분산 가상 환경에서 역할 기반 접근 제어 관리자 설계

정헌만[0] 탁진현 이세훈* 왕창종
인하대학교 전자계산공학과, 인하공업전문대학 전자계산기과
e-mail : hmjung@true.inhatc.ac.kr, tak@selab.cse.inha.ac.kr
seihoon@ true.inhatc.ac.kr, cjwangse@inha.ac.kr

A Design of Role Based Access Control Manager in Distributed Virtual Environment

Heon-Man Jung[O] Jin-Hyun Tak Sei-Hoon Lee* Chang-Jong Wang
Dept. of Computer Science & Engineering, Inha University
*Dept. of Computer Engineering, Inha Technical College

요 약

분산 가상 환경은 고속 통신망과 컴퓨팅 환경의 고급화로 응용 분야를 넓혀 가고 있으며, 보다 현실감 있는 상호작용으로 인해 만남과 대화, 협력 작업, 상거래, 오락 등의 인간의 사회적 활동을 지원하는 새로운 수단으로 자리잡고 있다. 가상 도시와 같은 대규모의 가상 환경에는 공원이나 거리, 건물의 로비 등과 같은 개방적인 공간과 사무실과 같은 업무 공간, 그리고 쇼핑몰과 같은 상거래 공간들이 공존하게 되므로 접근 제어와 보안이 보다 중요한 문제로 대두된다.

따라서, 이 논문에서는 분산 가상 환경내의 모든 사물들을 객체로 인식하고, 객체에 대한 역할을 기반으로 하는 접근 제어 모델을 제안하고, 제안한 모델을 기반으로 접근 제어 관리자를 설계하였다. 설계된 접근 제어 관리자는 가상 환경내 공간의 객체 뿐만 아니라 공간 자체도 하나의 객체로 인식하여 접근 제어를 하였다. 또한, 대규모 공간에서의 중요한 특징인 관리의 용이성과 동적인 변경을 가능하게 하기 위해, 역할을 기반으로 참여자와 객체를 연결하고, 객체가 갖고 있는 행위까지를 제어할 수 있었다.

1. 서론

다중 참여자의 상호작용을 지원하는 분산 가상 환경은 기존의 CSCW(Computer Support Collaborative Work) 환경에 비해 참여자 간의 상호작용을 보다 현실감 있게 지원할 수 있다는 장점을 지닌다[1,2]. 분산 가상 환경은 인터넷등의 통신망의 고속화와 개인 컴퓨팅의 고급화로 인해, 대중적으로 수용할 수 있는 인프라가 갖추어지면서, 컴퓨터를 기반으로 보다 현실감 있는 상호 작용과 협력 작업을 원하는 모든 응용 분야에 중요 기술이 되고 있어, 인간의 사회적 활동을 지원하는 새로운 수단으로 자리잡고 있다[3].

이러한 분산 가상 환경의 대표적인 연구는 군사 작전 시뮬레이션을 위한 SIMNET[4], NPSNET[5]등이 있으며, 상호 작용을 보다 발전시킨 Spline[6], Massive[7] 등이 있다. 인터넷이 통신망의 기반 인프라로 자리를 확실히 함으로써, 인터넷의 웹서비스를 기반으로 3 차원 가상 환경을 대중적으로 지원하기 위해 VRML 등의 표준 기술들이 발표되었고 OpenCommunity[8], BlacxxonInterative[9]등이 대표적이다.

기존의 분산 가상 환경 연구에서의 가장 큰 관심사는 참여자들 간의 인식 전달을 통한 가상 공간의 공유와 공유 객체에 대한 접근 제어를 통한 일관성 유지 등의 다중 사용자 지원에 있었다. 하지만 자유로운 만남과 업무 공간이 공존하는 복잡한 가상 환경에서는 보안(security)에 대한 고려가 필요하다.

따라서 이 논문에서는 분산 가상 환경의 모든 사물

즉 공간까지도 하나의 객체로 인식하여, 참여자와 객체와 객체의 행위까지를 역할을 기반으로 하여 연결하는 모델을 제안하고 접근 제어 관리자를 설계한다.

2. 접근 제어 관련 연구 고찰

이 장에서는 기존의 접근 제어 방식을 고찰하고 전통적인 보안 접근의 단점을 극복하기 위한 문제를 제기한다. 또한 분산 가상 환경 시스템의 공간 모델에 대해 설명하고 공간 영역에서의 기존의 접근제어 방식의 단점을 해결할 수 있는 방법을 제시한다.

