u-헬스케어 지원 분산 프레임워크에서 접근 제어 모델을 이용한 동적 보안 서비스☆

A Dynamic Security Service using Access Control Model in Distributed Framework Support for u-Healthcare

정 창 원* 김 동 호** 김 명 희*** 주 수 종****
Chang-Won Jeong Dong-Ho Kim Myung-Hee Kim Su-Chong Joo

요 약

본 논문은 분산 보안 정책을 지정하기 위해 객체그룹을 사용하는 u-헬스케어 컴퓨팅 환경에서 응용 서비스를 위해 동적 보안 서비스를 지원하는데 설계된 보안 객체에 대해 기술한다. 특히 u-헬스케어를 위한 분산 프레임워크의 보안 정책과 규칙 그리고 접근 제어에 사용되는 오퍼레이션을 포함한 보안 객체에 중점을 두었다. 그리고 DPD-Tool을 이용하여 서버 프로그램으로 구현된 객체들의 접근권한 부여 절차 및 클라이언트 프로그램 개발 과정을 보였다. 또한 DPD-Tool을 이용하여 모바일 모니터링 응용 개발 절차를 통해 u-헬스케어 지원 분산 프레임워크에서 지원하는 동적 보안 서비스의 수행성을 검증하였다.

Abstract

This paper describes a security object designed to support a dynamic security service for application services in u-healthcare computing environments in which domains are used to object groups for specifying security policies. In particular, we focus on security object for distributed framework support for u-healthcare including policy, role for security and operations use to access control. And then, by using the DPD-Tool, we showed the access right grant procedure of objects which are server programs, the developing process of client program. Also, we verified the executablility of security service supporting by distributed framework support for u-healthcare use to the mobile monitoring application developing procedure implemented through DPD-Tools.

☞ keyword : dynamic security service(동적 보안 서비스), access control model(접근 제어 모델), distributed object group framework(분산객체그룹 프레임워크)

1. 서 론

u-헬스케어를 위한 편재형 컴퓨팅 환경(pervasive computing environment)은 실제 공간에 센서들과 임베디드 컴퓨팅 자원 그리고 시스템의 서비스를 표현하기 위한 모바일 에이전트와 모바일 사용자 모두를 포함한다. 이러한 환경에서 유·무선 네트워크를 통해 다양한 디바이스들간 또는 각 프로세스 간에 표준화된 메소드를 통해 상호작용하고 있다. 전형적인 클라이언트/서버 모델을 따르는 분산 컴퓨팅 환경은 분산 객체 형태로 점차 변화되고 있다. 이러한 환경에서 정보처리의 확산과 개발 시 사용자 인증(User Certification), 접근제어(Access Control), 정보의 암

* 정 회 원 : 원광대학교 전기전자 및 정보공학부 박사후 연구원
mediblue@wonkwang.ac.kr
** 준 회 원 : 원광대학교 대학원 컴퓨터공학과 석사과정
dhkim1@wonkwang.ac.kr
*** 정 회 원 : 원광 디지털대학교 전임강사
hee@wdu.ac.kr
**** 종신회원 : 원광대학교 전기전자 및 정보 공학부 교수/정보전산원 원장
scjoo@wonkwang.ac.kr(교신저자)
[2007/06/29 투고 - 2007/07/23 심사 - 2007/09/14 심사완료]
☆ 이 논문은 2006년도 원광대학교의 교비 지원에 의해서 수행됨

호화(Encryption of information)와 같은 보안 기술에 대한 중요성은 점차 증가하고 있다[1, 2].

일반적인 보안 측면에서 보안은 인증되지 않은 접근으로부터 정보나 정보에 대한 오퍼레이션을 보호하기위해 신뢰성, 무결성, 유용성이 고려되어야 한다. 이와 함께 시스템을 설계할 때 몇 가지 제한이 추가로 고려되어야 하는데, 서로 방해가 되지 않도록 적절히 객체를 나누어야 하며, 사용자가 감수해야 할 손해를 줄이기 위해 사용자의 의무를 분리해야 한다. 보안은 직접적인 관계가 없는 것에도 영향을 줄 수 있기 때문에, 인증 서비스 등과 같은 보안 요소는 다른 요소들과 분리되어 보안만을 제공하도록 해야 한다[3].

최근 보안에 대한 연구 방향은 보안에 상황을 고려한 연구가 활발하게 진행 중에 있다[4]. 특히, 편재형 컴퓨팅 환경에서는 다양한 상황과 수시로 변하는 상황에 적합한 보안 서비스가 제공되어야 한다. 이에 관련된 연구로 대표적인 모델은 RBAC(Role Based Access Control)[5]와 상황기반 보안(Context based Security)[6]이 있다. 이들 모두 사용자의 상황을 고려하여 상황의 변화에 따르는 동적인 접근 권한 서비스를 제공하고자 한다.

본 논문에서는 u-헬스케어를 위한 애플리케이션 레벨뿐만 아니라 시스템 레벨의 시스템 자원의 효과적인 관리를 위한 분산 프레임워크의 동적 보안 메커니즘에 대해 기술한다. 분산 프레임워크에서 지원하는 보안 서비스는 보안 객체의 보안 정책에 따라 제공한다. 이는 JAVA의 Protected Domain 기술[1, 7]과 유사한 사용자의 식별과 자원에 대한 그룹 개념을 적용하여 보안 도메인을 형성하고, 각 분산객체에 대한 접근 권한과 시스템 자원에 따르는 규칙에 따라 분산객체와의 연관성을 정의하였다. 그리고 이를 기반으로 사용자뿐만 아니라 애플리케이션 레벨의 개별적인 분산 객체와 이들의 집합인 객체그룹 그리고 시스템 레벨의 시스템 자원에 대한 사용 권한과 인증을 통해 동적인 보안 서비스를 제공한다. 이를 위해 보안 객체는 접근제어 리스트(Access Control List : ACL)를 관리하며, 분산 프레임워크 상에 등록된 모든 자원에 대한 클라이언트의 접근을 제어한다. 끝으로 분산 프로그래밍 개발 도구를 이용하여 헬스케어 홈 서비스 응용 개발 과정에서 보안 설정 및 적용과정에 대해 보인다.

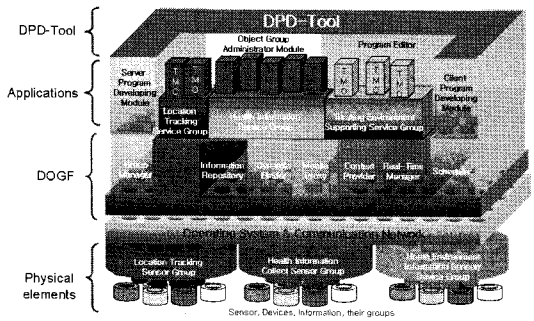
본 논문의 구성은 다음과 같다. 2장에서는 보안 객체를 포함한 분산 프레임워크에 대해 설명한다. 3장에서는 분산 프레임워크의 구성요소인 보안객체의 접근 제어 정책 및 규칙에 대해 기술하고, 헬스케어 홈 서비스를 위한 분산 응용 개발에 보안지원 과정을 4장에서 보이고 5장은 향후 연구 및 결론을 맺는다.

