MANET에서 wormhole 공격의 탐지 및 방지를 위한 알고리즘에 대한 연구
Study on the wormhole detection and prevention algorithm for MANET

김재홍, 김세헌
대전광역시 유성구 구성동 373-1 한국과학기술원 산업공학과
E-mail : jkim@tmlab.kaist.ac.kr;shkim@kaist.ac.kr

Abstract

In Mobile ad hoc networks (MANET), nodes could transmit packets for each other to communicate beyond their transmission range without centralized control. Unlike infrastructure-based wireless networks, due to the unique characteristics of MANETs such as open network architecture, stringent resource constraints and highly dynamic network topology, networks are vulnerable to wormhole attacks launched through colluding nodes. In this paper, we develop an wormhole detection and prevention algorithm for MANET.

I. 서론

MANET(Mobile Ad-hoc NETwork)는 다수의 독립적인 노드들이 서로 연결되어 기존의 중앙 기지국을 통한 중앙 집중적인 네트워크의 관리가 필요 없이 분산적인 통제를 통해 전송 거리 밖의 노드들과도 통신이 가능케 만든 무선 이동 네트워크이다. 이런 MANET은 새로운 노드들의 자유로운 네트워크 접속이 가능한 개방적인 네트워크 구조, 시시각각 변화하는 네트워크 토폴로지, 그리고 무선 주파수와 배터리 소모량 등에 대한 엄격한 자원의 제약 등의 특징을 갖고 있다.[1] 초기에 MANET이 개발되었을 때는 경로 상의 모든 노드가 성실하게 협조적으로 패킷을 포워딩한다는 가정 하에 이루어졌지만 실제적인 상황에서는 보안상에 큰 취약성을 갖게 된다. 특히 이동이 자유로우며 유선망을 필요로 하지 않고 쉽게 구축할 수 있다는 장점은 동시에 MANET의 취약점이 된다. 네트워크의 토폴로지와 프로토콜만 알고 있으면 누구나 네트워크에 연결할 수 있기 때문에 유선망에 비해 외부의 공격에 쉽게 노출되어 있다. 또한 네트워크의 각 노드의 구성요소가 외부에 노출되어 있는 경우 직접적으로 물리적인 공격을 받 을 수도 있다. 마지막으로 각 노드의 사용 가능한 전력과 연산 능력은 유선망에 비해 떨어지기 때문에 복잡한 IDS를 갖출 수가 없다. 이러한 문제점 때문에 MANET은 유선망에 비해 공격에 취약할 수밖에 없다.

MANET의 보안에 있어서 가장 활발히 연구되고 있는 분야는 secure routing이다. 아직까지 라우팅 방법이 확정되지 않은 상황에서 이에 관련된 연구가 집중적으로 이루어지고 있음은 당연한 현상으로 볼 수 있다. 많은 라우팅 연구가 안전한 환경을 가정하고 이루어지고 있으나 MANET이 가지는 기본 특성, 즉, 링크의 불안정성, 각 노드의 물리적 보호의 한계, 노드간 연결의 산재성, 토폴로지의 동적인 변화 등으로 의해 실제적인 라우팅 보안에 대한 위험성은 더욱 높은 상황이다. 특히 MANET에서 라우팅이 기존의 전통적 네트워크에서의 라우팅보다 훨씬 취약점을 가지는 이유는 MANET 네트워크에서는 각 노드들이 서비스를 받을 뿐 아니라 라우터로서의 역할을 동시에 수행해야한다는 점에 있다. MANET내의 노드를 하나만 오염시켜도 이 노드를 통해 잘못된 라우팅 정보를 퍼뜨림으로써 전체 네트워크를 마비시킬 수 있다는 것이다. 이처럼 적극적인 형태의 라우팅 관련 침입 형태가 있는가 하면 이보다는 심각성이 조금 낮은 공격 형태로서 이기적 노드가 있다.

