보안 이동 멀티캐스트를 위한 키 관리 방법

노종혁 진승헌

한국전자통신연구원, 정보보호연구단

{jhroh, jinsh}@kiss.or.kr

Key Management Scheme for Secure Mobile Multicast

Jong-Hyuk Roh° Seunghun Jin

Information Security Research Division, ETRI

요 약

멀티캐스트 환경에서 비밀키를 관리하는 방법은 많은 연구가 이루어져 왔지만, 대부분 유선 환경에 집중되어 있다. 본 논문에서는 이동 호스트를 지원하는 멀티캐스트 환경을 위한 두 개의 키관리 방법을 제안한다. 하나는 무선 네트워크 구조를 반영하는 트리 기반의 키 관리 방법이다. 다른 하나는 무선 영역과 유선 영역을 구분하여 키를 관리한다. 유선 영역은 기존의 논리적 키 관리 방법을 사용하고 무선 영역은 각 셀마다 독립적으로 하나의 그룹키를 관리한다.

1. 서 론

다수를 대상으로 한 실시간 멀티미디어 통신의 필요성이 나날이 대두됨에 따라, 현재 인터넷의 네트워크 자원과 구조적 한계를 극복하기 위한 여러 제안과 시도가 진행되고 있다. 대표적으로 네트워크 자원을 절약하고 효율적으로 다수의 수신자들에게 데이터를 전송하는 멀티캐스트는 차세대 인터넷의 중요한 역할을 할 것으로 기대된다. 이와 동시에, 무선환경에서의 이동성에 대한 연구 또한 활발히 진행되고 있다.

유료 시청, 실시간 증권정보 서비스 등 많은 멀티캐스트 응용은 인가된 사용자에게만 멀티캐스트 컨텐츠에 접근하기 위한 메커니즘이 요구된다. 이는 적법한 그룹 멤버들만 비밀키를 공유하도록 하여 멀티캐스트 데이터를 암호화 하면 된다.

멀티캐스트 환경에서 비밀키를 관리하는 방법은 많은 연구가 이루어져 왔지만, 대부분 유선 환경에 집중되어 있다. 무선 환경에 적합한 키 관리 방법은 많은 연구가 이루어 지지 않았다[7].

일반적으로 트리 기반의 멀티캐스트 키 관리 방법은 네트워크 구조와 무관하게 논리적으로 구성 되어있다. 하지만, [5]에서 네트워크 구조와 키 관리 방법에 관한 연관성을 설명하고, 구조에 적합한 키 관리 방법을 제안하였다. 본 논문에서도 이동 멀티캐스트 환경에 적합한 키 관리 방법을 제안하여 키갱신 메시지 전달을 지역적으로 집중화시켜 전송선 비용을 줄이도록 하였다.

본 논문에서는 두 개의 키관리 방법을 제안한다. 하나는 무선 네트워크 구조를 반영하는 트리 기반의 키 관리 방법이다. 다른 하나는 무선 영역과 유선 영역을 구분하여 키를 관리한다. 유선 영역은 기존의 논리적 키 관리 방법을 사용하고 무선 영역은 각 셀마다 독립적으로 하나의 그룹키를 관리하는 방식이다. 본 논문에서는 이 두 방법을 설명하고 여러 환경에서 장단점을 비교한다.

2. 보안 고려 사항

멀티캐스트는 기본적으로 언제나 사용자가 그룹에 가입하고 탈퇴할 수 있도록 되어 있다. 그러므로, 어느 누구나 멀티캐스트 데이터를 수신할 수 있다. 그러나, 특정 응용에서는 인가된 사용자만이 서비스를 받길 원하고 있다. 이를 해결하기 위한 방법은 그룹 멤버들이 비밀키를 공유하도록 하여, 데이터의 기밀성을 제공하면 된다. 이러한 환경에서, 새로운 사용자가 그룹에 가입하였을 때, 과거의 데이터에 접근을 하지 못하도록 멤버들이 공유하고 있는 그룹키를 갱신하여야 한다(Backward Secrecy). 또한, 그룹을 탈퇴한 멤버는 더 이상 멀티캐스트 데이터를 복호화하지 못하도록 그룹키를 갱신하여야 한다(Forward Secrecy) [2].

