위임과 보안 성질을 통한 OSI망과 TCP/IP 인터네트의 통합 관리

김 태 연† 서 재 현†† 노 봉 남†††

요 약

OSI 망과 TCP/IP 인터네트를 통합 관리하기 위해서 강력하고 융통성이 있는 패러다임인 응용 게이트웨이가 사용되고 있지만 게이트웨이의 미시 관리(micro management)로 응급 상황에서 통신 지연과 비용이 증가하여 성능이 저하된다. 또한 서로 다른 보안 정책을 사용하는 두 영역간에 접근 제어 정책을 사상하는 메카니즘이 필요하다. 이러한 문제는 서로 다른 표준으로 구성된 두 영역을 통합하는 데서 야기된다. 본 논문에서는 CMIP의 강력하고 융통성이 있는 서비스뿐만 아니라 관리 기능을 위임할 수 있는 응용 게이트웨이를 설계하였다. Diffie-Hellman의 키 분배 방식을 기반으로 하여 관리 서비스와 기능을 안전하게 전달하는 알고리즘을 정의하고 서로 다른 보안 정책을 사용하는 두 영역간에 안전한 통신이 보장될 수 있도록 보안 정책을 조정하는 메카니즘을 제시하였다.

Integrated Management of OSI network and TCP/IP internet with Delegation and Security Features

Taeyeon Kim†, Jaehyeon Seo††, and Bongnam Noh†††

ABSTRACT

To integrate both the OSI network and the TCP/IP internet, the application gateway that have the powerful and flexible paradigms has been used, but due to the micro-managements of the gateway produce the high costs and the long delay of communication in the case of emergency. The mechanism that maps the access control policies between two domains using the different security policies is needed. These problems are caused by integrating both domains with the different standards. In this paper, the application gateway that delegating to an agent the powerful and flexible services of the CMIP as well as the management functions were proposed. A proposed algorithm that delegates the management script to an gateway safely by capitalizing on the Diffie-Hellman's distribution method, and presents the security mechanism mediating the security policies for guaranteeing the secure communication between two domains using the different security policies.

1. 서 론

시간에 제한을 받는 복잡한 초고속 망에 양질의 서비스를 제공되지 못하면 심각한 문제를 야기한다. 관리 서비스는 시간적인 제한에 매우 민감하기 때문에 이러한 서비스를 관리하는 관리 응용은 실시간 처리가 이루어져야 한다. 현재, OSI 망관리를 위한 표준인 CMIP(Common Management Information Protocol)과 TCP/IP (Transmission Control Protocol/ Internet Protocol) 망관리를 위한 표준인 SNMP(Simple Network Management Protocol)를 기반으로 하는 응용 프로토콜이 널리 이용되고 있다. SNMP는 관리 대상을 인터네트 프로토콜 장비만을 한정하며, 이 장비에 대한 장애 관리와 구성 관리에 초점을 맞추어 개발되었다. 한편 CMIP는 모

†준 회 원 : 광주예술전문대학 컴퓨터그래픽 디자인학과 전임강사
††준 회 원 : 송원전문대학 전자계산학과 전임강사
†††종신회원 : 전남대학교 전산학교 교수
논문접수 : 1995년 7월 13일, 심사완료 : 1995년 11월 22일

든 망 장비들에 대한 관리가 가능하도록 설계되었다.

SNMP 인터네트 프로토콜에서 지원되는 서비스는 SET, GET, GET-NEXT, TRAP이 있고, OSI 망에서 제공되고 있는 CMIS 서비스는 M-GET, M-CANCEL-GET, M-SET, M-ACTION, M-CREATE, M-DELETE, M-EVENT-REPORT 등이 있다. 또한 CMIS에서는 관리자가 관리 객체(managed object)들 중에서 하나 또는 여러 개를 선택할 수 있는 강력한 수단을 제공하는 범위 지정(scoping)과 필터링(filtering), 동기화(synchronization) 기능이 있다[6, 12].

OSI 망과 TCP/IP 인터네트 대행자는 관리 정보베이스(MIB:Management Information Base)를 제어한다. 그러나 두 모델의 MIB구조는 서로 상이하다. 인터네트 모델에서 MIB는 인스턴스와 테이블 형태로 구성되며, OSI모델의 관리 객체는 속성, 행위, 통보, 연산에 의해서 정의되고, OSI의 MIB의 구현은 객체지향 접근 방법이 사용된다.

SNMP를 기반으로 하는 망관리의 장점은 현재 SNMP 대행자 소프트웨어가 널리 사용되고 있으며, 망 자원의 사용 비용이 싸고, 현재 사용중인 하드웨어나 소프트웨어 자원을 수정하지 않고 그대로 사용할 수 있다. 반면에, OSI 관리 모델은 객체지향 방식을 사용하고 있기 때문에 현존하는 소프트웨어의 설계를 변경해야 하는 단점을 가지고 있다. 또한 OSI 관리 모델의 일관성을 유지하기 위한 MIB 구현에 많은 부담을 갖게 된다[1, 4, 5]. 그러나 SNMP가 현재 널리 사용되고 있지만 몇 가지의 단점을 가지고 있기 때문에 미래에는 더 강력한 망관리 패러다임이 필요하다.

OSI 망관리와 널리 사용되고 있는 TCP/IP 인터네트를 상호 연결하기 위한 방법으로 한 지점에서 모든 망을 통합 관리하는 방법과 두 영역에서 접근할 수 있는 중복된 이중 MIB를 두어 관리하는 방법, 프로토콜 독립 대행자와 MIB를 사용하는 방법, 두 영역간에 프로토콜 변환에 의해서 망을 관리하는 응용 게이트웨이를 설치하는 방법 등이 있다[6, 7, 12]. 실시간 환경에서 OSI 망과 인터네트의 구조와 MIB를 변경하지 않고 상호 연결할 수 있는 패러다임인 응용 게이트웨이가 효율적이고 안전한 기능을 지원하기 위해서는 위임과 보안 기능이 필요하다.

