논문 01-26-6T-7 한국통신학회논문지 '01-6 Vol.26 No.6T

# BDL을 이용한 통신망관리 객체의 시간지원 능동특성에 대한 정형적 모델

정회원 김 종 덕*

# A Formal Model of Communication Network Managed Objects with Temporal and Active Properties Using BDL

Jong-Duk Kim* *Regular Member*

요 약

본 논문에서는 시간속성과 능동특성을 지원하는 통신망관리 객체의 동적특성 표현언어인 BDL(Behaviour Description Language)을 이용하여 시스템 망관리 모델의 관리기능을 정형적으로 표현하였다. 그리고 BDL로 표현된 관리기능을 CORBA IDL로 변환하는 BDL_to_IDL 컴파일러를 설계·구현하였다. 특히, 통신망 관리 정보베이스에 저장되어있는 관리객체를 안전하게 보호하기 위해 ITU-T 권고안에 정의된 강제적 접근제어 모델과 역할기반 접근제어 모델을 상호연동한 접근제어모델을 정의하였다. 또한, 관리속성값을 제어하는 관리연산을 연관된 유형별로 묶어 역할로 정의하고 관리자와 관리객체에 인가등급과 보안등급을 부여하여 역할배정규칙과 제약조건에 따라 관리정보의 접근을 제어함으로써 보다 무결성을 보장받도록 하였다.

ABSTRACT

In this paper, we described network management functions using a language for specifying behavioral aspects of managed objects, BDL(Behaviour Description Language), that supports temporal and active properties. And, With a BDL to IDL translator, network management functions can be easily coded and transformed into CORBA IDL. Also we define a new access control model which combines Biba model, one of the mandatory access control policies stipulated by ITU-T Recommendations, and RBAC model for securing managed objects in Management Information Base. In that model, we categorize management operations for administrative attributes as a role and assign security levels to both managed objects and network managers. This model ensures the integrity MIB by controlling accesses to managed objects with constraint conditions and role assignment rules.

## Ⅰ. 서 론

통신망 관리기능을 정의하는 관리객체 클래스는 통신망 구성 자원들의 정적 속성 및 동적 특성, 연관된 관리객체 클래스간의 상속관계 등에 대한 정보를 객체지향 개념을 기반으로 표현한다[1][2]. 따라서 통신망 관리시스템은 관리객체 클래스에 정의된 속성과 연산을 통해 통신망 구성요소 내부의 구현 방식과는 무관하게 관리대상 객체의 동작상태를 감시하거나 필요에 따른 적절한 제어기능을 수행할 수 있다[4][5].

망관리 시스템에서는 중요한 상황이 발생할 때, 시기 적절하게 대처할 수 있는 기능이 필수적으로 제공되어야 하며, 망관리 정보 베이스의 시간 데이터(temporal data)를 이용한 자원관리 기능이 첨가되어야한다. 따라서 망관리 정보 베이스 상태를 감독하고, 정의된 조건을 만족시키는 연산이 수행되었을 때 이에 대한 적절한 행위를 시간적 제약사항에

* 전남도립 담양대학 초고속정보통신공학부(jdkim@damyang.damyang.ac.kr)
논문번호 : T01004-0326, 접수일자 : 2001년 3월 26일

따라서 수행하는 시간지원 능동 특성을 갖는 망관리 시스템이 필요하다. 또한 엄격한 시간 제한 내에 수행되거나 일정한 주기를 갖고 반복적으로 수행되는 관리 서비스의 경우 망관리 정보 베이스의 무결성과도 밀접하게 연관이 되어 시간지원 개념이 절실히 요구된다.

본 논문에서는 정적 및 동적 시간속성과 능동특성을 지원하는 동적특성 표현언어인 BDL(Behaviour Description Language)을 정의하고 이 언어로 표현된 시스템 망관리 모델의 4가지 관리기능을 정형적으로 표현한다. 그리고 BDL 파서와 IDL 코드 생성기로 구성된 BDL_to_IDL 컴파일러를 개발하여 CORBA IDL 파일로 변환한다. 이는 기존 IDL_to_C++이나 IDL_to_Java 컴파일러를 이용하면 BDL로 정의된 관리객체의 동적 행위부분을 구현할 수 장점을 제공한다. 특히, 망 관리 정보베이스에 저장되어있는 관리객체를 안전하게 보호하기 위해 표준 권고안에 정의된 강제적 접근제어 모델과 역할기반 접근제어 모델을 상호연동한 접근제어 모델을 정의하여 관리자와 관리객체의 보안등급과 역할, 그리고 이들간의 제약조건에 따라 관리정보의 접근을 제어함으로써 보다 무결성을 보장하고자 한다.

