(19)대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) 。Int. Cl.[7]
H04L 12/24

(45) 공고일자 2005년05월17일
(11) 등록번호 10-0489216
(24) 등록일자 2005년05월03일

(21) 출원번호 10-2003-0028888
(22) 출원일자 2003년05월07일

(65) 공개번호 10-2004-0096079
(43) 공개일자 2004년11월16일

(73) 특허권자 한국전자통신연구원
대전 유성구 가정동 161번지

(72) 발명자 김성조
대전광역시유성구어은동한빛아파트109-1104

박대선
대전광역시유성구원내동한아름아파트108-303

허용준
서울특별시강남구신사동636-30

홍충선
경기도용인시상현동837금호3단지271-1101

(74) 대리인 신영무

심사관 : 신성길

(54) 단순 망 관리 프로토콜(ＳＮＭＰ)을 이용하는 네트워크관리 시스템 및 그 네트워크 관리 시스템에서의 정보 교환방법

요약

본 발명은 단순 망 관리 프로토콜(SNMP)을 이용하는 네트워크 관리 시스템 및 그 네트워크 관리 시스템에서의 정보 교환 방법을 제공한다. 매니저 모듈에서는 XML로 변환 및 암호화한 PDU를 XML 보안 정책과 함께 에이전트 모듈로 전송한다. 에이전트 모듈에서는 XML 형식으로 암호화된 PDU를 복호화시키고, XML 보안 정책을 이용해서 SNMP 메시지로 다시 변환한 다음 XML 보안 정책에 따라 보안 기능을 수행한다. 따라서 기존의 네트워크 관리 시스템에서 발생되는 보안상의 취약점을 효과적으로 해결할 수 있으며 호환성을 유지할 수 있다.

대표도

도 1

색인어

SNMP, XML, 보안 정책, 매니저, 에이전트, 암호화, 복호화

명세서

도면의 간단한 설명

도 1은 본 발명에 따른 네트워크 관리 시스템에서의 매니저 모듈의 구성도.

도 2는 본 발명에 따른 네트워크 관리 시스템에서의 에이전트 모듈의 구성도.

도 3은 본 발명에 따른 네트워크 관리 시스템에서의 매니저 모듈의 동작을 설명하기 위한 흐름도.

도 4는 본 발명에 따른 네트워크 관리 시스템에서의 에이전트 모듈의 동작을 설명하기 위한 흐름도.

<도면의 주요 부분에 대한 부호의 설명>

100: SNMP 응용 프로그램 101: 명령 생성블럭

102: 알림정보 생성블럭 103: 알림정보 수신블럭

104: XML 정책 결정블럭 110: XML 정책 저장소

120: SNMP 엔진 130: 처리블럭

131: PDU 처리영역 132: 메시지 처리영역

133: 트랜스포트 맵핑영역 140: 메시지 처리 서브시스템블럭

141 내지 144: SNMP 버전 150: 보안 서브시스템블럭

151: XML 변환영역 152: XML 암호화영역

153: USB 모델 154: 기타 보안 모델

160: 트랜스포트 프로토콜 170: 네트워크

200: SNMP 응용 프로그램 201: 프록시 전달블럭

202: 명령 응답블럭 203: 알림정보 생성블럭

204: XML 정책 실행블럭 205: MIB 정보 해석블럭

206: 정책 정보 베이스블럭 210: SNMP 엔진

220: 처리블럭 221: 트랜스포트 맵핑영역

222: 메시지 처리영역 223: PDU 처리영역

230: 메시지 처리 서브시스템블럭 231 내지 234: SNMP 버전

240: 보안 서브시스템블럭 241: XML 변환영역

242: XML 복호화영역 243: USB 모델

244: 기타 보안 모델 250: 처리 제어 서브시스템블럭

251: 처리 제어 모델 252: 인증영역

260: 트랜스포트 프로토콜

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 매니저와 네트워크 장비로 구성되는 네트워크 관리 시스템에 관한 것으로, 더욱 상세하게는 단순 망 관리 프로토콜(Simple Network Management Protocol; SNMP)을 이용하는 네트워크 관리 시스템 및 그 네트워크 관리 시스템에서의 정보 교환 방법에 관한 것이다.

현재 대부분의 네트워크 장비에는 기본적으로 단순 망 관리 프로토콜(SNMP) 서비스가 설정되어 있다. 매니저와 네트워크 장비 간의 관리 정보 베이스(Management Information Base; MIB)를 상호 교환하기 위한 망 관리 표준 프로토콜인 단순 망 관리 프로토콜(이하, SNMP라 칭함)은 기본적인 망 관리뿐만 아니라 원격 관리 구조의 형태를 가진 모든 모델에 광범위하게 적용되어 외부에서도 네트워크 장비를 관리할 수 있도록 한다. 하지만 SNMP은 시스템의 설정을 읽거나 변경할 때 사용하는 커뮤니티 스트링(Community String)이 기본값으로 설정되기 때문에 필요 이상으로 많은 정보가 노출될 수 있으며, 외부 네트워크에서도 SNMP을 이용하여 해당 장비의 설정을 변경할 수 있는 문제점이 있다. 또한, 악의를 가진 사용자로부터 비정상적인 메시지를 수신할 경우 시스템이 다운되거나 재부팅되는 문제가 발생될 수 있다. 이는 관리 정보 베이스(MIB)의 정보가 공유된 상태에서 침입자(Attacker)에 의한 프로토콜 데이터 유니트(Protocol Data Unit; PDU)의 분석이 가능함으로써 야기될 수 있는 문제로서 SNMP에서 프로토콜 데이터 유니트(PDU)의 분석을 방지할 수 있는 방법을 제시하지는 못하고 있는 실정이다.

