

개방형 네트워크와 정책 기반의 네트워크 관리기술

신영석

호남대학교 정보통신공학과

목 차

- I. 서론
- II. 객체지향 통신 프로토콜
- III. 개방형 네트워크 연구
- IV. 정책 기반의 네트워크 관리
- V. 결론

I. 서 론

인터넷 기술과 소프트웨어 기술의 접목으로 사용자는 새로운 서비스에 대한 관심과 요구가 높아지고 있다. 소프트웨어 기술은 90년 초반에 객체지향(object-oriented) 설계와 모델링 기술의 출현으로 소프트웨어 재사용과 모델링의 간편성 및 분산 시스템 환경에서 컴포넌트 운영 기술의 발전을 근간으로 네트워크의 정보모델링과 분산처리환경(DPE, Distributed Processing Environment) 기술의 도입으로 신규 응용 서비스 개발에 박차를 가하게 되었다. 최근 객체지향 패러다임을 적용하여 통신 프로토콜[1]과 통신망 관리를 위해 전송 시스템에 객체 모델로 정립하는 연구가 ITU-T M series로 결과를 보였다[2].

TINA(Telecommunication Information Networking Architecture) 컨소시엄은 분산처리환경에서 네트워크의 연결관리 기능과 응용 서비스를 통합한 객체모델링을 정립하여 기존의 통신망 구성장치(NE, Network Element)에 DPE를 수용한 소프트웨어 기능 구조로 네트워크 관리와 서비스를 쉽게 개발하는 연구를 시도해왔다[16,33]. 그러나 소프트웨어 패러다임과 방향 정립은 좋으나, 잦은 통신 프로토콜 변경과 짧은 신규 서비스 라이프 사이클로 인한 하드웨어 업그레이드, 중앙 집중적 관리에 어려움이 직면해 있다. 따라서 기본적으로 하드웨어 변경 없이 네트워크와 서비스 간의 통

합은 어려워져 하드웨어와 필요에 따라 네트워크의 요소 기능을 지원하는 개방형 소프트웨어 스위치와 액티브 네트워크(active network)가 출현하게 되었다[13,14,15].

액티브 네트워크는 기존 SAF(Store-And-Forward) 방식의 라우터에 컴퓨팅 처리 기능을 추가하여 SCF(Store-Computing-Forward) 방식으로서 필요에 따라 액티브 패킷(스마트 패킷)을 수용하여 기존 라우터에 지능화 기능을 부여하여 수행되도록 하였다. 이는 결국 모든 네트워크에 액티브 라우터 기능을 부여해야만 가능하다. 현실적으로 전 세계 네트워크를 액티브 라우터로 구조화해야 하며, 이들의 관리하기에는 어려운 형편이다. 따라서 기존 네트워크에 가능한 구현의 편리성과 데스크 탑 PC에서 통신망과 각종 서비스 장치 및 단말기를 보다 쉽게 관리하고[28], 응용 서비스를 개발하도록 개방형 API를 제공하는 방안[25,34]과 여러 표준화 기관은 이를 시스템을 객체화하여 쉽게 제어 관리하는 객체 정보모델링으로 표준화를 시도하고 있다[28,29,34].

본 논문에서는 현재 네트워크의 한계를 극복하려는 여러 개방형 네트워크 기술을 살펴보고, 이들 중에 최종 네트워크 인프라가 되기 전에 기존 네트워크에 손쉽게 접근하기 위해 정책 기반의 네트워크 관리(PBNM, Policy Based Network Management) 기술을 살펴본다. 정책 기반의 네트워크는 현재 DMTF, IETF, The Parlay Group

표준화 기관에서 서비스 품질(QoS, Quality of Service)과 정보보호 분야 그리고 제3 서비스 사업자를 위한 서비스 관리에 적용하고 있으며, 본 연구에서는 보안정책의 정보모델링과 관리기술을 살펴본다.

II. 객체 지향 통신 프로토콜

2.1 객체 지향 프로토콜

H. Zimmermann에 의해 OSI 참조모델(RM, Reference Model)이 제안된 후, 통신 프로토콜 기술은 단계적이며, 체계적으로 발전해 왔다. ITU-T는 B-ISDN PRM(Protocol RM)을 제안하여[3], 종래의 사용자평면과 제어평면에서 관리평면 기능을 확장하여 PRM을 정립하였다.

ISO는 OSI RM을 7개 계층과 평면의 프레임워크로 시스템 모델과 각 계층 간의 서비스를 제공하는 서비스 및 프로토콜 모델, 연결(connection)과 데이터그램의 추상적(abstraction) 정보에 기반을 둔 통신모델을 제안하여, 사용자들 간의 통신 연관(association)의 패러다임으로 연결과 프로토콜을 표현하였다. 특히 ISO 트랜스포트 계층은 성능, 신뢰도, 보안, 우선순위 등의 서비스 품질로 통신모델을 기술하였다. 이러한 표준화 연구는 객체지향 설계 및 모델 기술과 접목하여 객체지향 프로토콜 구조를 그림 1과 같이 계층과 평면 간의 모듈화된 통신 시스템을 모델화하고, 프로토콜을 객체로 구현하여 네트워크와 통신시스템을 통합하여 객체지향 모델기반으로 신규 서비스를 손쉽게 적용도록 하였다.

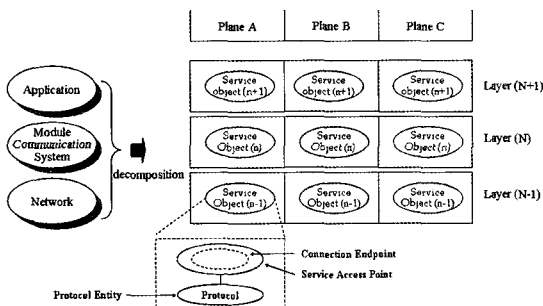


그림 1. 객체 지향 프로토콜의 시스템 모델

객체지향 프로토콜을 시스템 혹은 NE에 적용하기 위해 궁극적으로 네트워크 노드 모델이 요구된다. NE에 객체지향 프로토콜과 응용 서비스 제공을 위한 새로운 기능 구현을 위해 그림 2와 같은 노드 모델을 제공하고 있다. 네트워크 접속 기능과 통신을 위한 기능 모듈에 프로토콜과 시스템 운영을 위한 OS 그리고 응용 서비스를 위한 API(Application Programming Interface)로 모델을 제공한다.