이와 같은 이유로 다수의 노드로 구성된 MANET은 잘못된 라우팅 정보를 전달하거나 데이터를 중간에 소실 및 변경시키는 라우팅 메시지 변조 공격에 대해 매우 취약하다. 특히 라우팅 변조 공격 중 웜홀 공격의 경우 은 네트워크에서 사용하는 프로토콜에 대한 정보가 없어도 이루어질 수 있으며 직접적으로 네트워크에 피해를 입히지 않지만 라우팅 메커니즘을 흩트려 놓고 노드간의 거리 정보를 틀리게 만들기 때문에 네트워크의 오버헤드를 가중시키고 전체 네트워크의 배터리 소모를 가

"본 연구는 지식경제부 및 정보통신연구진흥원의 대학IT연구센터 지원사업의 연구결과로 수행되었음" (IITA-2008-C1090-0801-0016)

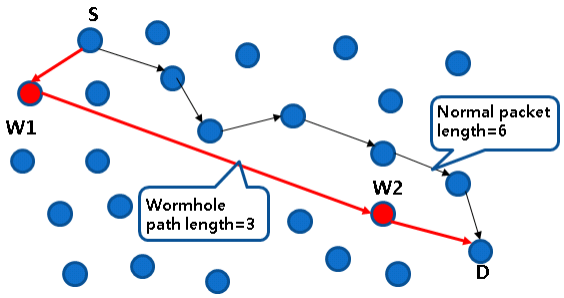
속화 시켜 전체 네트워크의 수명을 단축시키고 또한 다른 이차적인 공격을 실행시키기에 용이하므로 웜홀 공격에 대한 대응방법은 신중하게 고려되어져야 한다.

따라서 본 논문에서는 악의적인 노드들이 네트워크에 침입하여 tunneling을 통해 전송데이터를 dropping, eavesdropping, modification 하는 wormhole 공격을 탐지하고 방지하는 알고리즘을 제안하고자 한다.

II. 연구 배경 및 문제 정의

Wormhole 공격은 실제로는 원거리에 있는 두 개의 악의적인 노드가 마치 서로 이웃하고 있는 것처럼 주변 노드들을 속이고 터널을 형성하여(tunneling) 정상적인 라우팅 경로보다 더욱 짧은 홉수를 거쳐 패킷이 전달 되는 것처럼 거짓 정보를 Source 노드에게 흘려서 매력적인 경로로 보이게 만든다. 이를 통해 Source 노드가 패킷을 자신들의 잘못된 라우팅 경로를 통해 보내도록 속여 네트워크상의 대부분의 데이터 전송이 자신들이 형성한 터널을 통해 이루어지도록 하여 일차적으로는 네트워크의 정보를 몰래 도청하고, 이차적으로는 전송 데이터의 drop, modification를 감행한다.

이런 Wormhole 공격을 통한 false routing은 아래의 [그림1]을 통해 확인할 수 있다. 두 개의 악의적인 노드인 W1과 W2는 터널을 형성하여 Source 노드(S)에서 Destination 노드(D)까지 데이터를 전송할 때 마치 경로의 길이가 3인 것처럼 속여서 실제 최단 전송 경로의 길이인 6보다 훨씬 적은 노드를 거쳐 데이터를 전송하는 것처럼 보여 자신들의 터널을 이용하여 패킷을 전송하도록 유도하게 된다. 실제로 초기의 Wormhole 공격의 경우 더욱 강한 transmit power를 통해 다른 정상적인 노드들보다 더 넓은 전송 거리를 가진 악의적인 노드들을 통해 네트워크에 침입하였지만, 이런 wormhole 공격의 경우 쉽게 탐지가 가능하기 때문에 최근의 연구 추세는 packet encapsulation을 통한 공격에 대한 탐지 및 대응 기법이다.