IETF(Internet Engineering Task Force)에서 제안되었던 SNMPv1은 처음부터 보안을 전제로 작성된 프로토콜이 아니며, 또한 프로토콜 작성시 전제되었던 가정들은 더 이상 적용이 어려운 실정이다. SNMPv1에서는 단순히 커뮤니티(Community)와 커뮤니티 네임(Community Name)만을 가지고 인증(Authentication) 서비스를 제공하였지만, 그런 단순한 구조로는 SNMP 메시지에 대한 보안 문제를 해결할 수 없었다. 따라서 IETF Working 그룹에서는 보안 기능을 추가한 SNMPv2와 SNMPv3를 제시하였으며, 메시지 처리에 있어서는 USB(User-based Security Model, SNMPv3)을 제시하여 기본적인 보안 문제를 해결하였지만 여전히 고려하지 않은 부분들이 남아 있는 실정이다. 이는 SNMPv3에서 추가되었던 USB의 고려하지 못한 부분에 의해 발생되는 것으로 침입자에 의한 서비스 거부나 매니저와 에이전트 간의 트래픽 패턴을 침입자가 관찰할 수 있는 문제들에 기인하는 것으로 여겨진다.

발명이 이루고자 하는 기술적 과제

따라서 본 발명은 매니저 모듈에서 프로토콜 데이터 유니트(PDU)를 XML(Extensible Markup Language) 정책에 정의된 메시지 형식으로 변환하고, 정의된 보안 정책과 함께 에이전트 모듈로 전송함으로써 상기한 단점을 해소할 수 있는 단순 망 관리 프로토콜(SNMP)을 이용하는 네트워크 관리 시스템 및 그 네트워크 관리 시스템에서의 정보 교환 방법을 제공하는 데 그 목적이 있다.

상기한 목적을 달성하기 위한 본 발명에 따른 네트워크 관리 시스템에서 매니저 모듈은 XML 보안관련 정보가 저장되는 XML 정책 저장소와, 상기 XML 정책 저장소에 저장된 보안 정책 중 적용하고자 하는 보안 정책을 결정하고 전송을 위한 메시지를 생성하는 SNMP 응용 프로그램과, 상기 SNMP 응용 프로그램으로부터 상기 메시지와 보안 정책을 받고, 상기 보안 정책에 따라 상기 메시지를 XML로 변환하고 암호화한 후 상기 에이전트로 전송하는 SNMP 엔진을 포함하며, 에니전트 모듈은 상기 매니저로부터 전송된 메시지를 복호화하고, 상기 보안 정책을 이용해서 SNMP 메시지로 변환하는 SNMP 엔진과, 상기 SNMP 엔진으로 받은 상기 보안 정책에 따라 각 장치 관리와 보안 정책을 적용하는 SNMP 응용 프로그램을 포함하는 것을 특징으로 한다.

또한, 상기한 목적을 달성하기 위한 본 발명에 따른 네트워크 관리 시스템에서의 정보 교환 방법은 사용자 요구가 입력되면 상기 매니저 모듈에서 적용하고자 하는 보안 정책을 결정하고 메시지를 생성하는 단계, 상기 보안 정책에 따라 상기 메시지를 XML로 변환하고 암호화하는 단계, 상기 메시지에 보안 모델을 적용하고 상기 에이전트 모듈로 전송하는 단계, 상기 에이전트 모듈에서 상기 메시지를 수신하고 상기 메시지를 보낸 매니저에 대해 인증을 실시하는 단계, 상기 메시지를 복호화하고 상기 보안 정책을 이용해서 SNMP 메시지로 변환하는 단계, 상기 보안 정책에 따라 각 장치 관리와 보안 정책을 적용하는 단계를 포함하는 것을 특징으로 한다.

발명의 구성 및 작용

본 발명은 단순 망 관리 프로토콜(SNMP)을 이용하는 네트워크 관리 시스템에서 SNMP 매니저(Manager)와 SNMP 에이전트(Agent) 모듈의 보안성이 향상되도록 한다. 보안성 향상을 위해 SNMP 매니저는 프로토콜 데이터 유니트(PDU)를 XML(Extensible Markup Language) 정책에 정의된 메시지 형식으로 변환하고 정책 저장소에 정의된 보안 정책과 함께 SNMP 에이전트로 전송한다. 따라서 침입자가 프로토콜 데이터 유니트(PDU)의 분석을 통해 서비스를 거부하거나 매니저와 에이전트 간의 트래픽 패턴을 관찰하는 등의 보안상의 취약점을 해결할 수 있다.

그러면 이하, 첨부된 도면을 참조하여 본 발명의 바람직한 실시예를 상세히 설명하기로 한다.

본 발명에 따른 단순 망 관리 프로토콜(SNMP)을 이용하는 네트워크 관리 시스템에서의 매니저와 에이전트 모듈의 구조는 다음과 같다.