2.1 기존 분산 환경에서의 접근 제어 방식

접근 제어 정책은 크게 자율적 접근 제어 정책, 강제적 접근 제어 정책, 그리고 역할 기반 접근 제어 정책 등이 있다.

· 자율적 접근제어

자율적 접근제어 정책(Discretionary Access Control, DAC)은 주체나 또는 그들이 소속되어 있는 그룹들의 신분(ID)에 근거하여 객체에 대한 접근을 제한하는 방법이다.[10] 즉, 접근 통제는 객체의 소유자에 의하여 임의적으로 이루어진다. 그러므로 어떠한 접근 허가를 가지고 있는 한 주체는 임의의 다른 주체에게 자신의 허가를 넘겨줄 수 있다.

DAC 정책에서 내재적으로 상속되어지는 결점은 DAC 속성상 접근은 주체의 ID 에 전적으로 근거를 두고 있어서 메커니즘은 데이터의 의미에 대한 아무런 지식도 갖고 있지 않으며 이에 근거하여 접근 허가를 결정하지 않는다.

· 강제적 접근제어

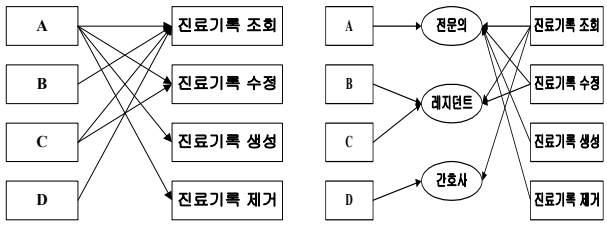
강제적 접근 제어 정책(Mandatory Access Control, MAC)은 객체에 포함된 정보의 비밀성과 이러한 비밀정보에 대하여 주체가 갖는 정형화된 권한에 근거하여 객체에 대한 접근을 제한하는 방법이다.[10]. MAC 정책은 DAC 정책에 비해 객체의 소유자에 의하여 변경할 수 없는 주체와 객체간의 접근제어 관계를 정의하며 주체가 객체를 판독하고 그 내용을 다른 객체에게 복사하는 경우에 원래의 객체에 내포된 MAC 제약사항이 복사된 객체에 전파된다. MAC 정책은 모든 주체 및 객체에 대하여 일정하며, 어느 하나의 주체대 객체 단위로 접근 제한을 설정할 수 없다.

· 역할기반 접근제어

시스템이 대규모화되고 다양해지면서 조직들은 그 조직 특성에 적합한 복잡한 보안 정책을 필요로 하게 되었고, 보안 정책의 일관성 유지 및 보안 정책의 변경을 실제 시스템에 적용하기 위한 비용이 높아졌다. 앞에서 언급한 기존의 자율적 접근제어와 강제적 접근제어의 메커니즘인 접근 제어 목록, 능력기반 접근제어, 레이블 기반 접근 제어 기법들은 규칙 수준에서 접근 제어 서비스를 제공하기 때문에 위와 같은 요구를 만족시키기 어렵다. [11].

기존의 접근 제어 기법에서는 각 사용자에게 권한을 할당하는 반면, 역할-기반 접근 제어 기법에서는 필요한 역할(Role)과 그 역할이 수행할 수 있는 연산을 보안 정책에 맞게 정의한 후, 실제 사용자들에게 각자 역할을 할당하는 기법이다.

[그림 1]는 기존의 접근권한 부여 방식과 역할기반 접근제어 메커니즘을 비교하고 역할기반 접근제어 방식의 장점을 나타내는 그림이다.



(a) 기존의 접근 제어 (b) 역할 기반 접근 제어

[그림 1] 접근 제어 메커니즘의 비교

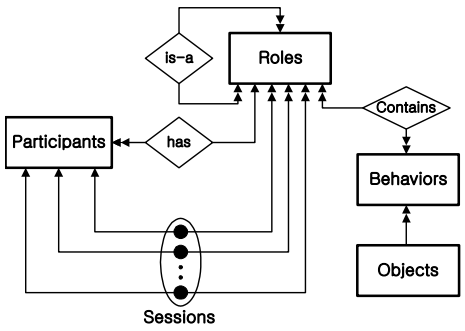
[그림 1]과 같이 역할 기반 접근 제어 기법은 보안 정책 관리자에게 사용자와 자원 접근 권한의 관계를 독립적으로 생각할 수 있게 함으로써, 추상화된 보안 정책의 적용이 가능하기 때문에 보다 효율적으로 보안 정책을 관리할 수 있다.