이러한 보안 멀티캐스트 환경에 이동 환경이 접목되면 호스트의 이동성으로 인한 보안 고려 사항이 발생한다. 현재 Mobile IP 멀티캐스트 프로토콜에는 bi-directional tunneling과 remote subscription 방법이 있다. Bi-directional tunneling은 홈 에이전트가 이동 호스트가 위한 곳으로 터널링을 통하여 유니캐스트로 멀티캐스트를 지원하는 방법이다. Remote subscription은 이동 호스트가 다른 무선 영역으로 이동했을 경우 이동 호스트가 위치한 무선 영역(Foreign network)에서 멀티캐스트를 받는 방법이다. 이동 멀티캐스트에 관한 대부분의 연구는 이 두 가지 방법을 조합해 사용함으로써 전송 지연을 최소화하는 방안을 제안한다. 즉, 멀티캐스트 데이터의 이동 경로를 줄이거나, 멀티캐스트 전송 트리 재구축 횟수를 줄이기 위한 방법이다[3].

본 논문은 이동 멀티캐스트 환경에서 보안 문제를 해결하기 위한 방법을 제안한다. 만약에 bi-directional tunneling만을 사용한다면, 전통적인 키관리 방법이 사용될 수 있다. 홈 에이전트를 호스트로 간주한다면, 유선 멀티캐스트 환경과 별다른 차이가 없기 때문이다. 그러므로, 본 논문에서는 새로운 무선 영역으로 이동하면, 새 영역의 BS(Base Station)으로부터 데이터를 전송 받는 것으로 한다. 또한, 멀티캐스트 트리 재구성에 대해서는 논하지 않는다.

다음은 보안 이동 멀티캐스트에서 다루어야 할 요소들이다.

- Forward/backward secrecy (Host join/leave): 현재 적법한 멤버들만이 멀티캐스트 데이터에 접근할 수 있다.
- Host mobility: 호스트 이동으로 인해 멤버쉽 변화가 발생할 수 있으며, 이에 따른 키갱신 작업이 요구된다.
- BS join/leave: 호스트의 이동으로 인해, BS 또한 멀티캐스트 그룹에 가입/탈퇴를 한다.

3. 제안 프로토콜

그림 1은 이동 멀티캐스트 환경을 보여준다. 네트워크는 유선 영역과 무선 영역으로 이루어져 있다. 유선 영역에는 멀티캐스트 그룹을 관리하는 GM (group manager)과 멀티캐스트 라우터, BS로 이루어진다. 멀티캐스트 라우팅 프로토콜은 DVMRP, CBT, PIM 등이 사용된다. 무선 영역은 BS와 이동 호스트로 이루어져 있다. GM은 신뢰 서버로, 멀티캐스트 멤버의 인증, 인가 작업을 수행하고 보안을 위해 그룹키를 관리하며 BS들을 관리한다. BS는 자신이 위치한 무선 영역의 멀티캐스트 멤버들에게 멀티캐스트 데이터를 전송하고, 영역의 멤버들을 관리한다[6].

Ri는 i번째 무선 영역을 나타내고 BS Bi에 의해 관리된다. 이동 호스트 Mx는 자신이 위치하는 무선 영역의 BS에 등록한다. 무선 영역에는 이동 호스트가 없거나 복수개가 존재할 수 있다. Ri에 있는 Mx가 멀티캐스트 그룹에 가입하면 Bi는 멀티캐스트 그룹에 가입을 하여야 한다. 멀티캐스트 트리는 Bi가 멀티캐스트 데이터를 전송 받을 수 있도록 재구축되어야 한다. Ri에 멀티캐스트 멤버가 하나도 존재하지 않게 되면, Bi는 멀티캐스트 그룹을 탈퇴한다.

본 논문은 이러한 이동 멀티캐스트 환경에 적합한 두 개의 키관리 방법을 제안한다. 하나는 KTMM (Key Tree in Mobile Multicast)으로, Mobile IP 네트워크 구조를 따르는 트리 기반의 키관리 방법이다. 다른 하나는 WSMM (Wireless Subgroup in Mobile Multicast)으로, 키관리를 유선과 무선으로 나누어 처리하는 방법이다.

