1999 年度 大韓電子工學會 夏季綜合學術大會 論文集 第 22 卷 第 1 號 99/6

신뢰 센터 기반의 안전한 이동 에이전트 전송 프로토콜

한 승 완°, 임 형 석
전남대학교 전산통계학과

A Trust Center Based Secure Mobile Agent Transfer Protocol

Seung-Wan Han°, Hyeong-Seok Lim
Dept. of Computer Science, Chonnam National Univ.

Abstract

A mobile agent is a program which is capable of migrating autonomously from host to host in the heterogeneous network, to perform some computation on behalf of the user. Mobile agents have many advantages in the distributed computing environment. But they are likely to suffer many attacks on the security due to the mobility. In order to make use of a mobile agent in the real applications, the security issues must be addressed. We deal with the problem which is concerned with protecting a mobile agent in transit and detecting a mobile agent clone. In this paper we propose a trust center based secure mobile agent transfer protocol. This protocol transfers a mobile agent securely from host to host and detects a mobile agent clone. We further show the security of the protocol against many attacks.

1. 서론

네트워크의 확산과 분산 처리 기술의 발달로 점차 전자상거래, 전자 결제 시스템, 인터넷 정보 검색 등 분산 컴퓨팅 환경의 응용들이 많아지고 있다. 특히, 웹과 자바의 등장은 분산 시스템에 관한 연구를 더욱 촉진시키고 있다. 이러한 분산 컴퓨팅 환경에서 분산 응용 프로그램들 간의 상호 협력은 전통적으로 메시지 전달 기법(message passing method)이나 원격 프로시져 호출(Remote Procedure Call)을 이용하는 클라이언트 서버 모델에 기반을 두고 있다. 그러나 분산된 응용 프로그램 사이의 많은 메시지 교환으로 인하여 높은 네트워크 부하를 발생시키거나 낮은 대역폭과 불안정한 통신 환경을 갖는 경우에 클라이언트 서버 모델은 적합하지 않다. 그러므로 새로운 형태의 상호 협력 메커니즘이 요구된다. 이러한 요구를 반영하여 분산된 응용 프로그램들 간의 새로운 상호 협력 메커니즘으로써 이동 에이전트 기술에 관한 관심이 대두되고 있다[4, 6].

※ 본 논문은 한국과학재단의 특정기초연구(98-0102-11-01-3) 연구비 지원에 의한 것임.

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. 이동 에이전트를 응용할 수 있는 예로는 정보 검색, 망 관리, 사건 모니터링, 이동 컴퓨팅 분야 등을 들 수 있다[4, 6].

이동 에이전트는 분산 컴퓨팅 환경의 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[3, 4, 6].

이동 에이전트 보안은 크게 이동 에이전트의 보호와 호스트의 보호로 나눌 수 있는데 그 중에서 사용자의 작업을 정확하게 수행하기 위해서는 이동 에이전트의 보호가 우선적으로 해결되어야 한다. 이동 에이전트 보호는 다시 이동 중인 에이전트 보호와 호스트 상에서 실행 중인 에이전트 보호로 나눌 수 있다. 본 논문에서는 이동 중인 에이전트를 보호하고 이동 에이전트 복제 검출을 위한 방법을 다룬다.

개방된 분산 환경에서 이동 에이전트가 호스트를 옮겨 다닐 때 이동 중인 에이전트는 불법적으로 도청 또는 변경될 수 있고 정당한 호스트가 고의적으로 변형된 악성 이동 에이전트를 전송할 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. 그러므로 이동 에이전트의 불법적인 복제를 검출할 수 있는 메커니즘이 필요하다[1].

본 논문에서는 이동 에이전트를 보호하기 위해 이동 중인 에이전트의 비밀성과 무결성을 제공하고 에이전트 전송에 참여하는 호스트들 간의 상호 인증을 수행하는 안전한 이동 에이전트 전송 프로토콜을 제안

한다. 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.

본 논문의 구성은 다음과 같다. 2장에서는 기존의 이동 에이전트 전송 프로토콜과 이동 에이전트 복제 검출에 대한 관련 연구를 살펴보고, 3장에서는 본 논문에서 제안한 안전한 이동 에이전트 전송 프로토콜과 복제 검출 메커니즘을 설명한다. 4장에서는 제안한 프로토콜과 메커니즘의 안전성을 가능한 위협 시나리오들을 통해서 분석하고, 5장에서 결론 및 추후 연구 방향을 기술한다.

2. 관련연구

이동 에이전트 기술이 '90년대 후반에 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.

[3]은 이동 에이전트 보안에 관한 일반적인 문제들과 요구 사항을 분석하고 보안 목표를 달성 가능성에 따라서 분류하였다. [5]은 이동 에이전트 보안을 크게 4가지 측면으로 나누고 악의적인 호스트로부터 이동 에이전트를 보호하는 코드 혼합(code mess up) 기법을 제안하였다. 또한, [7]은 이동 에이전트의 보호를 위해 암호화된 함수를 평가하는 이동 암호화 시스템(mobile cryptography)을 이동 에이전트 시스템에 적용할 것을 제안하였다. [2]에서는 이동 에이전트에 대한 인증과 권한 부여에 대해서 기술하였다.

