안전한 멀티캐스트 SNMP를 위한 구조

곽득휘[O] 김종원
광주과학기술원 정보통신공학과 네트워크 미디어 연구실
{dwkwak[O], jongwon }@gist.ac.kr

A Framework for Secure Multicast SNMP

Deuk-Whee Kwak[O] JongWon Kim
Networked Media Lab., Dept. of Information & Communications,
Gwangju Institute of Science and Technology (GIST)

요 약

안전한 그룹 통신은 원격 회의 또는 강의, 네트워크 게임, 그리고 주식정보 제공등 이미 다양한 분야에서 그 필요성을 인식하고 있지만, 그 개념을 망 관리 시스템에 적용하여도 통신망을 효율적으로 관리하는데 도움이 될것으로 기대된다. SNMP는 데이타 망관리를 위한 프로토콜로 일대일 통신에는 안전한 통신을 위한 방안을 제공하지만 안전한 그룹 통신을 위한 방안은 제공하지 않는다. 본 논문에서는 표준 SNMPv3를 확장하여 표준 SNMPv3와 호환이 가능하면서도 안전한 멀티캐스트 서비스를 제공하는 구조를 제안한다. 제안한 구조는 MIB-II를 확장하고, SET 명령과 표준 엔진의 동작을 수정하여 그룹 멤버쉽과 그룹 키를 처리할 수 있도록 하였다.

1. 서론

SNMP (Simple Network Management Protocol)는 데이타 망을 관리하기 위하여 개발된 표준 프로토콜로, 매니저는 표준 명령을 사용하여 에이전트에게 관리 데이터를 요청하거나 특정항목을 특정 값으로 설정하도록 요구한다[1]. 에이전트는 매니저의 요청을 수행하고 그 결과인 응답 메시지를 매니저에게 보낸다. 이 때 매니저가 보내는 명령 메시지나 에이전트가 보내는 응답 메시지가 외부의 보안 공격으로부터 보호 받지 못하면 변장(masquerade)이나 도청(eavesdrop) 공격이 가능하다[2]. 이러한 위협으로부터 시스템을 보호하기 위하여 SNMPv3가 개발되었다. SNMPv3는 USM (User Security Model)을 사용하여 인증과 기밀성 서비스를 제공한다[1, 2]. 그러나 USM은 하나의 매니저와 하나의 에이전트 간에 안전한 통신을 위한 메카니즘은 제공하지만 하나의 메니저가 동시에 다수의 에이전트와 통신하기 위한 효율적인 메카니즘은 제공하지 않는다. 본 논문에서는 기존의 SNMPv3 구조에 최소한의 표준 변경 및 기능 추가로 기존의 SNMPv3와 호환이 가능한 안전한 멀티캐스트 서비스를 제공하는 효율적인 구조를 제안 한다.

2. 안전한 멀티캐스트 SNMP의 필요성

안전한 멀티캐스트 개념을 표준 SNMPv3에 도입함으로써 다음과 같은 장점들이 있다[3,4]. 첫째 망관리의 효율성이 높아진다. 기존의 계층구조를 가지고 있는 망관리 구조에서는 상위 시스템이 관리 대상이 되는 하위 시스템들의 트래픽 통계 데이타를 얻거나 통제하기 위하여 상위 시스템의 동일한 관리 명령이 여러 하위 시스템에 동시에 전달되어야 하는 경우가 흔히 발생한다. 안전한 멀티캐스트 메카니즘을 사용하면 상위 시스템이 모든 하위 시스템들을 개별 접촉해야 하는 부담으로 벗어날 수 있으므로 상위 시스템의 부하를 줄일 수 있고 통신망 전체의 트래픽 양을 줄일 수 있을 뿐만 아니라 기존의 SNMPv3와 최소한 동일한 수준의 보안성을 제공한다. 둘째로 고장 감내(Fault Tolerance) 시스템 구축이 용이해 진다. 동일 그룹에 속하는 다수의 매니저가 망 성능 관리 데이타를 별도의 백업 과정 없이 중복 관리하므로 한 매니저의 고장이나 보안 공격에 의한 서비스 중단 상황이 발생하여도 곧 바로 다른 매니저가 그 역할을 대신할 수 있는 실시간 이중화 또는 삼중화 시스템을 구축할 수 있다. 세째로 매니저들과 에이전트들의 관리 목적에 따른 다양한 그룹핑으로 유연한 망 관리 구조를 구축할 수 있다. 마지막으로 다수의 매니저에게 기능 분산이 가능하다. 한 그룹에 속하는 성능 관리 데이타가 다수의 매니저들에게 실시간으로 중복되어 있으므로 망 관리 전체 업무를 각 매니저에게 기능별로 분할 담당케 할 수 있다.

