通信情報保護學會誌
第9券 第3號, 1999. 09

멀티캐스팅 네트웍에서의 정보보호를 위한 키 관리기술

김대호*, 박응기*, 김영수*

요 약

멀티캐스트 통신을 안전하게 하기 위해서는 멀티캐스트 트래픽을 보호하는 메커니즘을 추가하고 참여자를 인증하고 참여자에 대한 비 인가자의 접속을 막는 대책 등이 강구되어야 한다. 본 논문에서는 안전한 멀티캐스트를 구축하는데 필요한 보안요소를 전반적으로 살펴보며 핵심적인 요소기술로서 정보보호 키 관리기술의 최근 동향을 소개하며, 이들 기술을 비교·분석하였다.

I. 서 론

최근에 관심을 갖는 분산 응용분야, 예를 들어 멀티미디어 회의, 컴퓨터를 이용한 공동작업, 의료분야에서의 원격 진단 및 자문 등의 활성화는 다수의 참여자 사이에서 정보를 효율적으로 교환하는 방법에 달려있다. 네트웍 단위의 다수 수신을 위한 교환방식은 이러한 응용분야에서 주요한 통신모드로 등장하였으며 이를 멀티캐스트로 분류한다.[1,2]

그 동안은 멀티캐스트에 의해 발생되는 비밀과 프라이버시 문제를 구체적으로 고려한 일이 별로 없이 누가 참여하고 참여자의 보안레벨이 무엇인지를 제어하지도 않은 상태에서 세션을 열어 놓게 되었다. 전통적으로 원격회의는 전용선이나 dial-up 라인을 통하여 연결되므로 물리적 보안요소에 의존하면 되었다. 그러나, 인터넷이나 ATM(Asynchronous Tran Mode)처럼 복합적 네트웍에서 멀티캐스트 트래픽은 다른 종류의 트래픽과 함께 네트웍 자원을 공동으로 사용하게 되었으므로 이러한 종합적 이용을 위해서는 멀티캐스트 세션을 신속히 형성하고 융통성 있게 유지하여야 할 뿐만 아니라 보안성을 제공할 수 있어야 한다.

이들을 효율적으로 구현하기 위해 멀티캐스트를 사용하는 것을 제외하고는 소규모, 중간규모, 대규모 그룹 멤버들 사이에서 정보를 교환할 필요가 있다. 더욱이, 그룹은 수시로 구성멤버를 바꾸는 동적인 요소, 즉 멤버들은 언제든지 가입과 탈퇴를 임의로 할 수 있는 환경이 보장되어야 한다. 그리고 응용프로그램에 따라 다르지만 멤버들은 실제 그룹에 속한 다른 멤버들의 멤버쉽을 알 필요가 없는 가운데 이러한 응용프로그램을 이용하게 된다. IP 멀티캐스트 기능은 이러한 요구조건을 만족시키는 설계를 하고 있다.[2,3,4] 이 요구조건이 실용적며 신뢰성 있게 구현되려면, 적어도 수십만 가입자 이상을 수용하는 인터넷환경에서 운영되어야 하는데 이러한 확장성을 실현하는 것은 쉽지 않다.

본 논문의 II장에서는 멀티캐스트 정보보호에서의 문제점에 대해 설명하며, III장에서는

* 한국전자통신연구원 정보보호기술연구본부

안전한 멀티캐스트 통신을 위한 구현 기술을 설명하며, IV장에서는 안전한 멀티캐스트 통신을 위한 키 관리 방식에 대해 설명을 하였으며, V장에서는 안전한 멀티캐스트 통신을 지원하기 위한 키 관리 기술을 설명하고 비교분석 하였으며 마지막으로 VI장에서 결론을 맺는다.

II. 멀티캐스트 정보보호에서의 문제점

1. 기본적인 정보보호 서비스

안전한 멀티캐스트 통신을 보장하기 위해서는 유니캐스트 환경에서 발생하지 않는 특별한 문제들을 고려해야 한다.[2,3] ISO-7498에는 안전한 시스템을 설계하고 구현할 때 고려해야 할 다음 사항들을 정의하고 있다.

◇ 비밀성: 신뢰하지 못하는 제3자가 메시지에 접근할 수 없도록 하는 기능으로 암호 기법을 이용한다. 대칭형 암호기법에서는 모든 발신자와 그룹 구성원이 키를 공유하여야 한다. 비대칭형 암호 기법에서는 발신자의 공개키(public key)는 모든 수신자 구성원에게 분배되어야 한다.

◇ 무결성: 메시지가 전송 중 변경될 수 없음을 요구하는 기능이다. 무결성은 encrypted checksum이나 MD5 등을 이용한 keyed hash function을 이용하여 실현된다.

◇ 인증: 수신된 메시지가 정당한 발신자에 의해 발송되었음을 확인하는 기능이다. 멀티캐스트의 인증은 디지털 서명을 통해 구현된다. 키를 알고 있는 구성원도 그 내용을 변경하는 것은 불가능하다.

◇ 접근제어: 정당한 구성원만이 멀티캐스트 구성원에 연결되어 자원에 접근할 수 있음을 확인하는 기능이다. 접근제어는 키 분배용 접근제어 리스트를 이용하거나 디지털 서명을 이용하여 구현된다. 예를 들어 서명이 확인된 구성원만 멀티캐스트 구성원이 될 수 있으며, 정보 전송도 가능하게 된다. 적절한 접근제어가 없는 멀티캐스트 세션을 감청하는 것은 매우 쉽다.

◇ 부인봉쇄: 수신자 입장에서 발신자가 발신 사실을 부인한다 하여도 발신자가 송출하였음을 입증하는 기능이다. 부인봉쇄는 공개키 암호 기법과 디지털 서명을 사용해야 하며, 메시지마다 발신자의 비밀키(private key)로 서명되어야 한다.

2. 키 관리 문제

암호학적인 공격에 견딜 수 있는 강력한 암호 메커니즘을 멀티캐스트 세션에 사용한다고 가정하면 키 관리 및 키 분배가 중요한 문제가 되며 그리고 키에 관련된 자료에 대한 접근 제어가 중요시된다. 아무리 강력한 암호 메커니즘을 사용한다 하더라도 키 관리 및 분배 방식에 문제가 있다면 공격을 당할 여지는 항상 존재하게 되며, 인가되지 않은 다른 사람들에게 키가 분배된다면 멤버들 사이에서 통신하는 정보가 노출될 수 있다.

멀티캐스트 세션을 안전하게 보호하기 위해 필요한 알고리즘의 형태, 키의 크기, 키의 수 등은 적용하는 암호 메커니즘 및 키 구조에 따라 결정된다. 일반적으로 멀티캐스트 세션 참여자들은 세션 데이터를 암호하기 위해 그룹 멤버들이 공통으로 공유하고 있는 GTEK(Group Traffic Encryption Key)를 사용한다. 세션을 시작하는 사람(Initiator)은 그룹 멤버들에게 배포하는 다음의 세션키를 보호하기 위해 GKEK(Group Key Encryption Key)를 사용한다. 이처럼 마스터 키를 사용하는 방법을 도입한 이유는 세션마다 서로 다른 키를 사용하도록 함으로 마스터 키의 장기간 운영을 통하여 long term secrecy를 보장하며 그룹멤버와 키를 교환하는 부담을 줄이기 위한 것이다.[3]

어떤 특정 키로 암호화한 트래픽의 양과 시스템의 보안정책에 따라, 멀티캐스트 세션을 위해 정기적으로 새로운 키를 발급하거나 re-key을 할 필요가 있으며, re-key는 키가 노출되었을 때도 필요하다. 어떤 사이트가 노출되면 나머지 그룹 멤버들의 안전한 통신을 유지하기 위해 노출된 사이트를 배제해야 한다. 그룹으로부터 탈퇴한 참여자가 나중에 멀티캐스트 세션에 재등록하는 절차 없이 참여하는 것을 막기 위해서 그룹 전체의 re-key가 필요하며, 멀티캐스트 세션에서 배제된 멤버들이 결탁하여 새로운 그룹 키의 생성 및 재생성을 막을 수 있는 키 구조이어야만 한다. [3,4]

3. 그룹 멤버 확장성 문제

RSA와 같은 공개키 시스템에서 512비트의

키를 사용한다면 각 멤버마다 멀티캐스트 메시지 헤더에 64바이트 길이의 정보가 부가되어야 한다. 이러한 메시지 크기의 증가는 어떤 상황에서는 실용적이지 못할 수 있다. 이러한 문제를 해결하기 위해 short RSA키가 사용되기도 하며 다른 공개키 암호방식이 채택되기도 한다. 다른 방법으로는 그룹키와 안전한 키를 이용한 브로드캐스트 방식사이에서 세션의 중요도나 각 메시지에 따라 선택적으로 암호방식을 고르도록 하기도 한다.

