무선 메쉬 네트워크에서 악의적인 노드를 차단하기 위한 공개키 기반 메쉬 라우터 인증 기법

이광현*, 홍충선**
경희대학교 컴퓨터공학과
e-mail: khlee@networking.khu.ac.kr*, cshong@khu.ac.kr**

A PKI based Authentication Scheme for Mesh Router to Protect Against Malicious Node in Wireless Mesh Network

Kwang Hyun Lee*, Choong Seon Hong**
Dept of Computer Engineering, Kyung Hee University

요 약

무선 메쉬 네트워크는 무선 네트워크 환경을 구성하는 방안들 중 비교적 낮은 비용으로 서비스 지역을 효율적으로 늘릴 수 있다. 그러나 무선 네트워크의 특성상 많은 보안상의 문제점이 나타나고 공격 형태 또한 다양화 되고 있다. 특히 악의적인 노드에 의한 공격은 네트워크 성능을 저하시키거나 파괴시킬 수 있다. 현재 이러한 취약점을 해결하기 위해 많은 보안 메커니즘들이 나와 있지만 이 또한 완벽히 해결하지 못했다. 기존 공개키 기반 알고리즘은 인증된 노드들의 오류 동작과 인증된 노드가 악의적 해커에 의해 감염된 경우 차단할 수 없다. 본 논문에서는 이러한 무선 메쉬 네트워크에서 악의적인 노드를 차단하기 위해 기존 공개키 기반 알고리즘의 문제점을 보완한 메쉬 라우터 인증 기법을 제안한다.

1. 서론

무선 네트워크를 구성하는 많은 방법 중 무선 메쉬 네트워크(WMNs : Wireless Mesh Networks)[1]는 광범위한 지역에 효율적으로 무선 네트워크 망을 구축할 수 있다. 최근 많이 사용되고 있는 Wi-Fi의 경우는 서비스지역을 늘리기 위해서는 고가의 라우터를 배치해야한다[2]. 그러나 무선 메쉬 네트워크의 경우는 Wi-Fi에 비해서 저렴한 비용으로 서비스지역을 늘릴 수 있다.

무선 메쉬 네트워크는 MANET(Mobile Ad-hoc Network)과 비슷한 형태를 하고 있다[3]. MANET과 무선 메쉬 네트워크는 공통적으로 누구나 접근 가능한 무선 환경의 특성 때문에 높은 보안 단계를 적용해야 하지만 MANET의 경우 성능 상의 제약 때문에 높은 보안단계의 적용이 어렵다. 그러나 무선 메쉬 네트워크의 경우는 MANET에 비해 높은 성능 구현이 가능하므로 MANET과는 다른 보다 높은 레벨의 보안적용이 가능하다. 본 논문에서는 무선 메쉬 네트워크에 최적화된 보안 알고리즘을 적용하기 위해 기존 공개키 기반(PKI : Public Key Infrastructure)의 메쉬 라우터 인증 기법에 대하여 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 무선 메쉬 네트워크에 대한 간략한 설명과 무선 메쉬 네트워크에서 악의적인 노드에 의한 보안상 문제점에 대해 설명한다. 또한 3장에서는 Wormhole과 같은 악의 적인 노드를 차단하기 위한 공개키 기반의 메쉬 라우터 인증 알고리즘에 대해서 제안하고 4장에서 제안된 알고리즘의 공격 방어 시나리오에 대해 기술한다. 5장에서 성능평가를 기술하고 마지막으로 6장에서 결론 및 향후 연구과제에 대해서 설명한다.

"본 연구는 지식경제부 및 정보통신연구진흥원의 대학IT연구센터 지원사업의 연구결과로 수행되었음" (IITA-2009-(C1090-0902-0016))

2. 관련 연구

2.1 무선 메쉬 네트워크

무선 메쉬 네트워크는 기본적으로 메쉬 라우터와 메쉬 클라이언트로 구성되어 진다. 메쉬 라우터는 이동성을 가지지 않으며 메쉬 라우터 사이는 높은 대역폭의 무선으로 연결되어 있다. 메쉬 클라이언트는 메쉬 라우터를 통해 인터넷 게이트웨이 메쉬 라우터에 연결되고, 인터넷 게이트웨이 기능을 갖는 메쉬 라우터를 통해 인터넷에 연결할 수 있다. 또한 메쉬 라우터는 self-configuration, self-healing, self-organization 기능을 가지고 있어서 스스로 네트워크를 구성하고 수정할 수있다.

