논문 00-25-6T-9 한국통신학회논문지 '00-6 Vol.25 No.6T

통신망 관리정보베이스 접근제어 시스템

정회원 김 종 덕*

The Access Control System of Communication Network Management Information Base

Jong-Duk Kim* *Regular Member*

요 약

통신망관리 시스템에서 가장 핵심적인 요소는 망관리에 필요한 정보들인 관리 객체들의 저장소인 관리 정보베이스이다. 관리 정보베이스에 저장된 관리 객체들은 망관리에 필수적이며 중요한 모든 정보들을 유지하고 있기 때문에 안전하게 관리되고 유지되어야 한다. 본 논문에서는 접근 제어를 위한 포괄적인 클래스 정의 및 접근 제어 보안 모델을 정의한 ITU-T X.741 권고안의 표준 관리 객체 클래스 구조를 명시적 규칙과 묵시적 규칙으로 세분화함으로써 크게 확장 및 보완하였다. 또한 세분화된 접근 제어 규칙에 따라 해당 규칙이 적용되는 절차를 각 접근 제어 정책에 적용하여 봄으로써 접근 제어 규칙 수행의 타당성을 검증하였다.

ABSTRACT

MIB(Management Information Base), one of the key components of communication network management system, is a repository for the information of the managed objects. MIB stores and manages all the structural and operational data of each managed resources. Therefore, MIB should be protected properly from inadvertant user access or malicious attacks. International standard ITU-T X.741 describes several managed object classes for the enforcement of MIB security. In this paper, we divide managed object classes into two groups, explicit and implicit ones, and describe the access authorization procedure in specification language. It makes validation of access control rule that authorization procedure and rules are verified.

Ⅰ. 서 론

통신망 관리정보베이스에 대한 안전한 접근제어를 위해서는 합법적인 사용자들이 수행할 수 있는 동작이나 연산을 제어함으로써 통신망관리 정보를 안전하게 유지하는데 있다.

ITU-T X.741(Objects and Attributes for Access Control) 권고안에 망관리 정보의 접근 제어를 위한 포괄적인 클래스 정의 및 접근 제어 보안 모델을 정의하였다. 권고안에 정의된 접근 제어를 위한 관리 객체 클래스 구조는 접근 제어 정책중 자율적 접근 제어(DAC: Discretionary Access Control) 정책인 접근 제어 리스트(Access Control List) 스킴과 능력(Capability) 스킴, 그리고 강제적 접근 제어(MAC: Mandatory Access Control) 정책인 레이블 기반(Label based) 스킴에 대해서만 정의를 하였을 뿐, DAC과 MAC의 단점을 보완한 새로운 접근 제어 정책으로서 최근 들어 활발히 연구가 진행되고 있는 역할 기반 접근 제어(RAC: Role-based Access Control) 정책에 대한 정의가 포함되어있지 않다. 그리고 접근 제어를 위한 각종 관련 정보 및 규칙을 보안관리자가 사전에 정의해 놓은 명시적인 접근 규칙(Explicit Access Rule)만을 정의함으로써

* 전남도립 담양대학 전산·정보통신공학부(jdkim@damyang.damyang.ac.kr)
논문번호 : 00017-0315, 접수일자 : 2000년 3월 15일

망의 규모가 점점 확대되고 이로 인한 관리 객체의 수가 급격히 증가되는 경우에 모든 관리 객체에 대해서 명시적 규칙을 낱낱이 정의하기가 사실상 불가능하다. 따라서 이에 대한 보완책으로서 기존의 권고안 구조에 묵시적인 규칙(Implicit Access Rule)을 포함시킴으로써 명시되지 않은 규칙에 대해서도 관리 객체간의 상호 관계를 이용해 접근 제어 규칙을 융통성 있게 적용하여 보안관리자의 권한부여를 크게 단순화 시킬 수 있다.

본 논문의 구성은 다음과 같다. 2장에서는 관리 정보베이스에 대한 접근 제어 정책을 설명하고 3장에서는 ITU-T X.741 권고안을 바탕으로 접근제어를 확장하고, 4장에서는 역할기반 접근 제어를 위한 관리정보베이스 접근제어 시스템을 소개하고 각 접근제어 규칙이 적용되는 과정을 해당 모듈을 통해 확인 함으로써 역할기반 접근 제어 정책에 대한 접근제어 규칙의 타당성을 검증한다. 마지막으로 5장에서 결론을 맺는다.