2. u-헬스케어 지원 분산 프레임워크

2.1 소프트웨어 구조

분산응용을 구성하는 각각의 객체들은 서버객체로서 단일 및 중복형태로 분산 서버시스템 상에 존재한다. 이러한 분산객체들은 다수의 분산응용 구현을 위해 서비스별 관리 및 공유를 통해 분산응용에 적절한 서비스를 제공할 수 있어야 한다. 이와 함께 각 분산객체에 대한 보안뿐만 아니라 서비스별 관리를 위한 그룹에 대한 서로 다른 보안 정책이 필요하다. 따라서 u-헬스케어를 위한 컴퓨팅 환경에서는 분산응용을 구성하는 분산객체들을 하나의 논리적인 그룹으로 관리하며, 접근 권한을 갖는 클라이언트는 객체그룹 내의 분산객체들에 대한 식별자나 중복에 상관없이 서비스를 요청 한다. 분산응용은 하나 또는 그 이상의 객체그룹들로 구성될 수 있으며, 이들은 하나의 분산 응용 수행을 위해 논리적인 단일 뷰 시스템으로 관리된다. 우리는 분산 객체 관리 기술들을 연구하여 분산객체그룹 프레임워크(Distributed Object Group Framework : DOGF)를 개발하였다[8, 9, 10]. DOGF는 통신 및 미들웨어 계층과 분산응용 계층의 사이에 존재하며, 크게 객체그룹관리 지원 컴포넌트와 이동성 및 상황정

보 서비스 지원 컴포넌트 그리고 실시간 서비스 지원 컴포넌트로 구성된다. DOGF의 객체그룹관리 지원 컴포넌트는 그룹관리자객체(Group Manager object), 보안객체(Security object), 정보저장소객체(Information Repository object), 동적바인더객체(Dynamic Binder object)로 구성된다. 그리고 이동성 및 상황정보 서비스 지원을 위한 컴포넌트로는 모바일 프록시(Mobile Proxy)와 컨텍스트 제공자(Context Provider)로 구성된다. 또한, 실시간 서비스 지원 컴포넌트는 실시간관리자객체(Real-Time Manager object)들과 스케쥴러객체(Scheduler object)로 구성된다. 다음 (그림 1)은 DOGF를 기반으로 u-헬스케어 지원 분산 프레임워크 구조를 보인다.



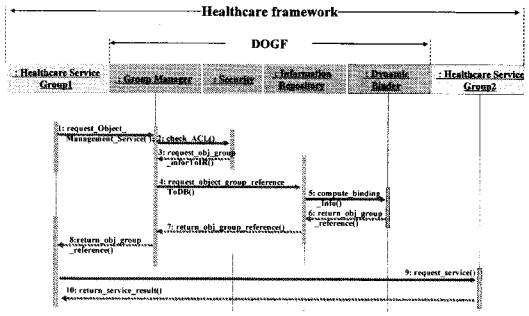
(그림 1) u-헬스케어지원 분산 프레임워크

(그림 1)에서 최상위에 위치한 분산 프로그래밍 개발 도구(Distributed Programming Developing Tool : DPD-Tool)는 DOGF 기반에서 헬스케어 홈 서비스를 위한 응용 개발을 지원한다. 헬스케어 홈 서비스는 목적에 따라 위치 추적 서비스 그룹과 헬스케어 정보 서비스 그룹 그리고 쾌적환경 지원 서비스 그룹으로 구분하였다. 이와 관련된 각 서비스 그룹은 개별적인 분산 객체는 TMO(Time-triggered Message-triggered Object)[11] 객체들과 물리적인 구성요소인 센서 또는 장치, 정보들의 그룹으로 구성된다. 그리고 이들간의 상호작용을 돕는 미들웨어 부분은 TMOSM(TMO Support Middleware)[12]기반으로 한다.

2.2 구성요소의 상호작용

DOGF의 그룹관리자객체는 객체그룹 내의 분산객체들의 전반적인 관리를 책임지며, 응용서비스를 지원하는 분산객체들과 클라이언트 간의 바인딩을 지원하기위한 인터페이스 역할을 수행한다. 클라이언트는 그룹관리자객체를 통하여 분산 응용을 지원하는 객체들을 요청하게 된다. 이때, 보안객체는 클라이언트 객체가 요청한 서버객체에 대해 보안정책을 적용하여 접근권한을 검사한다. 접근권한 검사는 접근제어 리스트를 참조하여 이루어지며, 접근제어 리스트는 허가받은 클라이언트에 대한 정보와 서비스 객체 또는 객체그룹에 대한 접근권한 정보를 갖는다. 그룹관리자객체는 클라이언트 객체가 서비스 요청 시 제공한 클라이언트명과 서비스명을 보안객체에게 전달하고, 보안객체는 접근제어 리스트를 검색하여 클라이언트 객체의 서버객체 접근을 인증한다. 또한 보안객체는 그룹관리자객체로부터 새로운 서버객체의 그룹 소속이나 탈퇴 요청을 받으면 접근제어 리스트를 갱신한다. 다음으로 그룹관리자객체는 정보저장소객체에게 서비스를 수행 할 서버객체의 레퍼런스를 요청한다. 정보저장소객체는 객체들의 속성정보를 저장한 객체리스트(object list)를 포함한다. 서버객체가 비 중복으로 등록되었을 경우 정보저장소객체는 그룹관리자객체에게 해당 서버객체의 레퍼런스를 반환한다. 동적바인더객체는 정보저장소객체에 존재하는 중복객체들에 대한 각각의 바인딩 우선순위 리스트(binding priority list)를 유지한다. 정보저장소객체로부터 서비스 요청을 받은 중복 서버객체 중 적정 서버객체를 선정 전략에 따라 결정한 후, 그룹관리자객체에게 결정된 객체의 레퍼런스를 반환한다. 중복객체들로부터 적절한 하나의 객체를 선정하기 위해, 동적바인더객체에서는 분산응용의 서비스 특성을 고려하여 다양한 서버객체 바인딩 알고리즘