일반적으로 NE 운영체제를 네트워크 운영체제(NOS, Network OS)로 분산 시스템 혹은 실시간 처리 커널을 기반으로 NOS가 NE 벤더들에 의해 개발되어 네트워크에 적용되고 있다. 한 예로 Cisco의 IOS(Interworking OS)도 NOS로 볼 수 있다.

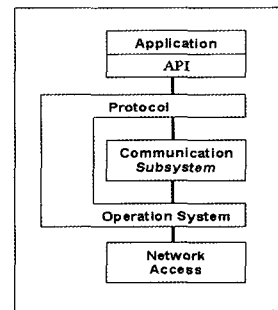


그림 2. 네트워크 노드 모델

2.2 NGN(Next Generation Network)

통신 시장은 음성 서비스를 기반으로 컴퓨터와 같은 지능형 단말기와 이동형 단말기로 유무선을 통한 데이터 중심의 통신 서비스로 변화되고 있다. 멀티미디어 서비스 출현으로 다양한 종류의 서비스 제공을 위해 네트워크에서는 멀티미디어, 다자간 통신(multi-party), 멀티 프로토콜(multi-protocol), 서비스 품질의 확대와 통합 네트워크(multi-network) 특성을 보이고 있다.

지금까지 통신 서비스는 여러 개별적인 통신망에서 다양한 응용 서비스와 통신 서비스를 제공하기 위해 하부 통신망의 능력을 이용하여 서비스를 제공하는 상향식(bottom-up) 개발 방법론으로 개발되어 왔다[24]. 이와 같은 상향식으로 개발한 통신 서비스는 하부 통신망의 구조 및 프로토콜에 절대적으로 의존하기 때문에 통신망의 한

제를 극복할 수 없는 결과를 낳게 되었다. 즉 서비스 개발에 많은 비용과 시간이 소요되며, 단기간에 다양한 멀티미디어 통신 서비스를 개발하여 여러 통신 사업자 혹은 서비스 사업자에게 제공하기에는 한계성이 있다. 이러한 환경을 보다 쉽게 해결하고자 차세대 통신망(NGN) 구조를 제시하고, 다양한 멀티미디어 서비스를 신속, 정확, 편리하게 개발하고 서비스를 제공하는 연구가 진행되고 있다[34].

NGN 서비스는 기본적으로 멀티미디어, 다자간 통신, 멀티 네트워크와 멀티 프로토콜 특성을 근간으로 함에 따라 음성, 문자, 화상 등의 멀티미디어 정보 전달에 유리한 패킷망을 구성해야 한다. 기존의 인터넷을 수용하고, 신규 서비스를 제공하도록 하부 통신망을 캡슐화와 필요 기능을 추상화하여 상위계층에서 이용 가능토록 계층 구조를 그림 3과 같이 3개의 계층으로 구조화한다.

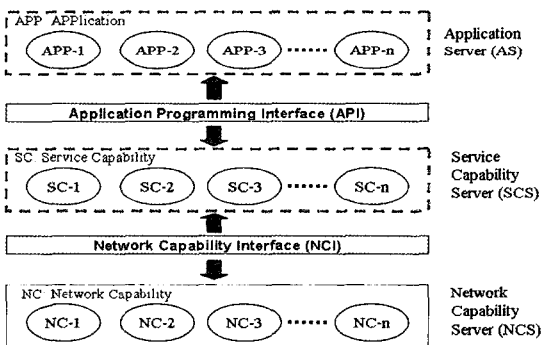


그림 3. NGN 네트워크 모델

네트워크 능력 계층(network capability layer)은 네트워크 내부와 하부의 기능(functionality)을 나타낸다. 비표준 혹은 전용 인터페이스를 제공하는 네트워크 자원과 표준 접속 프로토콜(NCI, Network Capability Interface)로 구성되며, MGCP, SIP와 같은 IP 단말의 세션 제어를 위한 프로토콜과 소프트 스위치 및 물리계층 연결을 예로 들 수 있다. 서비스 능력 계층은 네트워크 능력 계층에서 제공하는 기능을 추상화하여 개방형 네트워크 API 통해 접근하도록 추상화한다. 응용 계층(application layer)인 서비스 계층은 서비스 능력 계층에서 제공하는 API를 이용하여 접속되어 다양한 응용 서비스를 제공한다. 이로서 제3

사업자는 API에 따라 서비스 개발을 하면서, 통신 사업자에서 제공하는 NCI를 이용하여 서비스를 개발한다. 개발된 서비스는 특정 통신 사업자에 의존되지 않고 여러 사업자에게 적용됨에 따라 손쉽게 여러 자원을 절약하여 신속하게 서비스 개발이 가능한 인프라를 제공한다.

2.3 정보모델링

OMG는 객체 간의 정보를 교환하는 모델로 객체모델, 동적모델, 기능모델을 제시하여 이를 체계적으로 발전하여 분산 환경에서 객체 간의 접속 가능한 CORBA(Common Object Request Broker Architecture) 규격과 UML(Unified Model Language)를 제시하였다.

TINA 컨소시엄은 DPE 환경에서 NE 네트워크 자원(NRIM, Network Resource Information Model)과 서비스 컴포넌트 간의 정보를 모델화하기 위해 정보모델, 연산모델(computational model), 시스템 모델로 구분하여 객체와 객체 간의 오퍼레이션, 객체 혹은 컴포넌트의 시스템에 구현에 따른 모델을 제시하고 있다. 이와 같은 네트워크를 객체 모델화도 중요하지만, 실제 NE 관리하기 위한 객체 모델화가 네트워크 보다 우선되어야 한다. 결국 네트워크의 연결과 호 설정을 위해서는 기본적으로 NE 객체가 모델화하여 네트워크 API를 통해서 NE를 제어 관리해야 한다.

