Journal of The Korea Society of Computer and Information
Vol. 17, No. 11, November 2012
www.ksci.re.kr
http://dx.doi.org/10.9708/jksci/2012.17.11.073

# 애드 혹 네트워크에서 위치 정보와 홉 카운트 기반 ETWAD(Encapsulation and Tunneling Wormhole Attack Detection) 설계

이 병 관 *, 정 은 희 **

# A Design of ETWAD(Encapsulation and Tunneling Wormhole Attack Detection) based on Positional Information and Hop Counts on Ad-Hoc

Byung-Kwan Lee *, Eun-Hee Jeong **

## 요 약

본 논문에서는 애드 혹 네트워크의 노드 위치 정보와 홉 수를 이용하여 캡슐화 웜홀 공격과 터널링 웜홀 공격을 탐지하는 ETWAD(Encapsulation and Tunneling Wormhole Attack Detection) 기법을 설계하였다. ETWAD 탐지 기법은 애드 혹 네트워크 내의 노드 ID와 그룹 키로 노드의 신분을 확인할 수 있는 GAK(Group Authentication Key)를 생성하여 RREQ와 RREP에 추가하여 애드 혹 네트워크의 구성원임으로 인증할 수 있도록 설계하였다. 또한, ETWAD 탐지 기법은 RREP 메시지 내의 홉 수를 카운트 하고, 근원지 노드 S와 목적지 노드 D의 거리를 계산하여 임계치와 홉 수를 이용하여 캡슐화 웜홀 공격, 터널링 공격을 탐지하는 GeoWAD 알고리즘을 설계하였다. 그 결과, 평균 웜홀 공격 탐지율이 91%, 평균 FPR이 4.4%로 평가되므로 ETWAD 탐지 기법은 웜홀 공격 탐지율과 웜홀 공격 탐지의 신뢰성을 향상시켰다고 볼 수 있다.

▸ Keywords : 웜홀공격탐지, 위치정보, 홉 카운트, 그룹 인증키, 애드혹 네트워크

## Abstract

This paper proposes an ETWAD(Encapsulation and Tunneling Wormhole Attack Detection) design based on positional information and hop count on Ad-Hoc Network. The ETWAD technique is designed for generating GAK(Group Authentication Key) to ascertain the node ID and group key within Ad-hoc Network and authenticating a member of Ad-hoc Network by appending it to RREQ and RREP. In addition, A GeoWAD algorithm detecting Encapsulation and Tunneling Wormhole Attack by using a hop count about the number of

•제1저자 : 이병관 •교신저자 : 정은희
•투 고 일 : 2012. 10. 23, 심사일 : 2012. 11. 06, 게재확정일 : 2012. 11. 14.
* 관동대학교 컴퓨터학과(Dept. of Computer, Kwandong University)
** 강원대학교 지역경제학과(Dept. of Regional Economics, Kangwon National University)

Hops within RREP message and a critical value about the distance between a source node S and a destination node D is also presented in ETWAD technique. Therefore, as this paper is estimated as the average probability of Wormhole Attack detection 91% and average FPR 4.4%, it improves the reliability and probability of Wormhole Attack Detection.

▸ Keywords : Wormhole Attack Detection, Positional Information, Hop Count, Group Authentication Key, Ad-hoc Network

## I. 서 론

애드 혹 네트워크는 다양한 분야에서 활용되고 있으며, 특히 재난 예방을 위해 광범위한 영역에 대한 위험요소 감시 및 제어와 같은 긴급 상황을 알리는 역할로 사용이 증가함에 따라 성능향상을 위한 연구와 더불어 보안에 대한 중요성이 커지고 있다.

애드 혹 네트워크 라우팅 공격에는 악의적인 두 노드가 공모하여 라우팅 경로를 조작하여 데이터들이 악의적인 노드들을 지나가도록 하는 웜홀 공격이 있으며, 이 웜홀 공격을 방어하는 방법에는 Packet Leashes[1, 2], TESLA[3], 그리고 RSA를 이용하는 디지털 인증기법[4] 등이 있다. Packet Leashes는 Geographic Leashes와 Temporal Leashes가 있는데, Geographic Leashes는 모든 노드가 자신의 GPS 좌표를 알고 있어야 하고, 모든 노드들은 약하게 동기화된 시간 정보를 공유해야 한다. Temporal Leashes는 Geographical Leashes보다 강하게 동기화된 시계를 가지고 있기 때문에 애드 혹 네트워크의 자원을 보다 많이 사용한다는 단점이 있다. TESLA는 안전한 브로드캐스팅 기능을 제공하는 프로토콜이지만 Packet Leashes처럼 각 센서 노드들 사이에서 시간 동기화가 이루어져야 하고, 패킷 인증에 필요한 인증키의 지연으로 인하여 명령 전달 시간이 전체적으로 길어질 수 있다는 문제점을 갖는다. 또한, TESLA는 이러한 문제를 해결하기 위해서 짧은 시간 간격을 적용할 수 있지만 이는 시간 동기화를 더 어렵게 하고 키 체인이 더 빨리 고갈된다는 문제를 야기 시킨다. RSA 디지털 인증기법은 보통 전송 시간 슬롯 타임보다 3배정도 더 많은 시간이 걸린다는 단점이 있다.