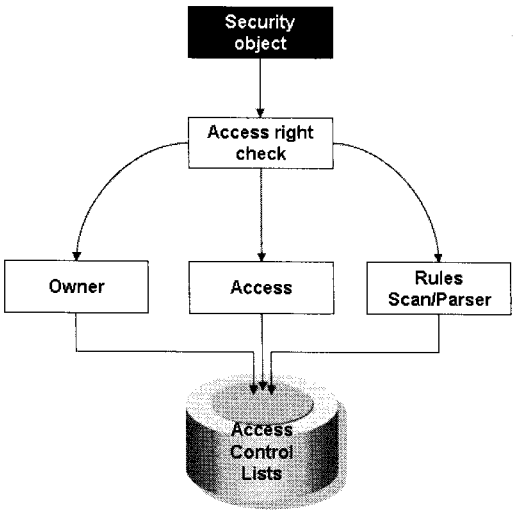
들 중 하나를 적용시킬 수 있다. 모바일 프록시객체는 이동성을 지원하기 위해 클라이언트에게 적합한 상황정보를 제공하기 위해 컨텍스트 제공자에 의해 생성된 콘텐츠를 클라이언트의 위치 이동에 따라 끊임없는 서비스를 제공한다. 컨텍스트 제공자는 다양한 콘텐츠 정보를 관리하며, 클라이언트의 위치, 시간, 공간적인 상황과 매칭 하여 클라이언트의 장치에 따라 가장 적합한 콘텐츠를 추출하여 제공한다. 실시간관리자객체는 클라이언트로부터 마감시간 정보를 전달 받아 시간제약조건을 적용하여 서비스 마감시간을 계산 후 스케줄러객체에 실시간 스케줄링을 요청한다. 스케줄러객체는 서버객체가 수행해야 할 요청 작업들에 대한 작업 우선순위 리스트(task priority list)를 가지며, 클라이언트 객체 정보와 마감시간 정보를 이용하여 요청작업들을 실시간 스케줄링 한다. 동적바인더객체와 같이 스케줄러객체에도 응용의 특성에 따라 다양한 실시간 알고리즘들을 적용시킬 수 있다. (그림 2)는 Rational Rose 2002를 이용하여 모델링한 헬스케어 홈 서비스를 위한 서비스 그룹과 DOGF 컴포넌트들의 상호작용 과정을 보인다.



(그림 2) DOGF 기반으로 한 헬스케어 서비스간의 상호작용

(그림 2)에서 보이는바와 같이 헬스케어 서비스그룹1은 헬스케어 서비스그룹2와의 상호작용을 위해 그룹관리자 객체의 request_Object_Management_Service()를 통해서 헬스케어 서비스그룹2의 레퍼런스를 DOGF의 그룹관리자객체에게 요청한다. 그룹관리자객체는 헬스케어 서비스그룹1이 헬스케어 서비스 그룹2에게 접근권한 여부를 검사하기 위해 check_ACL()을 통해 보안객체에게 서비스 그룹의 요청에 대해 접근권한 검사를 요청하고, 접근이 허가된 요청이라면 보안객체로부터 return_obj_group_infoToIR()을 통하여 접근허가정보를 반환 받게 된다. 또한 그룹관리자객체는 정보저장소객체에게 request_obj_group_ referenceToDB()를 통해서 헬스케어 서비스그룹2의 레퍼런스를 요청한다. 요청한 헬스케어 서비스그룹2가 하나만 존재할 경우 return_obj_group_reference()를 통해 해당 센서그룹의 레퍼런스를 반환한다. 그러나 요청한 헬스케어 서비스그룹2가 중복되어 존재할 경우 정보저장소객체는 compute_binding_Info()에 의해 동적바인더객체에게 동적바인딩서비스를 요청한다. 동적바인더객체는 적정 객체그룹 선정을 위한 알고리즘에 의해 헬스케어 서비스그룹2의 레퍼런스를 return_obj_group_reference()를 통해 반환하게 된다. 반환된 헬스케어 서비스그룹2의 레퍼런스는 그룹관리자객체의 return_obj_group_reference()를 통해 헬스케어 서비스그룹1에게 전달된다. 헬스케어 서비스그룹1은 헬스케어 서비스그룹2와 상호작용을 통해서 헬스케어 서비스를 수행한다. 보안객체에 대해 세부적으로 살펴보면 다음 (그림 3)과 같이 접근을 제어하는 자원에 대해서 해당 자원을 사용 할 수 있는 사용자와 현재의 사용자가 해당 자원을 사용할 수 있는지 판단하기 위해 ACL를 참조하며, 접근 권한 검사는 소유자, 자원에 대한 접근 여부 및 각 자원이 갖는 오퍼레이션상의 보안 규칙에 따라 인증된 클라이언트에 대해 DOGF상에 저장된 객체그룹 또는 서비스 객체 그리고 시스템 자원을 이용한다.

ACL은 특정 자원에 대해 접근하는데 허가에 대한 역할을 기록해 놓은 목록이다. 역할을 기반으로 하여 접근을 제어하는 경우에 ACL을 사용하여 해당자원에 대한 접근권한 승인을 얻어서 현재 사용자가 가지고 있는 역할과 ACL에서 허

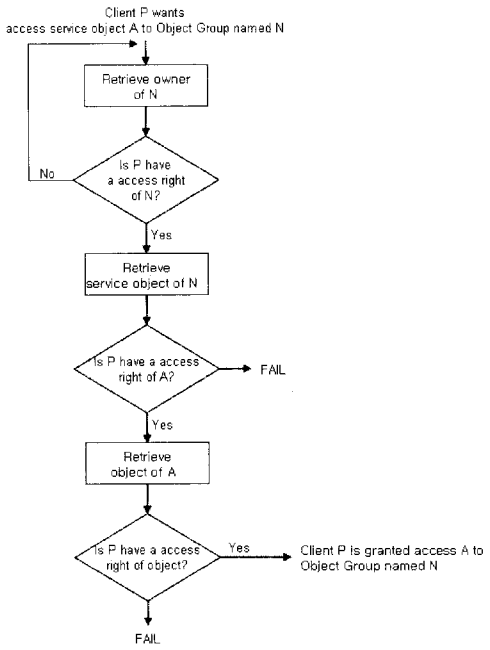


(그림 3) 보안객체의 접근 권한 검사

가된 역할들을 비교하여 사용자가 자원에 허가된 역할과 접근권한 여부를 판단한다. (그림 4)는 클라이언트 P가 N이라 불리는 객체그룹의 서비스 객체 A에 접근하고자 할 경우 이에 대한 사용권한 여부 확인을 위해 접근제어 리스트 검색하여 승인 받는 절차를 나타낸다. 먼저 클라이언트 P가 객체그룹 N의 소유 여부를 확인하기 위해 검색한다. 이때 클라이언트 P가 객체그룹 N에 접근할 수 있는 사용권한을 가지고 있는 경우에는 객체그룹 N에 포함된 서비스 객체들을 검색한다. 그리고 서비스 객체 A에 대한 사용권한을 갖고 있을 경우에는 해당 서비스 객체를 이용할 객체들을 검색한다. 그렇지 않은 경우는 서비스 객체 A를 이용할 수 없다. 끝으로 서비스 객체에 해당하는 객체에 대한 사용권한 여부를 확인하여 클라이언트 P는 객체그룹 N의 서비스 객체 A에 대한 접근 승인을 받는다.

