이동 에이전트 기반 역할 위임 기법*

정용우*, 고광선*, 김구수**, 엄영익*
*성균관대학교 정보통신공학부
**동양대학교 정보통신공학부
e-mail:{withdubu, rilla91, yieom}@ece.skku.ac.kr, gusukim@dyu.ac.kr

Mobile Agent based Role Delegation Scheme

Young-woo Jung*, Kwang Sun Ko*, Gu Su Kim**, and Young Ik Eom*
*School of Info. and Comm. Eng., Sungkyunkwan University
**School of Info. and Comm. Eng., Dongyang University

요 약

이동 에이전트는 네트워크를 이동하면서 사용자를 대신하여 작업을 수행하는 프로그램으로써 홈 네트워크, 텔레메틱스 등의 많은 응용분야에서 새로운 컴퓨팅 모델로 활용될 것으로 기대된다. 현재, 여러 응용분야에 활용 가능한 다양한 이동 에이전트 시스템들이 개발되고 있으며, 최근에는 RBAC을 활용한 이동 에이전트 시스템들이 개발되고 있다. 그러나 이들 RBAC을 활용한 시스템들은 특정 사용자에게 할당된 역할을 다른 사람에게 위임하기 위해서는 관리자로 하여금 시스템 내부 정보를 변경하거나 역할간의 계층을 변경하는 작업이 요구된다. 따라서 본 논문에서는 사용자가 위임하고자 하는 역할과 대상을 정의하고 이를 이동 에이전트를 이용하여 시스템에 반영할 수 있는 이동 에이전트를 이용한 역할 위임 기법을 제안한다.

1. 서론

이동 에이전트[1]는 네트워크 상에서 스스로 이동하면서 사용자를 대신하여 작업을 수행하는 프로그램으로써 일반적인 에이전트의 특징 중에서 이동성이 강조된 에이전트이다. 이동 에이전트는 네트워크 환경 변화에 동적이고 유연하게 적응이 가능하며, 특히 이동 에이전트의 비동기적 수행 능력은 대역폭이 낮은 네트워크 환경에서 유용하게 활용된다. 또한 이동 에이전트는 스스로를 복제하여 다수의 복제 에이전트를 네트워크로 전송하고 이후에 각각의 복제 에이전트가 가져온 데이터를 모아 복합적인 결과를 만들어 낼 수 있는 능력을 지닌다. 이러한 특징들은 홈 네트워크 환경, 텔레메틱스, 정보검색 시스템 등의 여러 응용분야에서 새로운 컴퓨팅 모델로서 활용될 수 있다.

이동 에이전트를 다양한 응용분야에서 활용하기 위해서는 이동 에이전트에 대한 인증과 접근제어가 반드시 이루어져야 한다. 최근에는 이러한 문제를 해결한 다양한 시스템들이 연구되고 있으며, 특히 이동 에이전트의 역할에 따라 접근제어가 이루어지는 시스템들이 개발되고 있다.

역할기반 접근제어[2, 3]가 가능한 시스템들은 이동 에이전트를 생성한 사용자의 신원에 기초하여 이동 에이전트에게 역할을 부여한다. 즉, 시스템은 특정 사용자가 부여받을 수 있는 역할들에 대한 정보를 관리한다. 만일, 특정 사용자의 부재로 인해 그 사용자에게 할당 된 역할을 다른 사용자에게 위임할 경우가 발생하게 되면, 이를 위해서 관리자가 개입하여 특정 사용자에게 할당된 역할을 다른 사용자에게 재할당해야만 하는 추가적인 작업이 필요하게 되며 이는 시스템의 사용자와 역할간의 정보의 변경을 동반하게 된다.

본 논문에서는 이동 에이전트를 이용한 역할 위임[4, 5] 기법을 제안한다. 본 기법은 사용자가 위임하고자 하는 대상과 역할을 정의하고 이를 이동 에

* 본 연구는 21세기 프론티어 연구개발사업의 일환으로 추진되고 있는 정보통신부의 유비쿼터스컴퓨팅및네트워크원천기반기술개발사업의 지원에 의한 것임 (2006-0391-0100).

이전트를 이용하여 시스템에 반영한다. 따라서 본 기법은 관리자의 추가적인 작업 없이 다른 사용자에게 역할 위임이 가능하며, 역할 위임 시, 시스템 내부 정보에 대한 변경이 필요하지 않으며, 역할 간의 계층 관계에 따라 전체 혹은 부분 역할 집합의 위임이 가능하다.

본 논문은 구성은 다음과 같다. 2장에서는 기존의 역할기반의 접근제어 기법을 활용한 이동 에이전트 시스템에 대해서 살펴보고, 3장에서는 본 논문에서 제안하는 이동 에이전트를 이용한 역할 위임에 대해 설명한 뒤, 마지막으로 4장에서는 결론을 맺는다.