때때로 세션의 멤버들은 상당히 많은 서브그룹을 구성하기도 한다. 예를 들어, 전화회의 응용프로그램에서 각자의 음성은 모든 수신자에게 방송되지만, 일부의 화상정보는 가까운 사람에게만 전송할 수 있다. 이러한 서브 그룹을 구성하는 방법은 비밀키를 사용한 브로드캐스트 알고리즘이 장점을 갖고 있는데, 그 이유는 데이터 암호키가 메시지 단위로 매우 동적으로 변경될 수 있기 때문에 이에 대비하여 가능성 있는 다량의 그룹키를 브로드캐스트 알고리즘에서는 저장할 필요가 없기 때문이다.[5]

초기에 사용자나 호스트에게 암호 키를 배정하는 일은 안전한 멀티캐스트에 참여하는 사용자나 호스트의 수가 증가함에 따라 점진적으로 늘어난다. 세션을 설정하는 메시지의 수와 멤버쉽을 변경하려는 메시지의 수는 세션의 사이즈에 따라 점진적으로 늘어난다. 이론적인 키 관리를 연구하는 단계에서는 소규모의 참여자를 고려한 키 관리 방안을 연구하면 되지만 범세계적 인터넷에서의 활용을 전제로 하게 되면 적어도 수십만 가입자는 처리할 수 있는 확장성과 임의로 그룹에 가입과 탈퇴가 가능한 동적 상황에서 전방보호와 후방보호가 확실히 보장되는 키 관리 방안을 연구하여야 한다.[2]

4. 멀티레벨 보안 문제

그룹에 대한 강제적 구성(mandatory bas에서 멀티 레벨 보안구조를 구현할 수 있다. 여기서, 그룹과 멤버는 다른 레벨에게는 비밀로 분류되며, 어떤 참여자는 자신에게 주어진 보안등급보다 상위 레벨의 그룹에 속할 수는 없다. 레벨에 따라 암호키가 배정된다. 자신보다 높은 레벨에 접속할 수 없으므로 암호할 경우, 키는 평문이 갖고 있는 보안레벨과 같거나 또는 상위 레벨이어야 한다. 이를 위해 멀티캐스트 네트웍을 각각의 보안등급에 따라 서로 다른 가상 네트웍을 구성하게 된다.

멀티레벨 보안에서는 낮은 레벨의 정보는 높은 레벨의 사용자가 접속할 수 있다. 이러한 것을 달성하는 방법의 하나는 낮은 레벨의 그룹 멤버들이 write-up기능을 가져 상위레벨에게 멀티캐스트 메시지를 보내는 것이다. 그러나, 발신측은 일반적으로 적절한 상위레벨 암호키를 소유할 수 없어 네트웍에서 신뢰할 수 있는 멀티레벨 네트웍 요소를 가져야 한다. 여기서는 상위레벨 멤버들이 이용할 수 있는 낮은 레벨의 키를 생성하거나, 낮은 레벨로 암호된 수신 메시지를 받아 복호한 후 메시지를 중계하기 전에 상위레벨 키를 사용하여 재 암호하는 게이트웨이 역할을 한다. 대신, 낮은 레벨 사용자는 상위레벨 공개키를 사용하여 write-up할 수 있다.

III. 안전한 멀티캐스트 구현 현황

1. IP 보안 구조

IP 보안구조[6]는 1995년8월 표준화되었으 1998년 8월 개정되어 RFC 2401로 발표된 있다. 많은 문서가 만들어졌으며, 일반 구조와 AH(Authentication Header), 공통 인증 알 즘(MD5) 및 ESP(Encapsulating Se Payload), 암호알고리즘(DES CBC모드)에 해 다루고 있다. IP 보안구조에서 키 관리 부분은 아직 정의되어 있지 않으며 현재 연구가 추진 중이다.

IP 보안구조에는 2종류의 보안 헤더(AH ESP)를 갖고 있으며, 강력한 암호기법이 일부 지역에서는 사용이 제한되고 있다. 미국에서는 암호에 대한 수출허가제가 운영되고 있어 어느 레벨 이상의 암호알고리즘이 장착되어 있는 시스템의 수출을 금하고 있다. AH는 IP레벨에서 동작하여 무결성과 인증 기능을 제공하며, IP패킷의 인증을 위해 사용된다. ESP는 비밀성을 제공하며, UDP(User Datagram Proto TCP(Transmission Control Protocol)와 상위 프로토콜에서 사용된다. 그러므로 AH만 사용하는 경우에는 수출과 사용에 제약을 전혀 받고 있지 않는다.

SA(Security Association)는 일련의 보안

보로서 목적지 번지와 SPI(Security Parameter Index)에 의해 유일하게 정의된다. SA에는 다음과 같은 많은 파라미터를 포함한다.

◇ 인증 알고리즘, 암호 알고리즘
◇ 인증 키, 암호 키
◇ 암호용 초기벡터(Initial Vector: IV)
◇ 키의 유효기간
◇ SA의 유효기간
◇ 발신자 번지

IPsec SA는 수신자에 의해 확인된다. 멀티캐스트 그룹은 멀티캐스팅 될 때에는 수신자로 간주된다. 그러나 실제로는 여러 개의 수신자 시스템이 존재하므로 그 중에 하나의 수신자 시스템이 SA와 SPI들을 정의해야 한다. 이 시스템이 그룹소유자(Owner) 또는 그룹발신자(Originator)가 될 수 있다.

유니캐스트 환경에서 통신 호스트들은 정보보호 서비스 제공을 위해 보안 파라미터를 협상할 수 있다. 그러나 참여자가 많은 멀티캐스트 환경에서 보안 파라미터를 협상하는 것은 일반적으로 비효율적이다. 따라서 멀티캐스트 환경에서 세션을 시작하는 사람(Initiator)은 전한 세션을 위한 보안 파라미터를 정의하여 그룹 멤버들에게 분배하며, 안전한 세션을 위한 보안 파라미터는 SA 형식으로 저장된다. 하나의 안전한 그룹 내에 여러 개의 SA 즉, SPI가 존재할 수 있다. 세션이 시작되기 전에 그룹 멤버들은 자세한 SA를 알아야 하며, 세션을 시작하는 사람(Initiator)은 세션을 시작하기 이전 SA를 안전하게 그룹 멤버들에게 분배하여야 한다.[3]

원칙적으로, 하나의 SA가 멀티캐스트 그룹에 사용될 수 있다. 발신자는 서로 다른 SPI를 선택하여 사용할 수 있으나, 강제사항은 아니다. 그러나, CBC모드 블록암호를 사용하는 시스템은 일부 경우에 Known-Plaintext공격에 대비책이 없으므로, 각 발신자마다 독립적인 SA를 사용할 것을 권고하고 있다.

2. 키 관리 시스템 구현 현황

IP 보안구조에서 제안된 키 관리 시스템으로는 SKIP(Simple Key-management for Internet Protocol)과 Photuris가 있다. Photuris는 statefull 연결성 프로토콜이며, SKIP은 stateless프로토콜인 점이 서로 다르며, SKIP이 라우터의 부하 안배 등이 가능한 프로토콜로서 네트워킹에 더욱 효율적인 것으로 평가되고 있다.[2,7]

GKMP(Group Key Management Pro는 멀티캐스트나 브로드캐스트를 위해서 개발된 키 관리 프로토콜이다. 원래는 군용으로 개발되었으며, 키 분배를 담당하는 그룹관리자를 필요로 한다.[8]

2.1. SKIP(Simple Key-management fo Protocol)

SKIP은 Diffie-Hellman(DH) 키 교환을 이용하고 있다. DH에서는 통신하고자 하는 쪽이 공유 비밀 값을 만들기 위해 비밀 값 i를 생성한 후 이 값을 이용하여 공개 값 gI (mod p)를 계산하여 상대방에게 전송한다. 이 경우 공유 비밀 값은

$(g^i)\ j(\text{mod } p) = g^{ij} (\text{mod } p)$ 이다.

