情報保護學會論文誌
第17卷 第4號, 2007. 8

애드혹 위치기반 라우팅을 위한 안전한 쿼럼기반 위치 서비스*

임 지 환,[1†] 김 상 진,[2‡] 오 희 국[1†]
[1]한양대학교, [2]한국기술교육대학교

Secure Quorum-based Location Service for Ad hoc Position-based Routing

Jihwan Lim,[1†] Sangjin Kim,[2‡] Heekuck Oh[1†]
[1]Hanyang University, [2]Korea University of Technology and Education

요 약

애드혹(Ad hoc) 네트워크에서의 위치기반 라우팅(position-based routing)은 노드의 지리적인 위치정보를 이용함으로써 효율적인 라우팅이 가능하다는 장점이 있다. 위치기반 라우팅에서 위치 서비스(location service)는 라우팅의 안전성과 효율성에 있어서 매우 중요한 부분이다. 본 논문에서는 위치 서비스에서 발생할 수 있는 보안 위협을 정의하여 기존 애드혹 라우팅에서의 보안 위협뿐 아니라 위치 서비스에서의 보안 위협에도 안전한 쿼럼기반 위치 서비스 프로토콜을 제안한다. 제안하는 프로토콜에서 노드는 공격 노드에 의한 거짓 위치 갱신, 거짓 위치 응답 공격에 대응하기 위해 스스로 생성한 공개키/개인키 쌍과 자신의 위치정보를 이용하여 주소를 생성하며 이를 위치기반 라우팅에 사용한다. 본 논문에서는 제안하는 프로토콜이 기존에 존재했던 다양한 공격들에 대해 안전하며 위치 서비스를 대상으로 한 공격에도 안전하게 대응할 수 있음을 보였고 시뮬레이션을 통해 프로토콜의 안전성 및 효율성을 분석하였다.

ABSTRACT

In ad hoc networks, position-based routing schemes, that use geographical positions of nodes, have been proposed to efficiently route messages. In these routing schemes, the location service is one of the key elements that determines and effects security and efficiency of the protocol. In this paper, we define security threats of location service and propose a new quorum based location service protocol. In our proposed protocol, nodes register their public keys in other nodes during the initialization phase and these registered keys are used to verify locations of other nodes and the messages exchanged. In this paper, we prove that our protocol is robust against traditional attacks and new attacks that may occur due to the use of position-based routing. We also analyze the efficiency of our protocol using various simulations.

Keywords : *location service, position-based routing, ad hoc, secure routing*

접수일: 2007년 2월 11일 ; 채택일: 2007년 5월 15일
* 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 (홈네트워크연구센터) 육성 지원사업의 연구결과로 수행되었음
† 주저자, jhlim@cse.hanyang.ac.kr
‡ 교신저자, hkoh@cse.hanyang.ac.kr

Ⅰ. 서 론

애드혹 네트워크는 모바일 노드(mobile node)들에 의해 자율적으로 구성되는 기반 구조가 없는 네트워크를 말한다. 이에 참여 노드들은 무선 인터페이스를 사용

한 다중 홉 라우팅 기능으로 통신 거리상의 제약을 극복하고 멀리 떨어진 다른 노드와 통신을 할 수 있게 된다. 참여 노드들의 이동이 자유롭기 때문에 네트워크 토폴로지가 동적으로 변화는 특징을 가진 애드혹 네트워크에서는 많은 라우팅 프로토콜들이 제안되고 있다.

지금까지 주로 연구되어 오던 테이블 기반 방식(table-driven)과 요구 기반 방식(on-demand)과는 다르게 최근에는 참여 노드들의 지리적인 위치좌표를 이용하여 효율적으로 라우팅을 하고자하는 위치기반(position-based) 라우팅에 관한 연구가 많은 주목을 받고 있다. 위치기반 라우팅에서 참여 노드들은 GPS (Global Positioning System)와 같은 장비를 통해 자신의 지리적인 위치를 알 수 있고 여기에 이웃 노드의 위치 정보와 목적 노드의 위치 정보를 이용하여 효율적으로 라우팅 경로를 설정할 수 있다. 이웃 노드의 위치 정보는 주변 노드와의 정보교환을 통해 쉽게 획득할 수 있으나 원거리에 떨어져 있는 특정 노드의 위치는 쉽게 획득할 수 없다.

위치기반 라우팅에서 위치 서비스는 통신을 원하는 특정 노드의 위치정보를 획득하게 해주는 서비스이다. 참여 노드는 특정 노드의 현재 위치를 가지고 있는 위치 서버(location server)에게 질의를 통해 응답받는 형식으로 상대의 위치를 알 수 있게 된다. 기간망이 없는 가운데 위치 서버는 여러 가지 형태로 구성될 수 있으나 특정 노드가 참여 노드 전체의 위치정보를 관리하는 중앙집중식 형태보다는 참여 노드 각각이 일부 노드의 위치정보를 관리하는 분산된 형태의 위치 서버가 더 적합하다. 즉, 특정 노드 또는 일부 노드 집합이 다른 노드 또는 다른 노드 집합의 위치 서버 역할을 하고 위치 요청에 응답을 해주는 방법으로 위치 서비스가 제공되어야 한다.

이러한 위치 서비스는 크게 위치 갱신(location update), 위치 요청(location request), 위치 응답(location response)의 3가지 요소로 구성되어있다. 우선, 위치 갱신은 네트워크에 참여한 노드들이 일정한 주기로 또는 이전 위치로부터 일정 거리 이상 이동했을 경우 현재 자신의 위치를 위치 서버에게 보고하여 최신 위치를 갱신하는 것을 말한다. 위치 요청은 임의 노드가 다른 참여 노드와 통신하기위해 해당 노드의 위치 정보를 위치 서버에게 요청하는 것을 말한다. 위치 응답은 이 요청에 대해 위치 서버가 해당 노드의 위치 정보를 요청 노드에게 응답해 주는 것을 말한다.

현재까지 연구되어 온 위치 서비스 프로토콜들은 위치 정보를 라우팅 경로 설정에 사용하기 때문에 특히 민감한 위치 정보를 다루고 있음에도 불구하고 존재할 수 있는 여러 보안 위협에 대하여 전혀 고려하지 않고 있다. 따라서 본 논문에서는 기본적인 애드혹 라우팅이 지니는 보안 위협들에 대해서 알아보고 위치 서비스에서 고려해야할 보안 위협에 대해 정의하여 이러한 위협들로부터 안전하게 위치 정보를 관리할 수 있는 안전한 위치 서비스 프로토콜을 제안한다.

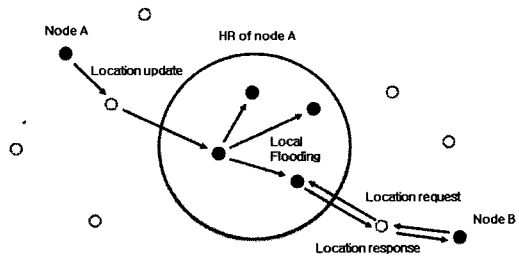
Ⅱ. 관련 연구

2.1. 위치 서비스

위치기반 라우팅을 위한 분산된 형태의 위치 서비스에 관한 연구는 HR(Home Region)형 위치 서비스와 쿼럼(quorum)형 위치 서비스로 분류할 수 있다.[1,2]

2.1.1. HR 기반 위치서비스

HR 기반 위치 서비스에서 각 노드는 [그림 1]과 같은 HR을 가진다. 모든 노드는 각기 다른 HR을 가지고 있으며 HR의 중심(fixed center)은 노드의 ID를 해쉬(hash)해서 얻어낼 수 있다. 특정 노드의 위치 정보를 획득하길 원하는 노드는 그 노드의 HR에 요청 메시지를 보내어 위치 정보를 획득할 수 있다. 모든 노드는 일정 주기로 또는 이전에 보고했던 위치로부터 일정 거리 이상 이동하게 되면 자신의 HR에 위치 갱신 메시지를 전송하여 자신의 현재 위치를 갱신한다. [그림 1]에서처럼 노드는 자신의 HR에 자신의 현재 위치를 갱신하고 이 노드의 위치 정보를 원하는 다른 노드는 이 노드의 ID와 해쉬 관계에 있는 HR로 요청 메시지를 보내 해당 노드의 위치 정보를 획득할 수 있다. HR 내의 노



[그림 1] HR 기반 위치 서비스 스킴

드들은 로컬 플러딩(local flooding)을 통해 위치 정보를 공유한다.

