DOI: 10.3745/KIPSTC.2008.15-C.6.573

마이크로 모빌리티 환경에서 보안 그룹키를 이용한 안전한 멀티캐스트 프로토콜

강 호 석[†] · 심 영 철[††]

요 약

컴퓨터의 성능 향상과 소형화, 그리고 무선 통신 기술의 향상으로 인하여 많은 고품질 서비스들이 등장하고 있다. 그 중 화상회의, 동영상 스트림, 인터넷 TV 등의 인터넷 멀티미디어 서비스의 증가로 인하여 멀티캐스트 서비스가 많은 주목을 받고 있다. 또 이러한 모바일 멀티캐스트 서비스를 이용하는데 안전성은 매우 중요한 요소이다. 본 논문에서 계층적 마이크로 모빌리티 환경에서 안전한 멀티캐스트 프로토콜을 이용할 수 있는 보안 기능을 제안하였다. 안전한 멀티캐스트 프로토콜은 대칭키/비대칭키 암호화 알고리즘과 케이퍼빌리티를 이용하여 인증, 접근제어, 비밀성, 무결성 등의 보안 서비스를 제공한다. 순방향/역방향 비밀성과 확장성을 제공하기 위하여 계층적 마이크로 모빌리티 환경에 맞는 서브그룹키를 사용하였다. 이러한 보안기능은 불법적 모바일 노드에 의해 멀티캐스트 서비스에 수행되는 모든 유형의 공격을 방지할 수 있다. 그리고 내부의 불법 노드에 의한 공격의 경우 패킷 삭제와 네트워크 자원의 낭비를 유발하는 공격을 제외하고 모든 공격을 방지할 수 있다. 제안한 안전한 멀티캐스트 프로토콜의 성능을 시뮬레이션을 이용하여 측정하였고 결과로 보안 기능의 추가로 인한 부하가 크지 않다는 것을 보여줬다.

키워드 : 멀티캐스트, 마이크로 모빌리티, 핸드오프, 모바일 IP, 보안

A New Secure Multicast Protocol in Micro-Mobility Environments using Secure Group Key

Ho-Seok Kang[†] · Young-Chul Shim[††]

ABSTRACT

The improved performance and miniaturization of computer and the improvement of wireless communication technology have enabled the emergence of many high quality services. Among them multicast services are receiving much attention and their usage is increasing due to the increase of Internet multimedia services such as video conference, multimedia stream, internet TV, etc. Security plays an important role in mobile multicast services. In this paper, we proposed a secure multicast protocol for a hierarchical micro-mobility environment. The proposed secure multicast protocol provides security services such as authentication, access control, confidentiality and integrity using mechanisms including symmetric/asymmetric key crypto-algorithms and capabilities. To provide forward/backward secrecy and scalability, we used sub-group keys based on the hierarchical micro-mobility environment. With this security services, it is possible to guard against all kinds of security attacks performed by illegal mobile nodes. Attacks executed by internal nodes can be thwarted except those attacks which delete packet or cause network resources to be wasted. We used simulator to measure the performance of proposed protocol. As a result, the simulation showed that effect of these security mechanisms on the multicast protocol was not too high.

Keywords : Multicast, Micro-Mobility, Handoff, Mobile IP, Security

1. 서 론

컴퓨터의 성능 향상과 소형화, 그리고 무선 통신 기술의 향상으로 인해 고품질 서비스들이 등장하고 있다. 그 중 화상회의, 동영상 스트림, 인터넷 TV등의 인터넷 멀티미디어 서비스의 증가로 인하여 멀티캐스트 서비스가 많은 주목을 받고 있고 현재도 이용률이 증가하고 있다. 이런 서비스들은 모바일 기기의 성능 향상과 무선 이동 통신의 발전으로 인하여 모바일 환경에 적용시켜야 하는 필요성이 생겨나고 있다. 즉 무선 모바일 환경에서 멀티캐스트를 이용하여 멀티미디어 서비스를 제공하여야 한다. 더 나가서는 출장이나

※ 본 연구는 한국과학재단 특정기초연구(KRF-R01-2006-000-10073-0) 지원으로 수행되었음.
† 정 회 원 : 홍익대학교 컴퓨터공학과 공학박사
†† 종신회원 : 홍익대학교 컴퓨터공학과 교수
논문접수 : 2008년 9월 11일
수 정 일 : 1차 2008년 10월 22일
심사완료 : 2008년 10월 23일

외부 파견으로 인하여 이동 중에 비밀회의에 참석해야 하는 경우도 있을 것이다. 그러므로 안전한 모바일 환경을 구축하여 멀티캐스트 서비스를 이용한 멀티미디어 서비스에 대한 필요성이 증가하고 있다.

모바일 노드의 IP 서비스를 위하여 모바일 IP가 사용되지만 잦은 이동으로 인하여 홈 네트워크의 등록 부하가 크게 증가한다. 이를 줄이기 위하여 마이크로 모빌리티(Micro-mobility) 프로토콜과 계층적 마이크로 모빌리티 프로토콜이 제안되었다[1]. 또 계층적 마이크로 모빌리티 환경에 멀티캐스트 서비스를 추가하여 마이크로 모빌리티 환경에서의 멀티캐스트 프로토콜[2]을 만들었다.

그러나 마이크로 모빌리티 환경에서의 멀티캐스트 프로토콜[2]은 악의적인 사용자가 마음대로 데이터를 가로채고 변형시키고 트리 구성을 바꾸고 네트워크 부하를 줄 수 있다. 이러한 취약점은 데이터의 신뢰를 떨어뜨리고 기존 사업자가 과금 서비스를 하는데 방해가 될 수 있다. 그래서 모바일 환경에서의 안전한 멀티캐스트 프로토콜이 필요하게 된다. 그러나 기존의 유선네트워크에서의 멀티캐스트 방법은 모바일 환경에서 발생하는 핸드오프에 대한 대처를 적절하게 할 수 없다. 이러한 문제점을 해결하고자 본 논문에서는 계층적 마이크로 모빌리티 환경[1]에서의 멀티캐스트 프로토콜을[2,3]에 안전하게 이용할 수 있도록 보안 기능[4]을 추가한 구조와 프로토콜을 만들었다.

프로토콜 구성요소 중 권한부여서버(AS, Authorization Server)를 통하여 모든 노드의 케이퍼빌리티를 만들어서 접근제어를 수행하게 하였다. 송신자별로 별도의 키를 생성하여 그룹키와 서브그룹키로 암호화 하여 전송함으로써 비밀성을 유지하였다. 특히 멤버 노드의 가입과 탈퇴, 핸드오프가 발생하면 서브그룹키만을 교체하여 순방향/역방향 비밀성을 유지하게 하였다. 뿐만 아니라 모든 메시지나 제어신호에 자신의 개인키로 서명을 하여 멀티캐스트 그룹 멤버가 송신한 메시지인지를 검증하여 무결성을 만족시킨다. 이렇게 설계한 보안기능은 인증, 접근제어, 비밀성, 무결성 등을 만족시키고 서브그룹키를 이용한 구조를 통하여 확장성을 높였다. 또 불법적 모바일 노드에 의해 멀티캐스트 서비스에 수행되는 모든 유형의 공격을 방지할 수 있고 내부의 불법 노드에 의한 공격의 경우 패킷 삭제와 네트워크 자원의 낭비를 유발하는 공격을 제외하고 모든 공격을 방지할 수 있다.

제안한 프로토콜의 성능을 측정하기 위하여 ns2 시뮬레이터를 이용하였다. 성능을 측정하기 위하여 보안기능이 없는 프로토콜과 비교 실험하였다. 메시지 암호화와 키 분배로 인하여 멀티캐스트 트리에 얼마나 영향을 주는지를 패킷 전송시간을 이용하여 측정하였다. 시뮬레이션 결과 보안 기능의 추가로 인한 영향이 크지 않다는 것을 보인다.

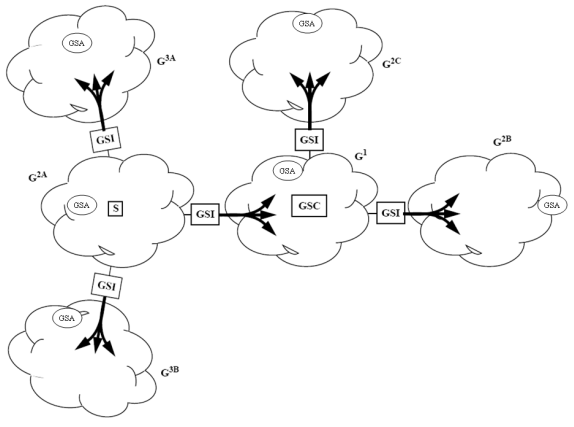
본 논문의 구성은 2장에서 관련연구를, 3장에서 안전한 멀티캐스트 프로토콜을 설명하기 위한 배경에 대하여 설명한 후 4장에서 안전한 멀티캐스트 프로토콜에 대하여 설명을 한다. 5장에서 설계한 프로토콜을 분석해보았고, 6장에서 제안한 프로토콜에 대한 성능을 측정 하였다. 마지막으로 7장에서 결론을 제시한다.

2. 관련연구

마이크로 모빌리티 환경에서의 안전한 멀티캐스트에 대하여 알아보기 위해서는 우선 안전한 멀티캐스트 방법에 대하여 알아야 한다. 이를 구현하기 위해서 여러 방법이 제시되었지만 그 목적은 어떻게 멀티캐스트 그룹 사용자에게 안전하게 암호화된 데이터를 전달하는가에 있다. 암호화된 데이터를 전달하는 방법으로 Enclaves[5], GKMP specfication[6], Sitinson방법[7], GKMP Architecture[8], 그리고 Bruschi방법[9]과 같은 다양한 방법이 제안되었다. 그러나 이 방법들은 멀티캐스트 가입자가 큰 그룹일 경우 잦은 키 교체로 인한 확장성 문제를 해결하지 못한다. 그 후 Iolus[10]에서 제안한 그룹키를 이용하여 확장성을 향상시키는 방법과 계층키를 이용한 방법[11]이 제안되었다. 더 나아가 데이터 뿐만 아니라 제어신호도 보호할 수 있는 KHIP[12]가 제안되었다. 이 장에서는 그룹키를 이용한 멀티캐스트 보안 방법과 계층키를 이용한 방법을 중심으로 하여 추가로 KHIP에 대하여 살펴본다.