본 논문에서는 CMIP의 강력하고 융통성이 있는 서비스와 관리 기능을 변환하고, 관리자의 미사용타로 인한 과부하를 받는 경우나 응급 상황에 따라 관리자로부터 전달된 위임 기능을 처리하고, 필요에 따라서 관리 스크립트를 생성하고 제어하는 응용 게이트웨이를 설계하였다. Diffie-Hellman의 키 분배 방식을 기반으로 하여 관리 서비스와 기능을 안전하게 전달하는 알고리즘을 제안하고, 서로 다른 보안 정책을 사용하는 두 영역간에 관리 객체의 접근을 제어하는 접근 제어 정책을 제시한다.

본 논문의 구성은 2장과 3장에서 관련 연구와 위임기능, 접근 제어가 지원되는 응용 게이트웨이의 구조를 소개한다. 4장에서는 서비스의 사상과 위임 기능, 접근 제어 정책 사상을 언급한다. 5장에서는 정성적으로 비교 분석하고, 끝으로 6장에서는 결론과 향후 연구 방안을 제시하였다.

2. 관련 연구

2.1 OSI과 TCP/IP 망의 상호 연결

SNMP와 CMIP의 통합에 관련된 문제와 전략, 기술에 대해서는 많은 연구가 있었다. Rose는 TCP/IP 기반 인터네트와 OSI 망 관리를 위한 전이(transition)와 공존(coexistence)에 대한 방법을 제안하였다[13]. 그의 논문은 인터네트와 OSI 프로토콜간에 전이와 공존이 가능한 방법을 프로토콜 기반 접근인 이중 스택 접근과 응용 게이트웨이 접근과, 전송 프로토콜 변환과 서비스 기반 접근인 TCP/IP 기반 망에서의 OSI 응용 실행과 전송 서비스 브리지, 망 서비스 터널로 나누어 기술하였다. Mazumdar은 SNMP와 CMIP 프로토콜을 지원할 수 있는 프로토콜 독립 관리 대행자/MIB의 구조를 제안하였다[7]. 이 접근방법은 다중 이름 등록 테이블을 사용하여 관리 객체들로 구성된 단일 프로토콜 독립 MIB가 어떻게 사용되는지와 CMIP MIB 구조를 SNMP MIB 구조로 변환하는 방법을 제안했다. Wu와 Mazumdar는 프로토콜 독립 MIB 객체를

위한 SNMP 프로토콜 객체 처리기를 제안하고 구현하였다. 프로토콜 독립 MIB의 생성은 CMIP와 SNMP 모두를 동시에 지원하기 위해 고안되었지만 현재는 SNMP만을 지원하는 객체 처리기를 구현하였다[7, 14, 15].

Kalyanasundaram과 Sethi는 OSI와 인터네트 연동관리를 위한 세가지 패러다임을 제시하고 응용 게이트웨이에 대한 이름과 인스턴스 사상, 기능 사상을 제안하였고[6], Abeck과 Clemm, Hollberg는 중개인 역할을 하는 게이트웨이를 사용하여 통합 모델인 CMIP에 SNMP를 연결하는 접근 방법을 제시했다[1]. Park과 Jung, Sunwoo는 OSI 망 관리와 TCP/IP 인터네트 관리의 통합 방법을 제안하고, 관리 응용 서비스를 제공하기 위한 소프트웨어 구조와 알고리즘을 제시하였다[9].

초고속 망에서 운용 보존 뿐만 아니라 망에 연결된 시스템에 대한 실시간 관리가 매우 중요하다. 위에 기술된 관련 연구들에서는 이기종망간에 상호 연결을 위한 게이트웨이의 기본적인 서비스와 기능 사상 방법 및 프로토콜 독립 관리 대행자를 두어 상호 연동시키는 방법에 대해서만 언급되었고, 응용 게이트웨이에서의 통신 비용과 지연 문제에 대해서는 고려하지 않았다. Yemini 등에 의해서 제시된 위임 기능은 동기종간인 관리자와 대행자 사이에 적용되고 있으며, 이기종망간에 위임 기능이 제공되는 접근 방법은 제시하지 않았다[6, 16].

2.2 안전한 위임 기능

관리자는 관리 제어를 요청한 후 결과가 도달할 때까지 대기하거나 모든 관리 행위에 대한 통제를 담당한다. 이러한 관리 행위를 미시 관리(micro management)라 하며, 미시 관리에는 많은 관리 정보의 교환으로 인한 통신량 과부하가 발생한다. 이러한 과부하를 줄이기 위한 많은 연구가 진행되어 왔으며, 그 중의 한 방법으로 Yemini등에 의해서 위임 모델이 제시되었다[16]. 이러한 위임 모델에서 관리 객체에 적용할 감시나 통제, 동작등을 기술하기 위해서는 관리 기술 언어(management scripting language)를 사용한다. 관리 기술 언어를 사용하여 관리 행위를 기술하는 것을 관리 스크립트라고 한다. 위임 모델에서 관리자는 필요에 따라서 대행자에게 스크립트의 수행을 위임함으로써 관리자와 대행자 간에 통신량을 현저하게 감소시킬 수 있다.

스크립트 관리를 위해서 제공되는 서비스는 스크립트 수행의 위임 및 위임 통지, 위임 해지, 관리 스크립트의 수정 및 수정 통지, 위임된 스크립트의 중지 및 재개 등으로 이루어진다. 이러한 스크립트는 관리자와 게이트웨이, 게이트웨이와 대행자간에 안전하게 전달되어야 하는데, 아래와 같이 위임 증명서(delegation certificates)를 사용하여 관리 스크립트를 전달하면 된다.

$$C_{M,D}=\{M_s, M_d, P_r, R, T_{time}, T_{task}\}$$

$C_{M,D}$는 관리자 M_s가 위임 스크립트 T_{task}를 수행하기 위해서 시간 T_{time} 동안 대행자(또는 게이트웨이) M_d에게 권한 P_r를 위임하는 것을 의미한다. 관리자 M_s는 관리자의 식별자로서 관리자의 신원을 확인하는데 사용된다.

M_d는 관리자가 보낸 위임 증명서를 받는 수신측 식별자로 사용된다. P_r은 대행자가 수행할 수 있는 제어 권한을 나타낸 것이며, R은 재전송을 막기 위해서 관리자가 생성한 난수값이다. 그리고 T_{time}은 위임 스크립트를 수행할 수 있는 기간을 지정한 것이고, T_{task}는 실제로 수행될 관리 기능을 지정한 것이다. 위임 증명서내의 이러한 정보는 비밀키에 의해서 암호화되어 전달되기 때문에 침입자가 알 수 없게 된다.