본 논문에서는 위치정보와 홉 카운트를 이용하여 웜홀 노드 및 웜홀 공격을 탐지하는 ETWAD(Encapsulation and Tunneling Wormhole Attack Detection) 기법을 설계한다. ETWAD 기법은 애드 혹 네트워크 내의 모든 노드들의 아이디(ID)와 애드 혹 네트워크 그룹의 그룹 아이디로 안전한 그룹 인증키를 생성하고, 이 그룹 인증키로 센서 노드가 네트워크의 구성원인지를 확인함으로써 웜홀 노드를 탐지하도록 설계한다. 이 그룹 인증키는 TESLA의 인증키 지연으로 인한 인증처리 시간의 문제점을 보완할 수 있을 것이다. 또한, 센서 노드의 위치 정보로 송신 노드와 수신 노드 사이의 거리와 홉 수의 비율로 캡슐화 웜홀 공격을 탐지하고자 한다.

## II. 관련 연구

### 1. 웜홀 공격

#### 1.1 캡슐화 웜홀

캡슐화 웜홀 공격은 웜홀 노드가 패킷에 캡슐을 씌워 홉 수를 증가하지 않도록 하는 공격으로 그림 1과 같다.

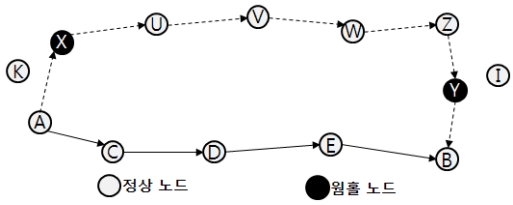



그림 1. 캡슐화 웜홀 공격
Fig. 1. Encapsulation Wormhole Attack

A는 송신 노드, B는 수신 노드이고, A와 B의 1 홉 범위 내의 노드 X와 Y가 웜홀 노드라고 하자. A가 B에게 패킷을 전송할 때, 1 홉 거리에 있는 X와 C에게 패킷을 전송하면, X가 패킷에 캡슐을 씌워서 U-V-W-Z 경로를 거쳐서 Y에게 전달하므로 홉 수는 증가하지 않게 된다. Y는 패킷의 캡슐을 풀어서 B에게 전달하므로, 결국 A는 A-X-Y-B라는 경로를 얻게 된다. 또한 A는 A-C-D-E-B라는 정상적인 경로를 얻게 되지만, A는 라우팅 정책에 따라 홉 수가 적은 A-X-Y-B 경로를 선택하므로 비정상적인 패킷 전달이 발생할 수 있다[5,6,7].

### 1.2 터널링 웜홀

터널링 웜홀 공격은 일반적으로 웜홀 노드들 사이에서 외부의 채널을 가지고 실행되는 공격으로 그림 2와 같다. A는 송신 노드, B는 수신 노드, X와 Y는 웜홀 노드이라고 할 때, A가 패킷을 전송하면, X가 외부 터널을 통해 Y에게 패킷을 전달한다. 그리고 Y는 패킷을 B에게 전달하므로 A는 A-X-Y-B인 경로를 획득한다. 또한 A는 정상적인 A-C-D-E- F-B인 경로를 획득하지만, 라우팅 정책으로 홉 수가 작은 A-X-Y-B인 경로를 선택한다. 하지만 이 경로에는 웜홀 노드인 X와 Y가 있으므로 패킷의 정상적인 송수신은 불가능하다[5,6,7].

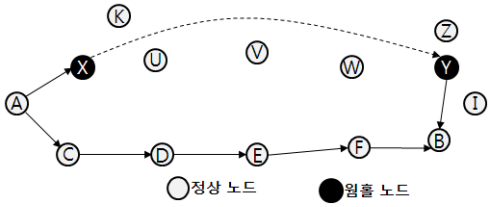



그림 2. 터널링 웜홀 공격
Fig. 2 Tunneling Wormhole Attack

본 논문에서는 이러한 캡슐화 웜홀 공격, 터널링 웜홀 공격을 탐지할 수 있는 ETWAD 기법을 설계하고자 한다.

## 2. 웜홀 공격 탐지 기법

### 2.1 Packet Leashes

Packet Leashes에는 Geographical Leashes와 Temporal Leashes가 있다[1,2,8].

Geographic Leashes는 각 노드가 GPS로 자신의 좌표를 알고 있어야 하고, 모든 노드들은 약한 동기화되어 패킷을 전송하기 전에 자신의 좌표와 패킷 전송시간을 패킷에 추가한 후 전송한다. 패킷을 수신한 노드는 전송 노드와의 거리와 시간을 계산하여 최대 전송거리보다 크다면 실제 이웃이 아닌 웜홀로 인한 이웃이라고 간주한다.

