SNMP 기반의 이동형 네트워크 장비 관리 기법

정회원 곽 득 휘*, 이 현 룡**, 김 종 원**

SNMP-based Management for Mobile Network Devices

Deuk-Whee Kwak*, HyunYong Lee**, JongWon Kim** ***Regular Members***

요 약

모바일 네트워크 노드, 이동형 액세스 포인트, ad-hoc 네트워크 노드 등과 같은 장비들은 수시로 이동할 수 있으며 그 사용 특성상 다수의 장비가 지역적으로 넓게 분포된다. 이러한 환경에서는 관리대상 노드는 물론 관리자 노드조차도 수시로 네트워크에서 이탈할 수 있으므로 네트워크의 토폴로지가 수시로 변한다. 기존의 많은 네트워크 관리 기법들은 대부분 토폴로지가 정적이며 상대적으로 적은 규모의 동질적인 네트워크 요소로 구성되는 네트워크를 관리하는 기법이므로 이동형 장비를 관리하는 기법으로는 적당하지 않다. 본 논문은 P2P (Peer-to-Peer)와 안전한 그룹통신 기법 그리고 SNMP (Simple Network Management Protocol)를 사용하여 이동성이 높은 장비들을 인터넷을 통하여 안전하게 어디서나 관리할 수 있는 기법을 제안한다. 제안한 기법은 구현을 통하여 그 실용성을 증명한다.

Key Words : Network Management, Ad-Hoc, Secure Group, SNMP, P2P

ABSTRACT

Some types of network nodes such as mobile network node, mobile access point, and ad-hoc network node can be relocated frequently and, by the nature of its usage, are deployed over broad area. In this environment, the network topology is changed constantly since even the manager node as well as the managed nodes can leave or join the management network frequently. The many of existing network management technologies are mostly for small sized and homogeneous networks with static topologies and not proper for the mobile network devices. In this paper, employing peer-to-peer (P2P), the secure group communication techniques, and simple network management protocol (SNMP), we propose a highly secure and available management technique that can be used to manage the mobile network nodes through insecure management network such as the Internet. The proposed technique is implemented to show that it is practically usable.

I. 서 론

모바일 네트워크 노드, 이동형 액세스 포인트, ad-hoc 네트워크 노드 등과 같은 장비들은 수시로 이동할 수 있다. 일반적으로 장비들의 이동성은 이들을 관리하는 관리자 노드와 관리대상 노드가 항상 동일한 지역 네트워크에 소속되어 있어야만 가능하다. 또한 이동형 액세스 포인트와 같은 장비들은 그 사용 특성상 다수의 장비가 지역적으로 넓게 분포되어 지역 관리자에 의한 관리 구조는 적절하지 않다. SNMP (Simple Network Management Protocol)를 포함한 기존의 네트워크 관리 기법들은

※ 본 연구는 지식경제부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었습니다 (IITA-2008-C1090-0803-0004).
※ 본 논문은 2008 jcci 우수논문으로 추천되었습니다.
* KT 플랫폼연구소 서비스플랫폼개발담당 (dhkwak@kt.com), ** 광주과학기술원 정보통신공학과 네트워크미디어 연구실 (hrlee, jongwon@nm.gist.ac.kr)
논문번호 : KICS2008-05-242, 접수일자 : 2008년 5월 28일, 최종논문접수일자 : 2008년 7월 13일

대부분 토폴로지가 정적이며 상대적으로 적은 규모의 동질적인 네트워크 요소로 구성되는 네트워크를 관리하는 기법이다[1]. 고정형 노드 관리 기법을 이동형 노드 관리를 위해 직접 적용하는 것은 이동형 노드 관리의 특성으로 인하여 다음과 같은 한계가 있다. 첫째 장애관리 접근법이 다르다. 고정형 노드 관리 기법은 고정된 IP[1]를 전제로 한다. 그러므로 관리대상 노드(이하 관리대상 또는 SNMP에서는 대행자)가 네트워크 관리자 노드(이하 관리자)의 관리 명령에 응답하지 않으면 관리 네트워크 또는 관리 대상이 고장인 경우이다. 하지만 관리대상이 이동이 가능한 환경에서 관리대상의 무응답은 이들이 고장인 경우도 있지만 관리네트워크상에 존재하지 않는 경우도 있다. 그러므로 이동형 노드 환경에서 장애관리 기법은 고정형 노드 장애관리 기법과는 접근방법이 다르며 더욱 어려운 문제이다. 둘째 네트워크의 토폴로지가 수시로 변한다. 이동형 노드들은 주변 환경에 따라 끊임없이 네트워크에 가입하거나 탈퇴하면서 토폴로지를 변경시킨다. 따라서 네트워크를 구성하는 노드 수는 매우 동적으로 변하므로 이동형 노드 관리 기법은 확장성이 좋아야 한다. 셋째 보안에 더욱 취약하다. 기존의 관리정보망은 폐쇄된 전용망을 사용하거나 대부분 유선구간이므로 상대적으로 보안 공격에 덜 노출되어 있다. 하지만 이동형 장비들은 대부분 무선 장비들이고 여러 관리 도메인에 걸쳐 분포될 가능성이 높다. 따라서 인터넷을 통하여 관리하는 것이 바람직하지만 이러한 환경은 보안 공격에 상대적으로 취약하다. 넷째 관리자 자체가 네트워크에 존재하지 않을 수도 있다. 관리자가 속한 네트워크가 이동 중에 관리대상들의 네트워크로부터 분리될 수 있으며 경우에 따라서 비활성 상태일 수도 있다. 그러므로 관리대상은 관리자가 관리 네트워크상에 존재하는지 여유와 관리자가 사용 중인 IP를 점검하여야 한다.

