멀티캐스트 보안을 위한 응용 모델

정회원 김 영 준*

Application Model for Multicast Security

Young Jun Kim* *Regular Member*

요 약

본 논문에서는 멀티캐스트 보안 응용 모델을 제안한다. 그룹 보안을 지원하는 멀티캐스트 환경에서 그룹에서 멤버쉽이 변경될 때 마다 요청되는 새로운 그룹키를 멀티캐스트 그룹은 안전하고 효율적인 방안으로 처리되어야 한다. 기존의 안전한 멀티캐스트 트래픽 전송을 위한 보안 메커니즘과 정보의 기밀성, 인증, 무결성등을 보장하기 위한 멀티캐스팅 서비스 구조 및 보안에 대한 방안으로 GKMP, SMKD, Iobus, MKMP등이 있다. 그러나 이러한 방안들은 멀티캐스트가 대규모로 확장되면 빈번한 그룹 키 재분배로 인하여 오버헤드가 커져 실효성이 떨어진다.

이러한 문제점을 액티브 네트워트를 응용하여 해결한다. 액티브 네트워크는 요청된 계산이 가능한 개념이다. 또한 기존의 네트워크가 가지는 구조적인 비 효율적인 문제점을 해결하는 대안이다. 보다 구체적인 방안으로는 액티브 라우터를 이용하여 SAKGM을 만들고 새로운 시스템의 작동을 위해 IGMP를 대체한 SAGMP를 설계하며, 이동 멀티캐스트에서의 접근제어 모델을 위한 lightweight X.509의 사용을 제안한다.

Key Words : Multicast security, Active network, X.509

ABSTRACT

In this paper, we propose that an Application Model for Multicast Security. In the multicast environment supporting group security, where is a multicast group has a single group key for itself and a new group key is required whenever member ship in the group, an efficient and secure way of transmitting a new group key is required whenever member ship is changed. To support this requirement, there has been a lot of on-going researches(GKMP, SMKD, Iobus, MKMP) on multicast group key management, dynamic member ship management. However, they have some problems of not being scalable and efficient for a number of leaving member. It is suggested that new network management scheme which adopts the active network technology to solve the problems mentioned above. Active networks are novel concept in network architecture in which network switches perform customized computation on the messages flowing through them. Multicast Group ky management model based on active networks is expected to resolve the problems which cannot be handled efficeently in most of existing passive network model. And, we propose the use of lightweight X.509 for Access Control Model in mobile multicast.

Ⅰ. 서 론

최근 유비쿼터스 사회가 다가옴에 따라 다양한 서비스가 개발되어 제공되고 있다. IP TV, DMB, 인터넷 방송등 다수의 가입자를 통한 서비스가 제공 되고 있다. 이러한 서비스는 특정한 사용자들에

※ 본 연구는 2007년도 인하공업전문대학 교내 연구비 지원에 의해 수행되었습니다.
* 인하공업전문대학 정보통신과(yjkim@inhatc.ac.kr)
논문번호 : 07099-1130, 접수일자 : 2007년 11월 30일

게 차별화된 금액을 받고 서비스를 제공하는 방안이 필요하다. 전체 사용자들 중에 특별한 사용자들에게만 서비스를 제공하는 방안으로 멀티캐스트 방식을 적용하여 서비스를 제공한다. 멀티캐스트는 유니캐스트나 브로드캐스트에 비해서 효과적인 그룹 접근 제어가 어렵고 트래픽이 많은 링크를 경유하기 때문에, 신분위장, 서비스거부 공격, 재전송 공격 등의 위험이 증가하고 있어 많은 공격기회를 제공하고 있다[1,2,3,4,5]. 이와 같은 서비스는 가입자를 확인하는 검증절차를 거치게 된다. 본 제안 방식은 멀티캐스트 방식에 보안 기술을 적용하여 각각의 특정한 사용자들에게 서비스를 제공할 수 있는 방안을 제시하고자 한다. 인터넷 통신기술중 멀티캐스트는 특정한 사용자에게만 데이터를 전송하는 것으로써, 현재 IPv6에 포함되어 있으며, IP TV나 인터넷 방송기술에 적용하여 이용할 수 있다. 다양한 멀티캐스트 보안 프로토콜이 연구되면서 멀티캐스트 그룹 통신에서 서브그룹 단위로 그룹 키를 분배하는 계층적인 보안프로토콜이 연구되었다[6,7,8,9]. 이러한 보안 프로토콜은 기존의 유니캐스트에서 사용한 보안 프로토콜과는 다른 1:N 구조나 혹은 N:N 구조의 서브그룹 단위로 그룹키를 관리하여 사용자의 가입/탈퇴에 따른 그룹키의 재분배를 한다. Naive, Iobus, Nortel 방식의 멀티캐스트 그룹 키 관리 방식은 다수의 가입자 수에 중점을 둔 그룹 키 관리 방식으로 서브 그룹의 규모가 매우 크다. 따라서 서브 그룹내에서 단 하나의 가입자가 탈퇴하여도 서브 그룹내에 모든 가입자에게 그룹 키의 재분배를 하여야 하기 때문에 빈번한 이동이 있을시 키의 재분배시간을 많이 요구한다. 또한 멀티캐스트 트래픽은 그 본연의 특징인 넓은 전송영역 때문에 유니캐스트 트래픽보다 보다 많은 보안상의 공격을 받을 수 있다. 즉 새로 가입한 멤버로부터는 가입이전의 통신을 보호하고, 탈퇴하는 멤버는 탈퇴이후의 통신을 보호하여야 한다. 따라서 안전한 멀티캐스트 트래픽 전송을 위한 보안 메카니즘과 정보의 기밀성, 인증, 무결성등을 보장하기 위한 멀태캐스팅 서비스 구조 및 보안에 대한 활용방안으로 엑티브 네트워크를 이용한다. 액티브네트워크를 이용하면 안전한 멀티캐스트 트래픽 전송을 위한 보안 대책이 확장된다.