2. RBAC을 활용한 이동 에이전트 시스템

본 절에서는 역할기반 접근제어 기법을 활용한 이동 에이전트 시스템들의 특징에 대해서 살펴본다.

이탈리아의 Bologna 대학과 Ferrara 대학에서 공동으로 개발한 SOMA(Secure and Open Mobile Agent)[6]는 이동 에이전트 환경에서 나타날 수 있는 다양한 보안 위협 사항에 대처하기 위해 개발된 이동 에이전트 시스템이다. SOMA는 크게 보안 위협 사항을 호스트에 대한 위협사항과 이동 에이전트에 대한 위협 사항으로 나누고, 각각에 경우에 필요한 보안 메커니즘을 제시한다. SOMA에서는 호스트로 진입하는 이동 에이전트에 대해 역할기반 접근제어 기법을 적용함으로써 불법적인 이동 에이전트의 호스트 접근을 제어한다.

중국의 Jiao Tong 대학에서 개발한 RCACM (Role-based Context Aware Coordination Model)[7] 역시 이동 에이전트의 역할에 기반 한 접근제어 기법을 제안한다. RCACM은 분산된 자원, 서비스, 그리고 객체로 구성된 튜플 스페이스(Tuple Space)라는 특정 공간으로 접근하는 이동 에이전트에게 역할을 할당하고 그 역할에 따라 튜플 스페이스의 자원 및 객체에 접근할 수 있는 권한을 할당한다.

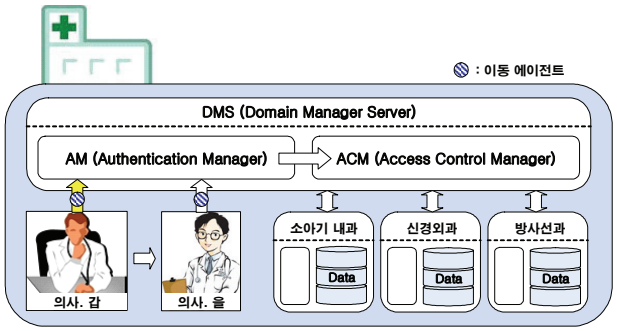
BRAIN(Behavioral Roles for Agent Interaction)[8] 은 이탈리아의 UNIMORE(Modena e Reggio Emilia) 대학에서 개발한 이동 에이전트 시스템이다. BRAIN은 이동 에이전트를 활용한 대규모 분산 시스템 환경에서 이동 에이전트간의 협업에서 나타 날 수 있는 문제를 해결하기 위해 이동 에이전트의 역할에 기반 한 접근제어를 활용한다.

그러나 기존의 역할기반 접근제어 기법을 활용한 시스템들은 다른 사용자에게 역할의 위임이 불가능하며 이를 위해서는 관리자로 하여금 사용자와 역할 간의 관계를 정의한 테이블을 수정하거나 또는 역할 간의 계층관계를 정의한 테이블을 수정해야하는 추가적인 연산이 필요하다. 본 논문에서는 이러한 관리자의 개입을 통한 테이블의 수정 없이 이동 에이전트를 이용하여 역할의 위임이 가능한 역할 위임 기법을 제안한다.

3. 역할 위임을 통한 이동 에이전트의 접근제어

3.1 적용 환경

그림 1과 같이 이동 에이전트를 이용하여 환자 기록을 검색할 수 있는 의료 시스템이 있다고 가정하자.



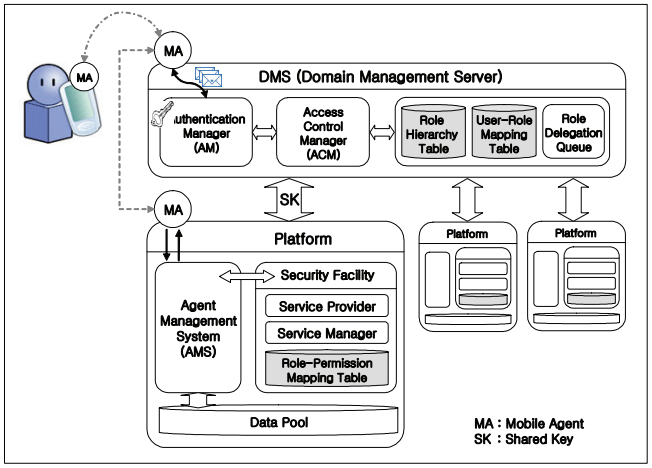
(그림 1) 이동 에이전트를 활용한 의료 검색 시스템

갑은 이동 에이전트를 생성하여 환자에 대한 의료 내역을 검색하고자 한다. 갑은 이동 에이전트를 생성하여 DMS(Domain Manager Server)로 이주시킨다. DMS의 AM(Authentication Manager)은 이동 에이전트를 생성한 갑의 신원을 바탕으로 인증을 수행한다. 인증에 성공한 이동 에이전트는 ACM (Access Control Manager)으로부터 갑에게 할당 가능한 역할들을 부여받는다. 역할을 부여 받은 이동 에이전트는 환자의 의료 내역 조회를 위해 의료 정보를 저장하고 있는 플랫폼들로 이주하여 정보를 취합한 뒤, 갑에게 돌아와 그 결과를 보고한다.