본 논문은 이동형 노드 관리의 특성을 고려한 이동성이 높은 장비들을 인터넷을 통하여 안전하게 어디에서나 관리할 수 있는 기법을 제안한다. 제안한 기법은 P2P (Peer-to-Peer)와 안전한 그룹 통신 기법 그리고 SNMP 를 사용한다. P2P와 데이터 기밀성은 관리대상의 정보를 안전하게 수집하기 위하여 사용한다. 안전한 그룹 통신은 개방된 인터넷 환경에서 안전한 그룹을 구성하고 SNMP 오퍼레이션과 응답 메시지를 더욱 효율적이며 안전하게 전달하기 위한 기법이다. 표준 인터넷 망 관리 프로토콜인 SNMP는 SNMPv3 (SNMP version 3)의 *pass phrase*를 안전한 그룹의 그룹 키로 활용할 수 있는 방안을 제시한다.

논문의 구성은 다음과 같다. 제Ⅱ절에서는 네트워크 관리에 P2P기법 적용이나 SNMP를 확장한 연구들을 살펴보고, 제Ⅲ절에서는 제안한 기법과 관련된 기술들을 소개한다. 제Ⅳ절에서는 본 논문에서 제안하는 기법을 상세히 설명한다. 제Ⅴ절에서는 제안한 기법을 구현한 시스템을 설명한 다음, 제Ⅵ절에서 결론과 향후 연구를 제시한다.

Ⅱ. 관련 연구

[1]에서 저자들은 P2P의 자율구성(Self-organization), 대칭형 통신, 분산 통제 기술들을 네트워크 관리 기술로 활용하여 확장성이 좋은 관리 프레임워크를 제안한다. 프레임워크를 구성하는 핵심요소는 AMC (Adaptive Management Component)이다. AMC는 요소관리 기능이 있어서 NE(Network Element)를 직접 관리하며, P2P기능이 있어서 AMC간 P2P통신으로 관리 정보를 교환하기도 한다. 즉 제안한 프레임워크는 AMC가 NE 수준의 관리 기능을 직접 수행하고, 네트워크 수준의 관리 기능을 수행하기 위하여 AMC간 관리정보 교환을 목적으로 P2P 기법을 활용한다.

[2]는 ad-hoc 네트워크 관리를 위하여 표준 SNMPv3와 호환성을 유지하면서 가벼운 ANMP (Ad-hoc Network Management Protocol)을 제안한다. ANMP는 ad-hoc 환경에서 필요한 정보 수집을 위하여 표준 SNMP의 MIB(Management Information Base)을 확장하고, SNMPv3와 호환이 가능하도록 SNMPv3와 동일한 PDU (Protocol Data Unit) 구조를 사용하며 UDP상에서 수행되지만, 표준 SNMP보다 훨씬 강력한 에이전트 통제 기능을 가지고 있다. 또한 ANMP는 표준 SNMP에는 없는 보안 멀티캐스트 기능을 가지고 있어서 네트워크 노드들을 효율적으로 설정할 수 있다.

[3]은 P2P 기술을 네트워크 관리 도구로 활용하는 3가지 방안을 제시한다. 첫째는 사람을 기반으로 한 협력관리 방식으로, 관리 업무를 수행하기 위하여 관리자인 사람이 최상위 수준에서 P2P의 메신저, 파일 공유 등을 통하여 다른 도메인에 속하는 관리자와 협력하는 방식이다. 둘째는 매니저와 에이전트 간에 메시지 교환을 위한 연결성을 향상시킬

1) 본 논문은IPv4를 전제로 한다.

목적으로 P2P를 사용하는 방식이다. P2P에 의한 응용계층에서의 라우팅은 TCP/IP보다 유연하며 신뢰성이 높은 연결성을 제공한다. 셋째는 관리 업무를 여러 매니저에게 분산시키는 방식이다. 관리업무를 중간계층의 관리 노드들에게 분산시키기 위하여 P2P에 의하여 관리 노드들을 피어 그룹으로 묶고, 동일한 그룹에 속하는 피어 노드들에게 부하를 균등히 분배한다.

Ⅲ. 관련 기술

본 장에서는 본 논문에서 제안한 기법과 관련된 기술들을 소개한다.

3.1 SNMPv3의 키 생성 기법

SNMPv3는 USM(User-based Security Model)을 사용하여 인증과 무결성 그리고 암호화 서비스를 제공하는데 각 사용자가 하나의 패스워드에서 다수의 서버들과 안전하게 통신할 수 있도록 키 지역화(key localization) 개념을 사용한다[4]. 먼저 매니저와 에이전트간에 사전에 공유한 *pass phrase*는 220 문자길이가 될 때까지 반복하여 연결(concatenate)한다. 이렇게 확장된 *pass phrase*는 MD5나 SHA-1 해쉬 함수를 통하여 16이나 20 문자길이의 마스터 키를 생성하게 되고, 생성된 마스터 키와 에이전트의 *engineID*를 연결한 문자열을 입력으로 다시 해쉬 함수를 통과시키면 각각의 *engineID*를 소유한 에이전트들과 매니저간에만 공유하는 비밀키가 생성된다 (그림 1 참고).

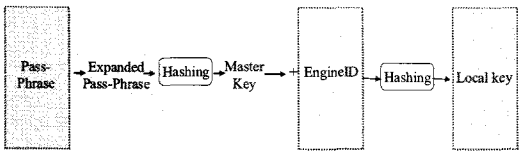


그림 1. SNMP의 지역키 생성 절차.