2.1 그룹키를 이용한 키 분배 방법

그룹키를 이용한 대표적인 방법으로 Iolus가 있다. Iolus는 전체 멀티캐스트를 여러 그룹으로 나누고 각각의 그룹들을 (그림 1)과 같이 보안 분배 트리(Secure Distribution Tree)로 만든다. 보안 분배 트리는 GSI(Group Security Intermediaries), GSC(Group Security Controller), GSA(Group Security Agent) 세요소로 구성되어 있다. 각각 서브그룹간의 연결 관리, 전체 그룹을 관리하는 서버, 각 서브그룹을 관리하는 서버 역할을 한다. 모든 GSA들은 GSC를 통하여 그룹키를 분배받고, 각 사용자들은 자신이 속한 서브그룹의 GSA를 통해 그룹키를 분배받는다. 송신자가 전체 그룹 멤버들에게 메시지를 전송하기 위해서는 송신자가 속한 그룹의 그룹키로 암호화 하여 전송한다. 멤버가 다른 그룹에 있



(그림 1) Iolus의 구조

을 경우 GSI를 거쳐서 해당 그룹의 GSA로 보내져 복호화 된 후 다시 해당 그룹의 그룹키로 암호화 되어 멤버에게 전달된다. 만약 멀티캐스트 멤버가 가입하거나 탈퇴할 경우 해당 그룹의 그룹키만 변경하여 분배하면 되기 때문에 확장성과 비밀성을 높일 수 있다.

그룹키를 이용하여 멀티캐스트 서비스를 이용하는 방법은 가입과 탈퇴가 발생하였을 경우 키의 교체가 한 그룹만 발생하므로 부하는 전체적으로 적어지지만, 멀티캐스트 멤버가 많은 그룹에 퍼져있다면 패킷 전달과정에서 각 그룹을 통과할 때마다 이웃한 그룹의 키로 복호화를 한 후 다시 자신의 그룹키로 암호화하여 전달하는 과정을 반복해야한다. 즉 키의 구조와 교체가 적고 간단하지지만 패킷 전달에 필요한 암호화 과정이 복잡해지게 된다.

2.2 계층키를 이용한 키 분배 방법

계층키를 이용한 방법은 키 그래프(Key Graphs)를 이용하여 발전 하였다. 키 그래프를 이용한 멀티캐스트 통신[10]은 계층적 구조로 이루어진 트리로 구성된 키 그래프를 이용하여 키를 분배한다.

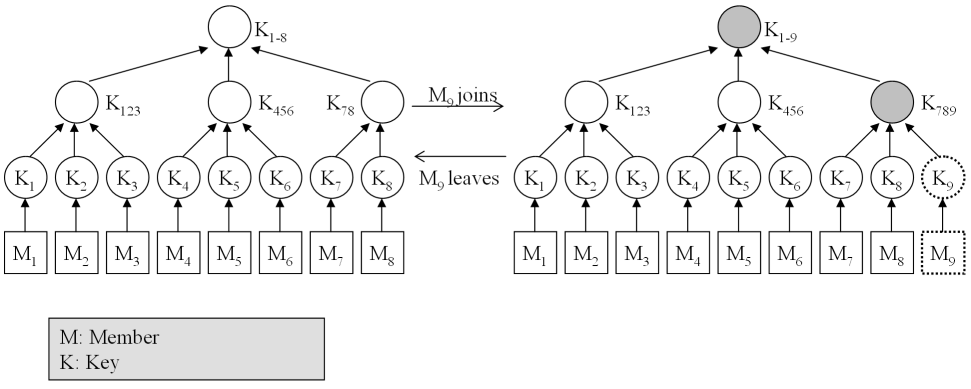
(그림 2)는 키 그래프를 이용한 계층키의 동작 과정을 나타내는 그림이다. Mn은 멀티캐스트 멤버 노드를 나타내고 각각의 멀티캐스트 멤버 노드는 키 Kn을 가지고 있다. 모든 멤버는 K_{1-8}(혹은 K_{1-9})을 공유하고 있고 K_{123}, K_{456}, K_{78}(혹은 K_{789})을 나누어서 가지고 있다. 즉 K_{123}은 M_1, M_2, M_3가 K_{456}은 M_4, M_5, M_6가 공유하고 있다. (그림 2)의 왼쪽의 구조에서 멤버 노드 M_9가 가입하게 되면 자신의 키인 K_9을 받고 상위 그룹키인 K_{789}와 K_{1-9}를 새롭게 받게 된다. 반대로 오른쪽 그림을 기준으로 모바일 노드 M_9가 탈퇴할 경우 새로운 키 K_{1-8}와 K_{78}을 분배하여 역방향 비밀성과 순방향 비밀성을 모두 만족하게 한다.

그룹키 방식의 키 분배와 다르게 계층키 방식은 패킷을 전달하는데 있어서 송신자와 수신자 위치에 있는 두 양 끝단 노드에서만 암호화와 복호화가 이루어진다. 그러나 키의 구조가 여러 층을 이루고 있기 때문에 멤버 노드의 가입과 탈퇴 시 키의 변경이 많아지게 된다. 물론 계층적으로 키의 구조가 이루어져 있어 (그림 2)의 M_1~M_6과 같이 가입과 탈퇴에 직접적인 영향이 없는 노드들은 기존키를 이용하여 멀티캐스트로 새로운 키를 받을 수 있지만, 키의 교체가 많아지게 된다.

이후 계층키를 이용한 다양한 방법들이 등장하였다. 그 중 Kronos[13]는 멤버의 이동에 관계없이 일정한 기간 동안 모든 그룹 멤버들은 하나의 정적 세션 키를 사용하도록 하는 방법이다. 또 은상아의 방법[14]은 그룹키에 대한 암호화 성능에 중점을 두었고 김태연의 방법[15]은 멀티캐스트 키 갱신 빈도를 서브그룹에 맞게 계산하여 확장성을 향상 시켰다. 그러나 이러한 방법 모두 유선네트워크에서의 멀티캐스트 프로토콜에 맞게 설계되어서 모바일 노드가 이동할 경우에 대하여 적용시킬 수 없다. 모바일 노드가 이동하게 되면 연결을 끊고 멀티캐스트 그룹에서 탈퇴한 후 다시 가입하는 방법으로 동작해야하기 때문에 키 분배 측면에서 많은 부하가 발생한다. 또 일부 방법의 경우 독자적인 네트워크에서 동작할 수 있게 설계되어 있어서 본 논문에서 제시한 마이크로 모빌리티 환경에 맞출 수 없다.

2.3 KHIP

KHIP는 멀티캐스트 데이터 뿐 아니라 제어신호를 보호하여 멀티캐스트 트리자체도 안전하게 하는 역할을 한다. KHIP의 구조는 계층적 멀티캐스트 라우팅 알고리즘을 확장하였고, lolus와 매우 흡사한 그룹키 관리 알고리즘을 채택하고 있다. 이 방법에서는 전체 멀티캐스트 그룹을 많은 도메인으로 나누고 도메인 내에 모든 멤버들은 똑같은 키를 공유하지만 모든 그룹 멤버가 공유하는 그룹키와 같은 것은 존재하지 않는다. 도메인의 공유키는 믿을 수 있는 라우터에 의해 만들어지고 갱신, 분배된다. 믿을 수 있는 라우터는 일반적으로 도메인의 최적 출구 라우터이며 도메인과 멀티캐스트 그룹의 센터 포인트로 향하는 다른 도메인과 연결한다. 그러나 KHIP는 경계 라우터이자 도메인의 키 관리자인 최적 출구 라우터가 자신을 통과하는 모든 패킷을 복호화하여 검사하고 다시 암호화하는 것이다. 이것은 경계라우터에 큰 부하를 발생시키게 되므로 경계라우터를 지나는 모든 패



(그림 2) 계층적 키 구조

킷은 지연되게 된다. 더욱이 송신자키의 생성 분배와 멤버와 송신자의 구분을 정확히 다루고 있지 않다[16].

3. 계층적 마이크로 모빌리티 환경의 멀티캐스트와 모바일 멀티캐스트 보안 요구사항

프로토콜이 적용될 마이크로 모빌리티 네트워크 환경을 정의한 후 멀티캐스트 프로토콜을 추가한 구조에 대하여 살펴본다. 그 다음 모바일 멀티캐스트 보안에 관한 요구사항에 대하여 알아본다.

3.1 계층적 마이크로 모빌리티 환경

안전한 멀티캐스트 프로토콜을 구성하려고 하는 네트워크 토폴로지는 유니캐스트 프로토콜에서 좋은 성능이 입증된 계층적 마이크로 모빌리티 구조[4]를 이용하였다. 이 구조는 또한 우리가 설계한 안전한 모바일 멀티캐스트 프로토콜에 적합하게 설계되어 있다.