이와 같은 HR 기반 위치 서비스 스킴을 사용하는 프로토콜로 SLURP(Scalable Location Update-based Routing Protocol)[3], SLALOM(Scalable Ad-hoc Location Management Scheme for Large Mobile Ad-hoc Networks)[4], ELF(Efficient Location Forwarding in ad hoc networks)[5], HLS (Hierarchial Location Service for mobile ad-hoc networks)[6] 등이 있다.

2.2.1. 쿼럼기반 위치 서비스

쿼럼기반 위치 서비스는 특정 지역에 있는 노드들이 항상 같은 노드의 위치 서버 역할을 하는 HR 기반 위치 서비스와 달리 임의 기준으로 선발된 집합 또는 그룹이 또 다른 노드 집합 또는 그룹의 위치 서버 역할을 담당한다. 노드들은 HR 기반의 위치 서비스와 마찬가지로 일정 주기마다 한번 씩 또는 이전에 보고한 위치로부터 일정 거리 이상 이동하게 되면 위치 갱신 메시지를 쿼럼에 전송하여 자신의 현재 위치를 갱신하게 된다.

쿼럼기반 위치서비스 프로토콜인 XYLS(column-row quorum-based location service)[7]에서 노드는 자신과 같은 열에 있는 노드들에게 자신의 위치를 보고하고 특정 노드의 위치 정보를 획득하고자 할 때에는 행으로 위치 요청 메시지를 보내는 기법을 사용한다.

2.2. 애드혹 라우팅에서의 보안

애드혹 네트워크에서는 기간망이 없는 가운데 참여 노드 스스로가 라우터 역할을 수행하기 때문에 많은 보안적 위협을 가지고 있다. 이에 가능한 공격들을 분류해 보면 다음과 같이 블랙 홀(black hole) 공격, 재전송(replay) 공격, 웜 홀(wormhole) 공격, 블랙메일(black-mail) 공격, 라우팅 테이블 오염(routing table poisoning) 공격 등으로 분류할 수 있다[8]. 이상의 공격들에 대응하기 위해서 기존에 제안된 많은 논문들은 공개키/대칭키에 기반을 둔 프로토콜들을 제안하고 있으나 노드의 참여와 이탈이 자유롭게 이루어지는 환경에서 모든 노드쌍이 서로 비밀 정보를 공유하고 있다고 가정한다거나[9-11] 기간망을 사용하지 않는 애드혹 환경에서 공통된 CA(Certification Authority)를 갖는 PKI(Public Key Infrastructure) 기반구조를 이용한다는 가정[12,13]은 현실적이지 못하다. 제안하는 프로토콜에서는 인증서를 사용하는 대신 노드를 그룹화하여 공개키를 그룹별로 등록하는 방법으로 축소된 형태의 공개키 시스템을 사용하게 된다.

2.3. 위치 서비스에서의 보안

위치 서비스에서는 기존 애드혹 라우팅에서 존재했던 보안 위협 외에 다음과 같은 위치 서비스에 특화된 보안 위협들이 있다. 공격자는 위치 서비스가 정상적인 서비스를 하지 못하게 하기위해 다음과 같은 공격을 시도하게 된다.

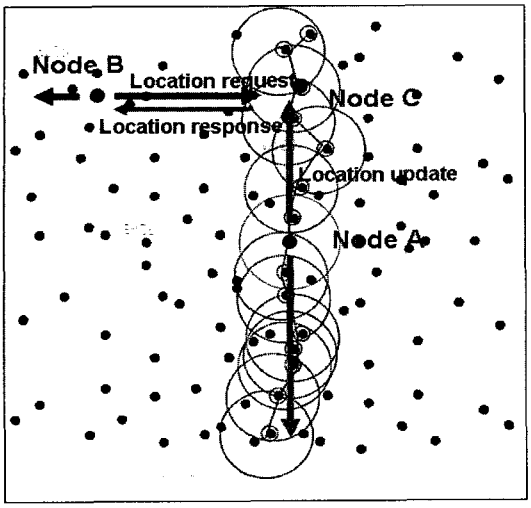
- 거짓 위치 갱신 공격: 공격 노드가 특정 노드를 가장하여 노드의 위치를 거짓으로 업데이트 하거나 정상적인 위치 갱신 패킷을 캡춰하여 거짓 위치정보를 삽입함으로서 위치 서버가 잘못된 위치정보를 유지하게 하는 공격.
- 거짓 응답 공격: 공격 노드가 특정노드의 위치를 요청하는 메시지에 대해 거짓 응답 메시지를 생성하여 잘못된 위치정보를 알려주는 공격.

애드혹 네트워크에서 노드의 위치 정보에 대한 프라이버시 문제도 하나의 보안 이슈이긴 하지만 위치 정보를 통해 최적의 라우팅 경로를 결정하는 위치 기반 라우팅을 사용하고 인프라의 도움 없이 분산된 형태로 노드들이 다른 노드의 위치 정보를 유지하고 관리하는 위치 서비스 프로토콜을 제안하는 본 논문에서는 노드의 위치 정보에 대한 프라이버시 문제를 고려하지 않는다.

Ⅲ. 제안하는 프로토콜

3.1. 개요

제안하는 프로토콜은 쿼럼기반의 XYLS[7]와 같은 위치 서비스 메커니즘을 사용하는 안전한 위치 서비스 프로토콜로 사각형 내에서 좌우를 가로지르는 직선과 상하를 가로지르는 직선이 항상 한 개의 점에서 교차하게 됨을 이용한다. 즉, 위치 갱신 메시지와 위치 요청 메시지 간에는 반드시 한 개의 교차점이 존재하게 되고 노드는 가로방향으로 위치 요청을 함으로써 원하는 노드의 위치 정보를 획득할 수 있게 된다.



〔그림 2〕 제안하는 위치서비스 개요 - 세로 방향으로 위치를 갱신하고 가로방향으로 질의한다.

참여 노드는 주기적으로 또는 이전 위치로부터 일정 거리이상 이동하게 되면 〔그림 2〕와 같이 세로방향으로 위치 갱신 메시지를 전송한다. 특정 노드가 위치기반 라우팅을 사용하기위해 통신을 원하는 대상 노드의 위치 정보를 획득하고자 할 때에는 가로방향으로 위치 요청 메시지를 전송하여 위치 정보를 획득하게 된다.

위치 요청 메시지를 수신한 노드는 자신의 위치 테이블에서 위치 정보를 확인하고 해당 노드의 위치 정보가 있을 경우 위치 응답 메시지를 생성하여 전송한다. 안전한 위치 서비스를 제공하기위해 제안하는 프로토콜에서 노드들은 네트워크 참여시 자신의 공개키/개인키 쌍을 생성하고 위치 정보와 함께 공개키 정보를 네트워크에 등록하는 공개키 등록 및 초기화 과정을 수행한다. 이후 각 노드들은 자신의 개인키로 서명한 주소를 위치 갱신, 위치 요청, 위치 응답 등의 메시지에 사용하여 위치 서비스 프로토콜을 안전하게 진행하게 된다.

제안하는 프로토콜에서 사용하고 있는 메시지 형태는 네트워크 환경에 영향을 받지 않기 때문에 쿼럼기반 위치 서비스는 물론 HR 기반 위치 서비스에서도 구현이 가능하다. 하지만 HR기반 위치 서비스의 경우 HR의 위치가 노드의 현재 위치로부터 많이 떨어져 있을 경우 주기적으로 위치 갱신 메시지를 생성하고 전달하는 노드들에게 부담이 많이 되며 위치 요청 비용 또한 매우 커져 효율적인 라우팅을 기대 할 수 없게 되는 경우가 빈번히 발생한다. 이를 보완 하기위해 제안된 다중 HR 기반 위치 프로토콜의 경우에도 여러 HR간의 그룹원 및 정보의 동기화 문제와 같은 보안을 적용하기에 복잡한 문제가 남아 있다. S.M Das 등[1]과 R. Friedman 등[2]은 기 제안된 위치 서비스 프로토콜들의 특징을 분석하고 시뮬레이션을 통해 각 위치서비스 프로토콜의 효율성을 비교 분석하였다. 이 논문의 결과에 따르면 XYLS는 제안된 시기가 위치 서비스 연구 초기임에도 불구하고 다른 여러 HR 기반 위치 서비스와 쿼럼기반 위치 서비스 프로토콜에 비해서 비용적으로 효율적이라고 평가되고 있으며 프로토콜 구성 또한 단순하고 간단하여 구현이 쉬운 장점이 있다. 따라서 제안하는 프로토콜은 쿼럼기반의 XYLS와 같은 위치 서비스 메커니즘을 사용하는 안전한 위치 서비스 프로토콜을 제안한다.

