

확장된 암호 실행추적으로 이동에이전트 보안 메커니즘

임형권*, 정창렬*, 고진광*

*순천대학교 컴퓨터과학과

e-mail : im_hk@hanmail.net, chari7@empal.com

Mobile Agent Security Mechanism through Expanding Cryptographic Execution Tracing

Im-Hyung Kwon*, Chang-Ryul Jung*, Jin-Gwang Koh*

*Dept of Computer Science, Sunchon National University

요약

이동에이전트는 안전한 활동을 보장할 수 있는 이동에이전트 보호가 선행되어야 한다. 본 논문에서는 이러한 이동에이전트를 보다 효과적으로 보호하고 안전성을 보장할 수 있도록 하는 이동에이전트 서버와 검증서버의 메커니즘을 제안한다. 또한 확장된 에이전트 시스템을 통한 실행추적이 기존의 에이전트 추적의 메커니즘과는 달리 확장된 암호화 실행추적을 통하여 안전하게 이동에이전트의 업무수행을 할 수 있도록 한다. 특히 확장된 암호화된 실행추적은 검증서버를 통하여 항상 안전성을 검증 받도록 함으로써 더욱 안전하게 이동에이전트를 보호할 수 있도록 하였다.

1. 서 론

컴퓨터와 정보통신기술의 발전은 일반 사용자의 정보기술 환경 또한 많은 변화를 가져왔다. 특히 실 세계에서 이루어지는 정보기술의 활용을 사이버 공간에서 전자적으로 사용하도록 하는 응용기술이 발전하게 되었는데 이러한 응용기술 중 이동에이전트 기술은 사용자를 대신해 업무를 수행할 수 있는 자율성(autonomy), 사회성(social ability), 반응성(reactivity), 주도적 능동성(pro-activeness) 등을 갖고 있어 시간과 비용의 절약을 가져오고 있다[1]. 이러한 기술은 메시지기반의 시스템이나 RPC(remote procedure call)에서 극복하지 못했던 것들을 극복할 수 있다.

이동에이전트기술은 이질적인 망에서 자신의 제어로 호스트를 옮겨 다니며 다른 호스트의 에이전트 서버나 에이전트와 상호작용을 하거나 자원을 이용하면서 사용자의 작업을 수행하는 임무를 수행한다. 그렇기 때문에 RPC와 RP(remote programming) 형태의 확장 개념으로 일반 환경에서는 모듈간의 통신 처리가 RPC에 의해서 이루어지는데 이동에이전트 시스템 환경에서는 실행프로그램이 실제로 존재하고 있는 장소로 이동하여 업무를 수행한다. 에이전트 프로그램의 이동코드(mobile code)를 수행하는 방식

으로 이동시킨다. 때문에 네트워크의 트래픽을 줄일 수 있으며 멀티유저에게 작업의 병행성을 높일 수 있고, 유연하고 능동적인 서비스를 제공할 수 있다.

그림 1은 전통적인 이동에이전트의 구조를 나타내고 있다.

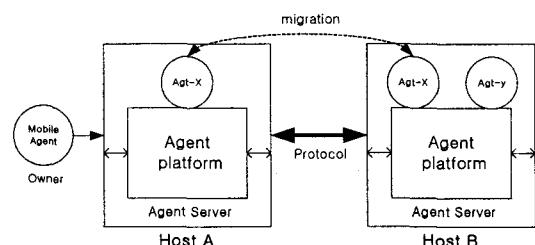


그림 1. 전통적인 이동에이전트 구조

에이전트에 대한 연구가 수년 전부터 이루어지면서 시스템 개발에 대한 연구 또한 매우 활발해졌다.

현재까지 개발된 에이전트시스템은 Ajanta를 비롯한 Java기반으로 많이 이루어지고 있다[2]. 표 1은 이동에이전트 시스템의 개발되어 있는 현황을 나타낸 것으로, 개발회사, 개발환경 등을 나타내고 있다. 현존하는 이동에이전트 시스템은 대부분 Java기반임

을 알 수 있다.

