디지털산업정보학회 논문지 제6권 제4호-2010년 12월

MANET에서 규칙을 기반으로 한 계층형 침입 탐지에 관한 연구*

정 혜 원**

The Study of Hierarchical Intrusion Detection Based on Rules for MANET

Jung, Hye Won

〈Abstract〉

MANET composed mobile nodes without central concentration control like base station communicate through multi-hop route among nodes. Accordingly, it is hard to maintain stability of network because topology of network change at any time owing to movement of mobile nodes. MANET has security problems because of node mobility and needs intrusion detection system that can detect attack of malicious nodes. Therefore, system is protected from malicious attack of intruder in this environment and it has to correspond to attack immediately. In this paper, we propose intrusion detection system based on rules in order to more accurate intrusion detection. Cluster head perform role of monitor node to raise monitor efficiency of packet. In order to evaluate performance of proposed method, we used jamming attack, selective forwarding attack, repetition attack.

Key Words : Intrusion Detection System, Intrusion Prevention System, Mobile Ad-hoc Network

Ⅰ. 서론

최근에는 네트워크 시장의 빠른 변화로 무선 인터넷의 사용이 증가하고 있는 실정이다. 기존의 고정된 기반 시설 없이 이동 노드들로만 구성된 네트워크를 Mobile Ad-hoc Network(MANET)이라고 한다[1]. 따라서 네트워크를 구성하는 모든 노드들이 데이터 전달을 하는 라우터 기능을 수행해야만 한다. 이러한 특성 때문에 보안의 심각한 문제를 가지고 있다. NANET에서의 보안은 크게 네 가지 분야로 나눌 수 있다. 먼저 노드들 간의 안전한 경로를 제공하기 위한 라우팅 보안 분야, 제한된 에너지 문제로 발생하는 이기적인 노드 해결 분야, 보안을 제공하기 위한 키 관리 분야, 중앙 기반 시설이 없기 때문에 더욱 신경을 써야만 하는 침입탐지에 관한 분야로 나눌 수 있다. 특히 노드들의 이동성 때문에 보안상의 문제를 가지고 있으며 악의적인 노드들의 공격을 탐지해 낼 수 있는 침입탐지 시스템이 반드시 필요하다. 개인의 정보보호 및 네트워크의 보호와 침입에 대처하기 위해 침입탐지 시스템(Intrusion Detection System : IDS), 침입방지 시스템(Intrusion Prevention System : IPS)을 도입하여 사용하여 왔다[2]. 침입탐지 시스템은 외부로부터의 침입이 발생할 경우 이를 탐지하여 시스템 관리자에 즉각 침입을 알리게 된다. 침입탐지 시스템은 방화벽, 침

* 본 논문은 2008년 조선이공대학 학술연구비 지원에 의해 연구되었음.

** 조선이공대학 시각영상디자인 교수

입탐지 시스템 라우터, 각종 로그 파일의 내용을 분석할 수 있는 특수한 도구라 할 수 있다. 그리고 기존에 잘 알려진 공격 서명 데이터베이스를 저장하고 있다가 로그 파일에서 분석한 행위나 트래픽을 이 서명과 비교하여 유사점이 있는지를 확인한다. 서명과 일치하는 행위를 찾았다면 침입탐지시스템은 경보를 발생시킬 수 있고 공격자를 찾아내기 위한 다양한 작업을 수행하고 능동적으로 증거를 수집할 수 있다.

무선 환경에서는 다음의 다섯 가지 보안요소들을 반드시 고려해야만 한다. 첫 번째로 공격자에 의한 DoS(Denial of Service) 공격에도 불구하고 네트워크 서비스의 붕괴가 초래되지 않아야함을 의미하는 가용성(Availability)이다. 두 번째로 노드들 간에 전달되는 데이터들은 인증되지 않은 노드들에게 노출되지 않아야함을 보장하는 신뢰성(Confidentiality)이다. 세 번째로 노드로 하여금 통신에 관여하고 있는 상대 노드의 신원을 확신하게 하는 것을 의미하는 인증(Authentication)이다. 즉 어떤 노드가 통신하고 있는 노드가 본래 의도했던 그 노드가 맞는지를 확신하는 것이 필요하다. 네 번째로 통신하는 노드간에 전달되는 메시지가 중간에 변질되지 않았음을 보장하는 무결성(Integrity)이다. 다섯 번째로 메시지를 보낸 곳에서 메시지를 보낸 사실을 부정하지 못하도록 하는 부인방지(Non-Reputation)이다.