SKIP에서는 수신자의 인증된 DH공개 값 g^{ij} (mod p)를 쉽게 이용할 수 있어야 하며, 렉토리 서비스나 수동 키 분배에 의해 가능하다. 이 공유 비밀 값은 수신자의 공개값과 발신자의 비밀 값으로 계산되어지므로, 발신자 입장에서는 수신자와 관계없이 계산할 수 있다.[7]

이 프로토콜에서는 키를 암호하는 키로서 공유 비밀 값을 사용한다. 암호나 인증에 사용되는 실제 키는 공유 비밀 값으로 암호되거나, 공유 비밀 값과 현재 시각 정보(time stamp)이용한 해쉬 값으로 주어진다.

SKIP은 아직 완성된 것이 아니며 IETF I Security 웍킹 그룹에서 Photuris와 함께 개중이다. SKIP은 발신자가 SA를 선택하기 때문에 IP Security 모델에 정확하게 부합되지는는다. 몇 가지 문제가 있으나, 가장 심각한 취약점은 전방보호(Forward Secrecy)가 안 된는 것이다. 만일 범죄자가 어떤 노드의 비밀키 정보 i를 알아낸다면 연결된 모든 노드의 SKIP 트래픽을 복호할 수 있게 된다.

SUN에서는 SPARC Solaris 2.4에 SK 구현하여 배포한바 있다. 이 배포는 미국의 수출허가제에 걸려 북미 지역으로 제한되어 있다. 그러나, SKIP을 구현하는 것은 GNU Public License에 의해 제약을 받지 않는다.

SKIP은 멀티캐스트 트래픽에 사용될 수 있도록 확장되어 개발되어 있다. SKIP이 사용될 수 있는 두 가지 다른 모드가 있는데, 하나는 임시 멀티캐스트 그룹에 적합한 모형이고 다른 하나는 고정 멀티캐스트 그룹이나 브로드캐스트 그룹에 적합한 모형이다.

임시 멀티캐스트 그룹에 사용되는 모드는 그룹소유자가 존재하여 키 분배를 담당한다. 그룹 구성원들은 Group Interchange Key(GI 확보하기 위하여 그룹소유자에게 키 전송을 요구한다. GIK는 키 암호용 키로서, AH와 ESP 사용되는 키를 암호하는 기능을 갖고 있다. 발신자마다 패킷 암호 및 인증 용 키를 선택하여 GIK로 암호하여 SKIP 헤더에 실어 보낸다.

멀티캐스트 그룹이 고정되어 있고 그룹소유자가 없을 경우에는, GIK는 모든 그룹 구성원에게 수동으로 전달되어야 한다. 이 경우, GIK가 키 암호용 키로서 사용되지 않으나 GIK나 시각정보에 대한 MD5 해쉬용으로 사용된다.

SKIP에서는 GIK를 얻기 위해 안전한 유니캐스트 프로토콜을 정의하고 있다. 예견되는 그룹 구성원들이 실제로 그룹에 가입하고자 할 때에는 이 프로토콜을 사용하게 된다.

2.2. GKMP(Group Key Management

멀티캐스트용 키 관리 시스템으로 개발된 방식이 GKMP이다.[8] 그룹 멤버 중에 하나 그룹 제어(Group Control)로 할당하여 액세제어 목록(ACL: Access Control List)에 되어 있는 그룹 멤버에게 토큰을 배정하는 기능을 수행한다. 이 때 보안에 대한 정도를 파악하여 그룹 멤버가 갖고 있는 보안 레벨(security level)과 범주(security category 라 적절한 토큰을 할당하는 기능을 수행한다.

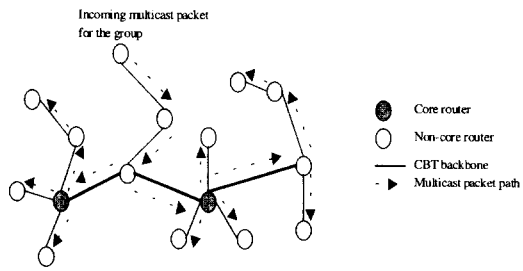
그룹 제어자는 그룹에 가입하는 정책을 수립하고 집행하며 그룹키 암호용 키(GKEK)와 그룹 세션 또는 트래픽 암호키(GTEK)를 생성하는 기능을 담당한다. 키에 대한 수명과 훼손된 키에 대한 재 주입 및 복구에 대한 요구사항을 정의하고 탈퇴하는 가입자에 대한 보증서 취소목록(Certificate Revocation List)을 작고 유지하는 기능도 담당한다.

GKMP에 대해서는 일부 프로토콜에 대한 방안이 RFC 2094으로 제시된 바 있으나 범용을 위한 연구가 계속 추진되고 있다.

3. CBT(Core-Based Tree) 멀티캐스트 프로토콜

일반적으로 라우팅 프로토콜은 유니캐스트 라우팅 프로토콜에서 사용하던 distance vect 알고리즘과 link state알고리즘을 이용하여 멀캐스트 용으로 확장한 알고리즘들이 주를 이루고 있다. 한편, 멀티캐스트 라우팅 알고리즘을 위하여 공유(shared tree) 알고리즘이 개발되 새로운 프로토콜이 개발되고 시험 중에 있다. PIM-SM(Protocol Independ Multicast-Sparse Mode)과 Core B Trees(CBT)가 이에 속하며 Sparse 모드로 류되어 그룹멤버가 광범위한 지역에 분산되어 있는 경우에 사용하기에 적합하다.[1] 특히 CBT는 기존방식보다 키 관리 기능에 확장성(scalable)과 효율성(efficient)을 부가하고 있 프로토콜에 따라 서로 다른 키 분배 방식이 개발될 수 있다.[2,3]

기존에 나와 있는 멀티캐스트 포워딩 알고리즘에 최근에 더해진 알고리즘이 CBT이다. 소스에서부터 출발하는 방식이나, (소스, 그룹쌍에 대한 가장 짧은 길을 찾는 기존의 알고리즘과는 달리 CBT는 한 그룹 내에 있는 모든 멤버들이 공유할 수 있는 배달 트리를 구성하는 방식이다. CBT알고리즘은 각 그룹에 대한 다른 core 중신의 트리를 구성할 수 있도록 허용하는 것만 제외하고는 spanning 트리 알고리즘과 유사하다. 각 그룹에 대한 멀티캐스트 트래픽은 소스와는 관계없이 동일한 배달 트리를 통하여 송수신을 한다.



[그림 1] 다중 core CBT 멀티캐스트 배달 트리

CBT는 멀티캐스트 배달 트리의 핵심으로 동작하는 라우터를 하나 또는 여러 개를 포함

할 수 있다. [그림 1]은 멀티캐스트 트래픽이 CBT 백본(backbone)을 통해 그룹 내의 모든 멤버에게 포워딩 되는 것을 보여주고 있다. CBT 백본에는 core 라우터와 non-core 라우터를 포함하고 있다.[1]

멀티캐스트 번지를 갖는 트래픽을 수신하기를 원하는 스테이션은 특정 멀티캐스트 그룹의 core 트리로 가입 메시지를 송신해야 한다. 그룹 멤버로 가입하고자 하는 멤버만이 유니캐스트 방식으로 가입 메시지를 송신하기 위하여 그룹 core 라우터 중의 하나의 번지를 알 필요가 있다. 가입 요구를 수신한 인터페이스가 그 그룹의 배달 트리에 속해 있음을 확인하는 중간 라우터에서 이 가입요구를 처리한다. 중간 라우터는 계속 가입 메시지를 core를 향해 포워드하며 그 요구가 core 라우터에 도착할 때까지 로컬 인터페이스에 주의를 기울인다.

아직 CBT방식에는 몇 가지 제약사항이 존재한다. CBT는 모든 소스로부터 core를 향해오는 트래픽이 동일한 링크를 이용하므로 core라우터 근처에서 트래픽 집중현상이 일어나며 병목현상을 야기하게 된다. 더욱이, 하나의 배달 트리를 공유하는 것은 지체현상이 증가하는 루트를 만들 수도 있어 멀티미디어 응용프로그램에서 심각한 사항으로 등장할 수도 있다.