만일, 갑이 해외 학회 참석차 자리를 비우고 을이 갑의 역할을 대신해야 한다고 가정 하자. 시스템 관리자는 갑에게 할당 가능한 각각의 역할들을 을에게 할당해야 하며, 이를 위해서 DMS 내부의 사용자와 역할 간의 관계를 정의한 정보들을 변경해야만 한다. 본 논문은 이러한 이동 에이전트 시스템에서 관리자의 의한 시스템 내부의 정보의 변경이나 역할간의 계층의 변경 없이 역할 위임이 가능한 접근제어 기법을 제안한다.

3.2 시스템 구조와 이동 에이전트의 접근제어

그림 2는 역할의 위임을 통한 이동 에이전트의 접근제어를 위한 시스템 구조를 나타낸다. 본 논문의 이동 에이전트의 다양한 기능 중 데이터 검색의 기능에 한하여 논지를 전개한다.



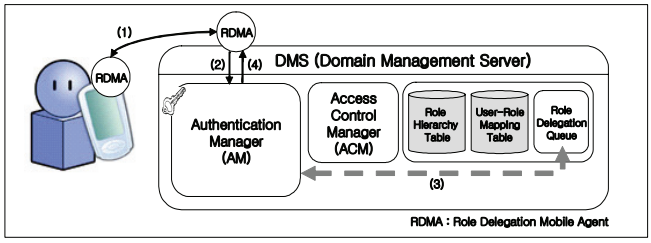
(그림 2) 시스템 구조

본 이동 에이전트 시스템은 크게 세 부분으로 나뉜다. 사용자를 대신하여 작업을 수행하는 이동 에이전트와 이동 에이전트의 인증과 역할 티켓 부여를 담당하는 DMS 그리고 이동 에이전트에게 정보를 제공해 주는 플랫폼으로 구성된다. 표 1은 본 시스템의 구성 요소와 기능을 나타낸다.

이동 에이전트를 통한 정보검색 절차는 다음과 같다. 사용자부터 생성된 이동 에이전트는 사용자로부터 이주하여 DMS를 통해 인증과정을 거친다. 인증에 성공한 이동 에이전트에 대해 DMS는 역할 티켓을 부여한다. 역할 티켓은 RHT, URMT, RDQ를 참조하여 이동 에이전트에게 발급된다. 역할 티켓을 발급받은 이동 에이전트는 플랫폼으로 이주하여 정보 검색을 위한 데이터 접근을 시도한다. 플랫폼의 SF는 이동 에이전트의 역할 티켓의 무결성을 검증하고 해당 역할에 따른 데이터 접근권한을 할당한다. 이동 에이전트는 부여받은 권한에 한하여 데이터 풀의 정보 검색이 가능하다. 정보 검색이 완료된 이동 에이전트는 결과를 이동 에이전트 내부에 저장하고 다른 플랫폼으로 이주한다.

3.3 이동 에이전트를 통한 역할의 위임

사용자는 자신의 역할을 다른 사람에게 할당함으로써 다른 사람으로부터 생성된 이동 에이전트가 자신의 이동 에이전트와 동일한 작업을 수행하도록 할 수 있다. 역할의 위임은 이동 에이전트를 통해 위임하고자 하는 역할을 RDQ에 등록함으로써 이루어진다. 그림 3은 DMS에 위임할 역할을 등록하는 과정을 나타낸다.