3. 역할 기반 접근 제어 모델의 설계

이 논문에서는 가상 공간에서 참여자의 역할에 따라 공간 영역 사이의 경계를 통한 진입 여부와 공간 내 객체에 대한 접근 허가 여부를 결정하는 공간 영역에 대한 역할 기반 접근 제어 모델을 제안하고 설계한다.

3.1 역할 기반 접근 제어 모델 제안

모델은 공간 영역 및 객체에 대한 접근 권한을 역할에 부여하고, 참여자가 역할을 부여 받아 접근 권한을 할당 받음으로써 접근 제어를 실행한다. 본 논문에서는 이러한 RBAC 모델을 기반으로 가상 환경에서 역할에 따른 객체 접근 제어 모델을 제안한다. [그림 2]은 제안된 모델의 개체(entity)와 개체들 간의 관계를 나타낸다.



[그림 2] RBAC 모델의 개체들간의 관련성

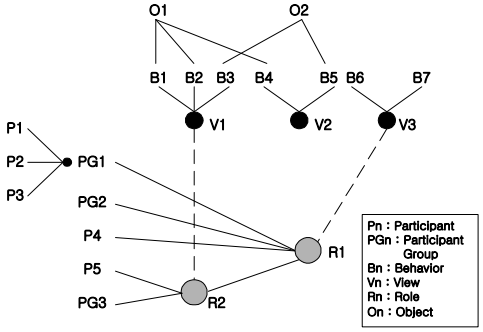
3.1.1 모델의 개체

모델의 개체는 참여자, 조작 권한, 객체, 역할, 세션으로 구성된다. 이러한 모델의 개체들을 정형화하여

표현하면 다음과 같다.

- 참여자(Participant) P = { $p_1, p_2, p_3, \ldots, p_i$ }
- 조작 권한(Behavior) B = { $b_1, b_2, b_3, \ldots, b_i$}
- 객체(Object) O = {$o_1, o_2, o_3, \ldots, o_i$ }
- 역할(Role) R = { $r_1, r_2, r_3, \ldots, r_i$ }, $r_k \in \wp(U) \times \wp(P)$
- 세션(Session) S = { $s_1, s_2, s_3, \ldots s_4$}

[그림 3]은 참여자/참여자 그룹, 뷰, 역할, 조작 권한, 객체의 관계를 나타낸다. 역할 객체 접근제어 정책은 역할 R : P × $\wp$(B)에서 함수 fr{u,b}로 표시할 수 있다. 즉, 역할객체 접근제어 정책은 참여자 집합 및 참여자를 조작권한의 집합으로 매핑하는 함수로 표현할 수 있다. 세션은 참여자 그룹의 역할 수행 단위이며 세션의 개념은 일반 접근제어에서 참여자를 대신하는 주체(Subject)의 개념과 동일하다. 각 세션은 단 하나의 참여자와 관계하고, 세션은 한 참여자에게 가능한 여러 역할을 수행할 수 있게 한다.



[그림 3] 참여자/참여자 그룹, 뷰, 역할, 조작권한, 객체의 관계

3.2 역할 그래프 모델

역할 그래프 모델(role graph model)은 역할의 계층, 상속 그리고 개별 역할을 보다 명확하게 표현하기 위해 도입 된다. 역할 그래프 모델에서 역할은 노드로 표현되고, 노드간의 링크는 역할간의 관계를 표시한다.