3.2 TGDH

그룹에 새로운 멤버가 가입하거나 기존 멤버가 탈퇴하여 그룹의 멤버쉽이 바뀌면 FS(Forward Secrecy)와 BS(Backward Secrecy)를 보장하기 위하여 그룹 키를 갱신하여야 한다. 그룹 키 관리(GKM: Group Key Management) 프로토콜은 그룹 키를 갱신하여 멤버들에게 분배하는 기능 외에도 그룹의 멤버쉽을 관리하는 기능을 수행한다. TGDH(Tree-based Group Diffie Hellman)는 중앙의 키 관리자 없이 멤버들간에 협의에 의하여 그룹 키를 생성하기 때문에 분산환경에 적용 가능한 그룹 키 생성 알고리즘이다[5].

TGDH는 키 트리와 그룹 Diffie-Hellman (DH) 키 교환 기법에 기초한다. 키 트리는 그룹 멤버들이 관리해야 하는 키의 수를 줄이기 위해 사용되며, DH 알고리즘은 안전하며 분산 속성을 지닌 키 생성을 위해 사용한다. TGDH에서의 키 생성은 OFT(One-Way Function Tree)의 방법과 유사하지만, 대신 OFT에서 사용하는 단방향 해쉬 함수가 아닌 DH 알고리즘을 사용한다. TGDH는 각 그룹 멤버들이 키 생성을 위해 필요한 정보들을 모두 제공하고, 모든 그룹 멤버들은 이 정보에 기초하여 그룹 키를 생성한다.

그룹 키를 형성하기 위해 각 노드는 자신(노드 i)로부터 키 트리 T의 루트에 이르는 경로(path)에 존재하는 노드의 형제 노드의 블라인드 키 $SIB_BLD(T, i)$를 알아야만 한다. 블라인드 키는 특정 노드가 생성한 키 값을 연산을 통해 변형시켜서 해당 키 값을 보유하지 않은 다른 노드들에게 공개하는 값으로 다음과 같이 계산된다. $f(x) = a^x \bmod p$(a는 지수의 밑, p는 소수)라고 정의할 때, 높이 l의 v번째 키 $K<l,v>$의 블라인드 키 $BK<l,v>$는 $f(K<l,v>)$로 계산된다. 키 $K<l,v>$를 생성하기 위해서는 자신의 자식 노드 중 한 노드의 블라인드 키 값과 다른 한 노드의 비밀 키 값을 알아야만 한다. 이러한 방법으로 키 트리의 리프 노드에서부터 루트 노드까지 순차적으로 적용하면서 그룹 키를 형성할 수 있다. 그룹 키는 키 트리의 루트 값인 $K<0,0>$이다.

만약 새로운 그룹 멤버가 그룹에 추가되면, 누군가가 새 멤버를 키 트리에 추가하고 새로운 키 트리 구조와 SIB_BLD를 계산하여 다른 멤버 노드들에게 전달해야 한다. TGDH에서 이 역할을 수행하는 멤버를 스폰서라 하고 어떤 그룹 멤버도 스폰서의 역할을 수행할 수 있다. 그룹 가입의 경우에는 스폰서 노드는 새로운 노드가 삽입된 서브트리의 가장 오른쪽 노드이다. 또한 그룹 탈퇴의 경우의 스폰서 역할은 탈퇴한 노드가 속했던 서브트리의 가장 오른쪽에 있는 노드가 담당한다.

Ⅳ. 제안 기법

본 절은 언제든지 이동이 가능한 네트워크 장비들을 인터넷과 같은 개방된 네트워크 환경에서 안

전하게 어디에서나 관리할 수 있는 기법을 제안한다. 제안 기법은 P2P 와 안전한 그룹 통신 기법 그리고 SNMP를 사용하여 모바일 네트워크 노드, 이동형 액세스 포인트, ad-hoc 네트워크 노드 등과 같은 이동 네트워크 장비를 안전하게 어디에서나 상태를 파악하고 제어할 수 있는 관리 기술이다. 즉 인터넷 상에서 이동 가능한 관리대상 장비들에 대해서 P2P 기법으로 네트워크상의 존재 여부와 사용중인 IP를 파악하고, 안전한 그룹 통신 기법을 사용하여 논리적으로 폐쇄된 안전한 그룹을 구성하며, SNMP에 의하여 장비의 상태를 파악하거나 제어한다. 제안 기법을 적용하기 위해서는 사전에 모든 그룹 멤버들은 관리자와 관리대상간에 독립적인 그룹 관리 프로토콜을 수행하여 얻어진 비밀키 *Ka*를 각각 공유한다고 가정한다[6].

4.1 P2P를 통한 시그니처 파일 전송 및 인증

본 논문이 제안하는 기법에서 P2P는 시그니처 파일(signature file)[2]을 공유하는 방법으로 사용된다. 사용할 수 있는 P2P기법에 대한 제약은 없지만 본 논문은 동적 네트워크 환경에 적합한 순수 P2P기법 중 하나인 메쉬 P2P를 사용한다.

시그니처 파일은 관리자나 관리대상이 사용중인 IP 주소와 이름 등의 정보가 저장된 일반 파일이다. 그러므로 노드가 이동하여 사용하는 IP 주소가 바뀌면 노드는 자신의 시그니처 파일을 갱신하고 특정 P2P 사이트에 공유시켜야 한다. 관리대상 노드의 시그니처 파일 *SigFile*의 포맷은 표 1과 같다.

표 1. 시그니처 파일의 포맷.