Ⅱ. 액티브 네트워크

2.1 액티브 네트워크의 개념

액티브 네트워크(Active Network)란 기존의 네트워크에서 라우터나 스위치와 같은 중간노드들이 단순히 패킷의 헤더만 처리하던 데서 한 걸음 더 나아가 패킷내에 실행프로그램코드와 데이터를 함께 넣어 전송하고 스위치나 라우터에는 이 패킷에 들어 있는 프로그램 코드를 처리 할 수 있는 실행환경을 가진 네트워크를 말한다[10]. 액티브 네트워크에서는 기존의 네트워크가 중간노드에서는 단순히 패킷을 경로 설정하고 전달하는 기능을 담당하고, 에러처리 및 흐름제어와 같은 패킷의 복잡한 처리는 종단의 단말장치에서만 처리하던 것과는 달리 중간노드에서 여러 가지 처리를 가능하게 함으로 인해 기존의 네트워크가 제공하지 못했던 유연성과 다양한 장점들을 제공할 수 있다. 액티브 네트워크는 망에 일종의 지능을 부여한다는 측면에서 전화망에서의 AIN(Advanced Intelligent Network)과 유사한 개념이라고 할 수 있다.

2.2 액티브 네트워크 구조

액티브 네트워크는 기존의 네트워크의 패킷에 해당하는 캡슐(액티브 패킷(Active Packets)이나 스마트 패킷(Smart Packets)으로도 불린다)과 이를 수행할 수 있는 중간노드의 실행환경(Execution Environment)으로 이루어져 있음을 그림 1에서 보여주고 있다. 캡슐은 기존의 패킷들이 중간노드가 실제로 보고 처리하는 부분인 헤더와 내용을 나타내는 페이로드(Payload)로 이루어져 있는 것과는 달리 실제 수행될 수 있는 프로그램코드와 데이터로 구성되어 있다. 라우터나 스위치와 같은 중간노드에서는 각 캡슐들을 읽어 들여 프로그램과 데이타를 수행(Execute), 처리(Process)할 수 있는 실행환경을

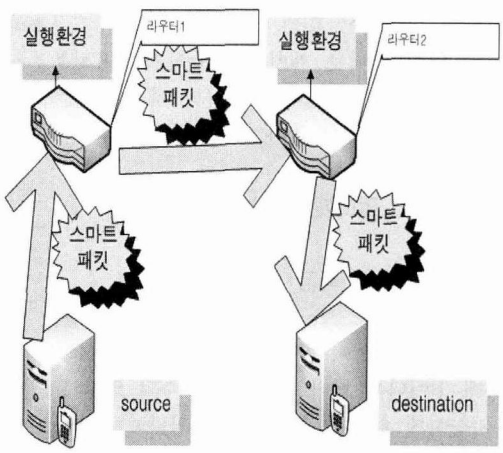

그림 1. 액티브네트워크
Fig. 1. Active Network

제공함을 그림 3에서 보여주고 있다. Spt 트리를 구성하기 위한 오버헤드를 제거하기 위해 Sht 방식을 기본적으로 수용하고, CBT 코어의 트래픽 집중현상으로 인한 병목현상과 잦은 트리전환에 따른 라우팅 정보의 폭주를 막기 위해 지역코어 단위의 트리 전환을 수행하여 광역 DIS환경에 보다 적합한 멀티캐스트 기능을 제공한다.

이러한 실행환경을 정의하는 데는 여러 가지 사항들을 고려해야만 한다. 이러한 고려사항들 중 중요한 것으로는 프로그램언어, 프로그램의 인코딩 방식, 프리미티브 제공문제, 그리고 자원의 할당 및 공유문제 등이 있다. 이와 같이 액티브 네트워크를 설계하는 데는 네트워크, 프로그램 언어, 운영체제, 보안과 같은 많은 분야의 연구가 필요하다.

그림 2에선 기존의 패킷과 액티브 네트워크에서 사용되어지는 스마트 패킷의 차이점을 그림으로 설명하고 있다. 일반 패킷과 가장 큰 차이점은 어떤 방식으로 패킷을 처리해야 하는지 알려주는 기능(function)부분이 있다. 이런 기능들을 수행하기 위한 메소드(Method)들을 포함한 스마트 패킷들이 망을 통해 전송되어지면, 각각의 액티브 노드에선 이러한 메소드들을 이용하여 해당 기능들을 수행해서 패킷들을 포워딩하거나 라우팅하게 되는 것이다.