3. 보안 객체의 보안 정책

본 장에서는 DOGF상에서 등록된 분산 객체들에 대한 보안 서비스를 제공하기 위해 보안객체가 제공하는 접근 제어 정책과 규칙에 대해 기술



(그림 4) 클라이언트의 서비스 객체 사용권한 여부 확인 절차

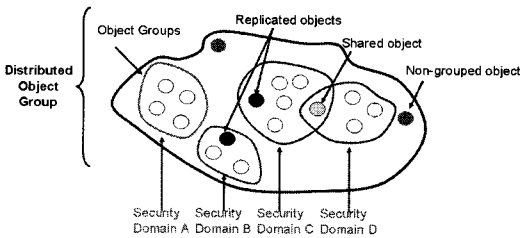
한다.

3.1 보안 도메인

기존의 일반적인 플랫폼 지향 시스템에서는 플랫폼에 의존적인 특정 도메인으로 제한되었으나, u-헬스케어와 같은 컴퓨팅 환경에서는 플랫폼과 보안 도메인과의 관계는 불필요하다. 분산 객체 컴퓨팅 패러다임은 다중 플랫폼 상에 자원을 포함한 도메인을 구성하고 있다. 또한 이러한 도메인은 중첩되거나 계층적인 구성을 하거나 해체가 가능하다. 이에 따라 보안 정책은 서로 다르게 적용되며, 도메인이 해체될 경우 각 분리된 도메인이 갖는 보안 정책에 따라 정의된다.

따라서, 보안 도메인은 분산객체프레임워크에 의해 구성되는 객체그룹에 따라 형성된다. 즉, 공통된 보안 정책을 적용한 자원의 집합으로 분산 객체들의 모임인 객체그룹을 의미한다. 이러한 보안 도메인은 클라이언트 서비스 요청에 따라 그

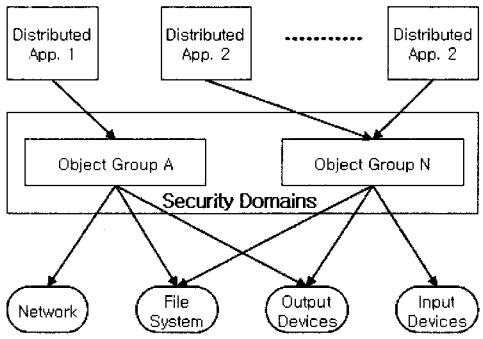
룹관리자 객체에 의해 생성된다. (그림 5)에서 나타난 바와 같이 보안 도메인은 객체그룹에 따라 서로 다른 보안 정책을 따른다. 보안 도메인 A의 경우는 클라이언트의 접근권한을 갖는 개별적인 분산 객체들로 그룹화 되어 있다. B와 C의 경우에는 중복된 분산객체를 포함하고 있으며, C와 D의 경우에는 중첩된 분산 객체를 포함하고 있다. 이는 개별적인 분산객체의 접근권한에 따라 보안 정책이 달라진다. 이에 대해 세부적으로 살펴보면, 보안 도메인은 실행 가능한 응용인 분산 객체 혹은 분산 응용의 특징에 따라 시스템 자원에 접근할 수 있는 부분을 분리시켜 한 시스템 또는 여러 시스템 영역 내에 가상적인 객체그룹으로 구성된다. 접근권한이 허용된 분산 객체 또는 분산 응용이 접근 가능한 시스템 자원 부분과 접근이 불가한 경우를 분산객체그룹에 의해 구분할 수 있다. 이는 분산 응용을 구성하는 객체그룹화에 따라 다중 보안 정책을 적용할 수 있어 유연성 및 안정성을 제공한다.



(그림 5) 보안 도메인

DOGF에서 보안을 위해 정의된 보안 도메인은 시스템 자원 부분과 분산 응용으로 나누어진다. 시스템 자원 부분으로는 파일 시스템, 네트워크, 모니터, 키보드 등이며, 분산 응용으로는 분산객체 및 분산 응용이 있다. 이에 대한 구조는 (그림 6)과 같다.

객체그룹 구조는 여러 시스템 상에 위치한 분산객체들의 그룹화를 통해 보안 도메인을 형성하고, 이러한 영역은 객체그룹 식별자를 통해 구분한다. 또한 객체그룹을 구성하는 분산객체에 대한

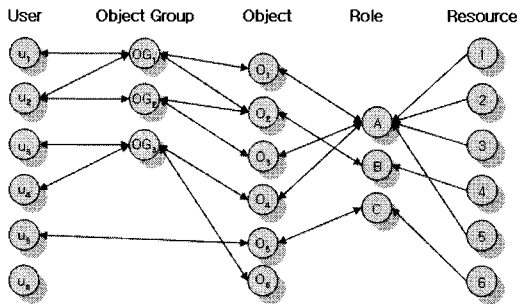


(그림 6) 분산객체그룹 프레임워크의 보안 도메인

동적 바인딩객체를 통해 하나의 에러가 전체적인 시스템 자원 관리 부분에 치명적인 위협이 되는 문제를 해결한다.

3.2 접근 제어 정책 및 규칙

보안 객체에 의한 접근 제어 정책은 접근제어 리스트에 의해 사용자별, 객체그룹별, 분산 객체별 그리고 시스템 자원으로 구분된다. 이들 간의 관계에 따르는 기능적인 역할에 의해 구분된 규칙을 적용하였다. 이에 대한 매핑 관계는 (그림 7)과 같다. 사용자는 접근권한이 있는 객체그룹과 연관되어 있다. 즉, 3개의 보안 도메인으로 형성된다. 각 객체그룹별 하나 이상의 분산 객체를 포함하고 있으며, 6개의 분산 객체는 6개의 시스템 자원들 각각이 갖는 특성에 따르는 규칙 3개 중에 하나에 동적으로 매핑되며, 이에 해당하는 자



(그림 7) 동적인 접근 제어 매핑 관계

원과 연관되어 있다.

이러한 구성에서 자원의 특성에 따라 1, 2, 3, 5는 규칙 A에 대한 내용이 ACL에 기록되며, 자원 4는 규칙 B에 대한 내용이 ACL에 기록된다. 그리고 자원 6의 경우에는 규칙 C에 해당하는 내용이 ACL에 기록된다. 예를 들면, 규칙 A는 입출력 가능한 자원이며, 규칙 B의 경우는 출력만 가능한 자원 그리고 C는 입력만 가능한 자원으로 정의한다.