4. 신뢰성 있는 멀티캐스트 프로토콜

RMTP(Reliable Multicast Tran Protocol)는 다양한 서비스를 제공하는데 사용되는 신뢰성 있는 멀티캐스트 전송 프로토콜이다. 각 발신자는 자신의 패킷 별로 순차적으로 정리하거나, 그룹으로 보내는 전체 패킷을 순차적으로 정리할 수 있다. RMP는 total order 이라고 불리는 기능이 있어 수신한 패킷을 응용소프트웨어로 보내기 전에 그룹 내에 있는 모든 구성원이 패킷을 제대로 수신했는지를 확인한다.

RMP는 특수 멀티캐스트 서버나 그룹관리자를 필요로 하지 않는다. 이 프로토콜은 토큰을 순환시키는 방법과 ACK(acknowledgeme /NACK(non acknowledgement) 신호를 송신하는데 기초하고 있다. 토큰은 모든 수신자 사이를 돌아다니며, 토큰소유자는 토큰을 갖고 있는 동안만 수신할 수 있는 패킷을 인식한다. 토큰은 다음 수신자로 이동되며 ACK/NACK 신호는 멀티캐스트 방식으로 보내진다. 다른 그룹 구성원들이 패킷 일부를 수신하지 못했다는 것을 인식하면 NACK신호를 원 발신자에게 보낸다.

멀티캐스트 그룹에 있는 각 구성원은 접근제어 리스트를 갖고 있어 수신자 구성원과 외부 발신자들을 포함한다. 외부 노드에서는 RMP 토큰 링을 통해 메시지를 보냄으로 멀티캐스트 그룹에 메시지를 보내게 된다. 구성원 가입 신청은 그룹 구성원 전체에게 보내게 된다.

이 방식은 일 대 다수(one-to-multi)의 우 멀티캐스트를 대상으로 개념이 개발되고 있으나 아직 해결되지 않은 문제점이 많으며 앞으로 다수 대 다수(multi-to-multi)까지 포함 멀티캐스트 개념이 완성되면 실용화 될 것으로 보인다.

IV. 멀티캐스트 키 관리 방식

1. 고전적인 키 관리 방식

1.1. 키 사전 분배 기법(Key Pre- distrib Scheme)

가능한 모든 그룹에 관련된 비밀 정보는 운영하기 전에 모든 멤버들에게 배포하는 기법이다.[3,4] 이러한 사전배포는 임의의 두 상대간 키 분배 프리미티브의 도움으로 수행된다. 그 후에 신청한 사람들의 보증서에 따라 만들어진 키 목록으로부터 어느 한 멤버는 특정한 그룹의 공통키를 읽을 수 있게 한다. 그룹 멤버쉽 변동이란 다른 그룹으로의 스위칭을 뜻하며, 사전에 배포된 키 목록으로부터 다른 공통키를 찾아내는 것을 의미한다. 이 기법은 그룹키 배포 센터를 신뢰할 수 있는 동안은 안전하다. 각 사용자에게 필요한 키 저장장소 즉 메모리의 양은 그룹 참여자의 수에 따라 기하 급수적으로 늘어난다.

1.2. Secure Lock

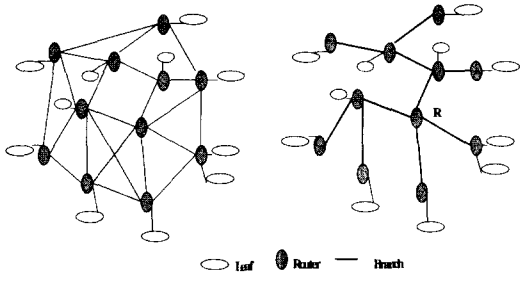
Secure Lock을 구현하는 것은 중국인의 머지 정리에 근거한다.[3] 여기서, 그룹 세션 키는 허가된 사용자의 키에 의해서만 세션키를 불러낼 수 있도록 하므로 안전하게 유지한다.

이러한 Secure Lock을 사용하는 것은 암호문의 하나의 복사 내용만을 보내게 되며 각 사용자가 갖고 있는 비밀키의 수를 최소로 하게 된다.

이 방법의 취약점은 각 참여자마다 다른 멤버와는 상대적 소수 관계를 갖는 큰 수를 하나씩 갖고 있어야 한다는 것과 그룹 세션키를 얻는 과정에 소요되는 계산량이 많다는 것이다. 이러한 조건으로 인해 이 프로토콜은 소규모 그룹의 경우에서만 사용되도록 제한되어 있다.

2. Spanning Tree 키 관리 방식

멤버들 사이에 구성된 Spanning 트리를 따라 키를 분배하는 방식으로서 모든 멤버들 사이에서 키에 대한 데이터의 변경 없이 안전하게 포워드 시킨다는 전제를 갖고 있다. 여기서는 그룹 멤버쉽을 안전하게 변경하는 방법을 다루고 있지 않으며 또한, 그 효율성도 다루고 있지 않다.[3,4]



[그림 2] Spanning 트리

Spanning 트리는 인터넷에 있는 어느 두 개의 라우터를 연결하는 실제의 길(path)이 오직 하나가 되도록 만든 트리 구조를 말한다.[1] [그림 2]은 라우터 R에 연결되는 사항과 Spanni 트리를 보이고 있다.

이러한 Spanning 트리 방식은 Spanning 리 프로토콜이 인터넷에서 오랫동안 사용되었으며 많은 경험이 있기 때문에 구현하기 쉽고 강력한 방안으로 알려져 있다. 그러나, Spanning 트리 방식은 몇 개의 링크로 트래픽이 집중됨으로 소스 서브네트워과 그룹 멤버사이에서 가장 효율적인 길을 제공하지는 않을 수 있다.

이를 보완하기 위하여 소스에서부터 방사되는 형태(source-rooted)의 트리를 구축하는 본적인 알고리즘으로 Reverse Pa Broadcasting(RPB)이 등장하였으며, 데이터그램이 멤버가 없는 서브그룹에게도 불필요하게 포워딩되는 경우를 제외시키기 위하여 Truncated Reverse Path Broadcasting(TRPB)이 등장하였다.

3. Clique 키 관리 방식

그룹 내에 같은 속성을 갖는 소규모 그룹을 구성하는 방식으로 동적으로 변화하는 그룹 내에서 세션 키를 분배할 수 있는 기능을 부여하는 방식이다. 그러나 이 방식은 멤버쉽이 바뀔 때마다 그룹 관리자는 O(n)의 메시지 교환을 수행하여야 하므로 대규모 가입자를 수용한 경우에는 그 메시지가 기하 급수적으로 늘어나 확장성이 떨어지는 단점을 갖고 있다.[4]

두 가입자 사이에서 비밀키를 안전하게 공유할 수 있는 방안으로 널리 알려진 Diffie-Hellman 키 교환방식을 n가입자까지 장하여 사용하고 있으며 여기서는, 멤버들이 논리적인 ring을 구성하며, 모든 멤버들이 동시에 가입하고 n-1라운드 참여하는 것으로 하였다. 주어진 라운드에서 각 참여자는 먼저 수신한 값에 자신의 비밀 값을 지수승하여 그 결과를 다음 참여자에게로 전달한다. n-1 라운드하면 모든 참여자는 동일한 키를 공유하게 된다. 이 프로토콜은 매우 큰 잠재력을 갖고 있으며, 정적인 키 배분의 경우에는 적합한 방식이다.

4. Iolus 키 관리 방식

이 방식에서는 대규모 그룹을 여러 개의 소규모 그룹으로 분할하여 서브 그룹을 만들어 둠으로 멤버쉽 변동에 따라 키 변경의 영향을 받는 멤버 수를 줄이는 기법을 사용하고 있다.[5] 중계 노드를 정의하여 관리에 대한 제어 및 패킷의 rekeying을 담당하도록 한다. 이 방식에서는 중계되는 전 과정이 신뢰할 수 있어야 하는 것은 아니나 전송지연이 발생되며 또한 중계 시 고장이 발생되면 잘 처리하지 못하는 단점을 아직 갖고 있다.

