이동 애드혹 네트워크에서 안전한 멀티캐스트 통신을 위한 효율적인 그룹 키 분배 방식

임 유 진† · 안 상 현††

요 약

그룹 통신을 기반으로 하는 이동 애드혹 네트워크(mobile ad hoc network (MANET)) 응용들에서는 안전한 멀티캐스트 데이터의 전송을 위하여 그룹 키를 이용한 데이터의 암호화를 주로 사용한다. 그러나 동적인 그룹 멤버쉽으로 인하여 각 그룹 멤버가 가입 또는 탈퇴할 때마다 그룹 키를 갱신하기 위한 키 분배 방식이 요구된다. 유선 망에서 사용되는 그룹 키 분배 방식은 크게 naïve 방식과 트리 기반 방식으로 나눌 수 있다. Naïve 방식은 유니캐스트를 기반으로 동작하므로 대규모 그룹 통신에는 적합하지 않다. 반면 트리 기반 방식은 그룹 크기에 대한 확장성을 가지나 그룹 키 분배를 위한 신뢰성 있는 멀티캐스트 기법을 필요로 한다. 신뢰성 있는 멀티캐스트 기법은 이동 노드로부터 많은 자원을 요구하기 때문에, 트리 기반 방식은 소규모 MANET 환경에는 적합하지 않다고 할 수 있다. 본 논문에서는 소규모 그룹 환경에서 naïve 방식을 기반으로 하는 새로운 그룹 키 분배 프로토콜인 PROMPT(PROxy-based key Management ProTocol)를 제안하였다. PROMPT는 무선 채널의 특성을 이용한 소스 노드로부터의 first-hop grouping과 프락시(proxy) 노드로부터의 last-hop grouping을 통하여 일반 naïve 방식의 메시지 오버헤드를 줄였다.

키워드 : 이동 애드혹 네트워크, 그룹 통신, 키 분배

An Efficient Group Key Distribution Mechanism for the Secure Multicast Communication in Mobile Ad Hoc Networks

Yujin Lim† · Sanghyun Ahn††

ABSTRACT

Secure delivery of multicast data can be achieved with the use of a group key for data encryption in mobile ad hoc network (MANET) applications based on the group communication. However, for the support of dynamic group membership, the group key has to be updated for each member joining/leaving and, consequently, a mechanism distributing an updated group key to members is required. The two major categories of the group key distribution mechanisms proposed for wired networks are the naïve and the tree-based approaches. The naïve approach is based on unicast, so it is not appropriate for large group communication environment. On the other hand, the tree-based approach is scalable in terms of the group size, but requires the reliable multicast mechanism for the group key distribution. In the sense that the reliable multicast mechanism requires a large amount of computing resources from mobile nodes, the tree-based approach is not desirable for the small-sized MANET environment. Therefore, in this paper, we propose a new key distribution protocol, called the proxy-based key management protocol (PROMPT), which is based on the naïve approach in the small-sized MANET environment. PROMPT reduces the message overhead of the naïve through the first-hop grouping from a source node and the last-hop grouping from proxy nodes using the characteristics of a wireless channel.

Key Words : Mobile Ad Hoc Network, Group Communication, Key Distribution

1. 서 론

이동 애드혹 네트워크(mobile ad hoc network (MANET))는 이동 기기들 사이에 무선 통신을 지원해주는 새로운 패러다임이다. MANET 환경에서의 이동 노드들은 고정된 기지국(base station)이나 스위칭 센터의 도움 없이도 통신이 가능하다. 노드의 전송 범위 내의 노드들은 직접 통신이 가능하며, 전송 범위 밖의 노드들은 다른 중간 노드들의 도움을 받아 통신이 가능하다. MANET은 원래 군사용으로 개발되었으나, 최근 들어 노트북과 같은 이동 기기들의 폭발적인 사용 증가로 상업적인 활용을 위한 연구도 많이 진행 중이다.

재난 구조나 회의실 또는 강의실에서의 정보 교환과 같은

※ This research was supported by the MIC(Ministry of Information and Communication), Korea, under the Chung-Ang University HNRC-ITRC (Home Network Research Center) support program supervised by the IITA(Institute of Information Technology Assessment).
† 정 회 원 : 수원대학교 정보미디어학과 전임강사
†† 정 회 원 : 서울시립대학교 컴퓨터과학부 부교수(교신저자)
논문접수 : 2006년 3월 22일, 심사완료 : 2006년 5월 16일

그룹 통신을 기반으로 하는 MANET 응용들에서는 무선 채널이 가지는 보안상의 취약성으로 인하여 안전한 그룹 통신을 지원하는데 어려움이 있다. MANET에서의 보안성 제공을 위해서는 기밀성(confidentiality)과 무결성(integrity), 인증(authentication)에 대한 고려가 필수적으로 요구된다[1].