도 1은 본 발명에 따른 네트워크 관리 시스템에서의 매니저 모듈의 구성도로서, SNMP 응용 프로그램(100), XML 정책 저장소(110) 및 SNMP 엔진(120)으로 구성된다.

SNMP 응용 프로그램(Applications; 100)은 명령 생성블럭(Command generator; 101), 알림정보 생성블럭(Notification originator; 102), 알림정보 수신블럭(Notification receiver; 103) 및 XML 정책 결정블럭(Policy decision; 104)으로 이루어진다. 명령 생성블럭(101)은 SNMP 요구(Request) 메시지를 생성한다. 알림정보 생성블럭(102)은 특별한 이벤트나 상태를 위해서 시스템을 모니터하고, 이러한 이벤트나 상태를 기초로 하는 메시지를 생성한다. 알림정보 수신블럭(103)은 알림정보 메시지를 기다리며 알림 메시지를 받은 경우 이에 대한 응답 메시지를 생성한다. XML 정책 결정블럭(104)은 적용하고자 하는 보안 정책을 결정한다.

XML 정책 저장소(Policy repository; 110)는 보안을 위해 사전에 설정된 XML 보안관련 정보가 저장되는 블럭으로 정책 데이터베이스 서버(Policy Database server)로 이루어진다.

SNMP 엔진(Engine; 120)은 처리블럭(Dispatcher; 130), 메시지 처리 서브시스템블럭(Message processing subsystem; 140) 및 보안 서브시스템블럭(Security subsystem; 150)으로 이루어지는데, 처리블럭(130)은 PDU 처리영역(PDU Dispatcher; 131), 메시지 처리영역(Message dispatcher; 132) 및 트랜스포트 맵핑영역(Transport mapping; 133)으로 이루어지며, 메시지 처리 서브시스템블럭(140)은 각기 다른 다수의 SNMP 버전(141 내지 144)으로 이루어지고, 보안 서브시스템블럭(150)은 XML 변환영역(Parser; 151), XML 암호화영역(Encryption; 152), USB 모델(Model; 153) 및 기타 보안 모델(154)로 이루어진다.

도 1에 도시된 본 발명의 매니저 모듈은 기존의 SNMPv3을 기본으로 구성하였으며, SNMP 응용 프로그램(100)에는 XML 정책 결정블럭(104)을, SNMP 엔진(120)의 보안 서브시스템블럭(150)에는 XML 변환영역(151)과 XML 암호화영역(152)을 더 포함시켜 기존의 SNMP과의 호환성을 유지하며 PDU의 보안성을 강화시킬 수 있도록 하였다.

도 2는 본 발명에 따른 네트워크 관리 시스템에서의 에이전트 모듈의 구성도로서, SNMP 응용 프로그램(200) 및 SNMP 엔진(210)으로 구성된다.

SNMP 응용 프로그램(Applications; 200)은 프록시 전달블럭(Proxy forwarder; 201), 명령 응답블럭(Command responder; 202), 알림정보 생성블럭(Notification originator; 203), XML 정책 실행블럭(Policy enforcer; 204), MIB 정보 해석블럭(205) 및 정책 정보 베이스블럭(PIB: Policy Information Base; 206)으로 이루어진다. 명령 응답블럭(202)은 SNMP 요구 메시지에 대한 응답 메시지를 생성하고, 프록시 전달블럭(201)은 SNMP 메시지를 전송한다.

SNMP 엔진(Engine; 210)은 처리블럭(Dispatcher; 220), 메시지 처리 서브시스템블럭(Message processing subsystem; 230), 보안 서브시스템블럭(Security subsystem; 240) 및 처리 제어 서브시스템블럭(Access control subsystem; 250)으로 이루어지는데, 처리블럭(220)은 트랜스포트 맵핑영역(Transport mapping; 221), 메시지 처리영역(Message dispatcher; 222) 및 PDU 처리영역(PDU Dispatcher; 223)으로 이루어지며, 메시지 처리 서브시스템블럭(230)은 각기 다른 다수의 SNMP 버전(231 내지 234)으로 이루어지고, 보안 서브시스템블럭(240)은 XML 변환영역(Interpreter; 241), XML 복호화영역(Decryption; 242), USB 모델(Model; 243) 및 기타 보안 모델(244)로 이루어지며, 처리 제어 서브시스템블럭(250)은 처리 제어 모델(View-based access control model; 251) 및 인증영역(Authorizatiom; 252)으로 이루어진다.

도 2에 도시된 본 발명의 에이전트 모듈은 기존의 SNMPv3을 기본으로 구성하였으며, SNMP 응용 프로그램(100)에는 XML 정책 실행블럭(204)을, SNMP 엔진(210)의 보안 서브시스템블럭(240)에는 XML 변환영역(241)과 XML 복호화영역(242)을 더 포함시켜 기존의 SNMP과의 호환성을 유지하며 PDU의 보안성을 강화시킬 수 있도록 하였다.

그러면 상기와 같이 구성된 매니저와 에이전트 모듈 사이에서 정보가 교환되는 과정을 도 3 및 도 4를 참조하여 설명하면 다음과 같다.

도 3은 본 발명에 따른 네트워크 관리 시스템에서의 매니저 모듈의 동작을 설명하기 위한 흐름도이다.

