이동 에이전트기반 CSCW 응용을 위한 객체 기반 접근 제어 관리 시스템

장진윤[0] 이승근 안치돈 왕창종
인 하 대 학 교 전 자 계 산 공 학 과
{ellio, sglee, cdahn}@selab.cse.inha.ac.kr, cjwang@inha.ac.kr

Object-based Access Control Management System for Mobile Agents based CSCW Application

Jin-Yoon Chang[0] Seung-Geun Lee Chi-Don Ahn Chang-Jong Wang
Dept. of Computer Science & Engineering, Inha University

요 약

역할 기반 접근 제어 방식은 역할의 포함관계를 갖는 역할 계층을 이용한다. 하지만, 이동 에이전트 기반 CSCW 의 경우 역할의 포함관계를 표현하는 역할 계층으로는 그룹 내에서의 동적인 역할 간의 사용 관계를 표현하지 못한다.

이 연구에서는 작업 그룹에 참여하는 이동 에이전트에 부여된 역할간 사용 방법을 표현할 수 있는 역할 관계 템플릿(Role relation template) 을 제안하고 기존 역할 기반 접근 제어를 확장한다. 제안되는 역할 관계 템플릿은 기존의 사용자와 역할의 관계에서 객체에 부여된 역할과 다른 객체에 부여된 역할 간의 사용 방법을 표현하고, 작업 그룹에서 발생할 수 있는 복잡한 역할 계층에 대한 추상화를 제공하도록 하여 이동 에이전트 기반의 CSCW 응용을 유연하게 지원할 수 있는 접근 제어 시스템을 설계한다. 따라서, 설계되는 시스템은 역할이 필요한 그룹이 생성될 때 상속과 제약이 추가로 생성되는 새로운 역할의 생성을 최소화하고 역할간의 관계를 명시적으로 표현함으로써 동적인 그룹변화에 유연하게 대처할 수 있다.

1. 서론

컴퓨팅 환경의 개방화에 따라 원격화상회의, 원격 교육 시스템, 원격 의료, 공동저작 등과 같은 컴퓨터 지원 공동 작업(CSCW, Computer Supported Cooperative Work) 에 대한 연구와 기존 분산 시스템의 문제 해결을 위한 대안으로써 이동 에이전트를 이용한 공동 작업에 대한 연구가 활발히 진행되고 있다[1].

이동 에이전트 시스템에서는 이동 에이전트의 지역 자원 접근 및 사용에 대한 보안 목적의 인증과 접근 제어가 필요하다[2]. 또한, 공동 작업은 그룹 단위로 다수의 사용자들이 서로의 상호작용을 통해 이루어지게 되며, 이동 에이전트 기반 CSCW응용에서 공동 작업을 위한 상호 작용은 각 사용자에 대한 이동 에이전트들간의 상호 작용에 의하여 이루어지므로 이를 고려한 접근 제어가 필요하다.

기존의 접근 제어 방식으로는 자율적 접근 제어(DAC : Discretionary Access Control) 와 강제적 접근 제어(MAC : Mandatory Access Control), 그리고 역할 기반 접근 제어(RBAC : Role -Based Access Control) 등의 방식이 있다. 특히, 사용자, 역할, 권한, 세션, 역할 계층 및 제약 조건 등의 요소로 구성되는 역할 기반 접근 제어 방식은 정보에 대한 사용자의 권한 부여 여부를 각 사용자의 식별자나 이미 정의된 규칙에 의해 판단하지 않고, 사용자가 소속된 조직 내에서의 역할에 의해 결정하는 방식이다. 즉, 역할과 객체간의 관계에 따라 접근 권한을 관리함으로써, 사용자와 객체의 수가 대단히 많은 환경에 적합한 특성을 제공한다[3][4][5].

그러나, 역할 기반 접근 제어 방식을 이동 에이전트 기반 CSCW 응용에 적용하는 경우, 역할의 포함 관계를 표현하는 역할 계층과 개별 역할에 대한 제약 조건으로 서로 다른 역할을 갖는 이동 에이전트간의 상호 작용에 따르는 동적인 사용 관계와 그 조건을 표현하기에 부족하다[6].

이 연구에서는 작업 그룹에 참여하는 이동 에이전트에 부여된 역할간 사용 방법를 표현할 수 있는 역할 관계 템플릿(Role relation template) 을 정의하고 이를 적용하여 이동 에이전트 기반의 CSCW 응용을 유연하게 지원할 수 있는 접근 제어 시스템을 설계한다.