이동에이전트는 에이전트 자체가 지니고 있는 문제 가 있기 때문에 에이전트기술을 실제 사용하는 데는 악의적인 호스트에 의해 에이전트가 위협을 받는 요인과 악의적인 에이전트에 의해 호스트가 위협을 받는 두 가지의 큰 장애요인이 있다[4].

[표 1] 이동에이전트시스템

시스템	개발기관/언어/보안
AgentTcl	Dartmouth College, USA/Tcl/ Not Supported
Ara	University of Kaiserslautern, Germany/Java
Aglets	IBM/Japan/Java/Not Supported
Concrdia	Mitsubishi/USA/Java/Not Supported
GrassHopper	IVK++/Germany/Java
JATLITE	Stanford University/USA/Java
Mole	University of Stuttgart/Germany/Java
Messengers	ICU/Korea/Java
Odyssey	General Magic/USA/Java
Tacoma	University of Tromso & Conel University
Voyager	ObjectSpace Inc./USA/Java/Not Supported
X MAS	K-JIST/Korea/Java

에이전트시스템은 이동에이전트가 가지고 다니는 에이전트의 실행상태와 출처가 분명치 않는 소스코드, 그리고 악의적인 바이러스등으로 호스트를 보호하는 메커니즘에 관한 연구가 최근에 많이 이루어지고 있다[2-4]. 그에 따라 악의적인 이동에이전트와 악의적인 호스트에 대한 공격으로부터 이동에이전트를 보호하는 문제이다. 사용자의 작업을 정확하게 수행하기 위해서는 이동에이전트의 보호문제가 선행되어야 한다. 특히 이동에이전트의 보호는 이동중인 에이전트의 보호와 호스트상에서 실행되는 동안에 에이전트를 보호하기 위해서는 에이전트를 실행하는 호스트로부터 에이전트의 코드나 자료를 감출 수 있는 효과적인 방법을 요구한다. 그러나 에이전트가 실행되는 동안에는 에이전트의 코드나 상태 등의 상황을 접근하여야 함으로써 호스트에게 프로그램이나 실행상태를 드러내지 않고 수행할 수 있어야 하기 때문[4][8]에 위,변조나 잘못된 실행을 방지하는 것은 매우 어렵다.

따라서 본 논문은 분산된 컴퓨팅 환경에서 이동에이전트가 실행되는 동안에 호스트로부터 에이전트를 안전하게 보호할 수 있도록 하는 이동에이전트 서버 구조와 확장된 암호화 실행 추적을 통해서 이동에이

전트를 안전하게 보호하는 방법을 제안한다.

본 논문의 구성은 제1장은 서론을 고찰하고, 2장에서는 확장된 이동에이전트 시스템에 대해 기술한다. 제 3장에서는 암호화된 실행추적으로 이동에이전트 보호하는 메커니즘을 제안한다. 마지막 4장에서는 결론 및 향후연구에 대해 기술한다.

2. 확장된 이동에이전트 시스템

이동에이전트시스템은 이동형 에이전트를 생성, 이동, 수행, 전송, 해석 및 폐기등 에이전트의 생명주기를 관리할 수 있는 플랫폼이다. 그리고 사용자의 소프트웨어 엘리먼트등의 행위들을 자동으로 확인한다[5-6]. 그러나 확장에이전트 시스템은 기존의 이동에이전트 시스템을 보다 견고한 형태의 이동에이전트 시스템을 구축될 수 있도록 에이전트시스템에 검증서버를 두어서 안정성이 확보될 수 있도록 하는 이동에이전트 시스템의 확장을 의미한다. 기존의 에이전트 시스템은 호스트에 에이전트 서버를 두어서 에이전트의 이동되는 동안에 에이전트가 임무를 수행할 수 있도록 되어 있다. 그러나 이런 경우 악의적인 호스트로 하여금 에이전트가 가지고 있는 정보를 변질시킬 경우, 정보의 무결성을 보장할 수 있는 안전한 인증을 받기가 어렵다.