Ⅱ. 관리 정보베이스 접근제어 정책

통신망 자원에 접근을 원하는 사용자가 자신의 신원을 제시하고 인증 시스템으로부터 신원 인증을 받은 후, 확인된 사용자에 대한 망 자원을 접근하는 권한을 확인하는 과정을 접근 제어라고 한다. 이러한 접근 제어를 효과적으로 수행하기 위해서는 접근 권한의 불법 취득을 방지하고, 접근 권한에 관한 불법 변조가 일어나지 않도록 하여야 한다.

관리 정보베이스의 보안 유지와 관련된 대표적인 접근 제어 정책은 크게 자율적 접근 제어(DAC: Discretionary Access Control) 정책, 강제적 접근 제어(MAC: Mandatory Access Control) 정책, 그리고 역할기반 접근 제어(RAC: Role-based Access Control) 정책 등이 있다. 이 중에서 어느 접근 제어 정책을 선택할 것인가는 관리되어야 할 환경의 특성과 그 응용에 따라 달라질 수 있다[3].

자율적 접근 제어는 접근을 요청한 관리자의 신원(Identification)에 근거를 두고 있다. '자율적'이라고 하는 말은 관리자가 관리 객체에 대한 접근 권한을 자율적으로 부여하거나 철회할 수 있다는 것을 의미한다. 자율적 접근 제어에서는 관리 객체에 대한 관리자의 접근 권한을 접근 제어 행렬의 형태로 표현할 수 있다.

자율적 접근 제어와는 달리 강제적 접근 제어는 새로운 객체가 생성될 때 특정한 보안등급 부여 메카니즘에 의하여 객체에 보안등급이 부여되어야 한다. 강제적 접근 제어 정책은 모든 주체 및 객체에 대하여 일정하며 어느 하나의 주체/객체 단위로는 접근 제한을 설정할 수 없다. 강제적 접근 제어 정책을 이용한 대표적인 예로 BLP(Bell and LaPadula) 모델이 있다[3]. BLP 모델은 정보의 비밀성을 중요시하며, 정보의 흐름이 낮은 곳에서 높은 곳으로 흐르게 되므로 비밀성보다는 무결성이 더 중요시되는 상업적인 응용에는 적합하지 못하다.

강제적 접근 제어 정책이 군대와 같은 엄격한 보안 통제를 필요로 하는 환경에서 개발되었고, 자율적 접근 제어는 학술 연구 단체와 같은 자율적이고 협동적인 환경에서 개발되었기 때문에, 두 보안 정책이 모두 상업적인 분야에 적용하기에는 다소 부적합한 면이 있다. 따라서 전통적인 자율적 접근 제어에서처럼 사용자나 사용자의 그룹에게 객체에 대한 접근 권한을 부여하고, 강제적 접근 제어에서처럼 접근 권한을 부여하는데 제한을 가할 수 있는 접근 제어 방법에 대한 연구가 진행되었다. 그 결과로서 역할기반 접근 제어 정책이 만들어지게 되었다.

역할기반 접근 제어에서의 역할은 관리를 단순화하고 그에 따라 접근 권한을 단순화해주는 적당한 형태로 조직될 수 있다. 이처럼 역할 계층 구조에는 객체지향의 중요한 개념인 상속개념이 적용되어 역할 권한의 흐름은 상위 역할에서 하위 역할로 적용될 수 있다.

Ⅲ. 관리정보베이스 접근제어 확장

ITU-T X.741 권고안에는 접근제어 관리기능에 대한 정의와 함께 관리 정보 및 연산에 대한 접근을 제어하기 위한 모델에 대하여 기술하고 있다[1]. 그리고 접근 제어 정책에 따라서 접근을 허용하거나 접근을 제한하는데 사용되는 관리 객체 및 속성들을 정의하고 있다[4][5].

1. 접근제어 관리객체 클래스 표준구조

접근제어 정보와 접근제어 절차는 관리 객체로서 모형화 되며 그림 1은 ITU-T X.741 권고안에 정의된 관리 객체 클래스들의 상속 계층구조로서 여기에는 접근 제어를 위해 필요한 관리 객체 클래스들을 모형화하여 계층구조로 표현하였다.

다음 그림 2는 그림 1에서 정의된 관리 객체 클래스 상속 계층구조를 이용해 관리 객체들 간의 상호관계를 나타낸 것이다.