Temporal Leashes는 Geographical Leashes와 달리 GPS에 의존하지 않고, 모든 노드들이 강한 클럭 동기화가 이루어져 있다고 가정하고 있다. 모든 노드들은 패킷을 전송하기 전에 패킷의 라이프 타임을 설정하여 전송한다. 패킷을 받은 수신 노드는 라이프 타임이 지나서 도착했다고 판단되면 웜홀로 의심하여 패킷을 버린다. 이 기법은 모든 노드들 간에 강한 클럭 동기화가 이루어져야 하고, 웜홀 노드 간에 전파 속도가 매우 빠르면 웜홀 탐지가 어려워진다.

### 2.2 TESLA

패킷인증기법으로 웜홀 공격을 탐지하는 대표적인 방법이 TESLA이다. TESLA는 패킷의 인증을 위해 대칭형 인증키를 사용하는데, 인증키를 체인화하는 기법과 체인화하지 않는 기법으로 크게 분류된다.

체인화 기법을 사용하지 않는 일반적인 방법은 현재 패킷의 인증을 바로 다음에 오는 패킷에 담긴 인증키를 사용하여 패킷 인증을 처리하는데, 바로 다음에 도착해야 할 패킷의 손실이 발생하면, 현재 패킷의 인증이 불가능하다는 단점을 가진다.

체인화 기법을 사용하는 인증기법은 키를 하나 잃어버려도 다음에 도착하는 키를 사용하여 키 생성이 가능하므로, 송신 노드가 패킷의 송신을 지연시킬 필요가 없다.

본 논문에서는 노드의 위치정보를 이용하여 노드간의 거리를 계산하고, 홉 수를 카운팅 하여 캡슐화 웜홀 공격과 터널링 웜홀 공격을 탐지하고자 한다. 또한, 노드마다 애드 혹 네트워크 그룹 인증키를 생성하도록 설계하여 웜홀 노드를 탐지하고자 한다.

## III. ETWAD 설계

멀티 홉 라우팅을 사용하는 네트워크에서 웜홀 공격으로 두 노드의 거리가 1 홉으로 짧아져서 경로 설정을 방해하거나, 악의적인 노드가 포함된 경로가 설정될 가능성이 증가한다. 따라서 웜홀 노드가 포함된 경로를 이용하는 모든 통신들은 공격자에 의해 감청될 수 있고, 메시지가 차단되거나 수정될 수 있는 위협이 발생한다.

본 논문에서는 노드 ID와 그룹 ID를 이용하여 애드 혹 네트워크 내의 모든 노드들이 안전한 그룹 인증키인 GAK (Group Authentication Key)를 생성하고, 이 그룹 인증키로 노드가 애드 혹 네트워크 내의 정상 노드인지를 확인함으로써 웜홀 노드를 탐지하도록 설계한다. 또한, 노드의 위치 정보로 송신노드와 수신노드 사이의 거리를 계산하여 캡슐화 웜홀 공격과 터널링 웜홀 공격을 탐지하고자 한다.

ETWAD 기법의 가정은 다음과 같다.

첫째, 애드 혹 네트워크의 모든 노드는 고유 ID를 보유한다.

둘째, 애드 혹 네트워크에 노드들 등록할 때, 그룹 ID를 부여받으며, 등록된 노드들의 목록 SNL(Sensor Node List)은 애드 혹 네트워크의 그룹 매니저인 싱크 노드가 관리한다.

셋째, 모든 노드들은 동일한 해시 함수와 ECC 암호화 알고리즘을 가지고 있다.

그림 3은 ETWAD 기법의 웜홀 탐지 과정을 설명한 것이

다. ETWAD 기법은 그룹 인증키를 생성하는 GAK 과정, 노드의 위치정보를 추가한 RREQ 메시지 설계, 중간노드의 노드 신분 확인 및 RREQ 메시지의 노드 리스트 추가과정, RREP 메시지 생성, 웜홀 공격 탐지 단계로 수행된다.