단계 MS1: 사용자 요구가 입력되면 SNMP 응용 프로그램(100)의 XML 정책 결정블럭(104)은 XML 정책 저장소(110)에 저장된 보안 정책 중 적용하고자 하는 보안 정책을 결정하고 명령 생성블럭(101)은 전송을 위한 PDU를 생성한다. 결정된 보안 정책은 생성된 PDU와 함께 SNMP 엔진(120)의 처리블럭(130)으로 보내진다.

단계 MS2: 처리블럭(130)은 메시지를 메시지 처리 서브시스템블럭(140)으로 보낸다. 이 때 처리블럭(130)의 PDU 처리영역(131)은 PDU의 유형을 구분하고, 메시지 처리영역(132)은 메시지의 유형을 구분한다.

단계 MS3: 메시지 처리 서브시스템블럭(140)은 SNMP 버전(141 내지 144)에 맞게 메시지를 할당하고 보안 서브시스템블럭(150)으로 전달한다.

단계 MS4: 보안 서브시스템블럭(150)의 XML 변환영역(151)은 보안성을 강화시키기 위하여 PDU를 XML 정책 저장소(110)에 정의된 보안 정책에 따라 XML로 변환한다. 이 때 XML 정책 결정블럭(104)에서 결정된 PDU는 XML로 변환할 필요가 없으며, 다른 응용 프로그램(Application)에서 생성된 PDU는 XML로 변환한다.

단계 MS5: 보안 서브시스템블럭(150)의 XML 암호화영역(152)은 XML로 변환한 PDU를 암호화시킨다.

단계 MS6: 보안 서브시스템블럭(150)은 전송하고자 하는 전체 메시지에 UBS 모델(154)이나 기타 다른 보안 모델(154)을 적용한다.

단계 MS7: 처리블럭(130)의 트랜스포트 맵핑영역(133)은 전송 가능한 트랜스포트 프로토콜(160)을 선택하고 네트워크(170)를 통해 메시지를 에이전트 모듈로 전송한다.

도 4는 본 발명에 따른 네트워크 관리 시스템에서의 에이전트 모듈의 동작을 설명하기 위한 흐름도이다.

단계 AS1: 상기 네트워크(170)를 통해 전송된 메시지가 수신 가능한 트랜스포트 프로토콜(260)을 통해 처리블럭(220)의 트랜스포트 맵핑영역(221)으로 수신되면 처리 제어 서브시스템블럭(250)의 인증영역(252)은 메시지를 보낸 매니저에 대해 접근 권한을 검사하는 인증을 실시하고, 처리 제어 모델(251)은 매니저로부터 받은 메시지를 보안 서브시스템블럭(240)으로 보낸다.

단계 AS2: 보안 서브시스템블럭(240)은 매니저로부터 전송된 메시지에서 SNMP 프로토콜의 USB 모델과 같은 암호화 작업이 수행된 부분에 대해 기타 다른 보안 모델(244)과 UBS 모델(243)에서 복호화 작업을 수행한다.

단계 AS3: 보안 서브시스템블럭(240)의 XML 복호화영역(242)은 XML로 암호화된 PDU를 복호화시킨다.

단계 AS4: 보안 서브시스템블럭(240)의 XML 변환영역(241)은 복호화된 PDU를 XML 정책 저장소(110)에 정의된 상기 XML 보안 정책을 이용해서 SNMP 메시지로 변환하고 메시지 처리 서브시스템블럭(230)으로 보낸다. 즉, XML 형식으로 변환된 매니저로부터 받은 메시지를 다시 SNMP 메시지로 변환한다.

단계 AS5: 메시지 처리 서브시스템블럭(230)은 버전이 다른 메시지들을 유효하게 만들기 위해 SNMP 버전(231 내지 234)에 맞게 PDU에서 데이터를 추출하고 처리블럭(220)으로 전달한다.

단계 AS6: 처리블럭(220)은 메시지를 처리하여 SNMP 응용 프로그램(200)의 XML 정책 실행블럭(204)으로 보낸다. 이때 처리블럭(220)의 PDU 처리영역(223)은 PDU의 유형을 구분하고, 메시지 처리영역(222)은 메시지의 유형을 구분한다.

단계 AS7: XML 정책 실행블럭(204)은 적합한 XML 보안 정책을 선택하고 미리 정의된 정책 정보 베이스블럭(206)의 보안 정책에 따라 각 장치 관리와 보안 정책을 적용하게 된다. 보안 정책을 적용하는 예로는, 매니저에서 선택한 보안 정책에 따라 각각의 사용자에게 서로 다른 장치를 관리할 수 있는 권한을 부여하고, 기존 SNMP 프로토콜의 취약점인 Denial of Service(공격자가 매니저와 에이전트 사이에서 주고 받는 메시지를 방해하는) 공격시 공격이 발생한 곳의 IP를 차단하는 것과 같이 보안 정책을 정책 정보 베이스블럭(206)으로 미리 설정하여 XML 정책 실행블럭(204)에서 정책을 적용하며, 인증되지 않은 사용자가 서비스를 요구하는 경우 오류 메시지를 생성하고 사용자의 ID, IP 어드레스를 모니터링할 수 있는 기능을 부여한다.

그러면 여기서 SNMP 관리 정보 베이스(MIB)를 XML로 변환하는 본 발명의 기본 배경에 대하여 살펴보면 다음과 같다.