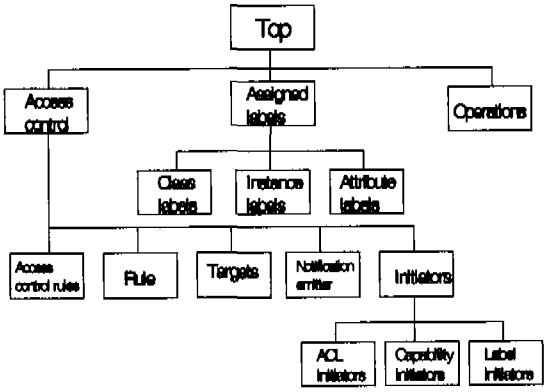


그림 1. 관리객체 클래스 상속계층구조

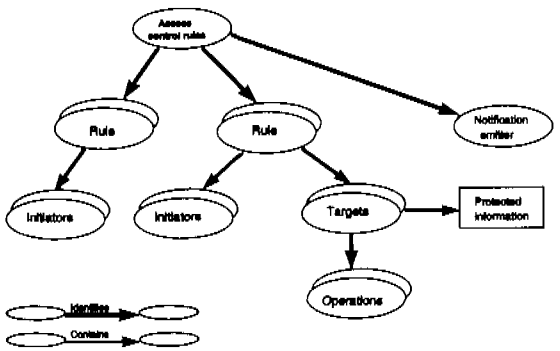


그림 2. 관리 객체 상호관계

2. 확장된 접근제어 관리객체 클래스구조

권고안(국제표준)에 정의된 접근 제어를 위한 관리 객체 클래스 구조는 접근 제어를 위한 각종 관련 정보 및 규칙을 보안관리자가 사전에 정의해 놓은 명시적인 접근 규칙(Explicit Access Rule)만을 정의함으로써 망의 규모가 점점 확대되고 이로 인한 관리 객체의 수가 급격히 증가되는 경우에 모든 관리 객체에 대해서 명시적 규칙을 날날이 정의하기가 사실상 불가능하다. 따라서 이에 대한 보완책으로서 기존의 권고안 구조에 묵시적인 규칙(Implicit Access Rule)을 포함하여 명시되지 않은 규칙에 대해서도 관리 객체간의 상호 관계를 이용해 접근 제어 규칙을 융통성 있게 적용함으로써 보안관리자의 권한부여 관리를 크게 단순화시킬 수 있고 각 규칙을 따로따로 정의하는데 따른 부가적인 간접경비를 대폭 줄일 수 있다.

다음 그림 3은 그림 1의 표준 관리 객체 클래스 계층구조를 확장한 것으로서 여기에는 규칙의 구조를 보다 명확하게 구체화하기 위해 명시적인 규칙(Explicit Rule)과 묵시적인 규칙(Implicit Rule)으로 구분하였다.

또한 RAC 정책을 지원하기 위해 'Initiators' 관리 객체에 'Role initiators' 관리 객체를 추가시킴으로써 DAC과 MAC의 단점을 보완할 수 있도록 하였으며, MAC에서 필요한 'Initiators'와 'Targets'의 레벨을 상호 비교하기 위해 'Constraints' 관리 객체를 추가하여 기존의 표준 구조를 크게 확장 및 보완하였다.

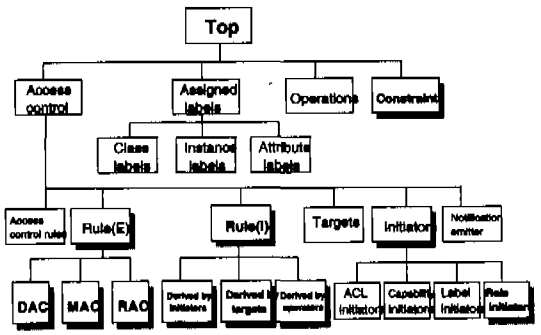


그림 3. 확장된 관리객체 클래스 상속 계층구조

위에서 정의한 확장된 관리 객체 클래스 상속 계층구조에 의해 다음 그림 4는 역할기반 접근 제어에 관련한 관리 객체 상호관계를 나타낸 것으로 명시적 규칙과 묵시적 규칙에 각각에 대해 'Role initiators'가 관리 객체들에게 역할을 부여하고, 주어진 역할에 따른 접근 제어를 할 수 있도록 함으로써 역할기반 접근 제어의 장점을 극대화하였다.