본 논문에서는 네트워크를 구성하는 노드들을 클러스터 형태로 구성한 후, 클러스터 헤드가 감시 노드의 역할을 수행하게 하였다. 그리고 클러스터 헤드가 보다 정확한 침입탐지를 수행하도록 규칙의 집합을 정의하고 이를 이용하도록 하였다. 본 논문에서는 각 노드들이 자신의 이웃 노드로 메시지를 전송할 때 클러스터 헤드에 의해 네트워크 실패 횟수가 계산되어 침입탐지를 수행할 수 있게 된다.

본 논문의 구성은 다음과 같다. 2장에서는 침입탐지시스템의 탐지 기법 및 유형에 대하여 살펴보고 3장에서는 본 논문에서 제안한 방법에 대하여 설명하였다. 4장에서는 제안한 방법의 성능을 평가하고 마지막으로 5장에서는 결론을 맺는다.

Ⅱ. 관련연구

2.1 침입탐지 시스템의 유형

침입탐지 시스템은 실시간으로 시스템에 침입을 시도하거나, 침입 행위가 일어나고 있거나, 발생한 침입을 확인하여 침입에 즉각 대응할 수 있도록 하는 시스템이다. 이러한 침입탐지 시스템은 탐지 유형에 따라 오용 탐지(Misuse Detection)와 비정상행위(Anomaly Detection)로 분류할 수 있다. <표 1>은 오용탐지에 주로 쓰이는 기법들이다.

<표 1> 오용탐지 기법의 종류

기 법	방 법
조건부 확률	특정 데이터가 침입일 확률을 공식에 의해 계산 후 탐지.
전문가시스템	침입 패턴들과 일치된 침입행위를 발견하는 경우 IF-THEN 규칙에 따라 처리함.
상태전이 분석	침입을 특정 시스템의 생태 전이의 순서로 표현하여 상태가 주어진 조건을 만족하면 다음 상태로 이동 / 분석함.
패턴 매칭	·잘 알려진 침입 유형에 대한 데이터를 가지고 침입 시나리오로 설정된 패턴들과 비교하여 탐지

오용 탐지는 시스템의 취약점에서 침입이 발생하는 경우 이를 탐지함으로써 침입이 발생할 때마다 정형적인 패턴들을 감시함으로써 탐지가 이루어진다. 즉, 침입에 사용되는 패턴들을 미리 가지고 있어 침입패턴만 찾으면 되므로 빠르게 검색할 수 있는 장점을 가지고 있다. 그러나 새로운 유형의 침입에 대해서는 탐지하기 어려운 단점이 있다[3-5].

비정상행위 침입 탐지는 일반적인 시스템 사용 패턴에서 벗어나는 행위를 말하는 것이다. 이러한 비정상적인 행위는 외부에서의 침입뿐만 아니라 내부 시스템 남용으로 인해 발생할 수 있으며, 잘 알려지지 않은 침입까지도 탐지할 수 있지만 감사 자료를 분석하여 판단해야 한다. 따라서 감사 자료를 분석하는데 많은 비용이 드는 단점을 가지고 있다.