NE 관리를 위한 정보모델의 표준화 연구는 다양한 표준화 기관과 공개 소프트웨어 기구에서 관리 및 응용에 관련된 권고와 표준화 연구가 시도되고 있다. NE를 관리하는 SNMP(Simple Network Management Protocol) 기반의 MIB (Management Information Base), 데스크탑 시스템을 관리하는 DMI(Desktop Management Interface) 기반의 MIF(Management Information Format), TMN(Telecommunication Management Network)을 위해 통신 시스템을 관리하는 CMIP (Common Management Information Protocol) 기반의 GDMO(Guidelines for the Definition Managed Object)가 대표적인 관리의 표준 규격으로 볼 수 있다.

관리 표준화 연구는 장기적으로 볼 때는 ITU-T의 CMIP으로 수렴되고 있으나, 신속한 구현 및

간편성에서는 IETF의 SNMP와 그림 4와 같은 DMTF에서 권고하는 DMI와 객체지향 구조의 CIM에 많은 벤더와 기관들이 컨소시엄으로 연구를 수행하고 있으며, 일부 벤더에서는 NE에 적용하여 상용 제품을 내놓고 있다[12,21,22,29].

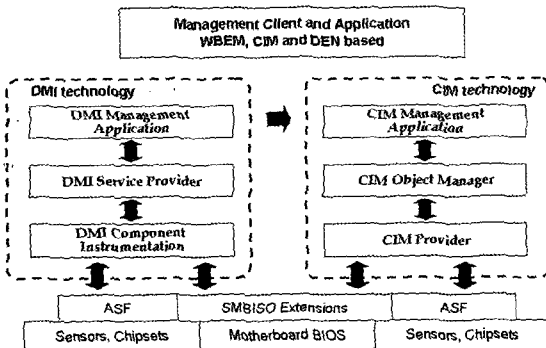


그림 4. DMTF의 관리표준과 관계

III. 개방형 네트워크 연구

3.1 TINA 연구

차세대 통합망의 진화발전 방향과 통신망 사용자들의 다양한 서비스 요구와 사용자 단말기의 멀티미디어화 추세에 따라, 통신망은 점점 더 복잡해지고 있다. 통신망이 복잡해질수록 통신망 관리 및 신규 멀티미디어 서비스의 수용은 어려워지며, 효율적인 망 성능을 유지하기 위해서 많은 문제점들을 해결해야 한다. 이러한 사용자의 다양한 서비스 요구와 통신망의 발전에 따라 원활한 멀티미디어 서비스를 제공하기 위하여, 효율적인 통신망 관리와 서비스 관리가 요구되어 TMN 도입과 신속한 멀티미디어 서비스를 위한 서비스 통합 및 표준화 활동에 많은 연구가 이루어지고 있다.

이러한 문제를 근본적인 해결하기 위해서 TINA는 신속한 멀티미디어 서비스 제공과 이동 통신 기능의 서비스, 다자간 연결 기능 등을 제공하기 위해 객체지향 설계 개념의 적용과 네트워킹 미들웨어 소프트웨어 개념을 도입하여 통신망 인프라를 정립하였다. 언제 어디서나 어떤 단말기로든지 멀티미디어 서비스를 제공받을 수 있도록

서비스와 통신망 관리가 통합되며, 기존 통신망 기술들을 충분히 수용하고, 신규 서비스를 쉽게 적용할 수 있는 객체지향 통신 소프트웨어 구조로 구성하였다. TINA 기술은 DPE 상에서 객체 단위로서 통신망 관리객체와 서비스 관리객체를 공유하거나 접속할 수 있도록 그림 5와 같은 소프트웨어 계층적 구조로 모델화하였다.

효율적인 통신망 관리와 소프트웨어의 재사용으로 신속한 신규 서비스를 제공하며, 종래의 통신망 위주의 신호방식(signaling)에서 세션을 사용하여 개별 통신망 사용자를 위주로 진화 가능한 유연한 호 연결 모델을 지원하도록 하였다.

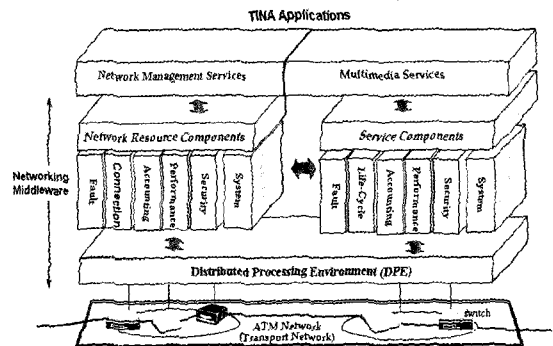


그림 5. TINA 구조

TINA 네트워크 자원은 통신 사업자 간의 영역 레벨, 통신망 영역레벨과 NE 레벨로 구성하여 각 레벨에 따른 객체로 객체 모델을 제시한다. 통신망 관리의 기능 중에는 FCAPS(Fault, Configuration, Accounting, Performance, Security)로 핵심 기술인 연결관리 분야의 기능이 세부적으로 객체 모델화가 추진되고 있으며, 연결관리 객체 모델링에 대한 정립과 기술 검증이 완료된 후, 관련 나머지 기능에 대한 기능 구조의 연구가 추진되고 있다. 서비스는 인터넷을 수용도록 시범 시연과 관련 프로젝트를 수행하고 있다. 그러나 TINA는 네트워크를 분산처리환경으로 구축하며, 서비스와 네트워크 자원을 객체로 표현하여 기존 통신망에 적용하기에는 위험성이 크다고 본다.

3.2 액티브 네트워크

액티브 네트워크는 '94년 미국 DARPA 연구회에서 시작되었다. 현재 네트워크 문제가 새로운

기술과 표준을 네트워크 시스템의 기반 구조에 적용하여 여러 프로토콜 계층에서 잉여 연산에 의존하는 성능과 신규 서비스를 기존 네트워크 구조에 적용하는 문제점을 지적하여 이에 대한 대안으로 제시되었다. 액티브 네트워크는 액티브 스위치 혹은 라우터를 통해 전달되는 메시지에 대해 사용자 연산 수행(customized computation)이 가능 하도록 하는 네트워크 구조에 대한 접근 방식이다. 이와 같은 구조는 JAVA의 이동코드 기술과 선도적인 사용자 응용 서비스로 가능하게 한다. 결국 다양한 서비스 제공을 위해 매번 네트워크 장치의 업그레이드와 잉여 성능을 NE의 인프라를 변환하여 소프트웨어적인 해결로 접근하는 방법으로서 구조적으로 네트워크에 손쉬운 접근으로 볼 수 있다.

