SNMPv3 통신망의 정책기반 보안관리를 위한 역할기반 보안관리 모델의 설계 및 분석

주 광 로[†] · 이 형 효[††] · 노 봉 남[†††]

요 약

정책기반 통신망관리 시스템은 다양한 사용자의 요구에 부응하고 대형화, 분산화되는 통신망의 효과적인 관리에 적합한 아키텍처이다. 이 시스템에서의 통신망 관리자는 각 통신망 구성요소에 대한 직접적인 동작설정 대신 미리 설정한 규칙에 따라 통신망 구성요소나 서비스의 동작을 결정하게 된다. 한편, 융통성있는 통신망 관리 프레임워크를 제시한 SNMPv3는 인증, 암호화, 접근통제 등의 보안서비스를 제공함으로써, 이전 SNMP 버전들이 제공하지 못했던 안전한 통신망 관리를 위한 기반기술을 제공하고 있다. 그러나, SNMPv3의 개선된 보안서비스에도 불구하고 통신망 관리자별로 인증과 암호화 과정에 이용되는 보안정보가 관리되고, 보안정보가 통신망 구성요소에 분산되어 있어 중앙집중방식의 체계적인 보안관리기능이 제공되지 않아 여러 관리자에 의해 운영되는 대규모 통신망을 효과적으로 관리하는데 부적합한 문제점을 가지고 있다. 본 논문에서는 중앙집중방식의 규모확장성과 통신망 보안관리기능을 제공하기 위해 보안관리정책을 지원하는 역할기반 보안관리 모델을 제시하고, 이를 추가한 SNMPv3의 확장된 보안시스템의 구조, 동작절차 및 보안관리 관점에서의 효율성 분석에 대해 기술한다.

Design and Analysis of Role-based Security Management Model for Policy-based Security Management in SNMPv3 Network

Gwang Ro Joo[†] · Hyung Hyo Lee[††] · Bong Nam Noh[†††]

ABSTRACT

Policy-Based Network Management (PBNM) architecture is to meet various needs of network users and to provide effective management facilities in distributed and large scale networks to network managers. In PBNM, network managers perform network management operations by stipulating a set of rules rather than control each network component. On the other hand, providing security services such as authentication, privacy of messages as well as a new flexible and extensible administration framework, SNMPv3 enables network managers to monitor and control the operation of network components more secure way than ever before. Despite of its enhanced security services, SNMPv3 has difficulties in managing distributed, large-scaled network because it does not provide centralized security management facilities. In this paper, we propose a new security model called Role-based Security Management model (RSM) with security management policy to support scalable and centralized security management for SNMP-based networks. Also, the structure and the operation of the security system as well as the efficiency analysis of RSM in terms of security management are also described.

키워드 : 통신망 보안관리(Security Management), 정책기반 통신망 관리(Policy-based Network Management) 보안관리정책(Security Management Policy), SNMPv3, 사용자기반 보안모델(User-based Security Management) 뷰기반 접근통제 모델(View-based Access Control Model), 역할기반 접근통제(Role-based Access Control) 역할기반 보안관리 모델(Role-based Security Management Model)

1. 서 론

통신망에 접속되는 구성요소의 수와 종류가 증가함에 따라 통신망 관리자에 의한 각 구성요소별 관리와 설정 작업이 점점 어려워지게 되었고, 이러한 문제를 해결하기 위해 제시된 방안이 정책기반 통신망 관리(PBNM : Policy-Based Network Management)이다[13, 17, 19]. 정책기반 통신망 관리는 사용자, 응용, 통신장비 등의 통신망 구성요소들이 준수해야 하는 상위수준의 규칙을 기술하고 실행함으로써 일관되고 안정된 통신망 운용과 관리를 목표로 한다[28]. 현재 정책기반 통신망관리 프레임워크 설계와 구현에 대한 다양한 연구가 진행중이며 대표적인 연구결과로는 IETF 워킹그룹의 문서들이 있다[3-6].

한편, 1999년 제정된 SNMPv3(Simple Network Mana-

※ 본 논문은 1999년도 전남대학교 학술연구비 지원에 의해 연구되었음.
† 종신회원 : 서강정보대학 컴퓨터정보과 교수
†† 정 회 원 : 원광대학교 정보·전자상거래 학부 교수
††† 종신회원 : 전남대학교 컴퓨터정보학부 교수
논문접수 : 2001년 7월 30일, 심사완료 : 2001년 9월 24일

gement Protocol) 표준안에서는 SNMP 구성요소들과 구성요소간의 관계, 표준화 문서들을 체계화함으로써 SNMPv1, SNMPv2에 대한 단순한 기능개선을 뛰어넘어 새로운 프레임워크를 제시하였다[22-24]. 또한 SNMPv2의 취약점이었던 보안기능을 개선하여 보안성이 취약한 인터넷 환경에서도 안전한 통신망 관리기능을 수행할 수 있게 되었다. 예를 들어, 관리정보베이스(MIB : Management Information Base)에 저장된 통신망 정보에 대한 뷰(view) 단위의 접근통제, 프로토콜 데이터에 대한 인증과 무결성 확인, 그리고 암호화 기능을 추가함으로써 매우 안전한 통신망 관리환경을 제공하고 있다[32, 33].

그러나, SNMPv3 보안기능은 통신망 관리자별로 인증과 암호화 과정에 이용되는 보안정보가 따로 관리되고, 보안정보가 통신망 구성요소에 분산되어 있어 중앙집중방식의 체계적인 보안관리기능이 제공되지 않아 여러 관리자에 의해 운영되는 대규모 통신망을 효과적으로 관리하는데 부적합한 문제점을 가지고 있다[15]. 따라서, 통신망 보안관리 분야에도 규모확장성(scalability)이 있고 하나의 관리시스템에서 통신망 보안정보를 통제할 수 있는 정책기반 관리가 필요하게 되었다. 통신망 관리시스템에 의해 수행되는 관리기능 중 보안관리는 다양한 보안위협으로부터 통신망과 통신망 관리시스템을 보호하기 위해 보안관련 정보의 안전한 관리, 주요 정보 및 자원에 대한 접근통제(access control), 그리고 암호/인증 알고리즘 지정과 키분배 및 관리, 보안감사기록의 저장 및 분석, 보안침해 보고기능 등의 포괄적 기능을 수행한다[11, 29].

본 논문에서는 보안관리 측면에서 현재 SNMPv3의 문제점과 원인을 분석하고, 이를 해결하기 위해 방안으로서 역할기반 접근통제 모델을 이용한 역할기반 보안관리 모델(RSM : Role-based Security management Model)을 제시한다. 또한 제시된 모델이 추가된 SNMPv3 보안시스템의 구조와 기능에 대해서도 기술한다. 제안된 RSM은 역할기반 접근통제 모델의 보안특성인 규모확장성 지원기능과 보안정보의 집중관리특성을 SNMPv3 프레임워크를 이용한 통신망 보안관리영역에 적용함으로써, 국제표준의 통신망 관리 프레임워크인 SNMPv3의 유용성과 활용도를 높일 수 있을 것이다.

본 논문의 구성은 다음과 같다. 2장에서는 정책기반 시스템, 정책기반 통신망 관리와 표준화 동향에 대해 기술하고 3장에서는 국제 표준의 통신망 관리 프레임워크인 SNMPv3의 보안서비스 특성 함께 보안관리 관점에서의 문제점을 분석한다. 4장에서는 SNMPv3 보안관리 문제점을 보완하기 위해 역할기반 보안관리 모델이 추가된 보안시스템의 구조, 기능 및 구현에 대해 기술하고, 마지막으로 결론과 향후 연구방향을 제시한다.

