이동 환경에서의 보안 멀티캐스트에 대한 연구†

구자범*, 박세현*

*중앙대학교 전자전기공학부

A Study on Secure Multicast for Mobile Environment

Ja Beom Gu*, Se Hyun Park*

*School of Electronics and Electrical Engineering, Chung-Ang University

요 약

본 논문에서는 이동환경에서 다수의 이동 단말을 대상으로 안전하고 효율적인 멀티캐스트를 실현하는 보안 이동 멀티캐스트 서비스의 특성을 알아보기 위해서 기존의 연구를 보안 이동 멀티캐스트에 적용했을 때 나타나는 문제점들에 대해 논의했다. 기존의 연구는 이동 멀티캐스트나 보안 멀티캐스트에 초점을 맞추고 있어서, 이러한 연구 결과를 보안 이동 멀티캐스트에 그대로 적용할 경우 새로운 문제점이 발생하거나, 서비스의 성능을 저하시키는 요인으로 작용하게 된다. 이러한 문제점을 해소하기 위한 방안으로 적응적 방식의 가능성에 대해서 논의한다.

I. 서론

최근 급증하고 있는 이동 환경에서의 멀티미디어 서비스에 힘입어 이동 환경에서 멀티캐스트를 이용한 다양한 서비스에 대한 요구도 증가할 것으로 보인다. 따라서, 멀티캐스트 서비스는 이제 네트워크 자원 낭비를 최소화하여 효율성을 높이고자 하는 본래의 목적을 뿐만 아니라 다양한 이동 환경의 QoS 요구를 보장할 수 있어야 한다. 특히, 유선망에서 이루어지고 있는 증권정보, 원격 회의, 유료 멀티미디어 서비스 등은 그 활용 무대가 이동통신 환경으로 옮겨가고 있어 이동 멀티캐스트에서 요구되는 보안 QoS도 서비스되는 어플리케이션의 종류와 형태에 따라 매우 다양하고 복잡해질 수밖에 없다. 따라서, 본 논문에서는 이동 환경에서 하나의 서버로부터 다수의 사용자에게 멀티캐스트 서비스를 제공하는 경우에 발생할 수 있는 문제점과 이러한 문제점을 해결하고 보안 QoS를 향상하기 위한 방안에 대해 논의한다.

이동 환경에서 하나의 멀티캐스트 소스 (multicast source)가 다수의 사용자 (multicast subscriber)에게 보안 서비스를 제공하는 예로 증권 시세를 정보 전송을 들 수 있다. 이 경우에 그룹의 관리자 (group controller)인 증권 정보 서버로부터 데이터가 전송이 되고, 사용자는 네트워크 상에서 이동을 하면서 데이터를 수신하게 된다. 많은 양의 데이터가 실시간으로 많은 수의 사용자에게 전송이 되어야 하므로 확장성이 있어야 한다. 또한 데이터는 그룹 관리자가 전자서명을 첨부하고, 암호화하여 전송할 필요가 있다. 본 논문은 이러한 보안 요구 사항을 만족시키기 위한 프레임워크를 구성함에 있어 고려해야 할 문제점들에 대해 논의하는 것을 목표로 한다.

다수의 그룹 멤버에게 암호화된 데이터를 전송하는 경우에는 키 관리의 효율성이 매우 중요한 문제로 작용한다. 특히 그룹의 크기가 크고, 키 관리 빈도가 증가하는 경우에는 키 관리가 전체 시스템과 네트워크의 성능에 미치는 영향으로 인해서 서비스가 불가능 해 질 수도 있게 된다. 서비스가 '완벽한 보안'(perfect secrecy, 2.1절에서 설명)을 제공해야 하는 경우에는 서비스를 받고자 하는 등록된 그룹 멤버만 데이터를 수신할 수 있어야 하기 때문에 키 관리의 중요성이 더욱 커지게 된다.