이와 같은 위임 증명서를 안전하게 전달하기 위해서 Diffie-Hellman 키 분배 방식을 사용하기 때문에 관리자와 게이트웨이, 게이트웨이와 대행자 사이의 다음과 같은 준비 단계가 필요하다[3].

▩ 준비 단계 1(임의의 솟수 N을 생성)
$N=P_i\ [1 \le i \le n]$
여기에서 P_i는 임의의 큰 솟수이다.
▩ 준비 단계 2(암/복호화 키(e, d)를 생성)
$e*d=1(\text{mod } N)\ [0 \le e, d \le 2^n-1]$

단계 2는 단계 1에서 생성한 솟수를 이용하여 암호화 키(e)와 복호화 키(d)를 생성하는 과정이다. 임의의 두 수를 곱한 결과를 솟수 N으로

나눈 다음 나머지가 1이 되는 것을 찾아 암호화 키와 복호화 키로 사용한다.

▨ 준비 단계 3(게이트웨이 비밀 정보(Sg)를 생성)

$$\alpha^{Sg} \equiv ID_g^e \pmod N$$

단계 3은 응용 게이트웨이의 식별자 ID와 를 이용하여 게이트웨이의 비밀 정보를 생성하는 과정이다. 여기에서는 유한체 GF(P_i)에 의해서 산출한 원시 원소이다.

▨ 준비 단계 4 (공개 정보 T를 생성)

$$T = \alpha^{-d} \bmod N$$

T는 공개 정보로 사용되는데, 복호화 키(d)와 원시 원소 에 의해서 구해진다. 그리고, 임의의 난수 r과 일방향 함수 h(x), 현재의 시간 t를 산출한다.

위 준비 과정을 통해서 생성된 정보들 중에서 d, T, N은 관리자 자신만이 알고 있어야 하는 비밀 정보이고, h( ), α, N, e는 관리자외의 다른 사용자들이 알게 되더라도 보안성은 유지되므로 공개하는 정보이다. 그리고, S_g는 게이트웨이만이 알고 있어야 하는 비밀 정보이고, 식별자 ID_g는 게이트웨이가 공개하는 정보를 나타낸다.

2.3 보안 정책

(1) 단순 보안 성질

단순 보안 특성은 주체(S)의 보안 등급이 객체(O)의 보안 등급보다 같거나 크면 읽기 접근을 허용한다. 이러한 성질은 낮은 보안 등급을 갖는 주체로부터의 읽기 접근을 방지하는 규칙이다. 아래 규칙에서 M은 연산들을 나타낸다. 이 규칙은 조건식을 만족하면 참이 되고 만족하지 않으면 거짓이 된다[8, 10, 11].

$$R(S, O, m) = \begin{cases} \text{true if } m \in \text{ .and. } C(S) \geq C(O) \\ \text{false otherwise} \end{cases}$$

(2) *- 보안 성질

*- 보안 성질은 주체(S)의 보안 등급이 객체(O)의 보안 등급보다 같거나 낮은 경우에만 쓰기 접근이 허용된다. 이러한 성질은 정보가 낮은 보안 등급으로 흐르는 것을 방지하는 규칙이다[8, 10, 11].

$$R(S, O, m) = \begin{cases} \text{true if } m \in \text{ .and. } C(S) \geq C(O) \\ \text{false otherwise} \end{cases}$$

(3) 자율적 보안 성질

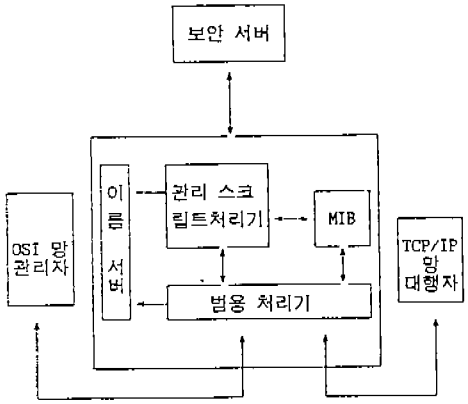
자율적 보안 성질은 접근 제어 리스트(ACL) 기반 정책과 역할 기반 정책을 사용하여 주체(S)의 객체(O)에 대한 접근 허용을 결정한다. 이 규칙은 주체(S)가 객체(O)를 접근 가능하거나 주체(S)의 역할이 객체(O)에 대한 접근이 가능하면 참이 되고 그렇지 않으면 거짓이 된다[8, 10, 11].

$$R(S, O, ACL, m) = \begin{cases} \text{true if } m \in \text{ .and. } (\{S,m\} \in ACL(O) \text{ or } \{S \in R \text{ .and. } \{R,m\} \in ACL(O)\}) \\ \text{false otherwise} \end{cases}$$

3. 응용 게이트웨이

3.1 안전한 응용 게이트웨이

여러 영역간에 효율적인 망 관리를 위해서는 통합 관리가 필요하다. 이러한 구조에서 관리자와 대행자의 관계뿐만 아니라 관리자들을 관리하는 상위 관리자와 하위 관리자의 관계가 있을 수 있다. 본 논문에서는 이러한 환경에서 안전한 위임 기능과 보안 성질을 기반으로 하여 서로 다른 영역간을 상호 연동시키는 응용 게이트웨이를 설계했다.



(그림 1) 응용 게이트웨이 구조
(Fig. 1) application gateway architecture

이기종망간에 각자의 망관리 구조를 변경하지 않고 모든 망을 관리할 수 있는 패러다임은 여러 가지가 있다. 그 중에서 OSI 망과 TCP/IP 인터네트를 효율적이고 간단하게 상호 연동시키는 응용 게이트웨이의 구조는 (그림 1)과 같다.

이 구조에서 OSI 영역 내의 관리자는 인터네트 대행자의 구조나 프로토콜에 관계없이 인터네트 노드를 관리할 수 있게 된다. 응용 게이트웨이는 한쪽에 OSI 영역과 연결되고 다른 한쪽에는 인터네트 영역과 연결된다. 만일 게이트웨이가 CMIP 요청을 받게 되면 그 출력은 SNMP 요청으로 변환된다. 또한 SNMP측으로부터 응답/트랩을 받으면 OSI측에 CMIP 응답을 보낸다.