이 구조는 기존의 모바일 IP[17], Cellular IP[18], HAWAII[19]같은 전통적인 마이크로 모빌리티의 장단점을 보완한 계층적인 마이크로 모빌리티 환경[1]을 이용하였다. 안전한 멀티캐스트 프로토콜에 사용될 구조는 (그림 3)과 같이 여러 도메인들로 구성되어 있다. 이 도메인은 최상위에 DRR(Domain Root Router)를 가지고 있고 많은 라우터들과 페이징 영역(Paging area)들을 포함하고 있다. 마찬가지로 각 페이징 영역 최상위에는 페이징 영역 라우터(PAR: Paging Area Router)가 있고 PAR 하부에는 트리 구조로 이루어진 BS(Base Station)들이 구성되어 있다. BS는 모바일 노드와 유선 네트워크를 연결하는 연결 지점의 역할도 하지만 각 BS간의 라우팅 기능도 겸하고 있다.

DRR, PAR, 그리고 라우터(R)로 이루어진 상위 네트워크는 네트워크 지정 라우팅 알고리즘 방식으로 동작하고, PAR과 BS들로 이루어진 하위 네트워크는 호스트 지정 라우팅 방식을 사용하여 동작한다.

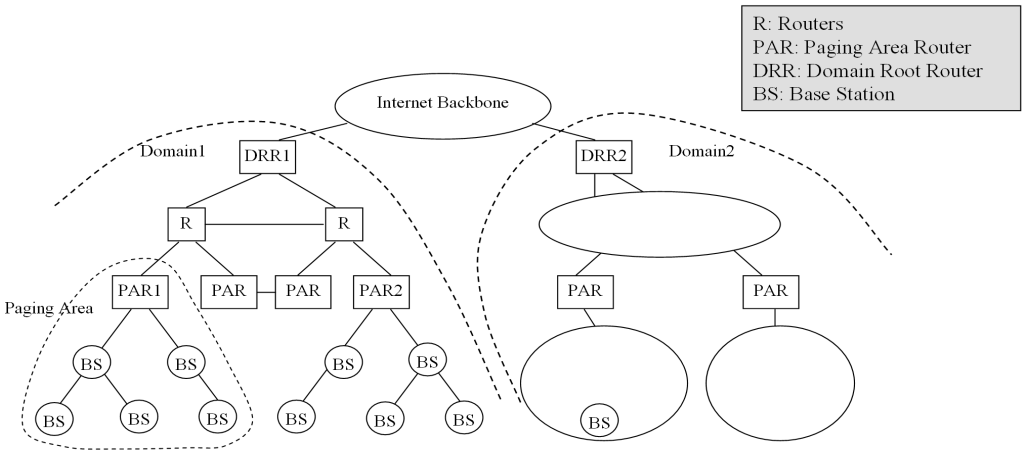
3.2 계층적 마이크로 모빌리티 환경의 멀티캐스트 프로토콜

모바일 IP에서 멀티캐스트 프로토콜 서비스를 하기 위하여 양방향 터널링방법(Bi-dirctional Tunnelgin)과 원격가입방법(Remote Subscription)을 IETF에서 제안하였다. 양방향 터널링 방법은 모바일 노드의 홈 에이전트까지 멀티캐스트 트리를 만들고 홈에이전트에서 모바일 노드까지 터널링을 하는 방법으로 홈에이전트와 외부에이전트의 거리가 멀면 멀티캐스트 트리가 비효율적이 된다. 양방향 터널링의 단점을 보완하기 위해 MoM[20]방법이 나왔지만 완벽하게 터널 집중 문제를 해결하지 못했다. 원격가입방법은 모바일 노드가 이동할 경우 새로 가입을 하는 방법으로 가입시간이 길어 패킷손실이 발생한다. 가입시간을 줄이기 위해 가입하는 동안 포워딩을 통하여 전송하는 MMA[21]방법이 제안되었지만 적절한 포워더 위치를 정의하지 못하였다.

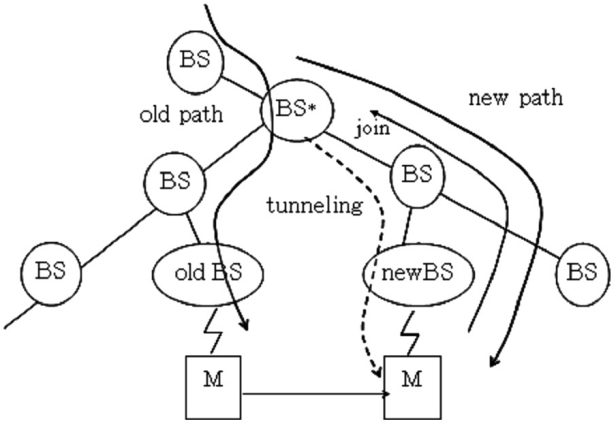
본 논문의 기반이 되는 모바일 멀티캐스트 프로토콜[2]은 코어 기반의 멀티캐스트 트리(Core-based Multicast Tree) 프로토콜[22]을 계층적 마이크로 모빌리티 환경에 사용한다. 모바일 노드가 핸드오프가 일어날 경우, 원격 가입방법을 기반으로 하는 MMA 방법을 이용하여 패킷 손실을 줄인다. 특히 MMA가 구현하지 못했던 적절한 포워더 위치를 계층적 마이크로 모빌리티 환경에 맞게 최적의 경로에서 전달할 수 있도록 결정하였다. (그림 3)과 같이 계층적 마이크로 모빌리티의 구조가 이루어져 있기 때문에 페이징 영역 내에서의 핸드오프, 페이징 영역간의 핸드오프, 도메인간의 핸드오프의 세 가지의 핸드오프가 생긴다.

3.2.1 페이징 영역 내에서의 핸드오프

(그림 4)는 페이징 영역 내에서의 핸드오프에 대한 그림이다. 멀티캐스트 서비스를 받고 있는 모바일 노드가 old BS에서 new BS로 이동하게 되면 new BS는 멀티캐스트



(그림 3) 계층적 마이크로 모빌리티 환경



(그림 4) 페이징 영역 내에서의 핸드오프 알고리즘

그룹의 코어 방향으로 멀티캐스트 가입메시지를 보내는 동시에 old BS와 new BS의 중간 노드인 BS*에게 포워딩을 요구한다. 중간 노드인 BS*가 포워더로서 멀티캐스트 패킷을 new BS를 통해 모바일 노드로 전달하게 된다. 코어 방향으로 보낸 멀티캐스트 그룹 가입 요청 메시지에 대한 응답으로 승인 메시지가 오게 되면, BS*에게 포워딩 중지 메시지를 보내게 되고, 멀티캐스트 서비스는 정상적인 멀티캐스트 트리를 이용하여 제공받게 된다. 이때 모든 BS는 네트워크 토폴로지를 모두 알고 있으므로 자신의 주변에 BS에 대한 중간노드의 리스트를 보관하고 있다.

3.2.2 페이징 영역간의 핸드오프와 도메인간의 핸드오프

페이징 영역간의 핸드오프와 도메인간의 핸드오프도 페이징 영역 내에서의 핸드오프와 동일하게 동작하지만 패킷을 전달하는 포워더의 위치가 틀려지게 된다. 페이징 영역간의 핸드오프는 같은 도메인이므로 현재 자신의 DRR이고 도메인간의 핸드오프는 old DRR이 효율적인 포워더의 위치이다. 그러나 보안기능이 포함된 구조에서는 키 관리 문제로 포워더의 위치가 바뀌어야 한다.

3.3 모바일 멀티캐스트 보안 요구사항

멀티캐스트 서비스에는 어떠한 종류의 공격이 이루어지고 있는지 알아보고 이러한 멀티캐스트 공격을 막기 위하여 반드시 고려되어야 하는 원칙에 대하여 설명한다.

멀티캐스트 서비스를 공격하는 종류에는 크게 공격의 위치와 공격 대상에 따라 나눌 수가 있다. 공격의 위치에 따른 공격 개념은 다음과 같이 가장자리 공격(Edge Attack)과 내부 공격(Internal Attack)으로 나눈다.

- 가장자리 공격: 멀티캐스트 트리의 끝단에서 행해지는 공격
  - 송신자 공격: 위조된 데이터나 제어신호를 멀티캐스트 주소를 통해 모든 호스트에 전송하여 대역폭의 낭비를 하게 만든다.
  - 수신자 공격: 멀티캐스트 멤버가 아닌 호스트가 멀티캐스트 패킷을 받아 이 호스트까지 패킷이 전송되므로 대역폭이 낭비된다.
- 내부 공격
  - 중간 노드나 라우터가 데이터를 공격하는 방법
  - 중간 노드나 라우터가 제어신호를 공격하는 방법

공격 대상에 따른 공격 개념은 다음과 같이 데이터 공격(Data Attack)과 제어신호 공격(Control Attack)으로 나눌 수 있다.

- 데이터 공격: 위조된 데이터를 멀티캐스트 데이터 스트림 안에 끼워 넣거나, 수정하거나 삭제하여 공격지점의 서브트리에 잘못된 데이터를 전달한다.
- 제어신호 공격: 위조된 컨트롤 패킷을 이용하여 멀티캐스트 트리에 공격자가 원하는 라우터를 가입 시켜 멀티캐스트 서비스를 잘못 동작하게 만든다.

다음은 앞에서 설명한 멀티캐스트 공격에 대하여 암호화 알고리즘을 설계하는데 반드시 고려해야할 사항에 대하여 설명한다.

- 동적 환경(Dynamic Environments): 새로운 가입자가 멀티캐스트에 가입하거나, 혹은 기존 가입자가 탈퇴할 경우의 키 관리에 관한 문제이다.
  - 순방향 비밀성(Forward Secrecy): 키를 알지 못해 데이터의 내용을 알 수 없지만 자료를 수신하여 보관하고 있다가, 특정 시점에 멀티캐스트 그룹에 가입을 하게 되면 키를 받게 된다. 이 키를 이용하여 기존에 저장해둔 데이터를 복호화하여 부당하게 사용하는 것을 막기 위한 문제이다.
  - 역방향 비밀성(Backward Secrecy): 이미 멀티캐스트에 가입되어서 서비스를 이용하는 사용자가 멀티캐스트 서비스를 탈퇴한 후에 기존의 키를 이용하여 패킷을 계속 수신하여 서비스를 이용할 수 있는 문제를 막아야한다.
- 멤버 시맨틱스(Member Semantics)
  - 멀티캐스트 그룹에는 보내고 받을 수 있는 멤버와, 보낼 수만 있는 송신자가 있다.
  - 모든 송신자의 경우 자신의 특별한 키를 가지고 있고 모든 멤버가 알고 있어야 한다.
- 확장성(Scalability)
  - 보안 메커니즘이 많은 멀티캐스트 멤버를 유지할 수 있어야 한다.
  - 라우터에게 주는 오버헤드를 줄여야 한다.