## Ⅱ. 관리정보 모델

### 1. 개 요

관리정보 모델의 관리객체를 정의하기 위한 가이드라인인 GDMO는 OSI환경에서 자원관리를 위한 관리객체 클래스를 표현하는데 사용되는 표기법을 정의하기 위한 국제 표준으로서 관리객체 클래스 템플릿, 패키지 템플릿, 매개변수 템플릿 등 9개의 템플릿을 이용하여 관리객체 클래스의 정적 및 동적 특성을 표현하고 있다[3][8]. 또한 관리정보 모델에 포함된 추상적인 모델링 개념과 OSI 환경에서 특별한 자원 관리를 위한 관리객체 클래스의 표현 요구조건과의 관계를 매핑해 주는 역할을 수행한다.

### 2. 대리자 관리 기능 모델

그림 1의 대리자 관리 기능 모델에서 대리자 관리객체는 망 관리 서비스를 제공할 뿐만 아니라 관리 객체 인터페이스와 개방형 통신 인터페이스간의 매핑을 제공한다. 또한 대리자에서는 수행되는 연산을 선택적으로 필터링하는 메커니즘과 통지를 통해 발생하는 데이터의 흐름을 제어하는 기능을 제공한다[9]. 국제표준안에서 제공하는 대리자의 기능에는 접근제어, 사건 보고, 스케줄링, 그리고 로깅 기능 등이 있다[6][7][10]. 관리자와 관리객체에 대한 접근 권한의 허가 여부를 결정하는 접근제어 기능과 관리객체에 대한 특정 사건이 발생하였을 때 관리자에게 통지하는 사건 보고 기능, 주기적이고 반복적인 스케줄링 계획에 따라 관리객체의 활동을 제어하는 스케줄링 기능 그리고 사건이나 통지, 관리객체 접근 등 전반적인 내용에 대한 감사 추적을 위한 로깅 기능 등이 있다.

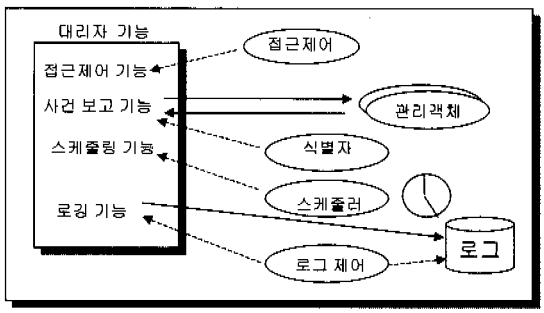


그림 1. 대리자 관리 기능 모델

## Ⅲ. 정형적 모델의 설계

### 1. 모델링 개념

본 논문에서는 시스템 망관리 모델의 4가지 관리기능을 동적특성 표현언어인 BDL을 사용하여 표현한 후 CORBA IDL로 변환하는 컴파일러를 개발하여 실제 망관리에 적용될 수 있는 기반을 제공한다.

### 2. 동적특성의 구성요소

관리 객체의 시간속성을 지원하는 능동특성의 시스템 망관리 모델의 관리기능을 정형적으로 표현하기 위한 구성요소는 다음과 같다.

#### 1) 외부요인(EVENT)

관리객체의 동작 절차의 결정요소로서 통신망 관리자로부터 전달되는 관리객체에 대한 관리연산의 실행요청과 다른 관리객체로부터 전달되는 통지 또는 사건보고 등이 있다.

#### 2) 선행조건(PRECOND) 및 불변조건(INVARIANTS)

선행조건은 관리연산의 정상적인 수행이나 통지가 발생되기 위한 논리조건을 표현하고 불변조건은 관리객체의 동작 전체 과정에서 지켜져야 하는 조건을 표현한다.