SigFile: Sig, (ID, IP, H(Sig|ID|IP))Ka	
항목명	항목 설명
Sig	시그니처
ID	관리대상 노드 ID
IP	노드가 사용중인 IP
Ka	관리자와 관리대상간 공유한 비밀키
H(M)	*M*을 입력으로 한 해쉬 함수. 해쉬 알고리즘은 MD5나 SHA-1등을 사용할 수 있음
(M)Ka	*M*을 키 *Ka*에 의하여 암호화. 암호화 알고리즘은 3DES나 AES등을 사용할 수 있음

관리대상 노드의 *SigFile*은 네트워크 상에서의 공격으로 보호하기 위하여 암호화하여 배포된다. 암호화에 사용되는 키 *Ka*는 관리대상이 그룹 가입 절차를 마치면 관리자와 관리대상 간 공유하게 되는 비밀키이다. 시그니처는 노출되는 정보이므로 시그니처의 대량생성으로 매니저의 부하를 가중시키는 악의적인 공격을 피하기 위하여 주기적으로 또는 필요할 때마다 갱신한다. 시그니처 갱신을 위한 시그니처의 생성 및 분배는 관리자가 수행한다. 시그니처의 갱신은 그룹 키 갱신 절차를 활용하여 효율적으로 수행할 수 있다. 즉 관리자가 그룹 키를 갱신할 때 각 관리대상에게 전달되는 키 갱신 메시지에 갱신된 시그니처를 추가하여 전송하면 미미한 추가적인 부하로 그룹 시그니처 갱신이 가능하다. 시그니처 파일을 수신한 노드는 파일의 무결성을 점검한다. 시그니처 파일은 *Sig, ID, IP*를 직렬로 연결하여 생성한 메시지를 입력 데이타로 사용한 해쉬 값인 *MD1= H(Sig|ID|IP)*을 포함하고 있다. 시그니처 파일 수신자는 수신한 시그니처 파일에서 *MD2= H(Sig|ID|IP)*를 계산하고 일치여부 (즉 *MD1=MD2*)를 확인하여 파일의 무결성을 점검한다.

4.2 관리자의 보안그룹 관리

관리자가 관리대상을 SNMP를 사용하여 관리하기 위해서는 관리자는 관리대상의 IP를 알아야 한다. 관리대상이 수시로 이동할 수 있는 환경에서는 관리대상의 IP의 변동이 가능하며, 관리대상의 네트워크상 존재 여부조차도 알 수 없다. 그러므로 관리자는 SNMP로 관리명령을 보내기 전에 관리 네트워크에 존재하는 관리대상과 이들이 사용하는 IP를 파악하여야 한다. 관리자는 관리대상을 찾기 위하여 P2P를 통하여 특정 파일 이름을 검색한다. 파일 이름은 그룹마다 유일하며 본 논문에서는 이것을 그

```
Manager:

group G;
if (not exist G) {
    create G;
    get agent signature file SigFile_A from the P2P;
    authenticate SigFile_A;
    invite the pre-members to join G;
    receive the join requests;
}
else {
    receive the group join request;
}
authenticate the pre-member;
create group key KG and agent signature Sig_A;
distribute KG and Sig_A to the group member;
```

그림 2. 관리자 알고리즘.

2) 이하에서 시그니처와 시그니처 파일은 특별히 언급하지 않으면 동일한 의미로 혼용한다.

룹의 시그니처이라고 한다.

관리자가 관리 대상을 파악하고 그룹 키를 분배하는 알고리즘은 그림 2와 같다. 관리자는 관리할 대상들의 집합인 그룹 *G*가 존재하지 않으면 *G*를 생성하고 관리대상들의 시그니처 파일 *SigFile_A*를 P2P를 통해 수집한다. *SigFile_A*가 유효하면 *SigFile_A*에 저장된 IP를 통하여 예비 멤버들에게 *G*에 가입하도록 초대하고 초대에 응한 관리대상들을 그룹에 가입시킨다. 그룹 멤버쉽이 변경되었으므로 관리자는 그룹키 *KG*와 시그니처 *SigFile*를 갱신하여 그룹 멤버들에게 분배한다.

관리자는 관리대상의 IP를 ID와 함께 DB (Data Base)에 저장하여 추후 관리 정보로 활용한다. DB의 스키마는 표 2와 같다.

표 2. 데이타베이스 스키마.

필드명	관리자 관점의 의미	관리대상 관점의 의미
grpID	관리할 그룹 명	소속된 그룹 명
grpKeyMaterial	그룹키	그룹키
Sig	그룹의 시그니처	그룹의 시그니처
mbrID	그룹 멤버의 ID	사용중인 ID
mbrIP	그룹 멤버의 IP	사용중인 IP

4.3 관리대상의 보안그룹 가입

관리대상이 네트워크에 연결되면 관리자의 관리를 받기 위하여 관리 그룹에 가입하여야 한다. 그룹 가입은 그룹의 관리자를 찾는 단계부터 시작된다. 관리대상은 가입하려는 안전한 그룹의 관리자를 찾기 위하여 P2P를 통하여 특정 파일 이름을 검색한다. 파일 이름은 특정 그룹 관리자마다 유일하며, 본 논문에서는 이것을 관리자 시그니처이라고 한다. 관리자의 시그니처 파일 *SigFile_M*의 포맷은 그룹의 시그니처 파일 포맷과 동일하다 (표 1 참고).

관리대상이 관리 그룹에 가입하고 그룹 키를 수신하는 알고리즘은 그림 3과 같다. 대행자는 관리자의 시그니처 파일 *SigFile_M*을 찾음으로써 네트워크상에 관리자가 존재하는지 확인한다. *SigFile_M*이 유효하면 *SigFile_M*에서 획득한 IP를 통하여 그룹 *G*에 가입신청을 한다. 정당한 관리자인지 확인후 관리자가 보낸 그룹 키 *KG*와 시그니처 *Sig_A*를 수신한다. *KG*로 그룹 키를 갱신하고 *Sig_A*로 시그니처 파일 *SigFile_A*을 생성한 다음 P2P사이트에

```
Agent:

group G;
search manager signature file SigFile_M from the P2P;
if (found SigFile_M) {
    authenticate SigFile_M;
}
else {
    receive G join invitation;
}
request to join G;
authenticate the group manager;
receive the group key KG and signature Sig_A;
update the group key with KG ;
create signature file SigFile_A;
place SigFile_A on the P2P;
```

그림 3. 대행자 알고리즘.