액티브 네트워크 노드 기능은 그림 6과 같이 노드 운영체제, 수행 환경(EE, Execution Environments), 액티브 응용 서비스로 구성된다. 그림 2의 객체지향 프로토콜을 지원하는 노드 모델과 모바일 코드 수행을 위한 환경이 별도로 요구됨을 알 수 있다. 따라서 EE는 스마트 패킷 전달을 통해 프로그래밍 되거나 제어되는 프로그래밍 인터페이스 혹은 가상 머신을 정의한다. EE는 일종의 유닉스 시스템의 shell 프로그램처럼 동작하며, 종단 간에 네트워크 서비스에 따른 인터페이스를 제공한다. 이를 위해서 노드 운영체제는 다양한 액티브 라우터 자원의 채널과 정책, 데이터베이스 혹은 여러 자원을 사용할 수 있도록 지원한다.

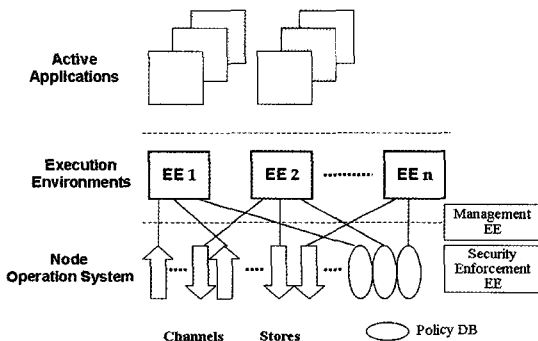


그림 6. 액티브 네트워크 노드의 구성요소

3.3 개방형 네트워크

개방형 네트워크 기술의 표준화는 The Parlay

Group를 중심으로 IEEE PIN(Programming Interface for Networks), MSF(Multi-service Switch Forum), ISC(International Softswitch Consortium)에서 개념 정립과 표준화 인터페이스에 대한 표준 연구를 수행하고 있다. 세계 유수의 통신 사업자 중심의 컨소시엄인 Parlay 표준화 기관은 새로운 방식의 개방형 네트워크 API 규격을 제정하고, 동시에 규격이 상용제품의 구현에 채택을 목표로 표준화 연구를 수행하고 있다. 새로운 네트워크나 신규 서비스 도입시 규격이 미치는 영향의 파급효과로 차세대 개방형 네트워크로 진일보를 하기위해 노력을 하고 있다. 국내에서도 Parlay 그룹의 규격을 수용한 BCN 그룹 결성으로 통신 사업자 간의 많은 발전과 다양한 서비스를 제공할 것으로 전망된다.

Parlay API 규격(그림 7)은 네트워크 사용자의 정보를 이용하여 동적인 서비스를 개발하고 유지보수를 가능하게 함으로서 API는 안정성과 특정 기술과 네트워크에 독립적이다. 세부 Parlay 그룹의 연구대상의 표준화 규격 항목은 표 1과 같다.

Parlay API는 서비스 인터페이스와 프레임워크 인터페이스를 제공한다. 서비스 인터페이스는 응용 서비스에 관련된 일련의 네트워크 기능과 정보 접근을 가능케 하는 접속 규격이다. 표 1의 generic call control service 등의 호 제어에 관련된 규격을 들 수 있다. 프레임워크 인터페이스는 서비스 인터페이스가 안전하고 견고하게 동작되도록 보조 기능의 인터페이스를 제공한다. 인증, 이벤트 공지(event notification)의 접속을 들 수 있다.

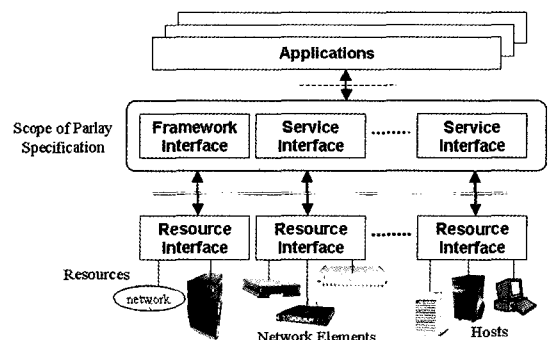


그림 7. The parlay Group의 API 기능 구조

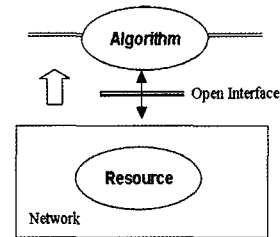
표 1. Parley/OSA API 규격 목록

SCF	Description
General	Contain the introduction and methodology used.
Common data	Generic data definition, used in other parts
Framework	defines the infrastructure capabilities like authentication. SCF discovery. SCF registration, fault management, etc.
Call Control	defines the call control family with capabilities ranging from setting up basic calls to manipulating multimedia conference calls
User Identification	SCF to obtain information from the end-user, play announcement, send short text messages, etc.
Mobility	SCF to obtain location and status information
Terminal Capability	SCF to obtain the capabilities of an end-user terminal
Data Session Control	SCF to influence data sessions
Generic Massaging	SCF for access to main boxes
Connectivity Management	SCF for provisioned QoS
Account Management	SCF to access end-user accounts
Charging	SCF to charge end-users for use of applications/data
Policy Management	These includes APIs to crease, update or view policy information
Presence & Availability Management	SCF to establish a standard for maintaining, retrieving and publishing information about digital identities, etc.

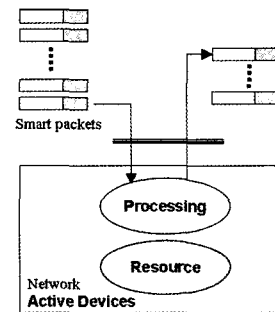
개방형 네트워크와 액티브 네트워크는 외부에서 제어 혹은 프로그램이 가능하게 함으로서 네트워크 운용에 유연성 제공에 목적이 있다. 제어 방법으로 표준 규격의 API를 제공하여 네트워크 자원을 추상화하여 API를 통해 외부에서 제어 관리되도록 한다.