본 논문에서는 이동 환경에서의 보안 멀티캐스트에 초점을 맞추고, 보안 QoS를 향상시키기 위한 방안을 논의한다. 이동 보안 멀티캐스트에서 요구되는 보안 QoS는 전송 지연 (delay)을 최소화하고 이동 중인 멤버에게 전송되는 패킷의 손실을 최소화하는 것을 포함하여, 추가된 보안 기능 (키 관리, 암호화 등)으로 인해 멀티캐스트 서비스에 관여하는 그룹 멤버나 네트워크 노드의 부담을 최소화하는 등의 요구사항을 포함한다.

본 논문의 구성은 다음과 같다. 2장에서는 보안 멀티캐스트와 이동 멀티캐스트로 구분하여 관련된 분야의 연구를 소개한다. 3장에서는 이동 환경에서 보안 멀티캐스트 제공할 때 발생하는 문제점과 해결 방안에 대해 논의하고, 4장에서 결론을 맺는다.

† 본 논문은 한국과학재단 목적기초 (R01-2001-00303) 지원으로 수행되었음.

II. 보안 멀티캐스트와 이동 멀티캐스트

보안 멀티캐스트와 이동 멀티캐스트에 대한 연구 노력은 오랜 기간동안 많은 관심을 끌어오던 분야이다. 따라서 이동성과 보안성을 동시에 제공할 때 발생하는 문제점에 대해 논의하기에 앞서 각각의 분야에서 선행된 연구에 대해 살펴보도록 한다.

1. 보안 멀티캐스트

멀티캐스트 보안을 위해서 많은 연구가 계속되고 있는데([2~5]), 궁극적인 목표는 완벽한 보안(perfect secrecy)을 제공하는데 있다고 할 수 있다. 이것은 "backward and forward secrecy"로 표현되기도 하는데, 그룹에 가입된 사용자만이 데이터를 받아볼 수 있어야 한다는 것이다. 즉, 그룹 서비스에 참여(join)하도록 인가되지 않은 멤버는 서비스에 참여하기 이전에 전송된 데이터의 내용을 볼 수 없어야 하고 (backward secrecy), 탈퇴(leave)한 멤버의 경우에도 이후에 전송되는 데이터의 내용을 볼 수 없어야 한다(forward secrecy)는 의미이다. 따라서 이러한 완벽한 보안을 제공하기 위해서는 그룹 키를 이용하여 멀티캐스트 데이터를 암호화 한 후 전송하고, 서비스에 참여하거나 탈퇴하는 멤버가 발생할 경우에는 그룹 키를 갱신(update)한 후에 갱신된 키로 암호화해서 전송해야 한다. 그룹 관리자가 키를 생성해서 전달하는 경우에는 각 멤버들에게 유니캐스트(unicast)를 통해서 전달할 경우에는 확장성이 매우 떨어지게 된다. 즉, 멀티캐스트의 그룹 특성상 멤버의 참여와 탈퇴가 빈번한 경우에는 그룹 키를 생성하고, 멤버들에게 전달하는 과정이 그룹 관리자와 그룹 멤버 그리고 서비스에 관여하는 네트워크 노드들 모두에 많은 영향을 미치게 되므로, 효율성과 확장성 (scalability)을 보장하기 위한 방안이 필요하다.

멀티캐스트 보안을 위해서 키 관리 효율성을 높이기 위한 많은 연구들이 계속되었는데, key graph[3]와 Iolus[4]가 대표적인 예이다. Key graph는 그룹 키를 분배하는데 있어 다수의 키를 사용하여 효율성을 높이는 방식이다. 즉, 계층 구조가 되도록 다수의 키를 생성하여 멤버들에게 전달해 주는 방식으로 하나의 멤버가 관리하는 키의 수는 비록 증가하더라도, 키 갱신을 위한 비용(키의 생성과 전달 측면에서)을 줄일 수 있는 방안이다. 이 방안은 암호화 비용을 대수적으로 줄여주는 한편, 한번의 브로드캐스트에 의해서 키 갱신이 가능하므로 네트워크 자원을 효율적으로 사용할 수 있다.