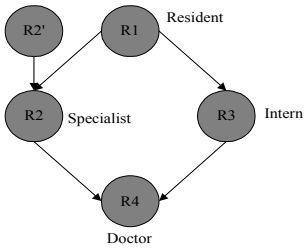
3.2.1 역할의 계층과 다중 상속

역할은 비순환 유향 그래프(directed acyclic graph)의 역할 계층도로 구성된다. 역할 계층에서 접근 권한은 상,하위 역할간의 천이 관계에 따라 계승될 수 있고, 반 순서 지배 관계를 만족하는 다중 계승이 이루어질 수 있다. [그림 4]는 역할의 계층도에서 역할 R2, R4 간에 “is-a”관계는 역할 R2 는 역할 R4 에 정의된 모든 조작 권한을 상속한다는 것을 의미한다. 역할 R1 은 역할 R2 와 R3 로부터 조작 권한을 상속 받고, 추가적인 특정 권한을 가질 수 있다. 이러한 다중 역할의 상속을 “다중 상속”이라 부른다.

역할 기반 접근 제어에서 역할 상속은 역할 상속을 지원하지 않는 접근 제어 보다 사용자에 대한 권한 부여를 구조화하는 향상된 방법을 제공한다. 그러나, 역할 계층은 권한 상속의 범위와 개별 권한의 사용에 대해서 문제가 될 수 있다.

3.2.2 개별 역할

상속을 통한 권한 할당은 접근 제어 관리를 단순화하지만, 권한 상속의 범위는 제한되어야 한다. 예를 들어, 어떤 특별한 조작 권한은 역할의 상위 계층에서 하위 계층으로 전달되어서는 안 된다. 상속 제한은 하위 역할 할당을 위한 새로운 개념이 요구된다.

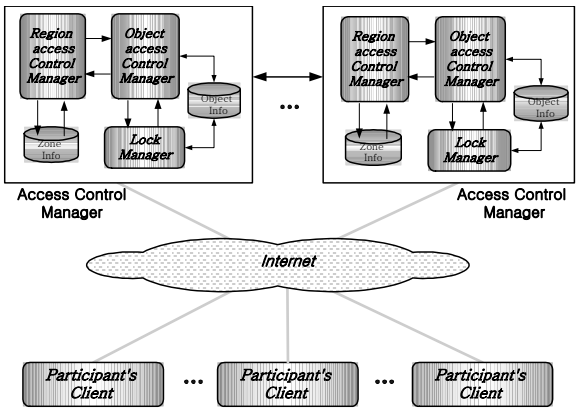


[그림 4] 역할 상속 및 개별 역할

[그림 4]는 역할 R1 이 역할 R2 와 R3 의 권한을 상속하지만, 역할 R2 는 R1 이 권한의 일부를 상속하지 않기를 원할 수 있다. 개인 권한 상속 문제를 해결하기 위해서, 역할 R2 의 개별 역할 R2’를 도입한다. 개별 역할(private role) R2’는 병원에서 전문의의 개인 권한 만을 포함하는 특별한 역할이다.

3.3 역할 기반 접근 제어 리자 설계

역할 기반 접근 제어 관리자는 영역 접근 제어 관리자(Region Access Control Manager)와 객체 접근 제어 관리자(Object Access Control Manager), 록 관리자(Lock Manager)로 구성되며, 시스템 구성도는 [그림 5]과 같다



[그림 5] 가상 환경에서의 역할 기반 접근 제어 관리자

역할 기반 접근 제어 관리자는 가상 환경에서 walk 경계에 의해 구분되는 영역마다 하나씩 존재하고, 가상 공간 내의 참여자가 공간 영역 사이의 boundary 객체를 통과 하고자 할 때 참여자의 역할에 따라 접근을 결정하고 영역내의 객체에 대한 접근을 참여자의 역할에 따라 수락/거부를 결정하며, 참여자 사이트에 복제 분산된 객체의 일관성을 유지하기 위해 병렬성 제어 기법을 제공한다. 참여자가 가상 환경 내에 들어

오면 참여자 사이트로 영역 접근 제어 관리자와 객체 접근 제어 관리자, 존 정보 테이블과 객체 정보 테이블을 전송하여 참여자 사이트에서 역할에 따른 접근 제어를 함으로써 전체적인 이벤트의 양을 줄이며 존 정보 및 객체 정보에 대한 변경이 있을 경우에 참여자 사이트로 변경 정보를 전송한다.