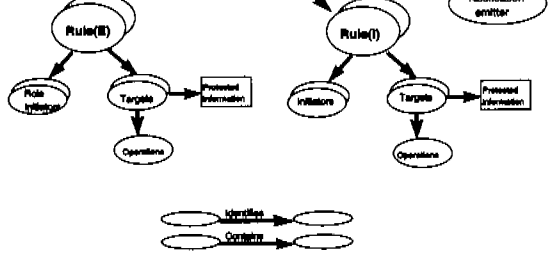


그림 4. 관리객체 상호관계(역할 기반 접근 제어)

Ⅳ. 관리정보베이스 접근제어 시스템

본 논문에서는 통신망 관리에 필요한 모든 정보들을 저장하고 있는 개념적인 정보 저장소인 망관

리 정보베이스에 대한 효율적인 접근 제어를 위해 접근 제어 모듈을 그림 5와 같이 크게 세 부분으로 나누었다[6].

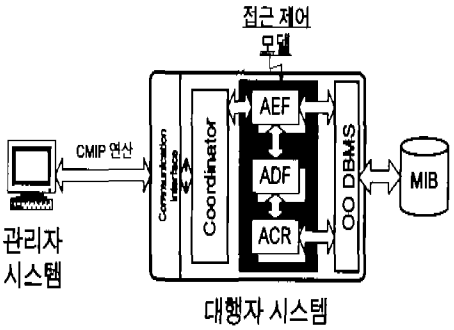


그림 5. 관리정보베이스 접근제어 시스템

접근 제어 수행(AEF:Access control Enforcement Function) 모듈은 관리자로부터

호출된 관리 연산을 받아서 관리 객체에 접근하여 관리 연산을 수행하는 모듈로서, 관리

객체에 접근하기 위하여 먼저 접근 제어 결정(ADF : Access control Decision Function) 모듈에 접근 허용 여부를 의뢰한다.

접근 제어 결정 (ADF) 모듈은 접근 제어 수행 모듈로부터 넘겨받은 접근 제어 정보를 접근 제어 규칙 모듈의 정보와 비교하므로써 접근 허용 여부를 결정하여 접근 제어 수행 모듈에게 통보하여 주는 역할을 수행한다.

접근 제어 규칙 모듈(ACR:Access Control Rule)은 접근 제어 결정 모듈에서 접근 허용 여부의 결정을 위하여 필요한 모든 정보를 제공하고 변경된 접근 제어 정보들을 첨가, 삭제, 그리고 수정하는 역할을 수행한다.

따라서 본 논문에서 제안한 접근 제어 규칙 모듈은 여러 가지 접근 제어 정책들에 대한 접근 규칙들을 하나의 모듈로 통합하였고, 접근 제어 수행 모듈과 접근 제어 결정 모듈 및 접근 제어 규칙 모듈들을 분리하여 작성하므로써 기존의 모듈들에 별다른 영향을 미치지 않고 새로운 접근 제어 정책의 삽입 및 삭제를 용이하게 하였다.

1. 접근 제어 규칙

1.1 자율적 접근 제어 규칙

자율적 접근 제어 정책에 해당하는 접근 제어 리스트 스킴과 능력 리스트 스킴에 필요한 관리 객체 및 속성은 다음과 같다.

- 'ACL initiators' 관리 객체 클래스는 접근 제어 리스트의 이름을 포함하고 있으며 관련속성에는 Attributes of ACL initiators, Access control list가 있다.
- 'Capability initiators' 관리 객체 클래스는 능력 리스트의 이름을 포함하고 있으며 관련 속성에는 Capability identities list가 있다.

1.2 강제적 접근 제어 규칙

강제적 접근 제어 규칙에 필요한 관리 객체 및 속성을 중심으로, 권고안의 기본구조와 함께 확장된 구조에서는 'Initiators'에는 인가등급을 부여하고, 'Targets'에는 비밀등급을 부여한 후 'Constraints'를 추가하여 'Initiators'와 'Targets'간의 다양한 상호비교가 가능할 수 있도록 하였다.

1.3 역할기반 접근 제어 규칙

여기서는 권고안을 바탕으로 역할기반 접근 제어 규칙을 Z 명세언어를 이용하여 모형화하고자한다[2][7].

역할기반 접근 제어 정책에 필요한 관리 객체 및 속성을 중심으로, 권고안의 기본구조와 함께 확장된 구조에서는 'Role Initiators'를 추가하여 역할기반에 의한 접근 제어가 가능하도록 하였다.