Ballarrdie는 확장성 있는 키 분배 기법 제시하였는데 이 기법은 CBT멀티캐스트 구조에 근거하고 있다.[9] 여기서는, 그룹키 분배센터(Group Key Distribution Center : GK 그룹키에 대한 액세스를 제어한다. 나중에, GKDC의 일부 기능이 그룹에 가입하고자 할 때의 path 상에 있는 다른 라우터로 옮겨진

다. 각 연결 라우터(joining router)에는 액세스 제어 목록과 그룹 keying material(KGRP)을 포함하는 그룹 액세스 목록이 패킷에 의해 제공된다. 이 기법에서는 라우터가 절대적으로 신뢰할 수 있어야 하며 새로운 그룹키를 설정하기 전에는 그룹키의 변화가 생겨서는 안 된다.

최근에는 Mittra가 매우 동적으로 변하는 대규모 그룹에서 확장성 항목을 다루는 해결방안을 제시하고 있다. 좀더 적은 규모의 안전한 멀티캐스트 서브 그룹들로 구성된 안전한 분배 트리는 안전한 멀티캐스트를 가능하게 하기 위해 사용된다. 서브 그룹들은 계층적으로 가상의 안전한 멀티캐스트 그룹을 만들며, 서로 독립적인 keying material을 사용하게 된다. 멤버쉽 변동에 따른 keying material의 변화에 대한 요성은 특정한 서브그룹으로 제한된다. 가입할 때는 원래의 KGRP 을 갖고 암호화 된 새로운 서브 그룹키 KGRP 는 기존의 서브그룹으로 멀티캐스트되고 새로 가입한 멤버에게는 구분된 안전한 채널을 이용하여 유니캐스트된다. 또한 탈퇴할 때에는 KSGRP 의 n개(여기서 n은 서브그룹에서 남아 있는 멤버라고 가정함) 복사본을 포함한 메시지를 멀티캐스트하며 KSGRP 의 각 복사본은 그 멤버의 비밀키로 암호되어진다. 이 방식에서는 서브그룹 에이전트 전체에 대한 신뢰를 필요로 한다. 전송되는 메시지 사이즈나 가입과 탈퇴 시 키 복호 관점에서 보면 이 프로토콜은 복잡하다.

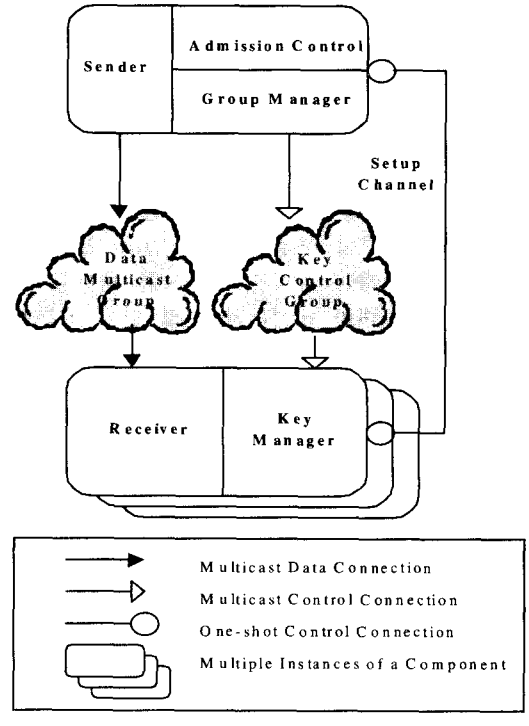
V. 멀티캐스트 키 관리 기술 연구동향

1. 키 관리 구조(Architecture)

1.1. 구성요소(Components)

〔그림 3〕은 한 발신자와 다수의 수신자로 구성되어 있는 기본적인 구조를 간단하게 표시하고 있다. 기본적이며 공통적인 기능을 우선 설명하고 확장과 변경을 위한 개별적인 기능에 대해서는 뒤에 제시하겠다. 일반적으로 구성요소는 두 개의 그룹으로 분리될 수 있다.〔4〕

1) 데이터와 관련된 그룹으로 기존의 보안기능이 없는 멀티캐스트나 브로드캐스트 통신 구조의 구성요소와 매우 유사하게 되어 있다. 발신자, 수신자 및 데이터 멀티캐스트 그룹으로 구성되어 있다.
2) 제어 혹은 키 관리와 관련된 그룹으로 키 관리와 키 교환에 필요한 모든 컴포넌트로 구성되어 있다.



〔그림 3〕 안전한 멀티캐스트의 구성요소

각 구성요소의 특성을 살펴보면 다음과 같다.

◇ 송신자(Sender): 응용 프로그램은 데터를 보안기능이 없을 때처럼 준비하고 난 후 그룹관리자로부터 현재의 트래픽 암호키(TEK Traffic Encryption Key)를 수신하여 패킷을 호한다.

◇ 수신자(Recipient): 데이터 멀티캐스 그룹으로부터 데이터를 수신하여 로컬 키 관리자가 발생한 TEK 키를 사용하여 복호한다. 응용 프로그램의 데이터 처리 과정에서는 암호와 인증된 결과와 차이가 있음을 경고하지는 않는다.

◇ 데이터 멀티캐스트 그룹(Data Multica Group): 발신자로부터 수신자 그룹으로 보내진 패킷을 안전하게 전달하는 멀티캐스트, 브로드캐스트 또는 애니캐스트의 채널로서 응용프로

그램에 의한 대량 데이터 전송에 이용된다.

◇ 그룹 관리자(Group Manager): 그룹 통신의 참여자로부터 가입과 탈퇴에 대한 요구를 받고 허용하며 처리한 후 키 관리자에게 필요한 키 변경을 수행하도록 메시지를 전송한다.

◇ 가입제어(Admission Control): 그룹 리자가 누구를 허용해야 하는 지를 가입제어에게 묻게 된다. 이 기능은 일반적으로 사람에게 위임될 수 있다.

◇ 키 관리자(Key Manager): 그룹 관리로부터 re-keying요구를 받아 해석하고 그 결과 TEK를 수신자에게 보낸다.

◇ 채널 설정(Setup Channel): 새 가입 가입신청은 유니캐스트 방식이나 다른 별도의 (out-of-band) 메커니즘을 통해 수신된다. 채널은 가입 요구가 있을 경우와 새 가입자와 그룹 관리자 사이에서 인증기능을 수행하는 경우에만 필요하다.

◇ 키 제어 그룹(Key Control Group): 관리자와 수신자 사이에서 패킷을 전달하는데 이용되는 멀티캐스트나 브로드캐스트 채널을 말한다. 이 사이에서 전달되는 트래픽은 참여자가 있는 키 관리자로 전송하는데 필요한 새로운 keying material로 구성되어 있다. 이 채을 통한 전송은 모든 참여자에 의해 수신되어야 하며 패킷이 수신자에게 분명히 전달되었음을 확인하기 위한 다양한 기법이 사용되어야 한다.

1.2. 기본동작

TEK를 안전하게 전송하려면 몇 개의 키 암호용 키(KEK: Key Encryption Key)를 하여 TEK를 포함하는 제어 트래픽(Contr Traffic)을 암호하여야 한다. 각 키를 구분하기 위해서는 제어 트래픽에는 고유한 ID와 버전 번호, 개정(revision)번호 및 keying mater 포함하고 있다. 버전필드와 개정필드를 사용함으로 제로 메시지 가입(zero-message joini 이 가능해진다.[4]

◇ 그룹 생성(Group Creation): 그룹관는 그룹정보와 액세스 제어정보로 구성되어 있으며 그룹 파라미터를 디렉토리 서비스를 사용하여 공표한다.

◇ 단일 가입(Single Join): 새 가입자의 키 관리자가 그룹관리자에게 가입 요구정보를 보내면, 이 참여자가 가입 가능한지 여부를 점검한다. 만일 가입이 가능한 참여자이면 그룹관리자는 고유한 ID를 배당하고 새 가입자에게 전송할 일련의 KEK를 선택한다. KEK를 선택하는 방법은 각 키 관리 기법에 따라 다르다.

그룹관리자는 모든 키(TEK, KEK)의 개정번호를 증가시키며 해쉬함수와 같은 일방향 함수를 이용하여 keying material을 보호한 후 가입자에게 키를 전송한다. 또한 발신자에게는 개정번호와 TEK를 변경하도록 알려 준다. 다른 참여자들은 정규 데이터 패킷을 통해 개정번호의 변경을 볼 수 있도록 통지하며 일방향 함수를 이용하여 TEK를 전송한다. 그 함수는 역방향 전환이 안 되므로 새로운 가입자는 이전에 사용하던 키를 알아낼 방법이 없다(전방보호).