3.3.1 영역 접근 제어 관리자

영역 접근 제어 관리자(Region Access Control Manager)는 참여자가 경계(boundary) 객체에 의해 구분된 영역을 통과하기 위해 충돌(collision) 이벤트를 발생시키면 참여자의 ID 에 할당된 접근 허가 역할(PermmittedRoles)을 영역 정보 테이블 내의 PermittedRoles 과 비교하여 통과 여부를 결정하고 영역 정보 테이블의 최대 참여자 수를 참조하여 영역 내의 제한 인원이 초과된 경우에는 접근을 통제한다. 객체가 참여자의 이동에 의하여 경계 객체에 의해 구분된 영역을 통과하여 이동할 경우에는 객체를 관리하던 객체 접근 제어 관리자에게 객체 정보 테이블내의 객체 정보를 요청하여 객체가 이동된 해당 객체 접근 제어 관리자에게 전송하고 또한 참여자 사이트에도 변경 정보를 전송한다. 영역 접근 제어 관리자가 관리하는 영역 정보 테이블의 속성은 [표 1]와 같다.

[표 1] 영역 정보 테이블

RegionID	Permitted Roles	Access Property		
		Max_ Exist	Present_ Exist	Group Policy

PermittedRoles 은 영역 내로 들어올 수 있는 참여자의 역할들을 나타내고, MaxExist 는 영역 내에 존재할 수 있는 최대 참여자 수를, PresentExist 는 현재 영역 내에 존재하는 참여자 들을 나타낸다. GroupPolicy 는 지역 안으로 통과할 수 있는 그룹 정책을 나타낸다.

모델에서의 그룹 접근 정책은 참여자들의 그룹 단위의 접근을 처리하기 위해 다음과 같이 공식화된 다른 방법을 제공한다. 정책이 max 인 경우는 Max(전문의, 레지던트, 시민) = 전문의의 역할을 적용하고 정책이 min 인 경우는 Min (전문의, 레지던트, 시민) = 시민의 역할을 적용하여 그룹을 제어한다.

3.3.2 객체 접근 제어 관리자

객체 접근제어 관리자(Object Access Control Manager)는 영역 내에서 객체에 접근을 시도하는 참여자의 이벤트를 받아 참여자 ID 에 할당된 접근 허가 역할(PermittedRole), 객체 ID, 행위 정보와 해당 영역의 객체 정보 테이블에 있는 정보와 비교하여 접근 여부를 결정한다. 또한 영역간의 객체 이동 시 객체 접근 제어 관리자의 객체 정보 테이블에 대한 정보 제공 및 변경에 대한 요청을 수행한다. [표 2]는 객체 정보 테이블의 속성이다.

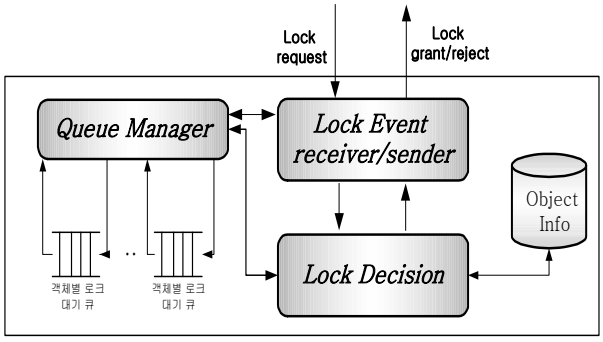
[표 2] 객체 정보 테이블

Object ID	Permitted Roles	Behavior	State	Owner ID	Service_ Participant

ObjectID 는 영역 내에 있는 객체들의 아이디이고, PermittedRoles 은 그 객체에 접근할 수 있는 접근 허가 역할을 나타낸다. Behavior 는 객체에 대한 조작 형태를 나타내며 OwnerID 는 객체를 소유하고 있는 참여자의 아이디를 나타낸다. 또한 State 는 객체의 록/언록 상태를 나타내며 ServiceParticipant 는 현재 그 객체를 사용하고 있는 참여자의 아이디이다.

3.3.3 록 관리자 (Lock Manager)

록 관리자는 [그림 6]와 같이 구성되며 경계에 의해 구분되는 영역 내에 존재하는 객체들에 대한 참여자의 접근 요구 시 객체에 대한 록 요청 및 언록 요청을 통제하고 객체에 대한 conflict 발생시 동시 접근을 제어 한다.