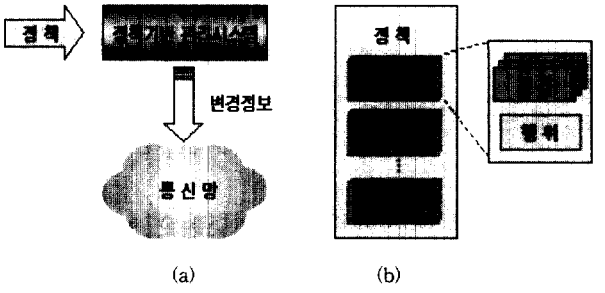
2. 정책기반 통신망 관리

2.1 목 적

정책기반 통신망 관리의 목적은 멀티미디어를 포함한 새로운 응용들에 대한 지원, 안정된 응용 실행환경 제공에 대한 통신망 관리자들의 요구사항들을 해결하기 위한 방안으로 제시되었으며[1,28], 통신망 관리자들의 요구를 해결하기 위한 통신망 대역폭의 단순한 확장보다 네트워크 구성요소의 자원을 효율적으로 관리함으로써 통신망을 효과적으로 관리하는데 있다. 정책기반 통신망 관리의 기본 구조는 (그림 1)의 (a)와 같다.

통신망 관리자가 통신망 구성요소나 서비스 동작을 통제하는 고수준의 정책을 생성하면 정책기반 관리시스템은 주어진 정책을 통신망 구성요소에 의해 집행할 수 있는 구체적인 변경정보로 변환하여 해당 통신망 구성요소들에게 전송하게 된다.

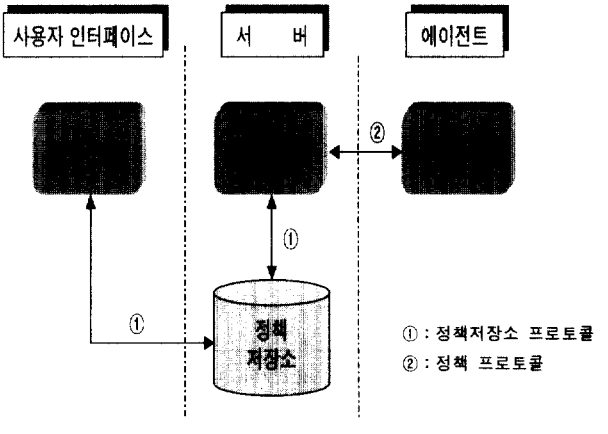
정책(policy)은 하나 이상의 규칙(rule)으로 구성되며, 각 규칙은 하나 이상의 조건(condition)과 그 조건이 만족된 경우 수행되는 행위(action)로 이루어진다(그림 1)의 (b).



(그림 1) 정책기반 통신망 관리구조와 정책 구성요소

2.2 정책기반 시스템 아키텍처

IETF(Internet Engineering Task Force) 워킹그룹에 의해 정의된 정책기반 시스템의 일반적인 아키텍처는 (그림 2)와 같고[3-7], 각 구성요소의 기능은 다음과 같다.



(그림 2) 정책기반 시스템 아키텍처

- 정책 콘솔(policy console) : 정책의 생성, 배포, 그리고 정책의 집행상황을 점검할 수 있는 사용자 인터페이스
- 정책 결정점(PDP : Policy Decision Point) : 관리대상 요소(통신망 구성요소나 서비스)의 상태와 관리정책에 따라 관리기능을 결정하는 프로세스
- 정책 집행점(PEP : Policy Enforcement Point) : PDP에 의해 결정된 관리기능을 실행하는 관리대상요소내의 프로세스
- 정책 저장소(policy repository) : 정책이나 관련 정보를 저장하는 디렉토리 또는 데이터베이스
- 정책통신 프로토콜(policy communication protocol) : 정책 저장소에 저장된 정책의 판독/기록을 위한 정책 저장소 프로토콜(예 : LDAP)과 PDP와 PEP간 정책 프로토콜(예 : COPS)

2.3 표준화 동향

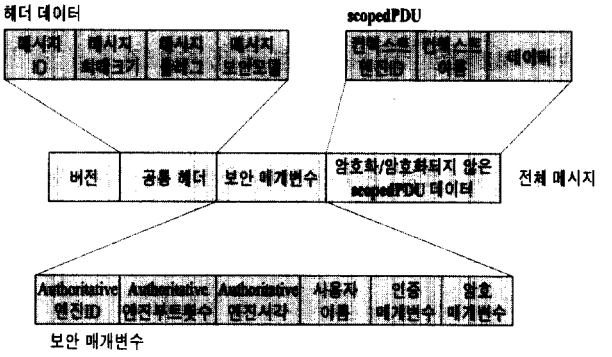
정책기반 시스템을 통신망 관리에 적용하기 위한 노력들이 IETF 워킹그룹에 의해 진행되고 있으며, 주요 연구내용은 다음과 같다. [6]은 DMTF(Distributed Management Task Force) 공통 정보모델(CIM : Common Information Model)의 일부로서 정책을 객체지향 정보모델로 기술하고 있고, [5]에서는 IP 네트워크에서 정책기반 관리시스템의 기본 요구사항과 프레임워크를 정의하고 있다. 한편, [3]은 정책정보를 LDAPv3(Lightweight Directory Access Protocol)를 접근 프로토콜로 사용하는 디렉토리로 매핑하는 방법을 정의하고 있고, [4]는 PDP와 PEP간 정책정보 교환의 새로운 프로토콜인 COPS(Common Open Policy Service)에 대해 기술하고 있다.

현재 정책기반 통신망 관리시스템은 여러 통신망 관리제품에서 채택되어 구현되어 있다. 정책기반 통신망 관리기법은 통신망 구성관리(Configuration Management), QoS(Quality of Service), 보안관리 등에 활용되고 있으며, 현재 Cisco사의 QoS Policy Manager(QPM), 3Com사의 Transcend Policy Service, HP사와 Intel사의 Intel PBNM, Nortel 사의 Optivity Policy Services(OPS), Cabletron사의 QoS Policy Manager 등의 제품이 개발된 상태이다[2].

3. SNMPv3의 보안서비스 특징 및 문제점

3.1 SNMPv3 보안관리 특징

SNMPv3 개발의 주요 목적중의 하나는 SNMP를 이용한 통신망 관리의 보안기능을 향상시키는 것으로, 강화된 메시지 출처 인증(message origin authentication), 메시지의 암호화, 메시지 스트림 변경방지, MIB에 대한 세분화된 접근통제 기능들이 추가되었다. SNMPv3 보안서비스는 비인가된 통신망 관리자에 의한 데이터의 변경(무결성 침해), 도청(비밀성 침해), 재사용 공격에 대응하는 기능을 제공하는 사용자기반 보안모델(USM : User-based Security Model)과 인가된 통신망 관리자의 MIB 접근을 통제기능을 제공하는 뷰기반 접근통제 모델(VACM : View-based Access Control Model)에 의해 제공된다. SNMPv3 메시지는 보안서비스 등의 매개변수 전송을 위해 재설계되었으며, 그 구조는 (그림 3)과 같다.



(그림 3) SNMPv3 메시지 구조

SNMPv3에서 제공되는 보안서비스의 특징을 정리하면 다음과 같다.

(1) 인증-암호화-접근통제를 이용한 다양한 강도의 보안서비스 제공

통신망 관리자가 관리대상 시스템에게 보내는 관리 메시지의 보안 강도에 따라 프로토콜 데이터의 인증과 암호화 여부를 선택할 수 있으며, 인증된 통신망 관리자에 대해서도 접근방법('READ', 'WRITE', 'NOTIFY')별로 접근이 허용된 관리정보를 지정하는 접근통제기능을 제공한다. 따라서, 통신망 관리자는 관리목적이나 관리정보의 중요도에 따라 다양한 강도의 보안서비스를 사용할 수 있게 되었다.

(2) 사용자기반 보안모델(USM : User-based Security Model)

사용자기반 보안모델에서는 메시지 출처 인증, 메시지 암호화, 메시지 스트림 변경방지 기능을 위한 보안서비스를 제공한다. 메시지 출처 인증을 위해 HMAC-MD5-96이나 HMAC-SHA-96 알고리즘이 사용되며, 메시지 암호화에는 CBC-DES 암호 알고리즘이 이용된다[5, 25]. 메시지 스트림 변경방지 기능을 제공하는 적시성(timeliness) 모듈은 SNMP 엔진ID(snmpEngineID), 부트횟수(snmpEngineBoots), 엔진시각(snmpEngineTime) 값을 이용한다.