<표 2> 비정상 행위 탐지 기법의 종류

기 법	방 법
통계적 접근	경험적인 자료를 토대로 처리하는 방식으로 사용자나 프로세스의 행위를 관찰 / 프로파일 생성 후 주기적으로 통계적 이상여부에 따라 처리하는 기법
특징 추출	특정 침입의 패턴을 추출하는 방법으로 침입의 예측, 분류 가능한 침입탐지 도구의 부분 집합을 결정하여 예측하고 분류하는 기법
신경망	명령의 순서를 신경망으로 학습시킨 후 다음에 실행할 명령을 예측하는 기법

<표 3> 구성 방법에 따른 침입탐지 시스템

	호스트 기반 IDS	네트워크 기반 IDS
OS와의 관계	종속적	독립적
침입흔적 삭제	가능	불가능
DoS 탐지	제한적	가능
암호화된 공격	가능	불가능
공격루트 탐지 범위	시스템 네트워크	네트워크에 제한적

침입탐지 시스템은 네트워크 구성 방법에 따라 호스트 기반 IDS와 네트워크 기반 IDS로 나눌 수 있다[6].

호스트 기반 IDS는 시스템 로그 정보와 감사(audit)기록 분석을 통해 침입을 탐지한다. 그리고 내부 사용자나 외부 침입자의 불법적인 시스템 사용이나 변경으로 부터 시스템을 안전하게 보호하는 기능을 수행하는 시스템이다. 호스트 기반 IDS는 non-promiscuous 모드에서 동작하고 이는 더 많은 시스템에서 사용될 수 있다는 장점이 있다. 하지만 호스트 기반 IDS는 보호하고자 하는 모든 시스템에 설치해야 한다는 단점이 있다. 네트워크 기반 IDS는 네트워크상의 모든 패킷의 헤더와 데이터를 분석하거나 트래픽을 분석하여 침입 여부를 판단한다. 네트워크 기반 IDS는 서명 분석(signature analysis)을 하는 경우가 많은데, 잘 알려진 공격을 탐지하는 능력은 뛰어나지만 알려지지 않은 공격이나 변형된 공격에는 탐지가 어렵고 암호화된 세션에 대한 침입탐지에도 취약하다[7]. <표 3>은 네트워크 기반 IDS와 호스트 기반 IDS의 특징을 비교하였다.

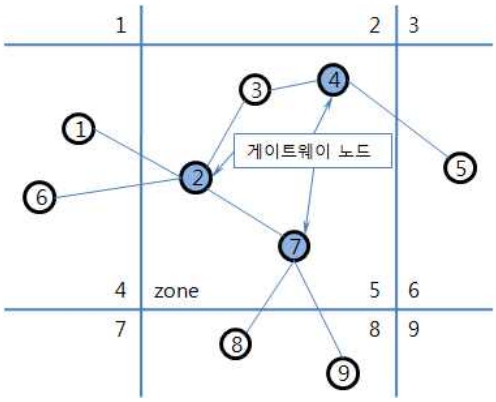
침입탐지시스템의 탐지 기법에 따라 시그너처 기반(signature-based) 탐지, 휴리스틱 침입(heuristic-based) 탐지, 명세기반(specification-based) 탐지, 규칙기반(rule-based) 탐지 등이 있다.

먼저 규칙기반 탐지기법은 전문가 시스템을 기초로 한다. 규칙의 집합을 이용하여 입력 자료에 대한 결론을 유도하는 작동 모듈로 구성된다. 이들 규칙은 침입 시나리오 실행 결과를 비교하여 반영하며, 어떤 규칙은 한 가지 이상의 침입 시나리오에 적용될 수 있다. 규칙기반 침입탐지의 단점의 유연성이 적고, 변형된 침입 시나리오는 탐지하기 어렵고, 규칙은 보안 전문가를 통하여서 생성되므로 대상 시스템의 상황 변화 등의 규칙 갱신이 어렵다. 휴리스틱기반 탐지 기법은 정상에서 벗어난 행위를 찾아내서 세 가지 특성인 정상, 위험, 기타중의 하나로 분류한다. 이때 침입탐지시스템이 학습하면서 어떤 동작들이 수용 가능한지 구분하게 된다. 동작들이 올바르게 분류 되었는가와 현재 동작들이 각 분류에 적합한 정도에 따라 제한을 받는다. 이 기법은 오탐지(false positive) 비율이 높다는 단점이 있다. 시그너처기반 기법은 잘 알려진 공격에 대응하는 탐지기법이다. 주로 패턴을 찾기 위해 단순한 패턴 매칭을 수행한다. 이 방법은 잘 알려진 공격에 대한 탐지 기법으로 오탐지 비율이 낮은 것이 특징이다. 그러나 시그너처 관리의 문제, 새로운 유형의 공격에 대한 시그너처를 수집해야하는 문제들이 있다. 마지막으로 명세기반 탐지 기법은 정상행위에서 벗어난 공격을 탐지한다는 점에서 이상탐지와 유사하다. 그러나 기계 학습 방법에 의존하지 않고, 적법한 시스템 행위들을 캡처해 수동으로 개발한 명세를 기반으로 한다. 그러므로 명세의 개발은 미탐지의 증가를 고려하여 개발해야만 한다.