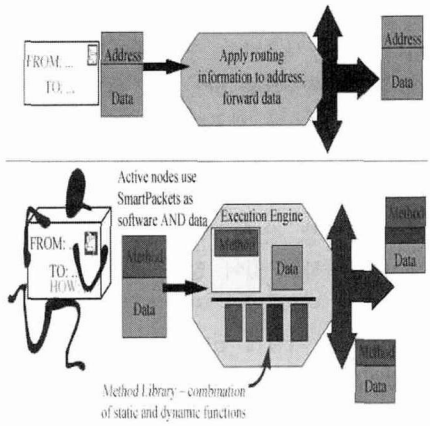

그림 2. 스마트 패킷
Fig. 2. Smart packet

2.3 액티브 라우터

액티브 라우터는 기존의 패킷보다 다양한 특징을 가진 액티브 패킷을 처리하기 위해서는 다양한 패킷 스케쥴링 기법과 자원 관리, 패킷 분류등 하드웨어와 소프트웨어의 두 가지 측면을 동시에 고려해야 한다. 버퍼 스케쥴링에서는 실행환경에 따라서 데이터의 특성에 따른 패킷 전송, 자원할당과 같은 서비스를 고려해야 한다. 이는 기존의 패킷구조의 처리와 달리 액티브 패킷의 캡슐화된 옵션부분을 처리하고, 모든 자원관리를 하나의 처리환경에서 제어할 수 있도록 해야 한다.

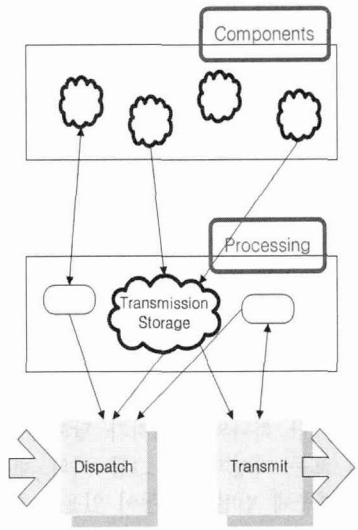

그림 3. 액티브 노드
Fig. 3. Active Node

Ⅲ. 멀티캐스트 보안 응용 모델

3.1 SAKDC 특징

다양한 멀티캐스트 그룹에서는 회원의 가입과 탈퇴가 빈번하게 일어나므로 그룹 키의 재 분배가 원활하게 일어나야 한다. 또한 많은 수의 회원의 가입을 가능하게 하려면 확장성을 지원하여야 한다. 이러한 확장성을 지원하기 위해서는 특정 단위별로 그룹 키를 분배하는 것이 효과적이다. 그림에서 보면 멀티캐스트 그룹을 서브 그룹으로 나누어 각 서브 그룹마다 그룹 키를 관리하게 하는 것을 보여주고 있다. 멀티캐스트 그룹을 서브 그룹화 했을 때와 안 했을 때의 비용을 비교해보면 다음과 같다. 서브 그룹화 하지 않았을 경우 회원이 N명인 멀티캐스트 그룹에서 회원의 변동이 생긴다면 N(회원수) x C (비용) 만큼의 오버헤드가 발생된다. 그러나, n개로 서브그룹화 하면 각 서브 그룹당 회원수는 N/n 명이므로 (N x C) / n 만큼의 비용 만큼만 발생한다. 즉 서브 그룹의 개수가 두 배 증가하면 키 재분배의 발생비용은 절반으로 줄어든다. 멀티캐스트 상의 액티브 라우터들은 각각 하나의 서브그룹을 형성하여 서브 그룹키를 분배하고 관리를 하는 SAKDC가

된다. SAKDC는 멀티캐스트 라우터나 호스트가 새로 그룹에 가입하면 그 멀티캐스트 라우터나 호스트의 공개키를 등록한다. 그러나 새로 가입하려는 멀티캐스트 라우터가 액티브 라우터라면 자신의 서브 그룹에 포함시키지 않는다. 대신 새로 가입한 액티브 라우터는 상위 SAKDC로부터 인증을 받아 또 하나의 서브그룹을 형성하는 SAKDC가 된다.

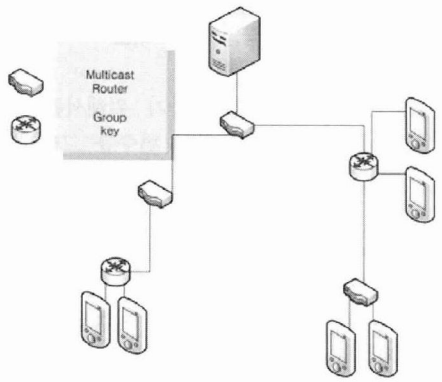

그림 4. 멀티캐스트 트리의 서브그룹
Fig. 4. Subgroup of Multicast Tree

3.2 SAKDC 구성

멀티캐스트 트리내에서 SAKDC가 생성되는 위치를 결정하는 데에는 원칙이 있다. 우선 액티브 라우터만이 SAKDC가 될 수 있고 송신자로부터 가장 가까운 액티브 노드가 SAKDC로 된다. 나머지 액티브 라우터들은 처음 생긴 SAKDC로부터 인증을 받아 SAKDC가 된다.