*SigFile_A*을 공유시킨다.

관리대상은 자신이 소속된 그룹 정보를 자신의 IP, ID와 함께 DB에 저장한다. DB의 스키마는 표 2와 같다.

4.4 그룹 멤버의 위치 이동에 따른 시그니처 파일의 갱신

관리자나 관리대상 등 그룹의 멤버가 이동하여 사용하는 IP가 변경되면, 바뀐 IP로 시그니처 파일의 IP정보를 갱신한다. 관리대상은 갱신된 파일을 관리자에게 전송하고, P2P를 통하여 공유하여 추후에도 매니저가 사용할 수 있도록 한다. 한편 관리자는 갱신된 파일을 P2P를 통하여 공유하지만, 관리자의 IP는 관리대상들에게 SNMP를 통하여 전송되기 때문에 관리대상들에게 전송하지는 않는다.

4.5 관리대상의 보안그룹 탈퇴

관리대상이 어떤 이유로 관리대상에서 일시적으로 벗어나고자 할 때 수행하는 절차이다. 먼저 관리대상은 관리자에게 그룹 *G*로부터의 탈퇴를 요청한다. 관리자는 탈퇴 신청을 처리하고 그룹 키 *KG*와 그룹 시그니처 *Sig_A*를 갱신하고 *KG*와 *Sig_A*를 *G* 멤버인 관리대상들에게 분배한다. 그룹 *G*의 멤버 관리대상들은 자신의 시그니처 파일 *SigFile_A*를 갱신하고 P2P를 통하여 공유시키며, 그룹 *G*에서 탈퇴한 관리대상은 P2P에서 자신의 시그니처 파일의 공유를 해제한다.

4.6 SNMP의 보안그룹 구성

네트워크 관리를 위한 프로토콜은 SNMP version 3 (SNMPv3)을 사용한다[4]. SNMPv1과 SNMPv2는

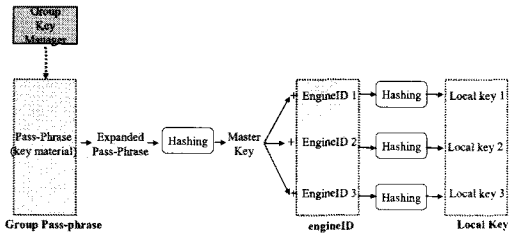


그림 4. SNMPv3에서 그룹 키 생성 절차.

사용자 인증 기능은 있으나 메시지 암호화 기능은 제공하지 않는다. SNMPv3는 인증과 기밀성 서비스를 위하여 *pass phrase*를 사용한다. 즉 *pass phrase*는 그 자체로 그룹키는 아니지만 SNMP *EngineID*와 함께 인증 및 암호화 키 생성에 사용된다. 즉 *pass phrase*는 일종의 키 생성 물질로 사용된다. 동일한 *pass phrase*를 여러 에이전트가 공유해도 각각의 에이전트의 *EngineID*가 서로 다르므로 결국 서로 다른 키가 생성된다. 하지만 SNMP 매니저와 에이전트 간 인증과 기밀성 서비스를 위하여 사용자가 감추어야 할 비밀은 *pass phrase* 뿐이다. 그러므로 *pass phrase*는 그룹 멤버들이 공유하는 그룹키로 간주할 수 있으며, SNMP 매니저와 에이전트들이 이 *pass phrase*를 통하여 안전한 그룹을 구성할 수 있다. 또한, 그룹 멤버쉽에 변화가 발생하면 *pass phrase*를 갱신함으로써 그룹 키 갱신의 효과를 얻을 수 있다. *pass phrase*로부터 그룹 키를 생성하는 과정은 그림 4와 같다.

그룹 키에 해당하는 *pass phrase* 갱신에는 중앙집중 키 관리 방식에서는 IETF의 GDOI(The Group Domain of Interpretation)[6]나 GSAKMP(Group Secure Association Key Management Protocol)[7] 등을 사용할 수 있고 분산협력 방식에서는 TGDH등을 사용할 수 있다. SNMP 환경에서 그룹의 멤버들이 공유한 그룹 키를 통하여 보안 그룹을 구성하는 예는 그림 5와 같다. 보안 그룹 멤버들은 하나의 *pass phrase*를 공유한다. 그림 5는 *KG1*과 *KG2*에 의하여 2개의 보안 그룹을 구성한 예이다. 비관리대상 장비들은 *KG1*이나 *KG2*를 알지 못하므로 이 두개의 *pass phrase*에 의하여 생성된 키에 의하여 암호화된 SNMP 오퍼레이션이나 결과메시지를 인터넷 상에서 받을 수는 있지만 해독할 수는 없다. 관리자는 관리 목적에 따라 여러 보안 그룹을 생성하여 관리대상들을 포함시킬 수 있지만 관리대상은 하나의 그룹에만 소속될 수 있다.

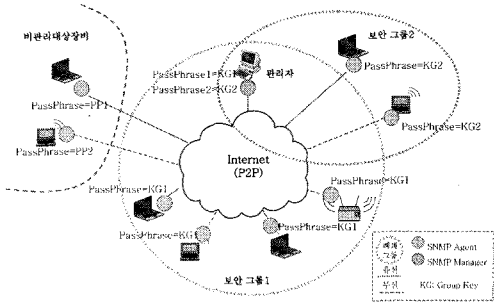


그림 5. SNMP 환경에서 보안 그룹을 구성한 예.