그러나, 중앙 집중적인 키 관리 방법은 여전히 많은 문제점을 안고 있다. 첫째는 '1 affects n'[4] 이란 말로 잘 설명될 수 있다. 즉, 전술한 바와 같이 한 멤버가 서비스에 참여하거나 탈퇴하는 경우 그룹 키를 갱신해야 하므로, 한 멤버가 나머지 모든 멤버에게 영향을 미친다는 의미이고, 이것은 확장성이 떨어지는 결과를 가져올 수밖에 없다. 키 갱신 회수가 잦아질 수록 효율성이 떨어지고, 키 갱신 메시지가 각 멤버들에게 정확히 전달되지 않을 확률이 커지게 된다. 둘째로, 키 갱신의 비일관성 문제가 발생한다. 과다한 트래픽이나 네트워크 장비의 이상으로 인하여 하나의 송신자로부터의 데이터 패킷은 넓은 지역에 분산되어 있는 다수의 수신자에게 같은 시간에 전송될 수 없다. 이러한 특성 때문에 키 갱신 메시지를 전달하는 경우에 어떤 멤버들은 다른 멤버들보다 먼저 이 메시지를 수신하거나 어떤 멤버들은 이 키 갱신 메시지를 놓칠 수 있게 된다. 따라서 키 갱신 메시지를 늦게 받은 멤버들은 일정기간 멀티캐스트 서비스를 받지 못하는 문제 등이 발생할 수 있다. 이와 같은 문제를 해결하기 위하여 분산구조 형태로 키를 관리하는 방법이 대두하게 되었다. Iolus[4]는 분산구조의 대표적인 예로 볼 수 있다. 즉, 하나의 멀티캐스트 그룹을 여러 개의 서브그룹 (subgroup)으로 나누고, 서브그룹에 관리자와 서브그룹용 키를 따로 두는 방안이다. 이 경우에 멤버가 서비스에 참여하거나 탈퇴하는 것은 비교적 크기가 적은 서브그룹에서만 키 갱신을 필요로 하므로 전체 그룹에 영향을 미치지 않아 확장성을 높이게 된다. 그러나, 이동 환경에서 분산구조를 적용하는 경우에는 또 다른 문제가 발생한다. 이 점에 대해서는 3 장에서 자세히 다루도록 한다.

키 관리의 효율성을 높이기 위한 또 다른 연구는 Kronos [11]에서 보여지는 주기적인 처리 방식이다. 이것을 일괄처리 (batch processing) 방식으로 표현하고 있는데, 서비스 참여나 탈퇴가 발생하여 키 갱신이 요구되는 경우에 이것을 즉시 처리하지 않고, 일정기간동안 모아서 처리하는 방식이다. 따라서, 주기적으로 키 갱신이 이루어지게 되고, 주기를 늘릴수록 키 갱신 빈도가 줄어들게 된다. 3장에서는 이동환경에서 이러한 일괄처리 방식을 적용할 경우의 문제점에 대해서도 다룬다.

2. 이동 멀티캐스트

이동 환경에서 멀티캐스트를 구현하려는 노력은 여러 각도로 이루어지고 있다[6~9]. 그 중 하나가 Mobile IP[9] 상에서 멀티캐스트를 구현하는 것이다. Mobile IP에서는 두 가지 방식의 멀티캐스트 프로토콜을 제안하고 있는데, remote subscription과 bi-directional tunneling이 그것이다. [7]에는 이 두 가지 방식의 장·단점에 대해 다음과 같이 기술하고 있다.

Remote subscription 방식은 이동 노드가 Foreign network로 이동했을 경우 자신이 위치한 곳(Foreign network)에서 멀티캐스트 서비스를

받는 방법이다. 이 방법의 가장 큰 장점은 멀티캐스트 데이터의 전송경로가 이상적이라는 것이다. 따라서, 최소화된 전송 지연이 보장된다. 하지만 이 경우에는 이동 노드가 다른 네트워크로 이동해서 foreign network으로부터 서비스를 받기까지의 지연이 있을 경우 패킷이 손실된다는 단점이 있다. 보안 기능이 추가된 경우에는 지연이 증가하므로 패킷 손실의 확률도 커지게 된다.

