애드혹 위치기반 라우팅을 위한 안전한 위치 서비스

임 지 환*, 김 상 진**, 오 희 국*

*한양대학교 컴퓨터공학과, **한국기술교육대학교 인터넷미디어공학부

Secure Location Service for Ad hoc Position-based routing

Jihwan Lim*, Sangjin Kim**, Heekuck Oh*

*Department of Computer Science a Engineering, Hanyang University
**School of Internet Media Engineering, 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 부분이며 본 논문에서는 안전한 위치 서비스 프로토콜을 제안한다. 제안한 프로토콜은 메시지를 인증하고 무결성을 보장하기 위해 공개키 시스템을 사용하지만 PKI(Public Key Infrastructure) 기반구조를 사용하지는 않는다. 노드는 자신이 생성한 공개키/개인키 쌍을 이용하여 자신이 소유주임을 주장할 수 있는 위치 주소를 생성하여 라우팅에 사용하게 되며 공격자는 이미 참여하고 있는 다른 노드를 가장하여 메시지를 보내거나 공격할 수 없다. 제안한 프로토콜은 기존에 존재했던 다양한 공격들에 대해 안전하며 위치 서비스를 대상으로 한 공격에도 안전하게 대응할 수 있다.

I. 서론

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

* 본 연구는 한국과학재단 특정기초연구(R01-2006-000-10957-0) 지원으로 수행되었음.

* 이 연구에 참여한 연구자는 '2단계 BK21 사업'의 지원을 받았음.

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 중앙 집중식 형태보다는 참여 노드 각각이 일부 노드의 위치정보를 관리하는 분산된 형태의 위치 서버가 더 적합하다. 분산된 형태의 위치 서비스에 관한 연구는 Home Region형[1-4]과 Quorum형[5-7]으로 다시 분류할 수 있다[8,9].

효율적인 라우팅에 관한 연구와 병행하여 애드혹 네트워크에서는 안전한 라우팅에 관한 연구가 계속 되어왔다[10-14]. 안전한 위치 서비스에 대한 연구는 기본적인 애드혹 라우팅 보안 요구사항 뿐만 아니라 위치정보를 경로 탐색에 사용하는 하기 때문에 발생하는 추가적인 공격에 대한 고려가 필요하다.

II. 관련 연구

1. 애드혹 라우팅에서의 보안

애드혹 네트워크에서는 기간망이 없는 가운데 참여노드 스스로가 라우터 역할을 수행하기 때문에 많은 보안적 위협을 가지고 있다. 이에 가능한 공격들을 분류해 보면 다음과 같은 공격들이 있다.

- 위치 노출(location disclosure) 공격: 트래픽 분석 기법이나 모니터링 등에 의한 방법으로 특정 노드의 위치정보를 획득하고 지속적으로 위치를 감시할 수 있는 공격.
- 블랙 홀(black hole) 공격: 공격 노드가 라우팅 경로 설정에 있어 거짓 정보를 흘려보내 자신을 포함한 경로가 최적 경로인 것처럼 속여 획득한 패킷을 드랍하거나 선택적으로 포워딩하는 공격.
- 재전송(replay) 공격: 이전에 획득한 메시지를 재전송하여 공격으로 최근에 사용된 메시지를 캡춰하여 변조 후 여러 공격에 사용함.
- 웜 홀(wormhole) 공격: 두 개 이상의 공격 노드가 협력하여 이루어지며 두 노드간의 터널링을 통해 메시지를 가로채는 공격으로 가로챈 메시지를 선택적으로 포워딩함으로써 공격의 여부를 알아차리기 힘든 특징이 있음.
- 블랙메일(blackmail) 공격: 공격자의 존재나 에러의 발생을 계속적으로 허위보고하여 잘못된 블랙리스트를 생성하게 하는 공격.
- 라우팅 테이블 오염(routing table poisoning) 공격: 공격 노드가 거짓 정보를 흘려 보내거나 정당한 라우트 업데이트 패킷을 위·변조하여 올바른 라우팅 경로 설정을 방해하는 공격.

