안전한 마이크로모빌리티 환경에서의 멀티캐스트

강호석*, 심영철*
*홍익대학교 컴퓨터공학과
e-mail:{hskang, shim}@cs.hongik.ac.kr

Secure Multicasting in Micro-Mobility Environment

Ho-Seok Kang*, Young-Chul Shim*
*Dept of Computer Engineering, Hongik University

요 약

핸드오프가 자주 발생할 경우 모바일IP에서 제어 메시지가 많이 발생하게 된다. 이러한 문제를 해경하기 위해서 마이크로 모빌리티 프로토콜이 제안되었다. 이 논문에서 마이크로 모빌리티 환경에서 안전한 멀티캐스팅 서비스를 제공하기 위한 방법에 대해 소개한다. 먼저 마이크로 모빌리티 환경에서의 멀티캐스팅 서비스 프로토콜을 소개하고 이 프로토콜을 기반으로 보안 서비스를 추하한다. 제안된 멀티캐스트 라우팅 프로토콜은 공유 멀티캐스트 트리를 만들고 다른 유니캐스트 마이크로 모빌리티 프로토콜을 고려하지 않는다. 추가된 보안 서비스는 인증, 권한, 기밀성, 그리고 완전무결성이 대칭이나 비대칭 암호와 알고리즘을 기반으로 하여 포함되어 있다. 또한 보안 프로토콜은 그룹의 멤버가 자주 바뀌고 핸드오프가 일어나는 현상을 다루기 위하여 페이징 지역을 기준으로 계층적 키 구조를 사용한다.

1. 서론

멀티캐스팅(Multicasting)은 많은 응용 분야에 사용되어 왔고 인터넷에서 새로운 서비스가 개발되면 앞으로도 더 중요한 분야로 발전해 나갈 것이다. 또 많은 응용분야에서 안전한 멀티캐스트 서비스를 요구한게 된다. 최근에 통신 네트워크와 모바일 장비가 발전하면서 무선과 모바일 네트워크의 성장이 급속하게 이루어 졌다. 모바일IP(Mobile IP)는 현재 IP 네트워크에서 매크로 모빌리트(Macro-Mobility)를 지원하는 표준으로 사용자들에게 자신의 홈 네트워크(Home Network)에서 외부로 연결해주는 기능을 지원하고 있다. 만약 모바일 노드의 움직임이 많은 경우, 이러한 등록과정이 복잡한 모마일IP특성 때문에 과중한 부하(overload)를 주게 된다. 이러한 모빌리티 관리(Mobility Management)로 인한 부하를 줄이기 위해서, 마이크로 모빌리티(Micro-Mobility) 프로토콜들이 제안되었다.

이 논문에서는 먼저 마이크로 모빌리티 환경에서의 멀티캐스팅 서비스 프로토콜을 소개하고 이 프로토콜을 기반으로 보안 서비스를 추하한다. 보안 프로토콜은 그룹의 멤버가 자주 바뀌고 핸드오프가 일어나는 현상을 다루기 위하여 페이징 지역을 기준으로 계층적 키 구조를 사용한다.

이 논문의 구성은 2장에서 관련연구, 3장에서 마이크로 모빌리티 환경에서의 멀티캐스트 라우팅 프로토콜에 대하여 설명. 4장은 3장에서 설명한 라우팅 프로토콜에 보안 서비스를 제공하는 프로토콜을, 마지막으로 5장에서는 결론을 제시한다.

2. 관련연구

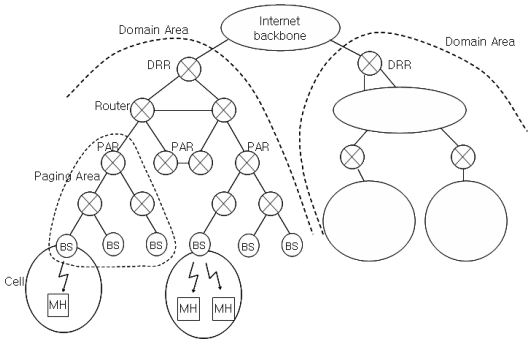
IETF는 모바일 멀티캐스트를 지원하기 위하여 바이-디렉셔널 터널링(bi-directional tunneling)과 원격 가입(Remote subscription)의 두 가지 방법을 제시하였다. 바이-디렉셔널 터널링 방법은 모바일 노드로의 데이터 전달을 홈 에이전트(Home Agent)가 수행한다. 이 홈 에이전트는 멀티캐스트 패킷들을 전달하는 에이전트 역할을 하게한다. 이 방법은 한 FN(Foreign Network)에 도착하는 패킷이 중복된