본 논문에서 제안하는 안전한 모바일 멀티캐스트 프로토콜은 중간 노드에서 전달받은 패킷을 다음 노드로 전달하지

않고 막는 문제와 DoS 공격을 제외한 모든 보안요구사항을 만족할 수 있게 설계되었다.

4. 마이크로 모빌리티 환경에서의 안전한 멀티캐스트 관리 및 전송기법

앞의 3장에서 설명한 내용을 바탕으로 안전한 모바일 멀티캐스트 프로토콜에 대하여 설명한다. 우선 프로토콜에 사용되는 용어에 대하여 설명하고 멀티캐스트의 생성, 가입, 탈퇴와 패킷이 안전하게 전달되는 과정, 그리고 핸드오프상황에 맞는 보안기능에 대하여 설명한다.

4.1 용어 정의

안전한 모바일 멀티캐스트 라우팅 프로토콜을 설명하기 위해 사용된 용어와 표기법에 대하여 설명한다. 앞으로 다음과 같은 표기법을 사용한다.

- PK-N: 노드 N의 공개키
- SK-N: 노드 N의 개인키
- $CERT_N$: 노드 N의 인증서
- D^K: K라는 키로 메시지 D를 암호화 한 경우
- $\{D\}^{SK-N}$: 노드 N의 개인키를 이용하여 메시지 D를 서명. $D \parallel (Hash(D))^{SK-N}$과 같다.

보안 기능 구성요소로 권한 부여 서버(AS)와 그룹 초기자(GI)가 있다.

- AS(Authorization Server): 케이퍼빌리티(Capability)를 생성하여 분배한다. 케이퍼빌리티는 해당 노드의 서비스 정보와 권한을 나타내는 자료로 AS에서 처음 생성되어 각 노드에 분배된다. 케이퍼빌리티의 형식은 다음과 같다.

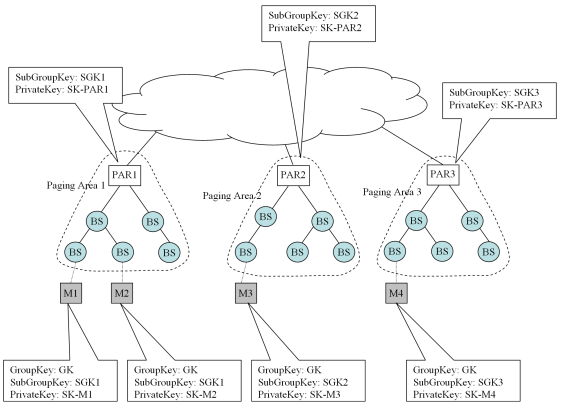
$$CAP_N = \{IP_N, CERT_N, MA, P, TS, L\}^{SK-AS}$$

IP_N은 노드 N의 IP, $CERT_N$은 노드 N의 인증서이다. MA는 멀티캐스트 주소이고, P는 멤버가 GI인지, 송신자인지, 송수신자인지를 결정하는 권한을 나타내며, TS는 타임스탬프, 그리고 L은 라이프타임을 나타낸다.

- GI(Group Initiator): 멀티캐스트 그룹을 처음 만드는 노드를 말한다. 그룹 생성을 위하여 모든 멀티캐스트 멤버의 ACL(Access Control List)을 만든다. ACL은 (이름, 권한)의 셋으로 구성되어 있고 모든 멤버의 접근 권한을 정의한 리스트를 말한다.

4.2 키의 종류와 용도

모든 멀티캐스트 멤버 노드는 공개/개인키 쌍을 가지고 있고 AS의 공개키인 PK-AS를 알고 있고 공개/개인키를 이용하여 인증과 서명을 하게 된다. 만약 이 멤버가 송신자라고 가정하면 메시지를 다른 멤버들에게 전송을 해야 한다. 이때 사용되는 키가 데이터키(Data Key)인 DK이다. DK는 송신자가 직접 생성하여 전송한 메시지를 암호화한다. 송신자가 생성한 DK는 다른 멤버들은 알 수 없으므로 DK를 메시지와 함께 전송한다. 그러나 멤버 이외의 다른 노드들까지 DK를 알게 되므로 멤버들만 소유한 그룹키(Group Key)인 GK를 이용해 DK를 암호화하여 전송한다. GK를 사영하면 멤버 이외에는 메시지를 볼 수 없지만, 멀티캐스트 가입과 탈퇴, 그리고 핸드오프가 발생하게 되면 GK를 변경시켜 주어야 순방향/역방향 비밀성을 유지할 수 있게 된다. 이 경우 가입, 탈퇴, 핸드오프가 일어날 때마다 모든 멤버에게 변경된 GK를 보내야하므로 키 분배로 인한 부하가 많이 발생한다. 그래서 페이징 영역을 기준으로 서브그룹을 만들고 서브그룹 내에서는 서브그룹키(Subgroup Key)인 SGK로 한번더 암호화를 하여 가입, 탈퇴, 핸드오프 발생 시 해당 SGK만을 교체하고 GK는 변경하지 않게 하여 키 분배 부하를 줄인다. SGK는 페이징 영역에 포함된 모든 멤버 노드들과 PAR만 소유하고 있다.



(그림 5) 계층적 마이크로 모빌리티 환경의 키 보유 상황

(그림 5)는 계층적 마이크로 모빌리티 구조에서 각 멤버들(M1~M4)과 PAR이 소유하고 있는 키를 설명한 그림이다.

4.3 안전한 모바일 멀티캐스트 프로토콜 설명

안전한 모바일 멀티캐스트 그룹 트리의 생성, 가입, 탈퇴 시 이루어지는 동작과 패킷이 전달되는 과정의 보안 프로토콜, 그리고 모바일 노드가 이동하여 핸드오프가 발생할 경우 이루어지는 동작과 보안 프로토콜에 대하여 설명한다.

4.3.1 안전한 멀티캐스트 그룹 생성

멀티캐스트 그룹 생성은 그룹 초기자인 GI에서 시작된다. GI는 ACL을 AS에게 보낸다. 노드 M1과 M2가 있다고 가정 할 경우 GI가 보내는 ACL은 다음과 같다.

(I,Group Initiator), (M1, Sender), (M2, Receiver)

AS는 이 ACL을 이용하여 케이퍼빌리티를 만들고 다시 GI에게 보내다. AS가 GI에게 다시 보내는 케이퍼빌리티는 다음과 같다. 노드 M1과 M2 그리고 GI에 대한 케이퍼빌리티이다.

$$GI\text{-}CAP_I = \{IP_I, CERT_I, MA, I\text{-}P, TS, L\}^{SK\text{-}AS}$$
$$S\text{-}CAP_{M1} = \{IP_{M1}, CERT_A, MA, S\text{-}P, TS, L\}^{SK\text{-}AS}$$
$$R\text{-}CAP_{M2} = \{IP_{M2}, CERT_B, MA, R\text{-}P, TS, L\}^{SK\text{-}AS}$$

AS는 케이퍼빌리티를 자신의 개인키를 이용하여 서명하고 GI로 보낸다. 그 후 GI는 멀티캐스트 그룹의 코어를 선택하고 코어의 주소인 IP_{CORE}를 저장하고 그룹키인 GK를 생성한다.

4.3.2 안전한 멀티캐스트 그룹 가입과 탈퇴

(그림 6)은 모바일 노드가 멀티캐스트 그룹에 가입과 탈퇴를 하는 그림이다. 먼저 멀티캐스트 그룹 가입의 경우 (그림 6)의 (a)와 같이 동작한다. 멀티캐스트 그룹에 가입을 원하는 모바일 노드 M1은 GI에게 연결하여 인증과정을 거친다. GI는 모바일 노드 M1에게 케이퍼빌리티와 코어의 IP 그리고 그룹키인 GK를 알려준다.

$$\{(GK, CoreIP, CAP_{M1})^{PK\text{-}M1}\}^{SK\text{-}GI}$$

그리고 M1이 속한 BS가 멀티캐스트 그룹에 포함되어 있지 않다면 BS는 코어를 향해 멀티캐스트 그룹 가입메시지를 보낸다.

이와 동시에 PAR1에게 그룹 가입을 알리면서 새로운 서브그룹키를 요청한다. 새로운 서브그룹키인 SGK2의 분배는 기존의 서브그룹키인 SGK1을 이용하여 해당 페이징 영역내의 기존 멤버 노드들에게 멀티캐스트를 이용하여 분배한다.