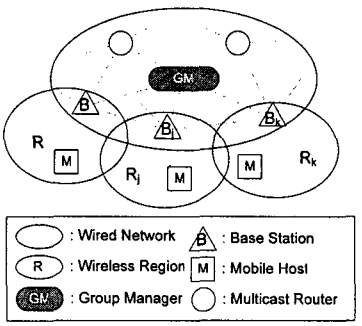

그림 1 이동 멀티캐스트 환경

두 방법을 설명하기에 앞서, 이동 멀티캐스트 환경에 기존의 LKH (Logical Key Hierarchy)를 사용한 경우에 대해서 설명한다. LKH는 네트워크 구조와 독립적이다. 키트리의 서브그룹 멤버들은 실제 네트워크에서는 근접한 지역에 존재하지 않는다. 즉, 키트리의 서브그룹 멤버들이 서로 다른 무선 영역에 위치할 수 있다는 것이다. 멤버쉽이 변경되면, 각 서브그룹별로 키갱신 메시지들이 생성된다. 다른 무선 영역에 위치하고 있는 서브그룹 멤버들에게 메시지를 전달하기 위하여 키갱신 메시지는 여러 번 복사되어야 하고 각각 다른 지역으로 전송되어야 한다. 이러한 문제를 해결하기 위해, 본 논문에서는 네트워크 구조를 반영하는 키관리 방법을 제안한다.

3.1 KTMM

KTMM은 이동 네트워크 환경에 적합한 키관리 트리를 제공한다. 그림 2는 KTMM의 키관리 트리를 보여준다. 키트리의 가장 아래 레벨은 무선 영역의 BS와 이동 호스트간의 관계를 의미한다. 서브그룹 k-node 중 최하위의 k-node는 BS와 이동 호스트간에 공유하는 키를 의미한다. 즉, 한 무선 영역을 서브그룹으로 구성하고, 그 외 부분은 기존의 키관리 구조처럼 네트워크 환경에 독립적이다. 그러므로, 일반적인 키관리 트리의 차수는 고정되어 있지만, KTMM의 키트리의 최하위 레벨의 차수는 제한을 두지 않도록 한다.

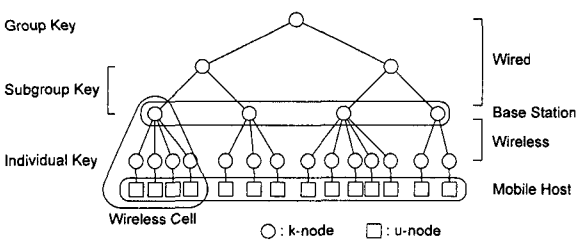

그림 2 KTMM의 키관리 트리

Multicast Data Transmission. 모든 그룹 멤버들은 데이터 전송을 위해 하나의 그룹키 kg를 공유한다. 송신자는 kg로 데이터를 암호화하고 수신자들은 kg로 데이터를 복호화한다.

Host Handoff. 그림 3은 KTMM에서 핸드오프를 보여준다. 이동 호스트 Mx가 Ri에서 Rj로 이동하면, Bj는 Mx를 인증한 후, Rj에서 공유되고 있는 서브그룹키를 Mx에게 전송한다. Bj가 그룹 멤버가 아니라면, Bj는 멀티캐스트 그룹에 가입하여야 한다. Mx가 이동한 후, Ri에 멤버가 존재하지 않게 되면, Bi는 멀티캐스트 그룹을 탈퇴한다. 핸드오프 과정을 거친 Mx는 Bi, Bj에 속한 서브그룹키를 모두 소유하게 된다. 그림 3 (b)는 이에 해당하는 키트리의 변화를 보여준다.

BS Join/Leave. 이동 호스트 Mx가 Ri에서 그룹 가입 메시지를 전송하였을 때, Bi가 그룹 멤버가 아니라면, Mx의 그룹 가입 보다 Bi의 그룹 가입이 먼저 이루어진다. GM은 Bi와 비밀키를 교환한 후, Ri에서 사용될 서브그룹키를 생성하고 이에 해당하는 k-node를 생성한다. 그리고 k-node를 기존의 키관리 트리에 접목시킨다. GM은 Bi의 k-node부터 키관리 트리의 루트 노드까지에 해당하는 키들을 Bi에게 전송한다. 멀티캐스트 전송 트리 또한 재구축되어야 한다.

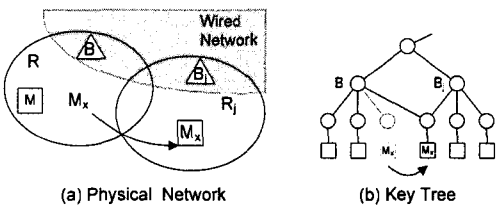

그림 3 KTMM의 핸드오프 처리

Ri에 그룹 멤버가 존재하지 않게 되면, Bi는 GM에게 그룹 탈퇴 메시지를 전송한다. GM은 Bi에 해당하는 k-node를 삭제함으로써 키관리 트리를 수정한다. 멀티캐스트 전송 트리 또한 수정된다.