- 각각의 액티브 라우터는 SAKDC가 되어 하위 노드와 호스트로 이루어진 그룹을 관리한다.(R1,R3,R4,R5,R6)
- 하위 노드에 액티브 라우터가 있을 경우, 그 액티브 라우터는 또 다른 SAKDC가 되어 상위 SAKDC로부터 분리된다. 즉 SAKDC는 다른 SAKDC의 서브그룹에 속하지 않는다.(R6)
- 하위 노드 그룹에 관리할 호스트가 없거나 액티브라우터만이 존재하고 호스트가 존재 하지 않을 경우에는 SAKDC의 기능을 해제된다.(R2)
- 송신자도 하나의 멤버로 볼 수 없기 때문에 송신자와 가장 가까운 액티브 라우터는 언제나 SAKDC가 된다.(R1)

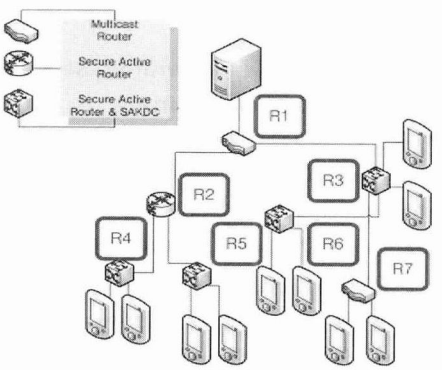

그림 5. SAKDC를 활용한 구성
Fig. 5. Configuration using SKADC

3.3 SAKDC 서브그룹 내부 구조

서브 그룹내에서는 서브 그룹키와 공개키를 동시에 활용하여 암호화/복호화를 한다. 송신자가 보낸 데이터그램을 SAKDC에서 서브그룹 키를 이용하여 암호화해서 전송한다. 그러면 그 서브그룹에 속한 멤버 호스트는 가지고 있던 서브 그룹키를 이용하여 데이터그램을 확인한다. 그러나 멤버가 아닌 호스트는 데이터그램을 가졌다 하더라도 서브 그룹키가 없으면 복호화 할 수 없다. 서브 그룹키를 공유하는 방법으로는 멤버가 새로 가입하거나 탈퇴 하였을 때 갱신된 멤버들에게 공개키로 암호화 하여 새로운 서브 그룹키를 유니캐스트를 이용하여 보낸다. 이 과정에서 멀티캐스트 그룹 관리를 위해 사용되는 IGMP보다 추가적인 기능이 요구되며, 이를 SAGMP(Secure Active Group Management Packet)을 정의하여 IGMP를 대체한다[11].

3.4 송신자 인증

실시간으로 전송되는 데이터가 다른 비 인증 사용자에 의해 방해가 된다면 송신자의 정보를 잃어버릴 수 있기 때문에 송신자를 인증하는 것은 멀티캐스트 그룹 키 관리에서 필수적이다. 본 논문에서는 전자서명 방식으로 공개키와 메시지 다이제스트를 이용한 방법을 사용한다. 공개키에 의한 전자 서명 방식은 계산 비용이 많이 들기 때문에 메시지 다이제스트를 통해 먼저 메시지 양을 줄이고 공개키를 이용하여 서명을 한다. 전자서명된 메시지는 제일 먼저 만나는 SAKDC에서 다음과 같이 송신자 인증 절차가 이루어지고 메시지를 서브그룹과 하위노드로 내려 보낸다.

1. MD(M)
2. $S_A(MD(M))$, Eg(M)
3. $V_A(S_A(MD(M)))=MD(M)$, $D_K(E_K(M))=M$
4. COMPARE(MD(M),MD(M))

3.4 수신자 인증

멀티캐스트에서는 보안성을 제공하기 위해서 주로 그룹 키 분배 방식을 사용하는데, 멀티캐스트 그룹의 모든 회원들에게 공통키를 안전하게 전달해 주는 역할을 한다. 이 방식을 사용하게 되면, 송신자가 수신자에게 개별적인 암호화를 보내지 않아도 된다는 장점이 있다. 그러나 새로운 멤버가 가입하거나 기본의 멤버가 탈퇴를 한다면 그룹키를 재분배하여야 한다. SAKDC 방식에서는 멀티캐스트에서 보안성을 제공하기 위한 방법으로 Iobus에서 제안한 그룹키 분배 방식을 이용한다. 이는 하나의 멀티캐스트 세션을 여러 개의 서브 그룹으로 나누어 각각의 서브그룹 별로 그룹키를 관리하는 방안이다.

3.5 SAGMP

액티브 노드간에 주고 받는 SAGMP(Secure Active Group Management Packet)의 패킷 포맷은 그림 6과 같다.

object_id는 SAKDC의 packet임을 의미하는 서비스 객체식별자이며, session_id는 세션 식별자이며, channel_id는 채널 식별자이다. 그리고 operation_code 는 SAKDC가 사용하는 서비스코드이며, payload or certificate는 전송할 정보 또는 인증정보이다. 다음의 표 1은 기능모듈에 관한 구성이다. 아래의 프로토콜은 SANEP(Secure Active Network Encapsulation Protocol)packet 과 smart packet을 이용하게 되며, smart packet의 payload 부분에 위치한다. 이 packet 정보는 IP packet으로 만들어져 네트워크상에 전달되고, 액티브 노드가 해독하여 해당 기능을 수행하게 된다.