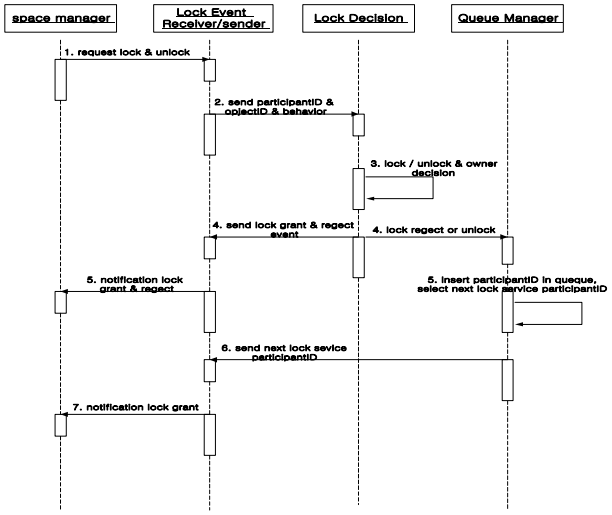
[그림 6] 록 관리자

록 이벤트 수신/송신자는 참여자의 객체 접근 이벤트를 받아 록 결정 모듈에 록 요청을 하고, 객체의 조작 완료 이벤트 시 언록 요청을 하며, 객체에 대한 록 허가(grant) 및 거부(reject) 메시지를 참여자에게 통보한다. 큐 관리자(Queue Manager)로부터 받은 록 대기 참여자 ID 에 해당하는 참여자에게 록 허가 메시지를 보낸다.

록 결정 모듈은 객체에 대한 록 요청 이벤트에 대하여 영역 내 객체 정보 테이블의 상태 (록/언록)를 조사하여 허가 및 거부를 결정하고 허가 되면, 록 이벤트 수신/송신자를 통해 참여자에게 접근 허가 메시지를 보낸다. 록이 거부되면 큐 관리자에게 록을 요청한 참여자 ID 를 전송하며 해당 객체가 언록되면 큐 관리자에게 객체가 언록 되었음을 알린다. 객체가 록 되었을 경우 객체의 소유자가 객체에 대한 조작을 시도하면 록을 객체 소유자에게 부여하고 조작중인 사용자는 해당 객체 록 대기 큐에 저장된다. 객체가 언록되고 그 객체에 대해 록을 요청하는 참여자가 없으면 해당 객체의 록은 록 관리자가 소유한다

큐 관리자는 참여자가 록을 요청한 객체가 다른 참여자에 의해 록 되었을 때 해당 객체 록 대기 큐에 참여자 ID 를 저장하고 록을 기다리는 객체가 언록 되었을 때 해당 객체 대기 큐 내에 대기하는 참여자 ID 를 록 이벤트 수신/송신자에게 보낸다.

참여자는 자신의 브라우저에서 해당 객체를 조작함과 같은 영역 내에 존재하는 참여자에게 조작을 멀티케스트로 알린다.



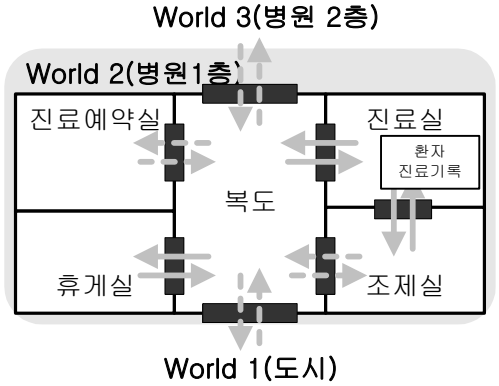
[그림 7] 로크 관리자에서의 록/언록 동작 과정

4. 실험 및 평가

4.1 역할 기반 접근 제어 모델

제안한 모델은 공간적 영역 사이의 경계 객체를 이용한다. 이 경계는 기존 가상 환경들에서의 공간 구분 단위의 경계로 대응되어 적용될 수 있다. 참여자가 특정 영역에 진입하기 위해서는 현재 속해 있는 영역과 진입하고자 하는 영역 사이의 경계 객체를 통과하여야 한다.

[그림 8]는 모델을 설명하기 위한 가상 병원의 예이다. 검은 색 사각형으로 표현된 경계는 서로 다른 가상 세계 사이의 portal(점선) 일 수 도 있고, 걸어서 통과 할 수 있는 것(실선)일 수도 있다. 각각의 영역들은 자신의 진입 경계를 통과할 수 있도록 허가된 역할들을 갖고 있고, 참여자들은 할당된 역할을 가지고 인증 과정을 거쳐 진입 경계를 통과하게 된다.