Host Join. 이동 호스트 Mx가 Ri에서 그룹 가입 메시지를 전송하면, GM은 Mx의 비밀키(individual key)를 공유한다. GM은 Mx에 해당하는 u-node와 k-node를 생성하고, Bi의 k-node에 Mx의 k-node를 연결한다. Backward secrecy를 보장하기 위해 GM은 새로운 그룹키를 생성한다. GM은 새 그룹키를 기존의 그룹키로 암호화한 후, 그룹 멤버들에게 멀티캐스트 한다. 그리고, GM은 Mx에게 그룹키와 서브그룹키를 비밀키로 암호화하여 전송한다.

Host Leave. 이동 호스트 Mx가 그룹 탈퇴 메시지를 전송하면, GM은 Mx의 u-node와 k-node를 삭제함으로써 키관리 트리를 수정한다. Forward secrecy를 보장하기 위해, Mx가 소유하고 있는 모든 키는 변경되어야 한다. Mx가 소유하고 있는 키들은 키관리 트리에 표현되어 있다. GM은 남아 있는 멤버들에게 [1]의 user-oriented 키갱신 방법을 사용하여 변경된 키를 전송한다. Mx가 많은 무선 지역을 이동할수록, 변경해야 할 서브그룹 키가 많아진다.

3.2 WSMM

WSMM은 멀티캐스트 그룹을 무선 영역과 유선 영역으로 구분한다. 각 무선 영역은 자체적인 서브그룹을 구성한다. 각 BS는 자신이 관리하는 영역의 이동 호스트들을 관리하고, 관리 영역에서 사용되는 서브그룹 키를 생성하고 관리 영역의 이동 호스트와 공유한다. 유선 영역은 BS를 멀티캐스트 멤버로 간주하여 기존의 LKH를 그대로 이용한다. GM은 그룹키를 생성하고 BS들과 공유한다. GM은 이동 호스트들의 그룹 가입/탈퇴를 처리하지만, 이동 호스트의 위치에 대해서는 관심을 갖지 않으며 이동 호스트의 그룹키 관리는 BS에게 위탁한다. 그림 4는 WSMM의 키관리 구조를 보여준다.

WSMM에서는 키관리를 무선과 유선으로 나누어서 관리하므로, 데이터 전송을 위해 유선 그룹키와 무선 서브그룹키 모두 사용된다. 그러므로 BS에서 멀티캐스트 데이터를 재암호화하는 과정이 필요하다. 멤버쉽이 변하면, 이에 해당하는 무선 영역에서만 키갱신이 이루어진다.

Multicast Data Transmission. 송신자는 자신이 속해있는 무선서브그룹키로 데이터를 암호화하여 BS에게 전송한다. BS는 데이터를 복호화한 후, 유선 그룹키로 데이터를 암호화하여 멀티캐스트 한다. 데이터를 수신 받은 다른 BS들은 유선 그룹키로 데이터를 복호화한 후, 자신이 속해있는 무선 서브그룹키를 암호화하여 무선 영역에 브로드캐스트 한다. 수신자는 무선 서브그룹키로 복호화한다. 즉, WSMM에서 멀티캐스트 데이터 전송은 두번의 재암호화 과정이 필요하다.

BS Join/Leave. 이동 호스트 Mx가 Ri에서 멀티캐스트 그룹에 가입을 요청하게 될 때, Bi가 그룹 멤버가 아니라면, 우선 Bi가 먼저 멀티캐스트 그룹에 가입을 하여야 한다. GM은 Bi와 비밀키를 공유하고 Bi에 해당하는 k-node와 u-node를 생성한 후 키관리 트리를 수정한다. Backward secrecy를 보장하기 위해 GM은 새로운 유선 그룹키를 생성하고 기존의 유선 그룹키로 암호화하여 기존 그룹 멤버들에게 멀티캐스트 한다. GM은 Bi에게 새 유선 그룹키와 서브그룹키를 비밀키로 암호화하여 전송한다. 멀티캐스트 전송 트리 또한 재구성된다.

Ri에 그룹 멤버가 존재하지 않게 되면, Bi는 GM에게 그룹 탈퇴 메시지를 전송한다. GM은 Bi에 해당하는 k-node와 u-node를 삭제함으로써 키관리 트리를 수정한다. Forward secrecy를 보장하기 위해, 기존의 유선 그룹키는 갱신되어야 한다. 이때 사용되는 방법은 user-oriented 키갱신 방법을 사용한다. 멀티캐스트 전송 트리 또한 수정된다.