3) 동작절차(PROCEDURE)

관리객체로 전달되는 외부요인이나 관리객체 내부의 속성값, 조건부 패키지의 선행조건 등을 이용한 ECA 규칙을 기반으로 작성된다. 관리객체에 대한 사건(EVENT)이 발생되면, 발생된 사건의 처리 여부를 결정(PRECOND)하고 사건에 대한 적절한 조치(ACTION)를 수행하는 구조를 가진다.

## 3. 동적특성 표현방법 설계

OSI의 기본적인 시스템 망관리 모델은 관리표준의 관리기능과 GDMO를 포함하는 관리정보의 구조 및 세부내용을 갖는다. 특히, 관리기능에는 상호연동한 접근제어 기능과 사건보고, 스케줄링 그리고 로깅기능으로 구성된다.

### 3.1 상호연동한 접근제어 기능

접근제어 기능은 관리객체의 보안을 위하여 사용자의 접근을 제어 및 관리하는 기능이다. 여기에서는 강제적 접근제어 모델중에서 무결성을 보장하는 Biba 모델과 실생활에 적용될 수 있는 역할기반 접근제어 모델을 상호연동한 접근제어 모델의 규칙을 기반으로 표현되었다. 그리고 상호연동한 접근제어 모델의 역할영역과 제약조건을 정의한 후 접근제어 규칙인 'rule' 관리객체 클래스를 BDL로 표현하였다. 특히, 표준안에 표현되어있지 않은 접근제어 관리 기능인 접근제어 결정함수와 접근제어 집행함수의 행위 템플릿을 세부적으로 명확하게 표현하였다.

### 3.2 사건보고 기능

사건 보고 기능은 시스템에 이미 발생한 사건이나 발생할 가능성이 있는 사건 등을 관리자에게 통지해 주는 역할을 수행한다. 사건에 대한 통지는 사건 전송 식별자(Event Forwarding Discriminator)에 의하여 선택되어 CMIS의 M-EVENT-REPORT 서비스를 이용하여 관리자에게 보내어진다[6].

다음은 BDL를 이용한 사건 보고 기능에 대한 시간 지원 동적 특성을 정형적으로 표현한 예이다.

```
eventForwardDiscriminator MANAGED OBJECT CLASS
DERIVED FROM discriminatior;
CHARACTERIZED BY efdPackage PACKAGE
B E H A V I O U R eventForwardingDiscriminatorBehaviour
BEHAVIOUR
DEFINED AS
  EVENT : PortentialReportEvent
                managedObjectClass: ObjectClass,
                managedObjectInstance: ObjectInstance,
                eventType: EventTypeID,
                .....
```

그림 2. BDL을 이용한 eventForwardDiscriminator MO Class 동작 특성 표현

### 3.3 스케줄링 기능

특별한 관리객체 인스턴스 내에 명세되어 있는 시간 관리객체의 활동을 제어하여 관리객체 내에서 자체적으로 발생하는 'trigger scheduling' 인 비주기적인 스케줄링과 관리객체의 활동에 사용되는 연산의 시간구간을 지정하여 일정하게 반복적으로 제어하는 'interval scheduling' 주기적인 스케줄링으로 나뉜다.

스케줄링 기능에 대한 스케줄러 관리객체의 시간지원 동적 특성의 정형적 표현은 다음과 같다.

```
scheduler MANAGED OBJECT CLASS
DERIVED FROM : top;
CHARACTERIZED BY schedulerObjectPackage,
                 duration;
schedulerObjectPackage PACKAGE
BEHAVIOUR schedulerObjectBehaviour
BEHAVIOUR
DEFINED AS
   EVENT : LockSchedulingManagedObject
           schedulerOjectName : schedulerObject,
           .....
```

그림 3. BDL을 이용한 scheduler MO Class의 동작 특성 표현

### 3.4 로깅 기능

다양한 객체에 의해 수행되어진 연산이나 이미 발생한 사건에 관한 정보를 유지할 필요가 있는데 OSI 관리 모델에서는 'log'나 'log record'라는 관리객체클래스를 사용하여 정보를 보관한다. 'log' 관리객체는 외부로부터 전달되는 사건 보고나 로컬 시스템에서 발생된 통지의 저장 기능을 수행한다.