멀티캐스트 데이터의 안전한 전송은 그룹 키를 사용한 데이터 암호화를 통해 제공 가능하다. 그러나 동적인 그룹 멤버쉽으로 인하여 각그룹 멤버가 새로이 가입 또는 탈퇴할 때마다 그룹 키를 갱신하기 위한 키 분배 방식이 요구된다. 유선 망에서 사용되는 그룹 키 분배 방식은 크게 naïve 방식과 트리 기반 방식의 두 가지 부류로 나눌 수 있다. Naïve 방식은 유니캐스트를 기반으로 동작하므로 대규모 그룹 통신에는 적합하지 않다. 반면 트리 기반 방식은 그룹 크기에 대한 확장성을 가지나 그룹 키 분배를 위한 신뢰성 있는 멀티캐스트 기법을 필요로 한다. 많은 자원을 필요로 하는 신뢰성 있는 멀티캐스트 기법은 에너지 자원이 제한적인 MANET 환경에서 효율적으로 동작하지 않는다. 그럼에도 불구하고 최근의 MANET 환경에서 보안상으로 안전한 멀티캐스트 기법에 대한 연구는 트리 기반 방식에 초점이 맞추어져 있으며 노드의 이동성을 거의 고려하지 않고 있다. 그러나 소규모의 MANET 응용들에서는 보다 실용적이고 간단한 기법이 요구된다.

본 논문에서는 naïve 방식을 기반으로, AODV[2]와 같은 MANET 라우팅 프로토콜로부터의 이웃 노드들에 대한 정보와 무선 링크의 브로드캐스트 특성을 이용하여 일반적인 naïve 방식의 그룹 키 갱신 오버헤드를 줄일 수 있는 새로운 키 분배 프로토콜을 제안한다.

논문 구성은 다음과 같다. 2장에서는 유선 네트워크와 MANET 환경에서 기존에 제안된 멀티캐스트 보안성 지원을 위한 키 분배 방법들의 장단점을 설명하고, 3장에서 본 논문에서 제안하는 프락시(proxy) 기반 키 분배 프로토콜인 PROMPT(PROxy-based key Management ProTocol)를 소개한다. 4장에서 PROMPT의 성능을 분석한 후 5장에서 결론을 맺는다.

2. 관련 연구

최근 들어 화상회의나 인터넷 상의 푸쉬(push) 정보 서비스와 같은 그룹 통신 응용들이 많은 관심을 받고 있다. 이러한 그룹 응용들과 깊은 연관이 있는 멀티캐스트 기법에서의 주된 이슈는 신뢰성과 보안성 제공이다. 멀티캐스트 보안은 오직 허가된 송/수신자만이 그룹 메시지를 송/수신할 수 있는 것을 의미한다. 멀티캐스트 데이터의 안전한 전송은 데이터 암호화를 통해서 이루어 질 수 있으며 이를 위해서는 그룹 멤버들 사이의 그룹 키 분배가 요구된다.

멀티캐스트 보안을 제공하기 위해서는 다음과 같은 요소들이 고려되어야 한다. 먼저, 그룹 멤버들은 데이터 암호화와 복호화를 위한 그룹 키를 공유해야 한다. 둘째로, 그룹의 가입(join)과 탈퇴(leave) 보안이 유지되어야 한다. 그룹 가입 보안은 새로이 가입한 멤버는 가입 이전에 전송된 메시지들을 해석할 수 없어야 한다는 것을 뜻한다. 이를 위해 새로운 멤버가 가입할 때마다 그룹 관리자는 그룹 키를 변경해야 하며, 새롭게 변경된 키를 예전의 그룹 키로 암호화하여 그룹 멤버들에게 전송해야 한다. 그룹 탈퇴 보안은 탈퇴한 멤버가 그룹 탈퇴 이후 전송된 어떠한 메시지도 해석할 수 없음을 뜻한다. 그러므로 멤버가 탈퇴할 때마다 그룹 키 갱신이 요구된다. 그러나 가입 보안과 달리 새로운 그룹 키가 예전의 그룹 키로 암호화되어 전송된다면, 그룹을 탈퇴한 멤버도 여전히 새롭게 갱신된 그룹 키를 해석할 수 있게 된다. 이러한 탈퇴 보안 유지를 위해서 사설 키(private key)가 각각의 멤버에게 할당되며, 멤버가 탈퇴할 때마다 새롭게 갱신된 그룹 키를 각 멤버의 사설 키로 암호화하여 해당 멤버에게 전송함으로써 탈퇴한 멤버에게는 새 그룹 키가 노출되지 않도록 한다.