[그림1] Wormhole로 인한 false routing

Wormhole 공격은 크게 hidden attack과 exposed attack 으로 분류된다. hidden attack은 라우팅 과정 중에 패킷의 헤더나 내요을 전혀 변경하지 않고 통신에 관여하는 공격으로 실제 라우팅 경로 상에는 존재하지만, 자신들의 라우팅 정보를 감추어 통신에 관여하는 공격 방식이다. 아래의 라우팅 경로(1)는 hidden attack의 한 예를 보여준다. 실제로 노드 A와 노드 B는 이웃하는 노드가 아니고 (fake neighbor) 두 노드 사이에 악의적인 노드 W1과 W2가 형성한 tunnel을 통해 연결되어 있지만 Source 노드와 Destination 노드는 아래와 같은 허위의 라우팅 정보를 가지게 되어 Wormhole 공격의 대상이 되게 된다.

$$S \rightarrow A \rightarrow B \rightarrow D \qquad (1)$$

Exposed attack의 경우 이와는 반대로 아래의 라우팅 경로 (2)처럼 악의적인 두 노드가 자신들의 정보를 라우팅 setup과정 중에 포함시키는 공격이다.

$$S \rightarrow A \rightarrow W1 \rightarrow W2 \rightarrow B \rightarrow D \qquad (2)$$

실제로 hidden attack의 공격의 경우 A와 B가 이웃하는 노드가 아님에도 불구하고 이웃하는 노드처럼 라우팅 경로가 형성되기 때문에 다른 주변 노드들의 센싱에 의해 쉽게 파악이 가능하지만 라우팅 경로상에 직접적으로 악의적인 노드들이 개입한 경우에는 W1과 W2가 packet encapsulation을 통해 tunnel을 형성하여 주변의 이웃노드들은 두 노드가 이웃하지 않은 노드라는 것을 파악하기가 힘들기 때문에 탐지하기가 더욱 어렵다.

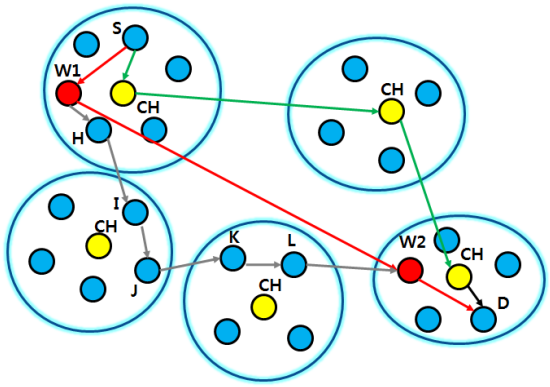
III. Cluster-based routing을 통한 wormhole attack detection

Wormhole 공격을 탐지하기 위해 많은 연구들이 진행되어 왔다. 기존에 제안되었던 packet leash [2], SEC-TOR [3], RTT mechanism [4], 과 같은 wormhole 공격 탐지 기법들은, 대부분 특수 장비가 요구되거나 정확한 노드들의 위치 정보와 엄격한 시간의 동기화를 요구하였다. 그래서 이런 단점을 보완한 DelPHI (Delay per Hop Indicator) [5], WAP(Wormhole Attack Prevention) [6] 등의 새로운 방법들이 제안되었다. 하지만 DelPHI 의 경우 Wormhole의 정확한 위치를 파악할 수 없다는 단점을 갖고 있고, WAP는 에너지 측면에서 매우 소모적이며, Threshold 값에 공격 탐지 율이 높은 상관관계를 갖고 있어서 Threshold 값에 따른 False positive rate가 불안정 하다는 약점을 갖고 있다.

본 논문에서는 이런 위의 기법들을 보안할 수 있는 cluster-based 통신 방법과의 비교를 통한 새로운 wormhole 탐지 기법을 제안하고자 한다.