J.P Martin-Flatin은 웹 기반의 통합 관리 구조(Architecture)에서 데이터 통합을 위한 방법으로 SNMP 관리 정보 베이스(MIB)를 XML로 변환하기 위한 모델을 제공하였다. 이는 모델-레벨 맵핑(Model-level mapping)이라고 정의되어 있는데, 모델-레벨 맵핑은 DTD(Document Type Definition)가 SNMP 관리 정보 베이스(MIB)에 특정하게 작성되는 방법이다. 즉, SNMP 변수명을 그대로 사용하여 XML DTD에서 엘레멘트(Element)와 속성(Attribute)을 작성한다. 또한, 메타 모델-레벨 맵핑(Metamodel-level mapping)은 일반화된 하나의 DTD를 정의하여 모든 관리 정보 베이스(MIB)에 적용하는 방법이다. 이 모델에서는 관리 정보 베이스(MIB)에 정의된 변수를 사용하여 엘레먼트를 명명하지 않고 일반적인 키워드를 사용한다.

본 발명에서는 하나의 DTD를 정의하여 모든 SNMP 관리 정보 베이스(MIB)에 적용이 가능하기 때문에 변환 프로그램이 용이한 장점을 갖는 메타 모델-레벨 맵핑을 사용하여 SNMP 관리 정보 베이스(MIB)를 XML로 변환하고, 변환된 데이터를 정책에 맵핑시킴으로써 네트워크 시스템을 제어할 수 있도록 한다.

상기와 같이 SNMP은 매니저와 에이전트 간의 메시지 송수신, 이벤트나 상태에 관한 모니터링 기능을 수행하게 되는데, 본 발명의 매니저 모듈에서는 XML 정책 결정블럭(104)이 XML 정책 저장소(110)에 저장된 보안 정책 중 적용하고자 하는 보안 정책을 결정한다. 그리고 XML 변환영역(151)이 PDU를 XML로 변환하고 XML 암호화영역(152)이 변환된 PDU를 암호화한다. 이와 같이 암호화된 PDU는 결정된 보안 정책과 함께 네트워크를 통해 에이전트 모듈로 전송된다.

또한, 에이전트 모듈에서는 XML 복호화영역(242)이 XML 형식으로 암호화된 PDU를 복호화시키고, XML 변환영역(241)이 복호화된 PDU를 XML 보안 정책을 이용해서 SNMP 메시지로 다시 변환한다. 그리고 XML 정책 실행블럭(204)이 XML 보안 정책에 따라 각 장치 관리와 보안 정책을 적용한다.

본 발명에서 상기 매니저 모듈과 에이전트 모듈의 SNMP 엔진에 포함되는 각 구성요소는 메시지를 송신하는 경우와 수신하는 경우에 상호 교환적으로 동작될 수 있다. 예를 들어, 보안 서브시스템블럭(150)의 XML 암호화영역(152)은 메세지 송신 시 XML로 변환한 PDU를 암호화시키는 역할을 수행하지만, 메시지 수신 시에는 XML로 암호화된 PDU를 복호화시키는 역할을 수행할 수 있다.

발명의 효과

상기한 바와 같이 본 발명은 보안성이 강화된 단순 망 관리 프로토콜(SNMP)을 이용하는 네트워크 관리 시스템을 제공한다. 매니저 모듈에서는 XML로 변환 및 암호화한 PDU를 XML 보안 정책과 함께 에이전트 모듈로 전송한다. 에이전트 모듈에서는 XML 형식으로 암호화된 PDU를 복호화시키고, XML 보안 정책을 이용해서 SNMP 메시지로 다시 변환한 다음 XML 보안 정책에 따라 보안 기능을 수행한다. 따라서 기존의 네트워크 관리 시스템에서 발생되는 보안상의 취약점을 효과적으로 해결할 수 있다.

또한, 본 발명의 네트워크 관리 시스템은 기존의 SNMP 매니저 모듈과 에이전트 모듈에 상기와 같은 보안상의 취약점을 해결하기 위한 구성요소를 추가하는 형식으로 구성되기 때문에 호환성을 유지할 수 있으며, XML 기반의 보안 정책을 사용함으로써 유연성을 제공할 수 있다.

(57) 청구의 범위

청구항 1.

단순 망 관리 프로토콜(SNMP)을 이용하며 매니저 모듈과 에이전트 모듈로 이루어지는 네트워크 관리 시스템에 있어서,

상기 매니저 모듈은 XML 보안관련 정보가 저장되는 XML 정책 저장소와,

상기 XML 정책 저장소에 저장된 보안 정책 중 적용하고자 하는 보안 정책을 결정하고 전송을 위한 메시지를 생성하는 SNMP 응용 프로그램과,

상기 SNMP 응용 프로그램으로부터 상기 메시지와 보안 정책을 받고, 상기 보안 정책에 따라 상기 메시지를 XML로 변환하고 암호화한 후 상기 에이전트로 전송하는 SNMP 엔진을 포함하며,

상기 에니전트 모듈은 상기 매니저로부터 전송된 메시지를 복호화하고, 상기 보안 정책을 이용해서 SNMP 메시지로 변환하는 SNMP 엔진과,

상기 SNMP 엔진으로 받은 상기 보안 정책에 따라 각 장치 관리와 보안 정책을 적용하는 SNMP 응용 프로그램을 포함하는 것을 특징으로 하는 단순 망 관리 프로토콜(SNMP)을 이용하는 네트워크 관리 시스템.