(3) 뷰기반 접근통제 모델(VACM : View-based Access Control Model)

뷰기반 접근통제 모델은 통신망 관리자 이름과 보안모델로 구성되는 그룹, 보안 레벨(noAuthNoPriv, authNoPriv, authPriv), 컨텍스트, MIB 뷰, 뷰 모드(read/write/notify)를 입

력으로 통신망 관리자가 접근하려는 관리정보에 대한 접근 통제 기능을 수행한다[26]. 특히, 특정 MIB 서브트리에 매스킹 기법을 적용한 뷰트리 패밀리 개념을 도입하여 통신망 관리자별로 매우 세분화된 접근통제 기능을 제공한다.

3.2 SNMPv3 보안관리 문제점

통신망 관리시스템은 통신망 관리자 인증, 통신망 관리메시지 암호화 및 인증 등의 기본적인 보안서비스 제공뿐만 아니라 보안관련 정보의 안전한 관리, 주요 정보 및 자원에 대한 접근통제(access control), 그리고 암호/인증 알고리즘 지정과 키분배 및 관리, 보안감사기록의 저장 및 분석, 보안침해 보고기능 등의 포괄적 기능을 수행해야 한다[11, 29]. 이러한 보안관리 측면에서 볼 때, SNMPv3는 향상된 보안서비스 제공에도 불구하고 다음과 같은 문제점을 가지고 있다.

3.2.1 인증 및 암호화를 위한 통신망 관리자별 암호절 관리

SNMPv3 사용자기반 보안모델은 인증과 데이터 암호화 과정에 관리시스템과 관리대상시스템이 공유하는 인증용 암호절(pass-phrase), 그리고 그 암호절로부터 각각 생성된 인증키과 암호키를 사용한다. 이를 위하여, 통신망 관리시스템의 초기화 단계에서 모든 관리시스템과 관리대상시스템에는 동일한 암호절을 설정하는 과정이 필요하며, 통신망 관리 수행 중에 발생할 수 있는 인증키 또는 암호키의 변경은 이미 설정된 인증키와 암호키를 이용하여 새로운 값으로 'SET' SNMP 연산을 통해 이루어진다. 그러나, 초기화 과정시 암호절의 설정은 현재의 SNMPv3 표준안에 정의되지 않기 때문에 암호절의 관리방법이나 설정방법은 사용자기반 보안모델을 구현하는 시스템마다 달라지는 문제점이 있다. 이 문제점은 관리시스템과 관리대상시스템의 사용되는 인증키, 암호키의 대칭성으로 발생된 것으로, 비대칭형 인증, 암호 알고리즘을 채택함으로써 해결할 수 있으나, 본 논문에서는 이 문제에 대해서 다루지 않는다.

3.2.2 통신망 보안관리정보의 분산관리

사용자기반 보안모델에서 사용되는 인증과 암호 알고리즘이 HMAC이나 CBC-DES와 같은 대칭키 기반의 알고리즘인 이유로 통신망 관리자들의 보안정보가 관리시스템과 관리대상시스템에 분산저장, 관리된다. 최악의 경우, 모든 통신망 관리자의 보안정보가 모든 관리시스템과 관리대상시스템에 저장되어야 하고, 통신망 관리자의 추가나 삭제, 변경 작업이 모든 시스템에서 이루어져야 하므로 규모확장성이 없는 단점을 가지고 있다.

3.2.3 중앙집중방식의 보안관리기능 부재

현재의 SNMPv3 표준에서는 통신망 관리자 인증정보, 통신망 관리자와 그룹간 배정정보, 그룹에 배정된 관리권한 정보 등의 보안관리정보가 각 관리대상시스템의 지역 구성정보 데이터베이스(LCD : Local Configuration Database)에 분산되어 저장, 관리된다. 이렇게 보안관리정보가 분산된 구조에서는 통신망 전체에 적용되는 보안정보의 파악과 변경이 용이하지 않으며, 규모확장성있는 통신망 관리에 부적합할 뿐만 아니라 보안관리정보의 일관성이나 무결성이 침해될 취약성이 있다.

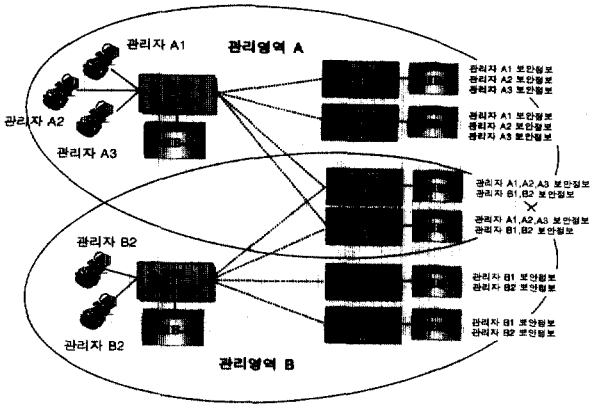
예를 들어, (그림 4)와 같은 통신망 관리구조를 가정하자. 두 개의 관리시스템에 의해 통신망 관리기능이 수행되는 환경에서 각 관리대상시스템별로 통신망 관리자별 인증키/암호키 정보, 통신망 관리자 그룹, 통신망 관리자 그룹별 관리권한 정보 등 보안관리정보를 LCD에 설정하여 관리해야 하며, 통신망 관리자는 자신의 암호절을 변경하려면 자신의 보안관리정보를 저장하고 있는 모든 관리대상시스템에 저장된 자신의 인증키/암호키를 변경하는 작업을 직접 수행해야 한다. 만일 일부 관리대상시스템에 대해서만 변경작업이 이루어질 경우, 보안관리정보가 일치하지 않게 되어 통신망 관리의 일관성이나 무결성이 침해될 수 있다.

3.2.4 통신망 관리자의 그룹배정 규칙의 모호성

통신망 관리자가 그룹에 배정되는 절차는 관리대상시스템에서 수행되는 뷰기반 접근통제 과정에서 이루어진다. 그러나, 현재의 SNMPv3 표준안에는 통신망 관리자와 그룹간 배정 규칙을 지정하지 않는 이유로 인해, 한 명의 통신망 관리자가 여러 그룹에 배정이 된 경우 통신망 관리자가 모든 그룹의 권한을 실행하게 되면 최소권한 원칙(least privilege principle)에 위배되는 문제가 있다. 따라서, 통신망 관리자의 관리권한을 결정하는 통신망 관리자와 그룹배정 규칙이 명확히 정의되어야 한다.

그리고, 통신망 관리자 그룹간 관계(relationship)가 정의되지 않아서 관리대상시스템의 계층적 관리가 불가능한 문제점이 있다. 대규모 기업의 통신망을 고려할 때, 통신망 구성요소가 수행하는 기능의 중요도에 따라 관리대상시스템을 그룹화하고 각 그룹에 대해 관리자 또는 관리자 그룹을 배정할 수 있다. 이런 경우, 일반적으로 중요한 통신망 구성요소 관리기능을 수행할 수 있는 통신망 관리자(상위 통신망 관리자)는 중요도가 낮은 통신망 구성요소를 관리하는 통신망 관리자(하위 통신망 관리자)의 관리권한을 부여받는다. 따라서, 관리자간 또는 관리자 그룹간 계층관계를 표현할 수 있다면, 하위 통신망 관리자의 권한이 상위 통신망 관리자에게 묵시적으로 상속되는 특성을 표현할 수 있게 되어 통신망 관리권한 부여를 단순화할 수 있는 장점이 있다.

위에서 기술된 SNMPv3의 보안관리 문제점은 최근 상업환경의 보안모델로서 최근 그 사용이 확대되고 있는 역할기반 접근통제(RBAC : Role-Based Access Control) 모델이 제공하는 보안특성을 이용하여 해결될 수 있다.



(그림 4) 통신망 관리자기반 통신망 관리구조 예

4. 역할기반 보안관리 모델

RBAC 모델은 사용자 대신 역할에 권한을 부여하고 역할간 상속관계(inheritance)를 효과적으로 관리하는 특성으로 인해 많은 사용자로 구성된 기업환경에 적용이 확산되고 있다. RBAC 모델의 주요 특징은 보호대상 자원이나 정보에 대한 접근권한을 사용자 대신 역할에 부여하고, 사용자를 역할에 배정함으로써 많은 사용자와 권한으로 구성된 시스템의 보안관리에 적합한 점이다. 그리고, 모델 구성요소의 변경을 통해 다양한 보안정책을 지원(policy-neutral)하는 특성으로 인해 정책기반의 시스템관리에 적합한 장점이 있다[27].