3.2. 가정 및 표기법

제안하는 프로토콜은 〔표 1〕과 같은 표기법을 사용하며 네트워크 환경에 대해서는 다음과 같은 가정을 한다.

- 애드혹 네트워크에 참여하는 노드들은 균일하게 분산되어 분포하며 임의의 속도와 방향을 가지고 이동한다.
- 참여 노드는 GPS를 통해 자신의 지리적인 위치정보를 획득할 수 있으며 GPS를 통한 정확한 시간 동기화가 이루어져 있다.
- 모든 노드는 같은 전송 반경과 계산능력을 가지고 있으며 노드간의 링크는 대칭형(symmetric link)이다.
- 참여 노드는 자신이 통신하고 싶어 하는 대상 노

〔표 1〕 표기법

A	Node A의 ID
A_{PK}, A_{PR}	Node A의 공개키, 개인키
$Sig_A(msg)$	msg에 대한 A의 서명
T_{A_I}	최초 공개키를 생성한 시간을 나타내는 타임스탬프
T_{A_C}	현재 시간을 나타내는 타임스탬프
Pos_A	GPS로 획득한 A의 지리적 위치(좌표)
$Addr_A$	Pos_A를 서명한 형태의 A의 지리적 주소 $Addr_A = Sig_A(A\|\|Pos_A\|\|T_A\|\|T_{A_C})$

드의 ID 정보를 알고 있고 그룹을 설정하는 알고리즘을 알고 이에 동의하고 있으며 위치기반 라우팅을 사용하여 통신한다.

보안요소에 대해서는 다음과 같이 가정한다.

- 참여 노드는 스스로 공개키/개인키 쌍을 생성할 수 있다.
- 위치기반 라우팅에 사용되는 주소는 GPS로부터 획득한 지리적 위치와 기타 정보를 메시지 첨부(appendix)형으로 서명하여 생성한 값이다.

3.3. 공개키 등록 및 초기화

제안하는 프로토콜은 서명을 사용하기 때문에 공개키 시스템을 사용해야 하나 애드혹 네트워크에서 공개키 기반구조를 사용할 수는 없기 때문에 다음과 같은 공개키 공표(public announcement of public key) 방법을 사용한다.

참여 노드들은 초기에 스스로 공개키/개인키 쌍을 생성하여 공개키 정보를 네트워크에 플러딩(flooding)한다. 참여 노드들은 다른 참여 노드의 공개키 정보를 저장하고 있기 때문에 네트워크에 참여한 노드 중 올바르게 행동하는 노드가 존재한다면 전송되는 메시지에 대해서 그 정당성을 검증할 수 있다. 즉, 정당한 노드는 자신이 가지고 있는 공개키 정보를 이용하여 자신을 거쳐 포워딩되는 메시지에 대해서 서명의 적법성(공개키의 적법성)을 검증할 수 있다.

초기 공개키 등록 과정에서 노드들은 자신의 ID와 공개키, 공개키를 생성한 시간의 타임스탬프를 포함해 (1)과 같은 서명을 생성한다.

$$Sig_A(A \| A_{PK} \| T_A) \quad (1)$$

이제 노드는 다음 (2)와 같은 공개키 등록 메시지 (*PK_init*)를 생성하여 방송한다. 여기서 *Type*은 '공개키 등록', '위치 갱신', '위치 요청' 등을 가리키는 메시지의 타입을 나타내고 Seq는 루프를 방지하고 중복된 메시지를 구분할 수 있게 하는 일련 번호(sequence number)를 나타낸다.

$$PK\_init = [Type, Seq, Sig_A(A \| A_{PK} \| T_A)] \quad (2)$$

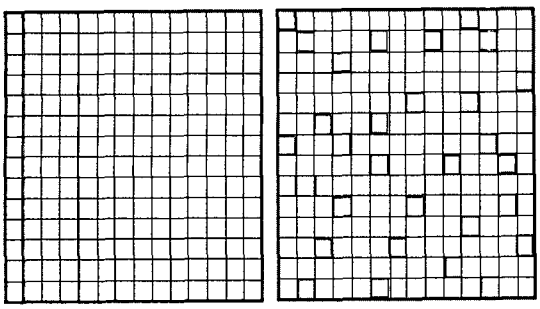
하지만 노드들이 다른 모든 참여 노드의 공개키 정보를 저장해야 한다면 저장 공간의 제약이 있는 애드혹 노드들에게는 부담이 될 것이다. 따라서 제안하는 프로토콜은 하나의 노드가 모든 참여 노드의 공개키 정보를 유지하는 것이 아니라 일부 그룹(group / quorum)의 공개키 정보만을 유지하는 방법을 사용한다.

이와 관련하여 두 가지 고려해야하는 문제가 있다. 하나는 공개키 분배와 관련된 문제로서 공개키 공표 방법으로 배포된 공개키에 대한 신뢰 문제이고 다른 하나는 일부 그룹이 다른 일부 그룹의 공개키 정보만을 유지하는 것으로 원하는 안전성을 거둘 수 있느냐는 것이다. 첫 번째 문제는 안전성분석 부분에서 자세히 다루기로 하고 두 번째 문제는 다음과 같은 공개키 질의를 사용하는 것으로 문제를 해결할 수 있다.

참여 노드는 기본적으로 자신을 거쳐 가는 메시지에 대해 자신이 유지하고 있는 공개키 정보에 대한 메시지만을 검증하게 된다. 하지만 뒤에서 설명할 *Err_alarm* 메시지를 수신한 경우나 자신이 메시지의 목적 노드일 경우에는 무조건 해당 메시지를 검증해보아야 하기 때문에 자신이 가지고 있지 않은 공개키 정보를 획득하기 위해서 공개키 질의를 하게 된다. 공개키 질의는 다음과 같은 공개키 질의 메시지를 가로 방향으로 전송하여 원하는 공개키 정보를 응답받아 서명을 검증할 수 있게 한다. 아래 메시지는 노드 D가 A의 공개키 정보를 요청하는 공개키 요청 메시지이다.

$$PK\_request = [msg, Sig_D(msg)]$$
$$msg = (Type, Seq, A, Addr_D)$$

다시 공개키 정보를 공유하게 될 그룹을 설정하는 방법에 대해 알아보면 제안하는 프로토콜은 [그림 3]과 같이 2가지 방법의 그룹설정 방법을 제안한다. 그룹이 설정된 이후 노드는 자신과 같은 그룹에 있는 노드들의 공개키 정보만 유지하게 된다. 방법 (a)는 노드가 최초 초기화하는 곳의 지리적 위치를 기준으로 하여 일정 너비의 같은 열에 위치하는 노드들을 묶어 그룹으로 설정하는 방법이고 (b)는 노드의 아이디를 입력으로 하는 잘 정의된 해쉬 함수를 이용하여 분산된 형태의 그룹을 형성하는 방법이다. 위 2가지 그룹형성 방법은 각각이 위치서비스의 운영적 측면에서 장단점이 있으며 이에 대해서는 4장에서 분석하기로 한다. 노드는 자신과 같은 그룹에 있는 노드들에게 (2)와 같은 공개키 등록 메시지를 전송하게 되고 다른 그룹원이 보내온 공개키 등록 메시지로부터 공개키 정보를 저장하여 유지한다. (a)와 같은 그룹형태라면 공개키 등록 메시지는 일정폭의



(a) (b)

〔그림 3〕 그룹을 설정하는 2가지 방법

같은 열에 위치하는 노드들이 수신할 수 있도록 세로 방향으로만 전송되면 된다. (b)의 경우는 그룹원들이 네트워크 전체에 고루 분산되어 위치하기 때문에 네트워크 전체에 메시지를 플러딩해야하는 비용이 소요된다.