2.2 무선 메쉬 네트워크의 보안 문제점

무선 메쉬 네트워크는 누구나 접근 가능한 무선 환경의 특성 때문에 많은 위협에 노출되어 있고 그 공격형태 또한 다양해지고 있다. 경로를 설정하는 과정에서도 악의적인 클라이언트나 메쉬 라우터의 공격에 의해 정상적인 통신이 방해 될 수 있다. 본 절에서는 악의적인 노드에 의한 공격 중 탐지가 어렵고 치명적인 2차 공격이 가능한 Wormhole Attack[4]에 대해 설명한다.

무선 메쉬 네트워크에서의 Wormhole 노드들은 정상적인 노드인 것처럼 무선 메쉬 네트워크에 포함이 되어있다. Wormhole Attack의 특징은 다른 라우팅 공격과는 다르게 단일 노드의 공격이 아닌 2개 이상의 노드들로 구성되어

있다. 이렇게 배치된 Wormhole 노드들은 서로 최적화된 방법으로 터널을 구성한다. Wormhole 노드는 이렇게 구성된 터널을 이용하여 주변노드들로 하여금 터널을 통해서 경로를 구성하도록 유도한다. 비용적인 측면으로 봤을 때 Wormhole 노드를 통한 경로구성은 유용한 것처럼 보이지만 이렇게 구성된 경로의 Wormhole 노드들은 패킷 조작, 패킷 드롭 등 2차적인 공격이 가능해서 Wormhole 노드의 발견 및 Wormhole 노드를 거치지 않는 경로 구성이 필요하다.

3. 제안하는 무선 메쉬 네트워크 보안을 위한 공개키 기반 메쉬 라우터 인증 기법

Wormhole Attack과 같이 악의적인 노드에의한 모든 공격들은 인증되지 않은 노드들에 의해 발생될 수 있는 공격들이다. 따라서 메쉬 라우터들에 대한 확실한 인증이 보장된다면 악의적인 노드에 의한 공격은 발생되지 않을 것이다. 이장에서는 악의적인 목적을 갖는 노드들의 공격을 차단하기 위한 공개키 기반의 메쉬 라우터 인증 기법에 대해 설명한다.

3.1 공개키 기반의 라우터 인증 기법

공개키 기반의 라우터 인증 알고리즘을 제안하기에 앞서 다음과 같이 가정한다. CA(Certification Authority)는 모든 정상적인 메쉬 라우터에 대한 리스트와 암/복호화 키를 가지고 있다. 그리고 모든 메쉬 라우터는 해시함수와 CA의 공개키를 가지고 있다. 라우팅 알고리즘으로는 DSR(Dynamic Source Routing)[5]을 사용한다.

각 라우터는 경로를 설정할 때 RREQ 메시지를 주변의 노드에게 전달하는데 이때 RREQ 메시지의 포맷은 (그림 1)과 같다. DSR 알고리즘의 RREQ 메시지에 추가적으로 메쉬 라우터의 디지털 서명을 추가하여 실제 라우터가 해당 경로를 기록했는지를 판단한다. 메쉬 라우터가 RREQ 메시지를 수신하게 되면 포함되어 있는 Random 메시지를 비밀키(KRa)를 이용하여 서명 값을 생성하고, 서명 값을 경로 저장 공간에 추가한다.

SEQ	Source Address	Destination Address	Path	Digital Signature	...	Path	Digital Signature
Random Message							

(그림 1) 제안하는 RREQ 패킷 포맷

메쉬 라우터를 인증하는 방법에는 중간 노드가 직접적으로 인증하는 방법과 중간 노드는 단지 WPA(Wormhole Prevention Algorithm)[6]의 WPT(Wormhole Prevention Time)에 의해서 드롭만 실시하고 소스 노드가 경로 상 라우터를 일괄적으로 인증하는 방법이 있다.

3.1.1 중간 노드에 의한 메쉬 라우터 인증

다음 홉 노드의 RREQ메시지가 브로드캐스팅 되고 그 메시지가 WPT 시간 안에 이전 홉 노드에게 overhearing 되면 이전 홉 노드는 이를 CA의 공개키로 암호화한다. 그리고 RAREQ(Router Authentication Request)와 암호화된 RREQ메시지를 CA에게 보낸다. RAREQ 메시지는 (그림 2)와 같이 경로 상 라우터가 실제로 서명했는지 판단하기 위해 CA에게 인증을 요청하는 메시지이다. CA는 중간 노드가 보낸 RAREQ메시지를 복호화 하고 이전 노드의 서명과 등록되어있는 실제 서명을 비교한다. 이 방법의 경우 악의적인 노드를 빠르게 발견하고 역 추적하는 것이 가능하지만 너무 많은 트래픽이 발생하여 네트워크에 과부하를 줄 수 있다.