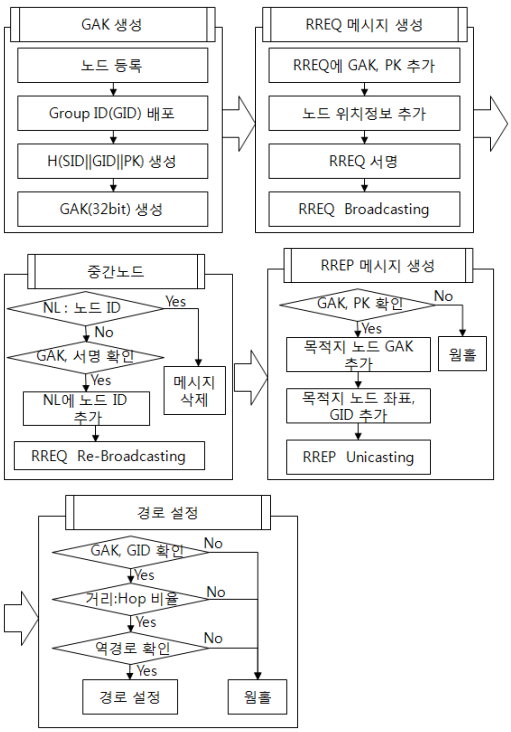



그림 3. ETWAD의 웜홀 탐지 흐름
Fig. 3 The Wormhole detection procedure of ETWAD

## 1. GAK(Group Authentication Key) 설계

ETWAD 기법은 애드 혹 네트워크 내의 모든 노드들에게 안전한 그룹키인 GAK(Group Authentication Key)를 생성하도록 설계한다. 본 논문에서 설계한 GAK는 노드 ID, 그룹 ID, 공개키로 구성되며 그 구조는 그림 4와 같다.

본 논문에서 설계한 GAK는 그룹 ID로 애드 혹 네트워크 그룹의 구성원인지를 확인하여 터널링 공격을 탐지하도록 설계 한다. 또한 인증기관으로부터 그룹 ID를 분배 받는 것이 아니라 애드 혹 네트워크의 싱크 노드에 노드의 고유 ID를 등록할 때, 그룹 ID를 배포하도록 한다.

GAK 생성 과정은 다음과 같다.

〔1 단계〕 새로운 노드가 싱크 노드에 노드 ID를 SNL(Sensor Node List)테이블에 등록한다. 그리고 싱크 노드는 그룹 ID를 새로운 노드에게 할당한다.

〔2 단계〕 노드는 ECC 알고리즘을 이용하여 자신의 비밀키에 대한 공개키를 생성한다.

〔3 단계〕 노드는 노드 ID(SID), 그룹 ID(GID), 노드의 공개키(PK)를 연접한 후 해시함수로 해시한다.

〔4 단계〕 해시된 값을 32bit 크기로 분리한 후, 폴딩(Folding)하여 32 bit인 GAK를 생성한다.

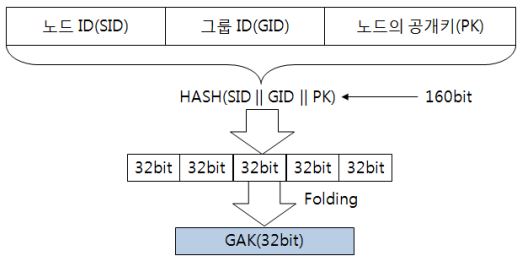



그림 4. GAK 구조
Fig. 4 The structure of GAK

## 2. 웜홀 검출 절차

본 논문에서 설계하는 ETWAD 기법은 요청 경로 메시지 RREQ(Route Request), 경로 응답 메시지 RREP(Route Reply)를 주고받을 때 각 노드의 GAK, 서명, 노드 간의 거리, 그리고 홉 수를 이용하여 터널링 웜홀 공격, 캡슐화 웜홀 공격을 검출함으로써 좀 더 안전한 경로를 선정한다.

### 2.1 근원지 노드 RREQ 메시지 생성

근원지 노드 S는 목적지 노드 D까지 경로를 탐색하고자 할 때, 경로 탐색을 초기화한 후 다음과 같은 단계로 RREQ 메시지를 생성한 후 브로드 캐스팅한다.

〔1 단계〕 근원지 노드 S와 목적지 노드 D의 식별자(ID)인 S와 D, 요청 순차 번호(#), 중간 노드들의 ID를 기록할 node list를 포함하는 RREQ 메시지를 생성한다[9,10].

```
(Rq, S, D, #, (node list))
```

〔2 단계〕 근원지 노드 S는 근원지와 목적지 식별자, 순차번호, 중간노드들의 node list, 위치정보를 해시된 그룹 ID로 서명을 한다. 그리고 근원지 노드 S의 그룹 인증키인 GAKs와 공개키 PKs는 메시지에 추가한다.

```
(Rq,S,D,#,(node list))
{S,D,#,(node list),Sp}H(GID)(GAKS,PKS)
```

〔3 단계〕 RREQ 메시지를 브로드 캐스트 한다.

## 2.2 중간 노드

중간노드를 지날 때 마다 그림 5의 단계별 과정을 거치게 된다. 이 과정을 설명하면 다음과 같다.