DOGF 상에서 사용자의 경우 분산응용의 수행환경을 전체적으로 관리하는 객체그룹 운영자와 서버객체의 그룹 등록 및 접근권한 설정하는 서버 프로그램 개발자 그리고 분산응용을 개발하기 위해 서비스 요청 프로그램을 개발하기 위한 클라이언트 프로그램 개발자로 구분하였다. 객체그룹 운영자는 신뢰할 수 있는 서버 개발자와 클라이언트 개발자들에게 객체그룹을 사용할 권한을 부여하고, 서버 개발자들이 등록한 객체그룹을 해체할 수 있다. 또한 DOGF의 동적 바인더객체를 통해 그룹별 동적 바인딩 알고리즘을 설정하여 중복 객체에 접근할 수 있도록 한다. 다음 <표 1>은 객체그룹 운영자의 보안 관련 오퍼레이션을 나타낸다.

〈표 1〉 객체그룹 운영자의 보안관련 오퍼레이션

오퍼레이션	설 명	비 고
F_GRO()	등록되어 있는 모든 서비스 리스트에 대한 정보요청	정보저장소
F_ACL()	저장된 모든 서비스들의 접근 권한 정보요청	ACL
F_Client()	저장된 클라이언트별 재구성된 그룹들의 정보요청	정보저장소, ACL
_RAL()	클라이언트별 서버 객체 접근권한 요청내용에 대한 정보요청	ACL
F_GM()	서버 객체에 메시지 전달, 그룹 등록 및 탈퇴, 접근권한 추가 및 삭제, 그룹별 동적 바인딩 알고리즘 설정, 클라이언트별 그룹 재구성, 서비스 검색	정보저장소, 동적바인더, ACL

서버 프로그램 개발자는 서버 프로그램 개발자 자신들이 구현한 서버객체들을 그룹화하여 정보저장소 객체에 등록한다. 클라이언트가 등록된 서버 객체를 사용하기 위해 접근권한 허가요청을 할 경우 보안객체는 클라이언트의 접근권한을 설정하여 사용할 수 있도록 한다. 이에 대한 오퍼레이션은 <표 2>와 같다.

〈표 2〉 서버 프로그램 개발자의 보안관련 오퍼레이션

오퍼레이션	설명	비고
Enter()	객체그룹에 서비스 객체 등록	정보저장소, ACL
Modify()	그룹에 등록된 서비스 객체 수정	정보저장소, ACL
Withdraw()	그룹에 등록된 서비스 객체 탈퇴	정보저장소, ACL
Insert()	클라이언트가 선택한 서비스 객체에 대한 접근권한 추가	ACL
Delete()	클라이언트가 선택한 서비스 객체에 대한 접근권한 삭제	ACL
RequestList()	클라이언트에 대한 접근권한 요청 리스트 확인	ACL

클라이언트 프로그램 개발자는 클라이언트 동작을 수행하는 분산응용을 개발하기 위해 정보저장소에 등록된 객체 그룹과 서비스를 검색하여 선택한 객체그룹 또는 서비스 객체를 사용하기 위한 접근 권한을 요청하고, 접근이 허가된 서비스들로 분산 응용을 개발한다. 이와 관련된 오퍼레이션은 <표 3>과 같다.

〈표 3〉 클라이언트 프로그램 개발자의 보안관련 오퍼레이션

오퍼레이션	설 명	비 고
Request()	클라이언트가 선택한 객체그룹 및 서비스 객체에 대한 접근권한 요청 및 그룹 재구성 요청	정보저장소, ACL
Permit()	클라이언트가 프로그램 개발을 위해 선택한 서비스 객체들로 재구성된 객체그룹에 대한 저장	정보저장소, ACL

앞에서 언급한 사용자 분류에 따르는 보안에 관련된 오퍼레이션은 다음 <표 4>에 기술된 ACL의 속성들을 참고한다.

〈표 4〉 ACL의 속성 정보

속 성	설 명
client_name	클라이언트 객체 이름
group_name	객체그룹 이름
service_name	서비스 이름
service_owner	서비스 객체의 소유자 정보
object_name	객체의 이름
object_description	객체가 제공하는 인터페이스 정보
location_address	서비스 객체의 위치 경로 정보
m_strSelectedGroup	그룹을 구분하기 위한 식별자
m_strSelectedService	서비스 객체를 구분하기 위한 식별자
m_strSelectedObject	객체를 구분하기 위한 식별자
m_nACL	서비스 객체에 대해 public, private 구분
m_strID	사용자 식별자(운영자, 서버 개발자, 클라이언트 개발자)
m_strPW	사용자 패스워드(운영자, 서버 개발자, 클라이언트 개발자)
m_strIP	객체그룹 관리 모듈 IP
m_strPort	객체그룹 관리 모듈 Port

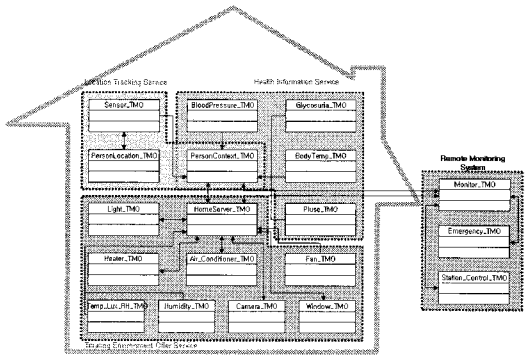
4. 헬스케어 응용 개발에 따르는 보안 적용 과정

본 장에서는 DPD-Tool을 이용하여 헬스케어 홈 서비스 응용 개발 과정을 통해 보안 설정 및 적용과정에 대해 기술한다. 이를 위해 먼저 헬스케어 홈 서비스 응용 개발 절차에 대해 기술하고, 헬스케어 홈 서비스 응용 개발과정을 사용자별 인증, 객체그룹의 사용권한 여부, 서비스 객체 및 객체에 접근하기위한 보안 과정을 단계별로 DPD-Tool에서 제공하는 GUI를 통해 보인다.

4.1 헬스케어 홈 서비스 응용 구성요소

헬스케어 홈 서비스 응용은 가정 내의 거주자에 대한 위치 추적과 거주자의 헬스케어 정보 수집을 기반으로 한 헬스 정보 서비스 그리고 거주자의 홈 환경을 최적의 환경상태를 유지하도록하기 위한 쾌적한 환경제공 서비스 그룹으로 구분된다. 각 서비스 그룹에 해당하는 분산 객체는 TMO 객체들로 하나 이상의 서비스 객체로 구성하였다.