MANET에서의 일반적으로 사용되는 Routing protocol 중 하나인 DSR(Dynamic source routing) 방법의 경우, 노드들의 신뢰성 측면을 고려하지 않았기 때문에 악의적인 노드들에 의한 Wormhole 공격에 대해 취약점을 갖고 있다. 특히 DSR의 Route discovery process에서 중간 노드(intermediate node)가 쉽게 라우팅 경로를 조작할 수 있는 보안 취약성을 갖고 있다. 이런 이유로 본 논문에서는 DSR 통신 방법의 보안 취약성을 보완하기 위해 네트워크상의 노드들을 여러 개의 Cluster들로 분류하여 Cluster head를 통한 패킷 포워딩 방식과 DSR을 통한 패킷 포워딩 방식의 비교를 통해 false route에 대한 탐지 및 악의적인 노드의 검출해 내는 방법을 제안하고자 한다.

MANET 상의 노드들을 hierarchical routing을 위해 몇 개의 그룹으로 clustering하는 algorithm들은 이미 연구가 되어 있다. [7][8] 위와 같은 clustering 알고리즘을 통해 MANET 네트워크상의 노드들을 몇 개의 cluster로 분류한 뒤 Cluster head를 선출하고 이 Cluster head를 이용한 통신 방법과 DSR routing을 통한 통신 방법의 비교는 아래의 [그림2]을 통해 묘사된다.



[그림2] Cluster based routing과 Wormhole routing의 비교

기존의 DSR 라우팅을 통해 Selection 된 False route와 Delay per hop count를 비교함으로써 Wormhole의 false route를 탐지 해내는 방법은 아래의 [그림2]에서 볼 수 있듯이 악의적인 두 노드 W1, W2간의 통신은 packet encapsulation을 통해 이루어진다고 가정하면 실제적인 라우팅 경로는 **S → W1 {→ H → I → J → K →L→ }W2 → D** 와 같이 이루어지게 된다. 따라서 Cluster head(CH) node들을 통한 통신 경로와 Delay per hop count를 비교하면 실제적으로 더 큰 value값을 갖게 되고 이는 DSR 라우팅 경로가 잘못된 경로임을 알 수 있는 기준이 된다. Delay per hop count는 [6]에서 제안된 다음과 같은 공식 (3)을 이용하여 계산된다.

$$\text{Delay per hop} = \frac{T_b - T_a}{Hop\,count} \quad (3)$$

위의 식에서 T_b는 source 노드에서 RREP 메시지를 받은 시간이고, T_a는 RREQ 메시지를 브로드 캐스팅한 시간을 의미한다.

위와 같이 Cluster based routing과 DSR routing path의 Delay per hop을 비교하여 DSR routing path가 더 높은 Delay per hop 값을 갖는 경우 잘못되었거나, routing attack을 당한 false route로 판단하고 Wormhole을 detection하기 위해서 본 논문에서는 ADCLU(Algorithm for Detection in a Cluster) 알고리즘[1]을 응용하였다. ADCLU 알고리즘은 MANET에서 Collaborative한 방식으로 Cluster상의 악의적인 노드를 검출하는 voting 방식의 알고리즘으로 N. Marchang과 R. Datta가 제안한 방식이다.[1] 본 논문에서는 위의 알고리즘과 같이 voting 방식의 cooperative한 탐지 방법을 응용한 클러스터 내에 악의적인 노드의 탐지 과정을 제안하였다. 그 탐지 과정은 다음과 같다.

Step 1) 잘못된 라우팅 경로 상의 노드가 자신의 클러스터 상에 있는 경우 CH 노드는 자신의 이웃노드들에게 MND(Malicious neighbor detection) 메시지를 cluster안의 노드들에게 전송한다.

Step 2) MND 메시지를 받은 이웃노드들은 자신의 beacon message를 브로드 캐스팅 한 후 자신의 메시지에 응답을 한 노드들을다음의 [표1]과 같이 Neigbor node와 응답시간에 대한 Neighbor node list 테이블을 작성한다.