2. 관련연구

기존의 접근 통제는 강제적 접근 제어, 자율적 접근 제어 그리고 역할기반 접근 제어로 분류할 수 있다. 자율적 접근 제어와 강제적 접근 제어는 각 사용자에게 권한을 직접 할당하여 대규모화되고 복잡화 되는 접근 제어 요구를 만족시키기 어렵다.

반면, 역할 기반 접근 제어는 각 사용자에게 권한을 할당하는 것이 아니라 필요한 역할과 그 역할이 수행할 수 있는 연산을 정책에 맞게 정의하고, 실제 사용자들에게 각자 역할을

할당하는 방식으로 다른 방식에 비하여 분산· 기업환경에적합하고 사용자 추가· 삭제에 대한 복잡도가 감소한다[4][5]. 하지만 이동 에이전트 기반의 CSCW 응용에 그대로 적용하는 경우, 동적으로 생성, 삭제 되는 그룹에서의 상호작용의 특성에 따라 생성되는 역할은 복잡한 역할 계층을 만들게 되며, 각각의 역할을 갖는 에이전트간의 동적인 상호 작용에 따른 역할간 접근에 유연하게 대처하기 어렵다. 즉, 역할의 포함 관계를 표현하는 역할 계층은 이동 에이전트간의 상호작용에 따르는 역할의 사용관계 표현에 부적절 하며 개별 역할에 대한 제약조건은 동적인 역할 사용에 대한 조건을 표현하기에 부족하다[6].

또한, 기존의 이동 에이전트 시스템에서의 접근 제어 방식은 악의적인 이동 에이전트로부터의 시스템 보호와 시스템으로부터의 에이전트 보호 등의 보안 측면에 초점을 맞추고 있으며, 이러한 보안 측면으로써 사용된 제어기법으로는 자율적 접근제어 기법인 접근 제어 리스트(ACL : Access Control List)와 역할 기반 접근 제어 방식 등이 사용되고 있다[7].

따라서, 이동 에이전트 기반의 CSCW 응용을 지원하기 위한 접근 제어는 보안 측면에서의 접근 제어 뿐 아니라, 응용측면에서의 작업을 지원할 수 있어야 하며, 기존의 역할 기반 접근 제어 방식의 확장이 요구된다.

이 연구에서는 이동 에이전트 시스템이 에이전트가 노드에서 수행하는 것을 허용하기 전에 에이전트에 대한 인증을 제공한다고 가정하고, 그룹에 참여하는 이동 에이전트에 능동적이고 정형화된 역할 부여 및 부여된 역할을 갖는 이동 에이전트간의 역할 사용 관계를 표현할 수 있는 역할 관계 템플릿(Role relation template) 을 정의하고 이를 적용한 접근 제어 시스템을 설계한다.

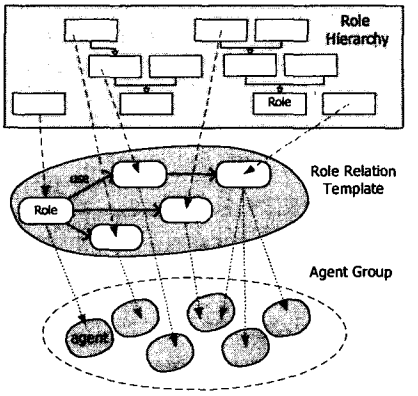
3. 역할 관계 템플릿

이 연구에서의 역할은 에이전트의 집합과 접근 권한의 집합을 동시에 고려하는 그룹화 개념이며, 역할 관계 템플릿은 에이전트 집합과 역할, 역할과 역할간의 사용 관계를 추상화한다. 이러한 역할 관계 템플릿은 에이전트가 자신의 역할을 통한 다른 역할의 에이전트와의 상호 작용위한 접근 권한을 표현한다. 따라서, 역할 관계 템플릿에 의한 기존 역할 기반 접근 제어의 확장은 다음과 같이 정의된다.