2.2 ZBIDS

ZBIDS는 네트워크가 중복되지 않는 지역(zone)으로 분할하여 브로드캐스트에 의한 오버헤드를 줄이고, 침입

탐지 효율을 높이기 위해 지역의 경계 지점에 위치한 게이트웨이 노드들이 지역 내에서 브로드캐스트된 정보를 통합하여 최종적인 침입탐지 정보를 생성하는 접근 방식을 가지고 있다. 침입탐지 정보에 대한 통합은 경계지점에 위치한 노드들에 의해 주기적으로 수행되며, 통합을 위해 사용되는 정보는 공격 클래스, 시간, 공격의 근원지 정보이다. 이러한 세 가지 정보들이 얼마나 유사성을 가지는지의 여부에 따라 전송된 정보들은 통합이 되거나 무시되며, 최종적으로 침입탐지 경보가 만들어지고 대응을 위해 브로드캐스트된다. 이러한 ZBIDS의 장점은 네트워크를 작은 지역으로 나눔으로써 브로드캐스트에 의한 오버헤드를 감소시키고 침입탐지 시스템의 성능향상을 위한 침입탐지 정보 통합 알고리즘을 이용하였다는 점이다. <그림 1>은 ZBIDS의 구조를 보여주고 있다.



<그림 1> ZBIDS 구조

Ⅲ. 제안한 방법

3.1 노드의 초기화 및 클러스터 형성

MANET을 구성하는 노드들은 자신과 1-hop 거리에 있는 이웃 노드들을 기초로 클러스터를 형성하였다. 노드들 사이의 안전한 통신을 제공하고 의심스러운 노드들의 효율적인 탐지를 위하여 클러스터를 이용하였다. 먼저 네트워크를 구성하는 노드들의 클러스터 형성 과정은 다음과 같다. 첫 번째 단계로 모든 노드들은 이웃 노드와의 링크수와 신뢰도 값을 방송한다. 이 두 개의 값이 가장 높은 노드가 클러스터 헤드가 된다. 여기서 링크수가 높은 노드를 이용하는 것은 주변의 많은 노드의 정보를 유지하고 있기 때문이고, 신뢰도 값이란 이웃 노드의 패킷을 성공적으로 전달해 준 값을 의미한다. 즉, 신뢰도를 이용함으로써 노드들의 이기적인 행동을 막을 수 있는 효과가 있기 때문이다. 이렇게 선출된 클러스터 헤드는 IDS의 역할을 수행하게 된다. <그림 2> 상태 결정 함수를 이용하여 노드들은 수신한 메시지와 비교하여 자신의 상태를 결정하여 방송하게 된다.

```
Select_status(&RcvMsg)
{
if((Nd. lnk<RcvMsg. lnk)||(Nd. trst<RcvMsg. trst))
{
        NdTbl. state = Mn;
        HelMsg = NdTbl;
        Broadcast(HelMsg);
}
else if((Nd. lnk>RcvMsg. lnk)
                        ||(Nd. trst>RcvMsg. trst))
{
        NdTbl. state = Cl;
        HelMsg = NdTbl;
        Broadcast(HelMsg);
}
else
{
        NdTbl. state = Gw;
        HelMsg = NdTbl;
        Broadcast(HelMsg);
}
```