[그림 8] 병원에서의 영역과 경계

가상환경 내에서 역할에 의한 접근 제어의 적법함을 보이기 위해 [그림 8]의 가상 병원 내에 방문자가 들어 와서 진료 예약을 하고 진료를 받는 경우와 참여자의 역할에 따른 객체 접근 제어 방법에 대해 모의 실험을 진행한다.

4.2 방문자 진료 예약 시

실험을 위해 진료 예약실의 Permitted_Roles = {전문의, 레지던트, 간호사, 시민}, 진료실의 Permitted Roles = {전문의, 레지던트, 간호사, 시민}, 조제실의 Permitted_Roles = {전문의, 간호사}로 가정한다. 참여자 아이디가 없는 새로운 방문자가 가상 병원에 들어오면 아이디와 '시민'이라는 역할을 부여 받는다.

참여자가 예약을 위해 진료 예약실 내로 접근 시도를 하면 예약실의 boundary 경계를 관리하는 영역 접근 제어 관리자는 [표 3]의 예와 같이 진료 예약실의 제한인원이 초과되지 않았으므로 참여자의 역할 '시민"과 진료 예약실 영역 정보 테이블[표 3]의 역할을 비교한 후 접근을 허가한다.

[표 3] 지역관리자의 영역 정보 테이블

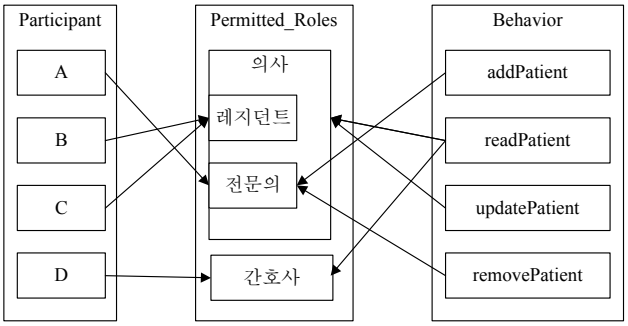
Region_ Name	Permitted_ Roles	Max_ Exist	Present_ Exist	Group_ Policy
진료 예약실	전문의 레지던트 간호사 시민	10	5	Max Or Min
조제실	레지던트 간호사	3	1	Max Or Min

또한 방문자는 진료실의 경계를 지나 진료를 받을 수 있으며, 조제실 영역으로 접근을 시도할 경우 조제실의 영역 정보 테이블의 Permitted_Roles 에 '시민'은 정의 되지 않았으므로 접근이 허가되지 않는다.

4.3 참여자의 객체 접근 시

참여자의 영역 내 객체에 대한 역할 접근 제어를 보이기 위해 참여자의 등급을 간호사와 의사로 구분하고, 의사 역할에서 레지던트와 전문의의 역할을 상속하여 정의한다. 참여자의 역할에 따라 허용하는 접근 수준을 달리 정의하기 위해 기본적인 진료 행위의 연산을 환자 진료 기록 추가, 삭제, 변경, 읽기의 네 가지 권한으로 구분하고 적법한 권한 사용과 불법적인 사용에 대해 예를 보인다.

실험을 위하여 4 명의 진료진을 전문의 1 명(A)과 레지던트 2 명(B, C), 간호사 1 명(D)으로 구성하였다. 구성된 진료진과 역할, 그리고 권한 관계는 [그림 9]과 같이 표현될 수 있다



[그림 9] 진료에 있어서 사용자, 역할 그리고 권한의 관계

레지던트 역할의 사용자 B, C 는 영역 내 하나의 객체로 볼 수 있는 환자 진료 기록[그림 9]에 읽기와 변경만 가능하고, 전문의 역할의 사용자 A 는 추가, 삭제, 변경, 읽기를 할 수 있다고 가정한다. 이 경우의 역할의 자료 구조는 [표 4]과 같은 형태로 정의 된다. [표 4]의 권한에서 + 접두어가 붙은 것은 해당 역할을 상속할 때 상속되는 공용 접근 권한을 의미하여, -접두어가 붙은 것은 개별 접근 권한을 의미한다.

본 실험에서는 다음에 제시하는 두 가지 연산들로 제시한 모델의 공간 내 객체에 대한 역할 기반 접근 제어 기능을 검증한다.