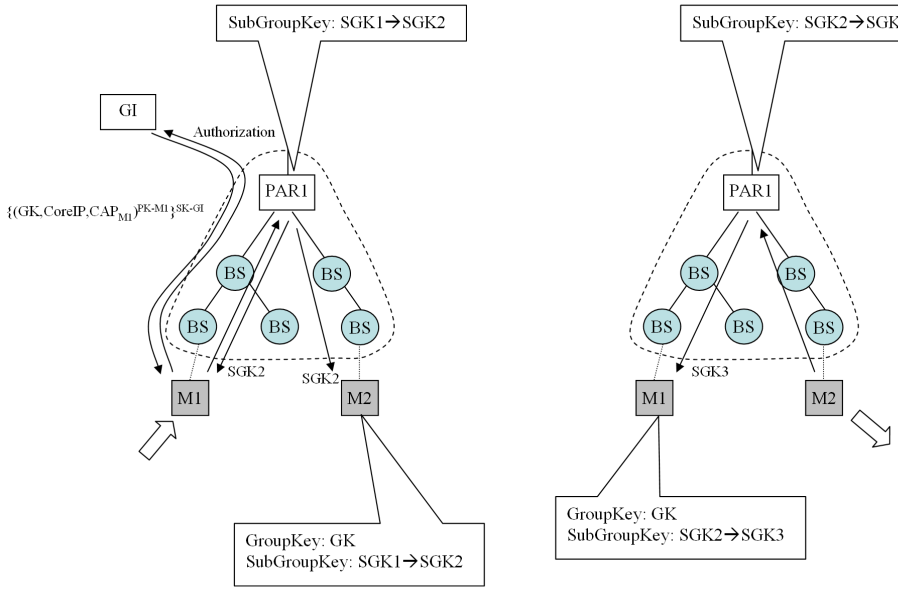
$$\{(SGK2)^{SGK1}\}^{SK\text{-}PAR1}$$

그러나 새로 가입한 멤버에게는 예전 키인 SGK1이 없기 때문에 유니캐스트로 직접 알려주게 된다. 다음은 BS에서의 멀티캐스트 그룹 가입 알고리즘이다.

```
Check the authenticity of the message and the capability;
Store the message;
Notify PAR of its paging area of M1's joining and request it to
      modify/distribute the key hierarchy for the subgroup within
      the paging area;
If (M is the first member of MA in this cell)
      Send the Join request toward the core;
```

(그림 6)의 (b)는 멀티캐스트 멤버 M2가 그룹 탈퇴를 할 경우이다. M2가 속해있는 BS는 M2가 자신의 마지막 멀티캐스트 멤버일 경우 코어를 향해서 멀티캐스트 그룹 탈퇴 메시지를 보낸다. 그리고 PAR1에게 멀티캐스트 그룹 탈퇴를 알려 키를 재분배 받게 한다. PAR1에서 기존의 서브그룹키인 SGK2가 새로운 SGK3로 생성되고 이 키는 탈퇴한 멤버를 제외한 서브그룹 내의 모든 다른 멤버에게 전달해야 한다. 가입과는 다르게 탈퇴한 멤버가 기존의 키인 SGK2를 알고 있으므로 새로 생성된 키인 SGK3를 멀티캐스트를 이용하여 분배할 수 없다. 즉 모든 멤버에게 유니캐스트를 이용하여 직접 전달한다.

다음은 BS에서의 멀티캐스트 탈퇴 알고리즘이다.



(a) 멀티캐스트 그룹 가입 (b) 멀티캐스트 그룹 탈퇴

(그림 6) 안전한 멀티캐스트 그룹 가입과 탈퇴

```
Check the authenticity of the message;
Remove the information about M from its storage;
Notify PAR of its paging area of M's leaving and request it to
      modify/distribute
      the key hierarchy for the subgroup within the paging area;
If (M is the last member of MA in this cell)
      Send the Leave request toward the core;
```

4.3.3 안전한 멀티캐스트 프로토콜의 패킷 전송

(그림 7)은 안전한 멀티캐스트 프로토콜의 메시지 전달 과정을 설명한 그림이다. 만약 멀티캐스트를 이용하여 멤버 M1이 메시지 D를 전송하려 한다면, 우선 D를 데이터 암호화키인 DK로 암호화하고 개인키를 이용하여 암호화한 메시지에 서명을 한다. 그리고 GK와 SGK1을 이용하여 DK를 이중으로 암호화한다.

$$\{D^{DK}\}^{SK-M1}, (DK^{GK})^{SGK1}$$

이 패킷은 우선 M1이 속한 셀의 BS로 보내진다. 멤버에서 BS로 보내는 패킷들은 멤버의 케이퍼빌리티를 검사하므로 실제 송신자인지를 검사할 수 있다. 페이징 영역으로 멀티캐스트 패킷을 전달할 경우 같은 서브그룹키를 가지고 있기 때문에 아무런 키의 변화 없이 패킷을 전달 할 수 있다. 그러나 페이징 영역 외부로 멀티캐스트 패킷을 보낼 경우는 PAR에서 수정을 하게 된다. (그림 7)에서 암호화된 패킷이 PAR1에 도착하게 되면 PAR1은 SGK1을 이용하여 페이징 영역의 밖으로 다음과 같은 형태로 전송한다.

$$\{D^{DK}\}^{SK-M1}, DK^{GK}$$

BS들과 PAR들은 이러한 패킷을 처리하고 포워딩할 수는 있지만 그룹키인 GK를 가지고 있지 않기 때문에 메시지 D를 읽을 수는 없다. 패킷이 페이징 영역2의 PAR2에 도착하게 되면 다시 DK^{GK}를 페이징 영역2의 서브그룹키인 SGK2로 암호화하여 전송한다.

$$\{D^{DK}\}^{SK-M1}, (DK^{GK})^{SGK2}$$

페이징 영역2에 있는 멤버들은 모두 GK와 SGK2를 가지고 있기 때문에 이 패킷을 읽을 수 있다. 역시 PAR2나 BS들은 GK를 가지고 있지 않으므로 메시지 D를 읽을 수 없다.

4.3.4 안전한 멀티캐스트 프로토콜의 핸드오프

핸드오프는 페이징 영역 내에서의 핸드오프와 페이징 영역간의 핸드오프 두 가지로 나눌 수 있다. 같은 페이징 영역내의 다른 BS로 모바일 노드가 이동하는 경우는 같은 서브그룹키를 가지는 구역이므로 키를 재 생성하지 않고 기존의 서브그룹키를 이용하여 패킷을 송/수신할 수 있다. (그림 8)은 페이징 영역 내에서의 핸드오프 과정을 나타내는 그림이다. 모바일 노드 M이 BS1에서 BS2로 이동하였지만 BS2가 멀티캐스트 서비스를 하지 않는 경우 멀티캐스트 가입 메시지를 IP_{CORE} 방향으로 보낸다.

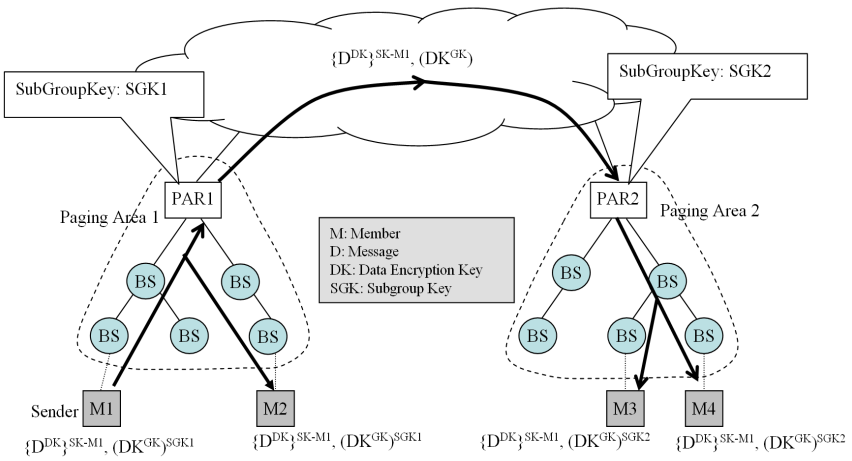
$$\{\text{Join Request}, IP_{M1}, MA, CAP_M\}^{SK-M}$$

그 후 BS2는 BS3에게 터널링 요구를 한다. BS3에서 포워딩되는 패킷도 역시 같은 서브그룹키인 SGK으로 암호화하여 보내게 된다.

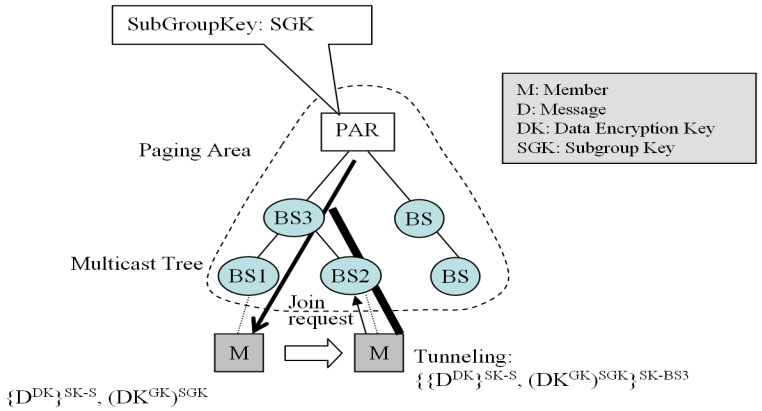
$$\{\{D^{DK}\}^{SK-S}, (DK^{GK})^{SGK}\}^{SK-BS3}$$

새로운 키 분배가 필요 없으므로 B3가 멀티캐스트 그룹에 가입 완료될 경우, 포워딩을 중단하고 기존과 똑같은 서브그룹키 SGK와 그룹키 GK로 암호화된 패킷을 받을 수 있다.