새롭게 갱신된 그룹 키 전송을 위한 방식으로는 크게 naïve 방식과 트리 기반 방식으로 분류할 수 있다[3]. Naïve 방식에서의 그룹 관리자는 하나의 그룹 키와 N개의 그룹 멤버에 대한 N개의 사설 키를 가진다. 가입 시 각 멤버들은 인증 후 그룹 키와 사설 키를 그룹 관리자로부터 부여 받는다. Naïve 방식에서 그룹 탈퇴 보안은 그룹 관리자가 새로이 갱신된 그룹 키를 각 멤버의 사설 키로 암호화하여 유니캐스트함으로써 유지된다. Naïve 방식의 장점은 간단하며 구현이 용이하고 신뢰성있는 멀티캐스트 프로토콜의 지원을 요구하지 않는다는 것이다. 그러나 그룹 관리자가 새로운 그룹 키를 각 멤버들에게 유니캐스트하기 때문에 그룹 규모가 커질수록 보다 많은오버헤드가 발생한다.

트리 기반 방식은 naïve 방식의 키 갱신 오버헤드를 줄이기 위해 제안된 것으로 그룹 키와 부 그룹 키, 그리고 사설 키로 구성된 논리적인 키 트리를 그룹 관리자가 구성해서 유지한다[4]. 부 그룹 키는 그룹 관리자가 키 갱신을 위하여 전송하는 메시지 수를 줄이기 위한 것이다. 효율적인 키 관리를 위하여 논리 K-ary 키 트리가 채택되었다. 크기가 N인 그룹의 각 멤버들은 키 트리 상의 루트로부터 자신까지의 경로상에 존재하는 모든 키들을 유지해야 한다. 그룹 관리자는 그룹 키뿐만 아니라 부 그룹 키와 N개의 사설 키까지 키 트리 상의 모든 키를 관리해야 한다. 그러므로 그룹 관리자에 의해서 관리되는 키의 전체 개수는 (KN-1)/(K-1)개이며 각 그룹 멤버가 유지해야 할 키 개수는 $\log_K N$개이다.

결과적으로 트리 기반 방식에서 각 멤버가 관리해야 하는 키의 개수는 증가하고 반면 그룹 관리자가 전송해야 하는 메시지 수는 감소한다. 그러므로 트리 기반 방식은 naïve 방식에 비하여 그룹 규모 측면에서 확장성을 가진다고 할 수 있다. 트리 기반 방식의 이러한 장점으로 인하여 최근 MANET 환경에서의 안전한 멀티캐스트 기법들은 주로 트리 기반 방식에 초점을 맞추고 있으며 트리 기반 방식에서 발생하는 오버헤드를 줄이기 위한 여러 연구가 제안되었다[5-7]. 이전에 제안된 몇몇 트리 기반 기법은 GPS 정보를 기반으로 동작한다. 그러나 MANET 환경에서 이러한 GPS

정보의 이용은 바람직하지 못하며, 또한 대부분의 GPS 정보를 이용하지 않는 기법들도 노드의 이동성을 거의 고려하지 않고 있다 (오직 [7]만이 이동성을 고려하였다). 새로 갱신된 키를 수신하지 못한 멤버들은 더 이상 그룹 통신에 참여할 수 없게 되기 때문에 트리 기반 방식의 키 분배는 신뢰성 있는 멀티캐스트 서비스를 기본 구성 요소로 가정하고 있다.

신뢰성 있는 멀티캐스트 서비스를 제공하기 위한 프로토콜들이 유선네트워크 환경에서 광범위하게 연구되었다. 최근 MANET에 대한 관심이 증가하면서 MANET 환경에서의 신뢰성 있는 멀티캐스트 지원을 위한 많은 연구들이 제안되었다[8-12]. 신뢰성 있는 멀티캐스트 기법은 손실된 패킷의 복구를 위하여 소스 또는 중간 노드들에서의 버퍼링을 요구하므로 유선 네트워크에서의 신뢰성 있는 멀티캐스트 기법은 노드들에게 과중한 부담을 지운다. 또한 신뢰성 있는 멀티캐스트 기법은 재전송 기반의 손실 패킷 복구 방법 채택으로 인하여 실시간 응용에서는 사용할 수 없다. 특히 이동성을 가진 노드들과 높은 에러 율(BER)을 가지는 무선 채널을 기반으로 하는 MANET 환경에서 이러한 신뢰성 있는 서비스를 제공하는 것은 유선 네트워크에서 제공하는 것보다 훨씬 어렵다. 더욱이 MANET 노드들은 에너지와 계산 능력 면에서 제약성을 가지므로 이와 같은 복잡한 기법의 사용은 바람직하지 않다.

그러므로 확장성에 대한 요구가 상대적으로 중요하지 않은 작은 규모의 MANET 환경에서는 신뢰성 있는 멀티캐스트 서비스를 요구하는 트리 기반 키 분배 방식 대신 naïve 방식이 보다 더 실용적이다. 본 논문에서 제안하는 프락시 기반 새로운 키 분배 프로토콜인 PROMPT(PROxy-based key Management ProTocol)은 naïve 방식을 채택하였으며 무선 채널의 브로드캐스트 특성을 활용하여 일반적인 naïve 방식의 메시지 오버헤드를 줄였다. 본 논문에서는 그룹 키 분배 방식에 초점을 맞추고 있으며 그 외 다른 보안 관련 이슈들, 예를 들어 악의적인 프락시 노드들에 관련된 이슈들은 다루지 않는다.