이 장에서는 SNMPv3 보안관리기능의 문제점을 해결하기 위해 RBAC 모델의 보안특성을 이용한 SNMPv3 역할기반 보안관리 모델(RSM : Role-based Security management Model)의 구성, 기능 및 역할기반 보안관리 모델이 추가된 SNMPv3의 보안시스템에 대해 기술한다.

4.1 RBAC 모델의 보안특성

RBAC 모델의 가장 큰 특징은 권한을 부여하는 단위가 사용자가 아니라 사용자가 수행하는 기능에 따라 분류된 역할이라는 점이다[10]. 따라서, 사용자는 보호대상 정보나 자원에 대한 접근권한을 얻기 위해서는 해당 접근권한을 가진 역할에 먼저 배정되어야 한다. 권한부여 및 관리 단위가 사용자가 아닌 역할이라는 이 특성은 많은 사용자로 구성된 환경에서 효율적 권한관리를 가능하게 한다. 또한, 역할간 계층구조를 통해 하위 역할에 배정된 권한이 상위 역할에 의해 사용될 수 있는 권한상속(permission inheritance) 특징을 제공한다. 권한상속 특성을 이용하여 계층구조를 가진 역할들에 대한 권한부여를 효과적으로 실행할 수 있다. RBAC 모델은 모델 구성요소 설정권한을 가진 보안 관리자가 모델 구성요소들의 구성정보를 변경함으로써 다양한 보안정책을 모델링할 수 있으며, 구성요소 관리를 통한 보안특성의 통제가 가능한 특징이 있다[10, 27].

4.2 정책기반 통신망 보안관리

역할기반 보안관리 모델은 중앙집중형 통신망 보안정보관리와 규모확장성있는 통신망 보안관리 기능의 제공을 목적으로 한다. 이를 위해, 역할기반 보안관리 모델은 각각의 통신망 구성요소(관리시스템, 관리대상시스템)별로 보안관리정보를 설정하고 관리하는 방식 대신 통신망 보안관리자에 의해 기술된 보안관리정책에 따라 전체 통신망 구성요소의 보안관리기능이 수행되는 정책기반 보안관리 기법을 이용한다.

정책기반 통신망 보안관리에는 보안관리정책을 고수준의 정형적인 형식으로 정의하는 기술언어와 통신망 구성요소가 실행하기 적합한 형태로 변환된 보안관리정책를 저장하는 보안관리 MIB 정의가 필수적이다.

(1) 보안관리정책 구성요소

역할기반 보안관리 모델에서 정의되는 보안관리정책은 관리대상 통신망에 포함된 모든 구성요소들의 보안정보를 통합적이며 일관성있게 표현할 수 있는 고수준(high-level)의 언어로 기술되어야 하고, 다음과 같은 구성요소들을 포함해야 한다.

- **관리 영역** : 관리대상 통신망을 구성하는 구성요소(관리시스템, 관리대상시스템)들의 식별자
  (예 : 도메인 이름, IP 주소 등)
- **통신망 관리자와 통신망 관리역할간 배정** : 통신망 관리역할별로 관리역할에 배정된 통신망 관리자 식별자
- **통신망 관리역할과 관리권한 배정** : 통신망 관리역할들에 배정된 통신망 관리권한
- **통신망 관리역할간 계층 정보** : 관리권한의 상속특성을 제공하는 통신망 관리역할별 계층구조
- **통신망 구성요소별 기능 정보** : 통신망 구성요소가 수행하는 기능(관리시스템, 관리대상시스템) 지정

(2) 보안관리정책 기술언어

보안관리정책은 보안관리자가 통신망 보안관리구조와 함께 보안정보를 용이하게 기술하고 해독할 수 있는 고수준의 기술언어로 기술되어야 한다. 그러나, 보안관리정책은 통신망의 구성과 성능관리를 위한 정책과 구조적 측면에서 다르다. 지금까지 진행된 정책기반의 통신망 관리의 대부분은 통신망의 구성 및 성능관리에 목적을 두고 있으며[8, 9, 12, 20, 21], 이 경우의 정책은 통신망의 구성정보의 변경이나 성능변화에 대한 대응절차를 기술하기에 적합한 ECA(Event-Condition-Action) 규칙을 기반으로 하고 있다[14, 16, 30, 34]. 그러나, 통신망 보안관리정책은 통신망 관리자의 인증정보, 프로토콜 데이터의 암호와 인증, 관리정보에 대한 접근통제 정보 등을 효과적으로 기술하고 관리하는데 목적이 있으므로 ECA 규칙기반의 정책 구조와는 차이가 있다.

보안관리정책 기술언어에 의해 기술된 정책은 통신망 구성요소가 인식할 수 있는 구체적 형태의 MIB 구조로 변환된 후, 보안관리 MIB에 저장된 정보의 용도에 의해 관리시스템들이나 관리대상시스템들로 각각 전달된다. 보안관리정책 기술언어에 대한 문법은 부록과 같다.

(3) 보안관리 MIB 구조

보안관리자에게 사용 편리성과 관리 용이성을 제공하기 위해 고수준으로 기술된 보안관리정책은 최종적으로 보안관리기능을 수행하는 관리시스템과 관리대상시스템이 인식할 수 있는 매우 구체적이며 표준화된 관리정보 형태로 변환되어야 한다. 보안관리정책을 구체적 표현하고 저장하기 위한 MIB 구조는 (그림 5)와 같다.

rsmUserToRoleTable

Object	Type	Access
rsmUserName	SnmpAdminString	read-create
rsmRoleName	SnmpAdminString	read-create

rsmRoleHierarchyTable

Object	Type	Access
rsmJuniorRoleName	SnmpAdminString	read-create
rsmSeniorRoleName	SnmpAdminString	read-create

rsmEngineTypeTable

Object	Type	Access
rsmEngineID	SnmpEngineID	read-create
rsmEngineType	INTEGER	read-create

rsmRoleAccessTable

Object	Type	Access
rsmRoleName	SnmpAdminString	not-accessible
rsmAccessContextPrefix	SnmpAdminString	not-accessible
rsmAccessSecurityModel	SnmpSecurityModel	not-accessible
rsmAccessContextMatch	INTEGER	read-create
rsmAccessReadViewName	SnmpAdminString	read-create
rsmAccessWriteViewName	SnmpAdminString	read-create
rsmAccessNotifyViewName	SnmpAdminString	read-create
rsmAccessStorageType	StorageType	read-create
rsmAccessStatus	RowStatus	read-create

(그림 5) 보안관리 MIB 테이블 구조

'rsmUserToRoleTable' 통신망 관리자와 관리역할간 배정 정보를 저장하는데 사용되며, 'smRoleHierarchyTable' 관리권한의 상속관계를 특성을 가지는 역할간 계층구조를 정보를 저장한다. 그리고, 'rsmRoleAccessTable' 사용자기반 보안모델에서 통신망 관리자 그룹에 관리권한을 부여한 것과 유사하게 각각의 통신망 관리역할에 어떤 관리권한이 부여되어 있는지를 'READ', 'WRITE', 'NOTIFY' 뷰를 기준으로 나타내고 있다. 마지막으로, 'rsmEngineTypeTable'은 통신망 구성요소가 관리시스템, 관리대상시스템, 또는 관리시스템과 관리대상시스템의 기능을 함께 수행하고 있는지에 대한 정보를 저장한다.

통신망 구성요소가 수행하는 기능에 따라 참조하는 보안관리 MIB 정보가 다르므로, 보안관리 MIB 전송 응용은 'rsmEngineTypeTable'을 참조하여 통신망 구성요소가 수행하는 기능에 따라 해당 보안관리 MIB 정보를 전송한다.