Bi-directional tunneling이라고 불리 우는 방법으로 HA가 이동 단말이 현재 위치한 위치로 터널링을 통한 유니캐스트로 멀티캐스트를 지원하는 방법이다. 그러나 이 방법의 가장 큰 단점은 멀티캐스트 경로가 매우 길어질 수 있다는 점이다. 또한, HA는 자신이 멀티캐스트 서비스를 해주고 있는 이동 단말이 같은 Foreign network에 위치하고 있더라도, 각각 하나씩의 중복된 멀티캐스트 데이터를 보낼 수 있다. 따라서, 네트워크 자원의 낭비를 초래하게 된다. MoM protocol[6]에서는 이 문제를 해결하기 위하여 DMSP (Designated Multicast Service Provider)란 개념을 도입해 오직 하나의 tunnel로부터 멀티캐스트 데이터를 받는 것을 제안했다. 그러나 보안 이동 멀티캐스트에서는 각각의 이 방법을 사용할 수 없는데, 이에 대해서는 3장에서 다룬다.

[7]에서는 이 두 가지 모드를 거리에 따라서 조합해 사용함으로써 전송지연을 최소화하는 방안을 제안하였는데, bi-directional tunneling 방식을 기본으로 하여 서비스를 하다가 노드가 홈으로부터 특정 거리이상으로 멀어지는 경우에 remote sub- scription을 사용하는 방안이다. 그러나, 멀티미디어 유료 시청이나 실시간 증권 정보의 경우처럼 이동 단말이 수신자 입장에서 보안멀티캐스트 서비스를 받는 경우 전송 지연뿐만 아니라 보안 멀티캐스트 서비스 제공 시 이동중인 단말 서비스 영역간을 이동할 때 발생하는 데이터 손실을 최소화 할 수 있어야 한다. 이 문제에 대해서는 3장에서 멀티캐스트에 이동성과 보안성을 동시에 제공하고자 할 때 발생하는 문제점을 논의하면서 자세히 다룬다.

III. 보안 이동 멀티캐스트

본 절에서는 보안 이동 멀티캐스트 서비스를 위해서 기존에 이동 멀티캐스트와 보안 멀티캐스트를 위해서 제시된 방안을 적용할 경우에 발생하는 문제점과 이것을 해결하기 위한 방안에 대해 논의한다.

1. 보안 이동 멀티캐스트 구조

이동 환경에서 보안 멀티캐스트를 적용할 때 발생하는 문제점을 알아보기 위해서 멀티캐스트 네트워크 구조를 다음과 같이 설정하였다 (그림 1). 우선, 서비스의 확장성을 높이기 위해서 Iolus와 같은 분산구조 갖는다. 즉, 일정한 범위로 서비스 영역을 나누고 각 서비스 영역별로 서비스 영역키를 갖는다. 이 서비스 영역키는 해당 영역에서 서비스 받는 이동 노드로 데이터를 암호화하여 전송해 줄 때 사용된다. 각 서비스 영역에는 서비스 영역키를 관리하고 이동단말에게 멀티캐스트 서비스를 제공하는 MSA (Multicast Service Agent)가 위치한다. 또한 중앙에는 멀티캐스트 서비스를 총괄하고 멀티캐스트 서비스의 소스인 MGC (Multicast Group Controller)가 위치한다. MGC로부터 각 멤버들에게 멀티캐스트 패킷이 전달되기 위해서 MGC와 MSA들로 구성된 보안멀티캐스트 경로가 형성된다. (본 논문에서는 라우팅 경로 생성에 대해서는 다루지 않지만, MGC에서 MSA까지의 경로는 항상 최적화되어 있다고 가정한다.) MGC에서 각 MSA까지 패킷이 안전하게 전달되기 위해서 MGC와 MSA들은 하나의 비밀키(secrete key)를 공유하게 되고, 멀티캐스트 패킷은 이 비밀키로 암호화되어 MGC와 MSA들 사이에 형성된 멀티캐스트 경로를 통해 전송된다. 각 MSA는 전달받은 멀티캐스트 패킷을 복호화 한 후에 다시 각각의 서비스 영역키로 암호화되어 이동 단말에게 전달된다. 서비스 영역 내에서 이동 노드가 서비스에 참여하거나 탈퇴할 때 키 갱신은 key graph 방식과 일괄처리 (batch process) 방식을 함께 사용한다.