개방형 네트워크는 그림 8-a와 같이 외부에서 분산 시스템 환경에서 네트워크가 제어되며, 액티브 네트워크는 네트워크 제어 및 관리가 스마트 패킷에 의해 NE에 로딩되어 처리 프로그램으로

노드에서 처리된다(그림 8-b). 액티브 네트워크와 개방형 네트워크 구조의 본질적인 목적은 같으나 실제 제어 관리하는 측면을 서로 상반된 알고리즘으로 전개되고 있다. 그러나 사용자와 통신망 및 사업자 관점에서 볼 때 어떤 구조가 적합한가 장기적으로 연구해야 한다.



(a) 개방형 네트워크



(b) 액티브 네트워크

그림 8. 액티브 네트워크와 개방형 네트워크 비교

IV. 정책 기반의 네트워크 관리

4.1. PBNM 통신 시스템

네트워크의 정보모델링 표준화 작업은 방대하다. 통신 사업자와 서비스 사업자, 벤더 간에 일치된 규격이 필요하다. 따라서 단기적으로 일치된 규격을 제시하며, 이를 적용하기엔 어렵다. 이러한 추세에 따라 단기간에 보다 네트워크를 효과적으로 관리하고 제어하기 위한 연구가 IETF와 DMTF 표준화기관에서 정책 기반으로 네트워크를 관리(PBNM)하고 운영하도록 정책을 객체화하며, 이를 통신 사업자와 정보공유를 위한 표준화 연구가 수행되고 있다[11].

정책 기반의 통신망 관리는 통신망에서 제공하는 QoS, 정보보호 및 네트워크 자원을 공통된 형태로 공유하도록 환경을 제공하며, 이를 효율적으로 관리하는 데 있다. 정책 기반의 네트워크 관리는 NE의 MIB, PIB(Policy Information Base)을 SNMP, COPS(Common Open Policy Service protocol), LDAP, HTTP 등의 프로토콜을 사용하여 네트워크 관리정보를 공유하여 정책을 관장하는 시스템에 설정된 정책규칙에 따라 운영된다. 정책관리 시스템은 동적으로 NE부터 수집된 정보를 분석하여 관리자가 설정하는 정책(혹은 정책 규칙)에 따라 수행하도록 명령을 내리면 된다.

PBNM 시스템은 정책규칙을 제정하고, 정책에 따라 통신망을 운영하기 위해서 NE를 실시간으로 모니터링하며, 동적으로 변화되는 정보에 대해 신속하게 설정된 정책에 따라 수행하는 환경을 제공한다. 또한 설정된 정책은 일관성 있게 정보를 공유하여 실시간으로 NE에게 전달되어야 한다.

IETF 표준화 기관은 정책 기반의 네트워크 관리 기능의 표준 규격 작성을 위해 그림 9와 같이 PMT(Policy Management Tools), PR (Policy Repository), PDP(Policy Decision Point), PEP 컴포넌트로 분류하였다. 정책 기반의 네트워크 관리를 위해 정책에 대한 기본모델 규격인 PCIM(Policy Core Information Model, RFC 3060)과 기본모델 규격을 확장한 PCIME(PCIM-Extension, RFC 3460)를 비롯하여 QoS와 IPsec(IP Security)에 적용을 위해 표준 규격을 작성하였으며, 이를 정보보호 네트워크에 적용을 위해 2003년부터 Opsec WG에서 표준화 연구를 수행하고 있다.

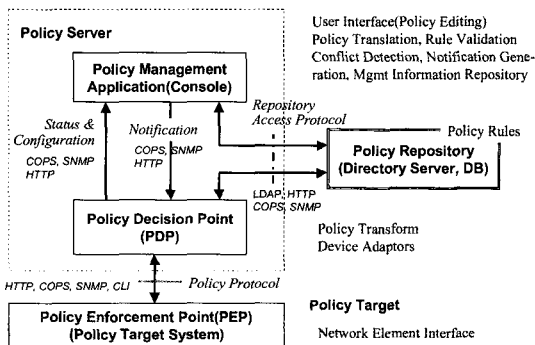


그림 9. PBNM 시스템 컴포넌트

4.2. 정책모델링

네트워크 정책에 대한 정보모델링을 위해 우선 정책을 적용한 서비스 범위를 설정해야 하며, 이를 기반으로 다양한 NE에 운용되도록 기본적인 서비스 정책 범주와 적용 디바이스에 따른 모델이 요구된다. 그림 10은 네트워크 보안정책에 대한 정보모델링 개념도를 보였다. 네트워크를 운영하는 통신사업자 관점에서 비즈니스 모델이 정립되며, 정보보호 서비스 범주, 이를 적용할 NE, 접속 및 확인 인증, 보안키 관리 등에 대한 범위를 설정한 후에 네트워크 정보보호 정책모델을 정립해야 하며, PEP에 적용하기 위해 다양한 NE에 따른 단계적 정보모델링이 요구된다.

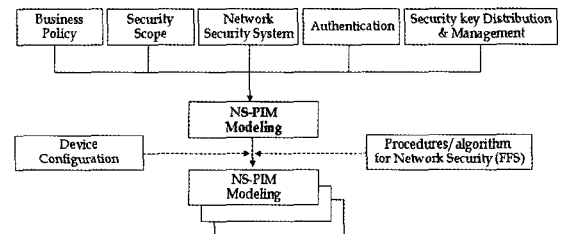


그림 10. 네트워크 보안정책 정보모델링 개념

4.3. 정책 정보모델

4.3.1. 네트워크 보안정책 모델

QoS와 정보보호 서비스 중에 네트워크 정보보호에 관련된 정책에 대한 보안정책 객체를 DMTF CIM(Common Information Model ver 2.8)과 IETF PCIME를 근거하여, 라우터, 방화벽, IP 스위치, IDS(Intrusion Detection System)에 적용 가능하도록 네트워크 보안정책 객체를 모델링을 한다. 이는 결국 액티브 네트워크의 액티브 라우터에도 적용이 가능하며, 스마트 패킷을 액티브 라우터에 정책 적용과 처리를 위해 먼저 네트워크 정보보안을 위한 정책을 모델링한다. 추후 연구로 액티브 네트워크 관리를 위한 보안정책 모델로 확장하도록 한다.