위치 추적 서비스 그룹은 위치 거주자의 위치를 식별하기 위한 PersonLocation _TMO와 주기적인 위치 정보를 수집하기위한 Sensor_TMO 그리고 거주자에 대한 위치 및 다양한 헬스케어 센서로부터 생체 수집을 위한 PersonContext_TMO 객체로 구성하였다. 헬스 정보 서비스 그룹은 거주자의 건강 상태를 체크하기 위한 센서들로 혈압(BloodPressure), 당뇨(Glycosuria), 체온(BloodTemp), 맥박(Pulse) 객체로 구성하였다. 쾌적 환경 지원 서비스 그룹은 가정내 설치되어 있는 스테이션인 전등(Light), 에어컨(Air Conditioner), 히터(Heater), 선풍기(Fan), 창문(Window), 방범 카메라(Camera) 그리고 실내 온도/조도(Temp_Lux_RH), 습도(Humidity)에 해당하는 객체로 구성하였다. 또한 가전을 제어하기 위해 HomeServer_TMO 객체를 두어 이들을 관리하도록 하였다. 다음 (그림 8)은 헬스케어 홈 서비스를 위한 그룹과 이들간의 상호작용을 나타낸다.



(그림 8) 헬스케어 홈 서비스를 위한 응용 서비스 그룹 및 상호작용

홈 환경을 모니터링하기 위해 시스템 상에는 가정 내의 거주자의 상황 정보와 스테이션 환경 정보를 수집하기 위한 Monitor_TMO와 위급상황 판단 및 통지 서비스를 제공하기 위한 Emergency_TMO 그리고 스테이션을 제어하기 위한 Station_Control_TMO 객체로 구성하였다.

4.2 헬스케어 홈 서비스 응용 개발 절차

헬스케어 홈 서비스를 위한 응용 개발은 서버와 클라이언트 프로그램 개발자들이 서로 독립적으로 DPD-Tool에서 제공하는 서버 프로그램 개발자와 클라이언트 프로그램 개발자 GUI 그리고 이들을 관리하는 객체그룹 운영자 GUI를 통해 개발한다. 그리고 각 모듈별 GUI 상에는 공통으로 사용자에 대한 인증과 서로 다른 목적의 자원에 대한 보안 기능을 갖고 있다. 다음 (그림 9)는 헬스케어 홈 서비스를 위한 응용 개발 절차와 각 모듈별 GUI상의 보안 기능을 보인다.

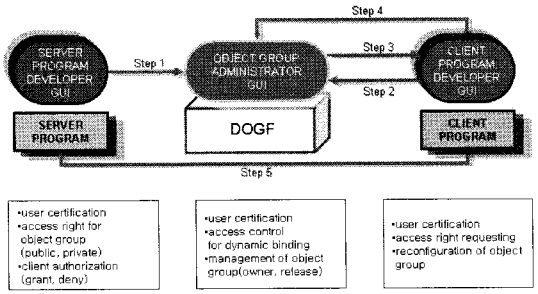
- Step 1 : 서버 프로그램 개발자는 클라이언트로부터 요청을 받을 수 있는 서버 프로그램을 개발한 후, 서버 프로그램 개발자 GUI를 이용해 객체그룹에 서버 프로그램을 등록한다. 이때 서버 프로그램인 객체그룹에 대해 public인지 private인지를 설정한다.

- Step 2 : 클라이언트 프로그램 개발자는 객체그룹에 등록된 전체 서버 프로그램에서 자신이 사용할 서버 프로그램들을 선정한 후 접근권한을 요청한다. 이때 public인 경우에는 접근권한 요청을 할 필요가 없다. 그러나 private인 경우에는 접근권한을 허가 받기 위해 요청한다.

- Step 3 : 서버 개발자로부터 접근권한을 허가받고 그룹을 재구성한 후 서비스를 요청하는 클라이언트 프로그램을 개발한다.

- Step 4 : 서버 및 클라이언트 프로그램 수행 시 클라이언트 프로그램은 DOGF에게 자신이 이용할 서버의 속성정보를 요청 후 반환한다.

- Step 5 : 서버 프로그램에 접속하여 서비스를 이용한다. 이때 접근권한을 갖고 있는 클라이언트만이 서버 객체에서 제공하는 서비스의 결과를 제공받는다.



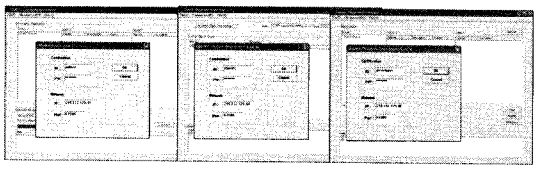
(그림 9) 헬스케어 홈 서비스 응용 개발 절차 및 각 모듈별 보안 기능

헬스케어 홈 서비스 프로그램 개발자가 서버 또는 클라이언트를 개발하는지에 따라 개발절차는 다를 수 있다. 서버 프로그램 개발자의 경우, Step 1만을 수행하여 개발한 서버 프로그램을 DOGF에 등록하기만 하면 된다.

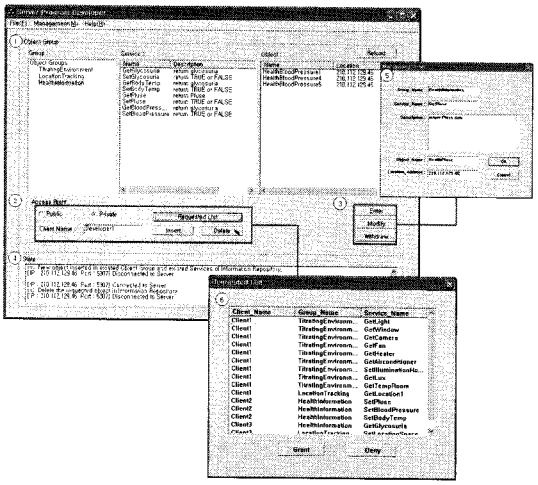
4.3 DPD-Tool을 이용한 헬스케어 홈 서비스 응용 개발

헬스케어 홈 서비스 응용을 개발할 경우 각 사용자 별 GUI를 통해 사용자 인증을 받는다. 인증을 받은 사용자만이 DPD-Tool에서 제공하는 GUI 모듈에 접근하여 목적에 따라 응용을 개발하거나 관리하게 된다.

헬스케어 홈 서비스 응용을 개발 절차에서 언급한 바와 같이 1단계는 서버 프로그램 개발자의 GUI를 통해 수행한다.