이상의 공격들에 대응하기 위해서 기존에 제안된 많은 논문들은 공개키/대칭키에 기반한 프로토콜들을 제안하고 있으나 노드의 참여와 이탈이 자유롭게 이루어지는 환경에서 모든 노드쌍이 서로 비밀 정보를 공유하고 있다고 가정한다거나[11-13] 기간망을 사용하지 않는 애드혹 환경에서 공통된 CA(Certificate Authority)를 갖는 PKI 기반구조를 이용한다는 가정[10,14]은 현실적이지 못하다고 하겠다.

2. 위치 서비스의 보안

공격자는 위치 서비스가 정상적인 서비스를 하지 못하게 하기위해 다음과 같은 공격을 시도하게 된다.

- 위장 공격: 공격 노드는 특정 노드를 가장하여 노드의 위치를 거짓으로 업데이트 하고 잘못된 위치정보를 유지하게 하는 공격.
- 패킷 변조 공격: 공격 노드는 다른 노드의 정상적인 위치 갱신 패킷을 캡춰하고 거짓 위치정보를 삽입함으로써 잘못된 위치정보를 업데이트 하게 하는 공격.
- 거짓 응답 공격: 공격 노드는 특정노드의 위치를 요청하는 메시지에 대해 거짓 응답 메시지를 생성하여 잘 못된 위치정보를 알려주는 공격.

III. 제안하는 프로토콜

1. 가정

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.

- 자신이 통신하고 싶어 하는 노드의 ID 정보를 알고 있다고 가정한다.

보안요소에 대해서는 다음과 같이 가정한다.

- 참여 노드는 스스로 공개키/개인키 쌍을 생성할 수 있다.
- 위치기반 라우팅에 사용되는 주소는 GPS로부터 획득한 지리적 위치와 기타 정보를 appendix형으로 서명하여 생성한 값이다.

2. 안전한 위치 서비스

제안하는 프로토콜은 세로방향(column)으로 자신의 위치정보를 갱신하고 가로방향(row)으로 특정 노드의 위치정보를 요청하는 I. Stojmenovic.의 프로토콜[15]과 같은 형식의 위치 서비스 프로토콜이다.

a) 표기법

A	Node A의 ID
A_{PK}	Node A의 공개키
A_{PR}	Node A의 개인키
$Sig_A(msg)$	msg를 A의 개인키로 서명함
T_{A_I}	최초 공개키를 생성한 시간을 나타내는 타임스탬프
T_{A_C}	현재 시간을 나타내는 타임스탬프
Pos_A	GPS로 획득한 A의 지리적위치(좌표)
$Addr_A$	Pos_A를 서명한 형태의 A의 지리적주소 $Addr_A = Sig_A(A\|\|Pos_A\|\|T_{A_I}\|\|T_{A_C})$

b) Location initiation: 네트워크에 참여한 노드들은 다음과 같은 *Loc_init* 메시지를 최초 한번만 네트워크 전체에 방송한다.

$$Loc\_init = [Type, Seq, A_{PK}, Addr_A]$$

먼저 소스 노드 A는 자신의 공개키/비밀키 쌍을 생성하고 GPS로 획득한 위치 정보와 타임스탬프 값으로부터 주소 $Addr_A$를 생성하여 메시지를 구성한다. 여기서 *Type*은 메시지의 타입을 나타내고 Seq는 루프를 방지하고 중복된 메시지를 구분할 수 있게 하는 시퀀스넘버를 나타낸다. 모든 참여 노드는 다음과 같은 형태의 Location Table을 유지하고 있으며 *Loc_init* 메시지를 수신한 노드들은 자신의 Location Table에 수신한 노드의 정보를 업데이트 한다.