보안정책이 보안 라우터를 비롯한 NE에 적용하는 기능을 구분하기 위해 NE에서 적용 보안 기능과 이에 따른 대책을 수립하여 정책규칙과

수행 가능한 원칙을 표 2와 같이 기능을 그룹핑한 후에 네트워크 보안정책을 정보모델링 한다.

표 2. 네트워크 보안정책에 따른 condition과 action

Function	Condition(factors)	Action
Alert Control Policy	source IP, destination IP, source port, destination port, protocol, attack ID, time interval	- suppress - aggregation - ignore
Attack Control Policy	Snot 2.0-based signature	- alert - drop - terminate
Access Control Policy	source IP, destination IP, source port, destination port, protocol, TCP 6 bits Flag, ICMP type, ICMP code, MAC address	- permit - deny - track
Traffic Control Policy	source IP, destination IP, source port, destination port, protocol, average rate, normal bucket, extended bucket	- export - intercept - rate limited control
Authenticate Control Policy	source IP, destination IP, source port, destination port, key, ID, password	- pass - fail & save

정책 기반의 보안정책 객체는 PolicySet을 근간으로 PolicyRule, PolicyGroup, Policy- Condition, PolicyAction로 구성된다. 그러나 NE를 단순히 관리자가 정책규칙에 의한 관리보다는 정보보호를 위해서는 통신망에서 운용되는 패킷과 정책규칙을 논리적으로 표현하는 객체로 인식해야 함에 따라 PolicyVariable, Policy- Value, Collection과 기존의 정책규칙 재사용하기 위한 PolicySet를 추가하여 Policy 객체와 의존성(dependency)을 가지도록 하였다.

PolicyCondition은 PolicyTimePeriodCondition 등의 PCIM과 PCIME 클래스를 상속 받으며, 표 2의 보안시스템 기능에 따른 조건을 충족시키는 객체와 벤더에서 독자적으로 정의한 Vendor-PolicyCondition 객체로 의존성을 가진다. Policy Repository는 PolicyCondition과 PolicyAction 객체와 Policy에 연관된 객체를 정책 서버에 객체 정보로 저장한다.

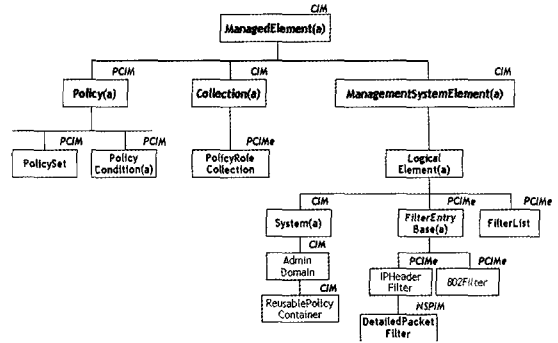
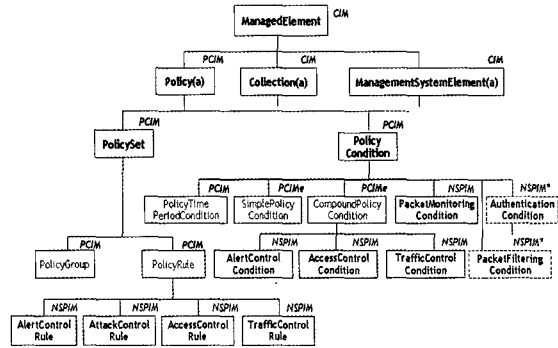
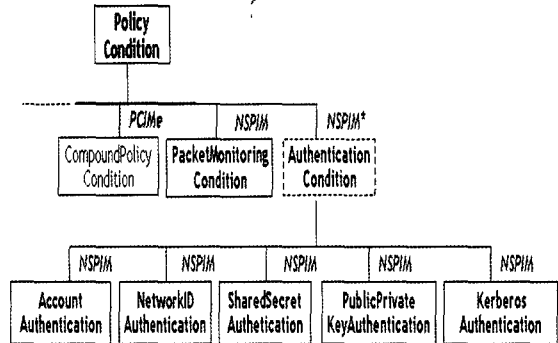


그림 11. 보안정책 정보모델의 기본 클래스



(a) PolicySet 정보모델



(b) PolicyCondition정보모델

그림 12. 보안정책의 PolicySet과 PolicyCondition 정보모델

보안정책은 운영자에 의해서 간단한 정책규칙을 비롯하여 정책규칙 속에서 아래와 같이 다른 정책규칙을 사용과 필터 기능에 따라 PolicyVariable를 다양하게 모델화 되어야 한다. 또한 보안정책 규칙은 PCIM과 PCIME의 Policy-

Rule 클래스를 근거로 설정된다. 네트워크 보안정책은 condition과 action으로 구조화된 형태로 정책규칙이 구성된다. 보안 정책규칙은 아래의 예제와 같이 복합적으로 논리화하여 규칙을 생성하는 경우에 이를 지원하도록 네트워크 보안정책 객체를 정보를 모델링해야 한다.

▷정책 예:

라우터에서 211.227.100.0 네트워크의 호스트는 접근 금지, 그러나 별도의 IP 주소인 211.227.100.23은 네트워크 A는 접속 가능하며, 211.227.100.2는 VPN으로 네트워크 B와 연결

▷정책 표현 예:

```
"if <IP == 211.227.100.23> then <host:: access to network A>"
"else if <IP == 211.227.100.2> then <VPN connection>"
"else if <network == 211.227.100.0> then <host:: not access to network A>"
```

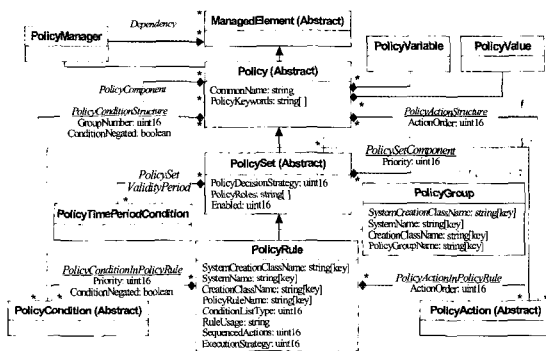


그림 13. 보안정책 PolicySet 정보모델

PolicyRule은 표 2에서 정의된 보안 시스템에 적용된 기능을 기반으로 AlertControlRule, AttackControlRule, AccessControlRule, TrafficControlRule을 구성하며, PolicyCondition에 CompoundPolicyCondition에 AlertControlCondition, AttackControlCondition, AccessControlCondition, TrafficControlCondition을 구성하여 보안 시스템의 주요 기능을 담당한다. 또한 PacketMonitoringCon-

dition, PacketFilteringCondition을 두어 각각의 패킷에 다른 조건을 부여하였으며, Authentication 클래스를 정의하여 보안 시스템의 접속 및 정책규칙 액세스에 따른 인증을 하도록 하였다.