'log record'는 로그에 저장되는 정보의 단위를 나타낸다.

## Ⅳ. 표현 모델의 구현

본 절에서는 관리객체의 행위부분을 정형화한 BDL 문법의 정확성을 검증하기 위하여 BDL_to_IDL 컴파일러를 구현하여 제시하였다.

### 1. BDL_to_IDL 컴파일러 설계

관리객체의 동적특성을 CORBA IDL로 변환하는 소프트웨어의 구현은 다음의 두 단계로 구성된다. 먼저, 관리객체의 행위부분을 표현하고 있는 BDL 파일에 대한 에러 검색과 문법을 점검하는 BDL 파싱 단계와, 파싱 작업이 성공적으로 끝났을 때 BDL 파일을 CORBA의 IDL로 변환하는 IDL 코드 생성 단계이다.

BDL_to_IDL 컴파일러는 BDL을 CORBA의 IDL 파일로 변환시켜 주는 프로그램이다. 먼저, 이 컴파일러를 실행시키기 전에 XGDMO2IDL 컴파일러를 통해 관리객체 클래스와 관련된 패키지 그리고 속성들을 CORBA IDL로 변환해주어야 한다. 이 컴파일러에는 X721.gdmo라는 관리정보베이스가 입력값으로 요구된다. X721.gdmo는 X.721 권고안에 표현되어있는 관리객체 클래스를 데이터베이스화한 GDMO 파일로서 관리객체 클래스와 관련된 패키지 그리고 클래스에서 정의된 속성들로 구성되어 있다. 이러한 X721.gdmo에 BDL 파일을 삽입한 후 XGDMO2IDL을 실행시킨다. 물론 BDL 파일의 처음과 끝부분에는 특정 문자를 삽입하여 실행하였으므로 출력되는 IDL 파일에는 주석으로 처리되어 나온다. 주석으로 처리되어진 BDL 파일은 BDL_to_IDL 컴파일러를 통해 IDL 파일로 변환되어진다(그림 4).

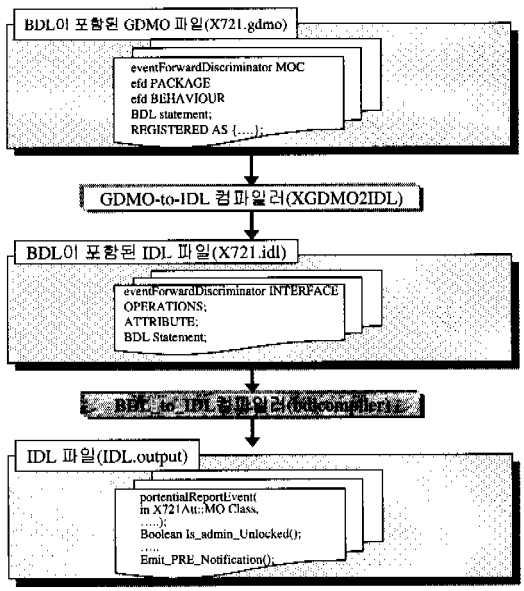


그림 4. BDL 파일의 IDL 변환 과정

#### 1) BDL 파서

BDL 파서는 컴파일러 생성 지원 도구인 Lex와 Yacc을 이용해서 구축되었다. DataType DB에는 BDL 파일의 속성 정의부분에서 사용되는 Data Type으로 ObjerctClass, ObjectInstance, EventTypeID, SecurityAlarmSeverity, BackUpStatus, ProbableCause, DiscriminatorConstruct 등을 가지고 있다. 이 DataType은 ASN.1에 정의된 타입이어야 한다.