<그림 2> 노드 상태 결정 함수

3.2 침입탐지 규칙 정의

선출된 클러스터 헤드가 공격을 감시하기 위해서 정의된 규칙들과 비교하여 침입을 탐지하게 된다. 이 결과

에 의해서 공격자의 침입여부를 판단하게 되는 것이다. 다음은 침입탐지를 위해 사용하는 규칙들에 대한 설명이다. 첫 번째로 반복 규칙은 똑같은 메시지는 같은 이웃에 의해 제한된 횟수만큼 재전송될 수 있다는 것이다. 이 규칙은 침입자가 어디서 똑같은 메시지를 몇 번 송신했는지를 검출할 수 있기 때문에 서비스거부 공격에 대응할 수 있다. 두 번째로 jamming 규칙은 감시 노드에 의해 측정된 송신 메시지의 충돌 횟수는 네트워크 내에서 기대 수보다는 적어야만 한다. 네트워크 안에 잡음을 만들고 통신 채널을 왜곡시킬 수 있는 jamming 공격은 이 규칙에 의해 검출될 수 있다. 세 번째로 지연 규칙은 이웃 노드들에 의해 전송되는 메시지는 정의된 시간 안에 이루어져야 한다는 것이다. 그렇지 않으면 공격으로 검출된다. 네 번째로 재전송 규칙은 수신한 메시지를 자신의 이웃 노드에게 전달하는지를 감시한다. 이 규칙에 의해 검출될 수 있는 두 가지 공격은 블랙홀과 선택적 포워딩 공격이다. 다섯 번째로 무결성 규칙은 수신된 메시지의 내용을 수정하는 공격을 검출하기 위한 것이다. 마지막으로 Interval 규칙은 메시지의 전송 시간이 제한된 시간보다 짧거나 긴 경우 실패가 발생한다. 이웃 노드에 의해 생성된 데이터 메시지를 송신하지 않는 공격과 반대로 에너지 소모량을 증가시키기 위해 메시지 송신 비율을 증가시키는 공격을 이 규칙에 의해 탐지할 수 있다.

3.3 침입탐지 알고리즘

본 논문에서 제안한 침입탐지 알고리즘은 세 단계로 이루어져 있다. <그림 3>은 감시 노드의 침입탐지 단계를 보여주고 있다.

감시 노드는 클러스터 헤드의 역할을 수행하면서 IDS 기능을 수행한다. IDS는 세 단계로 이루어져 있으며, 각 단계별 기능은 다음과 같다. 먼저 첫 번째 단계는 침입탐지를 위한 데이터 수집 단계이다. 이 단계에서 감시 노드는 promiscuous 모드로 메시지를 감시하다가 의심스러운 정보가 발견되면 이 메시지를 저장한다. 메시지로부

<그림 3> 침입탐지 과정

터 추출된 데이터는 배열에 저장된다. 배열에 저장된 데이터의 삭제는 지정된 시간이 초과하거나 메모리의 양이 부족할 때 이루어진다. 두 번째 단계는 수집된 데이터에 규칙을 적용하는 단계이다. 배열에 저장된 데이터들이 이미 정의되어 있는 규칙에 해당되는지를 평가하게 된다. 만약 어느 규칙에도 해당되지 않는다면 실패 카운터 값을 증가시키고 메시지를 삭제한다. 무선 노드들은 제한된 자원을 이용해야 하기 때문에 불필요한 데이터를 삭제하는 것이 유리하다. 이렇게 함으로써 실행 시간, 탐지 시간을 줄일 수 있다. 마지막으로 침입탐지 단계이다. 이 단계에서는 공격자의 의도에 의해 마치 네트워크 문제인 것처럼 보이는 공격을 탐지해 낼 수 있는 능력을 향상시키기 위해 클러스터 헤드 노드에 감시 기능을 추가하는 방법을 제안하였다. 이렇게 함으로써 데이터 위변조, 블랙홀, 선택적 포워딩, jamming 등과 같은 공격에 의해 생긴 문제들을 보다 쉽게 해결할 수 있게 되었다. <그림 4>는 침입탐지 과정에 대한 pseudo 코드를 보여주고 있다. 자신의 이웃 노드에 전송된 메시지를 분석하는 동안 감시 노드는 모든 이웃 노드에 대해 네트워크 실패 횟수 값을 얻은 후, 기대 값과 비교한다. 만약에 네트워크의 실패 횟수 값이 크다면 공격이 발생한 것으로 간주하고 그렇지 않다면 네트워크 실패 횟수 값을 조합