본 연구는 정보통신부 및 정보통신 진흥원의 대학 IT연구센터 육성.지원사업의 연구결과로 수행되었음

멀티캐스트 패킷이 많이 발생하는 네트워크 터널 집중 문제(Tunnel Convergence Problem)을 가져온다. Harrison은 하나의 HA(홈 에이전트, Home Agent)에서만 FN으로 전달하는 방법으로 바이-디렉셔널 터널링의 터널 집중문제를 해경하는 MoM을 제안하였다. 나중에 RBMoM과 MMA와 같은 프로토콜도 제안되었다.

안전한 멀티캐스트를 구현하기 위해서는 새로운 멤버는 그 그룹에 참여하기 전에 주고받은 패킷을 읽을 수 없게하고(backward secrecy) 탈퇴한 멤버는 그룹을 떠난 후에 주고받은 패킷을 절대 읽을 수 없어야 한다(forward secrecy). 이것은 메시지(패킷)를 암호화 하는 키가 그룹의 멤버가 변경될 때마다 변해야한다는 것을 의미한다. Mittra는 멀티캐스트 도메인의 계층에 기반을 둔 키 분배 방법을 제안하였다. Wong은 암호키의 계층화를 기반으로 하는 키 분배 알고르즘을 소개하였다. 모든 이러한 분야의 작업은 단지 특정 그룹을 위한 키 분배 방법만을 제시하였고 다른 멀티캐스트 보안 서비스에는 제공하지 못한다. Shields와 Garcia-Luna-Aceves는 안전한 멀티캐스팅을 위한 유연한 프로토콜을 제안하였다. 이 제안된 메커니즘은 HIP이라고 불리는 계층적 멀티캐스트 라우팅 알고리즘에 의해 모바일 노드로부터 측정된 다양한 공격적인 요소를 측정하여 보호를 위한 측정값을 제공한다.

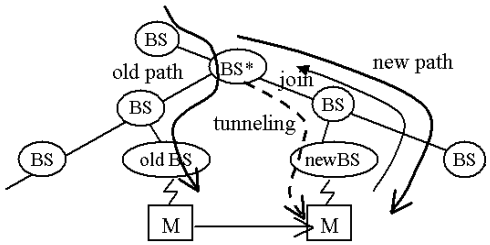
3. 멀티캐스트 구조



(그림1) 멀티캐스트 트리 구조

(그림 1)에서와 같이, 마이크로 모빌리티 도메인은 도메인 루트 라우터(DRR, Domain Root Router)와 연결되어 있는 페이징 영역(Paging area)이 여러개 모여서 구성되어 있다. 페이징 영역은 많은 셀들로 구성되어 있고 각 셀은 베이스 스테이션(BS, Base Station)에 의해 관리되고 있다. BS들의 집합으로 구성된 페이징 영역은 트리의 상위에 페이징 영역 라우터(PAR, Paging Area Router)에 연결되어 있다. PAR들은 여러 라우터들의 연결을 통해서 마이크로 모빌리티 도메인의 DRR에 연결되어 있다. 페이징 영역의 목적은 모바일 노드들의 핸드오프시 요구되는 제어 메시지들을 감소시키기 위해서 이다.

리시버로써 멀티캐스트 그룹에 참여하기를 원하는 모바일 노드는 BS에게 알린다. BS는 참여 요청(Join Request)을 코어(Core)에게 보낸다. 참여 메시지는 코어에게 도착하거나 혹은 멀티캐스트 트리 노드(BS 혹은 라우터)에게 도착할 때까지 상위로 올라간다.