호스트간의 에이전트 전송을 안전하게 수행하기 위해서 [6]은 Ajanta 시스템 구현에서 호스트 사이의 인증을 위해 질의-응답(challenge-response) 기반의 인증 프로토콜을 사용하고 암호화를 위해 ElGamal 공개키 암호화 시스템을 사용하였다. 그리고 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 있다[6].

이동 에이전트의 복제 검출에 관한 연구로는 [1]에서 에이전트의 상태 토큰을 이용하여 복제된 에이전트를 신뢰받는 조정자(coordinator)가 검출하는 방법을 제안하였다.

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 제기되는 문제들을 해결할 수 있는 적절한 조치가 취해져야 한다.

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.

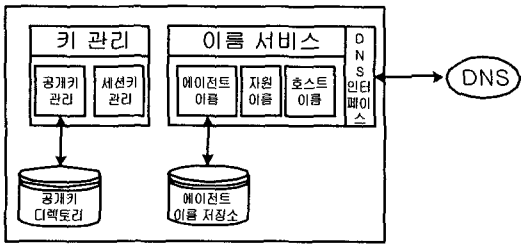
이동 에이전트는 사용자를 위하여 자율적으로 이동하며 수행되는 프로그램이므로 이동 에이전트를 실행하는 모든 호스트들은 이동 에이전트를 쉽게 복제할 수 있다. 그러므로, 이동 에이전트의 복제를 사전에 방지할 수 있는 현실적인 방법은 없고 다만 복제된 에이전트가 불법적으로 호스트 사이를 옮겨 다닐 때 이를 검출할 수 있다. 이동 에이전트 복제 문제는 이동 에이전트를 가지고 있는 호스트가 반복 전송을 시도하는 경우와 이동 에이전트가 지나온 호스트가 재전송을 시도하는 경우로 축소해서 고려할 수 있다. 이러한 에이전트의 복제 문제는 이동 에이전트의 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 이름 서비스를 제공한다.
- 신뢰 센터를 제외한 모든 호스트들은 신뢰할 수 없다.

- 부정을 저지른 호스트나 사용자들에게는 조직적 혹은 법적인 책임을 부가할 수 있다.

이러한 가정에서 동작하는 신뢰 센터의 구조는 그림 1과 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.

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

ID	소유자의 서명	현재 위치	이동지	이동 요청 플래그	현재 MA의 해쉬값	요청 시간
MA_{id}	$S_O(SHA(MA))$	A	B	On/Off	SHA(MA)	T_1
...	...	...	...	...	...	...

<그림 2> 에이전트 이름 저장소의 레코드 구조

그림 2에서 ID 필드는 에이전트 식별자이고, 소유자의 서명 필드는 이동 에이전트의 소유자가 초기의 이동 에이전트의 해쉬값에 서명한 값이다. 그리고 현재 이동 에이전트의 해쉬값은 에이전트를 전송하는 호스트가 전송 요청 후 전송하기로 한 이동 에이전트를 변경하지 않고 전송하였는지를 전송 받는 호스트가 확인하기 위한 필드이다. 또한 현재 위치, 이동지, 이동 요청 플래그 필드는 이동 에이전트의 현재 위치를 유지하고 이동 에이전트의 복제를 검출하기 위해서 사용된다.

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

<표 1> 사용된 암호화 기술 및 메커니즘

요소	기술 및 메커니즘
공개키 암호화	RSA (1024비트 키)
대칭키 암호화	IDEA (64비트 평문 블록, 128비트 키)
해쉬 함수	SHA (160비트 해쉬)
디지털 서명	DSS (320비트 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 프로토콜은 그림 3과 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 : $E_{KB}(A, R_A)$
④ B→T : B, A, $E_{KT}(R_A)$
⑤ T→B : $S_T(K_A)$, $E_{KB}(S_T(R_A, K, A, B))$
⑥ B→A : $E_{KA}(S_T(R_A, K, A, B), R_B)$
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 Deserialization : 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 : 에이전트 송신자　　B : 에이전트 수신자

<그림 3> 안전한 에이전트 전송 프로토콜

제안된 프로토콜의 단계 1에서는 신뢰 센터가 에이전트 이름 저장소의 해당 에이전트의 레코드를 찾아 이동 요청 플래그를 On으로 변경시킴으로써 에이전트 상태를 이동 중으로 변경한다. 단계 2에서 호스트 상호간의 인증과 안전한 통신 채널 형성을 위해 사용될 세션키 분배를 수행하고, 단계 3에서는 단계 2에서 생성된 세션키를 사용하여 에이전트를 전송한다. 그리고 단계 4에서 신뢰 센터는 호스트 B가 수신한 에이전트가 호스트 A가 전송하기로 한 에이전트인지를 확인하

여 맞을 경우에만 에이전트 전송 프로토콜의 수행이 올바르게 완료된 것으로 간주하고 에이전트 이름 저장소의 해당 에이전트의 위치 정보를 변경한다.