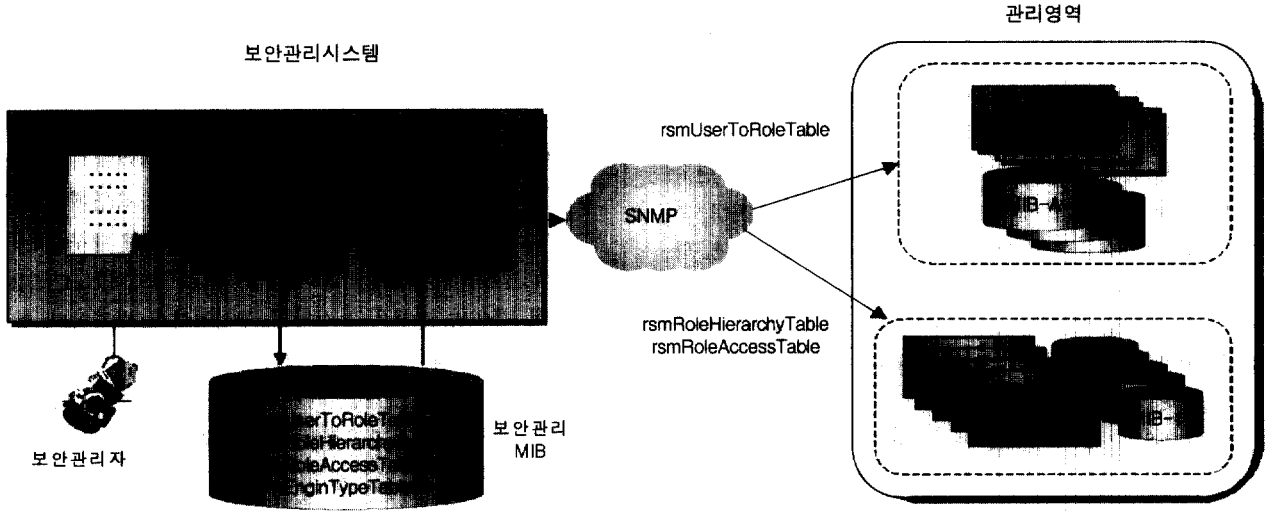
즉, 'rsmUserToRoleTable' 정보는 통신망 관리자의 인증 후 역할부여 여부를 결정할 때 이용되므로 관리시스템들에게 전송되고, 'rsmRoleAccessTable'과 'rsmRoleHierarchyTable'은 관리정보에 대한 접근통제 과정에서 참조되므로 관리대상시스템들로 전송된다. 'rsmEngineTypeTable'에는 통신망 관리영역에 포함된 모든 관리시스템과 관리대상시스템 정보를 함께 저장하고 있다.

(그림 6)은 보안관리자에 의해 기술된 보안정책이 보안관리 MIB으로 변환되고, 그 기능에 따라 관리시스템과 관리대상시스템으로 전송되는 구조를 나타내고 있다.

(4) 확장된 보안시스템 동작구조

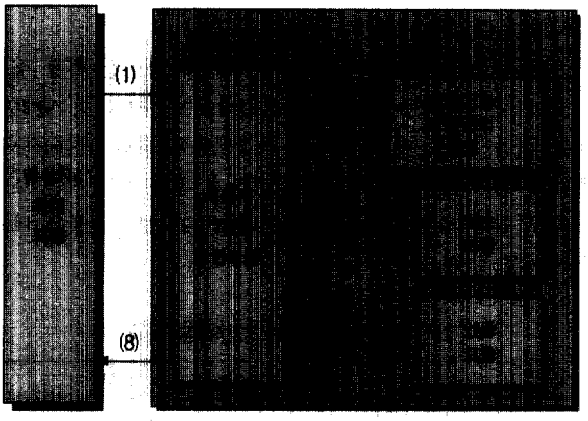
역할기반 보안관리 모델은 사용자기반 보안모델의 보안관리 취약성을 보완하는 기능을 수행하며, 사용자기반 보안모델에서 제공하는 메시지 인증과 암호 서비스를 이용한다. 역할기반 보안관리 모델이 추가된 보안시스템의 구조와 동작 절차는 (그림 7)과 같다.

(그림 7)은 메시지 인증과 암호 보안서비스를 모두 사용하여 전송되는 메시지의 처리 절차를 나타내고 있으며, 굵게 표시된 정보가 역할기반 보안관리 모델이 사용됨으로써 추가된 정보들이다. 통신망 사용자와 그룹간 배정을 명시적으로 기술하기 위해 (그림 7)의 데이터 (1)에 역할이름이 추가되었으며, 이 정보는 관리명령을 수행하는 통신망 관리자에 의



(그림 6) 보안관리정책 변환 및 전송 구조

해 지정된다. 역할기반 보안관리 모델은 입력으로 주어진 데이터 (2)에 대해 사용자가 역할에 배정되어 있는지를 점검하여 그 결과를 반환한다. 만일, 사용자가 역할에 배정되어 있으면 데이터 (3)에 해당 역할이름을 반환하여 메시지에 대한 인증과 암호 과정을 처리하고, 그렇지 않은 경우에는 정당한 통신망 관리자가 아니므로 처리절차를 중지하고 에러 메시지를 반환된다.



(1) 메시지 처리 모델 데이터, 헤더 데이터, 보안데이터, scopedPDU, 역할 이름
(2) 사용자 이름, 요청된 역할 이름
(3) 배정된 역할 이름 또는 오류 메시지
(4) 암호키, scopedPDU
(5) 암호 매개변수, 암호화된 scopedPDU
(6) 인증키, 전체 메시지
(7) 인증된 전체 메시지
(8) 인증/암호화된 전체 메시지, 전체 메시지 길이 인증, 암호 매개변수

(그림 7) 역할기반 보안관리 모델이 추가된 보안시스템의 동작 절차

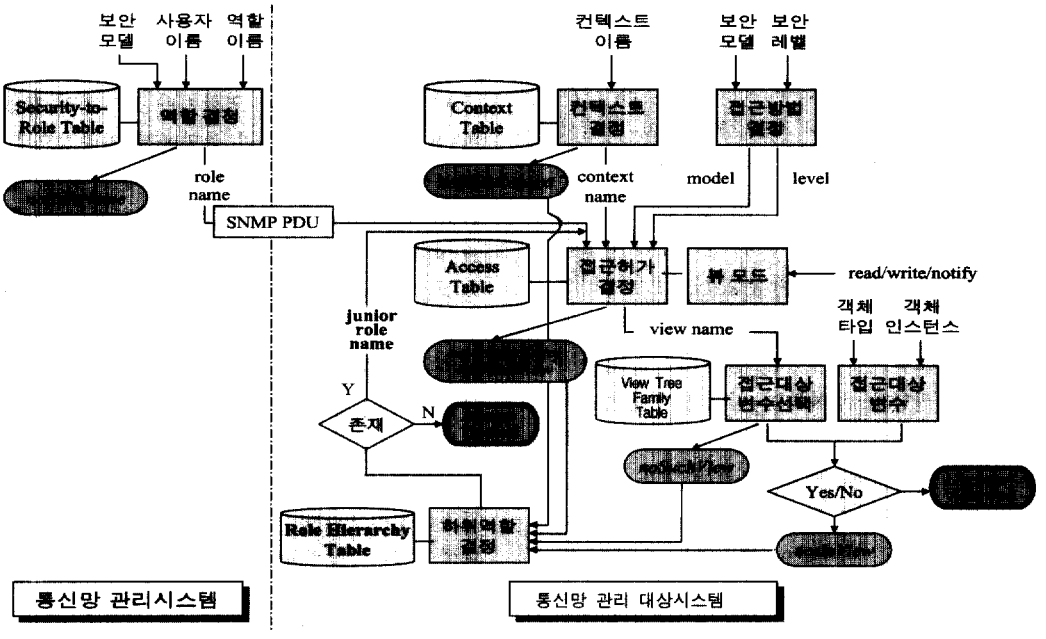
(5) 변경된 뷰기반 접근통제 절차

역할기반 보안관리 모델을 지원하기 위해 통신망 관리대상시스템에서 수행되는 뷰기반 접근통제 모델에 대한 변경이 요구된다. SNMPv3 표준안의 뷰기반 접근통제 절차는 통신망 관리자들로 구성되는 그룹별로 MIB 접근권한을 부여하지만, 역할기반 보안관리 모델이 추가된 보안시스템에서는 통신망 관리자의 역할별로 관리권한이 배정되고, 역할 계층을 고려한 접근통제 절차가 지원되어야 한다. (그림 8)은 역할기반 보안관리 모델을 적용한 뷰기반 접근통제 절차를 나타내고 있다.