3. SNMPv3 USM의 키 지역화 [2, 5]

SNMPv3는 USM을 사용하여 인증과 무결성 그리고 암호화 서비스를 제공하는데 각 사용자가 하나의 패스워드에서 다수의 서버들과 안전하게 통신할 수 있도록 키 지역화(key localization)개념을 사용한다. 먼저 매니저와 에이전트간에 사전에 공유한 패스프레이즈(또는 패스워드)는 220 문자길이가 될때까지 반복하여 뒤로 연결(concatenate) 된다. 이렇게 확장된 패스프레이즈는 MD5나 SHA-1 해쉬 함수를 통하여 16이나 20 문자길이의 매스터 키를 생성하게 되고, 생성된 매스터 키와 에이전트의 engineID를 연결한 문자열을 입력으로 다시 해쉬 함수를 통과시키면 각각의 engineID를 소유한 에이전트들과 매니저간에만 공유하는 비밀키가 생성된다.(그림 1)

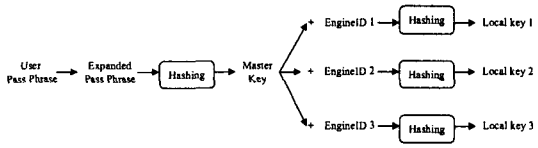

그림 1 USM의 키 지역화

4. 안전한 멀티캐스트 SNMP 의 구조

4.1 기본 개념 및 가정

표준 SNMPv3 상에서 안전한 멀티캐스트 서비스를 제공하기 위한 기본적인 방안은 다음과 같다. 먼저 모든 그룹의 멤버들은 하나의 (engineID, key) 쌍을 공유한다. 공유쌍 중 key는 GSAKMP (Group Security Association Key Management Protocol)나 GDOI(Group Domain of Interpretation)와 같은 일반적인 GKM (Group Key Manager)에 의하여 제공된다고 가정 한다[6]. 현 SNMPv3에서는 사용자의 비밀 키에 해당하는 패스 프레이즈(pass phrase)를 어떻게 생성하는지 그리고 각 에이전트들에게 어떻게 분배하는지에 관한 언급은 되어있지 않고 어떤 안전한 방법으로 사전에 공유하고 있다고 가정하고 있다. 본 논문에서는 모든 매니저와 에이전트들은 그룹 키 관리 프로코콜에 의하여 그룹 키가 적절히 관리 된다고 본다[5]. 동일한 engineID는 key의 앞 부분부터 필요한 길이 만큼 절취 하여 얻는다. 모든 그룹의 에이전트들이 동일한 그룹키 생성을 위하여 하나의 engineID를 공유 한다는 개념은 위의 키 지역화 개념과 정 반대의 개념이지만 키 지역화가 에이전트들에게 독립적인 비밀 키를 제공하기 위한 기법이지 보안성 정도를 향상 시키는 과정은 아니므로 키 지역화를 적용하지 않아도 추가적인 보안의 문제가 발생하지는 않는다. 사실 안전한 그룹 통신을 위한 비밀 키 생성 과정에서 engineID는 불필요한 변수이지만 이 변수를 그대로 유지하는 것이 시스템의 성능저하를 초래하지는 않으므로 본 구조에서는 기존의 SNMPv3 표준을 최소한으로 변경하기 위한 목적으로 engineID를 그대로 유지한다. 둘째로 멀티캐스트 주소와 포트 번호는 매니저가 결정하여 그룹 가입을 허락한 에이전트에게 전송한다. 세째로 그룹 통신을 위한 동일한 사용자 명(그룹 명)은 모든 그룹의 멤버가 사전에 생성하여 두었거나 필요한 경우 매니저의 명령 수행 중에 생성 한다고 가정하다. SNMPv3에서 매니저의 에이전트로의 접근 통제는 기본적으로 사용자 명을 기반으로 이루어지므로 그룹 통신을 위해서는 모든 그룹의 멤버들이 공유하는 그룹 명이 필요하다. 마지막으로SNMP와 GKM 사이에는 매니저와 에이전트들이 GKM에게 특정 그룹에 가입을 요청하여 응답을 받고 GKM으로 부터 그룹 키를 받기 위한 간단한 인터페이스나 API만이 존재 한다고 가정 한다. 본 아키텍처가 범용의 GKM를 활용할 수 있도록 최소한의 인터페이스나 API (Application Programming Interface)를 가정한 것이다.