청구항 2.

제 1 항에 있어서, 상기 매니저 모듈의 SNMP 응용 프로그램은 상기 메시지를 생성하는 명령 생성블럭과,

이벤트나 상태를 위해서 시스템을 모니터하고, 이벤트나 상태를 기초로 하는 메시지를 생성하는 알림정보 생성블럭과,

알림 메시지에 대한 응답 메시지를 생성하는 알림정보 수신블럭과,

상기 보안 정책을 결정하는 XML 정책 결정블럭으로 이루어지는 것을 특징으로 하는 단순 망 관리 프로토콜(SNMP)을 이용하는 네트워크 관리 시스템.

청구항 3.

제 1 항에 있어서, 상기 매니저 모듈의 SNMP 엔진은 상기 메시지를 처리하고 전송하는 처리블럭과,

상기 처리블럭으로부터 받은 메시지에 버전을 할당하는 메시지 처리 서브시스템블럭과,

상기 메시지 처리 서브시스템블럭으로부터 받은 메시지를 상기 보안 정책에 따라 XML로 변환하고 암호화하는 보안 서브시스템블럭으로 이루어진 것을 특징으로 하는 단순 망 관리 프로토콜(SNMP)을 이용하는 네트워크 관리 시스템.

청구항 4.

제 3 항에 있어서, 상기 보안 서브시스템블럭은 상기 메시지를 상기 보안 정책에 따라 XML로 변환하는 XML 변환영역과,

상기 변환된 메시지를 암호화하는 XML 암호화영역과,

상기 메시지에 적용하여 전송하는 USB 모델 및 기타 보안 모델로 이루어진 것을 특징으로하는 단순 망 관리 프로토콜(SNMP)을 이용하는 네트워크 관리시스템.

청구항 5.

제 1 항에 있어서, 상기 에이전트 모듈의 SNMP 엔진은 상기 매니저 모듈로부터 받은 메시지를 처리하고 전송하는 처리블럭과,

상기 메시지를 보낸 매니저에 대해 접근 권한을 검사하는 처리 제어 서브시스템블럭과,

상기 처리블럭으로부터 받은 메시지에서 버전에 맞게 데이터를 추출하는 메시지 처리 서브시스템블럭과,

상기 메시지를 복호화하고 상기 XML 보안 정책을 이용해서 SNMP 메시지로 변환하는 보안 서브시스템블럭으로 이루어지는 것을 특징으로 하는 단순 망 관리 프로토콜(SNMP)을 이용하는 네트워크 관리 시스템.

청구항 6.

제 5 항에 있어서, 상기 보안 서브시스템블럭은 상기 메시지를 복호화하는 XML 복호화영역과,

상기 메시지를 상기 보안 정책에 따라 XML로 변환하는 XML 변환영역과,

상기 메시지에 적용하여 전송하는 USB 모델 및 기타 보안 모델로 이루어진 것을 특징으로 하는 단순 망 관리 프로토콜(SNMP)을 이용하는 네트워크 관리 시스템.

청구항 7.

제 1 항에 있어서, 상기 에이전트 모듈의 SNMP 응용 프로그램은 상기 메시지를 전달하는 프록시 전달블럭과,

상기 메시지에 대한 응답 메시지를 생성하는 명령 응답블럭과,

이벤트나 상태를 위해서 시스템을 모니터하고, 이벤트나 상태를 기초로 하는 메시지를 생성하는 알림정보 생성블럭과,

상기 보안 정책에 따라 각 장치 관리와 보안 정책을 적용하는 XML 정책 실행블럭과,

MIB 정보 해석블럭과,

필요한 보안 정책을 미리 설정하기 위한 정책 정보 베이스블럭으로 이루어진 것을 특징으로 하는 단순 망 관리 프로토콜(SNMP)을 이용하는 네트워크 관리 시스템.

청구항 8.