3. PROMPT(Proxy-based Key Management Protocol)

PROMPT에서의 그룹 가입 보안은 각 멤버가 새롭게 가입할 때마다 새롭게 갱신된 그룹 키를 예전 그룹 키로 암호화하여 멀티캐스트함으로써 쉽게 지원될 수 있다. 그룹 탈퇴 보안을 위해서는 무선 채널의 브로드캐스트 특성을 활용하여 키 갱신(Key UPDATE) 메시지 오버헤드를 줄였다. FHG(First-Hop Grouping)와 LHG(Last-Hop Grouping)의 두 가지 방법이 PROMPT에서 새로이 정의되었다. FHG는 소스 노드가 새로운 키 정보를 이웃 그룹 멤버들에게 멀티캐스트하기 위하여 사용된다. 각 노드는 자신의 이웃 노드들에 대한 정보를 유지하고 있다고 가정한다. 소스 노드는 새 그룹 키를 이웃 멤버 노드들의 사설 키로 암호화한 후 이를 UPDATE 메시지에 담아 1-홉 플러딩(flooding)한다. UPDATE 메시지의 목적지 주소 필드에는 그룹 멀티캐스트 주소가, TTL 필드에는 1이 설정되며 데이터 필드에는 하나 이상의 [이웃 멤버 노드의 IP 주소, 해당 이웃 멤버의 사설 키로암호화된 새 그룹 키] 정보가 포함된다.

LHG는 많은 이웃 멤버를 가지고 있는 노드에 의해 1-홉 플러딩 기반으로 동작한다. 각 멤버 노드는 자신의 이웃 노드들 중에서 그룹 멤버인 노드가 누구인지 알아야 한다. 그

```
At the source,
    select proxy nodes according to the proxy node selection algorithm

    // first-hop grouping
    destination address ← group address
    TTL ← 1
    IP options field ← a list of [IP address of a neighboring member,
                        the new group key encrypted with the private key of the neighboring member] pairs
    broadcast the key update packet

    for each proxy node {
        destination address ← IP address of the proxy node
        IP options field ← [IP address of the proxy node,
                            the new group key encrypted with the private key of the proxy node]
        IP options field ← a list of [IP address of a neighboring member of the proxy node,
                        the new group key encrypted with the private key of the neighboring member of the proxy node] pairs
        unicast the key update packet
    }

    for each non-proxy node involved neither in first-hop grouping nor in last-hop grouping {
        destination address ← IP address of the non-proxy node
        IP options field ← [IP address of the non-proxy node,
                            the new group key encrypted with the private key of the non-proxy node]
        unicast the key update packet
    }

At a proxy node,
    when a key update packet is received {    // last-hop grouping
        destination address ← group address
        IP options field ← a list of [IP address of a neighboring member,
                        the new group key encrypted with the private key of the neighboring member] pairs
        TTL ← 1
        broadcast the key update packet
    }
```