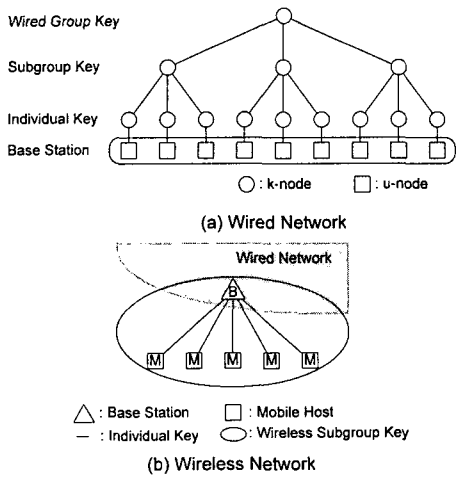

그림 4 WSMM의 키관리 구조

Host Join. 이동 호스트 Mx가 Ri에서 그룹 가입 메시지를 전송하면, GM은 Bi에게 Mx의 무선 서브그룹 가입을 수행하도록 지시한다. 만약에 Bi가 그룹 멤버가 아니라면 Bi가 먼저 그룹에 가입하여야 한다. Bi가 그룹에 가입한 후, 무선 Bi는 Mx와 비밀키를 공유한다. Backward secrecy를 보장하기 위해 Bi는 새 무선 서브그룹키를 생성한다. Bi는 기존의 무선 서브그룹키로 새 무선 서브그룹키를 암호화한 후, 무선 영역에 브로드캐스트 한다. Mx에게는 비밀키로 새 무선 서브그룹키를 암호화하여 전송한다.

Host Leave. 이동 호스트 Mx가 Ri에서 그룹 탈퇴 메시지를 전송하면, GM은 Bi에게 Mx의 무선 서브그룹 탈퇴을 수행하도록 지시한다. Forward secrecy를 보장하기 위해 기존의 무선 서브그룹키는 변경되어야 한다. Bi 새로운 서브그룹키를 남아 있는 멤버들에 대해 각각 비밀키로 암호화하여 개별적으로 전송한다.

Host Handoff. 이동 호스트 Mx가 Ri에서 Rj로 이동하면, Bi는 Mx에 대해 Host Leave 과정을 수행하고, Bj는 Mx에 대해 Host Join 과정을 수행한다.

4. 시뮬레이션

KTMM과 WSMM의 성능을 비교한다. 비교 항목은 멀티캐스트 데이터 전송, 멤버 가입, 멤버 탈퇴, 핸드오프의 평균 지연 시간이다.

실험 환경의 BS의 위치는 고정적이고 8x8 정방형으로 이루어져있다. 각 BS는 둘에서 네 개까지의 이웃 BS를 갖는다. 이동 호스트들은 랜덤하게 무선영역에 위치한다. 실험이 시작되면 이동 호스트들은 타 지역으로 이동을 시작한다.

표 1은 실험 환경 변수이다. KTMM과 WSMM의 키관리 트리의 차수는 4이다. [1] 논문에서 키관리 트리의 차수가 4일 때, 키갱신이 가장 효율적임을 보였다. KTMM 키관리 트리의 최하위 레벨은 차수가 제한되어 있지 않다. 모든 그룹 멤버들은 모두 이동 호스트이고, 데이터 전송은 many-to-many 방식이다.

표 1 실험 환경 변수

Parameter	Value
키관리 트리 차수	4
무선 영역 수	64
이동 호스트 수	100
데이터 패킷 크기	10000 bytes
무선 홉 간에 유선 지연 시간	1 ms
무선 지연 시간	10 ms
무선 영역 거주 시간	5 ms
데이터 암호화/복호화 시간	1 ms
키 암호화/복호화 시간	0.1 ms

Data Transmission Delay. 송신자가 데이터를 암호화하기 시작해서 수신자가 데이터를 복호화하는 데까지 걸리는 시간이다. KTMM은 평균 38.54ms, WSMM은 평균 42.82ms가 걸렸다. WSMM의 지연 시간이 큰 이유는 데이터 전송에 있어 재암호화가 두번 이루어지기 때문이다. 또한, 핸드오프 빈도가 높아질수록 WSMM의 데이터 전송 지연 시간이 커졌다. 그 이유는 WSMM에서 BS가 핸드오프에 의한 키갱신 처리가 데이터 재암호화 작업에 영향을 미친 것으로 분석되었다.