하여 기대 값을 갱신한 후 감시 노드가 값을 저장한다.

```
// N_f : 네트워크 실패 횟수 값
// E_f : 누적된 기대 값
begin
    Get N_f, E_f;
    while(all neighbor)
    {
        while(all failure types)
        {
            if (N_f value > E_f value) then
                alarm attack indication;
            else
                update E_f value by combining
                it with N_f value;
        }
    }
end
```

<그림 4> 침입탐지 pseudo 코드

Ⅳ. 실험 및 결과

4.1 실험 환경

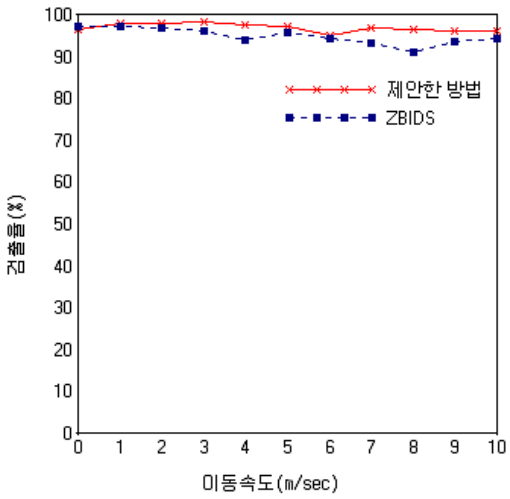
본 논문에서 제안한 침입탐지 시스템의 성능 분석을 위해 기존의 ZBIDS 기법과 성능을 비교하였다. 노드들의 이동 속도는 0m/s~5 m/s, 노드들의 정지 시간은 30초, 패킷의 크기는 64 바이트, 데이터 전송 범위는 150m로 하였다. 실험에 사용한 노드의 수는 50개이고 각 실험 시간은 300초로 하였으며 30번 반복 실험하였다. 본 논문에서 실험에 사용한 노드는 제한된 방향성을 가진 공간보다는 사용자가 자유롭게 움직일 수 있는 개방된 환경 하에서 동작한다고 가정한 것이다. 실험에 사용한 시스템은 cpu는 쿼드 코어 2.66Ghz, 메모리는 4G, 운영체제는 fedora linux 10을 사용하였으며 시뮬레이터는 ns-2를 사용하였다. 그리고 <표 4>에서와 같은 환경에서 실험하였다.

4.2 실험 결과

침입탐지 실험을 위해 jamming 공격, 선택적 포워딩, 반복 공격을 이용하였다. 각 공격은 임의로 발생시켰으며 실험 시간 동안 10번 발생시켰다. 실험에서 감시 노드는 수집된 데이터를 정의된 규칙에 적용하여 침입탐지 및 공격의 유형을 탐지하게 된다.