다음은 역할기반 접근 제어 관련 관리 객체 클래스들과 속성을 이용하여 접근 제어가 이루어지는 모형화에 대한 Z 표현으로서 접근 제어 정책에 공통으로 적용되는 관리 객체를 제외한 역할기반 접근 제어 관리 객체만을 나타내었다.

RoleACLinitiators

Initiators

ATTRIBUTE

roleAccessControlList:RoleAccessControlList

METHOD

GetRoleAccessControlList

ΞroleAccessControlList

output!:RoleAccessControlList

output!=roleAccessControlList

2. 접근 제어 수행

앞에서 모형화한 각 접근 제어 모델을 통해 망관리 정보베이스에 대한 안전한 접근 제어가 수행되는 절차를 확인한다. 즉, 각 접근 제어 정책에 따라 명시적인 규칙과 묵시적인 규칙에 대해 접근이 허

용되는 경우와, 허용되지 않는 경우를 접근 규칙으로서 정의하여 적용하여 봄으로써 접근 제어에 대한 수행 및 보안 검증을 하고자한다.

2.1 자율적 접근 제어 수행

자율적 접근 제어 보안 정책을 채택한 망관리 정보베이스에 대한 접근 제어를 위해 관리 정보베이스에 저장된 관리 객체 데이터에 대한 접근 요청을 보안 관리자에 의해 기술된 명시적 규칙과 접근 요청 'initiator', 'operator', 'object' 관리 객체별 상속 특성에 의해 추론된 묵시적 규칙을 이용한 접근 규칙을 통해 규정할 수 있다[8].

그림 6은 망관리 정보베이스 접근 요청에 대한 타당성 검증중 묵시적 규칙은 주어진 접근 제어 요청에 대해 위의 접근 권한 전파 특성을 이용하여 구성한 추론된 접근 제어 규칙 집합에 하나 이상의 명시적 규칙이 포함되어 있는지를 확인하는 과정이다.

추론된 접근 제어 규칙

= {(inf-initiator, inf-operator, inf-object)}

where

inf-initiator∈AccessPropagatedByInitiator (initiator?)

inf-operator∈AccessPropagatedByOperator (operator?)

inf-object∈AccessPropagatedByTarget (object?)

- AccessPropagatedByInitiator(initiator?), APBI(initiator?) : initiator들의 계층 구조에서 initiator?의 하위 계층에 속하는 initiator 집합 계산 함수
- AccessPropagatedByOperator(operator?), APBO(operator?) : operator들의 계층 구조에서 operator?의 하위 계층에 속하는 operator 집합 계산 함수
- AccessPropagatedByTarget(object?), APBT(object?) : 관리 대상 객체 클래스 계층 구조에서 object?의 상위 클래스 집합 계산 함수

2.2 강제적 접근 제어 수행

망관리 정보베이스에 대한 강제적 접근 제어 규칙에서는 'Initiator'와 'Target'에 각각 인가등급과 비밀등급이 명시적으로 부여되기 때문에 묵시적 규칙은 적용되지 않는다. 따라서 접근 요청 타당성을 판단하는 기능은 'constraint' 객체의 접근 결정 메소드에 의해 수행된다.

2.3 역할기반 접근 제어 수행

망관리 정보베이스에 대한 역할기반 접근 제어 규칙은 자율적 접근 제어 규칙의 'initiator'에 역할을 부여한 'role initiator'를 정의함으로써 명시적 규칙과 묵시적 규칙, 그리고 접근이 허용되는 경우와 허용되지 않는 경우를 자율적 접근 제어와 유사하게 표현할 수 있다[2][9].