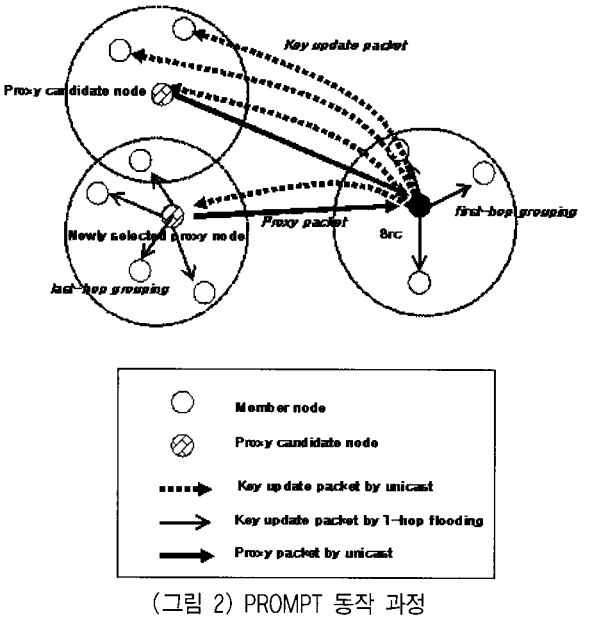
(그림 1) FHG와 LHG 과정

러나 그룹 멤버쉽 정보는 오직 소스에 의해서만 관리되므로 각 노드는 자신의 이웃 멤버 노드 정보를 알 수 없다. 그러므로 초기 단계에서 소스 노드는 새롭게 갱신된 키 정보를 자신의 FHG 범위에 속하지 않는 멤버 노드들에게 일반적인 naïve 방식에서 하는 것과 같이 유니캐스트한다. 이때 패킷의 IP option 필드에 멀티캐스트 그룹 주소를 포함시킴으로써, 각 멤버 노드는 자신의 전송 범위 내로 지나가는 패킷의 목적지 주소가 자신의 이웃 노드이고, 해당 패킷이 속한 세션의 멀티캐스트 주소가 자신이 현재 가입한 그룹의 주소와 일치한다면 이를 기반으로 이웃 멤버 노드 목록 정보를 유지할 수 있다. 소스 노드가 키 갱신 과정을 끝내고 데이터 전송을 시작하면 k개(멀티캐스트 세션 설정 과정에서 결정되는 시스템 파라미터) 이상의 이웃 멤버 노드를 가진 멤버 노드는 PROXY 패킷을 소스 노드에게 전송함으로써 자신이 이웃 멤버 노드들을 대표할 수 있는 프락시 후보 노드임을 알린다. PROXY 패킷에는 해당 멤버 노드의 이웃 멤버 노드들의 목록이 포함된다. 프락시 노드 선정 문제는 NP-hard 문제이므로[13], PROMPT는 이를 위하여 greedy 알고리즘을 채택하였다. PROXY 패킷을 수신한 소스는 서로 중복되지 않는 범위내에서 가장 많은 이웃 멤버 노드를 가지는 노드를 프락시 노드로 선택한다. (그림 1)은 소스에서의 FHG와 프락시 노드에서의 LHG에 대한 의사(pseudo) 코드이다.

(그림 2)는 PROMPT 동작의 예이다. 그림에서 모든 노드는 그룹 멤버라고 가정하였고 k는 3으로 설정하였다. 2개의 프락시 후보 노드는 각기 PROXY 패킷을 소스 노드에게 전송한다. 다음 번 키 갱신 과정에서 소스는 먼저 프락시 노드 선정 알고리즘에 따라 프락시 노드를 결정한다. 그림의 예에서 4개의 이웃 멤버를 가진 노드가 가장 많은 이웃 멤버 노드를 가졌으므로 프락시 노드로 선정된다. 3개의 이웃 노드를 가진 노드는 2개의 이웃 멤버 노드만이 자신의 영역 안에 남아 있으므로 프락시 노드로 선정되지 않는다.

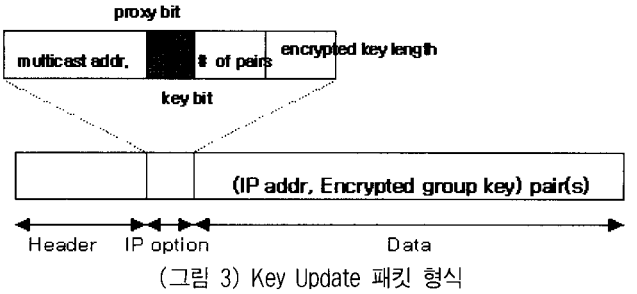
일단 프락시 노드가 선정되면, 소스는 프락시 노드에게 프락시 노드의 사설 키와 프락시 노드의 이웃 멤버들의 사설 키로 각기 암호화된 새로운 그룹 키를 포함한 키 UPDATE 메시지를 전송한다. UPDATE 패킷 내의 proxy 비트(그림 3 참조)가 1로 설정되어 있는 패킷을 수신한 노드는 자신이 프락시 노드임을 인식하고, 패킷의 목적지 필드 값을 자신의 주소 대신 멀티캐스트 그룹 주소로 변경한 후 1-홉 플러딩함으로써 이웃 멤버들에게 새로운 키값을 알린다.

(그림 2)에서 소스 노드는 FHG를 통하여 자신의 이웃 멤버 노드들에게 새 그룹 키 정보를 브로드캐스트하고, 프락시 노드와 프락시 노드의 이웃 멤버 노드들의 사설 키로 암호화한 새 그룹 키 정보를 프락시 노드에게 유니캐스트한다. 이를 수신한 프락시 노드는 LHG를 통하여 자신의 이웃 멤버 노드들에게 새 그룹 키 정보를 1-홉 플러딩한다. FHG와 LHG에 포함되지 않는 멤버 노드들에게는 소스가 키 정보를 유니캐스트한다. (그림 2)의 예에서 일반적인 naïve 방식에 기반하여 소스가 키 갱신을 위하여 전송하는 UPDATE 패킷의 개수는 11개이다. 그러나 PROMPT 방식에서는 소스로부터 2개의 UPDATE 메시지가 1-홉 플러딩되며 (FHG와 LHG을 위해), 4개의 UPDATE 메시지가 유니캐스트된다.



(그림 2) PROMPT 동작 과정

(그림 3)은 소스가 전송하는 키 UPDATE 메시지 형식이다. 데이터 필드에는 한 쌍 이상의 IP 주소와 해당 IP 주소를 가지는 노드의 사설 키로 암호화된 새 그룹 키 정보가 포함된다. 목적지 필드에는 프락시 노드의 IP 주소가 설정된다. IP 옵션 필드는 다음과 같은 부 필드를 가진다.