이 구조는 많은 융통성과 효율성을 제공하지만 단점으로는 응용 게이트웨이의 복잡도가 증가한다는 것이다. 즉, CMIP는 패킷 크기에 제한을 받지않지만 SNMP에서는 패킷 크기에 제한을 받기 때문에 OSI측에서 단일 요청은 인터네트측에서는 몇 개의 다중 요청으로 변환해야한다. 이러한 경우에 게이트웨이는 OSI측의 각 요청 상태를 유지하고 인터네트 영역으로부터 몇 개의 응답을 모은 다음 하나의 CMIP 응답으로 바꾸어서 보내야하기 때문에 게이트웨이가 많은 부담을 받게 된다. 본 논문에서는 이러한 문제를 해결하기 위해 복잡한 기능을 관리 스크립트에 의해서 대행자에게 위임하는 메카니즘이 지원될 수 있도록 하였다.

(그림 1)과 같이 응용 게이트웨이는 관리자에 대해서는 대행자 역할을 하고 대행자에 대해서는 관리자 역할을 한다. 결국 중간에서 전달 역할을 하는 응용 게이트웨이는 관리자가 사용하는 프로토콜과 대행자가 사용하는 프로토콜이 서로 다르기 때문에 변환 역할과 관리자의 신분 확인, 보안 정책을 조정하는 역할을 한다.

응용 게이트웨이의 구조는 범용 처리기와 관리 스크립트 처리기, 이름 서버, MIB로 구성된다. 범용 처리기는 이름 서버와 관리 스크립트 처리기 사이에 2단계 완료(2 phase commit) 단계로 구성되며, 기본적인 프로토콜 서비스와 관리 스크립트를 번역하고 변환하는 역할을 담당한다. 위임 기능에 관한 경우에는 관리 스크립트를 번역하고 변환하기 위해 관리 스크립트 처리기에게 관리 스크립트를 보낸다. 범용 처리기는 이름 서버에 의해서 관리 객체의 실제 인스턴스의 주소를 가져온다. 기본적인 서비스나 관리자로부터 보내온 관리 스크립트는 대행자의 프로토콜에 맞게 직접 변환하여 전달하고 그 응답만을 기다린다. 관리 스크립트 처리기에게 요청한 관리 스크립트는 관리 스크립트 테이블을 탐색하고 테이블에 없으면 테이블에 저장하고, 존재하는 경우에는 관리 스크립트에 변환 과정을 거치지 않고 대행자에게 전달하고 응답만을 기다리면 된다.

이름 서버는 범용 처리기로부터 받은 관리 객체 명칭과 속성에 대한 제약조건을 가지고 실제 관리 대상 인스턴스를 알아내기 위해 디렉토리 서비스를 호출한다. 디렉토리는 모든 관리 객체에 대한 저장소이고 디렉토리 서비스는 실제 인스턴스의 주소를 생성하여 이름 서버에게 전달하는 기능을 한다. 또한 관리 스크립트 처리기는 복잡한 OSI 관리 기능을 범용 처리기의 요청에 의해서 관리 스크립트를 번역하여 스크립트 테이블에 저장하고 범용 처리기에게 전달해 주는 기능을 한다. 응용 게이트웨이는 범용 처리기와 관리 스크립트 처리기, 이름 서버에 의해서 CMIP와 SNMP 사이에 명칭과 주소, 서비스 변환을 수행한다. 실제 사상은 객체에 대해 직접 일대일 사상이 되거나 인터네트 MIB의 특성에 따라 서로 다르게 사상될 수 있다.

3.2 안전한 위임 기능 전달 알고리즘

관리자가 대행자(게이트웨이)에게 위임 기능을 안전하게 전달하려면 위임 증명서를 암호화하여 전달해야 하는데 위임 증명서의 생성 알고리즘은 다음과 같다[3].

임의의 난수 r과 일방향 함수 h(t)를 계산한다. 여기에서 t는 현재의 시간을 나타낸다. 그 다음에 요청 프로세스는 다음과 같이 대행자 g에 대해서 IC1, IC2와 관리자와 대행자간의 비밀키 $K_{M,G}$를 계산한다.

▩ 암호화 알고리즘 : $E_M(ID_M, ID_g, t, C_{M,D})$

① $D_{M,D}=C_{M,D}$

② $IC_1=\alpha^r \bmod N$

③ $IC_2=T^{S_M} \cdot \alpha^{h(t.C_1)r} \bmod N$

④ $K_{M,B} = (ID_S)^{IC_2} \bmod N$

⑤ $C_{M\&D} = K_{M,B} \oplus D_{M\&D}$

$C_{M\&D}$는 위임 증명서를 나타내고, IC_1과 IC_2는 관리자에 의해서 구해진 특정 값이다. S_M은 2.2절의 $\alpha^{SM} \equiv ID_S \pmod N$에 의해서 구해진 관리자의 비밀 정보이고, $K_{M,B}$는 관리자와 대행자(또는 게이트웨이)간의 비밀 공유키이다.

대행자에 의해서 관리자가 보낸 메세지를 복호화하는 알고리즘은 다음과 같다. 대행자는 관리자로부터 받은 정보를 이용하여 식별자를 인증한다음 요청 프로세스의 식별자와 자신의 비밀 정보 S_B를 사용하여 요청 프로세스와 자신과의 공유키 $K_{M,B}$를 생성한다. 여기서 t는 재전송방지를 위해 사용된 타임스탬프이다.

※ 복호화 알고리즘 : $D_M(ID_M, IC_1, IC_2, t, C_{M\&D})$

① $\frac{(IC_2)}{(IC_1)^{ID_M}} \bmod N = ID_M \bmod N$

② 만일 ①의 식이 성립하면 ③으로 가고, 성립하지 않으면 불법적인 사용자로 간주한다.

③ $K_{M,B} = (IC_1)^{S_B} \bmod N$

④ $C_{M\&D} = K_{M,B} \oplus C_{M\&D}$

⑤ $C_{M\&D}$에 명시된 접근 제어 정책을 비교한다.