(그림 3) 위임할 역할의 등록 과정

<표 1> 시스템 구성 요소 및 기능

위 치	구성 요소		기 능
DMS (Domain Management Server)	AM (Authentication Manager)		이동 에이전트를 생성한 사용자의 신원을 기초하여 인증 수행 및 플랫폼 간의 공유키(SK: Shared Key)의 유지 관리를 담당한다.
	ACM (Access Control Manager)		RHT, URMT, RDQ를 참조하여 이동 에이전트에게 할당 가능한 역할을 확인하고 이동 에이전트에게 역할 티켓을 발급한다.
	RHT (Role Hierarchy Table)		시스템에 정의된 역할들 간의 계층 관계를 정의한다.
	URMT (User-Role Mapping Table)		이동 에이전트를 생성한 사용자에게 할당 가능한 역할들을 정의한다.
	RDQ (Role Delegation Queue)		특정 사용자에게 위임된 역할들에 대한 정보를 관리한다.
Platform	AMS (Agent Management Server)		이동 에이전트에 대한 생성, 이주, 복제, 서비스 제공 등의 기능을 담당한다.
	SF (Security Facility)	SP (Service Provider)	플랫폼으로 이주한 이동 에이전트의 역할 티켓의 무결성을 검증하고, 해당 서비스에 필요한 권한을 부여한다.
		SM (Service Manager)	RPMT를 참조하여 해당 역할에게 부여할 수 있는 권한을 확인한다.
		RPMT (Role-Permission Mapping Table)	역할에 따라 부여 될 수 있는 권한들을 정의한다.
	Data Pool		이동 에이전트에게 제공할 데이터를 저장한다.

사용자로부터 생성된 위임할 역할의 등록을 담당하는 RDMA(Role Delegation Mobile Agent)는 그림 4와 같은 위임 티켓을 이용하여 위임할 역할을 RDQ에 등록한다.

DT=(Credential | (Delegating_User | Delegated_User | RoleSet | Depth | Expired_Date))

(그림 4) 위임 티켓의 구조

위임 티켓은 인증에 필요한 신임장과 위임의 주체와 대상, 위임할 역할들의 집합과 또 다른 사용자에게 재 위임할 수 있는 깊이와 위임할 역할의 유효기간으로 표현된다.

DMS는 DT의 위임장을 이용하여 인증 절차를 수행하고, 인증에 성공한 DT를 대상으로 역할 위임 작업을 수행한다. 우선, DMS는 DT의 위임의 주체가 위임하고자 하는 역할들을 RHT, URMT를 통해 확인하고, 이들 중 위임의 대상이 원래 소유하고 있는 역할들과 중복되는지 비교하여 위임이 필요한 역할들만 추출한다. 또한 DMS는 RDQ를 검사하여 이미 할당된 역할이 있는지를 확인하고, 이러한 역할이 존재하면 유효기간을 비교하여 RDQ의 유효기간을 갱신한다. 마지막으로 DMS는 사전에 RDQ에 등록되지 않은 역할들을 대상으로 RDQ에 등록하고 결과를 RDMA에 통보한다. 만일, 위임받은 역할을 재 위임할 경우, DMS는 RDQ를 검사하여 재 위임 가능성을 확인하고, 가능할 경우에만 위임 절차를 진행한다.

4. 결 론

본 논문에서는 이동 에이전트를 이용한 역할 위임 기법을 제안했다. 본 기법은 사용자가 위임하고자 하는 대상과 역할들을 정의하고 이를 시스템에 반영시킴으로써 관리자의 직접적인 개입 없이 역할의 위임이 가능하다. 또한 위임된 역할을 관리하는 RDQ를 사용함으로써 사용자-역할 간의 관계와 역할간의 계층 관계를 표현한 데이터 테이블의 변형을 주지 않고 역할의 위임을 가능하게 한다.

참고 문헌

[1] A. Aneiba and J. S. Rees, "Mobile Agent Technology and Mobility," *Proc. of the 5th Annual Post graduate Symposium on the Convergence of Telecommunications, Networking and Broadcasting(PGNet2004)*, 2004.

[2] D. F. Ferraiolo, R. Sandhu, S. Gavrila, D. R. Kuhn, and R. Chandramouli, "Proposed NIST Standard for Role-Based Access Control," *ACM Trans. on Information and System Security(TISSEC)*, Vol.4(3), pp. 224-274, 2001.

[3] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Younman, "Role-based access control model," *IEEE Trans. on Computer*, Vol.20(2), pp.38-47, 1996.

[4] E. Barka and R. Sandhu, "Framework for Role-Based Delegation Models," *Proc. of the 16th Annual Computer Security Applications Conf.*, 2000.

[5] G.Ahn and B. Mohan, "Secure Information Sharing Using Role-Based Delegation," *Proc. of Int'l Conf. on Information Technology: coding and Computing(ITCC'04)*, 2004.

[6] A.Corradi, R. Montanari, and C.Stefanelli, "Security Issues in Mobile Agent Technology," *Proc. of the 7th IEEE Workshop on Future Trends of Distributed Computing Systems*, 1999.

[7] T. Xinhuai, Z. Yaying, and Y. Jinyuan, "RCACM: Role-Based Context Coordination Model for Mobile Agent Applications," *Proc. of the 2nd Int'l Workshop on Grid and Cooperative Computing*, 2003.

[8] G. Cabri, L.Ferrari, and F. Zambonelli, "Role-Based Approaches for Engineering Interactions in Large-scale Multi-Agent System," *Post-Proc. of Advances in Software Engineering for Large-Scale Multi agent Systems(SELMAS03)*, 2003.