Member Joining Latency. 새 멤버가 가입 요청 메시지를 송신해서 모든 그룹 멤버가 키갱신 메시지를 복호화하는 데까지 걸리는 시간이다. KTMM은 평균 54.12ms, WSMM은 평균 48.41ms가 소요되었다. KTMM에서는 모든 그룹 멤버가 키갱신을 수행하고 키관리 트리가 수정되기 때문에 해당 서브그룹에서만 키갱신이 이루어지는 WSMM에 비해 지연 시간이 더 크다.

Member Leaving Latency. 멤버가 탈퇴 요청 메시지를 송신해서 모든 그룹 멤버가 키갱신 메시지를 복호화하는 데까지 소요되는 시간이다. KTMM은 평균 66.38ms, WSMM은 평균 52.28ms가 소요되었다. 일반적으로 그룹키 관리 방법에서 멤버 탈퇴로 인한 키갱신 지연은 가입으로 인한 지연보다 더 크다. 그러나, WSMM은 가입 지연에 비해 탈퇴 지연시간이 크게 차이 나지 않는다. 그 이유는 키갱신이 서브그룹 내에서만 이루어지기 때문이다. 특히 KTMM에서 탈퇴하는 멤버가 무선 지역을 여러곳 돌아다닐수록, 탈퇴 처리 시간은 더 소요된다. 그 이유는 탈퇴 멤버가 소유하고 있는 서브그룹키가 많으므로 갱신되어야 할 키 개수가 늘어나기 때문이다.

Handoff Latency. KTMM의 핸드오프 지연시간은 23.12ms, WSMM은 28.71ms이다. WSMM은 핸드오프할 때, 키갱신 작업이 이루어지기 때문에 KTMM에 비해 지연시간이 크다.

표 2 실험 결과 (평균 지연 시간)

방법	데이터 전송	멤버 가입	멤버 탈퇴	핸드오프
KTMM	38.54 ms	54.12 ms	66.38 ms	23.12 ms
WSMM	42.84 ms	48.41 ms	52.28 ms	28.71 ms

정리하면, 데이터 전송과 핸드오프 처리에는 KTMM이 보다 좋은 성능을 보이고, 멤버 가입/탈퇴에 대해서는 WSMM이 좋은 성능을 보인다. 즉, 데이터 크기가 큰 멀티미디어 서비스 경우에는 KTMM이 좋은 선택이고, 멤버쉽 변화가 많은 환경에서는 WSMM이 좋은 선택이다.

5. 결론

본 논문에서는 이동 멀티캐스트 환경에 적합한 두 개의 키관리 방법을 제안하였다. 제안 방법은 멤버 가입/탈퇴 시 효율적인 키갱신을 위해 이동 환경에 적합한 구조를 제시하였고, 호스트 이동으로 인한 핸드오프 처리 방법을 제안하였다. KTMM과 데이터 전송에 보다 좋은 성능을 보였고, WSMM은 키갱신에 보다 좋은 성능을 보였다.

Reference

[1] C. K. Wong, M. Gouda, and S. S. Lam, "Secure Group Communications Using Key Graphs," IEEE/ACM Transactions on Networking, vol. 8, Feb. 2000.

[2] K. Chan and S.-H. G. Chan, "Key Management Approaches to Offer Data Confidentiality for Secure Multicast," IEEE Network, vol. 17, Sep.-Oct. 2003

[3] I. Romdhani, M. Kellil, and H.-Y. Lach, "IP Mobile Multicast: Challenges and Solutions," IEEE Communications Society Surveys and Tutorials First Quarter, 2004

[4] R. Prakash, A. Schiper, and M. Mohsin, "Reliable multicast in mobile networks," Wireless Communications and Networking, vol. 3, Mar. 2003.

[5] Y. Sun, W. Trappe, and K.J.R. Liu, "A Scalable Multicast Key Management Scheme for Heterogeneous Wireless Networks," IEEE/ACM Trans. on Networking, vol. 12, no. 4, Aug. 2004.

[6] B.DeCleene, L.Dondeti, S.Griffin, T.Hardjono, D.Kiwior, J.Kurose, D.Towsley, S.Vasudevan, and C.Zhang, "Secure group communications for wireless networks," Military Communications Conference, vol. 1, Oct. 2001.

[7] D. Bruschi and E. Rosti, "Secure Multicast in Wireless Networks of Mobile Hosts: Protocols and Issues," Mobile Networks and Applications, vol. 7, no. 6, Dec. 2002.