V. 구 현

본 구현에서는 논문에서 제안한 이동형 장비를 인터넷을 통하여 안전하게 관리하는 기법의 실용성을 검증하고자 한다.

5.1 구현 환경

시스템은 리눅스 시스템을 기반으로 하여 C 언어와 Python 언어를 사용하여 구현하였다. 구현에 사용한 리눅스 시스템의 종류는 Ubuntu 6.06 LTS이다. 시스템의 각 컴포넌트별 구현 사항은 다음과 같다.

- P2P 통신 및 노드 검색: 메쉬 기반 P2P 네트워크
- 그룹 키 관리: TGDH (Tree-based Group Diffie Hellman)
- 토폴로지 가시화: Python 언어
- SNMP: net-snmp-5.3.2
- 메시지 암호화/복호화: AES (Advanced Encryption Standard)
- 해쉬 함수: OpenSSL MD5

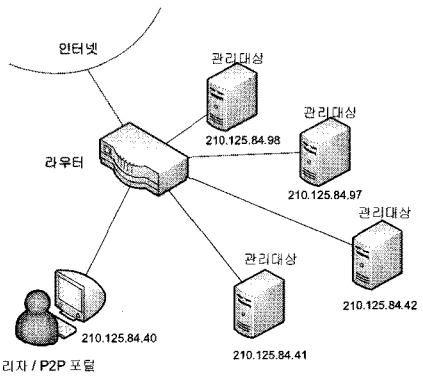


그림 6. 구현 시스템 적용 환경

5.2 관리 시스템 구조

본 프로토타입 시스템 구현은 크게 관리 대상을 검색하고 관리 대상으로부터 SNMP를 통해 정보를 수집하는 관리자와, 관리자를 검색할 수 있고 관리자의 명령에 기초하여 해당 정보를 관리자에게 전송하는 대행자의 구현으로 이루어진다. 그림 7은 관리자의 구조이고 그림 8은 대행자의 구조이다. 관리자와 대행자의 주요 구현 부분은 P2P 통신, 에이전트/매니저 검색, SNMPv3를 통한 노드 정보 수집, 노드 인증, 그룹 키 관리로 분류할 수 있다. 본 논문에서 노드 인증은 다른 프로토콜을 통하여 가능하다고 가정하여 구현하지 않았다 그림에서 실선으로 표시된 부분은 구현을 하지 않는 부분이며, 점선으로 처리된 것들은 구현한 부분이다. 그림의 화살표는 기능들 사이의 통신과 전달하는 정보를 나타낸다.

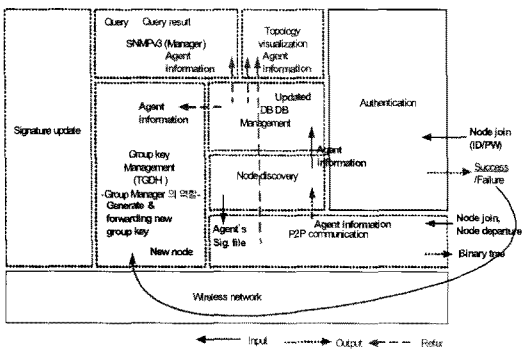


그림 7. 구현한 시스템의 관리자 구조.

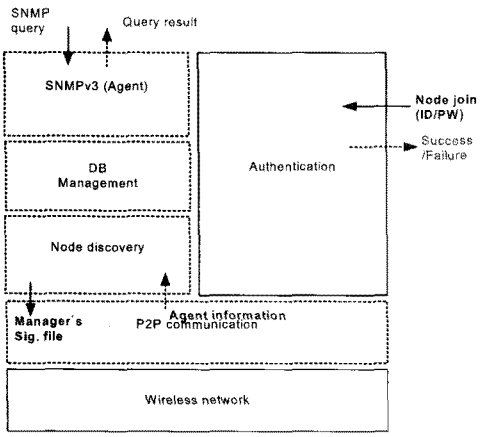


그림 8. 구현한 시스템의 대행자 구조.

5.3 관리자 구현

관리자 또한 데몬으로 실행이 된다. 관리자의 실행 화면은 그림 9와 같다. 관리자는 interactive 모드로

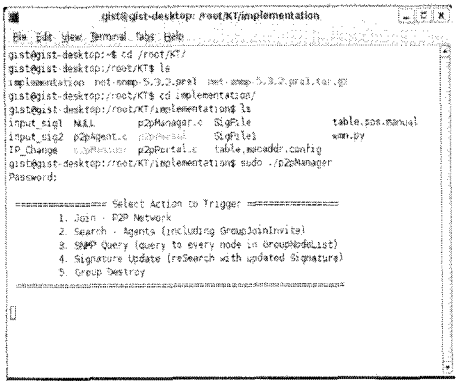


그림 9. 관리자의 실행 화면.

동작하며 지원하는 기능은 그림 9에서 보는 것처럼 5가지가 있다. 하지만 이는 구현된 관리자가 위의 5가지 기능만을 지원한다는 의미는 아니며, 앞선 절에서 설명한 프로토타입 시스템의 기능을 모두 지원한다. 다만 이 5가지의 기능은 사용자의 입력에 의해서 동작하며, 나머지의 기능들은 필요한 상황에 따라 동작하도록 구현이 되어 있다, '1'은 관리자가 P2P 네트워크에 참여하는 기능이며, '2'는 P2P 네트워크에서 시그니처에 기초하여 자신이 관리할 관리대상을 찾는 기능이다. '2'는 시그니처에 기반하여 P2P 네트워크에서 관리대상을 검색한 후, 해당 관리대상 노드에게 시그니처 파일을 요청하고 이에 기초하여 노드 검증을 실행한다. 만약 시그니처에 기반한 노드 검증이 성공적으로 진행되면 관리자가 관리할 그룹에 참여하도록 요청메시지를 보낸다. '3'은 관리자가 관리하는 그룹에 속한 노드들에게 SNMP 질의를 보내는 명령어이다. '3'의 명령을 통해 SNMP 질의를 관리대상에게 전송하기 위해서 사용자는 자신이 원하는 SNMP 질의를 선택해야 한다.