단순 망 관리 프로토콜(SNMP)을 이용하며 매니저 모듈과 에이전트 모듈로 이루어지는 네트워크 관리 시스템에서의 정보 교환 방법에 있어서,

사용자 요구가 입력되면 상기 매니저 모듈에서 적용하고자 하는 보안 정책을 결정하고 메시지를 생성하는 단계,

상기 보안 정책에 따라 상기 메시지를 XML로 변환하고 암호화하는 단계,

상기 메시지에 보안 모델을 적용하고 상기 에이전트 모듈로 전송하는 단계,

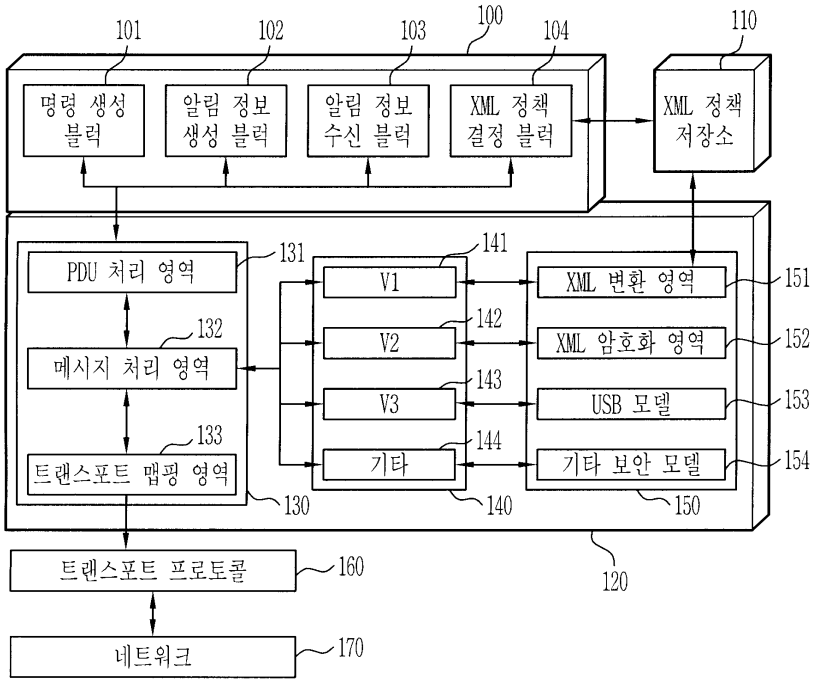
상기 에이전트 모듈에서 상기 메시지를 수신하고 상기 메시지를 보낸 매니저에 대해 인증을 실시하는 단계,

상기 메시지를 복호화하고 상기 보안 정책을 이용해서 SNMP 메시지로 변환하는 단계,

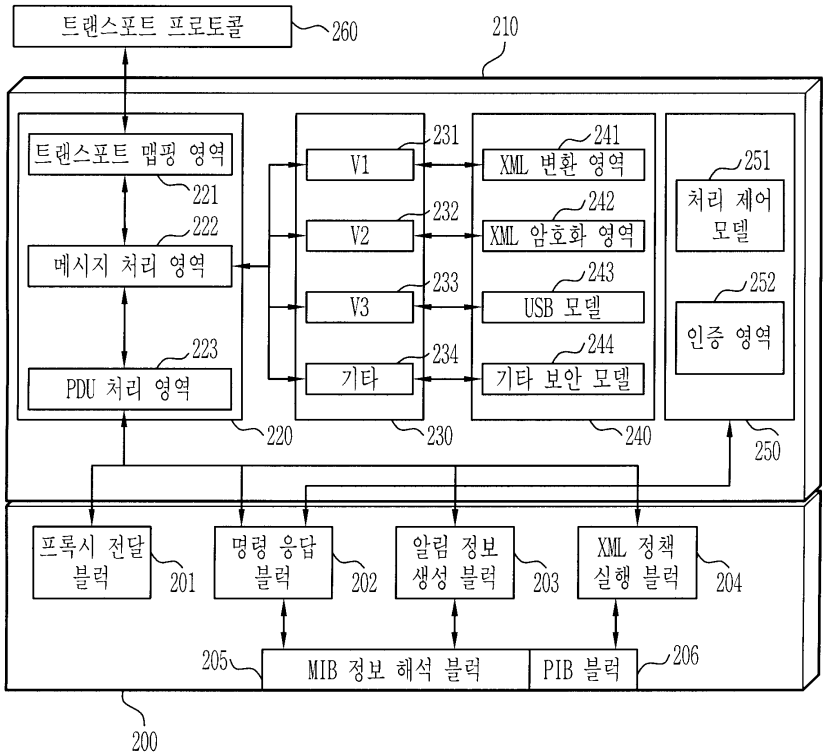
상기 보안 정책에 따라 각 장치 관리와 보안 정책을 적용하는 단계를 포함하는 것을 특징으로 하는 단순 망 관리 프로토콜(SNMP)을 이용하는 네트워크 관리 시스템에서의 정보 교환 방법.