(그림 2) 페이징 지역 내에서 발생하는 핸드오프

핸드오프는 세 가지의 경우가 있다. 페이징 지역 내의 핸드오프, 페이징 직역 외부에서의 핸드오프, 그리고 도메인 외부에서 발생하는 핸드오프이다.

```
M notifies the new BS of its arrival;
if (M is the first group member in the new BS) {
    The new BS requests the crossover BS
        (starred BS in the figure) of the old
        and new BSs to tunnel multicast packets
        so that it can relay to M;
    The new BS connects to the multicast tree
        by sending a join request;
    After receiving join ack, the new BS asks
        the crossover BS to stop tunneling;
    /* Now multicast packets arrive through
        the new path */ }
Else { /* The new BS is already connected to the tree.
        So there is nothing to do */ }
```

4. 안전한 멀티캐스트

이번 장에서는 앞장에서 설명한 멀티캐스트 라우팅 프로토콜에 보안 서비스를 추가한 프로토콜을 설명한다. 보안 프로토콜을 설계할 경우에는, BS들과 라우터들이 제어 신호를 전달할 경우와 키를 계층적으로 관리할 경우 모두 신뢰를 바탕에 두어야 한다. 그러나 이러한 것들은 데이터를 접근하기 위한 허락을 받지 못한 상태이다. 이번 장에서는 아래와 같은 표기법(Notation)을 사용하고, 구성요소의 존재를 가정한다.

- PK-N: 노드 N의 공개 키
- SK-N: N의 비밀 키

- $CERT_N$: N의 인증서
- D^K: K라는 키로 메시지 D를 암호화 한 경우
- $\{D\}^{SK-N}$: N의 비밀키를 이용하여 메시지 D를 서명한 메시지와 함께 암호화함.
- AS(Authorization server): 요청을 받아서 케퍼빌리티(Capability)를 결정하는 역할을 한다.
- GI(Group initiator): 멀티캐스트 그룹을 처음 만드는 역할을 한다.

안전한 멀티캐스 프로토콜을 설명하기 전에, 우선 프로토콜에 사용되는 키에 대하여 설명한다. 모든 노드 N은 공개/비밀 키 쌍을 가지고 있다. 또 모든 노드는 AS의 공개키인 PK-AS를 안다고 가정한다. 멀티캐스트 그룹이 만들어질 때, 그룹 초기자는 하나의 그룹키인 GK를 생성하고 노드들이 그룹이 참여할 때 모든 권한을 가진 그룹 멤버들에게 분배한다. 잦은 멤버의 변경이나 핸드오프로 인하여 발생하는 백워드 비밀성과 포워드 비밀성을 효율적으로 지원하기 위하여 페이징 지역에 있는 PAR과 모든 그룹멤버의 모바일 노드들은 [그림 3]에서 보는 것과 같은 계층적인 키를 유지한다. 하나의 키 계층은 각각의 페이징 지역에 있는 멀티캐스트 그룹에서 유지한다. PAR은 키 서버가 되고 키 계층에 있는 모든 키들을 생성하고, 저장하고, 수정하게 된다. 모바일 노드는 루트 키(Root Key)에서 리프 키(Leaf Key)까지의 경로에 있는 모든 키를 저장한다.

4.1 그룹 생성

그룹 생성은 그룹 초기자인 GI에서 시작된다. GI는 ACL을 AS에게 보낸다. ACL은 누가 GI이고 센더나 리시버에게 보낼 수 있는지를 알려준다. AS는 이 ACL 리스트에서 없는 케퍼빌리티를 만든다. 멀티캐스트 주소가 MA인 멀티캐스트 그룹의 ACL에 따라서 수신을 한다. AS는 GI에게 보내게 된다. GI는 멀티캐스트 그룹의 코어를 선택하고 코어의 주소인 IP_{CORE}를 저장하고 그룹키인 GK를 생성한다.

