에 대해서 안전하다

(증명) 제3의 호스트는 보조 정리 5에 보여진 메시지 재사용 공격뿐만 아니라 정당한 상대 호스트로 위장하는 공격을 생각할 수 있다 그러나 제안된 프로토콜은 안전한 서명 알고리즘을 사용하므로 제3의 호스트는 정당한 호스트의 서명을 생성할 수 없다. 그 결과 제3의 호스트는 정당한 상대 호스트로 위장할 수 없다.

그러므로 제안된 프로토콜은 제3의 호스트로부터의 공격으로부터 안전하다. □

5. 결 론

이동 에이전트 기반 전자상거래 시스템은 기반 기술로 이동 에이전트를 사용함으로써 기존의 전자상거래 시스템에 비하여 여러 가지 측면에서 장점을 갖는다. 그러나 이동 에이전트의 이동성 때문에 나타나는 보안 취약점들은 이동 에이전트 기반 전자상거래 시스템을 사용하여 안전한 전자상거래를 수행하는데 장애가 되고 있다. 이러한 보안 취약점을 해결하기 위해서 본 논문에서는 신뢰 센터 기반의 안전한 이동 에이전트 전송 프로토콜을 제안하였다.

본 논문에서 제안된 프로토콜은 이동 에이전트의 이동성으로부터 야기되는 보안 문제 중에서 이동 중인 에이전트를 안전하게 전송하는 문제와 에이전트의 불법적인 복제를 검출하는 문제를 해결하였다. 그리고 제안된 프로토콜이 가능한 공격들로부터 안전함을 증명하였다

참 고 문 헌

[1] Jusung Baek, Mobile Agent Clone Detection Protocol, M.S. thesis, K-JIST, Korea, 1999

[2] S. Berkovits, J. D. Guttman, and V Swarup, "Authentication for Mobile Agents," LNCS 1419, pp.114-136, Springer-Verlag, 1998

[3] P Dasgupta, L E Moser, and P. M. Melliar-Smith, "MAgNet : Mobile Agents for Networked Electronic Trading," IEEE Transaction on Knowledge and Data Engineering, Vol 11, No.4, July/August 1999

[4] W. M Farmer, J. D. Guttman, and V. Swarup, "Security for Mobile Agents Issues and Requirements," *Proc. of the 19th National Information Systems Security Conf.*, pp.591-597, Baltimore, MD, USA, October 1996.

[5] C. G. Harrison, D M Chess, and A. Kershenbaum, "Mobile Agents : Are they a good idea?," Research

Report, IBM Research Division T. J. Watson Research Center. March 1995

[6] F. Hohl, "Time Limited Blackbox Security : Protecting Mobile Agents from Malicious Hosts," LNCS 1419, pp.92-113, Springer-Verlag, 1998.

[7] Neeran Karnik, Security in Mobile Agent Systems, Ph.D thesis, University of Minnesota, 1999.

[8] P. Kotzanikolaou, G. Katsirelos, and V. Chrissikopoulos, "Mobile agents for Secure Electronic Transactions," Recent Advances in Signal Processing and Communications, pp.363-368, World Scientific Engineering Society, 1999.

[9] P J. Marques, L M Silva, and J G. Silva, "Security Mechanisms for Using Mobile Agents in Electronic Commerce," *Proc of the 18th IEEE Symposium on Reliable Distributed Systems*, Lausanne, Switzerland, October 1999.

[10] T Sander and C Tschudin, "Towards Mobile Cryptography," *Proc. of the 1998 IEEE Symposium on Security and Privacy*, Oakland, CA, May 1998

[11] Bruce Schneier, *Applied Cryptography*, Second Edition, John Wiley & Sons, Inc., 1996.

[12] 이민영 외 5인, 전자상거래 보안 기술, 생능출판사, 1999.

[13] AgentSpace, http://berlin.mesc.pt/agentspace/index.html

[14] D'Agents, http://agent.cs.dartmouth.edu/

한 승 완

e-mail : hansw@chonnam.chonnam.ac.kr

1994년 전남대학교 전산학과 졸업(학사)

1996년 전남대학교 전산통계학과 졸업(석사)

1996년~현재 전남대학교 전산통계학과(박사과정)

관심분야 분산 컴퓨팅 보안, 암호이론, 계산이론, 알고리즘

임 형 석

e-mail hslim@chonnam.chonnam.ac.kr

1983년 서울대학교 컴퓨터공학과 졸업(학사)

1985년 한국과학기술원 전산학과 졸업(석사)

1993년 한국과학기술원 전산학과 졸업(박사)

1996년~1997년 미국 퍼듀대학교 전산학과 방문교수

현재 전남대학교 전산학과 교수

관심분야 : 계산이론, 알고리즘, 병렬 및 분산처리, 암호이론