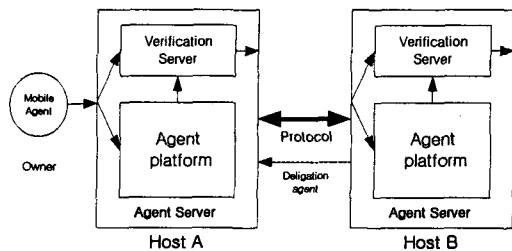


그림 2 확장된 이동에이전트시스템

또한 이동성을 지니는 에이전트는 물리적으로 저장되어 있는 자료를 적은 네트워크의 트래픽과 보다 많은 네트워크의 자원을 이용할 수 있도록 이동에이전트의 이동성을 네트워크 내에서 에이전트의 전송, 에이전트들의 상호작용과 보안에 관한 규약이 주지되어야 한다. 만약 그렇지 않으면 다른 호스트나 에이전트 서비스시스템의 이동에이전트의 안전한 정보처리 상호작용이 불가능해진다. 보안에 관한 문제는 이동에이전트 기술의 가장 어려운 부분이다[6-8]. 그렇기 때문에 이동에이전트의 인증, 프라이버스 문제, 데이터의 무결성 등 다양하고 비슷한 여러 관점에서

합법적인 책임이 따르게 된다. 호스트는 어떤 행위에 대해 에이전트의 요구를 알지 못하기 때문에 이 에이전트는 정말로 무엇을 사칭하고 있는가? 이런 종류의 데이터는 정말로 액세스해도 괜찮은가? 등에 관한 문명한 응답이 있어야 한다. 그렇게 하기 위해서 이동에이전트 시스템을 확장하여 호스트에 에이전트 서버와 검증서버를 두어서 암호화 실행추적을 통한 안전하고 정확한 임무수행을 위한 메커니즘으로 에이전트 보안문제를 해결한다.

3. 암호화된 실행 추적으로 이동 에이전트 보호

3.1 암호화된 이동에이전트 실행 추적

추적은 프로그램 실행의 증명을 위해 사용되며, 에이전트 실행의 안전성을 비교하여 체크하는 기법이다. 실행추적 기법은 이동에이전트 실행을 추적하면서 생성되는데 이는 코드의 정확한 라인에 추적된다. 이러한 추적의 활동은 에이전트의 모든 경로에 의해 이루어진다. 특히, 에이전트 소유자는 처음 호스트 플랫폼으로부터 에이전트 실행 시작의 완벽한 추적을 요구할 수 있도록 에이전트 방문계획에 따라 추적의 플랫폼으로부터 요구된다. 처리는 에이전트 방문계획에 의한 모든 호스트에서 처리되는 방법이다. 만약 약간의 악의적인 호스트의 의해 이동에이전트의 코드나 상태에 문제가 발생하여 원래의 상태와의 차이가 발생한다면 특별한 호스트 플랫폼에 의해 제공되어지는 추적의 검사 동안에 발견됨으로 악의적인 호스트를 찾을 수 있다.

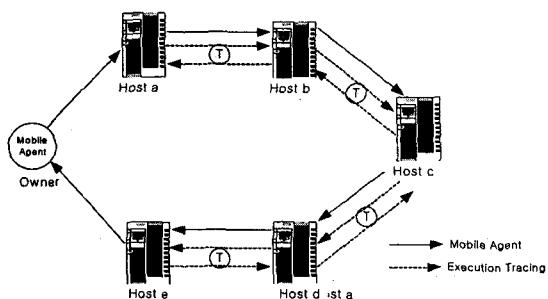


그림 3 이동에이전트 시스템의 암호화된 실행추적

이러한 접근은 약간의 문제가 발생할 수 있는데 그 문제점은 호스트에 의해서 유지되는 필요에 따라 추적으로 인하여 해당 호스트의 로그 사이즈와 수에 커지는 문제점과 관계가 있다. 그리고 검출처리기는