4.2 참가(Join)

멤버 M이 그룹에 참가하기를 원하면 GI에 연결을 하여 인증을 수행한다. 그리고 케퍼빌리티를 받고, 코어의 주소와 그룹키를 받는다. 만약 M이 센더일 경우에는 데이터 암호 키라고 불리는 대칭키 DK를 생성한다. 대칭키는 M으로부터 패킷들을 멀티캐스트 전송을 하기위해 암호화 하는데 사용된다. 센더는 그 자신의 DK를 가지고 있다. M은 다음의 메시지를 셀 안에 있는 BS에게 보내게 된다: $\{Join, IP_M, MA, CAP_M\}^{SK-M}$.

4.3 탈퇴(Leave)

그룹에서 탈퇴하기를 원하는 멤버 M은 셀 안에 있는 BS에게 다음의 메시지를 보낸다: $\{Leave, IP_M, MA, CAP_M\}^{SK-M}$. 이 메시지를 받고 나서 BS는 다음과 같은 작업을 한다.

```
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;
```

4.4. 패킷 전송(Packet delivery)

만약 멤버 M이 메시지 D를 가지고 그룹과 멀티캐스트를 하려고 한다면, 우선 D를 데이터 암호화키인 DK로 암호화한고 비밀키를 가지고 암호화한 메시지에 서명을 한다. 그리고 GK와 SGK1을 이용하여 DK를 이중으로 암호화한다: $\{D^{DK}\}^{SK-M}$, $(DK^{GK})^{SGK1}$. 이 패킷은 우선 M의 BS로 보내진다. 패킷이 실제로 BS가 기억하는 M의 케퍼빌리티를 검사하여 패킷들을 확인하므로 해서 실제로 생성된 키인지를 검사할 수 있다. 이 메시지는 페이징 영역 안에서의 멀티캐스트이다. 패킷이 PAR1에 도착하게 되면 페이징 영역의 밖으로 나가게 되는데, PAR1은 DK를 SGK1을 이용하여 복호화 하고 페이징 영역의 밖으로 다음과 같은 형태로 보내게 된다: $\{D^{DK}\}^{SK-M}$, DK^{GK}. BS들과 PAR들은 이러한 패킷을 처리하고 포워딩 할 수는 있지만 그룹키인 GK를 가지고 있지 않기 때문에 메시지 D를 읽을 수는 없다는 점에 유의를 해야 한다. SGK2를 가지고 있는 다른 페이징 영역의 PAR2에 패킷이 도착하게 되면 다시 DK를 SGK2로 암호화 하고 이 새로운 페이징 영역에 다음과 같이 멀티캐스트 하게된다: $\{D^{DK}\}^{SK-M}$, $(DK^{GK})^{SGK2}$. 새로운 페이징 영역에 있는 멤버들은 모두 GK와 SGK2를 가지고 있기 때문에 이 패킷을 읽을 수 있다.

4.5 Handoff

모바일 노드 M이 BS와 PAR이 BS1과 PAR1인 예전의 셀로부터 새로운 셀인 BS2와 PAR2로 움직일 경우를 고려한다. 페이징 영역 내에서의 핸드오

프일 경우 PAR1과 PAR2가 같다. 막약 핸드오프가 한 도메인에서 페이징 영역간이거나 도메인 간에 일어난 경우라면 PAR1과 PAR2가 다르게 된다. M이 새로운 셀로 움직일 때 다음과 같은 패킷을 BS2에게 보낸다: {handoff, IP_M, MA, CAP_M, BS1, PAR1}$^{SK-M}$. 패킷의 안정성을 검사한후에 BS2는 메시지를 저장하고 다음과 같은 작업을 수행한다.

```
If (PAR1=PAR2) {
   /* intra paging-area handoff so no need to
      change the key hierarchy */
   If (M is the first member of the new cell) {
      Request crossover BS of BS1 and BS2
         to forward multicast packets to M;
      Send Join request toward the core;
      Receive Join-ack;
      Request the crossover BS to stop forwarding }
   Else {
      /* BS2 can deliver multicast packets to M,
         so there is nothing to do */ }
Else /* either inter-paging area or inter-domain
         handoff */ {
   Request PAR1 to forward packets to M;
   Request PAR2 to change the key hierarchy
         within the new paging area;
   If (M is the first member of the new cell) {
      Send Join request toward core;
      Receive Join ack; }
   Request PAR1 to stop forwarding packets; }
```