4.2 Management Information(Data) Base 정의

에이전트와 매니저가 그룹 멤버쉽 관리를 위하여 정의한 usmUserGroupTable은 아래 표 1과 같다. 매니저는 매니저가 관리하는 그룹에 관한 정보와 각 그룹에 속하는 에이전트들에 관한 정보가 필요하지만, 에이전트는 자신이 가입된 그룹에 관한 정보와 응답 메시지를 전송할 목적지에 관한 정보가 필요하다. 매니저가 관리할 그룹 정보는 일반적인 데이타베이스의 테이블로 정의하여 관리하고, 에이전트가 관리할 그룹 정보는 표준 SNMP MIB-II에 그룹 관련 MIB을 추가한 확장 MIB으로 관리 한다.

표 1 그룹 관리를 위한 테이블

Field Name	Description	Manager	Agent
grpID	Group identification	√	√
grpAddr	Group IP address	√	√
grpPortID	Group port number	√	√
grpKeyMaterial	Key material from GKM	√	√
grpEngineID	Group member shared engine ID	√	√
destGrpID	Dest. group identification		√
userID	User name	√	√
userAddr	User IP address	√	√
userAuthKey	User authentication key	√	√
userPrivKey	User privacy key	√	√
status	Membership status	√	√

4.3 표준 SNMPv3의 확장

에이전트가 그룹에 가입하거나 탈퇴하는 방법은 매니저가 초청하는 경우(Manager-initiated)와 에이전트가 자발적으로 요청하는 경우(Agent-initiated)로 나눌 수 있으나 본 연구에서는 에이전트의 그룹에 가입과 탈퇴는 모두 매니저의 통제 하에 이루어진다고 보고 매니저가 초청하는 경우만 고려하였다.