3.3 서버의 보안 성질

(1) 쓰기 보안 특성

이 보안 특성은 주체(S : 관리자)의 보안 등급이 객체(O : 대행자)의 보안 등급과 같거나 클 경우, 또는 주체와 객체에 대한 접근 허용이 접근 제어 리스트(ACL)에 존재하거나, 주체의 역할(R)이 객체에 대해서 타당하고, S가 O의 관리자이면 M-SET, M-ACTION, M-CREATE, M-CANCEL-GET, M-DELETE 서비스를 허용한다. 이 규칙은 같은 영역에 있는 관리자와 대행자 사이에서만 적용되는 보안 특성이다.

여기에서 m은 관리 연산, 즉 M-SET(w)과 M-ACTION(ac), M-CREATE(cr), M-CANCEL-GET(cr), M-DELETE(de)를 의미하고 "S∈R .and. (R,m) ∈ CLR(O)"은 역할 기반 접근제어 정책이다. ancestor(S,O)는 S가 O에 대해서 상위 관리자나 관리자의 역할을 하는 것으로 정의한다.

R1(S, O, R, ACL, m) =

⎧ true if m={w, ac, ca, cr, de}. and.
⎪ <C(S)≥C(O)or(S,m)∈ACL(O)or
⎪ {S∈R' .and. (R,m)∈ACL(O)}>
⎪ .and. ancestor(S, O)
⎩ false otherwise

(2) 읽기 보안 특성

읽기 보안 특성은 주체(S : 관리자)의 보안 등급이 객체(O : 대행자)의 보안 등급과 같거나 크고 주체와 객체에 대한 접근 허용이 접근 제어 리스트(ACL)에 존재하거나, 주체의 역할이 객체에 대해서 타당하면 M-GET 서비스를 허용한다. 이 규칙은 서로 다른 영역에 있는 관리자와 대행자 사이에 요청자와 응답자 사이에 접근 보안 특성을 만족하면 읽기 접근을 허용하는 보안 특성이다.여기에서 m은 관리 연산, 즉 M-GET(r)를 나타낸다.

R2(S, O, R, ACL, m) =

⎧ true if m={w, ac, ca, cr, de}. and.
⎪ <C(S)≥C(O)or(S,m)∈ACL(O)or
⎪ {S∈R' .and. (R,m)∈ACL(O)}>
⎪ .and. ancestor(S, O)
⎩ false otherwis

(3) 사건보고 보안 특성

사건보고 보안 특성은 객체(O : 대행자)의 보안 등급이 주체(S : 관리자)의 보안 등급과 같거나 클 경우, 또는 주체와 객체에 대한 사건보고 허용이 접근 제어 리스트(ACL)에 존재하거나, 주체의 역할이 객체에 대해서 타당하고 주체 S가 객체 O의 후손이면 EVENT-REPORT나 TRAP 서비스를 허용한다.

이 규칙은 관리자와 대행자 사이에서 적용되는 보안 특성으로서 관리 객체에 사건이 발생했을 경우에 적용되는 보안 특성이다.

여기에서 m은 SNMP 관리 연산, 즉 Trap(e)를 의미하고, descendant(S,O)는 S가 O에 대해서 직계 대행자나 하위 대행자의 역할을 하는 것으로 정의한다.

R3(S, O, R, ACL, m)=

true if m={w, ac, ca, cr, de}. and.
<C(S)≥C(O)or(S,m)∈ACL(O)or
{S∈R' .and. (R,m)∈ACL(O)}>
.and. ancestor(S, O)
false otherwise

4. 서비스와 위임 기능 사상

이 장에서는 OSI 망관리에 사용되는 기본적인 서비스 요소와 고급 서비스인 범위 지정, 필터링, 동기화를 TCP/IP 인터네트의 관리에서 지원하는 알고리즘을 제시한다. SNMP 대행자와의 상호작용을 위해서는 SNMP 서비스는 신뢰할 수 없는 UDP의 데이타그램을 기반으로 하고 있으며, 타임아웃과 요청 재전송 메카니즘은 미결의 통보를 조절하기 위해 필요하다.

4.1 서비스 사상

OSI와 TCP/IP 인터네트 관리 모델에서는 관리자와 대행자간의 상호 교환 프리미티브(primitive)를 통해서 관리를 수행한다[9].

(1) 관리 객체 속성 지정과 검색

MIB에 저장되어 있는 관리 객체 속성 지정과 검색을 위한 관리 서비스는 M-SET과 M-GET, SET과 GET는 각각 CMIP와 SNMP에 대응된다. 응용 게이트웨이가 M-SET-indication과 M-GET-indication을 OSI로부터 받을 경우에 SNMP측에 대해서는 하나 이상의 SET-requests와 GET-requests를 생성한다. 게이트웨이가 SNMP 대행자의 응답(SET-response와 GET-response)들을 기다려야 하고 원하는 모든 응답을 받은 경우에는 CMIP 서비스 프리미티브인 M-SET-response와 M-GET-response로 사상한다. 예를 들어 CMIP를 SNMP서비스로 사상하는 알고리즘은 아래와 같다.

```
int i;
for(i=1; i< M; i++)
    GET(get) ;
```

(2) 관리 객체 인스턴스의 생성과 제거

SNMP는 인스턴스의 생성과 제거 서비스가 존재하지 않는다. 그래서 제거 기능은 SET서비스를 사용하여 객체 인스턴스의 필드를 거짓으로 지정하면 CMIP의 M-DELETE의 서비스의 기능이 되고, 생성 기능은 객체 인스턴스의 필드를 참으로 지정하면 CMIP의 M-CREATE 서비스의 기능이 된다.

(3) 관리 행위 시작

CMIP에서 관리 행위를 시작하기 위해서는 M-ACTION을 사용한다. SNMP에서의 행위 기능은 객체 인스턴스의 필드에 특정 값을 지정하면 된다.

(4) 사건과 통보

사건 감시와 긴급한 상황의 통보에 대해서는 CMIP와 SNMP가 서로 다른 서비스를 가지고 있다. CMIP는 사건 감시를 M-GET이나 M-EVENT-REPORT를 사용하고 SNMP는 TRAP을 사용한다.

4.2 위임 기능 사상

4.2.1 고급 CMIP 기능 사상

응용 게이트웨이의 변환 과정과 서비스 상태를 유지해야하는 부담을 줄이기 위한 관리 스크립트를 생성하고 전달하는 알고리즘은 다음과 같다.