[정의1] 역할 관계 템플릿에 의한 확장된 역할 기반 접근 제어

A, R, P, S and T.
(agents, roles, permissions, sessions and role relation template)
$PA \subseteq P \times R$;
$AA \subseteq A \times R$;
$SA \subseteq S \times T$;
$RH \subseteq R \times R$, *is partial order on R, also written as* $\geq$;
$Agent : S \rightarrow A$,
a function mapping each session s_i *to the single agent* $agent(s_i)$;
$template : (R1, R2) \rightarrow T$,
a function mapping $r1_i$ *using* $r2_i$ *to the template* $tempate(r1_i, r2_j)$;
$roles : T \rightarrow 2^R$,
a function mapping each template to a set of roles $roles(t_i) \subseteq \{r | (\exists r' \geq r)[tempate(r1_i r2_j), r' \in SA]\}$ *(which can change with time) and template* t_i *has the permission* $\cup_{r \in roles(ti)}[p | (\exists r'' \leq r)[(p, r'') \in PA]\}$.

[그림 1] 은 이러한 역할 관계 템플릿의 이동 에이전트, 역할 관련 템플릿, 역할 계층에 대한 관련성을 보인다.

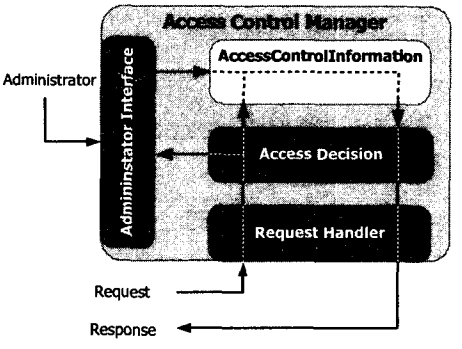


[그림 1] 역할 관련 템플릿

역할 관계 템플릿은 역할의 상속 개념에 의해서 역할의 확장을 표현해야 하는 것으로부터 오는 상속 그래프의 복잡성을 단순화시키고, 그룹에서의 역할의 범위를 명확히 한다.

4. 객체 기반 접근 제어 관리자의 설계

이 장에서는 공동 작업을 지원하기 위한 이동 에이전트 접근 제어 관리자를 설계한다. 설계되는 접근 제어 관리자(Access Control Manager) 는 시스템 관리를 위한 관리자 인터페이스(Administrator Interface) 와 전달되는 접근 요청에 대해서 접근 제어 기능을 제공하기 위한 접근 결정기(Access Decision) 및 요구 처리기(Request Handler) 로 구성되며, 역할 관계 템플릿을 포함한 역할별 접근 가능한 객체의 정보를 관리한다. [그림 2] 는 접근 제어 관리자의 구성도이다.



[그림 2] 접근 제어 관리 시스템 구성도

4.1 접근 결정기

에이전트가 특정 객체에 대한 접근 또는 역할 관계 템플릿에 따른 다른 역할의 사용을 위해서는 접근 결정기로부터의 승인이 있어야 하며, 이를 위해서 그룹 식별자, 역할, 사용할 객체와 접근하려는 방법 또는 사용할 역할과 그 메소드 등을 이용해서 질의한다. 접근 결정기는 해당 질의에 따라 역할별로 정의되어 있는 접근 제어 정보를 이용해서 사용자가 특정

객체에 대한 권한이 있는지를 조사하는 기능을 수행한다.

또한, 접근 제어 정보는 3 장에서 정의한 역할 관계 템플릿을 포함한 역할 및 권한 등 접근 결정기가 접근 제어를 위하여 사용하는 자료 구조이다. [리스트1]은 접근 제어 시스템에서 관리되는 자료구조를 보인다.

[리스트1] 접근 제어 정보의 자료구조

```
enum Permission {READ, WRITE};
struct ObjectData {
  ObjectID objectID;          // 객체 식별자
  Permission permission       // 객체에 부여된 권한
};
typedef sequence<ObjectData> ObjectDataList;
string Passive_role.method;   //객체 역할에 대한 메소드
typedef sequence<Passive_role.method> PRmethodList;
struct RoleRelation{
  Role active_role;           // 역할 사용의 주체 역할
  Role passive_role           // 역할 사용의 객체 역할
  PRmethodList passive_role_methodLis t; //역할에 대한 메소드리스트
};
typedef sequence<RoleRelationData> RoleRelationDataList;
struct RoleTemaplte{
  GroupID groupID;            // 에이전트 그룹 식별자
  RoleRelationDataList;       // 역할-역할 사용 리스트
};
struct AccessControlData {
  GroupID groupID;            // 에이전트 그룹 식별자
  Role role;                  // 사용자 그룹에 할당된 역할
  RoleTemplate roleTemplate;  // 역할 관계 템플릿
  ObjectDataList objDataList; // 객체-권한 리스트
};
typedef sequence<AccessControlData> AccessContolInform ation;
```

4.2 관리자 인터페이스

관리자 인터페이스는 관리자가 접근 제어를 위한 시스템을 유지 및 관리 하기 위하여 제공되는 인터페이스이다. 관리자는 이를 이용하여 접근 권한, 역할의 할당 등의 작업을 수행한다. [리스트 2] 는 접근 제어 관리자에서 관리자를 위하여 제공되는 인터페이스를 보인다.