표 1. 기능모듈
Table 1. Function Module

기능모듈	서비스 프리미티브
SAKDC 그룹관리	Create_SAKDC
	Delete_SAKDC
	Approve
	Disapprove
	Request_SAKDC_Authority
	Send_SAKDC_End
멤버 관리	Request_Join
	Request_Leave
	Approve
	Disapprove
키 관리	Periodic_Send
	Periodic_Report
	Update_GroupKey
	Update_Ack

0 4	8 12	16 28	32
ver	object_id	session_id	op_code
session_id		Checksum	
Payload or Certificate			

그림 6. SAGMP의 필드 규격
Fig. 6. Field Standard of SAGMP

Ⅳ. 성능평가 및 비교

멀티캐스트 보안구조를 만들기 위해서는 멀티캐스트 그룹이 가지는 여러 가지 변수를 고려해서 구축한다. 그예는 멀티캐스트 그룹의 크기, 회원 특성, 회원 변화, 생존 시간, 송신자의 수, 트래픽의 크기와 종류 등이 있다. 또한 멀티캐스트 구조 특성상 다자간 통신을 하기에 위험 요소에 노출된다. 이를 위한 요구사항은 무결성, 인증성, 접근제어, 부인봉쇄, 비밀성, 공정성, 확장성등이다. 다음은 다른 멀티캐스트 프로토콜에 관한 특징들이다.

4.1 GKMP(Group Key Management Protocol)

GKMP 프로토콜은 멀티캐스트 그룹의 멤버들을 관리하기 위한 대칭키를 생성하여 관리한다. 이프로토콜에서는 각각의 멀티캐스트 그룹이 전용의 그룹 컨트롤러를 가지고 그룹 키를 관리한다. 그룹 컨트롤러 역시 그룹 멤버로서, 여러 가지 주요한 프로토콜 동작을 수행한다. 예를 들면 키 생성, 키 분배와 그룹키 재구성 메시지를 생성하는 역할을 하며, 또한 이러한 동작에 대한 진행과정에 대한 보고를 담당한다. 그룹 컨트롤러는 선택된 그룹 멤버와 JOINT를 통해 그룹키를 생성한다. 이 기법에서는 그룹 컨트롤러가 모든 그룹 멤버에게 대한 키 전송을 전담한다.

4.2 SMKD(Scalable Multicast Key Distribution scheme)

일반적으로 키 분배 기능은 중앙의 네트웍 호스트나, 키 분배 센터에서 전담해 왔다. 그러나 이러한 기법들은 광범위 멀티캐스팅에 대한 확장성이 결여되어있다. DVMRP와 MOSPF등과 같은 네트웍 계층 멀티캐스트 프로토콜은 보안이 제공되지 않아, 단지 IP 자체내에서 제공하는 보안에 의존해야 한다. 그러나, SMKD는 Core-Base Tree(CBT)라우팅 프로토콜을 기반으로 구성되어, 확장성 있는 접근을 통해 CBT 그룹 트리에 안전하게 참여할 수 있게

해준다. IP 멀티캐스트 기법으로 DVMRP와 MOSPF와 같은 소스기반 전송 트리를 이용하지 않고, 한 그룹에 대하여 하나의 공유 트리를 사용한다. 공유 멀티캐스트 전송트리는 여러 개의 핵심 라우터들로 구성된다. CBT 트리가 초기화되면, 트리의 핵심 라우터는 그룹 컨트롤러처럼 작동하여 그룹 세션키와 키 분배 키를 생성한다. 라우터가 분배 트리에 참여하게 되면, 가입 멤버들을 인증하는 기능을 대신하여, 그룹 키를 제공해 준다.

4.3 Iobus

Iobus 키 관리 프로토콜에서는 멀티캐스트 그룹들을 계층적으로 배열된 서브그룹들로 나눈다. GSC(Group Security Controller)가 있어 최상위 레벨그룹을 관리하며, 각각의 서브 그룹들은 GSIs(Group Security Intermediaries)가 담당하여 관리한다. 각각의 서브 그룹은 관리자가 선택한 고유의 서브키를 가지게 된다. GSIs는 자신의 서브그룹과 좀 더 상위 레벨의 서브 그룹 키들을 알고 있어 상위 레벨로의 메시지 송수신이 용이하다. 단점으로는 GSIs로부터 각각의 패킷을 복호화하고 재암호화하는데 지연이 발생하는 점이다. 신뢰할 수 없는 GSI를 제거하는 것도 또한 복잡한 일이다.

4.4 MKMP(Multicast Key Management Protocol)

MKMP 키 관리 프로토콜은 초기의 키 관리자가 동적인 방법으로 키 분배권한을 다른 개체들에게 위임하도록 하는 기법이다. 우선 그룹키를 생성하여 키분배 권한을 요청하는 멀티캐스트 그룹의 개체들에게 위임한다. 이 메시지에는 키와 접근 리스트가 들어있어 요청한 그룹에서만 복호화 할 수 있다. 이러한 동적인 접근은 그룹 토폴로지가 온라인상에서 변하더라도 적용될 수 있는 장점을 가진다.