4.3.1 SET 명령의 확장

매니저는 어떤 그룹에 가입하기를 원하는 에이전트에게 보내는 초청 메시지로 SET 명령을 사용한다. 하지만 표준 SET명령은 매니저가 에이전트에게 특정 변수를 어떤 값으로 설정하도록 지시하는 명령이므로 표준 SET의 동작에 그룹을 처리할 수 있는 기능을 추가 하여야 한다. 표준 SNMPv3에서 SET 명령은 최소한 사용자 인증과정은 거치도록 규정되어 있다[5, 7]. 사용자 인증을 위해서 SET의 패러미터에는 매니저와 에이전트간에 공유한 사용자 이름과 패스워드를 포함한다. SET이 그룹에 관한 명령인 경우 SET명령은 확장된 MIB에 속하는 groupID, groupAddr, 그리고 groupPortID 등에 어떤 값을 가지고 에이전트에게 전송된다. 각각의 변수 값이 NULL이면 그룹 탈퇴 요청으로 인식하고 그렇지 않으면 그룹 조인 초청 명령으로 인식한다. 그룹 조인의 경우 먼저 SNMP 외부의 그룹 키 매니저로부터 그룹 키를 받는다. 받은 그룹 키로부터 그룹이 공유할 engineID를 그룹 키의 앞에서부터 사용하는 암호화 알고리즘에 따라 일정 부분을 절취하여 생성한 다음 에이전트로부터 응답 메시지를 받기를 기다린다. 에이전트로부터 받은 응답 메시지에 포함된 그룹 정보에 의하여 에이전트가 그룹 키 관리 시스템에 성공적으로 등록되었음이 확인되면 그 에이전트를 자신의 그룹 관리 테이블을 갱신함으로써 새로운 멤버로 추가 시킨다. 마지막으로 새로 전달 받은 그룹 키를 갱신한다. 그룹 탈퇴의 경우에는 그룹 탈퇴 요청이 성공적으로 수행되었음을 알리는 응답을 에이전트로부터 받으면 그 에이전트를 그룹 테이블에서 그 에이전트 자료를 불활성화 시킨다. 마지막으로 새로운 그룹 키를 키 매니저로부터 받아서 그룹 키를 갱신한다. 확장된 모듈들을 제외한 나머지 부분은 표준 SET

이 동작하는 과정이다. 표준 SET에서 SET명령이 그룹에 관한 명령일 때 SET이 에이전트에게 engineID를 받아오기 위해서 보내는 메시지 전송부분을 제외하면 나머지는 동일하다.

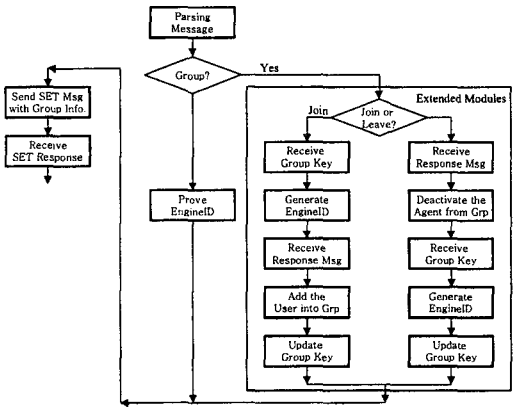

그림 2 수정된 SET명령의 동작

4.3.2 에이전트의 확장

표준 에이전트는 메니저의 SET이나 GET명령을 수행하고 그 결과인 응답 메시지만을 전송함으로, 표준 에이전트 엔진이 메니저의 SET 명령을 그룹 처리 명령으로 인식하고 그룹 멤버쉽과 그룹 키를 처리할 수 있는 모듈들이 추가되어야 한다. 확장된 MIB에 속하는 groupID, groupAddr, 그리고 groupPortID등의 값들이 NULL이 아니면 그룹 가입 초청 명령으로 인식하고 그렇지 않으면 그룹 탈퇴 요청으로 간주한다. 그룹 초청의 경우 수신한 그룹 정보에 의하여 자신의 MIB 테이블을 검색하여 이미 그 사용자 이름(에이전트 입장에서는 그룹 이름과 일반 사용자 이름을 구분하지 않음)이 usmUserTable에 존재하면 확장된 그룹 관련 MIB인 usmUserGroupTable에 존재하는 그룹 이름을 활성화 시키고, 존재하지 않을 경우 groupName의 값으로 새로운 사용자 이름을 생성하여 usmUserTable에 저장하고 관련 그룹 정보와 함께 usmUserGroupTable에도 새로운 행을 추가 한다. 다음으로 에이전트는 SNMP외부에 있는 그룹 키 관리 시스템에게 초청을 받은 그룹에 가입시켜 줄 것을 요청하여 그룹 키를 받고, 받은 그룹 키로부터 그룹이 공유할 engineID를 그룹 키의 앞에서부터 사용하는 암호화 알고리즘에 따라 일정 부분을 절취하여 생성한다. 마지막으로 그룹 usmUserGroupTable에 그룹 정보를 갱신한다. 탈퇴 요청의 경우에는 그룹 키 관리 시스템에게 탈퇴를 요청하여 요청에 대한 응답을 받으면 usmUserGroupTable의 관련 그룹 이름을 불활성화 시킨다. 확장된 모듈들을 제외한 나머지 부분은 표준 에이전트가 동작하는 과정이다. 표준 에이전트에서 SET 명령이 그룹에 관한 명령일 때는 SET이 에이전트에게 engineID를 받아오기 위한 메시지가 없으므로 engineID를 전송하는 부분을 제외하면 나머지는 동일하다.