에이전트를 조작함으로 유일하게 알아채는 요인이 됨으로 본 논문에서는 검증 서버를 두어서 에이전트의 안전성을 검증할 수 있도록 한다. 그럼 3은 이동에이전트 시스템의 암호화된 실행추적 메커니즘으로 중간에 검증서버를 두어서 에이전트의 안전성을 검증 받았으나 그렇지 않고 바로 암호화된 검증서버를 통해서 안전성을 검증 받는다.

3.2 실행 추적에 따른 이동에이전트 보호 메커니즘

이동에이전트의 실행추적을 위한 확장된 시스템을 본 논문에서 제안한다. 제안된 확장 에이전트시스템은 크게 에이전트서버와 검증서버로 구분되어 있는데, 에이전트 서버는 주고 자원을 받아서 이동에이전트가 이동하고자 하는 계획에 따라 이동할 수 있는 기능만을 제시한다. 검증서버는 본 논문에서 제안하는 암호화 실행추적을 위한 메커니즘의 구조를 가지고 있어서 에이전트 무결성과 인증을 비롯한 암호키를 이용한 에이전트를 보호한다.

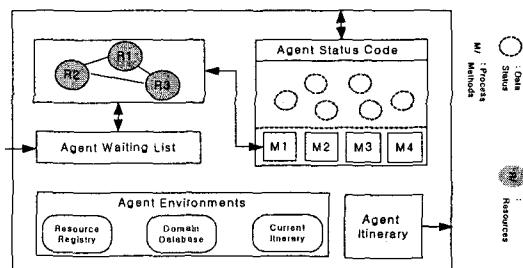


그림 4 실행추적을 위한 이동에이전트서버 구조

이동에이전트의 검증서버에서 전자서명과 타임스탬프는 에이전트 코드나 데이터의 무결성을 보장하기 위해 사용한다.

여기서 해쉬함수를 이용하는 이유는 에이전트의 코드의 무결성을 보장하기 위한 에이전트 코드의 전자서명을 하기 위함이다.

그림 4는 이동에이전트 서버의 구조를 나타내는 것으로서 에이전트가 게이트웨이를 통하여 에이전트서버로 들어오면 자원들을 에이전트 관리시스템에 의해서 데이터의 상태코드들을 관리한다. 관리되어진 에이전트의 상태코드들은 이동 에이전트들의 이동계획일정과 함께 검증서버로 보내어 진다.

그림 6은 이동 에이전트를 안전하게 실행하기 위해 추적할 수 있도록 하는 검증 시스템으로 에이전트 서버로부터 받은 에이전트의 상태코드를 통하여 무

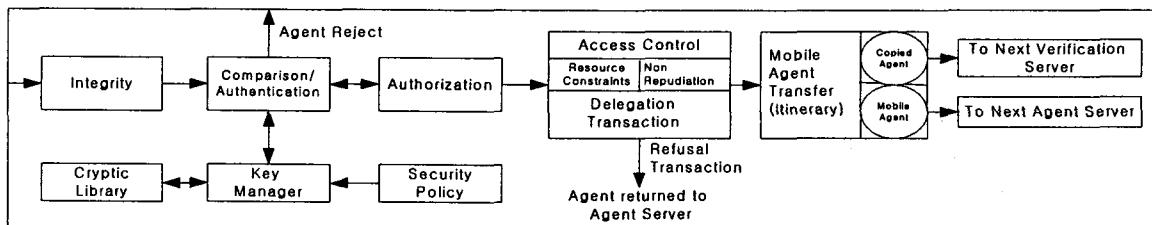


그림 5 검증 서버 구조

결성을 체크한다. 이전 에이전트시스템으로부터 이동하여 온 에이전트를 비교하여 에이전트에 대한 번질이 없다면 에이전트에 안전성을 보장하는 인증을 한다. 인증이 이루어지면 인증을 토대로 하여 에이전트를 액세스 할 수 있는 권한을 위임한다.