표 2는 위에서 기술한 멀티캐스트 그룹 키 분배 모델을 확장성, 키 분배 권한의 위임 가능성, 범용성, 침입자 접근 가능성, 그룹 키 보안등의 기준으로 평가한 것이다. 확장성은 멤버가 다수 참여하여 멀티캐스트 그룹 트리가 커졌을 때에도 얼마나 성능에 저하가 없는지를 판단하는 요소이다. GKMP와 MKMP의 경우 중앙 집중적인 구조이므로 규모가 커지면 키 재분배 오버헤드가 커진다. 키 분배 권한 위임 여부는 확장성에 관련된 요소로서 GKMP만이 중앙에서 키 분배를 전담한다. SAKDC는 액티브 라우터를 이용해 합법적인 송신자가 보낸 정보인지를 판단하는 송신자 인증 기능이 가능한 구조로 되어있고, 불법적인 송신자가 멀티캐스트 정보를 받아도 암호문을 풀지 못하는 구조이다. 따라서 전체적인 보안 요구 사항에 적합한 구조이다. 오버헤드나 그룹키 유일성 관점에서 볼 때, 다른 방식보다 우수함을 다음 표 3을 통해서 알 수 있다.

표 2. SAKDC의 비교
Table 2. Comparisin of SAKDC

	GKMP	SMKD	Iobus	MKMP	SAKDC
확장성	X	O	O	△	O
키분배권한 위임	X	O	O	O	O
범용성	O	X	O	O	O
침입자보안성	O	X	X	△	O
그룹키보안	O	△	△	△	O

표 3. 키 관리 방식 비교
Table 3. Comparison of Key Management Method

	GKMP	SMKD	Iobus	MKMP	SAKDC
그룹키의 유일성	X	X	O	X	O
복호화/재 암호화 오버헤드	X	X	O	X	X
키생성 오버헤드분산	X	O	O	X	O
공개키 사용	X	X	X		O
송신자 인증	O	△	O	△	O

멀티캐스트 키 분배에 있어서 기존의 방식이 가지는 가장 큰 문제점은 멤버가 증가할 수록 키 재분배가 빈번히 일어나 대규모로 확장이 어렵다는 점이다. 이에 비해 SAKDC는 멀티캐스트 서브그룹을 서브그룹화 하여 대규모로 확장이 가능하도록 했다. 기존의 그룹 키 분배방식과 SAKDC를 이용했을 때, 각 각 멤버 호스트의 숫자가 늘어남에 따라 키 재 분배를 위한 비용이 얼마나 증가 하는지 성능평가를 했다. 이를 위해서 다음과 같은 가정을 한다.

1. 멀티캐스트 트리 구성시 모두 이진트리가 된다.
2. 새로운 노드가 추가 생성시 ROOT에 가까운 자리에 우선 배치한다.
3. 한 노드에 소속되어 있는 호스트는 10개로 한정한다.
4. 각 링크간 코스트는 단위 없이 1로 한다.

5. 노드 자체의 코스트는 무시한다.
6. 멤버 호스트 수의 증가에 비례하여 멤버의 가입과 탈퇴 횟수가 일정하게 증가하는 것으로 한다.

위와 같은 가정으로 결과를 도출하면 그림 7과 같다. 그림 7에서 보면, 호스트가 증가함에 따라 그룹 키 재 분배를 위한 트래픽 증가는 다른 방식에서는 정도의 차이는 있으나, 급속적으로 증가하고 있다. 이에 반해 SAKDC를 이용하면 거의 직선에 가까운 완만한 곡선을 그린다. 다른 방식에서는 멤버가 변경 될 때 마다 키의 재 분배가 일어나고, 새로운 키를 모든 멤버에게 유니캐스트로 전달해주어야 한다. 또한 멤버수가 증가할 수록 키의 재 분배가 증가하며, 키 재 분배 트래픽도 증가하게 된다.

그래서 멀티캐스트 규모가 커지면 키 재분배 트래픽은 기하급수적으로 증가하게 된다. 그러나 SAKDC를 이용하면, 멤버 변경의 경우 키의 재 분배는 서브 그룹안에서만 일어나므로 멤버의 수가 증가했을 경우, 키 재분배 빈도에만 영향을 받는 관계로 키 재 분배 트래픽이 급격히 증가하지 않는다.

이는 다른 그룹 키 분배 방식의 확장성에 있어 취약한 부분을 SAKDC를 이용하여 멤버의 증가에 따른 트래픽 증가를 완만하게 하여, 대규모의 확장성을 용이하게 만든다.

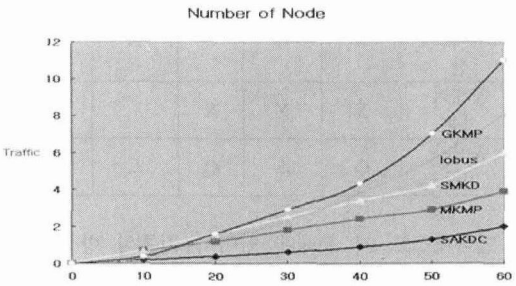

그림 7. 트래픽 비교
Fig. 7. Traffic Comparison

V. 이동 멀티캐스트를 위한 보안응용모델에 대한 고찰

무선 네트워크 구조를 반영하는 키 관리구조에서 먼저 고려하여야 할 사항은 보안 멀티캐스트 환경에서 이동 환경이 접목되면, 호스트의 이동성으로 인한 보안에 대한 고려사항이 발생한다.