▩ 위임 프로토콜

① 범용 처리기는 위임 프로그램 생성기에게 위임 프로그램을 요청한다.

② 위임 프로그램 처리기는 스크립트 테이블을 검색하여 대응되는 위임 프로그램가 있으면 그 스크립트를 범용 처리기에게 전송한다. 그렇지 않으면 스크립트를 생성하여 테이블에 저장한 다음 범용 처리기에게 전송한다.

③ 범용 처리기는 위임 프로그램을 관리 서비스와 구분시켜서 대행자에게 전송한다.

④ 위임 프로그램 스케줄러에 의해서 위임 프로그램의 수행을 제어한다. 즉, 위임 프로그램 처리기는 관리자가 요청하는 위임, 위임취소와 수정, 재개 그리고 중지 등과 같은 위임 프로그램 서비스를 제어한다.

SNMP에서는 제공되지 않는 범위 지정, 필터링, 동기화와 같은 고급 CMIP 기능을 관리 스크립트로 바꾼 다음 대행자에게 위임한다.

정보 상태를 유지하는 게이트웨이가 개념적으로 대행자의 완전 포함(complete containment) 트리를 이용할 수 있기 때문에 간단하게 게이트웨이 구현에 의해서 모든 범위 지정이 가능하다. CMIP에 의해서 제공되는 또 다른 고급 서비스로서 필터링과 동기화가 있다. 필터링은 주어진 조건에 만족하는 관리 객체를 선택하도록 허용하는 서비스이다. 이러한 조건이 범위 지정된 관리 객체에 적용된다. 이러한 방법에 필터링 메카니즘은 관리자 시스템으로부터 적합한 객체 값만을 받도록 함으로써 통신량 과부하를 줄일 수 있다. 필터링 기능은 SNMP와 호환성을 유지하지 않기 때문에 SNMP에서 필터링 기능을 지원해주는 알고리즘이 필요하다. 동기화는 범위 지정과 필터링에 의해 관리 객체의 조건이 정해지고 이들이 결정되면, 수행 대상인 관리 객체들의 순서가 정해지게 되는데 이것을 동기화라고 한다. 사용자는 원자성(atomicity), 최선책(best effort) 방식의 동기화 중 하나를 사용할 수 있다.

4.2.2 관리 스크립트 사상

스크립트 관리 기능은 관리자가 다른 관리 기능 수행으로 인해 특정한 관리 기능을 수행할 여유가 없는 경우나 과도한 관리 통신량으로 인한 시스템의 부담을 줄이고자 할 경우에 관리 스크립트의 수행을 대행자 시스템으로 위임하는데 사용한다. CMIP와 게이트웨이 간에 전달되어 오는 관리 스크립트는 CMIP 대행자에 해당하기 때문에 게이트웨이는 SNMP 대행자에 적용될 수 있는 관리 스크립트로 변환한 다음 대행자에게 전달해야 한다.

OSI에서 전달한 관리 스크립트는 SNMP에서 이해할 수 있도록 변환된 관리 스크립트는 다음과 같다[16].

■ SNMP 대행자가 실행할 스크립트

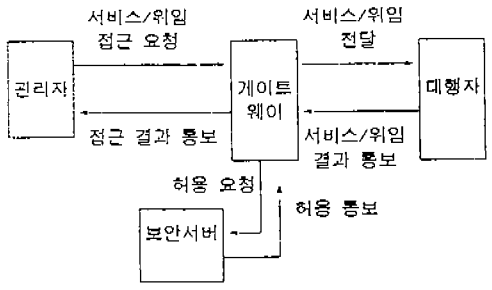
```
int link_congestion, flag, i;
  // 링크의 혼잡도 측정

flag = 0;
link congestion = 0;
while(1)
{
for(i=1; i< M; i++)
  GET( get );
    // 각 장치들의 상태 정보 접근
if(get_params == 1) flag = 1;
    // 혼잡도 측정/비교
link—congestion = flag;
if(link—congestion) break;
    // 각 장치들에 대한 상태 정보 접근
       종료
}
for(i=1; i< M; i++)
  SET(log—file); // 로그 화일에 기록
M—EVENT—REPORT(CMIP—Event);
    // 관리자에게 결과 통보
}
```

수신된 알고리즘의 M-GET()과 M-SET()은 사건 발생의 감시하는 서비스와 사건에 대한 복구를 수행하는 서비스이기 때문에 해당되는 관리 객체의 인스턴스 수만큼 반복 수행하는 과정을 for문으로 구성하였다.

4.3 접근 제어 사상

게이트웨이에 서비스나 위임 기능을 받은 경우에 기능 변환 뿐만 아니라 불법적으로 관리 객체를 접근하는지의 여부를 확인하는 과정이 필요하다. (그림 2)는 응용 게이트웨이와 보안서버의 관계를 나타낸 것이다.

서로 다른 접근 제어 정책을 사용하는 단일 시스템이나 분산 시스템이 새로운 분산 시스템을 구성하기 위해 상호 연동 시키는 경우에 보안 위



(그림 2) 보안 서버 역할
(Fig. 2) Security server roles

험이 야기된다. 따라서 이러한 환경에서 안전하게 정보가 전달될 수 있도록 자율적 접근 제어와 강제적 접근 제어 정책이 적절하게 사상되어야 한다. 관리자 측에서 사용하고 있는 정책과 대행자 측에서 사용하고 있는 정책이 서로 다른 경우는 보안 서버에 의해서 조치가 취해지게 된다. 그리고 접근 제어 정책의 특성에 따라 응용 게이트웨이는 자원 공유를 허용하여 역할기반 분산 시스템의 장점을 효율적으로 이용할 수 있다.

이 장에서는 관리자와 대행자간에 모든 서비스와 위임 기능에 대한 접근 제어를 사상하는 안전한 망관리가 이루어질 수 있는 메카니즘을 설명한다.