(그림 10) DPD-Tool의 각 GUI에서 사용자 인증

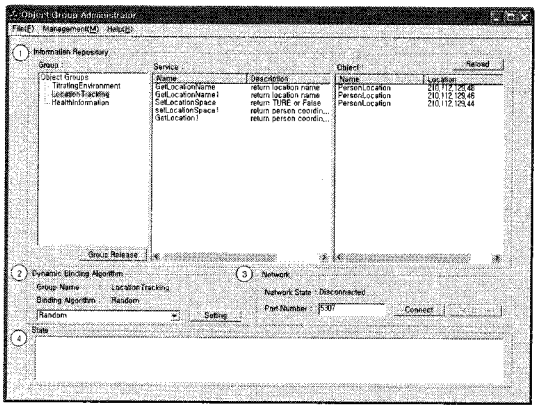


(그림 11) 서버 프로그램 개발자 GUI 상의 보안 설정

(그림 11)에서 나타난바와 같이, 서버 개발자 소유의 DOGF의 정보 저장소에 등록된 객체그룹과 객체그룹을 구성하는 서비스 객체 그리고 수행 객체에 대한 정보를 출력한다(①). 또한 소유하고 있는 각 객체그룹에 대해 public과 private을 설정한다. public로 설정한 객체그룹의 경우에만 클라이언트 개발자 GUI에 사용 가능한 객체그룹 리스트를 확인할 수 있으며, 클라이언트로부터 서비스 객체에 대한 접근권한 허가 요청 목록을 확인하고, 접근권한을 승인 및 거절할 수 있다(②). private인 경우에는 클라이언트 개발자 GUI에 보이지 않는다. 그리고 서버 프로그램 개발자가 개발한 새로운 객체그룹을 등록하거나 삭제 그리고 수정한 사항에 대한 상태정보를 출력한다(④). 또한 ⑤는 ③의 [Enter]에 의해 개발한 서버 프로그램을 등록하기 위한 대화상자로 객체에 대한 이름, 서비스 이름 그리고 객체에 대한 상세정보 기술과 위치 정보를 기입한다. ⑥은 클라이언트별 서비스 객체에 대한 접근권한 허가 요청 리스트를 보이고 있다. 서버 프로그램 개발자는 개발한 각 서비스 객체에 대한 사용 권한을 주거나(Grant) 거절(Deny) 할 수 있다.

서버 프로그램 개발자가 등록한 헬스케어 홈 응용 서비스에 따라 객체 그룹(Location Tracking, Health information, Titrating Environment) 서비스 객체에 대한 접근 권한의 설정에 따라 클라이언트 프로그램 개발자별 서비스 객체에 접근 권한에 대한 승인을 얻기 위해 요청과정을 거쳐야 한다. 서버 프로그램 개발자는 요청 목록을 통해 승인과 거절을 통해 개발한 객체그룹에 대한 사용 접근을 제어한다.

서버 프로그램 개발자 GUI를 통해 등록된 객체그룹들은 DOGF의 정보 저장소 객체에 저장되며, 이에 대한 정보는 객체그룹 운영자 GUI를 통해 관리된다. 또한 등록된 객체그룹내의 서비스 객체들 중에 중복된 객체를 포함할 경우 적정 객체를 선정할 수 있는 알고리즘을 설정할 수 있다.

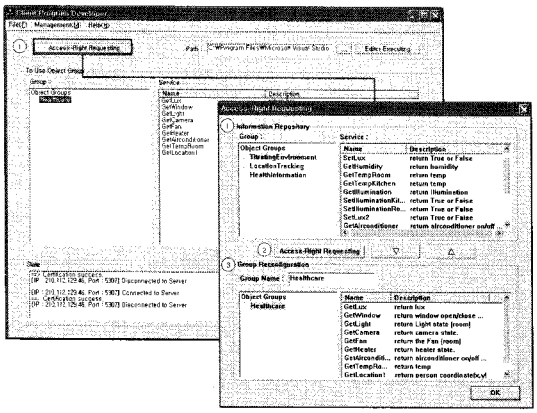


(그림 12) 객체그룹 운영자 GUI

(그림 12)에서 서버 프로그램 개발자 GUI를 통해 등록한 3개의 객체그룹에 대한 정보를 나타내고 있다(①). [Group Release]는 관리목적상 객체그룹의 생명주기가 끝났을 경우 해제하는데 사용되

며, 위치 추적 서비스를 제공하기 위한 그룹의 중복 객체인 PersonLocation 객체들에 대한 동적 바인딩 알고리즘을 설정하고 있다(②). 클라이언트 개발자 사용자 인증을 거친 GUI와 통신하기 위해 네트워크와 포트를 설정 부분(③)과 객체 그룹 운영자 GUI상에서 그룹 관리를 위한 설정 및 상태 정보를 출력한다(④).

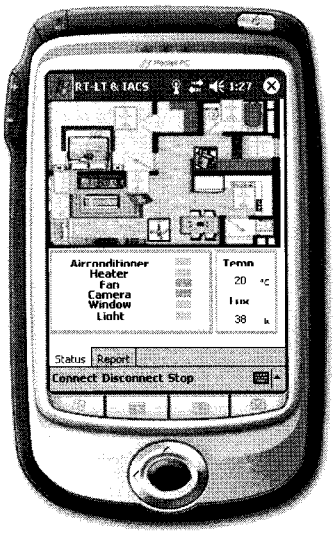
클라이언트 프로그램 개발자는 서버 프로그램 개발자가 등록한 객체그룹을 재구성하여 목적에 맞는 응용을 개발한다. 이때 서버 프로그램 개발자가 등록한 객체그룹의 접근권한 설정이 private인 경우, 접근권한 요청을 통해 승인을 받은 객체그룹만을 사용할 수 있다.



(그림 13) 클라이언트 프로그램 개발자 GUI상에서 접근권한 요청을 통한 객체그룹 재구성

(그림 13)은 클라이언트 프로그램으로 거주자의 위치 추적 및 스테이션 제어 상황을 파악하기 위해 Healthcare라 명명하고, 이와 관련된 객체그룹 중에 Titrating Environment 객체그룹의 서비스 객체에 대한 접근권한 승인 요청을 통해 재구성함을 보이고 있다.

다음 (그림 14)는 앞서 언급한 헬스케어 홈 서비스에서 모바일 디바이스에 응용 서비스를 개발하기 위해 클라이언트 프로그램 개발자가 재구성한 Healthcare 객체그룹을 이용하여 PDA(HP ipaq 4150, pocket pc 2003)상에서 거주자의 위치 추적과 가정 내 설치된 스테이션의 제어 상황을 파악하는 모니터링 응용을 구현 결과를 나타낸다.



(그림 14) 모바일 모니터링 서비스 구현 결과 화면

모바일 모니터링 서비스 구현결과, 현재 거주자는 실내에 없으며, 이에 따른 방범 카메라의 동작과 실내 온도를 거주자가 설정한 온도를 유지하기 위해 선풍기를 동작시킨 결과와 실내 온도 20도와 조도 38 Lux에 대한 정보를 나타내고 있다.

5. 결론

u-헬스케어 컴퓨팅 환경에서 정보 또는 객체가 분산된 시스템 사이를 이동할 수도 있기 때문에 공격당하기 쉽고, 여러 시스템에서 정보에 접근할 수 있으므로 보안 문제가 빈번하게 발생한다. 이를 해결하기 위해 접근 제어, 보안 관리, 식별과 인증 메커니즘을 적용하고 있다.