만약 핸드오프가 같은 페이징 영역에서 이루어진 것이라면, 키 계층은 아무것도 변할 필요가 없다. 그래서 만약 새로운 BS가 이미 멀티캐스트의 그룹 멤버라면 M은 새로운 BS로부터 패킷을 받으면 된다. 그렇지 않으면 새로운 BS가 그룹에 가입할 때까지 교차 BS로부터 패킷들을 받는다. 만약 M이 다른 페이지 영역으로 이동한 것이라면, M은 예전의 페이징 영역의 키 계층 안에서의 키들을 가지고 있기 때문에 예전의 페이징 영역으로부터 패킷들을 받아야 한다. M은 새로운 페이징 영역으로부터 M이 새로운 페이징 영역의 새로운 키 계층의 키를 받고 새로운 BS가 그룹에 가입한 후에 패킷들을 받는다.

5. 결론

모바일 IP에서, 모바일 노드의 잦은 핸드오프는 등록을 포함한 위치 관리로 인하여 제어 메시지의 심각한 오버헤드를 야기 시킨다. 이러한 제어 메시지의 오버헤드를 감소시키기 위하여 마이크로 모빌리티 프로토콜이 제안되었다. 이 논문에서는 마이크로 모빌리티 환경에서의 안전한 멀티캐시팅 서비스들을 효율적으로 제공하기위한 프로토콜을 제시하였다. 먼저 마이크로 모빌리티 환경에서의 멀티캐스트 라우팅 프로토콜을 소개하였다. 여기에 제안된 멀티캐스팅 서비스에 보안 서비스를 추가하는 프로토콜을 제시하였다. 이 추가된 보안 서비스는 인증, 권한, 기밀성, 그리고 완전무결성이 대칭이나 비대칭 암호와 알고리즘을 기반으로 하여 포함되어 있다. 또 페이징 영역에서 빈번한 멤버의 변화나 핸드오프에 로 인한 백워드 기밀성과 포워드 기밀성을 효율적으로 제공하기 위하여 키 계층 메커니즘을 사용하였다.

참고문헌

[1] S. Das et al: TeleMIP: Telecommunications - Enhanced Mobile IP Architecture for Fast Intradomain Mobility. IEEE Personal Communications, August 2000.

[2] T. Harrison, C. Williamson, W. Mackrell & R. Bunt: Mobile Multicast (MoM) Protocol: Multicast Support for Mobile Hosts. Proc. of ACM MOBICOM, 1997.

[3] C. R. Lin & K.-M. Wang: Scalable Multicast Protocol in IP-Based Mobile Net-works. Wireless Networks, 8, 2002.

[4] S. Mittra: Iolus: A Framework for Scalable Secure Multicasting. Proc. of ACM SIGCOMM Conf., 1997

[5] R. Ramjee et al: HAWAII: A Domain-Based Approach for Supporting Mobility in Wide-Area Wireless Networks. IEEE/ACM Trans. on Networking, 10(3), June 2002.

[6] C. Shields, J.J. Garcia-Luna-Aceves: KHIP - A Scalable Protocol for Secure Multi-cast Routing. Proc. of ACM SIGCOMM Conf., 1999.

[7] Y.-C. Shim & S.-K. Kang,: New Center Location Algorithms for Shared Multicast Trees. Networking 2002, LNCS 2345, 2002.

[8] Y.-J. Suh, H.-S. Shin, & D.-H. Kwon: An Efficient Multicast Routing Protocol in Wireless Mobile Networks. Wireless Networks, 7, 2001.

[9] C. Wong, M. Gouda, & S. Lam: Secure Group Communications using Key Graphs. Proc. of ACM SIGCOMM Conf., 1998.

[10] G. Xylomnenos & G. Polyzos: IP Multicast for Mobile Hosts. IEEE Communications Magazine, Jan. 1997