5.1 모바일 IP 멀티캐스트 프로콜의 방안

첫째는 홈에이전트가 이동 호스트을 위하여 터널링을 통하여 유니캐스트로 멀티캐스트를 지원하는 방안과 둘째, 이동 호스트가 다른 무선 영역으로 이동했을 경우 이동 호스트가 위치한 무선 영역에서 멀티캐스트를 수신하는 방안이 있다.

이동 멀티캐스트에 관한 대부분의 연구는 이 두 가지 방안을 적절하게 사용하여 전송지연을 줄이거나, 멀티캐스트 전송트리 재구축 횟수를 줄인다[12].

다음은 이동 보안 멀티캐스트에서 다루어야 할 사항이다.

- Forword/backward security:현재 적법한 멤버들만이 멀티캐스트 데이터에 접근 할 수 있다.
- Host mobility: 호스트 이동으로 인해 멤버쉽 변화가 발생할 수 있으며, 이에 따른 키 갱신 작업이 요구된다.
- BS join/leave: 호스트의 이동으로 인해, BS 또는 멀티캐스트 그룹에 가입/탈퇴를 한다.

그림 8은 이동 멀티캐스트 환경을 나타낸다.

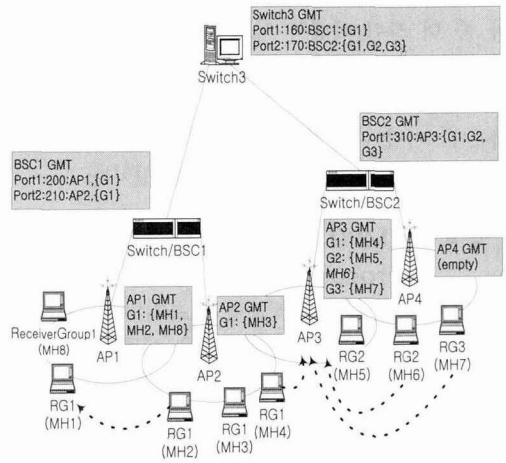

그림 8. 이동 호스트
Fig. 8. Mobile Host

5.2 PKI(Public Key Infrastructure)

PKI는 공개키 암호방식을 이용하여 보안(인증, 무결성, 부인방지)을 제공해주는 광범위하고도 강력한 기술이다. 주 개념은 사용자의 개인정보와 공개키를 묶어 CA(Certification Authorities)의 개인키로 전자서명을 한 인증서를 이용한다. 사용자의 개인키가 노출되거나 변경되면, 사용자는 CA에게 자신의 인증서에 대한 폐지요청을 하며, CA는 이 정보를 모아 주기적으로 CRL(Certificate Revocation List)를 발행한다. 인증서가 폐지되었는지에 대한 정보를 CSI(Certifiacte Status Information)라고 하며, CRL

는 CSI를 제공해 주는 잘 알려진 방식이다.

5.3 인증서

인증서는 사용자의 개인 정보와 공개키를 연결해 주는 전자문서로 인증기관이 개인키로 전자서명을 하여 생성된다. 따라서 이는 사용자와 대응하는 공개키가 실제로 사용자의 소유자임을 증명해주는 역할을 한다. 인증서의 효율적인 관리를 위하여 인증서에는 사용자의 공개키 이외에 인증서 버전, 순서번호, 발행자, 소유자, 유효기간등이 포함된다. PKI에서 인증서의 발행대상은 인증기관과 사용자, 서버 등으로 인증기관에게는 상위 인증기관이 하위 인증기관의 적법성을 증명하기 위해 발행한다. 사용자는 다시 개인 사용자와 법인 혹은 단체 그리고 서버 운영자로 구분된다. 인증서의 유효기간은 일반적으로 1년이다.

5.4 이동 멀티캐스트 환경에서의 접근 제어 프로토콜을 위한 lightweight X.509

사용자의 접근 권한을 부여하기 위한 접근제어 프로토콜을 제안한다. 유비쿼터스 컴퓨팅 환경에서 사용자의 접근 권한 문제와 효율적인 시스템 사용 및 관리에 관한 보안응용서비스를 목적으로 한다. 이를 위해서는 이동 멀티캐스트 환경에서 수정된 인증서 형식이 필요하다. 기본의 X.509 프로토콜은 이동 멀티캐스트를 위한 보안 응용모델에 적합하지 않다[13,14,15]. 표 4는 X.509 버전4의 인증서 형식을 나타낸다.

인증서의 표준형식은 1988년 ITU-T가 X.509의 초기 버전을 공표하였고 1993년에 버전 2를 발표하였으며, 1995년 아후 로는 ISO/IEC 9584-8의 문서와 함께 공동 개발 되어왔다. 1997년에는 버전 3이 발표되었으며, 2000년 버전 4가 발표되어 현재에 이르고 있다. 다음은 위의 인증서를 바탕으로 이동 멀티캐스트 환경에서 적합한 이동 멀티캐스트 환경에서의 lightweight X.509이다.