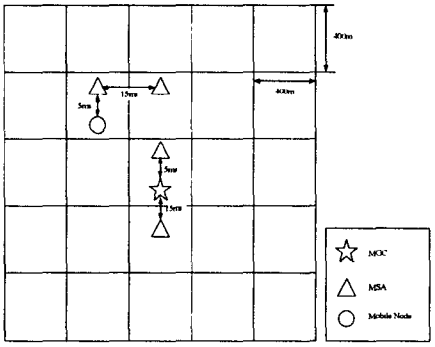

그림 1: 보안 이동 멀티캐스트 구조.

2. 서비스 모드

본 절에서는 Mobile IP에서 제시된 이동 멀티캐스트 서비스 방안을 수정하여 두 가지 형태로 보안 이동 멀티캐스트 서비스를 설정하고, 각 서비스가 갖는 장·단점을 알아본다.

1) Direct mode

Direct mode는 Mobile IP[9]의 remote subscription 방식과 유사한데, 이동 노드가 현재 위치한 서브그룹으로부터 서비스를 제공받는 방식이다. 따라서 이동 노드가 다른 지역으로 이동하는 경우에는 다시 등록과정을 수행하고 지역 키를 제공받아야 계속적인 서비스가 가능하다. 그룹 관리자 (MGC)로부터 서브그룹 관리자인 MSA까지의 멀티캐스트 경로는 최적화 되어 있다고 가

정하였으므로, 이동 노드까지의 경로도 항상 최적화 되어 있다고 할 수 있다. 그림 2는 이 서비스 모드를 나타내고 있다. 그림 2에서 이동 노드인 a_1은 최초에 A 지역에 위치해 있으므로 A 지역에서 서비스를 받는다. B 지역으로 이동하는 경우에 a_1은 B 지역의 MSA로부터 서비스를 제공받는다. a_1이 다시 다른 지역으로 이동하는 경우에는 이 과정이 반복된다. 그러나, 노드의 이동뿐만 아니라 보안성까지 고려한 다면 direct mode는 다음과 같은 문제점을 갖고 있다. 첫째, 이동 노드가 새로운 지역으로 이동하여 재등록 과정을 수행해야 하므로, 노드는 즉시 서비스를 받지 못하게 되어 패킷 손실이 증가하게 된다. 즉, 패킷 손실은 재등록 과정이 길수록, 그리고 이동이 빈번할수록 커지게 된다. 둘째, 서브그룹에서 키 갱신 횟수가 증가하게 된다. 본래 멤버가 서비스에 참여하고 탈퇴할 때 키 갱신이 요구되었지만, 서브그룹으로 나누어져 있는 경우에는 멤버의 이동에 의해서도 키 갱신이 요구되게 된다. 따라서, 멤버의 이동이 잦을 수 록 키 갱신 횟수가 증가하게 되고, 서비스 질 저하의 요인이 된다. 셋째, 노드의 이동으로 인해서 패킷 시퀀스 불일치 현상이 발생하게 된다. 패킷 시퀀스 불일치는 서브그룹간에 패킷 시퀀스가 동일하지 않은 현상을 말하는데, 병목 현상 등 네트워크의 특성에 따라서 패킷 시퀀스가 다른 서브그룹보다 늦어질 수 있기 때문에 생기는 현상으로, 고정망에서는 전혀 문제가 되지 않는 부분이지만 이동 환경에서는 패킷 손실을 유발하게 된다. 그림 3에서 한 예를 보이고 있는데, 이동 노드 a가 A 지역에서 B 지역으로 이동하는 경우를 보이고 있다. 이때 A 지역에서는 4, 5, 6번 패킷이 전송되고 있고, B 지역에서는 7, 8, 9번 패킷이 전송되고 있다. 이 경우에 B 지역으로 이동한 노드는 중간 패킷을 받지 못하게 된다. 이것은 물론 패킷의 전송 특성에 따라서 달라지기는 하지만, 이동 환경에서는 불가피한 현상이고, 이동 노드의 속도에 따라서 그 특성이 두드러지게 나타나게 된다.