◇ 단일 탈퇴(Single Leave): 그룹을 탈하는 데에는 침묵 탈퇴(Silent Leave), 자유퇴(Voluntary Leave) 및 강제 탈퇴(Fo Leave)의 세 가지 방법이 있다. 이 중에서 3번째 방식인 강제탈퇴의 경우에만 그룹관리자가 관여하게 된다. 어떤 참여를 희망하는 자가 배제될 필요가 있다고 가입제어가 판단하면 탈퇴 메시지를 보내게 된다. 또한 그룹에 참여자도 가입제어에게 어떤 멤버의 배제를 요구할 수도 있는데 이 모든 경우는 관리정책에 따라 다루어진다.

어떤 멤버를 배제시키려면 그 멤버에게 알려진 모든 키를 새로운 keying material을 사용여 대치하여야 한다. 그리고 남아있는 다른 참여자들이 이 사실을 알아야 하므로 이 경우 개정번호를 변경하게 된다. 또한 그룹관리자는 배제된 멤버를 제외한 모든 참여자의 키 관리자에게 그들이 복호할 수 있는 형태로 암호된 새로운 keying material을 포함한 메시지를 보게 된다.

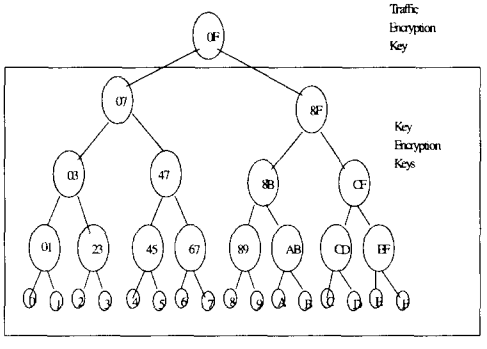
2. 중앙 집중형 Tree-Based 키 관리

개인별 참여자를 가장 밀접하게 제어하는 방안은 중앙 집중형 기법을 사용하면 가능해지며, 고도의 보안을 필요로 하는 응용분야에 적합한 방안이 된다. 이 방안은 구현하기 쉬우며 유지하기도 쉽고 네트워이나 수신자의 부담도

매우 적은 기법이다.[3,4] 모든 keying material은 그룹관리자에 의해 중앙에서 관리되며, 모든 참여자는 여기에 등록하여야 한다. Keying material을 저장할 때에는 이진 트리(binary tree)를 사용한다. [그림 4]는 최대 16개의 그룹 멤버를 갖고 있으며 깊이(depth)가 4인 트리를 나타낸다.[4]

설치단계 과정에서 각 참여자는 그룹관리자와 공유 비밀 값을 정한다. 이 공유 비밀 값은 그룹관리자와 해당 참여자만이 알고 있으며, 가장 낮은 레벨의 키 암호키(KEK)로 사용한다 그룹관리자가 소유하고 있는 이진 트리의 노드들은 많은 KEK를 포함하고 있으며, 그룹의 멤버쉽을 변경하고자 할 경우에 새로운 keying material을 위해 KEK를 사용하여 효율적인 신을 수행한다.

각 참여자는 트리 위에 있는 키 중에서 극히 일부의 서로 다른 키의 부분집합만을 갖고 있으며, 좀더 명확히 말하자면 참여자가 있는 노드에서 최상위 루트 노드까지 연결되는 path 상에 있는 키들만을 갖고 있으며, 이들은 TEK로서 사용된다. 메시지를 그룹의 일부만 이해하면 된다면, 예를 들어 KEK 47을 사용하여 암호된 메시지를 참여자 4부터 7까지만 이해할 수 있다면 이와 같은 중간단계의 KEK를 사용하면 이러한 목적을 이루게 된다. 이러한 방법을 사용하면 새로운 키를 전송할 경우 제한된 수신자에게만 키를 전송하고 나머지 멤버에게는 키를 전송하지 않아도 되는 것이다.



[그림 4] 이진 계층 키 구조
16진수로 표시된 KEK값은 이 범위 내의 가입자만 이 키를 알 수 있다는 것을 나타냄

◇ 가입(Join): 가입 동작에서, 참여자의 관리자는 그 요구사항을 유니캐스트 방식으로 그룹관리자에게 보낸다. 여기서는 가입제어 여부를 점검하고 ID(예를 들어 4)를 할당하며 참여자의 개인 키를 저장한다.

그룹관리자는 참여자의 노드로부터 루트 노드를 향한 path에 있는 모든 키의 개정번호를 증가시키며(KEK가 45, 47, 07, TEK가 0F 방향 함수를 거쳐 저장하며, 가입한 참여자에게는 키에 대한 새로운 개정번호를 보내는데 해당 버전 번호와 함께 보낸다. 동시에, 모든 발신자에게는 개정번호가 변경되었음을 가급적이면 신뢰할 수 있는 방법으로 알려주며, 이때부터 새로운 TEK를 사용하기 시작한다. 새로운 증가된 개정번호를 사용하여 발신자가 보낸 첫 번째 데이터 패킷을 수신하게 되면 다른 수신자들은 TEK의 변화를 알게 된다. 이렇게 함으로 트래픽을 줄이면서도 개정번경 사실을 전달할 수 있게 된다.

◇ 탈퇴(Leave): 탈퇴 동작을 수행하려면 그룹관리자는 남아있는 참여자들의 키 관리자에서만 복호할 수 있는 새로운 key material 포함한 메시지를 보낸다. 또한, 탈퇴한 참여자가 사용했던 슬롯을 해제하여 새로운 신청 시 재 사용할 수 있도록 한다.

참여자 C가 탈퇴한다고 가정하자. C가 알고 있었던 키(KEK가 CD, CF, 8F 및 TEK가 들은 노출된 것으로 볼 필요가 있으므로 C가 알 수 없는 방법으로 이 키들이 변경되어야 한다. 이는 탈퇴한 사람이 속해 있던 하위 노드로부터 TEK를 저장하고 있는 루트 노드까지 path를 따라 효율적으로 수행되어야 하며, 적절한 모든 노드의 키를 사용하여 새로운 키를 암호해야 한다. [그림4]에서 보인 예에서 새로운 KEK가 CDnew (CD의 대체)라면 CDnew 는 에게만 수신될 필요가 있으며, CFnew 는 참여자 D, E, F에게 보내진다. 8Fnew 는 8에서까지와 D에서 F까지의 참여자에게 보내지며 새로운 TEK 0Fnew 는 C를 제외한 모든 참여자에게 보내져야 한다. 이렇게 함으로 참여자 각각에 대하여 개별적으로 새로운 키를 암호하여 전송하는 대신 기존의 계층구조의 이점을 이용할 수 있다.

3. 중앙 집중형 Flat 키 관리

계층적이며 트리 방식에 근거하여 키를 분

배할 수 있게 ID의 각 비트를 구성하는 대신에 키 관리 방식을 평면으로 할당할 수 있다.[4] 이 방안은 데이터베이스에 대한 요구사항을 줄이는 이점을 갖고 있으며, 발신자가 메모리에 모든 참여자의 정보를 갖고 있을 필요가 없게 된다. 애당초, 그들이 그룹에 속해 있는 지 여부를 알지 않고도 참여자를 배제시키는 것이 가능하게 된다.

TEK		
KEK 0,0	KEK 0,1	ID Bit #0
KEK 1,0	KEK 1,1	ID Bit #1
KEK 2,0	KEK 2,1	ID Bit #2
KEK 3,0	KEK 3,1	ID Bit #3

Bits Value=0 Bits Value=1

[그림 5] Flat ID 할당

그룹관리자가 갖고 있는 데이터 구조는 2W+1개의 엔트리가 있는 간단한 테이블이다 한 엔트리에는 현재의 TEK가 있으며 나머지 2W개 슬롯에는 KEK가 있다. W는 참여자 I가 갖고 있는 비트의 양을 나타내며, 보통은 전송 계층이나 네트워 번지와 동일하다. 네트워 번지에 있는 각 비트에 대해서 두 개의 키가 이용 가능하다. 각 참여자는 그 키의 W값을 알고 있으며 그것은 그 번지에 있는 단일 비트에 의존하는 값이다. 모든 키는 위에서 거론한 트리 구조에서 설명한 것과 같은 버전과 개정번호를 포함하고 있다.