표 4. X.509 버전 4의 인증
Table 4. authentication of X.509 version 4

필드명	내용
Version	버전
Serial Number	순서번호
Signature	인증서 서명을 위한 사용된알고리즘 식별자
Issuer	발행자의 이름
Validity	유효기간(시작일과 종료일)
Subject	소유자의 이름
Subject Public Key Info	인증되는 공개키의 정보
Issuer Unique Identifier	발행자를 표시하는 식별자
Subject Unique Identifier	소유자를 표시하는 식별자
Signature Algorithm	인증서 서명을 위해 사용된 알고리즘 OID
Extensions	추가적인 속성
Signature Value	발행자의 속성값

표 5. 이동 멀티캐스트 환경에서의 lightweight X.509 인증
Table 5. lightweight X.509 Authentication in mobile multicast Environment

필드명	내용
Issuer	발행자의 이름
Validity	유효기간
Subject	소유자의 이름
Issuer Unique Identifier	발행자를 표시하는 식별자
Subjdet Unique Idenfifirer	소유자를 표시하는 식별자

V. 결 론

본 논문에서는 멀티캐스트 트래픽 전송을 안전하게 하도록 하는 보안 메카니즘 설계을 위한 기반 기술로서 멀티캐스트에서 보안의 필요성과 멀티캐스트에서 고려하여야 할 보안 구성 요소에 대해 논했으며, 이를 실제 통신망에서 적용할 보안 응용모델을 연구하였다. 실제로 액티브 네트워크를 이용하여 멀티캐스트 보안 시스템 구조를 만들 경우 멀티캐스트 라우터의 구조에 맞추어서 계층적으로 그룹 키를 관리하는 확장성이 우수해진다. 또한 네트워크 계층에서 그룹 키를 관리 할 수 있으므로 멀티캐스트를 위한 라우팅과 동시에 인증이 이루어져, 인증이 별도의 과정으로 될 때 보다 부가적인 오버헤드가 줄어든다. 또한 이동 멀티캐스트 환경에서의 보안 응용모델을 고찰하였다.

참 고 문 헌

[1] K. Psounis, "Active Networks: Applications, Security, Safety, and Architecture", IEEE Communication Surveys, 1999.

[2] T. Hardjono and G. Tsudik, "IP Multicast Security:Issues and Directions", Annales de Telecom, July-August 2000, pp 324-340.

[3] D. X. Song and A. Perrig, "Advanced and Authenticated Marking Schemes for IP Traceback," In Proceddings of the IEEE

Inforcomm 2001, April 2001.

〔4〕 Chu, H., Qiao, L., and Nahrstedt, K: A secure multicast protocol with copyright protection, in ACM SIGCOMM Comp, Comm. Review, Vol. 32, No. 2, pp.42-60, Apr. 2002.

〔5〕 Salekul Islam and J.willian Atwood, " Security Issues in PIM-SM Link-local Messages", LCN 2004.

〔6〕 Salekul lslam and J,william Atwood, "A Framework to Add AAA Functionalities in IP Multicast", AICT/ICIW 2006.

〔7〕 Thomas Hardjano, Brad Cain, N Doraswamy, "A Framework for Group Key Management for Multicst Security." draft-ietf-ipsec-gkmframework-03.txt, Feb., 2000

〔8〕 Michael Steiner, Gene Tsudik, "Key Agreement in Dynamic Peer Groups" IEEE Transactions on Parallel and Distributed Systems, August 2000.

〔9〕 K. Chan and S.-H. G. Chan, "Key Management Approaches to Offer Data Confidentiality for Secure Multicast," IEEE Network, vil. 17, pp. 30-39, Sep.-Oct 2003.

〔10〕 Danny Raz, Yuval Shavitt, Active Networks for Efficient Distributed Network Management, IEEE Communication Magazine, Vol. 38, No. 3, March 2000.

〔11〕 T. Hayashi, "Internet Group membership Authentication Protcol(IGAP)", Internet Draft, work in progress.

〔12〕 I Romdhani, M. Kellil, and h.-Y. Lach, "IP Mobile Multicast: Challenges and Solutions," IEEE Communications Society Surveys and Tutorials First Quarter, 2004.

〔13〕 Carlisle Adams, Stephen Farrel, "Internet X.509 Public Key Infrastructure: Certificate Management Protocols", Request for Comments(RFC):2510.

〔14〕 Carlisle Adams, Peter Sylvestor, Michael Zolotarev and Robert Zuccherato, "Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols", IETF RFC 3029, February, 2001

〔15〕 Russell Housley, Warwick Ford, Tim Polk and David Solo, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", IETF RFC 3280, April, 2002.

김 영 준(Young Jun Kim) 정회원

1986년 한양대학교 전자공학과 학사

1991년 한양대학교 전자공학과 석사

2001년 2월 한양대학교 전자공학과 박사

1996년 3월~2001년 9월 혜천대학 정보시스템계열조교수

2001년 9월~현재 인하공업전문대학 정보통신과 부교수

<주관심분야> Mobile IP, Multicast