3.4. 위치 갱신

참여 노드들 A는 주기적으로 또는 일정 거리 이상을 이동하게 되면 다음과 같은 형태의 *Loc_update* 메시지를 세로방향으로 방송한다.

$$Loc\_update = [msg,\ Sig_A(msg)]$$
$$msg = (Type, Seq, width, Addr_A)$$

참여 노드들은 다음과 같은 위치 테이블(location table)을 유지하고 있게 되는데 메시지를 수신한 노드는 자신의 위치 테이블에 위치 정보를 갱신하고 메시지를 다음 홉으로 전달한다.

$$Location\ Table : [A, A_{PK}, T_{A_I}, T_{A_C}, Addr_A, \Gamma]$$

T_{A_I}와 T_{A_C}는 표기법에 설명한 바와 같이 각각 공개키를 처음으로 생성한 시간과 현재 시간을 나타내는 타임스탬프 값이고 Γ는 해당 노드의 신뢰도를 나타내는 값으로 신뢰도가 일정수준 이하인 노드는 네트워크에 참여할 수 없게 된다. 신뢰도 Γ는 프로토콜이 진행됨에 따라 조정되게 되고 신뢰도의 임계치는 애드혹 네트워크의 응용에 따라 정책적으로 결정할 수 있다. 메시지의 검증은 위치 갱신 메시지를 전송한 노드와 동일한 그룹에 속해있는 노드가 서명을 검증하여 이루어지고 오류 발생시 *Err_alarm* 메시지를 방송하여 잘못된 위치 갱신 메시지임을 역경로로 전송해 잘못된 위치 갱신을 복원(recovery)할 수 있게 한다. *width*는 전송하는 메시지의 전송 폭을 결정하는 인자 값으로 *width*가 1로 설정되어 있다면 세로 방향으로 업데이트되는 위치 갱신 패킷을 수신한 노드로부터 가로로 1홉 거리에 있는 노드 역시 위치갱신에 참여하여 1홉의 폭을 가지고 세로로 전송되어진다는 의미이다. 이는 위치 서비스의 정확도를 위해 조정될 수 있는 시스템 변수로서 *width* 값이 크면 노드의 밀도가 낮은 환경에서 보다 안정적으로 위치 서비스를 제공할 수 있지만 노드의 전송 참여 횟수, 데이터 중복 등의 효율성 측면에서 이율배반 관계(trade-off)가 있다. 위치 갱신 패킷은 수신 노드가 따로 검증할 필요는 없으며 *Err_alarm* 메시지가 수신되지 않는다면 해당 노드의 위치 정보를 갱신한다. 이후 다른 노드가 A의 위치를 요청한다면 저장하고 있던 주소 $Addr_A$를 요청하는 노드에게 그대로 전송하게 된다. 〔그림 4〕와 〔그림 5〕는 각각 특정 노드가 위치 갱신 이벤트를 일으키게 되는 알고리즘과 다른 노드의 위치 갱신 메시지를 수신했을 때의 알고리즘이다.

〔그림 4〕에서 처럼 노드는 자신의 위치 갱신 주기가 만료되었거나 현재 위치와 이전 위치의 거리차가 임계

```
while(true){
 if(update lifetime expired ||
  (|previous_location - current_location|>= Δ)){
    generate location_update
    sendToNorthAndSouth location_update
 }
}
```

〔그림 4〕 노드의 위치 갱신 알고리즘

```
receive(location_update){
  if(!havePK(location_update)){
     updateLocationTable(location_update)
     sendToNext(location_update)
  }else{
     if(!verification(location_update)){
        generate Err_alarm
        sendToReverse Err_alarm
     }else{
        updateLocationTable(location_update)
        sendToNext(location_update)
     }
  }
}
```

〔그림 5〕 다른 노드의 위치 갱신 메시지를 수신한 노드의 알고리즘

치 Δ를 넘게 되면 위치 갱신 메시지를 생성하고 이를 세로방향으로 전송한다. 이 위치 갱신 메시지를 수신한 노드는 먼저 자신의 위치 테이블에서 위치 갱신 메시지를 생성한 노드의 공개키 정보를 가지고 있는지 확인하고 만약 가지고 있다면 이를 검증한다.

노드는 검증결과에 따라 *Err_alarm* 메시지를 생성하여 메시지를 수신했던 방향으로 *Err_alarm* 메시지를 전송할 수 있다. 만약 검증결과가 아무 이상이 없거나, 해당 공개키 정보를 가지고 있지 않다면 자신의 위치 테이블을 갱신하고 다음 홉으로 메시지를 전달한다.

3.5. 위치 요청

위치기반 라우팅을 사용하는 참여 노드 B는 노드 A와 통신하기위해 가로방향으로 노드 A의 위치 정보를 요청하는 *Loc_request* 메시지를 전송한다.

$$Loc\_request = [msg,\ Sig_B(msg)]$$
$$msg = (Type, Seq, A, Addr_B)$$

메시지의 구성은 메시지 타입, 일련 번호, 대상 노드 ID, 자신의 주소로 이루어져 있으며 메시지에 대한 검증은 앞의 위치 갱신 과정과 같다. *Loc_request* 메시지를 수신한 노드는 자신의 위치 테이블에서 A의 위치 정보를 찾아보고 A의 위치 정보가 없으면 다음 홉으로 메시지를 다시 포워딩한다. A의 위치 정보를 가지고 있는 노드는 *msg*의 타임스탬프와 자신의 위치 테이블의 타임스탬프를 비교해 만료기간이 지나지 않은 정보에 대해 *Loc_response* 메시지를 생성해 응답하게 된다.

3.6. 위치 응답

*Loc_request*에 대한 *Loc_response* 메시지는 유니캐스트(unicast)로 요청 노드에게 전송되어진다. 노드 C가 노드 B의 요청으로 A의 위치를 알려주는 위치 응답 메시지는 다음과 같다.

$$Loc\_response = [msg,\ Sig_C(msg)]$$
$$msg = (Type, Seq, Addr_B, Addr_A, Addr_C)$$

메시지의 구성은 메시지 타입, 일련 번호, 수신노드 주소, 요청노드 주소, 송신노드 주소로 이루어진다. 위 메시지는 B에게 C가 A의 위치를 알려주는 *Loc_Response* 메시지이다.

3.7. 보안 관리

메시지 전송에 참여하는 노드는 자신이 전송한 메시지를 이웃 노드가 제대로 포워딩하는지 여부를 모니터링하고 자신이 포워딩하는 메시지에 대해서는 자신이 메시지 서명에 사용된 공개키 정보를 가지고 있다면 이를 검증한다. 이상 행동이 감지되었을 경우 노드는 다음과 같은 *Err_alarm* 메시지를 자신이 메시지를 수신했던 방향으로 되돌려 전송한다. *Err_alarm* 메시지를 수신한 노드는 메시지를 검증한 후 자신의 위치 테이블에서 *err_type*에 따라 해당노드의 신뢰도를 감소시키고 다시 방송한다.

$$Err\_alarm = [msg, Sig_D(msg)]$$
$$msg = (Type, Seq, ID, Addr_D, err\_type)$$

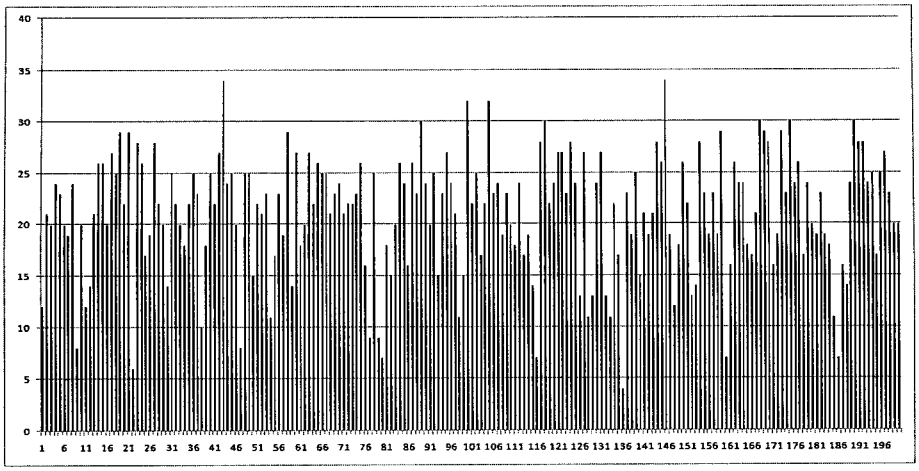
만약 *Err_alarm* 메시지가 위치 갱신 메시지에 대해서 발생한 것이라면 갱신한 위치 정보를 이전 것으로 다시 복원하고 *Err_alarm* 메시지를 다시 방송한다. *Err_alarm* 메시지는 유니캐스팅이 아닌 방향성을 지닌 브로드캐스팅(broadcasting) 메시지이므로 공격자가 임의로 메시지 전송을 중단하거나 차단할 수 없다. 이 때 해당 노드의 신뢰도가 네트워크 환경에 따라 정책적으로 결정되는 임계치 이하로 떨어지면 이 노드를 공격노드로 가정하고 해당 노드로부터의 메시지를 무시한다. 이 경우 공격 노드의 신뢰수치는 *Err_alarm* 메시지를 수신한 인근 모든 노드에 의해서 감소하게 되고 국지적으로 동기화 된다고 볼 수 있으므로 노드 각각이 공격노드의 메시지를 무시하기만 하여도 해당지역의 네트워크에서 배제되는 효과를 거둘 수 있다.