본 논문은 u-헬스케어 지원 분산 프레임워크의 보안 서비스에 중점을 두어 기술하였다. 본 프레임워크의 구성요소인 보안 객체는 접근제어 리스

트를 이용하여 클라이언트와 서버 객체에 대한 접근권한 인증 메커니즘으로 동적인 보안 서비스를 제공한다. 접근제어 리스트는 사용자 인증을 위한 정보, 애플리케이션 레벨의 개별적인 분산 객체와 이들의 집합인 객체그룹 그리고 시스템 레벨의 시스템 자원에 대한 사용 권한 정보를 포함하고 있다. 이를 통해 사용자 혹은 클라이언트 객체로부터 서비스 객체에 대한 접근을 제어하였다.

이를 위해 분산 프레임워크에서 보안을 위한 정책과 규칙을 서비스를 구성하는 객체그룹 단위로 보안 도메인을 설정하고, 사용자별 사용권한을 부여하였다. 또한 객체그룹을 구성하는 서비스 객체나 수행 객체에 대한 서로 다른 보안 설정으로 통해 사용자 또는 클라이언트 객체의 접근권한을 인증 받아야 접근할 수 있도록 하였다. 이러한 메커니즘의 수행성을 검증하기 위해 분산 프로그래밍 개발 도구를 이용하여 모바일 위치 추적 및 가전제어 상황 모니터링 응용 개발 과정을 통해 보안 서비스가 적용됨을 보였다.

향후 u-헬스케어를 위한 시스템 환경에 적용하기 위해 상황기반의 동적 보안 정책에 관한 연구와 다양한 물리적인 센서장치에 대한 보안에 연구를 진행할 예정이다.

참 고 문 헌

[1] Satoru Tezuka, Ryoichi Sasaki, Masanori Kataoka, "Seamless Object Authentication in Different Security Policy Domains, proceedings of the 33rd Hawaii International Conference on System Science, 2000.

[2] Deborah J. Bodeau, Charles M. Schmidt, Vipin Swarup, F. Javier Thayer, "Distributed Object Computing Security : Paradigms and Strategies", MITRE Product, November, 1998.

[3] Konstantin Beznosov, "Object Security Attributes : Enabling Application-Specific Access Control in Middleware" LNCS 2519, pp. 693-710, 2002.

[4] Patrick Brezillon, Ghita Kouadri Mostefaouim, "Context-Based Security Policies ; A New Modeling Approach" Proceeding of Second IEEE Annual Conference on Pervasive Computing and Communications Workshops(PERCOMW'04) 2004.

[5] R. Sandhu, E. Coyne, H. Feinstein, and C. Youman, "Role Based Access Control Models", IEEE Computer, Vol 29 No.2, pp. 38-47, Feb. 1996

[6] Patrick Brezillon, Ghita Kouadri Mostefaoui, "Context-Based Security Policies: A New Modeling Approach", Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops, pp.154-158, 2004

[7] Malkhi, D.; Reiter, M.K., "Secure execution of Java applets using a remote playground", Software Engineering, IEEE Transactions on Volume 26, Issue 12, pp. 1197-1209 Dec. 2000.

[8] Chang-Sun Shin, Myoung-Suk Kang, Chang-Won Jeong, and Su-Chong Joo, "TMO-Based Object Group Framework for Supporting Distributed Object Management and Real-Time Services", Lecture Notes in Computer Science, Vol. 2834, pp. 525-535, 2003. 9.

[9] Chang-Sun Shin, Chang-Won Jeong, and Su-Chong Joo, "Construction of Distributed Object Group Framework and Its Execution Analysis Using Distributed Application Simulation", Lecture Notes in Computer Science, Vol. 3207, pp. 724-733, 2004. 7.

[10] Chang-Won Jeong, Dong-Seok Kim, Geon-Yeob Lee, and Su-Chong Joo,

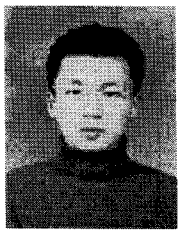
"Distributed Programming Developing Tool Based on Distributed Object Group Framework", Lecture Notes in Computer Science, Vol. 3983, pp. 853 - 863, 2006. 2.

[11] Kim, K.H., "Real-Time Object-Oriented Distributed Software Engineering and the TMO Scheme", Int'l Jour. of Software Engineering & Knowledge Engineering, Vol. No.2, April 1999, pp.251-276.

[12] Kim, K.H., "Object-Oriented Real-Time Distributed Programming and Support Middleware", Proc. ICPADS 2000 (7th Int'l Conf. on Parallel & Distributed Systems), Iwate, Japan, July 2000, pub. by IEEE CS Press (keynote paper), pp.10-20.

◐ 저 자 소 개 ◑

정 창 원(Chang-Won Jeong)
1993년 원광대학교 컴퓨터공학과 졸업
1998년 원광대학교 컴퓨터공학과 졸업 (석사)
2003년 원광대학교 컴퓨터공학과 졸업 (공학박사)
2004년~2006년 전북대학교 차세대 LBS 응용 연구센터 연구교수
2006년~현재 원광대학교 전기전자 및 정보공학부 박사후 연구원
<관심분야> 분산객체 컴퓨팅, 멀티미디어 데이터베이스, LBS, 텔레매틱스
E-mail : mediblue@wonkwang.ac.kr



김 동 호(Dong-Ho Kim)
2005년 원광대학교 전기전자 및 정보공학부 졸업(학사).
2006년 - 현재 원광대학교 대학원 컴퓨터공학과 석사과정
<관심분야> 분산객체 컴퓨팅, 객체지향 프로그램, 유비쿼터스 컴퓨팅.
E-mail : dhkim1@wonkwang.ac.kr

김 명 희(Myung-Hee Kim)
1993년 원광대학교 컴퓨터공학과 졸업(학사).
1996년 원광대학교 컴퓨터공학과졸업(공학석사).
2001년 원광대학교 컴퓨터공학과 졸업(공학박사).
2002년~현재 원광 디지털대학교 전임강사.
<관심분야> 분산 실시간 컴퓨팅, 시스템 최적화, 운영체제
E-mail : hee@wdu.ac.kr

◐ 저 자 소 개 ◑

주 수 종(Su-Chong Joo)

1986년 원광대학교 전자계산공학과 졸업
1988년 중앙대학교 컴퓨터공학과 졸업 (공학석사)
1992년 중앙대학교 컴퓨터공학과 졸업 (공학박사)
1993년 미국 University of Massachusetts at Amherst, Post-Doc.
2003년 미국 University of California at Irvine, Visiting Professor.
1990년~현재 원광대학교 전기전자 및 정보 공학부 교수
2007년~현재 원광대학교 정보전산원 원장
관심분야 : 분산 실시간 컴퓨팅, 분산객체모델, 시스템 최적화, 멀티미디어 데이터베이스
E-mail : scjoo@wonkwang.ac.kr