테이블에는 W를 구성하는 각 비트(b) 마다 2개씩 키가 주어져 전체적으로 2W개의 KEK가 존재하며 이진수 v에 대응하여 표시한다. 값 v를 갖으며 비트 b와 관계 있는 키를 Kb.v(비트키)로 표시한다. 테이블에 있는 키들은 트리와 같은 키 구조를 만드는데 사용될 수도 있으며 서로 독립적으로 사용된다.

이렇게 생성된 결과는 트리를 이용한 제어 방식과 매우 유사하지만, 키 스페이스는 매우 적다. W비트의 길이를 갖는 어떤 ID에 대해서 TEK를 포함하여 2W+1개의 키 만이 필요하며 참여자의 실제 수와는 관계가 없다. 참여자의 수가 2W로 제한되어 있으며 아직 키의 수와 변경 메시지의 크기가 클 필요가 없어 여기서는 W에 32를 사용하여 점검해 본다. 저장장소와 통신의 수를 축소하는 이외에도 이 방안은 지금 누가 멤버인지를 추적하고 있지 않아도 되며 아직은 그룹관리자만이 원하지 않는 참여자를 강제 탈퇴시킬 수 있다.

◇ 가입(Join): 가입하기 위하여 신청자는 그룹관리자와 접촉하여 개정번호를 증가한 후 고유한 ID를 할당받고 ID의 각 비트에 해당하는 키를 수신한다. ID는 네트워 번지로부터 얻을 수도 있다. 예를 들어, 이진수로 ID가 001인 새로운 가입자는 Kb.v형태의 키로 TEK와 KEK로서 K3.0, K2.0, K1.1 및 K0.0을 (setup) 채널을 통해 안전하게 수신한다. 물 개정번호는 증가된다.

◇ 탈퇴(Leave): 탈퇴하는 사람이 알고는 모든 키(TEK 및 W개의 KEKs)는 유효하지 못한 것으로 간주한다. 이 키들은 탈퇴자가 추적할 수 없는 방법, 그러나 남아 있는 참여자들은 계산하기 쉬운 방법으로 교체되어야 한다. 그룹관리자는 두 개의 부분으로 구성된 멀티캐스트 메시지를 보낸다. 우선, 그 메시지에는 남아 있는 사람들의 KEK로 암호된 새로운 TEK를 포함하며, 이는 탈퇴자의 ID와는 적어도 한 비트 이상 차이가 나지만 나머지 모든 참여자들은 새로운 TEK를 계산할 수 있게 된다. 두 번째로는 그 메시지에는 무효가 된 KEK 각각에 대하여 과거 KEK와 새로운 TEK를 둘 다 사용하여 암호한 새로운 KEK를 포함하고 있어, 그룹에 남아있는 모든 참여자들이 먼저 갖고 있던 KEK를 변경할 수 있게 된다. 그러나 다른 가입자가 갖고 있는 키에 대한 어떤 정보도 이 과정을 통해 얻을 수는 없다. 예를 들어, 이진수로 0110의 ID를 갖는 가입자가 탈퇴할 때 발생되는 메시지의 형태를 살펴보자.

$E(KEK\ 0.0_{new})$	$E_{KEK0.1}(TEK)$	ID Bit #0
$E_{KEK1.0}(TEK)$	$E(KEK\ 1.1_{new})$	ID Bit #1
$E_{KEK2.0}(TEK)$	$E(KEK\ 2.1_{new})$	ID Bit #2
$E(KEK\ 3.0_{new})$	$E_{KEK3.1}(TEK)$	ID Bit #3

Bits Value=0 Bits Value=1

[그림 6] 중앙 집중형 Flat : 참가자 0110을 제하기 위한 메시지

중앙 집중형 트리 방식과는 달리 참여자끼리의 결탁을 찾아내어 배제시키는 것이 용이하

지 않다. 여기서, 그들은 키 테이블을 서로 공유할 수 있으며, KEK를 공유하고 있지 않은 서브그룹을 정의하고 커버할 수도 있다. 서로 결탁하고 있는 가입자 중 적어도 하나가 갖고 있는 개별적 KEK를 공유하는 모든 참여자는 결탁한 사람이 갖고 있는 keying material을 자신의 것들과 구분할 수 없다. 지금까지 알려진 대부분의 방안에서는 결탁한 경우 배제시키는 것이 불가능한 것으로 알려져 있다. Flat 방안에서는 보안정책에 결탁한 사람을 배제하는 범위를 일일이 열거함으로 가능해 진다. 즉, 결탁한 사람이 소유할 수 있는 모든 키를 고려하여 정책에 반영하는 것이다. 이 방안은 유효한 가입자의 경우도 일부 배제시키게 되어, 이 경우 유효한 참여자의 경우 그룹관리자에게 재등록해야 하는 불편함이 따른다.

4. 분산형 Flat 키 관리

중앙 집중형 방식에서의 주요한 문제점은 집중된 키 관리요소의 고장으로 인해 시스템 전체에 대한 내부 붕괴의 위험성이 존재한다는 것이다.[3,4] 키 관리 문제를 해결하기 위하여 분산된 방안을 찾는다면 이러한 문제점을 극복할 수 있어 매우 매력적인 일이 된다. 이 해결방안으로 중앙 집중형 Flat 키 관리방안의 키 데이터베이스를 완전히 분산하는 방법으로서 모든 가입은 동등하게 발생되며, 완전한 정보를 갖고 있는 사람은 아무도 없는 방안이 된다. 중앙 집중형 Flat 키 관리방안에서와 마찬가지로 각 가입자는 자신의 ID와 부합되는 키만을 갖고 있으며, 다수 참여자에 의한 공동작업을 하는 경우에는 전 그룹에 대한 키 변경을 요구하게 된다. 전용 그룹관리자는 없으며 대신 각 참여자가 가입제어 동작을 수행할 수 있는 방안이다.[4]

사용되는 ID에 관한 정보를 알고 있는 그룹 관리자는 없으므로, ID는 저마다 유일하게 발생되어져야 한다. 가장 분명한 방법은 각 가입자의 네트워 번지를 사용하거나 충돌이 발생하지 않는 해쉬 함수를 적용하는 것이다.

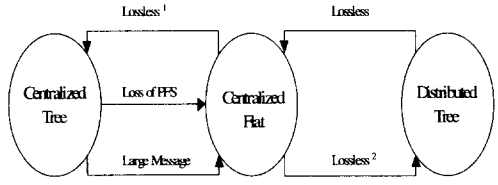
이 기법은 자가 치료 능력이 있으므로 네트워이나 노드의 절단에 대해 가장 탄력 있으나, 내부 공격자에 대해서는 다른 방법보다 더 취약하다.

◇ 최초 참여(First Participant): 그룹에 최초 참여하는 사람은 중앙 집중형 Flat키 관리방안에서 그룹관리자로부터 수신했던 키들(TEK와 W개의 KEK)을 스스로 발생하기 시작한다. 그리고, 스스로 시작신호를 전파하기 시작하며 이 시작신호를 통하여 자신이 지금 발생한 키의 소유자임을 알린다. 이 신호에는 각 키에 대한 버전, 개정번호 및 생성자 번지가 포함되어 있다.

◇ 가입(Join): 초기 가입 이후 새로 가입하는 경우에는 네트워으로부터 이 시작신호를 듣게 되어 앞서 참여한 참여자의 정보를 선택하면 된다. 이 소개자(Introducer)는 새로운 가자에게 둘이 공유할 수 있는 키를 보낸다. 이 정보에는 TEK와 적절한 KEK 및 증가된 개정번호가 포함되어 있다. 새로 가입하는 사람에게는 필요하지만 아직 존재하지 않은 KEK는 초기 동작을 통해 생성된다. ID가 네트워 번지를 통해 계산되므로 참여자들은 나머지 키를 쉽게 찾을 수 있다.

◇ 탈퇴(Leave): 탈퇴 동작은 중앙 집중 flat키 관리방안과 유사하다. 이 탈퇴자는 버전번호가 증가된 키들을 알 수 없으므로 변경된 키에 대한 현재의 키 소유자는 버전번호를 증가하고 키를 중계하면 된다.

5. 키 관리 기술 사이의 변환(Transitions)



[1] No security gain for old participants: Colluding old participants still cannot be expelled, participants joining after transition can.
[2] Previous Group Manager still knows all keys and thus cannot be expelled.