(그림 8)의 수정된 뷰기반 접근통제 절차와 사용자기반 보안모델과 연동하는 경우와의 다른 점은 통신망 관리자가 실행할 수 있는 관리권한이 관리시스템에서 미리 결정되어 관리대상시스템으로 전달되는 것이다. 즉, 관리명령의 수행 허가 여부를 결정하는 통신망 관리자의 역할이 관리시스템에서 결정되고 프로토콜 데이터에 포함되어 관리대상시스템으로 전송된다. 이 방식은 통신망 관리자와 그룹 배정규칙이 명확하지 않은 문제점을 보완하는 장점을 제공하며 최소권한 원칙을 준수하도록 한다.

또 다른 특징은 관리시스템으로부터 전달된 역할에 대해 관리정보에 대한 접근이 허가되지 않아 보안오류가 발생한 경우에, 주어진 역할의 하위역할들을 이용하여 접근허가 여부를 재검사하는 것이다. 이때 통신망 관리역할간 계층구조 정보가 사용되며, 이 정보는 보안관리시스템에서 보안관리자에 의해 설정되고 관리영역내의 모든 관리대상시스템으로 분배된다.

(그림 9)는 정책기반 보안관리모델이 적용된 SNMPv3 보안시스템에서 관리대상시스템에서 수행되는 접근허가 결



(그림 8) 역할기반 보안관리 모델을 적용한 뷰기반 접근통제 절차

정함수인 'IsAccessAllowedInRSM'의 알고리즘이다. 이 알고리즘에서 호출되는 'IsAccessAllowed' 함수는 입력으로 주어진 역할에게 부여된 관리권한만을 이용한 접근통제 함수를 의미한다. 입력으로 주어진 역할이 관리정보에 대한 접근권한이 허용되지 않은 경우, 관리대상시스템 MIB에 저장된 'rsmRoleHierarchyTable'을 이용하여 해당 역할의 하위 역할들을 계산(GetJuniorRoles())한 뒤, 각 역할에 배정된 관리권한들을 점검한다.

```
Algorithm IsAccessAllowedInRSM
Input
role : SnmpAdminString
context : SnmpAdminString
model : SnmpSecurityModel
level : SnmpSecurityLevel
op : 'READ', 'WRITE', 'NOTIFY'
oid : OBJECT IDENTIFIER
Output
TRUE // access allowed
FALSE // access denied
Begin
if (IsAccessAllowed (role, model, level, context, op, oid)
    == FALSE) then
        role_list ← GetJuniorRoles(role) ;
        for each role r in role_list do
            if (IsAccessAllowed(r, model, level, context, op, oid)
                == TRUE) then
            return TRUE ;
        done
else
    return TRUE ;
  endif ;
  return FALSE ;
End
```

(그림 9) 정책기반 접근통제 알고리즘

4.3 사용자기반 보안모델과의 비교

역할기반 보안관리 모델은 사용자기반 보안모델이 제공하지 못하는 보안관리기능을 보완하는데 목적이 있으며, 사용자기반 보안모델에서 제공하는 메시지 인증과 암호 보안서비스를 활용한다. 통신망 보안관리 관점에서 역할기반 보안관리 모델은 역할기반 접근통제 모델의 보안특성을 활용하여 많은 수의 통신망 구성요소와 통신망 관리자로 구성된 통신망에 대한 중앙집중방식의 규모확장성있는 보안관리서비스를 제공한다.

역할기반 보안관리 모델에서 통신망 관리자가 수행하는 역할을 기준으로 관리권한을 부여하는 방식은 사용자기반 보안모델에서 통신망 관리자 그룹에게 관리권한을 부여하는 것과 유사하다. 그러나, 역할간 계층관계에 의한 관리권한 상속특징을 이용하기 때문에 통신망 관리자 그룹단위로 관리권한과 통신망 관리자를 반복하여 배정하는 과정이 없어지고, 그 과정에서 발생할 수 있는 오류를 줄일 수 있는 장점이 있다.

그리고, 통신망 관리역할의 종류가 통신망 관리자 수보다 작고, 관리대상시스템이 관리시스템보다 많은 경우가 일반적인 점을 고려할 때 각 관리대상시스템에 저장, 관리되는 보안관리정보(통신망 관리자 인증 정보)가 적게 되어 통신망 전체적으로 볼 때 보안정보 관리에 소요되는 오버헤드가 줄어드는 특징이 있다. 이밖에도 보안관리시스템에서 기술된 보안관리정책에 의해 보안관리정보가 중앙관리되고 분배되는 특징은 사용자기반 보안모델에서 보안관리정보가 분산관리됨으로써 발생할 수 있는 보안관리정보의 무결성이 침해되는 취약성을 줄일 수 있다.

그러나, 관리시스템에 통신망 관리자와 역할간 배정 정보를 추가로 저장하고, 관리대상시스템에서 수행되는 관리정보에 대한 접근통제 과정에서 역할계층에 의한 권한상속을 추가로 점검하는 오버헤드가 발생하게 된다. 역할기반 보안관리 모델과 사용자기반 보안모델의 주요 보안특성을 비교하면 <표 1>과 같다.

〈표 1〉 USM과 RSM 보안특성 비교

	USM	RSM
보안정보 관리방식	· 관리시스템, 관리대상시스템에서 분산관리	· 보안관리정책에 의한 중앙집중형 보안관리
관리시스템의 보안관리 MIB 정보	· 통신망 관리자 인증 정보	· 통신망 관리자 인증 정보 · 역할 인증 정보 · 통신망 관리자-역할 배정 정보
관리대상시스템의 보안관리 MIB 정보	· 통신망 관리자 인증 정보 · 통신망 관리자-그룹 배정 정보 · 그룹-관리권한 배정 정보	· 역할 인증 정보 · 역할-관리권한 배정 정보 · 역할계층 정보
접근통제 절차 특징	· 그룹에 부여된 관리권한 기반	· 역할에 부여된 관리권한과 하위역할들에 배정된 관리권한 기반

4.3.1 분석

본 논문에서 제안된 역할기반 보안관리 모델과 사용자기반 보안모델을 보안관리 측면에서 정량적으로 비교하기 위해 관리시스템과 관리대상시스템에서 저장, 관리되는 보안관리 정보의 갯수와 중복저장 정도를 기준으로 분석한다. 그 이유는 통신망의 보안관리에 사용되는 보안관리 정보의 갯수가 많거나 보안관리 정보가 중복되어 저장되면 정보의 일관성 유지가 어렵고 무결성 침해 위험이 높아지기 때문이다. SNMPv3 통신망 관리환경에서 중요한 보안관리 정보로는 통신망 관리자의 암호절과 인증절 정보, 통신망 관리자 그룹 정보와 관리권한 정보가 있으며, 특히 통신망 관리자의 암호절과 인증절은 SNMPv3 보안서비스의 안전성을 결정하는 보안관리 정보로서 관리시스템이나 관리대상시스템에 중복을 최소화하여 저장, 관리되어야 한다.

분석과정에서 사용되는 표기법들은 다음과 같다. 통신망 관리기능을 수행하는 통신망 관리자의 수를 N_{admin}, 관리시스템들에 저장된 통신망 관리자의 수를 $N_{admin'}$이라 할 때

한 명의 관리자가 하나 이상의 관리시스템에서 관리기능을 수행할 수 있으므로 $N_{admin} \leq N_{admin'}$의 관계가 성립한다. 그리고, 관리대상시스템들에 저장된 통신망 관리자수를 $N_{admin''}$ 이라 하고, 한 명의 통신망 관리자가 하나 이상의 관리대상시스템을 관리하는 일반적인 통신망 관리환경을 고려하면, $N_{admin'} < N_{admin''}$의 관계가 성립한다(식 1). 또한, 역할기반 보안관리 모델에서 통신망 관리를 위한 역할의 수, 관리시스템들에 저장된 역할의 수, 그리고 관리대상시스템들에 저장된 역할의 수를 N_{role}, $N_{role'}$, $N_{role''}$으로 각각 표기할 때, $N_{role} \leq N_{role'} < N_{role''}$의 관계가 성립한다(식 2). 그리고, 하나의 통신망 관리역할을 여러 명의 통신망 관리자가 수행하므로 식 (3)의 관계가 성립한다. 관리대상시스템들에서만 저장,관리되는 그룹과 관리권한의 수는 각각 $N_{group''}$과 $N_{perm''}$ 으로 표시한다.

$$N_{admin} \leq N_{admin'} < N_{admin''} \quad (1)$$

$$N_{role} \leq N_{role'} < N_{role''} \quad (2)$$

$$N_{role} < N_{admin},\ N_{role'} < N_{admin'},\ N_{role''} < N_{admin''} \quad (3)$$

<표 2>는 사용자기반 보안모델과 역할기반 보안관리 모델에서 관리시스템과 관리대상 시스템에 저장되는 보안관리 정보의 갯수를 비교하고 있다.