위임된 권한으로 검증서버에서는 자원을 액세스하는데 여기서 에이전트의 상태코드를 실행 추적하여 자원을 거절하여 다시 에이전트 서버로 돌려 보내거나 그렇지 않고 안정하고 정상적이면 에이전트의 임무를 수행하고 이동에이전트 트랜스퍼에 의해서 에이전트서버로부터 받은 에이전트 이동계획에 맞추어 전송을 하는데, 이때 에이전트 트랜스퍼를 이동되는 에이전트를 복사하여 동일한 에이전트를 다음 에이전트 시스템으로 보낼 때 전송프로토콜을 통해서 에이전트를 에이전트서버와 검증서버로 보낸다.

이렇게 보내어지면 수신된 에이전트 시스템에서는 두개의 에이전트를 검증서버를 통해서 비교하여 안전성과 무결성을 보장한다.

4. 결 론

이동에이전트는 이질적인 망에서 에이전트 자체 지니고 있는 이동성으로 인하여 다른 에이전트와 상호 작용을 할 수 있다. 그에 따른 많은 문제를 지니고 있는데 이에 대한 많은 연구가 이루어지고 있다. 본 논문도 이동에이전트를 보다 효과적으로 보호하고 안전성을 보장할 수 있도록 하는 이동에이전트 서버와 검증서버의 메커니즘을 제안하였다. 이러한 구조를 통해서 암호화된 실행추적을 하여 안전하게 이동에이전트를 보호할 수 있도록 하였다. 이는 확장된 에이전트 시스템을 통한 실행추적이 기존의 에이전트 추적의 메커니즘과는 달리 암호화된 실행추적을 통하여 안전한 이동에이전트의 업무수행을 할 수 있도록 하였다. 검증서버를 통하여 항상 안전성을 검증 받도록 함으로써 이동에이전트가 목적지까지 이동할 수 있도록 하였다.

참고문헌

- [1] P. Dasgupta, L. E. Moser, P. M. Melliar-Smith, "MagNet:Mobile Agents for Networked Electronic Tracing", IEEE Transaction on Knowledge and Data Engineering, Vol. 11, No.4, July, 1991.
- [2] A. Villazon and W. Binder, "Portable Resource Reification in Java-based Mobile Agent Systems", In Mobile Agents : Proc. of the 5th International Conference, Number 2240 in LNCS, Springer-Verlag, Altanta, USA, 2001.
- [3] H. K. Tan, L. Moreau, "Extending Execution Tracing for Mobile Code Security", In Proc. of the 2nd International Workshop on Security in Mobile Miti-Agent Systems, associated to AAMAS-2002, Bologna, Italy, July, 2002.
- [4] C. R. Jung et al. "An Agent System Protection Mechanism for Secure Action of Mobile Agent in Open Network System", in the Journal of KIMICS, Korea, April, 2002.
- [5] T. Taka, T. Mizuno, T. Watanabe, "A Model of Mobile Agent Services" in enhanced for the International Conference on Parallel and Distributed Systems, pp.274-281, 1998.
- [6] C. Raibulet, C. Demartini, "Mobile Agent Technology for the Management of Distributed System-a Case Study", in Journal of Computer Networks Vol.34, pp.823-830, 2000.
- [7] T. Sandholm, Q. Huai, "Nomad: Mobile Agent System for an Internet-based Auction House", IEEE Internet Computing Vol.4, No.2, pp.80-86, 2000.
- [8] J. Alesheimer, C. Cachin, J. Camenisch, G. Karjoh, "Crytographic Security for Mobile Code", In Proc. IEEE Symposium on Security and Privacy(S&P 2001), pp.2-11, may, 2001.