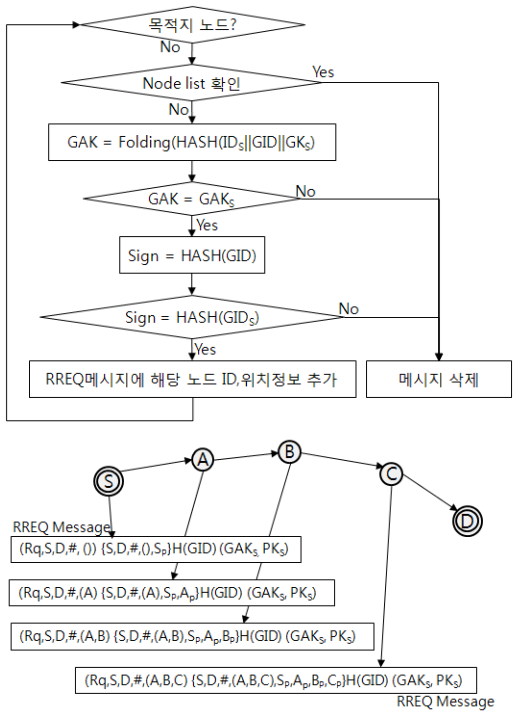



그림 5. RREQ 메시지 전송 흐름도
Fig. 5 The transmission flowchart of RREQ message

〔1 단계〕 RREQ 메시지의 node list에 자신의 ID가 등록되어 있는지를 확인한다.

〔2 단계〕 node list에 자신의 ID가 등록되어 있으면, RREQ 메시지를 삭제한다.

〔3 단계〕 node list에 자신의 ID가 등록이 되어 있지 않으면 RREQ 메시지의 근원지 노드 ID, PKs과 중간 노드의 그룹ID인 GID를 각각 해시한 후 32bit로 Folding한 중간노드의 GAK와 RREQ 메시지의 GAKs와 비교함으로써 웜홀 노드인지를 검사한다.

〔4 단계〕 이 값이 일치하면, 중간 노드는 애드 혹 네트워크 그룹 소속인 정상 노드로 간주하고 node list에 ID를 추가한다. 그리고 중간 노드의 위치정보를 추가하고, GID 해시값으로 서명을 한 후, RREQ 메시지를 다시 브로드캐스트 한다.

〔5 단계〕 이 값이 일치하지 않으면, 중간노드의 그룹 ID인 GID 해시값이 다르므로 서명을 풀 수 없다. 따라서 중간 노드의 위치정보를 추가할 수 없다. 그런데, 웜홀 노드가 임의로 틀린 그룹 ID로 서명을 생성하여, RREQ 메시지를 생성하여 다시 브로드캐스트 하더라도 그 다음번 정상 노드에서 서명이 틀린 것을 확인하므로 RREQ 메시지가 삭제된다.

## 2.3 목적지 노드의 웜홀 공격 탐지 및 RREP 메시지 생성

RREQ 메시지가 목적지 노드 D에 도착하면, 목적지 노드 D는 첫째, RREQ 메시지의 웜홀공격을 검사하고, 둘째, RREQ 메시지를 인증한 후, RREP 메시지를 생성하여 근원지 노드 S에게 유니 캐스트 하는데 그 절차는 다음과 같다.

〔1 단계〕 목적지 노드 D는 RREQ 메시지의 공개키, 근원지 노드 S의 ID, 목적지 노드 D의 그룹 ID를 연접하고 해시한 후, 32bit로 폴딩한 목적지 노드의 GAK와 RREQ 메시지의 GAKs와 비교하여 웜홀 노드인지를 검사한다.

〔2 단계〕 GAK와 GAKs가 일치하면, 목적지 노드 D는 그룹 ID를 해시하여 H(GID) 서명으로 메시지를 풀어서, RREQ 메시지의 S, D, #, (node list)와 비교하여 메시지의 유효성을 검사한다. 만약 노드 리스트가 일치하지 않으면, 근원지 노드 D는 경로가 변조 된 것으로 간주하여 RREQ 메시지를 버린다.

〔3 단계〕 목적지 노드 D는 RREQ의 순차번호가 근원지 노드 S가 보낸 마지막 순차 번호 보다 큰지를 점검한다. 순차번호가 크다면, 노드의 수(홉 수)를 카운트한다.

〔4 단계〕 목적지 노드 D는 RREQ 메시지가 제공한 근원지 노드 S의 위치정보와 자신의 위치 정보를 이용하여 거리를 계산하고, 거리 값이 (임계치×홉 수)보다 작으면 캡슐화 웜홀 공격으로 간주하고, (거리 값/임계치)가 홉 수 보다 작으면 터널링 웜홀 공격으로 간주하여 RREP 메시지를 버린다. 근원지 노드 S와 목적지 노드 D의 위치 정보는 $S(x,y), D(x',y')$ 이라고 할 때, 두 노드 사이의 거리를 계산은 유클리디안 거리(Euclidean distance) 계산방법을 사용하였으며 식(1)과 같다.

$$distance(S,D) = \sqrt{(x-x')^2+(y-y')^2} \quad \ldots 식(1)$$

〔5단계〕 근원지 노드 S는 경로 내에 웜홀 노드와 웜홀 공격이 존재하지 않으므로, RREP 메시지를 생성한다[9,10].

| (Rp, S, D, #, (node list)) |
|---|

〔6 단계〕 RREQ 메시지에서 누적된 경로인 node list를 추출하고, 그것의 복사본을 RREP 메시지에 포함시킨다.