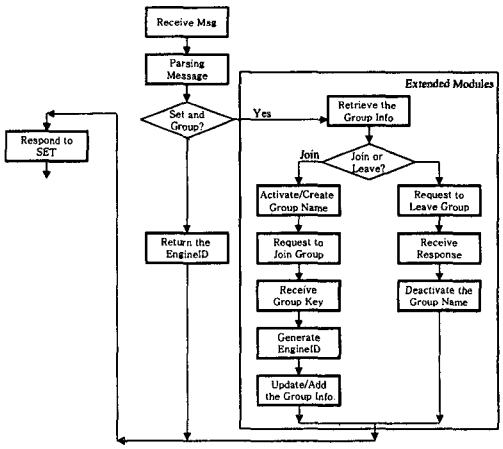

그림 3 수정된 SNMP 엔진의 동작

5. 결론

기존의 망 관리 시스템들의 구조는 하나나 둘 정도의 중간 관리 시스템이 전체 관리 대상 시스템들 중 일부를 관리하고 이러한 중간 관리 시스템들을 모아서 다시 상위의 관리 시스템이 통제하는 계층 구조이다. 표준 SNMP를 사용하는 망 관리 시스템 환경에서도 비슷한 형태의 망 관리구조를 가지게 되는데 그 주된 원인인 일대일 연결에서 벗어나 안전한 멀티캐스트 개념을 도입함으로써 다양한 형태의 효율적인 관리 구조를 정의할 수 있다. 본 논문에서는 표준 SNMP와 호환이 가능하면서도 안전한 멀티캐스트 서비스를 제공할 수 있는 방안을 제안 하였다. 제안한 구조는 망 관리 객체들을 적절히 그룹핑 하였을 때 매우 효과적으로 활용될 수 있다고 본다.

참고문헌

[1] D. Zeltserman, " A Practical Guide to SNMPv3 and Network Management," Prentice Hall, 1999

[2] W. Stallings, " SNMPv3: A Security Enhancement for SNMP," IEEE Communications Survey, Vol.1 No.1, 1998

[3] E. Al-shaer, Y. Tang, " Toward Integrating IP Multicasting in Internet Network Management Protocols," June 2000

[4] J. Schoenwaelder, " *Using Multicast-SNMP to Coordinate* Distributed Management Agents, " Proceedings of the 2nd IEEE International Workshop on Systems Management (SMW'96), p.136, June 19-21, 1996

[5] U. Blumenthal and B. Wijnen, " User-based Security Model (USM)for version 3 of the SNMP," IETF RFC 3414, Dec. 2002.

[6] 곽득휘, 김종원, " 안전한 실시간 멀티캐스트를 위한 그룹 키 관리 프로토콜 표준들의 비교," 제4회 RMT 프로토콜 워크샵, 2003년 4월.

[7] J. Case, D. Harrington, R. Presuhn, and B. Wijnen, " Message Processing and Dispatching for the SNMP," IETF RFC 2572, April 1999.