4. 프로토콜의 안전성

일반적으로 개방된 분산 환경에서 세션키의 생성은 믿을 수 있는 신뢰 센터에서 수행되어야 한다. 그리고 메시지의 재전송을 막기 위한 메커니즘으로 clock을 사용할 경우 호스트 사이의 타이머 동기화를 위한 추가 비용이 요구되므로 nonce를 사용하는 것이 더 바람직하다. 이러한 요구를 만족시키기 위해서 제안된 안전한 이동 에이전트 전송 프로토콜은 호스트의 상호 인증과 키 분배를 위해 신뢰 센터가 세션키를 생성하고 재전송 공격을 방지하기 위해서 clock 대신 nonce를 사용하는 공개키 기반의 Woo-Lam 프로토콜을 사용하였다. 아직까지 Woo-Lam 프로토콜은 취약점이 알려진 바가 없어 안전하다고 믿어진다[8]. 본 논문에서 제시한 프로토콜의 호스트 상호 인증 및 키 분배 부분의 안전성은 Woo-Lam 프로토콜의 안전성에 근거하고 있다. 그러나 Woo-Lam 프로토콜은 메시지 수와 암호화 회수가 많아서 다른 공개키 기반의 상호 인증 및 키 분배 프로토콜에 비해 성능이 좋지 않다. 그러므로 성능 향상을 위해 조건을 만족하는 기존의 다른 프로토콜이나 새로운 프로토콜을 사용할 수 있다.

제안된 프로토콜의 또 다른 측면인 에이전트의 위치 유지와 복제 검출에 대해서도 많은 위협들이 존재할 수 있다. 각각의 가능한 위협들에 대해서 제안된 프로토콜은 다음과 같이 안전하다.

- A가 갖고 있지 않는 에이전트의 전송 시도
  → ①에서 A와 에이전트의 현재 위치 비교
- A가 B와 C에 시간차를 두고 에이전트 전송 시도
  → 첫 시도의 ①에서 에이전트의 상태 플래그 변경
- B가 받은 에이전트의 수신 확인 거부
  → ⑫에서 에이전트의 위치 정보를 변경시키지 않음
- B가 받지 않은 에이전트에 대한 수신 확인 시도
  → B가 ⑪을 구성할 수 없음
- A가 에이전트 전송 시도 중에 전송 철회 요청
  → 신뢰 센터는 이동 요청 플래그를 Off로 바꿈
  만약, 프로토콜을 위반한 경우 A와 B 사이에 분쟁이 발생하게 되고 호스트 사이에 주고받은 메시지로부터 위반자를 찾아냄
- A가 약속과 다른 에이전트 전송(⑨) 시도
  → ⑫에서 B는 신뢰 센터로부터 Bad 응답을 받음
- C가 A(①) 또는 B(⑪)로 위장
  → C는 A 또는 B의 디지털 서명을 생성할 수 없음
- C가 ①이나 ⑪ 메시지의 재사용
  → C는 A나 B의 이동 에이전트 상태 변경 요청 메시지의 순서를 예측할 수 있으나 위조할 수 없음
- A와 B가 협력하여 프로토콜 위반 시도
  → 에이전트 이동 경로 상에 있는 일련의 호스트들의 협력에 의한 위협은 한 호스트의 위협으로써 고려할 수 있음

5. 결론 및 추후 연구

이동 에이전트는 이질적인 망의 호스트들을 자율적으로 옮겨다니며 사용자의 작업을 수행하는 프로그램으로써 분산 컴퓨팅 환경의 많은 분야에서 장점을 갖는다. 그러나 이동 에이전트의 이동성 때문에 나타나는 보안 취약점들은 이동 에이전트 기술을 실제 응용에 활용하는데 장애가 되고 있다.

본 논문에서는 신뢰 센터 기반의 안전한 이동 에이전트 전송 프로토콜을 제안하여 이동 에이전트의 이동성으로부터 야기되는 보안 문제 중에서 이동 중인 에이전트를 안전하게 전송하는 문제와 에이전트의 불법적인 복제를 검출하는 문제를 해결하였다. 그리고 제안된 프로토콜이 가능한 위협들로부터 안전함을 보였다.

추후 연구에서는 제안된 프로토콜을 BAN 논리나 Coloured Petri Net을 사용하여 정형화된 분석 및 검증을 수행할 예정이다.

참 고 문 헌

[1] Jusung Baek, Mobile Agent Clone Detection Protocol, M.S. thesis, K-JIST, Korea, 1997

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

[3] 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.

[4] 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.

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

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

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

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