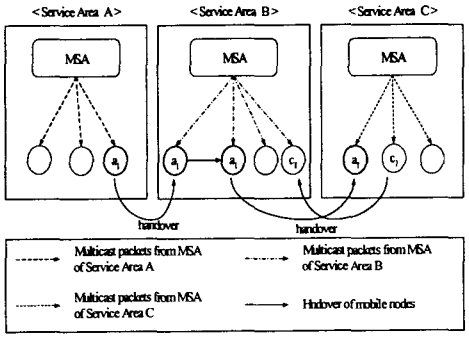

그림 2: Direct mode

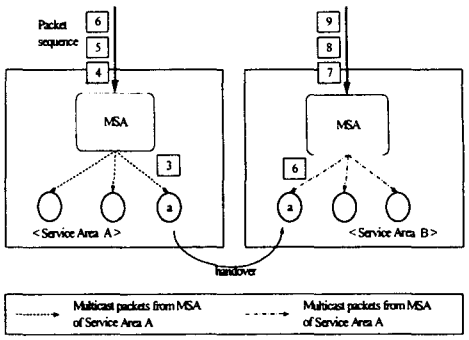

그림 3: Direct mode에서 발생하는 패킷 시퀀스 불일치

2) Indirect mode

Indirect mode는 Mobile IP의 bi-directional subscription과 유사한 방식으로 (home agent의 역할을 MSA가 담당) 이동 노드가 최초로 서비스를 받기 시작한 위치의 MSA가 계속적인 서비스를 담당하게 된다(그림 4). 즉, 이동 노드가 다른 지역으로 이동하는 경우에도 재등록 과정을 거치지 않고 최초에 서비스 받던 곳으로부터 전달받는 방식이다. 따라서, 노드가 이동함에 따라서 발생하는 키 갱신이 전혀 없다는 장점이 있다. 그러나, 이 모드는 노드가 이동해 감에 따라서 라우팅 경로가 증가하는 단점이 있다.

또한, 이동 노드에게 끊김 없는 서비스를 제공하기 위해서 각 이동 노드마다 Indirect mode를 유니캐스트로 패킷을 전달하는 것은 매우 비효율적이다[6]. 그림 4에서 보이듯이 B 지역에 위치한 노드인 a1, c1, c2에게 서비스하기 위해서 C 지역과 A 지역의 MSA가 여러 개의 중복된 패킷을 보내는 것이 비효율 적이라는 것이다. MoM protocol[6]에서는 이 문제를 해결하기 위하여 DMSP (Designated Multicast Service Provider)란 개념을 도입해 오직 하나의 B의 MSA가 중복된 패킷 중 하나만을 택하는 방식을 제안하였다. 그러나 보안 이동 멀티캐스트에서는 각각의 Indirect mode를 제공하는 패킷을 암호화한 키가 다르기 때문에 [6]과 같은 방법을 사용할 수는 없다.