〈표 2〉 USM과 RSM의 보안관리 정보 갯수 비교

		USM	RSM
관리시스템들	통신망 관리자별 암호절, 인증절	2 x Nadmin'	2 x Nadmin'
	역할별 암호절, 인증절	-	2 x Nrole'
	역할-통신망 관리자 배정 정보	-	Nrole' + Nadmin'
관리대상시스템들	통신망 관리자별 암호절, 인증절	2 x Nadmin''	-
	역할별 암호절, 인증절	-	2 x Nrole''
	그룹-관리권한 배정 정보	Ngroup'' + Nperm''	-
	역할-관리권한 배정 정보	-	Nrole'' + Nperm''
	역할계층 정보	-	Nrole''

먼저, 관리시스템들에 저장되는 보안관리 정보의 갯수를 비교하면, 두 보안모델 모두 통신망 관리자에 대한 암호절과 인증절 정보($2xN_{admin'}$)를 저장하지만 역할기반 보안관리 모델에서 역할에 대한 암호절과 인증절 정보($2xN_{role'}$), 그리고 역할에 배정된 통신망 관리자에 대한 보안정보($N_{role'} + N_{admin'}$)를 추가로 저장, 관리해야 하는 오버헤드가 발생한다.

관리대상시스템들에서는 사용자기반 보안모델의 경우 각 관리대상시스템에 관리기능을 수행하는 모든 통신망 관리자에 대한 암호절과 인증절 정보($2xN_{admin''}$)가 저장되는 반면, 역할기반 보안관리 모델에서는 통신망 관리자에 대한 보안관리 정보 대신 역할에 대한 암호절과 인증절 정보($2x-N_{role''}$)가 저장된다. 그리고, 사용자기반 보안모델의 그룹과 역할기반 보안관리 모델의 역할은 관리권한이 배정되는 단위로서 그룹과 역할의 갯수를 정량적으로 비교하는 일반적인 규칙이 없으므로 두 정보의 차는 크지 않다고 가정한다. 그러나, 역할기반 보안관리모델에서는 역할계층을 이용한 관리권한 상속특성을 이용하여 관리권한 배정의 중복성을 없애는 장점이 있다.

종합하면, 역할기반 보안관리모델에서는 역할에 보안관리 정보를 저장하는 오버헤드($N_{role'} + N_{admin} + 2xN_{role'} + 2xN_{role''}$)가 추가되는 반면 사용자기반 보안모델에서 관리대상시스템들이 관리해야 했던 통신망 관리자들에 대한 암호절 및 인증절 정보($2xN_{admin''}$) 관리 오버헤드를 제거하는 장점이 있다. 역할기반 보안관리 모델을 적용함으로써 발생하는 보안정보 관리오버헤드를 다시 표현하면 (식 4)와 같다.

$$\begin{aligned} & N_{role'} + N_{admin'} + 2 \times N_{role'} + 2 \times N_{role''} \\ & < 2 \times N_{admin'} + 2 \times N_{role'} + 2 \times N_{role''} \\ & < 4 \times N_{admin'} + 2 \times N_{role''} \end{aligned} \quad (4)$$

(식 4)에서 한 명의 통신망 관리자가 여러 개의 관리대상시스템을 관리하는 일반적인 통신망 관리환경($N_{admin'} \ll N_{admin''}$) 과 하나의 관리역할에 배정된 통신망 관리자의 수가 많은 일반적인 특성($N_{role''} \ll N_{admin''}$)을 고려할 때, (식 4)에 해당하는 관리정보의 갯수가 사용자기반 보안모델을 적용한 경우의 보안관리 정보($2xN_{admin''}$)의 갯수보다 작다고 분석할 수 있다. 위의 분석 결과로부터 역할기반 보안관리 모델은 동일한 통신망 관리역할을 수행하는 통신망 관리자의 수가 많고, 다수의 관리대상시스템들로 구성된 대규모의 통신망의 보안관리에 적합하다는 결론을 얻을 수 있다.

그리고, 보안관리 정보의 중복저장 정도를 비교하면 사용자기반 보안모델의 경우 통신망 관리자의 암호절, 인증절 정보가 관리시스템과 관리대상시스템에 중복 저장되는데 반해, 역할기반 보안관리 모델에서는 관리시스템에서만 통신망 관리자의 보안관리 정보가 저장되므로 사용자기반 보안모델에 비해 보안관리 정보의 중복저장 정도가 낮은 장점이 있다.

역할기반 보안관리 모델을 추가하여 확장한 보안시스템의 프로토타입은 SNMPv3를 지원하는 NET-SNMP 패키지[18, 20, 31]를 수정하여 구현되었다. 현재는 텍스트 에디터를 이용하여 보안관리정책을 작성하고, 보안관리정책을 보안관리 MIB으로 변환하는 프로그램과 보안관리 MIB 전송 응용의 수행이 명령어 기반으로 실행되지만, 앞으로 그래픽 사용자 인터페이스 기반의 보안관리정책 편집기, 보안관리 MIB 전송 응용 등의 통합운영환경의 추가적 개발이 필요하다.

5. 결론 및 향후 연구방향

통신망 구성요소가 복잡화, 이질화되고 분산화됨에 따라

통신망 관리자가 요구하는 다양한 서비스 제공을 위해서 통신망 관리의 중요도가 증가하고 있다. 통신망 관리제품들은 통신망 관리자들이 보다 효과적으로 통신망의 동작상태를 감시하고 관리할 수 있도록 개발되고 있다. 정책기반 통신망관리 개념은 통신망 관리자가 각 통신망 구성요소에 대한 직접적인 동작설정 대신 미리 설정한 규칙에 따라 통신망 구성요소나 서비스의 동작을 결정하게 한다. 통신망 보안관리 역시 통신망 관리자와 통신망 구성요소의 수가 증가하고, 인증과 암호와 같은 보안서비스가 널리 사용되면서 보안정보에 대해 체계적인 관리의 필요성이 증대되었다.

본 논문에서는 보안관리 측면에서 현재 SNMPv3 보안시스템의 문제점과 원인을 분석하고, 이를 해결하기 위해 방안으로 정책기반 보안관리기능을 지원하는 역할기반 보안관리 모델을 설계하고 보안관리 측면에서의 효율성을 분석하였다. 역할기반 보안관리 모델은 보안정보에 대한 중앙집중식 관리가 가능하고 사용자나 권한에 대한 규모확장성있는 관리기능을 제공하는 역할기반 접근통제 모델을 활용하였다. 그리고, 지정된 보안관리시스템에서 통신망 보안정보의 관리나 접근통제 규칙을 보안관리정책으로 표현하고, 기술된 정책이 변환된 보안관리 MIB 정보가 통신망 구성요소에 분산, 중복되지 않도록 관리함으로써 현재의 SNMPv3가 가지는 보안정보의 중복과 분산관리에서 발생할 수 있는 보안관리 취약성을 보완한다.

앞으로는 보안관리정책 편집과 보안관리정책의 보안정보 MIB 변환, 보안관리 MIB 전송 응용의 통합 환경 구현과 비대칭형 암호 알고리즘을 이용한 통신망 관리자, 메시지 인증 및 암호 서비스 개발에 대한 연구가 필요하다.