PolicyAction에 보안 시스템의 주요 기능인 AlertControlAction, AttackControlAction, AccessControlAction, TrafficControlAction을 정립하고, NetworkPacketAction와 RejectConnectionAction을 정의 하였다. 표 2의 주요 기능에서 본 바와 같이 조건에 따른 동작(action)을 AlertControlAction은 AlertSupressAction, AlertIgnoreAction, AlertAggregationAction 등으로 그림 14와 같이 정의하였다.

본 논문에서는 보안정책 정보모델은 IETF PCIM/E를 근거로 작성하였으며, 객체 접속에 따른 인증을 위해 Authentication을 5개 객체로 정립하였으며, PolicyAction에 PCIME 객체의 NetworkPacketAction, RejectConnectionAction을 추가하여 연결 및 접속에 따른 제어를 하였다.

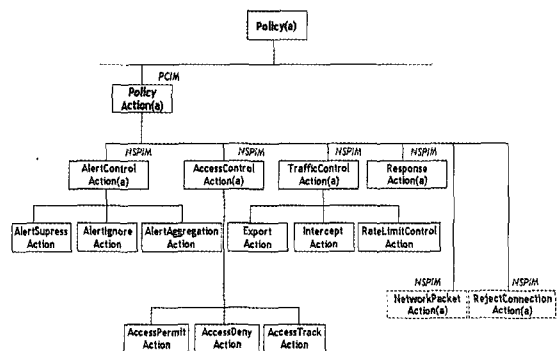


그림 14. 네트워크 보안정책의 PolicyAction 정보모델

4.3.2. 정보모델링 예제

네트워크 보안정책 클래스의 PolicyCondition 중에 트래픽 제어를 담당하는 TrafficControlCondition 객체를 정보 모델링하는 간단한 예를 다음과 같이 보였다.

TrafficControlCondition은 트래픽 폭주를 판단하는 조건으로써, 발신지(source) IP, 목적지 IP, 발신지 포트, 목적지 포트, 프로토콜에 대한 비교

를 각각 SimplePolicyCondition의 인스턴스(instance)로 생성하고, 이들을 묶어서 Traffic-Control-Condition으로 구성한다. 일정 시간 동안의 트래픽 용량에 대한 평균 비율, 정규 용량, 초과 용량과 특정 서비스의 요구 및 반복을 조건 수립에 가능한 속성을 갖는다.

1) TrafficControlCondition 클래스
 NAME TrafficControlCondition
 DERIVED FROM CompoundPolicyCondition
 ABSTRACT False
 PROPERTIES AverageRate, NormalBucket, ExtendedBucket(ServiceTurn), (IterationNumber)

2) Property AverageRate
 NAME AverageRate
 SYNTAX uint16
 DEFAULT VALUE 0

4.4. 보안정책 관리기술

DMTF CIM 모델링은 MOF(Microsoft Object Formatter)를 사용하여 보안정책을 모델링 하였다 [12]. 그러나 MOF 방식은 클래스 정의를 일관적으로 정의함으로써 표준화 규격 작성이 유리하나 실제 개발자에게 클래스 간의 오퍼레이션 표현에 다소 불편한 점이 있는 바, 보안정책 객체는 UML 도구(ROSE tool)를 사용하며, 클래스 다이어그램과 협력/시퀀스 다이어그램을 기반으로 설계된다. CIM 정보모델링에 사용한 MOF 방식을 일부 보안정책 클래스 정의에 적용한 바, ManagedElement 객체 컴포넌트 수용과 객체 간의 상속성 유지와 정의된 클래스에 따른 syntax, 클래스 계위 및 instantiate 등의 편리성을 제공한다. 그러나 네트워크 보안정책 객체를 텍스트 형식으로 표현을 IETF의 표준규격의 기술 방식에 의존하였다. 객체 속성과 오퍼레이션, 상호연관 등의 클래스 정의는 UML 도구로 설계하여 확인할 수 있다.

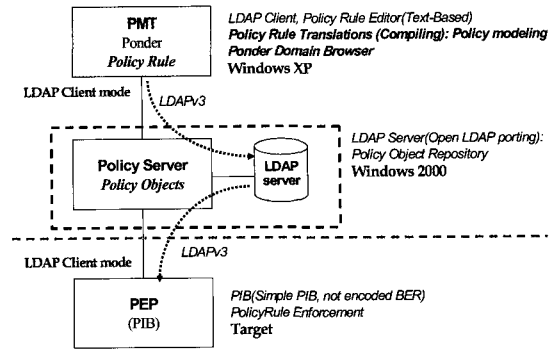


그림 15. 보안정책 정보모델 적용 환경

V. 결 론

본 논문은 개방형 네트워크에서 신규 서비스 제공을 위한 방향과 표준화 과정을 기술하였다. 객체지향 설계기술의 출현으로 소프트웨어 기술과 인터넷 통신기술이 결합하여 분산처리환경이 구축된 후, 네트워크와 서비스를 대상으로 객체 모델링을 적용한 네트워크 인프라 연구가 TINA와 개방형 네트워크 그룹에서 시도되었다. 그러나 대규모 네트워크에 분산시스템 환경을 적용하기가 어려운 바, 액티브 네트워크 패러다임으로 라우터 및 스위치가 SCF 기능으로 확장하여 통신 서비스를 제공하는 연구가 활발히 진행되며, 최근 이를 지능망에도 도입하고 있다[20]. 액티브 네트워크를 전세계 네트워크에 적용하기는 무리다. 우선 실질적으로 노드 제어와 관리가 전제되어야 한다. 이를 위해 정책 기반의 NE를 제어 관리하는 구조와 표준화 기관의 연구를 살펴보았다.