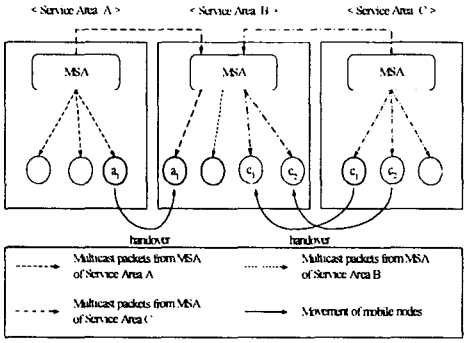

그림 4: Indirect mode

3. 키 관리와 패킷 손실

앞 절에서 논의된 서비스 모드의 장·단점을 종합하여 다음과 같이 패킷 손실 형태를 세 가지로 분류해 볼 수 있다. 그림 5는 이 세 가지 패킷 손실 형태를 키 갱신 빈도에 따라 나타낸 것이다.

● **Case 1**: 첫 번째 경우는 잦은 키 갱신에 의한 패킷 손실이다. 보안 이동 멀티캐스트에서 키 갱신은 서비스에 참여 또는 탈퇴뿐만 아니라 노드의 이동에 의해서도 발생하므로 키 갱신 빈도는 매우 증가하게 된다 (키 갱신 주기가 감소). 따라서, 증가한 키 갱신 빈도에 의해서 네트워크와 이동 노드에 가해지는 부담이 증가하고, 그래프에 나타난 것처럼 패킷 손실이 급격히 증가하게 된다. 키 갱신 빈도를 줄이기 위해서 전체 그룹을 서브그룹으로 나눈 것이 본래의 목적이었는데, 노드가 갖는 이동성 때문에 오히려 성능이 저해되는 결과를 가져오는 경우라고 할 수 있다. 또한 키 갱신의 빈도를 줄이기 위해서 Kronos[11]에서 제시된 일괄처리 방식을 이용할 수도 있지만, 이것은 또 다른 형태의 패킷 손실을 가져온다. 이것은 그림 5에서 Case 2로 표현되어 있다.

● **Case 2**: 두 번째 경우는 키 갱신의 지연에서 오는 손실이다. 노드가 새로운 지역으로 이동하는 경우에 서비스를 지속하기 위해서 재등록을 하여 새로운 서브그룹 키를 부여받아야 하는데, 이 재등록이 완료될 때까지 노드는 서비스를 받지 못하고 패킷 손실이 발생하게 된다. 등록에 걸리는 시간이 증가하면 증가할수록 패킷 손실도 증가하는 형태를 보인다. Kronos[11]에서 제안된 일괄처리 방식은 상황을 더욱 악화시키는 결과를 가져온다. 본래 Kronos에서 제안된 방안은 노드의 이동성을 전혀 고려하지 않고, 오직 서비스에 참여하고 탈퇴하는 경우만을 대상으로 하였기 때문에, 이것을 이동 환경에 그대로 적용하기에 적합하지 않은 상황이 발생하는 것이다.

● **Case 3**: 세 번째 경우는 각 서브그룹 간에 패킷 시퀀스 불일치에 의해 발생하는 손실이다. 이것은 그림 5에서 그래프의 전체적인 높이를 결정하는 요소로 표현되어 있다. 이것은 네트워크의 특성과 밀접한 관련이 있기 때문에 서비스에 지속적인 영향을 미치게 되기 때문이다.

이러한 문제점들을 종합해 볼 때 보안 이동 멀티캐스트의 QoS 요구사항을 다음과 같이 요약할 수 있다. 즉,

● 전송 지연 문제를 최소화

● 이동에 의한 패킷 손실 최소화

● 키 갱신 빈도를 적절한 수준으로 유지하면서도, 패킷 손실을 최소화

● 이동 노드로 전달되는 패킷 중복 최소화

본 연구는[1, 14]에서 연구된 내용을 기반으로 하여 진행되고 있는데, [14]에서는 이러한 요구사항을 해결하기 위해서 direct mode와 indirect mode를 적응적으로 적용하는 방안에 대해 연구되었다. 본 연구의 결과와 [14]의 연구를 종합한 연구가 계속 진행 중에 있다.