실행된 관리자가 지원하는 명령어 '4'는 시그니처 갱신을 위한 것이다. 앞서 설명한 것처럼 동일한 시그니처를 계속 사용하는 것은 보안상 위험이 있기 때문에, 주기적으로 시그니처를 갱신하도록 하여야 한다. 본래의 프로토타입 시스템의 설계에서 시그니처 갱신은 그룹 키 갱신과 동시에 이루어지도록되어 있다. 하지만, 오랜 시간 그룹에 변화가 없을 경우에는 그룹 키, 시그니처 갱신이 이루어지지 않기 때문에, 관리자가 능동적으로 시그니처를 갱신할 수 있도록 하였다. '5'는 관리자가 관리하는 그룹을 폐쇄하는 명령어이다. 자신이 관리하는 그룹에 속한 모든 관리 대상 노드들에게 그룹 폐쇄 메시지를 전송하고 현재 자신이 관리, 보유하고 있는 그룹

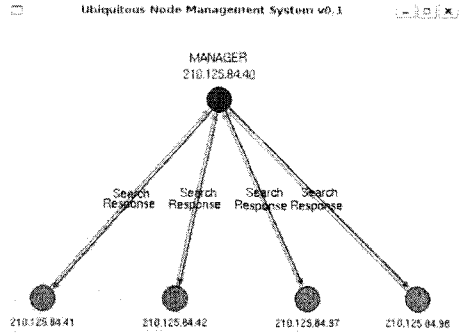


그림 10. 프로토타입 시스템 구현 실행도.

에 대한 정보를 초기화 시킨다.

관리자는 관리자가 지원하는 명령어 지원을 위한 입력창 뿐 아니라 현재 어떤 노드들이 P2P 네트워크에 참여하고 있으며, 어떤 노드들이 자신이 관리하는 그룹에 속하였는지에 대한 정보를 보여주는 관리창을 생성한다. 위 그림 10은 4개의 관리대상 노드가 P2P 네트워크 및 관리자가 관리하는 그룹에 참여하고 있는 상황을 보여준다. 표시된 정보는 그룹에 참여하고 있는 관리자 및 관리대상 노드의 IP이며 관리자 및 관리자가 전송하는 메시지를 보여주는 선은 빨간색으로 표시되고, 관리대상 및 관리대상이 전송하는 메시지를 보여주는 선은 녹색으로 표시된다. 또한 관리자와 관리대상 사이에 존재하는 선 위에 나타나는 메시지는 관리자가 관리대상에게, 관리대상이 관리자에게 최종적으로 전송한 메시지를 보여준다. 위쪽의 메시지는 관리자가 전송한 것이며, 아래쪽의 메시지는 관리대상이 전송한 메시지이다. 그림10에서 보여주는 상태는 관리자가 명령어 '2' 를 통해 P2P 네트워크에서 시그니처를 사용하여 관리 대상 노드를 검색하기 위해 메시지를 전송하고, 관리 대상이 이에 기초하여 응답하는 상황을 보여준다. 현재 관리자가 보여주는 가시화 정보는 전체 토폴로지 정보라기 보다는 관리자 관점에서 그리는 네트워크의 정보이다. 즉, 어떤 노드들이 P2P 네트워크에 참여해 있으며, 어떤 노드들이 자신이 관리하는 그룹에 참여하고 있는지 또한 관리대상들과 어떤 메시지들을 주고 받았는지에 대한 정보만을 보여주고 있다. 라우팅 경로와 같은 전체적은 네트워크의 정보는 현재의 구현된 버전에서는 보여주고 있지 않다.

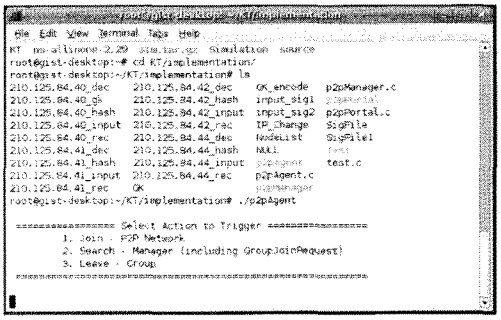


그림 11. 관리대행자의 실행 화면

5.4 관리대상의 관리 대행자 구현

관리대상 또한 관리자처럼 몇몇의 기능은 interactive 모드로 지원하며, 다른 기능들은 적절한 상황에서 동작하도록 구현이 되었다. 그림 11은 관리대상의 실행 화면을 보여준다. 관리대상은 interactive 모드에서 3가지의 기능을 제공한다. '1'은 관리자처럼 P2P 네트워크에 참여하는 기능이며, '2'는 자신이 참여하고자 하는 그룹의 관리자를 찾는 기능이다. '2'는 관리자의 시그니처에 기초하여 관리자를 찾고 관리자의 시그니처를 요청하며 시그니처에 기반한 인증을 수행한다. 만약 인증이 성공적이라면 관리자에게 그룹 가입 요청 메시지를 전송한다. '3'은 관리대상이 자신이 속한 그룹에서 탈퇴하기 위해서 관리자에게 그룹 탈퇴 의사를 전송하는 기능이다.