| (Rp, S, D, #, (A,B,C)) |
|---|

〔7 단계〕 목적지 노드 D와 근원지 노드 S, 순차번호, 누적

된 경로, 각 노드의 위치정보에 해시된 그룹 ID인 H(GID)로 서명한다.

```
(Rp,S,D,#,(A,B,C))
{S,D,#,(A,B,C), SP,AP,BP,CP,DP}H(GID)
```

〔8 단계〕. 그리고 난 후, 패킷에 목적지 노드 D의 $GAK_D$와 공개키 $PK_D$를 추가한다.

```
(Rp,S,D,#,(A,B,C))
{S,D,#,(A,B,C),SP,AP,BP,CP,DP}H(GID)(GAKD,PKD)
```

〔9 단계〕 RREP 메시지를 node list 역순서로 유니 캐스트 한다.

### 2.4 중간 노드 RREP 메시지 확인

중간 노드는 RREP 메시지를 받으면, 자신의 위치 정보가 변경되었는지 확인한다. 만약에 위치 정보가 변경되었으면, RREP 메시지를 삭제하고, 그렇지 않으면 RREP 메시지의 노드 리스트 역순서로 유니 캐스트 한다.

### 2.5 근원지 노드의 웜홀 공격 탐지 및 경로 설정

근원지 노드 S는 목적지 노드 D의 RREP 메시지를 수신 받았을 때, RREP 메시지의 유효성을 인증하고, 캡슐화 웜홀 공격과 터널링 공격을 탐지 한다. 웜홀 공격 탐지 알고리즘은 그림 6과 같으며, 단계별 처리과정은 다음과 같다.

〔1 단계〕 근원지 노드 S는 RREP 메시지에 의해 리턴되는 순차번호가 근원지 노드 S가 전송한 RREQ 메시지의 순차번호가 같은지를 확인한다.

〔2 단계〕 만약에 일치하면, RREP 메시지는 유효한 것으로 간주하고 근원지 노드 S는 RREP 메시지를 인증한다.

〔3 단계〕 RREP 메시지를 인증하기 위해, 근원지 노드 S는 목적지 노드 D의 노드 ID, 근원지 노드 S가 보유하고 있는 그룹 ID, 그리고 목적지 노드 D의 공개키를 연접하여 해시한 GAK를 계산한다. 그리고 RREP 메시지의 $GAK_D$와 비교한다.

〔4 단계〕 비교가 일치하면, 근원지 노드 S는 근원지 노드의 그룹 ID를 해시한 값을 이용하여 서명되어 있는 RREP 메시지를 푼다.

〔5 단계〕 근원지 노드 S는 RREP 메시지의 노드 리스트가 일치하는지 확인하고, 노드의 수(홉 수)를 카운트한다. 만약 노드 리스트가 일치하지 않으면, 근원지 노드 S는 RREP 메시지 내의 경로가 변조 된 것으로 간주하여 RREP 메시지를 버린다.

〔6 단계〕 목적지 노드 D의 웜홀 공격 탐지방법과 같은 방법으로 식(1)을 이용하여, 근원지 노드 S와 목적지 노드 D의 위치정보를 이용하여 거리를 계산하고, 거리 값이 (임계치×홉 수)보다 작으면 캡슐화 웜홀 공격으로 간주하고, (거리 값/임계치)가 홉 수 보다 작으면 터널링 웜홀 공격으로 간주하여 RREP 메시지를 버린다.

〔7단계〕 근원지 노드 S는 경로 내에 웜홀 노드와 웜홀 공격이 존재하지 않으므로, RREP 메시지의 노드 리스트의 순서대로 경로로 선정한다.

```
GeoWAD(m, GID){
 m : RREP message
 GID : Group ID
 if((check(sequence_num)){ //순차번호 확인
  GAK = Folding(HASH(ID||GID||PK), 32);
      // 32bit GAK 생성
  if(GAK == GAKm){ // 그룹인증키 확인
    Sign = HASH(GID);
    if(Sign == Signm){ // 서명 확인
      if(compare(node_list)){//노드 리스트 확인
        hop = count(node_list);
            // node list에서 hop수 계산
        distance_SD=SQRT(power((xS-xD),2)
                -power((yS-yD),2)); // 거리계산
        if(distance_SD < critical_distance*hop){
          //거리가 임계치보다 작으면
          delete(m);
          broadcast("Wormhole attack: encapsulation");
          return;
        }
        if(distance_SD/critical_distance < hop){
          // hop 수가 작으면
          delete(m);
          broadcast("Wormhole attack: Tunneling");
          return;
        }
        confirm(route, node_list); //경로 선정
        return;
      }else
          delete(m);
    }else
      delete(m);
  }else
    delete(m);
 }
 delete(m);
 return;
}
```

그림 6. GeoWAD 알고리즘
Fig. 6 GeoWAD Algorithm

## IV. 시뮬레이션

ETWAD 기법의 시뮬레이션은 NS-2 version 2.35 시뮬레이터〔11〕〔12〕를 이용하였고, DSR 라우팅 프로토콜, 200sec 실험시간, MAC/802_11을 사용하였으며, 그 외 파라미터는 표 1과 같다. 실험에 사용된 노드는 총 100개이며, 웜홀 노드의 수를 2, 4, 6, 8, 10으로 증가시키면서 실험하였으며, 웜홀 노드의

생성은 1-10사이의 노드 번호로 지정하여 생성하지만, 웜홀 노드의 위치는 랜덤하게 위치 시켰다.