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

테이블에 저장되는 Γ 값은 각 노드들의 신뢰도를 나타내는 값으로 이 값이 임계치 이하로 내려간 노드는 공격노드로 간주된다. 결국 노드들은 네트워크에 참여하고 있는 모든 노드들의 아이디/공개키 쌍을 유지하고 있게 되며 이때 등록된 아이디/공개키 쌍이 PKI의 공개키 인증서를 대신하게 된다.

c) Location update: 참여 노드들은 주기적으로 또는 일정거리 이상을 이동하게 되면 다음과 같은 형태의 *Loc_update* 메시지를 세로방향(column)으로 방송한다.

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

메시지를 수신한 노드는 서명을 검증하여 메시지를 인증하며, 검증되면 자신의 Location Table에 위치 정보를 갱신하고 메시지를 재전송 한다. 메시지의 인증은 프로토콜 정책적으로 결정되는 일부 노드만이 서명을 검증하여 오류 발생시 *Err_alarm* 메시지를 방송하는 것으로 다른 노드의 공개키 연산에 대한 부담을 줄여 줄 수 있다. 예를 들면 '*TTL%3*'과 같이 인수를 설정하면 3홉당 한 번씩 메시지를 검증하게 된다. *width*는 전송하는 메시지의 전송 폭을 결정하는 인자 값이다. 즉 *width*가 1로 설정되어 있다면 세로 방향으로 업데이트 되는 업데이트 패킷은 가로로 1홉 거리의 노드들을 포함하는 폭을 가지고 세로로 전파되어 진다는 의미이다. 수신 노드가 $Addr_A$를 따로 검증할 필요는 없으며 특정 노드가 A의 위치를 요청하면 저장하고 있던 주소 $Addr_A$를 요청하는 노드에게 그대로 전송한다.

d) Location request: 참여 노드들은 특정 노드의 현재 위치를 알아내기 위해 가로방향(row)으로 다음과 같은 *Loc_request* 메시지를 전송한다.

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

msg의 구성은 메시지 타입, 시퀀스넘버, 대상 노드 ID, 자신의 주소로 이루어져 있으며 메시지에 대한 검증은 앞의 location update와 과정과 같다. *Loc_request* 메시지를 수신하고 A의 위치 정보를 가지고 있는 노드는 msg의 타임스탬프와 자

신의 Location Table의 타임스탬프를 비교해 만료기간이 지나지 않은 정보라고 판단될 시 *Loc_response* 메시지를 보내 응답한다.

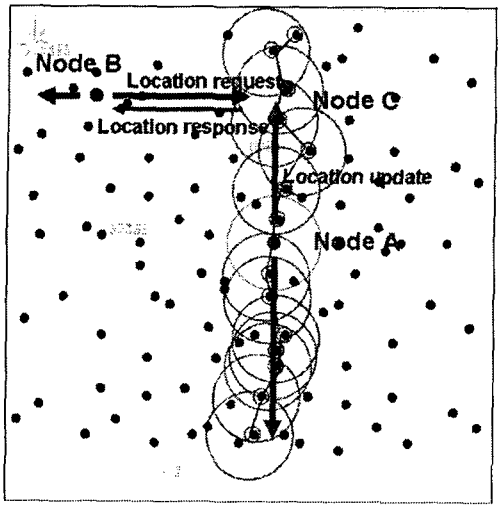

그림 2 위치서비스 개요 - 세로 방향으로 위치를 갱신하고 가로방향으로 질의한다.

e) Location response: *Loc_response* 메시지는 유니캐스트(unicast)로 요청 노드에게 전송되어지며 다음과 같은 형태로 구성된다.

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

위 메시지는 노드 B에게 C가 A의 위치를 알려주는 *Loc_response* 메시지이다.

f) Security management: 메시지 전송에 참여하는 노드는 자신이 전송한 메시지를 이웃 노드가 제대로 포워딩하는지 여부를 모니터링한다. 이상 행동이 감지되었을 경우 노드는 다음과 같은 *Err_alarm*메시지를 세로와 가로방향으로 방송한다.