			E_{KRCA}				
Type	SEQ	Source Address	$Path_1$	Digital Signature	...	$Path_n$	Digital Signature
Random Message							

(그림 2) 제안하는 RAREQ 패킷 포맷

3.1.2 소스 노드에 의한 메쉬 라우터 인증

중간 노드는 다음 홉 노드가 보낸 메시지를 overhearing 한다. 이때 지정된 WPT 이내에 메시지가 도착하지 않으면 패킷을 드롭 시키기만 하고 별도로 CA에게 RAREQ메시지를 보내지 않는다.

소스노드가 보낸 RREQ 메시지가 목적지에 도달하게 되면 목적지 노드가 RREP 메시지와 CA의 공개키로 암호화된 RAREQ 메시지를 소스노드에게 전송한다. RREP 메시지를 수신한 소스 노드는 첨부된 RAREQ 메시지를 CA에게 전송한다. RAREQ 메시지를 수신한 CA는 중간 노드들에 대한 서명을 실제 라우터 서명 값과 비교한 뒤, 요청 노드에게 RAREP(Router Authentication Reply) 메시지를 보낸다. (그림 3)에서도 알 수 있듯이 RAREP 메시지는 정상적인 메쉬 라우터인지 아닌지 여부를 판단하여 경로 뒤에 명시하여 요청노드에게 보내진다. 이때 다른 노드에 의해 변조되는 경우를 차단하기 위해 메쉬 라우터 인증 결과 부분을 요청 노드의 공개키로 암호화하여 전송한다. 이 방법의 경우 중간노드에 의한 메쉬 라우터 인증 방법보다 낮은 트래픽이 발생되지만 만일 악의적인 노드가 WPT 이내에 RREQ를 발생시킨다면 목적지 노드의 RREP 패킷을 기다려야 하는 단점이 있다.

			E_{KUSN}				
Type	SEQ	Destination Address	$Path_1$	Positive or Negative	...	$Path_n$	Positive or Negative

(그림 3) 제안하는 RAREP 패킷 포맷

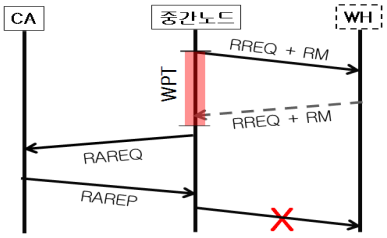
3.2 메쉬 라우터 신뢰도 테이블

메쉬 라우터들은 주변노드 혹은 자신이 판단한 이웃 메쉬 라우터에 대한 정보를 이용해 메쉬 라우터 신뢰도 테이블을 작성한다. 메쉬 라우터의 경우 다중경로 라우팅 프로토콜을 사용하므로 주변 노드로부터 이웃노드에 대한 메시지를 수신하고 라우팅 신뢰도 테이블에 적용시킬 수 있다. 따라서 한 개의 비정상 노드가 존재하는 네트워크가 있다고 가정하면 그 주변 노드들은 비정상적인 노드를 발견하게 될 것이고 이는 라우터 신뢰도 테이블에 반영된다. 일정 이상의 비정상 노드메시지를 통보받은 이웃노드에대

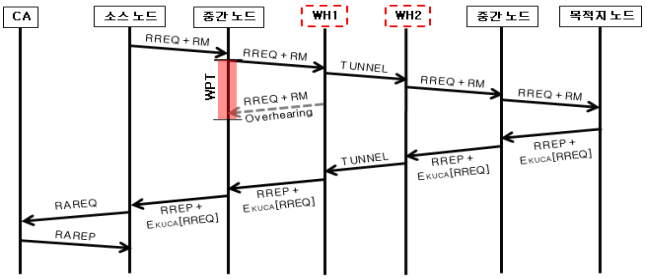
해서 악의적인 노드라고 판단하고 이를 라우팅 테이블에서 제외시킨다.

4. 제안하는 공개키 기반 메쉬 라우터 인증 기법 시나리오

본 절에서는 앞서 설명한 Wormhole 공격의 차단에 대한 공격방어 시나리오에 대해 설명한다. 중간 노드는 소스 노드로부터 받은 RREQ 메시지를 다시 브로드 캐스트하고 이웃노드의 브로드 캐스트를 기다린다. 만약 Wormhole 노드가 브로드 캐스팅 기능이 없어서 단지 포워딩만 한다면 RREQ 메시지는 WPT 안에 도착할 수 없을 것이다. Wormhole 1이 중간 노드에게 거짓으로 WH 2의 이웃노드로 위장하여 브로드 캐스팅하는 경우 중간노드 또는 소스노드에 의한 메쉬 라우터 인증기법을 통해 차단할 수 있다. 중간 노드에 의한 메쉬 라우터 인증 기법의 경우 (그림 6)와 같이 직접적으로 CA에게 RAREQ 메시지를 보내고 RAREP메시지를 확인하여 악의적인 노드 여부를 판단한다.