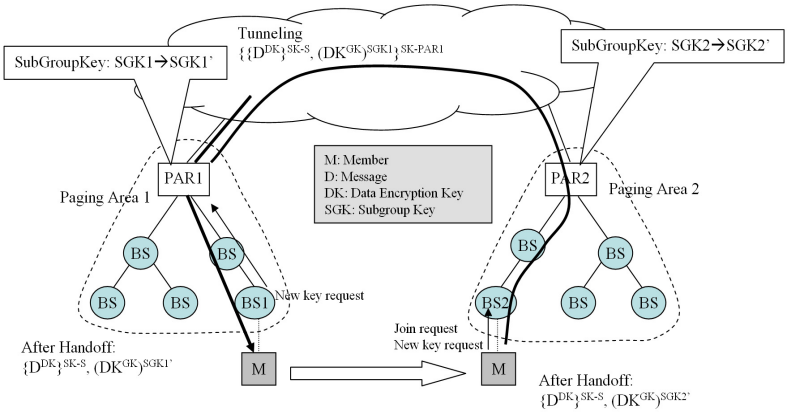
$$\{D^{DK}\}^{SK-S}, (DK^{GK})^{SGK}$$



(그림 7) 안전한 멀티캐스트 프로토콜의 메시지 전달과정



(그림 8) 페이징 영역 내의 안전한 핸드오프



(그림 9) 페이징 영역간의 안전한 핸드오프

페이징 영역간의 핸드오프는 (그림 9)로 설명할 수 있다. 모바일 노드 M이 페이징 영역1에 속해있는 BS1에서 페이징 영역2에 속한 BS2로 이동하였다. 이 때 BS2가 같은 멀티캐스트 그룹에 가입하고 있을 경우도 있고 아닐 수도 있다. 두 경우 모두 PAR2에게 새로운 서브그룹키를 요청해야 한다. 그리고 만약 BS2가 멀티캐스트 그룹에 가입하고 있지 않을 경우 멀티캐스트 가입 메시지를 IP_{CORE}로 보내고 PAR1에게 포워딩을 요청한다. 그리고 BS1도 모바일 노드 M이 다른 영역으로 넘어간 것이므로 PAR1에게 새로운 서브그룹키를 요청한다. PAR1은 M에게 기존의 서브그룹키인 SGK1을 이용하여 패킷을 전달한다.

$$\{\{D^{DK}\}^{SK-S}, (DK^{GK})^{SGK1}\}^{SK-PAR1}$$

이 때 PAR1과 PAR2는 새로운 서브그룹키인 SGK1′과 SGK2′을 생성하여 분배하기 시작한다. 여기서 핸드오프를 완료하기 위해서는 두 가지 동작이 완료되어야한다. 첫 번째는 BS2가 멀티캐스트 그룹에 가입이 완료되었을 경우이고, 두 번째는 페이징 영역2의 새로운 서브그룹키인 SGK2′의 분배가 완료되었을 경우이다. 첫 번째 경우는 BS2가 멀티캐스트에 이미 가입되어 있을 경우도 있다. 그러나 새로운 키를 받지 못했으므로 반드시 키 분배가 완료될때까지 포워딩을 받아야한다. 핸드오프가 완료되면 PAR1에게 포워딩 종료를 요청하고 연결을 끊는다.

BS에서의 안전한 핸드오프 알고리즘은 다음과 같다.

```
Check the authenticity of the message;
if(old PAR== new PAR) {
   if(M is the first member of the new cell) {
      request crossover BS to forward multicast packets to M;
      send join request toward core;
      receive join ack;
      request the crossover BS to stop forwarding;
   }
   else
      /* new BS can deliver multicast packets to M so there is
        nothing to do */
}
else {
   if(M is the first member of the new cell) {
      request old PAR to forward multicast packet to M;
      send join request toward the core;
   }
   old BS in old paging area requests new subgroup key;
   new BS in new paging area requests new subgroup key;
   if(Receive new subgroup key && join ack)
      request old RAR to stop forwarding;
}
```

5. 프로토콜 분석 및 실험

본 논문에서 제안한 보안 멀티캐스트 프로토콜은 인증, 접근제어, 비밀성 그리고 무결성을 만족해야한다. 또 3.3에서 서술한 다양한 공격방법을 막고, 멀티캐스트 보안 요구사항인 동적환경과 확장성, 그리고 멤버 시맨틱스를 만족해야 한다. 이러한 요구사항을 만족하고 있는지 분석해 보고, 실험을 통하여 성능을 평가 하였다.

5.1 안전한 모바일 멀티캐스트 프로토콜 분석

인증과 접근제어는 그룹 초기자인 GI와 권한 부여 서버인 AS가 수행한다. 노드가 GI에 인증을 요청하게 되면 AS는 GI의 ACL을 이용하여 생성된 케이퍼빌리티 생성하여 노드에게 전달하게 된다. 이러한 과정을 통하여 인증과 접근제어를 만족시킨다.

비밀성은 송신자가 생성한 암호화키인 DK와 이 키를 암호화하여 중간노드가 볼 수 없게 한 그룹키 GK가 있다. 그리고 가입, 탈퇴, 핸드오프시 키 변경으로부터 데이터를 보호할 수 있게 변경하는 서브그룹키인 SGK를 이용하여 데이터를 멤버 이외의 노드가 볼 수 없게 하고 있다.

무결성은 송신자가 보내려고 하는 메시지를 송신자의 개인키를 이용하여 서명한 후 전송함으로써 만족시킨다. 송신자는 정해진 해쉬함수를 이용하여 메시지를 요약하고 이 요약된 값을 자신의 개인키를 이용하여 서명하여 실제 메시지와 함께 멀티캐스트 멤버들에게 보내게 된다. 메시지를 수신한 멤버는 송신자의 공개키를 이용하여 서명부분을 복호화하여, 보내진 메시지의 해쉬 결과와 같은지를 확인하여 무결성 검사를 하게 된다.

다음으로 멀티캐스트 보안 요구사항인 동적환경, 확장성, 그리고 멤버 시맨틱스를 만족하고 있음을 보인다.

서브그룹키인 SGK의 교체는 순방향/역방향 비밀성을 유지하므로 동적환경을 만족시킨다. 노드가 멀티캐스트 멤버에 가입하거나 탈퇴하게 되면 멤버가 포함되어 있는 페이징 영역의 서브그룹키를 교체하기 때문에 순방향/역방향 비밀성을 지킬 수 있다. 멤버가 다른 페이징 영역으로 넘어가게 되면 이전 페이징 영역과 새 페이징 영역의 서브그룹키를 교체한다.

설계한 안정한 모바일 멀티캐스트 프로토콜은 적용되는 네트워크 환경이 마이크로 모빌리티이므로 많은 수의 노드를 성능 저하 없이 수용할 수 있다. 또 멀티캐스트 멤버가 많이 늘어나도 키의 구조가 커지는 계층키 구조가 아닌 그룹키 구조를 적용하고 있어서 확장성에 유리하다.

메시지 전송시 송신자가 데이터 암호화키를 생성하고 이 키를 암호화하여 모든 수신 멤버에게 보내므로 멤버들은 이 키를 알 수 있다. 또 ACL을 이용한 케이퍼빌리티는 사용자가 송신과 수신을 할 수 있는 멤버인지 아니면 수신만 가능한 멤버인지를 구분할 수 있다.

멀티캐스트 공격방법은 공격대상에 따른 분류와 공격 위치에 따른 분류를 이용하여 가장자리 데이터 공격, 가장자리 제어신호 공격, 내부 데이터 공격, 그리고 내부 제어신호 공격의 네 종류로 나눌 수 있다. 가장자리에서 데이터에 대한 공격은 멀티캐스트 멤버인 송신자가 데이터키를 멤버만 알고 있는 그룹키와 서브그룹키로 암호화하고 자신의 개인키로 서명을 하였기 때문에 위조, 삽입, 삭제 도청이 불가능하다. 가장자리에서의 제어신호 공격은 가짜 참여, 탈퇴 메시지를 보내는 것으로 멤버가 아닐 경우 BS에서 거부되므로 불가능하다. 내부에서의 데이터에 대한 공격에서 데이터의 수정과 삽입의 경우 메시지가 서명이 되어 있으므로 수신하는 멤버에서 확인이 가능하므로 안전하다. 그러나 데이터를 삽입 하는 경우 잦은 데이터 삽입 동작을 반복하여 네트워크 자원을 낭비시킬 수 있다. 그리고 중간의 악의적인 노드가 패킷을 전달하지 않고 삭제를 하는 경우 막을 방법이 없다. 마지막으로 내부에서 제어신호의 공격은 가장자리에서의 제어신호의 공격과 마찬가지로 멤버가 아닐 경우 BS나 다음 라우터에서 거부되어 공격을 막을 수 있다. 결론적으로 제안한 안전한 모바일 멀티캐스트 프로토콜은 모든 가장자리 공격을 모두 막을 수 있고, 내부공격 중에서 데이터를 삭제하는 공격과 데이터의 삽입으로 인한 자원낭비를 제외한 모든 공격을 막을 수 있다.

5.2 실험 및 성능 평가

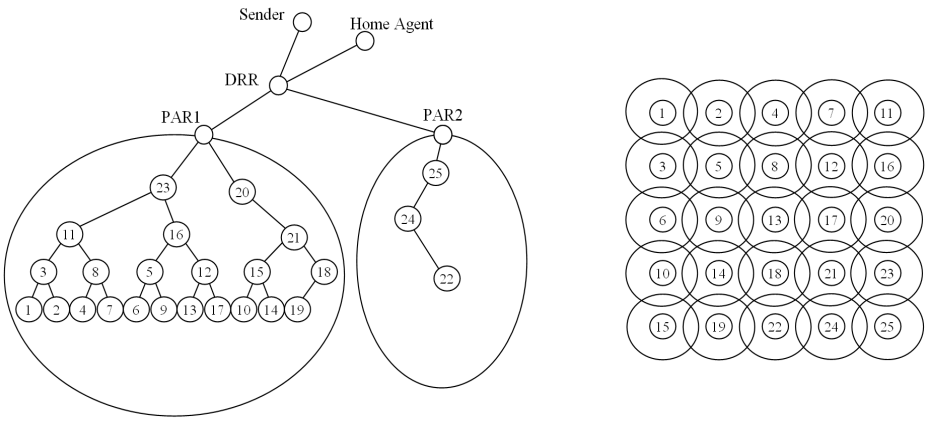
안전한 멀티캐스트 프로토콜의 성능을 알아보기 위하여 보안기능을 제거한 모바일 멀티캐스트 프로토콜[2]과 비교하는 실험을 ns2[23]를 이용하여 수행하였다. 단순히 두 프로토콜만을 비교 실험하는 이유는 지금까지 마이크로 모빌리티 환경에서 멀티캐스트 프로토콜의 키 분배와 암호화 알고리즘에 대하여 체계적으로 기술한 자료가 없기 때문이다. 제안한 멀티캐스트 프로토콜이 키 분배와 데이터 암호화 같은 보안 기능을 제거한 모바일 멀티캐스트 프로토콜에 비해 어느 정도 부하가 더 발생하는지에 대하여 전송 속도를 이용하여 실험하였다.