Ⅳ. 분 석

4.1. 안전성 분석

제안하는 프로토콜은 안전한 위치 서비스를 제공하기위해 공개키 공표 방법에 의한 공개키를 사용하고 있으며 노드의 저장 공간 부담을 줄이기 위해 노드가 유지하는 공개키 수를 그룹화하여 분산시켰다. 따라서 본 장의 안정성 분석에서는 다음의 사항을 분석한다.

- 인증서 없이 사용되는 공개키가 공격 노드에 의해 위조된 공개키와 구별되어 안전하게 사용될 수 있는가?



〔그림 6〕 시각 t=0에서 참여 노드들의 이웃노드 수

- 저장 공간의 제약으로 노드 각각이 일부 노드의 위치정보만을 가지고 있는 환경에서 메시지의 인증이 정상적으로 이루어질 수 있는가?
- 기존 애드혹 라우팅에서의 보안 위협과 위치 서비스에서의 보안 위협에 대응해 안전하게 서비스 제공할 수 있는가?

이를 위해 먼저 이론적으로 가능한 결과를 분석하고 시뮬레이션을 통해 결과를 입증하는 방법을 사용하였다.

4.1.1. 공개키 등록 및 메시지 인증

제안하는 위치 서비스 프로토콜은 애드혹 환경에서 공개키 기반구조를 사용하지 않는 대신 각자의 ID, 공개키 정보를 네트워크 참여 초기에 등록하는 과정을 거침으로써 축소된 형태의 공개키 시스템을 사용할 수 있다. 본 논문에서는 R. Anderson등[14]의 공격모델을 적용하여 네트워크 초기의 공격확률이 낮다는 현실적인 공격모델을 가정한다. 즉 공격자가 네트워크 초기에 참여하지 않은 노드들의 ID와 공개키 정보를 등록하는 식의 공격은 고려하지 않는다. 이후 안전하게 등록된 참여 노드의 공개키 정보는 타임스탬프에 근거하여 관리된다. 참여 노드들은 GPS를 통해 정확한 시간 동기화가 이루어져 있기 때문에 공개키 등록 메시지의 타임스탬프 필드에는 현재 시간을 기록해야 한다. 만약 공격 노드가 생성한 특정 노드의 공개키가 정당한 공개키처럼 보이게 하려면 공격자는 공개키 등록 메시지의 타임스탬프 필드에 T_{A_I}보다 이전 시간을 기록해야 하나 현재 시간을 기록해야하는 T_{A_I}필드 값을 임의로 변경할 수 없다. 따라서 노드 A의 공개키가 등록되어 있는 상태에서 노드 C가 A인척 공개키 등록 메시지를 생성하여 플러딩 한다면 이를 수신한 다른 노드들은 등록되어 있는 공개키 정보의 타임스탬프 값과 수신 타임스탬프 값을 비교하여 위조된 공개키를 구분할 수 있게 된다.

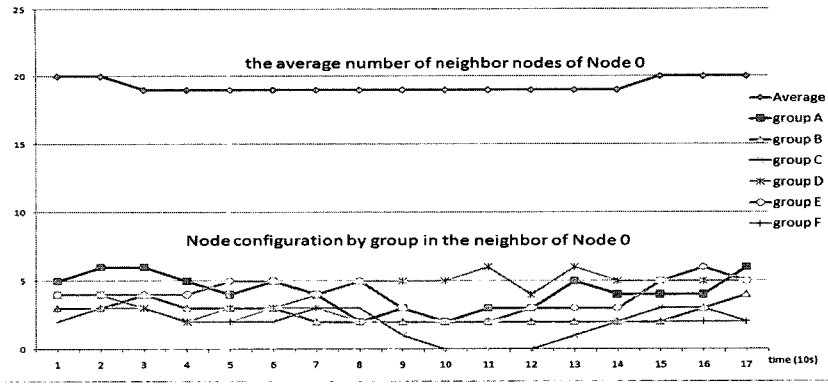
메시지의 인증은 전송구간 내에서 메시지에 사용된 서명이 참여 노드에 의해서 검증되어 메시지가 확인되면 가능하므로 다음과 같이 정리해 볼 수 있다. 애드혹 네트워크에서 노드들이 고르게 분포되어 있다고 한다면 반경 1Km^2 크기의 네트워크에 200개 노드가 존재하고 (네트워크 노드 밀도 $d(n/Km^2)$) 각 노드의 통신 반경 $r(m)$이 200m라고 하면 1개의 노드는 다음과 같이 평균 25개의 이웃노드를 갖게 된다.

노드의 이웃 노드 수

$$= d \times r^2 \times \pi = (200/Km^2) \times (0.2Km)^2 \times \pi \fallingdotseq 25$$

〔그림 3〕과 같은 방법으로 그룹핑된 노드들이 고르게 분포되어 있다고 한다면 하나의 그룹에 30개(ρ)* 의 노드가 그룹핑된다고 할 때 약 6.7개 노드 당 1개 정

* 여기서 그룹의 크기는 프로토콜의 효율성에 영향을 미치는 요소로서 그룹의 크기가 커지면 네트워크 전체에 분포하는 동일 그룹 노드의 밀도가 증가하게 되나 노드가 유지해야하는 공개키 정보의 양이 증가하게 된다. 반대로 그룹의 크기가 너무 작아지게 되면 동일 그룹 노드의 밀도가 낮아져 공개키/메시지 검증의 효율이 떨어지게 된다. 실험에서는 노드의 통신반경을 고려해 30으로 정하였으나 그룹의 크기는 환경에 따라 변경가능하다.



〔그림 7〕 노드의 평균 이웃 노드 수 변화와 이웃 노드 구성 변화

도의 동일 그룹 노드가 존재하게 된다. 즉, 임의 노드의 이웃 노드들 중 특정 그룹의 노드가 약 4개씩은 존재하게 된다.

동일 그룹 노드의 밀도 $= d / \rho = 200/30 \fallingdotseq 6.7$

식을 좀 더 구체적으로 정리하여 임의 노드에서 생성한 서명이 메시지 전송이 완료되는 시점까지 전송에 참여하는 노드로부터 검증될 확률은 해당 노드의 공개키를 소유한(동일 그룹) 노드가 전송영역 내에 하나라도 존재하게 되는 확률이므로 다음과 같이 정리될 수 있다.

일반적으로 애드혹 네트워크에서 가정하는 노드 분포는 균일 분포(uniform distribution)로서 네트워크 내에 노드들이 균일한 분포로 분산되어 있음을 가정한다.[15-17] 만약 네트워크 내의 노드 분포가 균일 분포를 따른다면 네트워크 노드 밀도 $d(n/Km^2)$, 그룹 사이즈가 ρ인 애드혹 네트워크에서의 통신반경이 $r(m)$인 노드에는 특정 그룹의 노드가 $\pi r^2 \times \rho$개 포함되게 된다. 만약 위치 요청 및 응답 메시지의 전송이 이뤄지는 K홉 구간을 생각한다면 전송 구간 내에 포함되는 특정 그룹 노드 수는 더 늘어나게 된다. 1Km^{2}에 200개 노드가 있고, ρ=30, r=200m 일 때 K가 평균 4홉이라고 하면 약 12.25개의 노드가 포함된다(홉간 중첩 영역의 크기를 $\frac{1}{4}$로 계산).

$$\left((\pi r^2 \times K) - (\frac{K-1}{4}\pi r^2)\right) \times \rho$$
$$= \left((\pi \times 0.2^2 \times 4) - (\frac{3}{4}\pi \times 0.2^2)\right) \times 30 \fallingdotseq 12.25$$

하지만 애드혹 네트워크에서 '균일하게'라는 것은 노드들이 완전하게 균일한 간격(밀도)으로 고르게 분산되어 있다기 보단 평균 밀도에 기준하여 정규 분포(normal distribution)을 따른다고 보는 것이 합당할 것이다. 즉 애드혹 네트워크 내의 노드들은 평균 밀도 d를 중심으로 하는 정규 분포 곡선을 그리면서 분포하게 되고 임의 노드 전송 영역 내에 특정 그룹 노드가 포함될 확률도 정규 분포를 따른다고 할 수 있다. 따라서 통신 반경 내에 특정 그룹 노드가 1개 이상 존재할 확률은 다음과 같이 정리될 수 있다.

$$P(x>1) = \int_a^b \frac{1}{\sqrt{2\pi\sigma}} e^{-\frac{1}{2\sigma^2}(x-\mu)^2} dx \qquad (3)$$

실험적 통계를 통해 평균과 분산 a, b의 값을 결정하면 해당 확률을 구할 수 있으나 통신 반경 내에 포함된 특정 그룹 노드의 최소 개수를 나타내는 a값이 항상 1보다 큰 값을 가지게 되고 그래프는 x>1 인 영역에서 정의되게 되어 식 (3)의 확률은 1이 된다.