〔그림 7〕 키 관리 기술 사이의 변환

세 가지 기법은 긴밀하게 관련되어 있다. 그러므로 동작 중에 이 기법들 사이에서의 변환이 생길 가능성을 탐구해 보는 것은 가치가 있다. 가능한 모든 변환과정은 〔그림 7〕에 보이고 있다.[4]

두 개의 Flat 기법 사이에서 변환은 같은 데이터 구조를 사용하고 있으므로 단순하다. 중

앙 집중형 Flat방안을 향한 변환은 새로 그룹 관리자를 지정하고 모든 키를 전달해 주면 된다. 다른 방향으로는 현재 존재하는 그룹관리자를 포기한 후에 수행되어질 수 있다. 이들을 위한 유일한 요구사항으로 각 참여자는 액세스 제어 기능을 수행할 수 있거나 이를 행하는 과정에서 다른 참여자를 신뢰할 수 있어야 한다.

이러한 변환은 두 개의 기법이 갖고 있는 장점을 쉽게 구현할 수 있어 매우 좋은 방법이 된다. 중앙 집중형 Flat방안은 그룹관리자가 과부하 상태이거나 기능 장애의 상태가 아니면 모든 참여자들의 기능을 단순화 할 수 있는 경우에 언제든지 사용된다.

두 개의 중앙 집중형 방안 사이에서의 변환은 키 구조의 변화를 포함시켜야 하므로 복잡해진다. 계층구조는 flat 테이블로부터 생성되며 이 계층구조로부터 얻어진 키들은 그룹관리자가 갖고 있는 트리 데이터 구조로 이동시키는데 이용된다.

중앙 집중형 트리에서 중앙 집중형 Flat으로의 변환은 더 어려우며, 그룹관리자가 갖고 있는 keying material 발생기의 내부 설계에 따라 달라진다. 만일 keying material이 완벽 전방보호기능을 보증하도록 설계되었으면 변환 기능에는 기본적으로 각 참여자에게 새로운 keying material을 이동하고 있다는 사실을 통지하는 기능을 포함하여야 한다. 그러나 전방보호의 일부 기능만 구현되어 있다면 다른 발생과정을 사용할 수도 있다.

6. 키 관리 기술 비교분석

이 중앙 집중형과 분산형 구조의 동작은 O(log N) 이하의 복잡도를 갖고 있어 성능이 양호한 편이며, 제3자의 신뢰가 필요 없고, 인증과 프라이버시를 만족하는 등, 비교적 안전하게 동작한다고 볼 수 있다. 그러나, 자원 활용 및 배분, 네트워 부하, 동작의 효율성 및 보안 측면 등에서 개선해야 될 점이 많이 있을 것으로 여겨지며, 멀티캐스트의 발전추세를 고려할 때, 개선된 키 관리 기술이 향후 지속적으로 제안되리라 여겨진다. 세 가지 키 관리 기술의 특성을 비교·분석하여 〈표1〉에 정리하였다.

VI. 결 론

멀티캐스트 키 관리 구조는 1996년 Spanning 트리 구조에서 출발하여, 현재는 크게 중앙 집중형과 분산형으로 구분된다. 본 논문에서는 멀티캐스트 정보보호에서의 키 관리

〈표1〉 키 관리 기술별 특성 비교

특 성	중앙 집중형tree	중앙 집중형flat	분산형flat
그룹 기반 프라이버시 및 인증	YES	YES	YES
완전한 전방보호 가능	YES	YES	YES
동적인 가입과 탈퇴 가능	YES	YES	YES
제3자의 신뢰성 요구	NO	NO	NO
중앙 제어기능 요구	YES	YES	NO
제어 엔터티가 모든 참여자를 알아야함	YES	NO	NO
다수 탈퇴	YES	DIFF	DIFF
참여자의 결탁을 배제	YES	DIFF	DIFF
그룹들의 결합과 분리	EASY	YES	YES
동작 중 궤환 채널의 필요성	NO	NO	YES
IDs 혹은 네트웍 ID 할당	BOTH	BOTH	NET
한지점에서의 고장 시 심각성	YES	YES	NO
복구하는 정도	NO	YES	YES
작은 데이터베이스	NO	YES	YES
다수의 참가자 가입/탈퇴	NO	NO	YES

와 관련된 정보보호 구성요소와 키 관리 기술을 분석하였다. 멀티캐스트 키 관리 기술의 핵심은 서로 다른 속성을 갖고 있으나 동일한 기본 개념에서 출발하고 있다. 본 논문에서 소개한 키 관리 기술은 그룹 멤버들이 실제로 키를 필요로 하기 이전에 키를 발생하지 않은 상태에서 유일한 방법으로 키를 할당할 수 있는 키 스페이스를 구성하는 것이다. 새로운 그룹키를 정할 필요가 있는 경우에만 그 변화에 영향을 받는 그룹멤버에게만 국한해서 키를 생성하고 배부하는 것이다.

이 세 가지 기술은 몇 가지 중요한 관점에서 서로 다르다. 그 밖의 사항에 대해서는 다음 사항을 고려하여 설계자가 선택해야 한다.

◇ 키 관리의 중앙 집중 또는 분산
◇ 다른 참여자의 신뢰도 여부
◇ 참여자마다의 부하의 변화정도
◇ 그룹에 대한 밀접한 제어 혹은 분산 동작에 대한 안전장치

현재 선진국에서는 안전한 멀티캐스트 통신을 지원하기 위한 키 관리 기술의 초기 시제품이 구현되어 동작 중에 있지만, 대규모이며 분산된 그룹에게 적용된 실험은 아직 없다. 결국은 소프트웨어 시제품을 현재 이용 가능한 플랫폼에 SKIP이나 ISAKMP/Oakley에서처럼 운영할 계획을 갖고 있다. 특히, 중앙 집중형과 분산형 Flat에서의 데이터 구조 사이에서의 효율적인 변환 알고리즘을 개발하고 분석할 필요가 있다. 앞으로 이러한 방법을 통해 본 논문에서 분석한 키 관리 기술들의 성능을 이론적으로 분석하여 확인하고, 실험적으로 구성하여 동작을 통하여 개선사항을 도출하여야 하리라 본다.

참고문헌

[1] T. Maufer, C. Semeria, Introductio Multicast Routing, IETF draft-ietf-m -intro-multicast-02.txt, Mar. 1997.

[2] Pekka Pessi, Secure Multicast, 110.501 Seminar on Network Security,

[3] P.S Kruus, A Survey of Multicast Security Issues and Architecture, NISSC98, 1998.

[4] G. Caronni, M. Waldvogel, D. S Plattner, Efficient Security for larg Dynamic Multicast Groups, WETICE98

[5] S. Mittra, Iolus: A framework for s secure multicasting, In Proceedings o SIGCOMM '97, pages 277-288, Sept 1997.

[6] S. Kent and R. Atkinson, Se Architecture for the Internet Protoco 2401, Obsoletes 1825, November 1998.

[7] Ashar Aziz, T. Markson, Prafullchandra, Simple Key-Manageme Internet Protocols(SKIP), IETF dra ipsec-skip-03.txt, Oct. 1995.

[8] H. Harney, C. Muckenhirn, Grou Management Protocol(GKMP) Archit IETF RFC 2094, 1997.

[9] A. Ballardie, Scalable Multicast Key Distribution, RFC1949, May 1996.

著者紹介 ----------

김대호

1977년 한양대학교 전자공학과 학사
1984년 한양대학교 산업대학원 전자공학과 석사
1993년 Univ. of Maryland at Collage Park 방문 연구원
Dept. of Computer Science Visiting Scholar
1995년 전기통신 기술사, 정보통신 기술사
1977년 ~ 현재 한국전자통신연구원 책임연구원

※관심분야 : 전송분야, 통신 및 컴퓨터 보안

박웅기

1986년 중앙대학교 전자계산학과 학사
1988년 중앙대학교 대학원 전자계산학과 석사
1999년 아주대학교 대학원 컴퓨터공학과 박사과정 수료
1988년 ~ 현재 한국전자통신연구원 선임연구원

※관심분야 : 네트워크정보보호, 컴퓨터정보보호

김영수

1986년 한남대학교 전자계산공학과 학사
1990년 한남대학교 대학원 수학과 석사
1999년 한남대학교 대학원 컴퓨터 공학과 박사과정 수료
1986년 ~현재 한국전자통신연구원 선임연구원

※관심분야 : 네트워크정보보호, 컴퓨터정보보호