#### 2) IDL 코드생성기

IDL 코드생성기는 BDL 파서에 의해 어휘분석과 구문분석이 성공적으로 끝난 BDL 파일을 받아서 IDL 파일로 변환한다. IDL 코드생성기는 먼저 BDL 파일을 버퍼로 읽어 들이고 이 버퍼에서 토큰을 가져와 Event부분, Precondition부분, Invariants 부분, Procedure부분 중 하나를 선택해서 적당한 IDL 파일을 생성한다. 이때, BDL 파일은 IDL 파일에 주석으로 처리된 후 그것에 해당하는 IDL 파일이 삽입된다. BDL 파일을 주석으로 처리하는 것은 프로그램 개발자가 고급언어로 변환하고자 할 경우 도움이 되고자 하는데 그 이유가 있다.

### 2. 실행결과 고찰

BDL_to_IDL 컴파일러인 bdlcompiler는 XGDMO2IDL에서 출력값으로 생성된 IDL 파일중에서 행위부분을 표현하고 있는 BDL 파일만을 추출하여 IDL로 변환해주는 컴파일러이다. bdlcompiler는 BDL 파서 기능과 IDL 코드생성기 기능을 수행하는 컴파일러로 BDL 파일과 속성값을 출력하기 위한 권고안 타입이 입력값으로 들어간다. BDL 파일에 대한 어휘분석과 구문분석을 마치면 CORBA의 IDL 파일로 변환된 IDL.output 파일이 생성된다.

## Ⅴ. 결 론

통신 장비를 구성하고 있는 요소들이 복잡해지고 규모가 커지고 있는 요즘, 복잡한 전체 망의 원활한

제어와 관리기능을 제공하는 망관리 시스템은 필수적이다.

본 논문에서는 정적 및 동적 시간속성과 능동특성을 지원하는 동적특성 표현언어인 BDL로 표현된 시스템 망관리 모델의 4가지 관리기능을 정형적으로 표현하였다. 그리고 BDL 파서와 IDL 코드생성기로 구성된 BDL_to_IDL 컴파일러를 개발하여 CORBA IDL 파일로 변환하였다. 이는 기존 IDL_to_C++이나 IDL_to_Java 컴파일러를 이용하면 BDL로 정의된 관리객체의 동적 행위부분을 구현할 수 장점을 제공한다. 특히, 망 관리 정보베이스에 저장되어있는 관리객체를 안전하게 보호하기 위해 표준 권고안에 정의된 강제적 접근제어 모델과 역할기반 접근제어 모델을 상호연동한 접근제어 모델을 정의하여 관리자와 관리객체의 보안등급과 역할, 그리고 이들간의 제약조건에 따라 관리정보의 접근을 제어함으로써 보다 무결성을 보장한다.

## 참 고 문 헌


[1] Elisa Bertino, Claudio Bettini, Pierangela Samarati, "A Discretionary Access Control Model with Temporal Authorizations", IEEE New Security Paradigms Workshop, 8, 1994.

[2] Oliver Festor, Georg Zorntlein, "Formal Description of Managed Object Behavior - A Rule Based Approach," Proceedings of the IFIP TC6/WG6.6 3rd International Symposium on Integrated Network Management, 1993

[3] Masum X. Hasan, "An Active Temporal Model for Network Management Databases," Proceedings of the 4th International Symposium on Integrated Network Management, 1995

[4] Sylvia Osborn, "Mandatory Access Control and Role-Based Access Control Revisited", Second ACM Workshop on RBAC, pp. 31-40 11. 1997.

[5] Morris Sloman, Network and Distributed Systems Management, Addison-Wesley, 1994

[6] ITU-T X.720 : "Information Processing Systems - Open Systems Interconnection - Management Information Model", Geneva

[7] ITU-T X.721 : "Information Processing Systems - Open Systems Interconnection - Management Information Services - Structure of Management Information Part 2: Definition of Management Information", Geneva

[8] ITU-T X.722 : "Information Processing Systems - Open Systems Interconnection - Management Information Services - Structure of Management Information Part 4: Guidelines for the Description of Managed Objects", Geneva

[9] ITU-T X.723 : "Information Processing Systems - Open Systems Interconnection - Management Information Services - Structure of Management Information Part 5: Generic Management Information"

[10] ITU-T X.734 : "Information Technology - Open Systems Interconnection - System Management - Event Report Management Function "



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 초고속정보통신공학부 조교수

<주관심 분야> 인터넷보안, 통신망관리, 정보통신보안, 객체지향 시스템