여기서 위 수학적 분석 내용을 시뮬레이션을 통해 분석해 보았다. 〔그림 6〕은 시뮬레이션을 통해서 임의의 1개 노드에 포함되는 평균 이웃 노드 수를 측정한 그래프로 시각 t=0 에서 전체 노드의 평균 노드수를 나타낸 것이다. 참여 노드들은 실험 결과 그래프에서 보여 지는 것처럼 평균 22개의 이웃 노드를 가지게 된다. 평균값을 기준으로 0번부터 199번까지의 노드들은 최대 34개부터 최소 4개까지의 분포 편차를 보였다. 〔그림 7〕은 시뮬레이션 시간동안 특정 노드의 평균 노드 수 변화와 해당 노드의 이웃에 몇 개의 서로 다른 그룹 멤버가 존재하는지를 시간에 따라 나타낸 그래프이다. 실험은 1Km^{2}크기의 네트워크에 200개 노드가 분산되어 위치하고 있는 상황에서 〔그림 3〕의 (b)와 같은 그룹형성 방식을 사용해 6개 그룹을 설정하였다(a그룹=34, b그룹=34, c그룹=33, d그룹=33, e그룹=33, f그룹=33). 노드의 전송반경은 200m로 설정하였고 노드의 평균 이동속

도는 2.5m/s, 최대 이동속도는 5m/s로 설정하여 180초 동안 시뮬레이션하여 결과를 알아보았다. 그림에서 보면 시뮬레이션이 실행되는 동안 일정 수 이상의 노드들이 특정노드에 이웃노드로 존재하게 되며 따라서 일관성(consistence)있게 공개키에 대한 검증을 수행할 수 있음을 알 수 있다.

4.1.2. 공격 위협에 대한 안전성

제안하는 위치 서비스는 기존 애드혹 환경에서의 여러 공격 위협들은 물론 위치 서비스를 대상으로 한 공격 위협에도 안전하게 서비스를 제공한다.

- 거짓 위치 갱신 공격: 제안한 프로토콜에서 참여노드는 자신이 생성한 공개키/개인키를 이용하여 서명 형태로 자신의 위치 주소를 생성하고 라우팅에 사용하기 때문에 공격자는 다른 노드로 가장하여 주소를 생성하지 못하고 결과적으로 거짓 위치 갱신 메시지를 생성하지 못한다. 또한 위치 갱신 메시지는 서명되어 전송되기 때문에 수신 노드는 서명을 검증하여 메시지를 인증하고 무결성을 확인할 수 있다. 따라서 거짓 위치 갱신 공격은 계산적으로 어렵다.
- 거짓 응답 공격: *Loc_response* 메시지에 포함된 요청 노드 주소는 최초 노드 A가 개인키로 서명하여 생성한 주소로써 수신노드는 A의 공개키로 $Addr_A$를 검증하는 것으로 정당한 주소인지 여부를 결정할 수 있다. 따라서 공격 노드는 임의의 주소를 거짓 *Loc_response* 메시지에 삽입하여 거짓 응답 할 수 없다.
- 블랙 홀 공격: 제안하는 프로토콜에서 참여노드들은 자신의 위치를 알고 있기 때문에 공격자는 이웃 노드에게 자신의 위치를 거짓으로 보고 할 수 없다. 따라서 위치기반 라우팅을 사용하는 본 프로토콜에서 공격자는 모든 메시지가 자신에게 라우팅되도록 유도하지 못하게 되어 블랙 홀 공격이 불가능하다.
- 재전송 공격: 전송되는 모든 메시지에는 GPS를 통해 동기화된 타임스탬프와 메시지 일련번호가 포함되어 있기 때문에 메시지의 최신성을 증명할 수 있다.
- 웜 홀 공격: 메시지에 포함된 시간적 정보(타임스탬프)와 공간적 정보(위치정보)를 통해 공모한 공격노드에 의해 생성된 터널의 존재를 감지해 낼 수 있고 웜 홀 공격에 대응할 수 있다.
- 블랙메일 공격: *Err_alarm* 메시지는 최초 생성자가 서명하여 방송하기 때문에 메시지의 원천지를 인증할 수 있으므로 *err_type*에 따라 발생한 오류에 대해 확인하는 절차가 수반되면 블랙메일 공격에 대응할 수 있다.
- 라우팅 테이블 오염 공격: 블랙 홀 공격과 마찬가지로 공격자는 자신의 위치를 거짓으로 보고할 수 없고 위에 설명한 것처럼 재전송 공격 또한 할 수 없기 때문에 라우팅 테이블 오염 공격이 불가능하다.

4.2. 효율성 분석

본 논문의 효율성 분석에서는 보안을 고려하지 않은 기존 위치 서비스 시스템에 비해 안전한 위치 서비스를 제공하기위해 제안한 프로토콜의 노드가 추가적으로 부담해야하는 비용에 대해서 분석하고자 하며 이는 다음과 같이 정리할 수 있다.

- 네트워크 초기에 발생하는 노드의 공개키 등록비용
- 위치 갱신 시 발생하는 위치주소의 서명비용
- 위치 갱신/요청/응답 메시지의 서명비용 및 검증비용
- 서명 검증을 위해 발생할 수 있는 공개키 질의비용

하지만 공개키 시스템을 사용하는 애드혹 네트워크에서 공개키 암호화와 복호화로 볼 수 있는 서명의 검증과 생성 비용은 안전한 통신을 위한 기본비용으로 간주할 수 있기 때문에 노드가 총 몇 번의 서명을 생성하고 검증하는 지를 측정하는 것은 중요하지 않다. 대신 우리는 안전한 통신을 위해 몇 번의 추가적인 메시지 전송이 발생했는지를 측정하였다.

먼저 공개키 등록 및 초기화과정에서 노드가 추가적으로 부담해야 하는 비용에 대해서 알아보자. 애드혹 위치기반 라우팅을 위한 위치 서비스에서 노드들은 네트워크에 참여하여 통신하기위해 기본적으로 자신의 위치를 위치 서버에 등록해야 하여야 한다. 따라서 노드의 첫 위치 등록 메시지의 전송과 함께 이루어지게 되는 공개키 등록과정은 메시지의 크기와 메시지 구성 내용만 변화 시킬 뿐 추가적인 전송을 필요로 하지 않는다. 4.3절에서의 제시한 시뮬레이션 결과를 보면 공개키 등록을 위한 메시지 전송이 그룹의 형성방법에 따라 얼마

〔표 2〕 제안하는 프로토콜과 XYLS의 전송 메시지 수 비교

	XYLS〔7〕		제안하는 프로토콜 - 그룹 (a)		제안하는 프로토콜 - 그룹 (b)		비고
	홉수	메시지 수	홉수	메시지 수	홉수	메시지 수	
위치 등록 / 공개키 등록	1397	200	1397	200	4568	200	메시지 크기 증가
공개키 질의	0	0	648	90	16	4	
계	1,397	200	2,045	290	4,584	204	

나 발생했는지 알 수 있다.