(1) M-GET 연산

M-GET 연산은 같은 영역(domain)이나 다른 영역에 있는 주체(S)와 객체(O)의 관계가 선조나 후손인 경우는 주체 S를 그대로 사용하여 GET 서비스를 사상하고 그렇지 않는 경우는 주체 S를 관리자로 대치하여 사상한다. 예를 들어 선조 관리자가 아닌 관리자가 다른 영역에 있는 정보를 접근하기 위해서는 자신의 관리자에게 원하는 정보를 접근하여 그 결과를 보내주도록 하는 방법이다. 위의 두 조건을 만족하지 않는 경우는 거절을 한다. 여기에서 CLR()은 게이트웨이에 의해서 대행자의 보안 정책을 변환할 경우에 보안 등급이나 접근 리스트, 역할 등을 나타낸다. R2는 3.3절의 규칙이다. ACL은 접근어 리스트이고 CLS는 접근 허용을 나타낸다.

```
if(S Sset .and. O Oset .and.
        R2(S, O, R, ACL, m))
  then if ancestor(S,O)
    then issue( S, O, M−GET, CLR(S))
  else reject
```

(2) M-SET 연산

M-SET 연산은 쓰기 연산으로서 3.3절의 규칙 R1이나 R3을 만족하는 경우에 SET 서비스를 사상한다.

```
if(S Sset .and. O Oset .and.(R1(S, O, R,
     ACL, m) or R3(S, O, R, ACL, m)) )
then issue( S, O, M−SET, CLR(S) ) )
else reject
```

(3) M-ACTION 연산

M-ACTION 연산은 3.3절의 규칙 R1을 만족하는 경우로서 관리자가 대행자에게 요청하는 연산이다.

```
if(S Sset .and. O Oset .and.
        R1(S, O, R, ACL, m))
then issue(S, O, M−ACTION, CLR(S))
else reject
```

(4) M-DELETE 연산

M-DELETION 연산은 (3)과 같이 3.3절의 규칙 R1을 만족하는 경우로서 관리자가 대행자에게 요청하는 연산이다.

```
if S Sset .and. O Oset .and.
        R1(S, O, R, ACL, m))
then issue( S, O, M−DELETE, CLR(S) )
else reject
```

(5) Trap 연산

Trap은 사건 발생시에 관리자에게 통보하는 연산으로서 3.3절의 규칙 R3을 만족했을 경우만 가능하다.

```
if(S Sset .and. O Oset .and.
        R3(S, O, R, ACL, m))
then issue( S, O, Trap, CLR(S) )
else reject
```

(6) EVENT-RECOVERY 연산

EVENT-RECOVERY 연산은 (5)에 대한 복구 조치로서 3.3절의 규칙 R1을 만족하고 로그화일에 사건 발생에 대한 쓰기 연산이 있는 경우에 가능한 연산이다.

```
if( S Sset .and. O Oset .and.
R1(S, O, R, ACL, m) .and. O−event LOG )
  then issue( S, O, M−SET, CLR(S))
  else reject
```

관리자와 대행자간에 이와 같은 제약조건을 사용함으로써 통신량을 줄이고 망관리가 안전하게 이루어질 수 있게 된다.

5. 결과 분석

응용 게이트웨이에 위임에 의한 관리기능과 보안 기능을 첨가함으로서 전체적인 분산 망 관리의 효율성과 안전성을 보장할 수 있었다. 기존의 응용 게이트웨이에 의한 상호연동 패러다임 환경에서 관리자는 원거리 응답을 기다리는데 상당히 많은 시간을 소비하기 때문에 통신량과 통신 지연이 비교적 긴 망을 관리하는 것은 비효율적이다. 기존의 응용 게이트웨이를 사용함으로서 야기되는 문제점은 개략적으로 살펴보면 다음과 같다.

첫째, 실시간 환경에서 장애 발생을 통보하는 경우에 인터네트 관리 모델은 폴링 방법을 사용하는 반면에 OSI 모델은 사건위주 방법을 사용하기 때문에 기존의 응용 게이트웨이는 서로 다른 망을 효율적으로 관리하는데 제약을 받는다.

둘째, 관리 객체를 검색하거나 지정하는 경우도 인터네트 모델에서는 OSI망 관리 모델에서 지원하는 범위지정과 필터링, 동기화와 같은 기능을 지원하지 않기 때문에 응용 게이트웨이는 에뮬레이션의 기능을 제공해야 한다. 예를 들면, CMISE의 M-GET 서비스에 대해서 관리자와 게이트웨이간에는 한번의 서비스로 관리 요청이 가능하지만, 응용 게이트웨이와 대행자간에는 여러번의 서비스로 변환하여 요청해야 되는 경우에는 중계 역할을 담당하는 응용 게이트웨이는 에뮬레이터의 역할을 해야 한다.

세째, 관리자는 직접 모든 관리 행위에 대한 통제를 담당함에 따라 관리국의 통신량 폭주와 관리 행위에 대한 응답을 기달려야 하는 문제가 발생한다.

넷째, 관리국과 게이트웨이에서 관리 정보를 계산하고 분석하기 때문에 많은 처리 비용이 든다.

다섯째로, 관리자와 대행자간에 안전한 관리 정보의 교환을 기대하기 어렵다.

관리자가 직접 관리 행위를 제어하지 않고 통신량과 업무에 따라 대행자에게 관리 행위를 위임함으로서 망 전체의 통신량과 관리국의 미시관리로인한 병목현상을 줄였다. 또한 보안 기능을 첨가로 인해 안전한 관리 행위를 보장하였다. 〈표 1〉은 기존의 응용 게이트웨이와 개선된 응용 게이트웨이를 정성적으로 분석한 결과이다. 개선된 응용 게이트웨이는 〈표 1〉과 같은 장점을 얻을 수 있었지만 위임과 보안 기능을 첨가함에 따라 시스템 구현에 있어서 부가적인 부담을 갖게 된다.