표 1. 시뮬레이션 파라미터
Table 1. Simulation parameter

| 파라미터 | 값 |
|---|---|
| Simulator | NS-2 version 2.35 |
| Simulation Time | 200sec |
| Simulation Area | 1000 × 1000m |
| 센서 노드의 총 수 | 100 |
| Wormhole 노드의 수 | 2, 4, 6, 8, 10 |
| 라우팅 프로토콜 | DSR |
| 트래픽 유형 | CBR(UDP), TCP |
| 전송 범위 | 250m |
| Movement model | static |

본 논문에서 제안한 ETWAD 기법은 패킷 전송 비율, 웜홀 공격 탐지율, FPR(False Positive ratio)로 분석하였다. 패킷 전송 비율(Packet Delivery Ratio)은 근원지 노드에서 목적지 노드까지의 전달된 패킷의 비율을 말하며, 비율의 계산식은 식(2)와 같다.

$$PDR = \frac{\text{목적지노드에 수신된 패킷의 수}}{\text{근원지노드에 의해 전송된 패킷의 수}} \times 100$$

...식(2)

웜홀 공격 탐지율(Wormhole Attack Detection Ratio)은 웜홀 공격으로 탐지된 공격의 수를 실제 웜홀 공격수로 나눈 것을 말하면, 계산식은 식(3)과 같다.

$$WADR = \frac{\text{웜홀공격으로 탐지된 공격의 수}}{\text{웜홀 공격의 수}} \times 100$$

...식(3)

FPR(False Positive Ratio)는 정상인데 웜홀 공격으로 탐지된 수를 정상 패킷의 수로 나눈 것을 말하며, FPR 계산식은 식(4)와 같다.

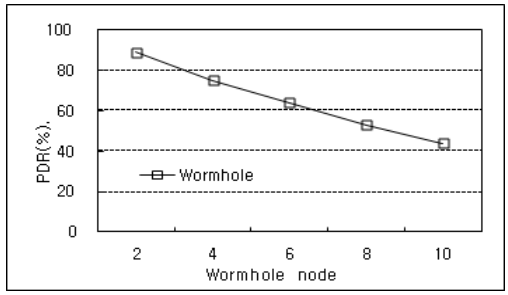
$$FPR = \frac{False\ Positive\text{로 탐지된 수}}{\text{정상 패킷 수}} \times 100$$

...식(4)

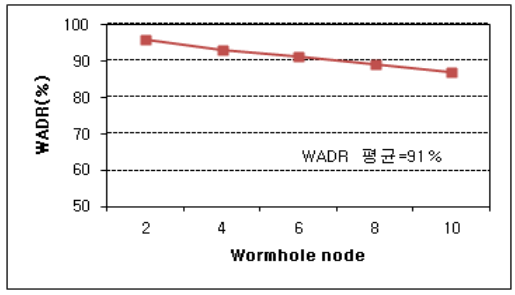
그림 7은 ERWAD 기법의 패킷전송비율, 웜홀 공격 탐지율, FPR의 결과를 설명한 것이다. 패킷 전송 비율은 웜홀 노드 및 웜홀 공격이 증가할수록 삭제되는 패킷의 수가 증가하므로 패킷 전송 비율이 감소하게 된다. 그림 7(a)는 웜홀 공격이 탐지되었을 경우 패킷 전송 비율을 설명한 것으로, 평균적으로 35%정도 감소하는 것으로 나타났다.

ETWAD 기법의 웜홀 공격 탐지율은 그림 7(b)에서 설명하고 있듯이 웜홀 노드 수가 증가할수록 웜홀 공격의 탐지율이 감소하는 것으로 나타나며, 웜홀 공격 평균 탐지율은 91%이다. 그림 7(c)는 ETWAD 기법의 FPR을 설명한 것으로 웜홀 노드가 2일 경우에는 3.75에서 웜홀 노드의 수를 10으로 증가시키면 4.98으로 증가하는 것으로 나타난다.

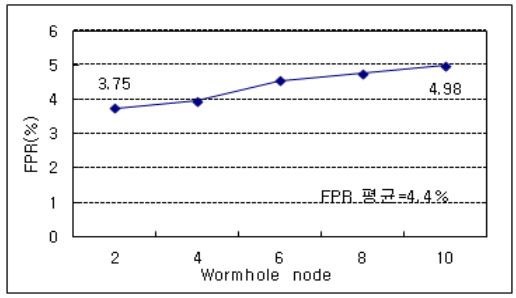
ETWAD 기법은 91%의 평균 WADR과 4.4%의 평균 FPR로 평가되므로 웜홀 공격 탐지율과 웜홀탐지의 신뢰성을 향상시켰다고 볼 수 있다.