(그림 3) Key Update 패킷 형식

- 그룹 멀티캐스트 주소
- 수신 노드가 자신이 프락시 노드인지 확인할 수 있는 proxy 비트
- 사용자 데이터 패킷인지, 키 정보를가지는 패킷인지 나타내는 key 비트
- [IP 주소, 암호화된 그룹 키] 개수
- 암호화된 그룹 키 길이

프락시 노드 선정은 이전의 그룹 키 갱신 단계에서 수집된 정보를 기반으로 하므로, 노드가 이동성을 가지는 경우에 대한 고려가 필요하다. 노드의 이동 범위가 grouping 범위 내로 한정되는 작은 경우라면 별다른 문제없이 이에 대한 처리가 가능하며, 노드의 이동 범위가 grouping 범위를 넘어서는 넓은 경우에는 프락시 노드의 일부 이웃 멤버 노드는 키 UPDATE 메시지를 수신하지 못 할 수도 있다. 이 경우 프락시 노드는

소스에게 이러한 이웃 노드의 존재를 알려 소스가 직접 해당 노드에게 UPDATE 메시지를 유니캐스트하도록 한다.

PROMPT 프로토콜은 그룹의 밀도가 높을수록 좋은 성능을 보일 것으로 예상되나, 그룹의 밀도가 높을 경우 이웃 멤버 노드를 k개 이상 가진 노드가 증가하게 되고, 이러한 노드가 Proxy 패킷을 동시에 소스에게 전송하게 되어 패킷 폭증(packet explosion) 문제가 발생할 수 있다. 이를 위하여 PROMPT에서는 소스에게 Proxy 패킷을 전송한 노드가 이러한 사실을 이웃 노드들에게 알림으로써 이웃 노드들이 중복하여 Proxy 패킷을 소스에게 전송하지 못 하도록 한다.

그룹 밀도가 낮은 최악의 경우, 즉 이웃 멤버 노드의 개수가 작아 어떤 노드도 프락시 노드로 선정되지 않는 경우에도 PROMPT의 성능은 naïve 방식의 성능과 비슷한 수준으로 유지될 것이다.

4. 성능 평가

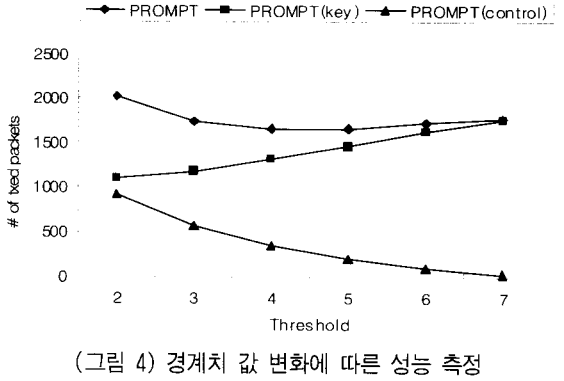
PROMPT의 성능 평가를 위하여 GloMoSim 시뮬레이터[14]를 사용하여 시뮬레이션을 수행하였다. GloMoSim은 분산 시뮬레이션 언어인 PARSEC을 이용하여 만들어진 무선 네트워크 시스템 시뮬레이션 패키지이다. 실험 환경은 1000 x 1000m 범위 내에 50개의 이동 노드로 구성된다. 각 노드의 전송 범위는 반경 250m이며 채널 용량은 2Mbps이다. 각 이동 노드의 이동 방향은 무작위로 선정되며, 자유공간 전파 모델을 채택하여 신호 세기가 거리 d에 대하여 $1/d^2$만큼씩 감소된다고 가정하였다. 하부의 MAC(Medium Access Control) 프로토콜로 IEEE 802.11을, 유니캐스트 라우팅 프로토콜로 AODV[2]를 사용하였고, 소스와 그룹 멤버들은 무작위로 선정하였다. 전체 실험 시간은 1000초로 설정되었다.

이웃 멤버 노드의 개수가 경계치 값(k) 이상인 노드는 소스에게 PROXY 패킷을 전송하므로 경계치 값이 너무 작으면 전송되는 PROXY 패킷 폭증 문제가 발생한다. 반면 경계치 값이 너무 크면 PROXY 패킷의 수가 감소하여 일반 naïve 방식과 유사한 성능을 보이게 된다.