5.2.1 실험 환경

실험을 위한 모바일 네트워크 환경은 (그림 10)과 같이 구성하였다. (그림 10) (a)는 네트워크의 논리적인 구성이고 (b)는 물리적인 구성을 나타낸다. 페이징 영역 1에 22개의 BS를, 페이징 영역 2에 3개의 BS를 연결하였다. PAR, DRR, 송신자, 홈 에이전트는 구성하였다. 유선 네트워크의 대역폭은 10Mbps이고 무선은 1Mbps로 설정하였다.

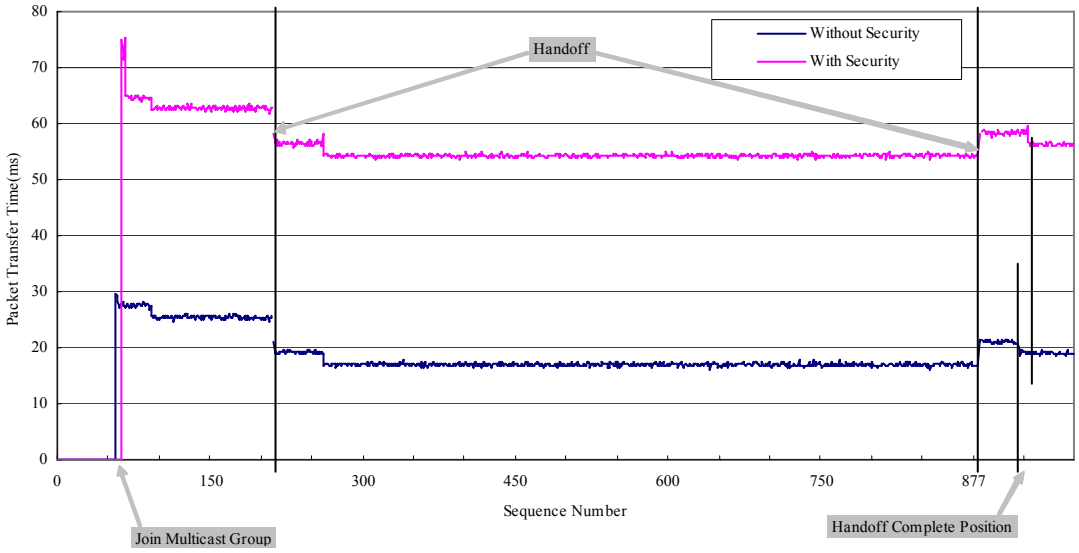
보안 기능이 포함된 안전한 모바일 멀티캐스트 프로토콜의 성능 평가는 다음과 같이 세 가지 관점에서 진행하였다.

- 하나의 모바일 노드에서의 부하 측정: 하나의 노드가 멀티캐스트 가입과 핸드오프를 거치면서 발생하는 패킷 전송시간을 측정하여 키 분배가 미치는 부하를 측정한다.
- 서브그룹키 분배로 인한 노드들의 평균 부하 측정: 노드들의 이동성을 증가시켜 많은 핸드오프를 발생시켜 그에 따른 서브그룹키의 분배가 미치는 노드의 부하를 측정한다.



(a) 논리적인 구성 (b) 물리적인 구성

(그림 10) 실험을 위한 네트워크 구성



(그림 11) 한 노드의 일정시간 동안의 전송시간의 변화

- 암호화에 따른 부하 측정: 위 두 가지 방법을 측정하면서 암호화에 따른 부하가 측정 가능하다. 즉 따로 실험은 하지 않고 위 두 실험을 이용하여 분석해 본다.

  암호화에 사용된 알고리즘과 키 구조는 다음과 같다.

- 공개키 알고리즘(PK-N, SK-N): RSA알고리즘을 1024bit의 키로 사용하였다. 주로 서명을 하기 위하여 사용하였지만, 인증작업시 메시지를 암호화하는데 쓰였다.
- 비밀키 알고리즘: 메시지와 키를 암호화하는 알고리즘으로 3DES 알고리즘을 사용하였고, 56bit의 키 두 개를 사용하였다.

5.2.2 실험 결과

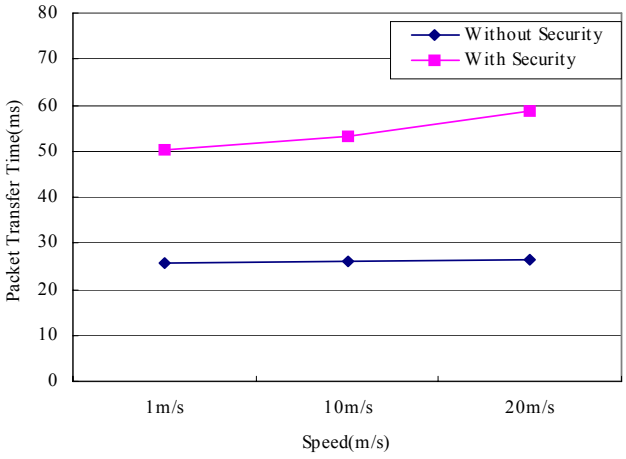
멤버 노드의 가입과 이동으로 인한 키 분배와 핸드오프 시간의 변화를 알아보기 위하여 (그림 11)과 같이 일정시간 동안 하나의 모바일 멤버 노드에 도착하는 패킷의 전송시간을 측정하였다. 전원이 들어와 멀티캐스트 그룹에 가입하면서부터 두 번의 핸드오프가 일어나는 상황이다. 시퀀스 번호 60근처에서 노드가 멀티캐스트 그룹에 가입신청을 하고 인증과 키 분배를 받기까지의 시간이 보안이 적용된 구조에서 더 많이 걸리고 전송시간 차이도 더 심한 것을 볼 수 있다. 전 구간에서 보안이 적용된 구조와 적용되지 않은 구조의 전송시간 차이가 일정하게 나타난다. 이것은 실제 암호화되는 구간은 송신자, 수신자 그리고 DRR, PAR 에서만 일어나고, 그 이외의 노드에서는 단순히 패킷만 전달하기 때문이다. 그런데 핸드오프를 해서 전송 경로가 틀려졌다고 해도 암호화와 관련된 노드들의 숫자는 같게 되므로 보안구조를 적용한 것과 적용하지 않은 두 방법의 전송시간 차이는 비슷할 수밖에 없다.

(그림 11)에서 핸드오프는 시퀀스 번호 220과 877 위치에서 두 번 발생한다. 220위치에서 발생한 핸드오프는 같은 페이징 영역이므로 서브그룹키의 재분배가 필요 없기 때문에 두 방법 모두 동일한 시점에서 핸드오프가 완료된다. 그러나 시퀀스 번호 890의 위치에서 발생한 핸드오프는 완료 시점이 틀리다. 보안기능이 추가된 구조에서 키 분배가 늦어져 핸드오프 완료 시점이 지연된 것이고, 보안기능이 없는 구조는 기존대로 멀티캐스트 가입이 완료된 시점에서 핸드오프가 종료되었다.

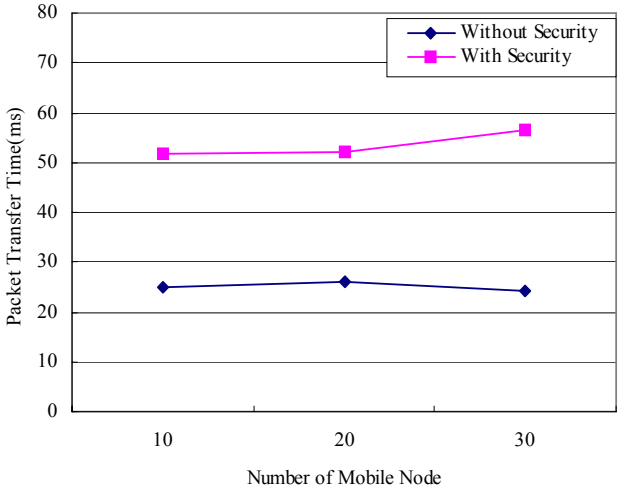
키 분배가 전체 네트워크에 주는 오버헤드를 측정하기 위하여 모바일 노드의 개수와 평균 이동속도를 변화시켰을 경우 평균 패킷 전송시간의 변화를 측정하여 (그림 12)와 (그림 13)의 그래프를 얻었다. (그림 12)에 사용된 모바일 노드 수는 20개이고, (그림 13)의 모바일 노드 평균 이동속도는 10m/s이다.

(그림 12)는 모바일 노드의 평균 속도를 1m/s에서 20m/s까지 증가시켰을 경우 패킷의 전송시간의 변화를 기록한 그림이다. 우선 보안 기능이 추가된 방법의 경우 데이터의 암호화로 인하여 보안구조가 없는 방법보다 전체적으로 30ms 정도 지연되었다. 물론 노드의 평균 이동속도가 늘면서 차이는 커지지만 그 차이가 10ms정도이다. 그리고 모바일 노드의 평균 이동속도가 증가하였을 경우 보안기능이 적용되지 않은 방법은 전송 시간의 차이가 없는 반면 보안기능이 추가된 모바일 멀티캐스트 프로토콜 방법은 모바일 노드의 속도가 증가할수록 크지는 않지만 전송시간의 증가를 보였다. 이는 평균 모바일 노드 이동 속도가 빨라지면서 핸드오프의 발생 빈도도 같이 증가하게 되는데 이 때 키 분배로 인하여 평균 전송 시간이 증가하였기 때문이다.