VI. 결 론

본 논문은 이동형 장비들을 인터넷과 같은 공중망을 통하여 어디에서나 안전하며 효율적으로 관리할 수 있는 기법을 제안하였다. 제안한 기법은 리눅스 시스템과 C 언어 기반으로 프로토타입을 구현하고, 테스트 베드를 통한 시연을 통하여 실용성을 증명하였다. 프로토타입은 제안한 기법에 집중하여 구현한 관계로 이동형 노드 환경에서 매우 중요한 노드 인증 부분을 외부의 인증 프로토콜을 사용하여 인증 절차를 수행하였다고 가정하고 구현하지 않았지만 본 연구와 병행으로 진행중인 ad-hoc환경에서의 인증 기법 연구에서 얻을 결과를 본 프로토타입에 적용할 예정이다. 이 밖에도 매우 규모가 크고 동적인 보안 그룹의 멤버쉽을 효율적으로 관리하는 기법과 관리자의 시그니처를 이용한 보안 공격에 대비하여 관리자의 시그니처를 갱신할 수 있는 기법들을 연구하여 본 프로토타입에 추가 구현할 예

정이다. P2P를 통하여 관리자나 관리대상을 파악하는 방식은 중앙에 위치한 P2P서버에 의존하는 구조이므로 순수 ad-hoc네트워크와 같은 환경에서는 사용상에 제약이 있다. 그러므로 추후에는 P2P서버가 없는 환경에서 관리자나 관리대상을 파악하는 기법도 연구할 예정이다.

참 고 문 헌

[1] M. Zach, D. Parker, J. Nielsen, C. Fahy, R. Carroll, E. Lehtihet, N. Georgalas, R. Martin, and J. Serrat, "Toward a framework for network management applications based on peer-to-peer paradigms," in *Proc. NOMS*, Apr. 2006.

[2] W. Chen, N. Jain, and S. Singh, "ANMP: Ad hoc network management protocol," *IEEE Journal of Selected Areas in Communications*, Vol.17, No.8, Aug. 1999.

[3] L. Granville, D. Rosa, A. Panisson, C. Melchoirs, M Almeida, and L. Tarouco, "Managing computer network using peer-to-peer technologies," *IEEE Communications Magazine*, Oct. 2005.

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

[5] Y. Kim, A. Perrig, and G. Tsudik, "Group key agreement efficient in communication," *IEEE Trans. on Computers*, Vol.53, No.7, July 2004.

[6] M. Baugher, B. Weis, T. Hardjono, and H. Harney, "GDOI: The Group Domain of Interpretation," IETF RFC 3547, July 2003.

[7] H. Harney, U. Meth, A. Colegrove, and G. Gross, "GSAKMP: Group Secure Association Key Management Protocol," IETF RFC 4535, June 2006.

[8] J. Wu, *Handbook on Theoretical and Algorithm Aspects of Sensor, Ad Hoc Wireless, and Peer-to-Peer Networks*, Auerbach Publications, 2005.

[9] P. Peng, "P2P-HGKM: An efficient hierarchical group key management protocol for mobile ad-hoc networks," M.S. Thesis, The University of British Columbia, July 2004.

[10] D. Kwak and J. Kim, "A decentralized group key management scheme for the decentralized P2P environment," *IEEE Communications Letters*, July 2007.

[11] 곽득휘, 김종원 "GSAKMP와 GDOI 그룹 키 관리 프로토콜 비교 분석" *한국통신학회하계학술대회*, July 2003.

[12] I. Taylor, *From P2P to Web Services and Grids: Peers in a Client/Server World*, Springer, 2005.

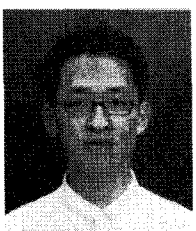
[13] D. Zeltserman, *A Practical Guide to SNMPv3 and Network Management*, Prentice Hall, 1999.

[14] *The Net-SNMP Homepage*, http://net-snmp.sourceforge.net/.

곽 득 휘 (Deuk-Whee Kwak) 정회원

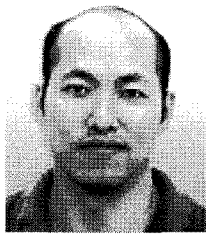
1985년 2월 전남대학교 계산통계학과 졸업
1988년 2월 중앙대학교 전자계산학과 석사
2006년 2월 광주과학기술원 정보통신공학과 박사
1990년 11월~현재 KT 연구개발본부 책임연구원
2003년 7월~2004년 7월 미시간대학교 전기전자전산학과 방문연구원
2006년~현재 정보보호학회논문지 책임편집위원
<관심분야> 그룹 키 관리, P2P 보안, Ad Hoc 네트워크 보안, 홈네트워크 보안, 네트워크 관리

이 현 룡 (HyunYong Lee) 정회원



2003년 6월 전남대학교 정보통신공학부 졸업
2005년 2월 광주과학기술원 정보통신공학과 석사 졸업
2005년 3월~현재 광주과학기술원 정보통신공학과 박사과정
<관심분야> Overlay network, P2P, Future Internet

김 종 원 (JongWon Kim) 정회원



1987년 서울대학교 제어계측공학과 학사

1989년 서울대학교 제어계측공학과 석사

1994년 서울대학교 제어계측공학과 박사

1994년 3월~1999년 7월 공주대학교 전자공학과 조교수

1997년 8월~2001년 7월 University of Southern California 연구 조교수

1999년 12월~2000년 7월 Technology Consultant for VProtect Systems Inc.

2000년 7월~2001년 6월 Technology Consultant for Southern California Division of InterVideo Inc.

2001년 9월~현재 광주과학기술원 정보통신공학과 교수

<관심분야> Networked Media Systems and Protocols focusing "Reliable and Flexible Delivery for Integrated Media over Wired/Wireless Networks," (네트워크미디어: http://nm.gist.ac.kr)