인터넷 상에서 네트워크 관리정보를 보다 효율적인 관리를 위해 정책 기반의 정보보호 관리 시스템이 필요하다. 이를 위해 DMTF와 IETF에서 제안하는 객체 모델링 방식을 도입하여, 보안정책의 기능 정립과 보안정책 객체를 정보모델링 하였다. 보안정책 객체는 PolicySet를 비롯하여 표 2에서 정의된 기능을 기반으로 5개의 PolicyCondition, PolicyAction, PolicyVariable, PolicyValue 객체로 구분하였으며, ManagedElement는 DMTF CIM 컴포넌트를 상속하였다.

앞으로 다양한 NE에 보안정책 정보모델에 대

한 적용과 정보보호를 위한 적극적인 보안정책
 객체 발굴이 요구된다. 또한 액티브 네트워크에
 적용을 위한 기본 모델을 정립하고 이를 수용하
 는 방향을 제시하고, 이를 위한 국내외 표준화 규
 격 연구가 요구된다. 또한 개방형 네트워크와 액
 티브 네트워크, 정책 기반의 통신망관리 기술의
 진화 발전에 따른 연계와 연동기술의 연구가 필
 요하다.

참고문헌

- [1] Stefan Boecking, "Object-Oriented Network Protocol", Addison-Wesley, 2000.
- [2] ITU-T, M.3100 Recommendation, "Generic Network Information Model", Oct 1992.
- [3] ITU-T, I.321 Recommendation, "B-ISDN Protocol Reference Model and its Application", 1998.
- [4] Hiroshi Yasuda, "Active Networks", proceeding of IWAN 2000, Springer, 2000.
- [5] Stephen F. Busg and Amit B. Kulkarni, "Active Networks and Active Network Management: A Proactive Management Framework", Kluwer Academic/Plenum Publishers, 2001.
- [6] Morris Sloman, et al. "Using CIM to Realize Policy validation within the Ponder Framework", GMC-2003, July 2003.
- [7] Emil Lupu, et al. "Security and Management Policy Specification", IEEE Network, Vol 16, No 2, March 2002.
- [8] B. Moore, et al., "Policy Core Information Model-Version 1 Specification", RFC 3060, IETF, Feb. 2003.
- [9] B. Moore, et al., , "Policy Core Information Model Extension", IETF, RFC 3460, Jan. 2004.
- [10] Nicodemos Damianou, et al., "Ponder: A Language for Specifying Security and Management Policies for Distributed Systems", Version 2.3, Imperial College Report Document, Oct. 2000.
- [11] Andrea Westerinen and Winston Bumpus, "The Continuing Evolution of Distributed Systems Management", IEICE Trans. INF & SYST, Vol. E86-D, No. 11, Nov. 2003.
- [12] DMTF Document, "CIM Core Policy Model", Version 2.9, DMTF, Aug. 2004.
- [13] Thomas M Chen, "Evolution to the Programming Internet", IEEE Comm. Mag, March, 2000.
- [14] Macus Brunner and Rolf Stadler, "Service Management in Multiparty Active Networks", IEEE Comm. Mag., March, 2000.
- [15] Fawzi Daoud, "Integrated Open Service Mode for Active Networks and Services", IEEE Comm. Mag., Sep 1999.
- [16] Takeo Hamada et al., "Service Quality in TINA: QoS Trading in Open Network Architecture", IEEE Comm. Mag., August 1998.
- [17] 김도수, 신영석, 김진오, "정책 기반의 보안 게이트를 위한 보안정책 정보모델링", 한국정보처리학회 추계학술대회, 2003.11.
- [18] 손승원, "Active Security 기술 발전 방향", Sigcomm Review, 한국정보처리학회, Vol. 1, No. 1, 2000.12.
- [19] 김현주, 장범환, 정태명, "Active 네트워크의 관리 기술 현황과 전망", Sigcomm Review, 한국정보처리학회, Vol. 1, No. 1, 2000.12.
- [20] 오행석, 남택용, "액티브 네트워크를 활용한 능동 지능형 서비스", ETRI 전자통신동향분석, 제9권 제6호, 2004. 12.
- [21] 김영호, 김지연, 조희남, "시스템 관리 표준 정보모델(CIM) 분석", ETRI 전자통신동향분석, 제9권 제6호, 2004.12.
- [22] 나중찬, 김진오, 손선경, 장종수, "정보통신 인프라 정보보호 제어 프레임워크 연구", 한국통신학회지, 제21권 제9호, 2004.9.
- [23] 손선경, 신영석, "LDAP을 이용한 정책 정보모델링 및 공유관리", 한국인터넷정보학회지, 제5권 제4호,

2004.12.

- [24] 이호경, 이영무, 홍경표, "새로운 통신 서비스 플랫폼을 위한 차세대 통신망", <http://iita6.iita.re.kr:8888/korean/journal>, 2004.
- [25] The Parlay group, "Policy Management SCF", ETSI ES 202 915-13 Ver 1.1.1, Jan 2004.
- [26] Open LDAP Foundation, "open LDAP 2.1 Administrator's Guide", Jan 2003.
- [27] Ponder, <http://www-dse.doc.ic.ac.uk/Research/policies/ponder.shtml>, 2003.
- [28] DMTF, <http://www.dmtf.org>, 2004.
- [29] IETF, <http://www.ietf.org>, 2004.
- [30] Cisco, <http://www.cisco.com/en/US/products/sw/secursw/ps2133/>, 2004.
- [31] Orchestream, <http://www.orchestream.com>, 2003.
- [32] TINA consortium, <http://www.tinac.org>, 2004.
- [33] The parlay Group, <http://www.parlay.org>, 2004.

저자소개



신영석

1982년 전북대학교 전자공학과(공학사)
 1984년 전북대학교 대학원 전자공학과(공학석사)
 1993년 전북대학교 대학원 전자공학과(공학박사)
 1984년~1998년 2월 : ETRI 선임연구원
 1993년~1994년 8월 : 일본 NTT 통신망 연구소 객원연구원
 1998년 3월~현재 : 호남대학교 정보통신공학과 부교수
 ※관심분야 : 초고속 프로토콜, 객체지향 모델링, 통신망관리, BcN 등