(그림 13)은 전체 네트워크에 사용된 모바일 노드의 개수를 증가시켰을 경우 패킷 전송시간의 변화를 기록한 그림이다. (그림 12)와 같이 보안 기능이 추가된 방법이 보안기능이 없는 방법보다 전체적으로 패킷 전송 시간이 30ms 늦다. 그러나 그래프의 기울기는 (그림 12)와 틀리게 된다. 보안기능이 적용되지 않은 방법의 경우 모바일 노드가 점점 증가



(그림 12) 평균 속도 변화에 따른 평균 전송시간



(그림 13) 모바일노드 수 변화에 따른 평균 전송시간

하게 되면 어느 시점에서 많은 BS가 멀티캐스트 그룹에 가입되어 있기 때문에 포워딩이나 멀티캐스트 가입과 같은 동작이 일어나지 않을 확률이 증가하여 평균 전송시간이 낮아진다. 보안기능이 적용된 방법도 마찬가지로 모바일 노드가 증가할수록 멀티캐스트에 이미 가입된 BS로 이동할 확률이 증가하지만 핸드오프가 발생하게 되면 멀티캐스트 그룹의 가입 여부와 상관없이 서브그룹키를 새로 받아야 하기 때문에 전송시간이 증가 할 수밖에 없다. 즉 핸드오프의 완료시간이 멀티캐스트 가입이 완료되는 시점이 아닌 새로운 키를 받는 시점이기 때문이다.

6. 결론 및 향후 연구과제

계층적 마이크로 모빌리티 환경에서의 안전한 멀티캐스트 프로토콜을 제안하였다. 보안에 취약한 프로토콜을 안전하게 만들기 위해 보안 기능을 추가하였다. 보안 기능이 추가된 프로토콜은 대칭키, 비대칭키 암호화 알고리즘과 케이퍼빌리티를 이용하여 인증, 접근제어, 비밀성, 무결성 등의 보안 서비스를 제공한다. 순방향/역방향 비밀성과 확장성을 제공하기 위해 보안 그룹을 사용하였다. 이러한 보안기능은 악의적인 노드에 의해 멀티캐스트에서 수행되는 모든 유형의 공격을 방지할 수 있다. 그리고 내부의 악의적인 노드에 의한 공격의 경우 패킷 삭제와 네트워크 자원의 낭비를 유발하는 공격을 제외하고 모든 공격을 방지할 수 있다.

제안한 프로토콜의 성능을 측정하기 위하여 ns2 시뮬레이터를 이용하였다. 키 분배에 따른 부하는 하나의 모바일 노드에 미치는 영향과 키 분배가 전체 네트워크에 미치는 영향을 측정하였다. 또 암호화가 전체 네트워크에 미치는 영향을 패킷 전송시간을 이용하여 보안기능이 제거된 모바일 멀티캐스트 프로토톨과 비교 측정하였다. 하나의 모바일 노드에 키 분배가 미치는 영향은 멀티캐스트 그룹에 가입되는 시간보다 키 분배가 늦어지는 경우 핸드오프가 몇 시퀀스가 늦어지는 경우가 발생하지만 키 분배가 먼저 끝나는

경우도 발생하여 차이가 거의 없었다. 키 분배가 전체 네트워크에 주는 부하는 노드 수와 평균 이동 속도 증가함에 따라 평균 전송 시간이 늦게 되지만 아주 적은 변화만 있었다. 마지막으로 암호화에 따른 성능은 암호화 강도나 키의 크기에 따라 틀려지지만 실제 많이 사용하는 키와 알고리즘을 이용하여 전송 시간을 측정 하였다. 전체적으로 30ms~40ms정도의 전송시간이 증가한 것을 보여줬다.

본 연구의 보안 기능은 비밀성, 기밀성, 무결성 등을 보장하지만 중간에서 악의적인 노드가 메지시나 제어신호를 전달을 방해하거나 외부의 악의적인 노드가 멀티캐스트 트리의 중간이나 끝단 노드에게 DoS공격을 가하는 것을 막거나 탐지할 수 없다. 또 현재 모바일 노드의 프로세스 파워의 경우 노트북을 대상으로 하고 있지만 더 파워가 적은 핸드폰이나 PDA같은 장비일 경우 암호화에 따른 부담이 심하게 된다. 그러므로 추가적으로 더욱더 강력한 보안기능을 가진 구조를 설계하고, 또 핸드폰이나 PDA같은 프로세서 파워가 적은 모바일 노드에서도 무난히 동작할 수 있는 가벼운 보안기능을 설계해야 한다.

참 고 문 헌

[1] Y.-C. Shim, H.-A. Kim and J.-I. Lee, “Design and Evaluation of a New Micro-mobility Protocol in Large Mobile and Wireless Networks,” ICCSA, LNCS3480, 2005.

[2] 강호석, 심영철, “대규모 마이크로 모빌리티 환경에서의 멀티캐스트 프로토콜의 구현과 평가”, 정보처리학회 논문지 제15-C 1호, pp.51-60, 2008년 2월.

[3] Ho-Seok Kang and Young-Chul Shim, “Design and Evaluation of a New Multicast Protocol in Micro-Mobility Environmnets,” WSEAS ACOS’07 pp.549-553, April, 2007.

[4] Ho-Seok Kang and Young-Chul Shim, “Secure Multicasting in Micro-Mobility Environments,” ICN’05, LNCS3421 pp.868-875, April, 2005.

[5] L. Gong, “Enclaves: Enabling Secure Collaboration over The Internet,” IEEE J. Select. Areas Communications, pp.567 - 575, Apr., 1997.

[6] “Group key Management Protocol (GKMP) Specification,” RFC2093, July, 1997.

[7] D. R. Stinson, “On Some Methods for Unconditionally Secure Key Distribution and Broadcast Encryption,” Design, Codes and Cryptography, Vol.12, Issue 3, pp.215-243, 1997.

[8] H. Harney and C. Muckenhirn, “Group key Management Protocol (GKMP) Architecture,” RFC 2094, July, 1997.

[9] D. Bruschi and E. Rosti “Secure Multicast in Wireless Networks of MobileHosts: Protocols and Issues,” Mobile Networks and Applications, Vol.7, 2002.

[10] S. Mittra, “Iolus: A Framework for Scalable Secure Multicasting,” ACM SIGCOMM’97, pp.277-288, 1997.

[11] C. Wong, M. Gouda and S. Lam, “Secure Group Communications using Key Graphs,” ACM SIGCOMM Conf., 1998.

[12] C. Shields, J.J. Garcia-Luna-Aceves, “KHIP - A Scalable Protocol for Secure Multicast Routing,” ACM SIGCOMM Conf., 1999.

[13] Sanjeev Setia and Samir Koussih and Sushil Jajodia, “Kronos: A Scalable Group Re-keying Approach for Secure Multicast,” IEEE Symposium on Security and Privacy, 2000.

[14] 은상아외 5, “안전한 멀티캐스트 서비스 제공을 위한 효율적인 그룹 관리 메커니즘 및 구조”, 정보처리학회 논문지, 제9-C권 제3호 pp.323-330, 2002년 6월.

[15] 김태연, 김영균, “대규모 동적 그룹에서 안전한 멀티캐스트를 위한 키 분배 프로토콜”, 정보처리학회 논문지 제9-C권 제4호 pp.597-604, 2002년 8월.

[16] 심영철외 5, “멀티캐스트 키 분배 메커니즘 설계 및 구현에 관한 연구,” 한국 전자통신 연구원, 1999년.

[17] C. Perkins, “IP Mobility Support,” RFC 2002, Mobile IP Networking Group.

[18] A.G. Valki, “Cellular IP: A New Approach to Internet Host Mobility,” Computer Communications Rev., Jan., 1999.

[19] R. Ramjee et al, “HAWAII: A Domain-Based Approach for Supporting Mobility in Wide-Area Wireless Networks,” IEEE/ACM Trans. on Networking, Vol.10, No.3, June, 2002.

[20] T. Harrison, C. Williamson, W. Mackrell & R. Bunt, “Mobile Multicast(MoM) Protocol: Multicast Aupport for Mobile Host,” ACM MOBICOM’97 pp.151-160, 1997.

[21] Y.-J. Suh, H.-S. Shin and D.-H. Kwon, “An Efficient Multicast Routing Protocol in Wireless Mobile Networks,” Wireless Networks, Vol.7, pp.443-453, 2001.

[22] A.J. Ballardie, “Core Based Trees Multicast Routing Architecture,” RFC2201, Sept., 1997.

[23] The Network Simulator - NS2, http://www.isi.edu/nsnam/ns

강 호 석

e-mail : hskang@cs.hongik.ac.kr

2000년 홍익대학교 컴퓨터정보통신학과 (학사)

2002년 홍익대학교 대학원 전자계산학과 (이학석사)

2008년 홍익대학교 대학원 컴퓨터공학과 (공학박사)

관심분야 : 무선 네트워크, 네트워크 보안, 센서 네트워크 등

심 영 철

e-mail : Shim@cs.hongik.ac.kr

1979년 서울대학교 전자공학과(학사)

1981년 한국과학기술원 전기 및 전자 공학과(석사)

1991년 University of California, Berkeley 전산학(박사)

1993년~현 재 홍익대학교 컴퓨터공학과 교수

관심분야 : 무선이동 네트워크, 보안, 유비쿼터스 컴퓨팅 등