Negibor node	Correspond time
A	2ms
B	1ms
C	3ms
D	4ms

[표1] Neighbor node list

Step 3) 자신이 작성한 Neighbor node list를 다시 CH 노드에게 전송하면 이 정보를 바탕으로 CH 노드는 다음과 같이 악의적인 노드의 소재를 탐지를 수행하게 된다.

1. 자신의 그룹안의 노드들이 작성한 테이블을 취합하여 가장 적게 포함되어 있는 노드와

가장 응답시간이 느린 노드를 파악한 뒤 다른 CH 노드에게 이 노드가 포함되어 있는지 확인하는 message를 전송한다.
2. 만일 다른 그룹 안에 이 노드의 존재한다는 메시지를 받으면 이 노드를 Neighbor node list에 포함한 노드를 파악한다.
3. CH노드는 주변의 노드들에게 2에서 파악한 노드가 악의적인 노드임을 자신의 그룹안의 노드들에게 브로드 캐스팅한다.
4. 그룹안의 노드들은 이 노드를 Malicious node list에 포함시키고 다음 라우팅 설정 시에 이 노드를 제외시킨다.

V. 결 론 및 향후 연구 방향

본 논문에서는 Cluster-based 통신방식과 비교를 통한 False route의 탐지 및 False route 내에 있는 악의적인 노드들을 이웃 노드들의 neighbor node list들을 통해 탐지 할 수 있는 탐지 기법을 제안하였다. 본 논문에서 제안한 방식을 통해 엄격한 시간 동기화 및 위치 정보가 없이도 Wormhole 공격의 tunneling 방지 및 wormhole 공격을 유발한 악의적인 노드들을 탐지 할 수 있는 방법이다. 하지만 Cluster-based 통신과 Wormhole 탐지 과정에서 Cluster head 노드의 배터리 소모가 타 노드들에 비해 상대적으로 많은 단점이 있기 때문에, Cluster head의 결정 및 에너지 소모량에 따른 새로운 Cluster head의 선출과정에 대한 추가적인 연구를 진행할 계획이다.

< 참 고 문 헌 >

[1] N. Marchang and R. Datta, "Collaborative techniques for intrusion detection in mobile ad-hoc networks", Ad Hoc Networks vol. 6, pp-508-523, 2008.
[2]Y.-C. Hu, A. Perrig, and D. B. Johnson," Packet leashes:A defense against wormhole attacks in wireless networks", IEEE INFOCOM, Mar 2003.
[3] S. Capkun, L. Butty´an, and J.-P. Hubaux, "SECTOR: secure tracking of node encounters in multi-hop wireless networks", In ACM Workshop on Security of Ad Hoc and Sensor Networks(SASN), pp. 21-32, Oct 2003.
[4] J. Zhen and S. Srinivas, "Preventing replay attacks for secure routing in ad hoc networks" In ADHOC-NOW, LNCS 2865, pp 140-150, 2003.
[5]D. A. Maltz, D. B. Johnson and Y. Hu, "The dynamic source routing protocol (DSR) for mobile ad hoc networks for IPv4", RFC 4728, The Internet Engineering Task Force, Network Working Group, Feb 2007.
[6] S. Choi, D. Kim, D. Lee and J. Jung, " WAP:Wormhole Attack Prevention Algorithm in Mobile Ad Hoc Networks", IEEE international Conference on Sensor Networks, Ubiquitous, and Trustworthy computing, PP.343-348, 2008.
[7]M. Chatterjee, S.K. Das and D. Turgut, " WCA: a weighted clustering algorithm for mobile ad hoc networks", Journal of Cluster Computing (Special Issue on Mobile Ad hoc Networks) vol.5, pp. 193-204, 2002
[8]P. Krishna, N.H. Vaidya, M. Chatterjee and D.K. Pradhan, "A cluster-based approach for routing in dynamic networks", ACM SIGCOMM Computer Communication Review, pp.49-65, 1997.