<표 4> 실험에 사용한 환경 변수

환 경 변 수	값
이동성 모델	Random waypoint model
무선 전송 모델	Two-Ground(1/r4)
MAC 프로토콜	IEEE 802.11 DCF
네트워크 크기	1000 × 1000
대역폭	1Mbps

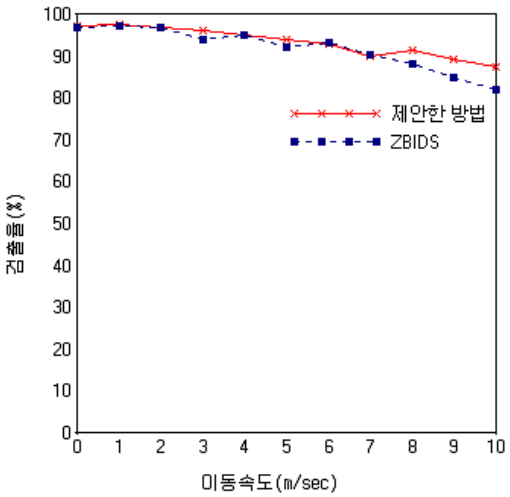


<그림 5> Jamming 공격 탐지

<그림 5>는 Jamming 공격 탐지율을 보여주고 있다. Jamming 공격은 클러스터 헤드나 게이트웨이 노드에 의해 보내진 메시지의 충돌 횟수가 네트워크내의 기대 수보다 적어야 한다. 만약 기대 수치보다 크게 된다면 이를 공격으로 간주하게 된다. 네트워크 내에 잡음을 만들고 통신 채널을 왜곡시킬 수 있는 jamming 공격도 쉽게 탐지해 낼 수 있었다. <그림 5>에서 나타나듯이 노드의 수

가 많고 이동 속도가 빠를수록 패킷의 충돌 횟수가 증가함에 따라 자연스러운 네트워크 오류를 공격으로 잘못 탐지하는 비율이 약간 높아졌다.

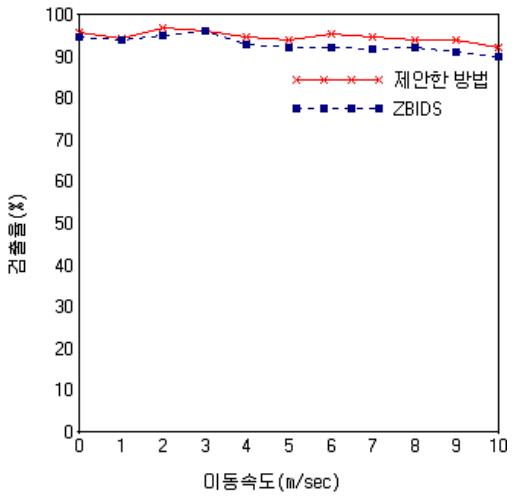
<그림 6>에서 보여주는 선택적 포워딩 공격은 감시 노드에 의해서 이웃 노드의 행동을 파악하고 있기 때문에 높은 탐지율을 보여주고 있다. 그러나 노드들의 이동 속도가 빨라짐에 클러스터의 형성이 빈번히 발생함에 따라 공격의 오탐지율이 약간 높아졌다. 왜냐하면 데이터의 재전송 횟수나 노드 자체의 오류로 인하여 이를 공격으로 탐지하는 경우가 발생하였기 때문이다. ZBIDS도 마찬가지로 노드들의 이동 속도가 빨라짐에 따라 탐지율이 떨어지는 것을 확인할 수 있었다.



<그림 6> 선택적 포워딩 공격 탐지

<그림 7>에서는 반복 공격 탐지율을 보여주고 있다. 클러스터 헤드는 이웃 노드들에 의해 전송되는 패킷을 감시하고 있기 때문에 공격자가 어디에서 같은 메시지를 반복해서 전송하는 것을 쉽게 탐지해 낼 수 있었다. 그림에서 보듯이 제안한 방법과 ZBIDS는 거의 비슷한 성능을 보여주고 있다.

<표 5>는 반복 실험을 통해 얻은 공격 유형별 평균 탐지율을 보여주고 있다. 표에서와 같이 제안한 방법이



<그림 7> 반복 공격 탐지

실험에 사용한 모든 공격 유형에서 기존의 ZBIDS에 비해 탐지율이 낫다는 것을 확인할 수 있었다. 또한 모든 공격에 대한 안정된 탐지율을 나타내는 것도 확인할 수 있었다.