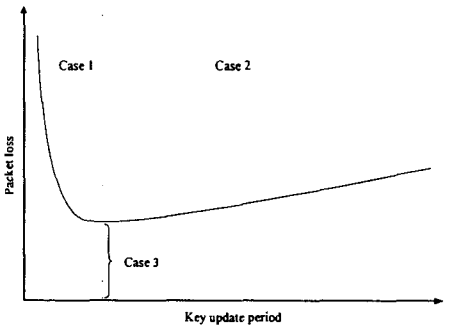

그림 5: 키 관리 빈도에 따른 3 가지 형태의 패킷 손실

IV. 결론

본 논문에서는 보안 이동 멀티캐스트 서비스의 특성을 알아보기 위해서 이동 멀티캐스트와 보안 멀티캐스트에 관련된 연구들을 살펴보았고, 이들을 보안 이동 멀티캐스트에 적용했을 때 나타나는 문제점들에 대해 논의했다. 이것을 통해서 보안 이동 멀티캐스트 서비스를 효율적으로 제공하기 위한 새로운 방안이 필요함을 알 수 있었다. 본 연구의 연장으로 direct mode와 indirect mode를 조합한 적응적 방식의 서비스에 대한 연구를 진행하고 있고, 이에 대한 시뮬레이션 방안을 모색중이다. 적응적 방식의 경우, 3장에서 제시되었던 전송지연 문제와 패킷 손실 최소화, 그리고 키 갱신 빈도의 영향을 최소화하는데 큰 장점이 있

을 것으로 기대된다.

참고문헌

[1] J.Y. Ahn, J.B. Gu and S.H. Park, "A Secure Mobile Multicast(SMM) Protocol for Effi- cient Key Management and Low Transmis- sion Delay", Five minute presentation, IEEE Symposium on the Security and Privacy, 2001.

[2] M.J. Moyer, J.R. Rao and P. Rohotgi, "A Survey of Security Issues in Multicast Communications", IEEE Network, Volume: 13 Issue: 6, Nov.-Dec. 1999.

[3] C.K. Wong, M. Gouda, S.S. Lam, "Secure Group Communication Using Key Graphs", Proc. of ACM SIGCOMM'98, pp.68-99, Sep. 1998.

[4] S. Mittra, "Iolus: A Framework for Scalable Secure Multicasting", Proc. of ACM SIGCOMM'97, pp.277-288, March 1997.

[5] R. Canetti, J. Garay, G. Itkis, D. Micciancio, M. Naor and B. Pinkas, "Multicast security: A Taxonomy and Some Efficient Construc- tions", Proc. of the IEEE INFOCOM'99, pp. 708-716, 1999.

[6] T.G. Harrison, C.L. Williamson, W.L. Mackrell, R.B. Bunt, "Mobile Multicast (MoM) Protocol: Multicast Support for Mobile Hosts", Proc. of ACM/IEEE MOBICOM'97, pp.151-160, Sep. 1997.

[7] C.R. Lin and K.M Wang, "Mobile Multicast Support in IP Networks", Proc. of the IEEE INFOCOM 2000, pp.1664-1672, March 2000.

[8] G. Xylomenons and G.C. Polyzos, "IP Multicast for Mobile Hosts", IEEE Commun. Mag., Jan. 1997.

[9] C. Perkins, "IP Mobility Support", RFC 2002, October 1996.

[10]C. E. Perkins, "Mobile IP", International Journal of Communication Systems, 1998.

[11] S. Setia, S. Koussih, S. Jajodia and E. Harder, "Kronos: A Scalable Group Re-Keying Approach for Secure Multicast", Proc. of Security and Privacy 2000, 2000.

[12] L.H. Sahasrabuddhe and B. Mukherjee, "Multicasting Routing: Algorithms and Pro- tocols: A Tutorial", IEEE Network, January/ February 2000.

[13] C. Perkins, "IP Encapsulation within IP", RFC 2003, October 1996.

[14] 안재영, 구자범, 이재일, 박세현, "적응적 서비스 모드에 기반한 이동보안멀티캐스트 구조 및 프로토콜에 관한 연구", 한국정보보호학회논문지, vol. 12, no. 2, 2002.