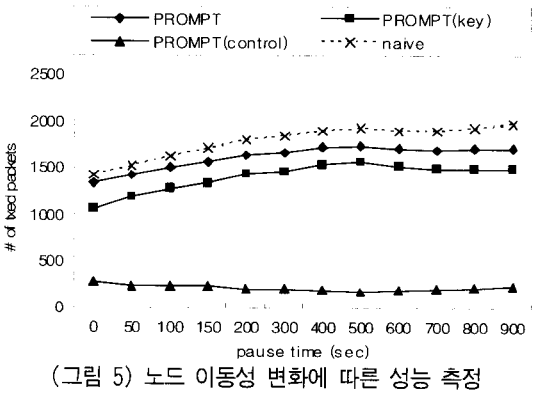
(그림 4)는 경계치 값 변화에 따른 전송 패킷 수(PROXY 패킷과 키 UPDATE 패킷 포함)의 변화를 측정한 것이다. 실험에서 그룹 크기는 15로, 정지 시간(pause time)은 300초로 설정하였다. 경계치 값이 작을수록 프락시 후보 노드가 될확률이 높아지므로 그만큼 많은 PROXY 패킷이 전송되는 것을 볼 수 있다 (그림 4에서 PROMPT(control) 값 참조). 경계치 값이 커질수록 LHG의 가능성이 낮아지기 때문에 소스가 전송해야 하는 키 UPDATE 패킷이 많아진다 (그림 4에서 PROMPT(key) 값 참조). 그림에서 PROMPT 값은 PROMPT(control)과 PROMPT(key) 값을 합친 것이다. 주어진 실험 환경에서의 적당한 경계치 값은 5인 것을 알 수 있다.

(그림 5)와 (그림 6)은 경계치 값이 5일 때 노드의 이동성과 멀티캐스트 그룹 크기의 변화에 따른 성능을 측정한 것이다. (그림 5)에서 보는 바와 같이, 노드 이동성의 변화에 상관없이 PROXY 패킷의 수가 일정하게 유지되므로 일반적인 naïve 방식에 비해 PROMPT 방식이 전송 패킷 수와 제어 오버헤드 측면에서 보다 나은 성능을 보임을 알 수 있다. 그림에서 패킷의 개수가 노드의 이동성이 낮아질수록 증가하는 것처럼 보이는 이유는 전송된 패킷 개수를 세는 과정에서 멤버 노드가 패킷 수신에 성공한 경우에 대해서만 전송된 패킷 개수를 측정했기 때문이다.

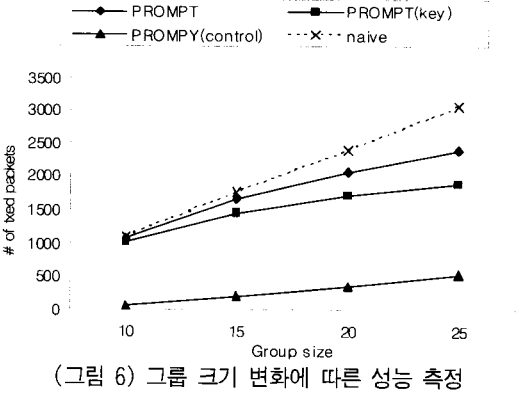
(그림 6)은 소규모 그룹 환경 (그룹 크기: 10~25) 에서 그룹 크기 변화에 따른 전송 패킷 수를 보인 것이다. 전체적으로 PROMPT가 더 나은 성능을 보이며 그룹 크기가 커질수록 그 현상이 뚜렷하다. 이는 그룹 크기가 커질수록 이웃 멤버 노드가 증가할 가능성이 높아지기 때문이다. 결론적으로 PROMPT는 그룹 밀도가 높을수록 naïve 방식에 비하여 좋은 성능을 보임을 알 수 있으며, 그룹 밀도가 아주 낮은 환경에서도 최소한 naïve 방식을 채택했을 경우보다는 낫거나 비슷한 성능을 보임을 알 수 있다.



(그림 4) 경계치 값 변화에 따른 성능 측정



(그림 5) 노드 이동성 변화에 따른 성능 측정



(그림 6) 그룹 크기 변화에 따른 성능 측정

5. 결 론

이동 애드혹 네트워크(MANET)는 이동 기기들 사이에 무선 통신을 지원해주는 새로운 패러다임이다. 그룹 통신을 기반으로 하는 MANET 응용들에서는 무선 채널의 보안상의 취약점으로 인하여 멀티캐스트 통신 보안에 대한 요구가 높다. 이를 위해 그룹 키를 이용한 데이터 암호화 방식이 도입되었으나, 그룹 멤버쉽의 동적인 특성으로 인하여 그룹 키 갱신이 필요하게 되었고 이를 위해 키 분배 프로토콜이 제안되었다. 유선 망에서의 대표적인 두 가지 키 분배 프로토콜 방식으로는 naïve 방식과 트리 기반 방식이 있다. 크기가 작고 노드 밀도가 높은 특성을 가지는 MANET 환경에서는 신뢰성있는 멀티캐스트 프로토콜을 요구하는 트리 기반 방식보다는 naïve 방식이 보다 효율적이라고 할 수 있다. 따라서 본 논문에서는 키 분배 방식으로 naïve 방식을 채택하고, 일반적인 naïve 방식의 메시지 오버헤드를 줄이기 위한 프락시 기반 새로운 키 분배 프로토콜인 PROMPT(PROxy based key Management ProTocol)를 제안하였다. PROMPT는 하나 이상의 이웃 멤버 노드들을 대표하는 프락시 노드 개념을 채택하였으며 무선 채널의 브로드캐스트 특성을 이용하여 키 분배 오버헤드를 최소화하였다. 성능 평가를 통하여 그룹 밀도가 높을수록, 또한 노드의 이동성이 높을수록 PROMPT가 naïve 방식에 비하여 좋은 성능을 보임을 알 수 있었으며, 최악의 경우에도 naïve 수준의 성능을 유지함을 알 수 있었다.