· 사용자 A 의 환자 진료 기록 추가 연산
request(전문의, A, addPatient)
· 사용자 B 의 환자 진료 기록 갱신 연산
request(레지던트, B, removePatient)

[표 4] 환자 진료 기록 객체에 대한 역할의 자료 구조

Permitted _Roles	Inherits from	Behavior	Participant
의사	_defaultRole	+readPatient	A,B,C
간호사	_defaultRole	+readPatient	D
레지던트	의사	+readPatient -updatePatient	B,C
전문의	의사	+readPatient -pdatePatient -removePatient +addPatient	A

첫 번째 연산의 경우 전문의 역할의 자료에서 참여자 A 가 등록되었다는 사실을 알 수 있고, 전문의 역할에는 환자 진료 기록 추가 연산이 정의되어 있음을 알 수 있으므로, 해당되는 요청은 정상적으로 처리된다. 그러나 두 번째 연산에 있어서는 레지던트 역할의 자료에서 참여자 B 가 등록되어 있지만, 레지던트 역할에는 환자 진료 기록 삭제 연산이 정의되어 있지 않으므로, 이러한 경우 이벤트 서비스를 통해 오류가 발생했음을 통보 받게 된다.

이 장에서는 공간 영역에서 역할 기반 접근 제어를 이용한 시뮬레이션 방식의 실험을 통하여 제안한 접근 제어 설계가 공간 영역 기반의 가상 환경 응용에 적합함을 보였다.

5. 결론

이 논문에서는 경계 객체로 구분되는 영역별로 접근이 허용된 역할을 가진 참여자만이 진입할 수 있도록 하는 공간 영역에 대한 접근 관리 모델을 제안하고, 제안한 모델을 기반으로 접근 제어 관리자를 설계하였다. 설계된 접근 제어 관리자는 기존 가상 환경 시스템들에서 제공하는 공유 객체에 대한 접근 제어 뿐만 아니라 공유 객체들이 속해 있는 공간적 영역에 대한 역할 기반의 접근 제어를 제공함으로써, 개방된 공간과 보안이 요구되는 공간이 공존하는 대규모의 복잡한 가상 환경의 보안 정책을 쉽게 관리할 수 있도록 해준다.

또한, 참여자의 역할 상속 및 개별 역할 개념을 도입하여 지속적으로 규모가 확장되는 가상공간의 다양한 접근 제어 요구를 효율적으로 관리할 수 있다.

향후 연구 방향으로는 공간 내의 영역별 보안성에 근거한 공간 접근 제어를 지원하도록 확장하는 것이다.

참고문헌

[1] 성운재, 심재한, 원광연, “다중 참여자 네트웍 가상현실 시스템을 위한 복수 멀티캐스트 통신구조,” 한국 시뮬레이션 학회 논문지 7 권 1 호, 1998. 7

[2] 탁진현, 이승근, 장진윤, 이세훈, 왕창종, “관련 영역 관리 방식을 이용한 가상 공간 관리기의 설계,” 제 9 회 HCI 학술 대회, 2000. 1

[3] Robert Rockwell, “An Infrastructure for Social Software,” IEEE SPECTRUM, 1997.3

[4] Miller, D., and J.A.Thorpe. SIMNET : The advant of simulator networking. In proceedings of the IEEE 83(3) : 1114-1123, August 1995

[5] Macedonia, M. Zyda, M., Pratt, D., and Barham, P., “Exploiting Reality with Multicast Groups: A Network Architecture for Large-scale Virtual Enviroments,” in Proc 1995 IEEE VRAIS ’95, 1995

[6] Barrus, J., Anderson, D., “Locales and Beacons,” in Proc 1996 IEEE VRAIS ’96, 1996

[7] MASSIVE 1,2,3 available at MASSIVE Web site : http://www.crg.cs.nott.ac.uk/research/systems

[8] Open Community Web site : http://www.meitca.com/opencom

[9] Blaxxun Web site : http://www.blaxxun.de/products/index.html

[10] D.F. Ferraiolo, j, Cugini and R. Kuhn, “Role-Based Access Control : Features and Motivations,” National Institute of Standards and Technology, August, 1995.

[11] S.I. Garila, J.F. Barkley “Formal Specification for Role Based Access Control User/Role and Role/Role Relationship Management,” National Institute of Standards and Technology, 1998.