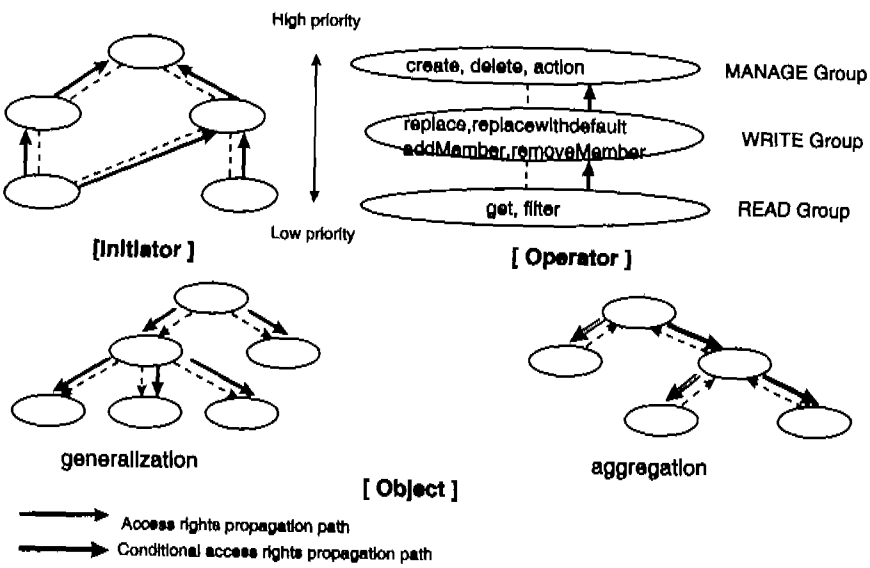


그림 6. 접근 권한 전파 특성

V. 결 론

본 논문에서는 관리 영역간 접근 제어 상호 운영을 통해 전체적인 통신망 관리를 보다 효율적으로 수행할 수 있는 관리자 기본 모델을 제안하였다. 즉 접근 제어를 위한 포괄적인 클래스 정의 및 접근 제어 보안 모델을 정의한 ITU-T X.741 권고안을 바탕으로 기존의 표준 관리 객체 클래스 구조를 크게 확장 및 보완하였다. 확장된 관리 객체 클래스 구조에서는 규칙의 구조를 보다 명확히 하기 위해 명시적 규칙과 묵시적 규칙으로 세분화하여 표현하였다. 그리고 역할기반 접근 제어를 위한 역할 관리 객체 클래스를 포함시켰고 강제적 접근 제어의 보안등급 비교를 위해 제약사항 관리 객체 클래스를 추가함으로써 접근 제어 규칙의 명확성과 융통성을 함께 보장하였다. 또한 확장된 접근 제어 규칙에 따라 프린터 관리 정보베이스를 이용해 실제 접근 제어 규칙이 적용되는 절차를 각 접근 제어 정책에 따라 적용하여봄으로써 접근 제어 시스템에 대한 수행부분을 검증하였다.

참 고 문 헌

[1] ISO/IEC 10164-9/ITU-T X.741, "Objects and Attributes for Access Control"

[2] Matunda Nyanchama, Sylvia Osborn, "Role-Based Security, Object Oriented Databases & Separation of Duty," SIGMOD RECORD, Vol. 22, No. 4, December pp. 45-51, 1993.

[3] David d. Clark, David R. Wilson, "A Comparison of commercial and Military computer security policies," IEEE, 1987.

[4] Oliver Festor, Georg Zormtlein, "Formal Description of Managed Object Behaviour - A Rule Based Approach," IFIP Integrated Network Management, pp45-58, 1993.

[5] E. B. Fernandez, R. B. France, and D. Wei, "A formal specification of an authorization model for object-oriented database," Workshops In Computing security for object-oriented systems, Washington DC, 1996.

[6] Rumbaugh J, Michael Blaha, "Object-Oriented Modeling and Design," Prentice Hall, Inc 1991.

[7] David Rann John Turner and Jenny Whitworth, "Z: A Beginner's Guide," School of Computing Staffordshire University UK, 1994.

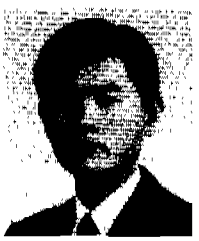
[8] Ravi S. Sandhu, Pierangela Samarati, "Access Control: Principles and Practice," IEEE Communications Magazine, September 1994,

[9] ISO/IEC 10165-2/ITU-T X.721, "Definition of Management Information," 1992.

[10] ISO/IEC 10165-4/ITU-T X.722, "Guidelines for the Definition ofManaged Objects," 1992.

[11] ISO/IEC 10164-3/ITU-T X.732, "Attributes for Representing Relationships," 1992.

김 종 덕(Jong-Duk Kim) 정회원



1983년 : 전남대학교 전산학과 졸업(이학사)

1988년 : 국방대학원 전자계산학과 졸업(이학석사)

1997년 : 전남대학교 대학원 전산통계학과 졸업 (이학박사)

1995년~1997년 : 전남대학교 전산학과 시간강사

1998년~현재 : 전남도립 담양대학 전산·정보통신공학부 조교수

<주관심 분야> 통신망관리, 정보통신 보안, 객체지향 시스템