공개키 질의는 위치 서비스의 기본 동작은 아니지만 제안하는 프로토콜에서 노드가 서명의 검증에 필요한 공개키를 획득하기위해 추가적으로 부담해야하는 비용으로 볼 수 있다. 〔그림 8〕의 시뮬레이션 결과를 보면 두 가지 그룹 형성 방법에 따라 시뮬레이션 시간동안 네트워크 전체적으로 몇 번의 공개키 질의가 발생했는지를 볼 수 있다. 이와 관련해서는 4.3절의 그룹 설정 방식에 따른 효율성 분석 부분에서 시뮬레이션 시간동안 몇 번의 공개키 질의가 발생했는지 등을 측정하여 자세히 분석하였다.

이상의 시뮬레이션 결과를 〔표 2〕에 정리하였다. 〔표 2〕의 홉수와 메시지 수를 보면 제안하는 프로토콜이 XYLS에 비해 많은 통신비용을 소모하는 것처럼 보이나 노드의 기본 오퍼레이션에서 발생하는 비용을 고려한다면 상대적으로는 많은 비용을 소모하는 것은 아니다. 예를 들면 위 시뮬레이션 환경에서 노드의 위치 갱신 주기는 대략 60초에서 80초가 되는데 180초의 시뮬레이션 시간 동안 약 3번의 위치 갱신 이벤트가 발생한다고 할 수 있다. 따라서 200개 노드의 총 위치 갱신 메시지 수는 600개가 되고 평균 7홉의 전송 횟수를 가지는 위치 갱신 메시지의 총 홉수는 4,200번이 된다. 여기에 위치 갱신 비용을 고려한 것처럼 위치 요청과 위치 응답 메시지의 비용도 추가로 고려해 준다면 상대적인 비용차이는 더 줄어들 것이다.

4.3. 그룹 설정 방식에 따른 효율성 분석

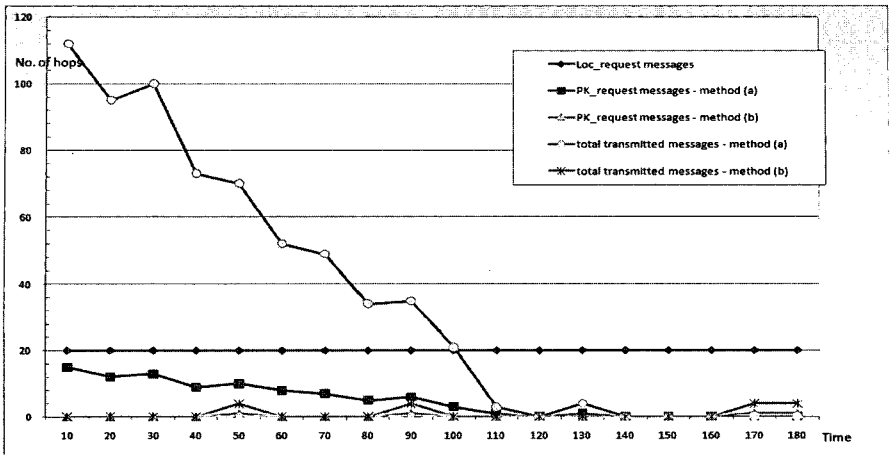
이 절에서는 3장에서 설명한 2가지 그룹설정에 따른 소요비용을 비교하여 분석한다. 3장에서 설명한 바와 같이 〔그림 3〕의 2가지 그룹 설정 방식에는 위치 서비스 운용적 측면에서의 장단이 있다. 즉 〔그림 3〕의 (a)와 같은 그룹 설정은 초기 공개키 등록비용에 있어 (b) 방법보다 효율적이지만 그룹 멤버가 자유롭게 이동하여 네트워크에 고루 분포되기 까지 서명 검증을 위해 공개키를 질의해야하는 비용이 부가적으로 발생 할 수 있다. 반대로 〔그림 3〕의 (b)와 같은 그룹 설정 방식은 그룹 멤버가 네트워크 전체에 고르게 분산되어 위치하기 때문에 공개키 등록 직후부터 안정적으로 메시지에 사용된 서명을 검증할 수 있다는 장점이 있지만 공개키 등록 메시지를 초기에 플러딩해야 한다는 단점이 있다. 본 논문에서는 시뮬레이션을 통해 이 2가지 형태의 그룹설정 방식의 효율성을 분석한다.

공개키 등록에 있어 전송의 효율성을 위한 데이터 애그리게이션(aggregation)을 고려하지 않는다고 한다면 한 개 그룹에 포함된 모든 노드가 각자 자신의 공개키 정보를 전송해야하므로 그룹의 크기가 33이고 평균 7홉*으로 전송이 이루어진다고 할 때 그룹 당 약 33 × 7 = 231번의 전송이 이루어진다. 여기서 공개키 등록 메시지의 평균 홉수가 위치 요청 및 응답의 평균 홉 수 4홉보다 큰 이유는 등록 메시지가 중간 노드에 의해 중단(응답)되는 일 없이 네트워크 전체로 메시지가 전달되어야하기 때문이다. 〔그림 3〕의 (b)와 같은 그룹 설정 방법에서는 1개 노드가 네트워크 전체에 1개의 메시지를 플러딩 할 때 실행되는 전송횟수를 t라 하면 t × 33번의 전송이 이루어지게 된다. 실험에서의 t의 평균치는 약 23이었으며 한 개 그룹이 공개키를 모두 등록하는데 평균 761번의 전송이 이루어 졌다. 761번이라는 전송 횟수는 역시 숫자적으로 많은 비용이 소모 되는 것처럼 보일 수 있으나 보안을 고려하지 않는 위치 서비스에서

〔표 3〕 그룹 별 공개키 등록 비용

n=200, r=200,							
그룹 형성 방법	그룹 별 등록 메시지 전송 홉수						
	a	b	c	d	e	f	계
그림 3-(a): ρ=33 (a:35, b:30, c:45, d:29, e:30, f:31)	246	208	302	211	210	220	1,397
그림 3-(b): ρ=33 (a:33, b:33, c:33, d:33, e:34, f:34)	755	753	749	760	770	781	4,568

* 네트워크 크기에 따라 평균 홉수가 결정된다. 위 실험에서 위치 갱신 및 공개키 등록은 평균 7홉으로 전송이 이루어졌다.



〔그림 8〕 공개키 질의 비용 분석

33개의 노드가 한 번 위치 갱신하는데 231번의 전송이 이루어지는 것을 감안한다면 네트워크 초기에 한번만 실행되는 공개키 등록 과정은 크게 부담이 되는 것은 아니다.

이제 2가지 그룹 형성 방법으로 공개키를 등록한 이후 위치 서비스가 실행됨에 따라 공개키 질의에 소요된 비용이 얼마인지를 분석해 본다. 공개키의 질의는 전송되는 모든 형태의 메시지에서 검증을 위해 발생할 수 있으며 메시지의 전송 구간 내에 해당 메시지에 사용된 공개키를 저장하고 있는 노드가 없을 때 발생한다. *Err_alarm* 메시지의 경우 전송구간내의 모든 노드가 서명을 검증하여야하나 메시지의 발생 빈도가 높지 않다는 가정 하에 제외시키고 위치 요청의 경우 메시지를 검증할 필요가 없으므로 위치 갱신 메시지와 위치 응답 메시지의 경우에 대해서만 공개키 질의 비용을 생각해 본다.

위치 갱신의 경우 메시지 검증은 같은 열에 있는 노드들을 대상으로 이루어지게 되므로 네트워크 형성 초기 공개키 질의 메시지의 생성 빈도는 〔그림 3〕의 방법 (b)보다 방법 (a)가 더 작아지게 된다. 위치 응답의 경우 메시지 검증은 위치 요청 메시지를 전송하여 위치 응답 메시지를 수신한 노드에 의해서 실행되므로(유니캐스트) 네트워크 초기에 동일 그룹 노드들이 일정지역에 모여 있게 된다면 공개키 질의를 해야 할 확률이 높아지게 된다. 따라서 〔그림 3〕의 방법 (b)가 방법 (a)보다 더 효율적이라고 할 수 있다.