(a) 패킷 전송 비율(PDR)




(b) 웜홀공격탐지율




(c) False Positive Ratio

그림 7. ETWAD 실험 결과
Fig. 7 The simulation result of ETWAD

## V. 결론

본 논문에서는 애드 혹 네트워크 노드의 인증키 지연으로 인한 인증처리 시간의 문제점을 보완하고, 웜홀 공격을 탐지하는 ETWAD(Encapsulation and Tunneling Wormhole Attack Detection) 기법을 설계하였다.

첫째, 애드 혹 네트워크 내의 모든 노드들이 인증기관과는 독립적으로 노드 ID와 그룹 ID, 공개키로 GAK(Group Authentication Key)를 생성하도록 설계하였다.

둘째, ETWAD 기법은 중간 노드가 GAK를 이용하여 애드 혹 네트워크의 구성원인지를 확인함으로써 웜홀 노드를 탐지하도록 설계하였다.

셋째, RREQ와 RREP 메시지 내의 홉 수를 카운트 하고, 근원지 노드 S와 목적지 노드 D의 거리를 계산하여 임계치와 홉 수를 이용하여 캡슐화 웜홀 공격, 터널링 공격을 탐지하도록 설계하였다.

그 결과 ETWAD 기법은 평균 웜홀 공격 탐지율이 91%이고, 평균 FPR이 4.4%으로 평가되므로 웜홀 공격 탐지율과 웜홀 공격 탐지의 신뢰성을 향상시켰으며, 좀 더 안전한 경로를 선정한다고 볼 수 있다.

## 참고문헌


〔1〕 Yih-Chun Hu, "Wormhole Attack in Wireless Networks," IEEE Journal, Communication, Vol.24, No.2, pp. 370-380, Feb. 2006

〔2〕 Yih-Chun Hu, Adrian Perrig and David B. Johnson, "Packet Leashes : A Defense against Wormhole Attacks in Wireless Ad Hoc Networks," In Proceedings of IEEE INFOCOM 2003, pp.1976-1986, April 2003

〔3〕 Adrian Perrig, Ran Canetti, J. D. Tygar, and Dawn Song, "Efficient Authentication and Signing of Multicast Streams over Lossy Channels," Security and Privacy 2000 IEEE, pp.56-73, May 2000

〔4〕 R. L. Rivest, "A method for obtaining digital signature and public-key cryptosystems," Communication of the ACM, Vol.21, No.2, pp.120-126, Feb. 1978

〔5〕 Intae Kim, Seungjin Han and Junghyun Lee, "Wormhole Detection using Multipath in Sensor Network," KSCI review, Vol.15, No.1, pp.77-81, 2007

〔6〕 Issa Khalil, Saurabh Bagehi and Nesss B. Shroff, "LITEWORP:A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Networks," In Proceedings of the International Conference on Dependable System and Networks, pp.612-621, 2005

〔7〕 A. VANI and D. Sreenivasa Rao, "A Simple Algorithm for Detection and Removal of Wormhole Attacks for Secure Routing In Ad Hoc Wireless Networks," IJCSE, Vol.3, No.6, pp. 2377-2384, June 2011

〔8〕 Khin Sandar Win, "Analysis of Detecting Wormhole Attack in Wireless Networks," World Academy of Science, Engineering and Technology 48, pp.422-423, 2008

〔9〕 Jun Jie Piao and Tae Mu Chang, "Transmission Power Based Source Routing Protocol for Mobile Ad Hoc Networks with Unidirectional Links," ICHIT 2011, LNCS Vol.6935, pp. 146-153, Sept. 2011

〔10〕 Rakesh Babu Bobba, Laurent Eschenauer, Virgil Gligor and William Arbaugh, "Bootstrapping Security Associations for Routing in Mobile Ad-Hoc Networks." Technical Report TR 2002-44, University of Maryland, May 2002

〔11〕 The Network Simulator NS-2, http://www.isi.edu/ nsnam/ns/

〔12〕 Nam: Network Animator, http://www.is.edu/nsnam/ nam

## 저 자 소 개

이 병 관

1979 : 부산대학교 기계설계학과 공학사
1986 : 중앙대학교 전자계공학과 공학석사
1990 : 중앙대학교 전자계산공학과 공학박사
현 재 : 관동대학교 컴퓨터학과 교수
관심분야 : 네트워크 보안, 인터넷 보안
Email : bklee@kd.ac.kr

정 은 희

1991 : 강릉대학교 통계학과 이학사
1999 : 관동대학교 전자계산공학과 공학석사
2003 : 관동대학교 전자계산공학과 공학박사
현 재 : 강원대학교 지역경제학과 부교수
관심분야 : 네트워크보안, 인터넷보안
Email : jeongeh@kangwon.ac.kr