도면

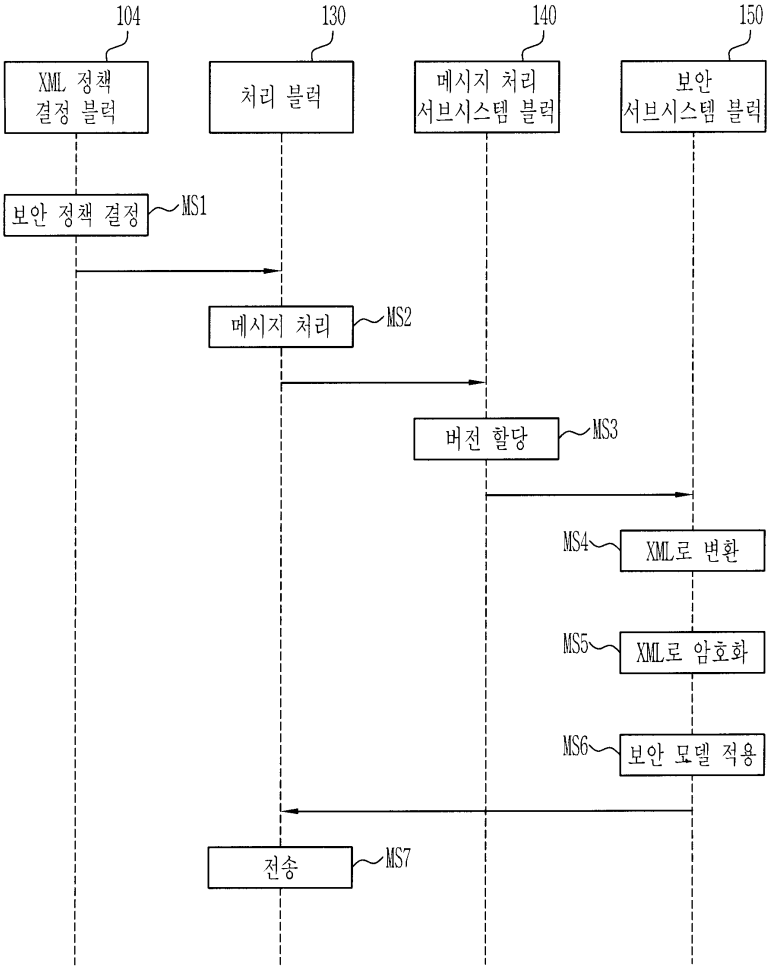
도면1


101
102
103
100
104
110
명령 생성 블럭
알림 정보 생성 블럭
알림 정보 수신 블럭
XML 정책 결정 블럭
XML 정책 저장소
PDU 처리 영역
131
메시지 처리 영역
132
트랜스포트 맵핑 영역
133
130
V1
141
V2
142
V3
143
기타
144
140
XML 변환 영역
151
XML 암호화 영역
152
USB 모델
153
기타 보안 모델
154
150
120
트랜스포트 프로토콜
160
네트워크
170

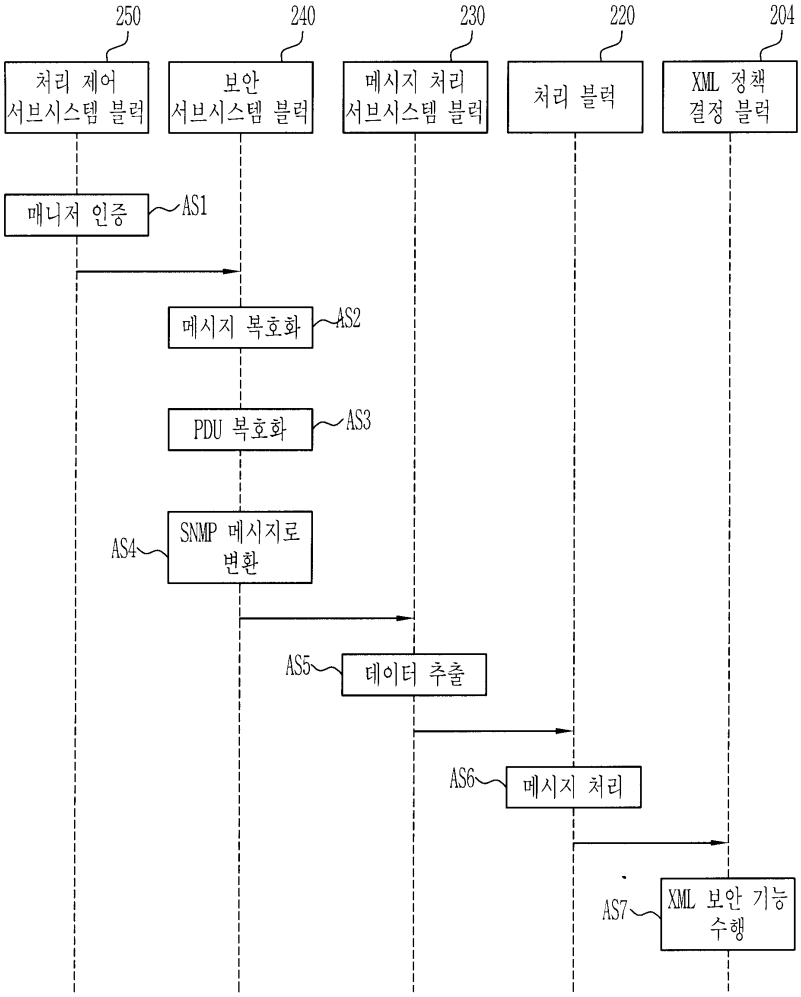
도면2


트랜스포트 프로토콜
260
210
트랜스포트 맵핑 영역
221
메시지 처리 영역
222
PDU 처리 영역
223
220
V1
231
V2
232
V3
233
기타
234
230
XML 변환 영역
241
XML 암호화 영역
242
USB 모델
243
기타 보안 모델
244
240
처리 제어 모델
251
인증 영역
252
250
프록시 전달 블럭
201
명령 응답 블럭
202
알림 정보 생성 블럭
203
XML 정책 실행 블럭
204
205
MIB 정보 해석 블럭
PIB 블럭
206
200

도면3


104
130
140
150
XML 정책 결정 블럭
처리 블럭
메시지 처리 서브시스템 블럭
보안 서브시스템 블럭
보안 정책 결정
MS1
메시지 처리
MS2
버전 할당
MS3
MS4
XML로 변환
MS5
XML로 암호화
MS6
보안 모델 적용
전송
MS7

도면4


250
240
230
220
204
처리 제어 서브시스템 블럭
보안 서브시스템 블럭
메시지 처리 서브시스템 블럭
처리 블럭
XML 정책 결정 블럭
매니저 인증
AS1
메시지 복호화
AS2
PDU 복호화
AS3
SNMP 메시지로 변환
AS4
AS5
데이터 추출
AS6
메시지 처리
AS7
XML 보안 기능 수행