[리스트 2] 접근 제어 관리자의 관리 인터페이스

```
interface ManagerAdmin {
  boolean createRole (in GroupID groupID, in Role role,
            in Object obj, in Permission permission );
  boolean discardRole( in GroupID groupID, in Role role);
  boolean addPermission ( in GroupID groupID, in Role role,
            in Object obj, in Permission permission );
  boolean deletePermission (in GroupID groupID, in Role role,
            in Object obj, in Permission per mission );
  boolean createTemplate (in GroupID groupID,
           in RoleRelationList relationList );
  boolean discardTemplate (in GroupID groupID, in RoleTemplte template );
  boolean addRelation (in GroupID groupID, in RoleRelation relation);
  boolean removeRelation (in GroupID groupID, in RoleRelation relation);
  boolean modifyRight(in GroupID groupID, in Role role,
                      in Object obj, in Right right);
  boolean createGroupData(in GroupID groupID);
  boolean deleteGroupData(in GroupID groupID);
  boolean inherit(in GroupID groupID, in Role parentRole,
                  in Role childRole , Constraint constraint );
};
```

4.3 요구 처리기

요구 처리기는 에이전트가 특정 객체나 상호작용을 위하여 다른 역할이 할당된 에이전트에 대한 접근 요구를 받아들이고 이를 접근 제어기에 전달하며, 결정된 승인 여부를 요구한 에이전트에게 통지하는 기능을 수행한다.

5. 결론

이 연구에서는 CSCW 응용을 위한 이동 에이전트 시스템에서의 객체 기반 접근 제어 관리 시스템을 설계하였다. 설계된 시스템은 기존의 역할 기반 접근 제어 방식에 역할간의 사용 관계를 표현할 수 있는 역할 관련 템플릿을 사용한다. 이 템플릿은 기존의 사용자와 역할의 관계에서 객체에 부여된 역할과 다른 객체에 부여된 역할 간의 사용 관계를 표현하고, 작업 그룹에서 발생할 수 있는 복잡한 역할 계층에 대한 추상화를 제공한다. 따라서, 새로운 역할이 필요한 그룹이 생성될 때 상속과 제약이 추가로 생성되는 새로운 역할의 생성을 최소화하고 역할간의 관계를 명시적으로 표현함으로써 동적인 그룹변화에 유연하게 대처한다.

향후 연구 과제로는 설계된 접근 제어 시스템을 이용하여 CSCW 응용에서의 공동 작업에 필수 적인 공유객체 관리 방식에 대한 연구가 필요하며, 이동 에이전트 기반의 CSCW 응용 개발을 위한 프레임워크에 대한 연구가 요구된다.

5. 참고 문헌

[1] Hyacinth S. Nwana, "Software Agents : An Overview, " Knowledge engineering Review, Vol 11, No3, 1996.

[2] T.Taka, T.Mizuno, T.Watnabe. "A Model of Mobile Agent Services Enhanced for Resource Restrictions and Security", IEEE 0-8186-8603-0/98, 1998

[3] J. Barkley, "Comparing Simple Role Based Access Control Models and Access Control Lists, " National Institute of Standards and Technology, Aug, 1995.

[4] Sandhu, R.S., et al., "Role-Based Access Control Models," IEEE Computer, Vol 29, No2, 1996. pp. 38-48.

[5] David F. Ferraiolo, J anet A. Cugini, D. R ichard. Kuhn, "Role-based access control : Features and Motivations ," 11th Annual Computer Security Applications Co nference, 1995.

[6] John Barkley, Konstantin Beznosov, Jinny Uppal, "Supporting Relationships in Access Control Using Role Based Access Control, " pp55 -65, Proceedings of the 4 th ACM workshop on Role-based access control, Oct, 1999.

[7] G. Cabri, L. Leonardi, F. Zambonelli, "Mobile-Agent Coordination Models for Internet Applications", IEEE Computer, Vol. 33, No. 2, Feb. 2000.