(그림 6) 중간 노드에 의한 메쉬 라우터 인증 기법



(그림 7) 소스 노드에 의한 메쉬 라우터 인증 기법

(그림 7)은 소스 노드에 의한 메쉬 라우터 인증 기법에 대해 나타내고 있다. 소스 노드에서 출발한 RREQ 메시지가 목적지 노드에 도착하면 목적지 노드는 패킷이 전송된 경로와 메쉬 라우터의 디지털 서명 값을 함께 CA의 공개키로 암호화한다. 그리고 RREP 패킷과 함께 암호화된 메시지를 소스노드에게 전송한다. 전송 시 전송경로와 디지털 서명 값을 암호화하는 이유는 중간에 Wormhole 노드가 패킷을 조작할 수가 있기 때문이다. CA의 공개키로 암호화된 전송 경로와 디지털 서명 값을 CA에게 전송하면 CA는 자신의 개인키로 복호화 하여 이 경로의 무결성을 확인 하고 소스노드에게 RAREP 메시지를 보낸다. 따라서 Wormhole 노드가 브로드 캐스팅 기능을 가지고 있어도 메쉬 라우터의 디지털 서명 값에 의해 그 경로는 차단될 수 있다.

5. 성능 평가

본 논문에서 제안된 알고리즘은 기존 무선 메쉬 네트워크에서의 공개키 기반 알고리즘 보다 보안이 강화되었다. 본 논문에서 제안된 기법은 최초 인증된 메쉬 라우터라도 경로를 재설정하는 경우 서명 값을 확인함으로서 악의적인 노드의 라우팅 공격을 차단할 수 있다.

본 논문에서 제안한 기법은 공개키 기반 알고리즘과 WPA의 단점을 상호 보완한다. 공개키 기반의 알고리즘은 인증된 노드에 의한 오류 동작 혹은 해커에 의해 감염된 경우에도 메쉬 라우터의 서명 값을 통해 차단할 수 있다. 또한 WPA의 WPT를 통해 보다 효율적으로 브로드 캐스팅 기능이 없는 악의적인 노드를 차단할 수 있다. 한편으로 WPA의 경우 브로드 캐스팅 기능 있는 악의적인 노드를 차단 할 수 없었지만 메쉬 라우터의 서명 값을 통해 실제 라우터 서명값과 비교하여 악의적인 노드를 차단할 수 있다.

6. 결론 및 향후 연구 과제

무선 메쉬 네트워크는 MANET보다 높은 성능의 구현이 가능하므로 보안 레벨을 높일 필요성이 있다. 본 논문은 무선 메쉬 네트워크 환경에 적합한 보다 강화된 메쉬 라우터 인증 기법에 대해 제안하고 있으며 이렇게 적용된 알고리즘은 Wormhole 공격뿐만 아니라 다른 악의적인 노드들에 의한 공격 차단을 할 수 있다.

향후 연구과제로는 공개키 기반의 알고리즘 특성상 각 노드에 과부하가 걸릴 위험이 있으므로 보다 경량화 된 알고리즘 개발하고 최적화된 암호화 알고리즘 적용이 필요하다.

참고문헌

[1] IAN F. AKYILDIZ, “A Survey on Wireless Mesh Networks”, IEEE Radio Communications, September 2005

[2] Ben Salem, N. Hubaux, J.-P, “Securing wireless mesh networks”, Wireless Communications, IEEE, Volume 13, Issue 2, 50-55, April 2006

[3] Deepti Nandiraju, Lakshmi Santhanam, Nagesh Nandiraju, and Dharma P. Agrawal, “Achieving Load Balancing in Wireless Mesh Networks Through Multiple gateways”, Mobile Adhoc and Sensor Systems (MASS), 807-812, Oct. 2006

[4] Glass. S, Portmann. M, Muthukkumarasamy. V, “Securing Wireless Mesh Networks”, Internet Computing, IEEE, Volume 12, Issue 4, 30 - 36, July-Aug. 2008

[5] David B. Johnson, David A. Maltz, "Dynamic Source Routing in Ad Hoc Wireless Networks", Mobile Computing, 1996

[6] Sun Choi, Doo-young Kim, Do-hyeon Lee, Jae-il Jung, “WAP:Wormhole Attack Prevention Algorithm in Mobile Ad Hoc Networks”, 2008 IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, 343 - 348, 11-13 June 2008