여기서 공개키 등록에 소요되는 비용, 즉 통신비용은 전송비용, 수신비용, 계산비용으로 구분될 수 있는데 송신비용≫ 수신비용≫ 계산비용의 관계가 있으며[18] 전송과 수신은 비례관계에 있기 때문에 전송비용을 공개키 등록비용의 메트릭(metric)으로 간주하여 시뮬레이션 결과를 분석하였다. 〔그림 8〕의 시뮬레이션은 공개키 등록 시와 같은 환경(F: 1Km^2, N=200, r=200m, 평균 이속=2.5m/s, 최대 이속=5m/s)에서 수행한 결과로 시뮬레이션 타임 동안 매 10초간 20개의 위치 요청 이벤트를 생성 시켰을 때 공개키 질의에 관련된 메시지의 전송횟수만 계산한 결과이다. 2가지 그룹 형성 방법에 따른 공개키 질의 메시지의 경우 〔그림 3〕의 (a) 방법으로 형성된 그룹은 네트워크 초기에 생성된 위치질의 메시지에 비례하게 공개키 질의 메시지가 생성됨을 알 수 있고 그룹 (b) 방법으로 형성된 그룹의 경우는 별도의 공개키 질의 메시지 없이 안정적으로 서비스가 수행됨을 알 수 있다.

〔그림 8〕의 결과와 〔표 2, 3〕의 결과를 종합하여 네트워크 전체에 누적 홉수를 계산해보면 비용적 측면에서 〔그림 3〕의 (a)방법이 더 효율적임을 알 수 있다. 또 위 시뮬레이션 결과를 보면 〔그림 3〕에서 그룹핑된 노드들이 네트워크 전체에 걸쳐 고르게 분포되기 까지 어느 정도 시간이 소요됨을 알 수 있는데 이는 참여 노드의 평균 이동 속도와 관련이 있다. 즉 네트워크 참여노드들의 이동성이 강한 환경이라면 〔그림 3〕의 (a)와 같은 그룹 설정이 더욱 효율적일 것이며 이동성이 작고 정적인 환경이라면 〔그림 3〕의 (b)와 같은 그룹 설정이 비용적 측면에서 더 효율적일 것이다.

V. 결 론

애드혹 위치기반 라우팅에서 위치 서비스는 효율성이나 안전성에 있어 매우 중요한 부분이다. 위치 기반 라우팅을 위한 다양한 위치 서비스 프로토콜들이 제안되었으나 이들은 위치 정보를 라우팅에 사용하기 때문에 특히 민감한 위치 서비스에서의 보안을 고려하지 않고 있다. 본 논문에서는 위치 서비스의 보안 위협을 정의하고 기존 애드혹 라우팅 보안 위협 및 위치 서비스를 대상으로 한 보안 위협에도 안전한 위치 서비스를 제안하였다. 제안한 프로토콜은 메시지를 인증하고 무결성을 보장하기위해 공개키 시스템을 사용하지만 공개키 기반 구조를 사용하지는 않는다. 노드는 자신이 생성한 공개키/개인키 쌍을 이용하여 자신의 주소를 생성하고 서명하여 라우팅에 사용하며 공격자는 이미 참여하고 있는 다른 노드를 가장하여 메시지를 보내거나 공격할 수 없다. 본 논문은 시뮬레이션을 통해 제안한 라우팅 프로토콜의 안정성을 분석하였고 기존의 다양한 보안 위협에 대해서 안전하게 서비스를 제공할 수 있음을 분석하였으며 제안한 그룹 설정 방식에 따른 효율성을 분석하였다.

참고문헌

[1] S.M Das, H. Pucha, Y.C. Hu, "Performance Comparison of Scalable Location Services for Geographic Ad hoc Routing," *Proc. of the IEEE INFOCOM2005*, vol. 2, pp. 1228-1239, 2005.

[2] R. Friedman, G. Kliot, "Location Services in Wireless Ad hoc and Hybrid Networks: A Survey," Tech. Rep. TR-2006-10, Haifa Univ., 2006.

[3] S-C.M. Woo, S. Singh, "Scalable Routing in Ad hoc Networks," Tech. Rep. TR00.001, Oregon State Univ., 2000.

[4] C. Cheng, H. Lemberg, S. Philip, E. van den Berg, T. Zhang, "SLALoM: A Scalable Location Management Scheme for Large Mobile Ad-hoc Networks," *Proc. of the IEEE Wireless Comm. and Net. Conf.*, vol. 2, pp. 574-578, 2002.

[5] S. Philip, C. Qiao, "ELF: Efficient Location Forwarding in Ad hoc Networks," *Proc. of the IEEE Global Telecommunications Conf.*, vol. 2, pp. 913-918, 2003.

[6] H. Füßler, W. Kess, J. Widmer, M. Mauve, "Hierarchical Location Service for Mobile Ad hoc Networks," *ACM SIGMOBILE Mobile Comp. and Comm. Review*, vol. 8, pp. 47-58, 2004.

[7] I. Stojmenovic, "A Routing Strategy and Quorum based Location Update Scheme for Ad hoc Wireless Networks," Tech. Rep. TR-99-09, Ottawa Univ., 1999.

[8] P.G. Argyroudis, D.O Mahony, "Secure Routing for Mobile Ad hoc Networks," *IEEE Comm. Surveys & Tutorials*, vol 7, No. 3, pp. 2-27, 2005.

[9] P. Papadimitratos, Z. Haas, "Secure Routing for Mobile Ad hoc Networks," *Proc. of Comm. Net. and Distributed Sys. Modeling and Simulation Conf.*, pp. 27-31, 2002.

[10] Y.C. Hu, D.B. Johnson, A. Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad hoc Networks," *Proc. of the IEEE Workshop on Mobile Comp. Sys. and App.*, pp. 3-13, 2002.

[11] Y.C. Hu, A. Perrig., D.B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad hoc Networks," *Proc. of the 8th ACM Int. Conf. on Mobile Comp. and Net..*, pp. 12-23, 2002.

[12] M.G. Zapata, N. Asokan, "Secure Ad hoc On-demand Distance Vector routing," *ACM SIGMOBILE Mobile Comp. and Comm. Review*, vol. 6, pp. 106-107, 2002.

[13] K. Sanzgiri, B. Dahill, B.N. Levine, C. Shields, E.M. Belding-Royer, "A Secure Routing Protocol for Ad hoc Networks," *Proc. of the IEEE Int. Conf. on Net. Protocols*, pp. 78-87, 2002.

[14] R. Anderson, H. Chan, A. Perrig, "Key Infection: Smart Trust for Smart Dust,"

Proc. of the IEEE Int. Conf. on Net. Protocols, pp. 206-215, 2004.

[15] Y. Zhao, B. Li, Q. Zhang, Y. Chen, W. Zhu, "Efficient Hop ID based Routing for Sparse Ad hoc Networks," *Proc. of the IEEE Int. Conf. on Net. Protocols*, pp. 179-190, 2005.

[16] K. Yamamoto, S. Yoshida, "Analysis of Distributed Route Selection Scheme in Wireless Ad hoc Networks," *Proc. of the IEEE Int. Symp. on Personal Indoor and Mobile Radio Comm.*, vol. 1, pp. 584-588, 2004.

[17] Y. Ganjali, A. Keshavarzian, "Load Balancing in Ad hoc Networks: Single-path Routing vs. Multi-path Routing," *Proc. of the IEEE INFOCOM2004*, vol. 2, pp. 1120-1125, 2004.

[18] R.C. Shah, D. Petrovic, J.M. Rabaey, *Energy Aware Routing and Data Funneling in Sensor Networks, Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems*, CRC Press LLC, 2005.

〈著者紹介〉

임 지 환 (Jihwan Lim) 학생회원
2005년 2월 : 한양대학교 전자컴퓨터공학부(학사)
2007년 2월 : 한양대학교 컴퓨터공학과(석사)
2007년 2월~현재 : 한양대학교 컴퓨터공학과 (박사과정)
<관심분야> 네트워크 보안
URL:http://infosec.hanyang.ac.kr/jhlim/

김 상 진 (Sangjin Kim) 종신회원
1995년 2월 : 한양대학교 전자계산학과(학사)
1997년 2월 : 한양대학교 전자계산학과(석사)
2002년 8월 : 한양대학교 전자계산학과(박사)
2003년 3월~현재 : 한국기술교육대학교 인터넷미디어공학부 조교수
<관심분야> 암호기술 응용
URL:http://infosec.kut.ac.kr/sangjin/

오 희 국 (Heekuck Oh) 종신회원
1983년 : 한양대학교 전자공학과(학사)
1989년 : 아이오와주립대학 전자계산학과(석사)
1992년 : 아이오와주립대학 전자계산학과(박사)
1993년~1994년 : 한국전자통신연구원 선임연구원
1995년 3월~현재 : 한양대학교 컴퓨터공학과 부교수
<관심분야> 암호프로토콜, 네트워크 보안
URL:http://infosec.hanyang.ac.kr/~hkoh/