〈표 1〉 기존의 응용 게이트웨이와 개선된 응용 게이트웨이의 비교

〈table 1〉 Comparison of existed application gateway with advanced application gateway

구 분		기존의 응용 게이트웨이	개선된 응용 게이트웨이
서비스 측 면	관리 기능 전달 방법	사상	사상/위임
	서비스 교환 횟수(통신량)	1 : N	1 : 1
	응용 게이트웨이의 계산과 판단 부담	많음	적음
	실시간 관리 적용	불가능	가능
	관리자는 요청에 대한 응답 대기	필요	불필요
	대행자의 계산부담	적음	많음
	에뮬레이션 기능	필요	불필요
	관리기능	무변화	무변화
	관리행위 통제 장소	관리자측	관리측/대행자측
	범위지정, 필터링, 동기화 기능의 제공	제공하지 않음	간접적으로 제공
MIB 측면	게이트웨이내에관리객체에 대한 개념적인 상태 유지	필요	필요
	위임 관리 스크립트 테이블	유 지 하 지 않음	유지함
보안 측면	보안 서비스 지원	인증	인증, 접근제어
	암호화	제 공 하 지 않음	연결접속시 통신키 수령

6. 결 론

OSI망과 TCP/IP 인터네트를 통합하기 위해서 강력하고 융통성이 있는 패러다임인 응용 게이트웨이가 사용되고 있지만 게이트웨이가 응급 상황에서 통신 지연과 비용으로 인하여 성능이 저하된다. 또한 서로 다른 보안 정책을 사용하는 두 영역간에 접근 제어 정책을 사상하는 메카니즘이 필요하다. 이러한 문제는 서로 다른 표준으로 구성된 두 영역을 통합하는 데서 야기된다.

본 논문에서는 CMIP의 강력하고 융통성이 있는 서비스뿐만 아니라 관리 기능을 변환하고, 시간 제한을 받는 응급상황에 따라 관리자는 대행

자에게 관리를 위임하는 기능을 지원하는 응용 게이트웨이를 설계하였다. Diffie-Hellman의 키 분배 방식을 기반으로 하여 관리 서비스와 관리 스크립트가 안전하게 전달될 수 있도록 송신측을 인증하고, 메세지의 노출을 방지하였으며, 약한 접근제어 정책을 사용하여 두 영역간에 안전한 통신이 이루어질 수 있도록 하였다. 기존의 응용 게이트웨이와 개선된 응용 게이트웨이를 정성적으로 분석한 결과와 같이 개선된 응용 게이트웨이는 안전성과 효율성에 있어서 많은 이점을 얻을 수 있었다. 앞으로의 연구 과제는 위임과 보안 기능이 지원되는 응용 게이트웨이의 성능평가에 관한 연구가 뒤따라야할 것으로 사료된다.

참 고 문 헌

[1] S. Abeck, A. Clemm, U. Hollberg, "Simply Open network Management : An Approach for the Integration of SNMP into Management concepts", Proc. 3rd International Symposium on Integrated Network Management, pp. 361-374, April 1993.

[2] M. Gasser, Ellen McDermott, "An Architecture for Practical Delegation in a Distributed System", 1990 IEEE Computer Society symposium on Security and Privacy, pp. 20-30, 1990.

[3] L. Harn and S. Yang, "ID-Based Cryptographic Schemes for User Identification, Digital Signature, and Key distribution", IEEE Journal on Selected Areas in Communications, Vol. 11, No. 5, pp. 757-760, June 1993.

[4] ISO/IEC 9595, Information Processing Systems-Open Systems Interconnection-Common Management Information Service Definition.

[5] ISO/IEC 10164, Information Processing Systems-Open Systems Interconnection-Systems Management-Part 1, 2, 3, 4, 5, and 6.

[6] P. Kalyanasundaram, A. S. Sethi, "An Application Gateway Design for OSI-Internet Management", proc. 3rd International Symposium on Integrated Network Management, pp. 389-40, April 1993.

[7] S. Mazumdar, S. Brady, and D. W. Levine, "Design of Protocol Independent Management Agent to Support SNMP and CMIP Queries", Proc. 3rd International Symposium on Integrated Network Management, pp. 377-388, April 1993.

[8] I. Mohammed and D. M. Dilts, "Design for dynamic user-role-based security", Computers & security, 13. 1994, pp. 661-671.

[9] J. T. Park, Y. W. Choi, J. W. Jung and J. S. Sunwoo, "The Integration of OSI Network Management and TCP/IP Internet Management using SNMP", IEEE First International Workshop, pp. 145-154, April 1993.

[10] Ch. P. Pfleeger, Security in Computing, Prentice Hall, Englewood Cliffs, New Jersey 07638, pp. 242-258.

[11] M. Reitenspiess, "Open System Security Standards", Computers & security, 12, 1993, pp. 341-361.

[12] W. Stallings, SNMP, SNMPv2, and CMIP-The practical Guide to Network Management Standards, Addison-Wesley Publishing Company, July 1993.

[13] M. T. Rose, "Transition and Coexistence Strategies for TCP/IP to OSI", IEEE Journal on Selected areas in Communications Vol. 8. No. 1, pp. 57-66, January 1990.

[14] S. F. Wu, S. Mazumdar, S. Brady and D. Levine, "On Implementing a Protocol Independent MIB", In Second IEEE Network Management and Control Workshop, Tarrytown, New York, September,

1993.

[15] S. F. Wu, S. Mazumdar, S. Brady, "EMOSY : An SNMP Protocol Object Generator for the Protocol Independent MIB", IEEE First International Workshop on Systems Management, pp. 133-144, April 1993.

[16] Y. Yemini, G. Goldszmidt, S. Yemini, "NETWORK MANAGEMENT BY DELEGATION", Proc. 2nd International Symposium on Integrated Network Management, pp. 95-107, April 1991.

김 태 연

1986년 전남대학교 계산통계학과 이학사

1988년 전남대학교 대학원 계산통계학과 이학석사

1993년~현재 광주예술전문대학 컴퓨터그래픽 디자인학과 전임강사

관심분야 : 통신망 관리, 분산처리 시스템, 통신 보안, 컴퓨터 그래픽스 등

서 재 현

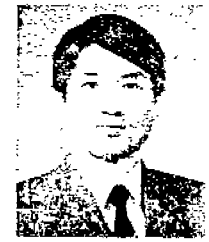
1985년 전남대학교 계산통계학과 이학사

1988년 중앙대학교 대학원 전자계산학과 이학석사

1993년~현재 전남대학교 대학원 전산통계학과 박사과정

1988년~현재 송원전문대학 전자계산학과 전임강사

관심분야 : 통신망 관리, 객체지향 시스템, 분산처리 시스템, 정보 보안 등



노 봉 남

1978년 전남대학교 수학교육과 이학사

1982년 한국과학기술원 전산학과 공학석사

1994년 전북대학교 대학원 전산통계학과 이학박사

1983년~현재 전남대학교 전산학과 교수

관심분야 : 객체지향 시스템, 통신망 관리, 정보 보안, 컴퓨터와 정보사회 등