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

Err_alarm 메시지를 수신한 노드는 메시지를 검증한 후 Location Table에서 *err_type*에 따라 해당노드의 신뢰수치를 감소시키고 다시 방송한다. 이 때 신뢰수치가 임계치 이하로 떨어진 노드가 발생하면 이 노드를 공격노드로 가정하고 네트워크 전체로 *Err_alarm* 메시지를 방송하여 해당 공격노드를 차단한다.

IV. 안전성 분석

본 논문은 공개키 기반구조를 사용하지 않는 대신 각자의 ID, 공개키 쌍 정보를 네트워크 참여 초기에 등록하는 과정을 거침으로써 축소된 형태의 공개키 시스템을 사용할 수 있다. 참여 하지 않은 노드의 정보를 먼저 등록하는 식의 공격은 무의미하기 때문에 고려하지 않으며 등록을 마친 노드는 공개키 기반구조 없이도 안전하게 통신할 수 있다.

- 위장 공격: 제안한 프로토콜에서 참여 노드는 자신이 생성한 공개키/개인키의 서명 형태로 자신의 위치 주소를 사용기 때문에 공격자들은 다른 노드로 가장하여 주소를 생성하지 못하고 메시지를 생성하지 못한다. 따라서 위장 공격은 불가능 하다.
- 패킷 변조 공격: 제안한 프로토콜은 공개키 시스템의 서명을 사용하고 있으므로 수신노드는 서명을 검증하여 메시지를 인증하고 무결성을 확인할 수 있다.
- 거짓 응답 공격: *Loc_response*에 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: 공격노드는 이웃 노드에게 자신의 위치를 거짓으로 보고 할 수 없기 때문에 위치기반 라우팅을 사용하는 본 프로토콜에서는 블랙 홀 공격이 불가능하다.
- 재전송 공격: 전송되는 모든 메시지에는 GPS를 통해 동기화된 타임스탬프와 메시지 시퀀스넘버가 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: 공격 노드는 패킷을

재전송 하거나 위·변조 하지 못하고 자신의 위치를 거짓으로 보고하지 못하기 때문에 라우팅 테이블 오염 공격이 불가능 하다.

- 위치 노출 공격: 위치정보를 라우팅에 사용하는 위치기반 라우팅의 특성과 모든 참여 노드가 각각 특정 노드의 위치 서버역할을 수행하는 프로토콜의 특성상 내부 공격자에 의한 위치정보의 노출에는 대응하기 어렵다.

V. 결론

이 논문에서는 공개키 기반구조를 사용하지 않으면서도 인증 가능한 주소를 사용하여 안전하게 위치기반 라우팅을 할 수 있게 하는 위치 서비스 프로토콜을 제안하였다. 공격노드는 네트워크에 참여하고 있는 다른 노드로 가장하지 못하고 메시지 위조 공격 또한 불가능하며 다른 노드의 위치를 거짓으로 응답할 수도 없기 때문에 안전한 위치 서비스를 제공할 수 있다.

참고문헌

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

[2] 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.

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

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

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

[6] G. Karumanchi, S. Muralidharan, and R. Prakash,. "Information Dissemination in Partitionable Mobile Ad hoc Networks," Proc. of the IEEE Sym. on Reliable Distributed Sys., pp 4-13, 1999.

[7] Z.J. Haas and B. Liang. "Ad hoc Mobility Management with Randomized Database Groups," Proc. of the IEEE Int. Conf. on Comm., pp. 1756-1762, 1999.

[8] S.M Das, H. Pucha and Y.C. Hu, "Performance Comparison of Scalable Location Services for Geographic Ad Hoc Routing," Proc. of the IEEE Comp. and Comm. Societies, vol.2, pp. 1228-1239, 2005.

[9] T. Camp, J. Boleng, and L. Wilcox, "Location Information Services in Mobile Ad hoc Networks," Proc. of the IEEE Int. Con. on Comm., pp. 3318-3324, 2002.

[10] 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.

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

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

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

[14] M.G. Zapata, and N. Asokan, "Secure Ad hoc On-demand Distance Vector routing," ACM Mobile Comp. and Comm. Review, vol. 3, no. 6, pp. 106-107, 2002.

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