[부 록] RSM 보안관리정책 기술언어 문법

RSM_Policy : == [**'RSM DOMAIN'** RSM_Domain]
'RSM_UA' RSM_Role_User_Assignment
'RSM_PA' RSM_Role_Permission_Assignment
'RSM_RH' RSM_Role_Hierarchy
'RSM_FA' RSM_Function_Assignment

RSM_Domain : == Domain_Elements Domain_Element | Domain_Element

RSM_Role_User_Assignment : == UA_Elements

UA_Element | UA_Element
UA_Element : == Role_Name ' : ' Admin_Name_Lists

Admin_Name_Lists : == Admin_Name_Lists Admin_Name | Admin_Name

RSM_Role_Permission_Assignment : == PA_Elements
PA_Element | PA_Element

PA_Element : == Role_Name ' : ' Admin_Perm_Lists

Admin_Perm_Lists : == Admin_Perm_Lists Admin_Perm | Admin_Perm
RSM_Role_Hierarch.y : == RH_Elements RH_Element | RH_Element

PA_Element : == Role_Name ' : ' Junior_Role_Names

Junior_Role_Names : == Junior_Role_Name Junior_Role_Name | Role_Name

RSM_Function_Assignment : == FA_Elements
FA_Element | FA_Element

FA_Element : == SNMP_Engine ' : ' SNMP_Engine_Function

Domain_Element : == IP_Address | Domain_Name

IP_Address : == **IpAddress** -- defined in RFC1155

Domain_Name : == **SnmpAdminString** -- defined in RFC2571

Role_Name : == **SnmpAdminString**

Admin_Name : == **SnmpAdminString**

Admin_Perm : == Context_Prefix Context_Match View_Type View_Name ViewTreeFamilyNames

Context_Prefix : == **SnmpAdminString**

Context_Match : == **INTEGER** -- defined in RFC1212

View_Type : == **'READ'** | **'WRITE'** | **'NOTIFY'**

View_Names == **SnmpAdminString**

ViewTreeFamilyNames : == ViewTreeFamilyNames | ViewTreeFamilyName

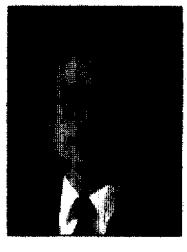
ViewTreeFamilyNames : == **SnmpAdminString**

SNMP_Engine : == **SnmpAdminString**
SNMP_Engine_Function : == **'AGENT'** | **'MANAGER'** | **'AGENT_AND_MANAGER**

참 고 문 헌

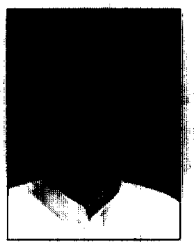
[1] 신영석, 정책기반의 보안 네트워크 구조, NETSEC-KR2001, April, 2001.
[2] Wang Changkun, "Policy-based Network Management,"

Communication Technology Proceedings, 2000.
[3] Policy Framework Core Information Model, draft-ietf-policy-core-info-schema-02.txt, Internet Draft, February 1999.
[4] The COPS(Common Open Policy Service) Protocol, draft-ietf-rap-cops-06.txt, Internet Draft, February 1999.
[5] Policy Framework, draft-ietf-policy-framework00.txt, Internet Draft, September 1999.
[6] Policy Framework Core Information Model, draft-ietf-policy-core-info-model-02.txt, Internet Draft, October 1999.
[7] Requirements for a Policy Management System, draft-ietf-policy-req-02.txt, November, 2000.
[8] Policy QoS Information Model, draft-ietf-policy-qos-info-model-03.txt, April, 2001.
[9] Information Model for Describing Network Device QoS Datapath Mechanisms, draft-ietf-policy-qos-device-info-model-04.txt, June, 2001.
[10] David F. Ferraiolo, Janet A. Cugini, D. Richard Kuhn, "Role-Based Access Control(RBAC) : Features and Motivations," Proceedings of the 11th Annual Computer Security Applications Conferences, December 1995, pp. 241-248.
[11] Warwick Ford, *Computer Communications Security : Principles, Standard Protocols and Techniques*, Prentice-Hall, 1994.
[12] Ashfaq Hossain, Houshing F. Shu, Charles E. Gasman, Randolph A. Royer, "Policy-based Network Load Management," Bell Labs Technical Journal, October-December, 1999.
[13] A Prime on Policy-based Network Management, Open View Network Management Division, Hewlett-Packard Company, September 1999.
[14] Thomas Koch, Christoph Krell, Bernd Kramer, "Policy Definition Language for Automated Management of Distributed Systems," Proceedings of 2nd IEEE International Workshop on Systems Management, 1996.
[15] HyungHyo Lee, DongIk Lee, BongNam Noh, "Policy-based Security Management in SNMPv3 : Role-based Approach," Workshop on Information Security Applications, November, 2000.
[16] Jorge Lobo, Randeep Bhatia, Shamin Naqvi, "A Policy Description Language," Proceedings of AAAI99, 1999.
[17] Masullo, M., Calo , S., "Policy Management : An Architecture and Approach," Proceedings of the 1st International Workshop on System Management, April, 1993.
[18] MG-SOFT, http : //www.mg-soft.com/mgMibBrowserPE.html, 2001.
[19] Moffet, J. D., Sloman, M., "Policy Hierarchies for Distributed Systems Management," IEEE JSAC Special Issue on Network Management, Vol.11, No.9, December 1994.
[20] The NET-SNMP Home Page, http : //net-snmp.sourceforge.net, 2001.
[21] Rajan, R., Chiu, A., Civanlar, S., "A Policy based Approach for QoS-on-demand over the Internet," Proceedings of the 8th International Workshop on Quality of Service, 2000.
[22] RFC 1902, Structure of Management Information for Version 2 of the Simple Network Management Protocol, January, 1996.
[23] RFC 2571, An Architecture for Describing SNMP Management Frameworks, May, 1999.
[24] RFC 2572, Message Processing and Dispatching for the Simple Network Management Protocol(SNMP), May 1999.
[25] RFC 2574, User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3), April 1999.
[26] RFC 2575, View-based Security Model (VACM) for the Simple Network Management Protocol(SNMP), April 1999.
[27] Ravi S. Sanhdu, Pierangela Samarati, "Access Control : Principle and Practice," IEEE Computer, September 1994, pp.40-48.
[28] Susan J, Shepard, "Policy-Based Networks : Hype and Hope, IT Pro," January-February 2000.
[29] Morris Sloman, Network and Distributed Systems Management, Addison-Wesley, 1994.
[30] Morris Sloman, Emil Lupu, "Policy Specification for Programmable Networks," Proceedings of the 1st International Working Conference on Active Networks(IWAN '99), June, 1999.
[31] OpenSSL Home Page, http : //www.openssl.org, 2001.
[32] Stallings, W. SNMP, SNMPv2, SNMPv3 and RMON1 and RMON2, Third Edition, Addison-Wesley, 1998.
[33] Mani Subramanian, Network Management : Principles and Practice, Addison-Wesley, 2000.
[34] Wies, R., "Using a Classification of Management Policies for Policy Specification and Policy Transformation," Proceedings of the IFIP/IEEE International Symposium on Integrated Network Management, May, 1995.



주 광 로

e-mail : grjoo@seokang.ac.kr
1982년 전남대학교 계산통계학과 학사
1985년 전남대학교 대학원 계산통계학과 석사
1995년 전남대학교 대학원 전산통계학과 박사수료
1985년~현재 서강정보대학 컴퓨터정보과 부교수
관심분야 : 정보보안, 통신망관리, 웹응용기술 등



이 형 효

e-mail : hlee@wonkwang.ac.kr

1987년 전남대학교 계산통계학과 졸업

1989년 KAIST 전산학과 석사

2000년 전남대학교 전산통계학과 박사

1990~1992년 삼보컴퓨터 기술연구소

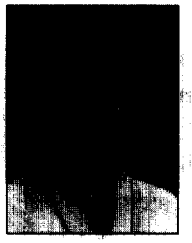
1993~1997년 한국통신 연구개발원

1995년 정보처리기술사(전자계산조직응용)

2000년 광주과학기술원 BK21 Post-Doc.

2001년~현재 원광대학교 정보·전자상거래 학부 전임강사

관심분야 : 정보보안, 보안모델, 통신망관리 등



노 봉 남

e-mail : bongnam@chonnam.ac.kr

1978년 전남대학교 수학교육과

1982년 KAIST 전산학과 석사

1994년 전북대학교 전산통계학과 박사

1983년~현재 전남대학교 컴퓨터정보학부 교수

2000년~현재 ITRC 리눅스 시스템보안 연구센터 소장

관심분야 : 리눅스보안, 시스템 및 네트워크 보안, 사이버사회와 윤리 등