<표 5> 공격 유형별 평균 탐지율

	제안한 방법	ZBIDS
Jamming 공격	96.8%	91.4%
선택적 포워딩 공격	95.3%	90.9%
반복 공격	96.6%	90.2%
평 균	**96.2%**	**90.8%**

V. 결론

본 논문에서는 MANET을 구성하는 노드들을 클러스터로 형성한 후 선출된 클러스터 헤드로 하여금 정의된 규칙의 집합을 이용하여 공격을 탐지할 수 있는 침입탐지시스템을 제안하였다. 노드들의 이동성 때문에 보안에 취약한 부분이 많고 무선을 이용한 침입이 유선에 비해 더욱 다양하고 쉽기 때문에 기존의 보안 시스템을 적용

하는데 어려움이 많다. 따라서 공격자의 악의적인 공격을 탐지하고, 오탐지율을 낮추기 위해서 다양한 공격에 대한 규칙을 정의하였다. 그리고 이웃 노드로 부터의 공격을 분석하기 위해 클러스터 헤드가 감시 노드의 역할을 수행하였다. 이렇게 함으로써 네트워크내의 이상한 행동을 하는 노드를 쉽게 파악할 수 있게 되었으며 공격의 오탐지율을 낮추게 되었다. 향후 연구로는 감시 노드의 전원 문제를 해결할 수 있도록 다양한 연구가 이루어져야 할 것이다.

참고문헌

[1] 유응구, "MANET에서의 에너지를 고려한 라우팅 프로토콜," 디지털산업정보학회, 디지털산업정보학회논문지 제3권, 제3호, 2007.

[2] Yongguang Zhang, Wenke Lee, "Intrusion Detection in Wireless Ad-Hoc Networks," Proceedings of the sixth international conference on Mobile Computing and Networking(MobiCom 2000), Boston, MA, August 2000.

[3] 최윤정, "침입탐지시스템의 정확도 향상을 위한 개선된 데이터마이닝 방법론," 디지털산업정보학회, 디지털산업정보학회논문지 제6권, 제1호, 2010.

[4] Salvatore J. Stolfo, et al., "Anomaly Detection in Computer Security and an Application to File System Accesses," Proceedings of 15th International Symposium of Foundations of Intelligent Systems, 2005.

[5] Shi Zhong, Taghi M. Khoshgoftaar, and Naeem Seluya, "Evaluating Clustering Techniques for Network Intrusion Detection," In Proceeding of the 10th ISSAT International Conference on Reliability and Quality and Design, Las Vegas, Nevada, 2004, pp. 149-155.

[6] Y. C. Hu, A. Perrig, and D. B. Johnson, "Packet leashes: A defense aginst wormhole attacks in wireless networks," In Proceeding of IEEE Infocomm, 2003, pp. 349-364.

[7] J. Deng, R. Han, and S. Mishra, "A performance evaluation of intrusion-tolerant routing in wireless sensor networks," In Proceeding of IEEE 2nd Int'l Workshop on info Processing in Sensor Networks, April 2003.

* 본 논문은 2008년 조선이공대학 학술연구비 지원에 의해 연구되었음.

■ 저자소개 ■

정 혜 원
Jung, Hye Won

2001년 3월~현재 조선이공대학 시각영상콘텐츠과 교수
2005년 2월 조선대학교 전산멀티미디어전공 (이학박사)
1998년 8월 조선대학교 산업디자인학과 (미술학 석사)
1992년 2월 전남대학교 시각디자인전공 (미술학사)

관심분야 : 콘텐츠 보호, 모바일 콘텐츠, 정보보호
E-mail : hwjung@chosun-c.ac.kr

논문접수일 : 2010년 10월 19일
수 정 일 : 2010년 11월 2일(1차), 11월 16일(2차)
게재확정일 : 2010년 11월 22일