참 고 문 헌

[1] L. Zhou, and Z. J. Haas, "Securing Ad Hoc Networks," IEEE Network, pp.24~30, Nov., 1999.

[2] C. Perkins, E. Bolding-Royer, and S. Das, "Ad hoc On-Demand Distance Vector(AODV) Routing", IETF RFC 3561, July., 2003.

[3] M. J. Moyer, J. R. Rao, and P. Rohatgi, "A Survey of Security Issues in Multicast Communications," IEEE Network, pp.12~23, Nov., 1999.

[4] C. K. Wong, M. Gouda, and S. S. Lam, "Secure Group Communication Using Key Graphs," Proceedings of ACM SIGCOMM, 1998.

[5] L. Lazos and R. Poovendran, "Energy-Aware Secure Multicast Communication in Ad-hoc Networks Using Geographic Location Information," IEEE International Conference on Acoustics Speech and Signal Processing (ICASSP '03), Vol.4, pp.201~204, April. 2003.

[6] M. Moharrum, R. Mukkamala, and M. Eltoweissy, "CKDS: An Efficient Combinatorial Key Distribution Scheme for Wireless Ad-Hoc Networks," IEEE International Conference on Performance, Computing, and Communications (IPCCC '04), pp.631~636, April. 2004.

[7] S. Zhu, S. Setia, S. Xu, and S. Jajodia, "GKMPAN: An Efficient Group Rekeying Scheme for Secure Multicast in Ad-Hoc Networks," International Conference on Mobile and Ubiquitous Systems: Networking and Services (MOBIQUITOUS '04), pp.42~51, Aug., 2004.

[8] R. Chandra, V. Ramasubramanian, and K. Birman, "Anonymouns Gossip: Improving Multicast Reliability in Mobile Ad-Hoc Networks," 21st International Conference on Distributed Computing Systems(ICDCS), pp.275~283, April. 2001.

[9] S. Gupta and P. Srimani, "An Adaptive Protocol for Reliable Multicast in Mobile Multi-hop Radio Networks," IEEE WMCSA '99, pp.111~122, Feb., 1999.

[10] L. Klos and G. Richard III, "Reliable Group Communication in an Ad Hoc Network," IEEE International Conference on Local Computer Networks (LCN 2002), 2002.

[11] A. Sobeih, H. Baraka, and A. Fahmy, "ReMHoc: A Reliable Multicast Protocol for Wireless Mobile Multihop Ad Hoc Networks," IEEE Consumer Communications and Networking Conference (CCNC), Jan., 2004.

[12] K. Tang, K. Obraczka, S.-J. Lee, and M. Gerla, "Reliable Adaptive Lightweight Multicast Protocol," IEEE ICC 2003, May., 2003.

[13] T. H. Cormen, C. E. Leiserson, and R. L. Rivest, "Introduction to Algorithms," MIT Press, 1990.

[14] UCLA Computer Science Department Parallel Computing Laboratory and Wireless Adaptive Mobility Laboratory, "GloMoSim: A Scalable Simulation Environment for Wireless and Wired Network Systems," http://pcl.cs.ucla.edu/projects/domains/glomosim.html

임 유 진

e-mail : yujin@suwon.ac.kr

1995년 숙명여자대학교 전자계산학과(학사)

1997년 숙명여자대학교 전자계산학과 (석사)

2000년 숙명여자대학교 전자계산학과 (박사)

2000년 서울대학교 Post-Doc

2000년 서울시립대학교 연구교수

2003년 University of California Los Angeles, Post-Doc

2003년 삼성종합기술원 전문연구원

2004년~현재 수원대학교 정보미디어학과 전임강사

관심분야 : 센서 네트워크, 애드혹 네트워크, 홈 네트워크 등

안 상 현

e-mail : ahn@uos.ac.kr

1986년 서울대학교 컴퓨터공학과(학사)

1988년 서울대학교 컴퓨터공학과(석사)

1989년 University of Minnesota 컴퓨터학과(박사)

1988년 (주)데이콤 연구원

1994년 세종대학교 컴퓨터학과 전임강사/조교수

1998년~현재 서울시립대학교 컴퓨터과학부 부교수

관심분야 : 애드혹 네트워크, 센서 네트워크, 홈 네트워크, 이동통신, 라우팅 프로토콜 등