디지털산업정보학회 논문지 제14권 제1호-2018년 3월
http://dx.doi.org/10.17662/ksdim.2018.14.1.035

Mobile Ad Hoc Network에서 분산 모니터링을 이용한 향상된 침입탐지 기법 연구

양 환 석*

A Study on Improved Intrusion Detection Technique Using Distributed Monitoring in Mobile Ad Hoc Network

Yang Hwanseok

〈Abstract〉

MANET composed of only wireless nodes is increasingly utilized in various fields. However, it is exposed to many security vulnerabilities because it doesn't have any infrastructure and transmits data by using multi-hop method. Therefore, MANET should be applied the intrusion detection technique that can detect efficiently malicious nodes and decrease impacts of various attacks. In this paper, we propose a distributed intrusion detection technique that can detect the various attacks while improving the efficiency of attack detection and reducing the false positive rate. The proposed technique uses the cluster structure to manage the information in the center and monitor the traffic of their neighbor nodes directly in all nodes. We use three parameters for attack detection. We also applied an efficient authentication technique using only key exchange without the help of CA in order to provide integrity when exchanging information between cluster heads. This makes it possible to free the forgery of information about trust information of the nodes and attack nodes. The superiority of the proposed technique can be confirmed through comparative experiments with existing intrusion detection techniques.

Key Words : Intelligent Intrusion Detection, Malicious Nodes, MANET, Trust Management

Ⅰ. 서론

노트북 또는 무선 태블릿 등의 무선 컴퓨팅 디바이스들의 광범위한 보급으로 인프라스트럭처 도움 없이 네트워크를 구성할 수 있는 MANET은 많은

* 중부대학교 정보보호학과 조교수

인기를 얻고 있으며 그 활용 분야도 매우 다양해지고 있다. 하지만 MANET은 다중 홉 방식으로 데이터 전송이 이루어지기 때문에 라우터나 AP와 같은 네트워크상의 제어 장치가 존재하지 않는다[1]. 따라서 기존 네트워크에서 적용되었던 라우팅 프로토콜이 그대로 적용될 수 없으며, 노드들의 이동에 의한 동적인 환경 그리고 무선 환경의 특성 등으로 인해 많은 보안 위협에 쉽게 노출될 수밖에 없다[2-3]. 이러한 라우팅 공격을 막기 위해 많은 방법의 보안 라우팅 기법에 대하여 연구가 이루어져 왔다. 이러한 연구는 크게 네트워크 전역 정보를 수집하는 기법, 네트워크에 참여하는 노드들에 대한 인증 기법, 지리적 라우팅 기법으로 구분된다. 그럼에도 불구하고 MANET에는 이렇게 보안에 취약한 많은 특성들 때문에 공격의 종류도 매우 다양하게 존재한다. 따라서 이러한 공격들로 인한 충격을 최소화시키고 네트워크네 악의적인 노드들에 대한 효율적인 침입탐지 시스템은 반드시 존재해야 한다[4]. 이러한 침입탐지시스템은 오탐율을 낮추면서 동시에 여러 공격을 탐지할 수 있는 능력을 갖고 있어야만 한다. 이렇게 된다면 결과적으로 네트워크 수명을 증가시키고 신뢰도를 높일 수 있게 된다[5~7].

본 논문에서는 동적 환경에서 특정 공격의 효율적인 탐지를 위해 분산 침입탐지 기법을 제안하였다. 분산 침입탐지를 위해 네트워크에 참여하는 모든 노드에서 자신과 1-hop 거리에 있는 이웃 노드들에 대한 트래픽 감시하며 패킷 포워딩 비율, 패킷 생성 비율, 패킷 폐기 비율을 측정하였다. 측정된 값들의 효율적 관리를 위해 클러스터 구조를 적용하였다. 측정된 매개변수 값들은 다차원 벡터로 저장되며, 클러스터 헤드에서 이 값들을 활용하여 공격 노드에 대한 탐지를 수행하게 된다. 또한 클러스터 헤드들 간의 공격 노드 정보와 노드들의 신뢰 정보를 교환할 때 무결성을 제공하기 위하여 어떠한 CA의 도움 없이 공개키와 공유키 교환 과정만을 통한 인증 방법을 적용하였다. 이러한 방법을 통해 노드들의 신속하고 안전한 데이터 전송을 보장할 수 있게 되었다.

본 논문의 구성은 다음과 같다. 2장에서는 MANET에서 적용된 침입탐지 기법에 대하여 살펴보고 3장에서는 본 논문에서 제안한 분산 침입탐지 기법에 대하여 설명하였다. 4장에서는 실험을 통해 제안한 기법의 성능을 평가하였으며 마지막으로 5장에서는 결론을 맺는다.

II. 관련연구

2.1 침입탐지 기법

MANET은 다중 홉 방식의 데이터 통신과 동적인 토폴로지의 특성으로 인하여 많은 공격에 노출되어 있다. 이러한 보안 취약점들은 심각한 문제를 야기할 수 있기 때문에 MANET에서는 가용성, 기밀성, 무결성, 부인방지, 인증 등의 보안 요구사항들을 잘 지켜야만 한다[8]. 특히 라우팅 과정에서 발생할 수 있는 많은 공격들에 대비하여 그 동안 다양한 침입탐지 기법들이 연구되어 왔으며 몇 가지 기법들의 특징들을 살펴보면 다음과 같다.

DLM(Dynamic Learning Method) 기법은 동적 학습을 기초로 한 공격탐지 기법이다[9]. 이 기법에서 공격 탐지를 위해 감시 대상은 RREQ와 RREP의 양, RREQ와 RREP의 시퀀스 번호이다. 이 기법은 공격으로 판단하는 기준 값 초과여부를 감시하여 이를 초과하면 공격 노드로 간주고 그렇지 않다면 정상 노드로서 마지막에 측정된 데이터를 동적 업데이트하게 된다.

SRP(Secure Routing Protocol) 기법은 소스 노드

로부터 수신된 패킷 수가 송신한 패킷 수를 비교하여 공격을 탐지하는 기법이다[10]. 즉, 수신한 패킷보다 송신 패킷이 많을 경우 소스 노드는 자신의 ID를 이용하는 공격 노드가 존재하는 것으로 인지하고 경고 메시지를 방송하게 된다. SRP 기법의 단점은 서로 통신을 하는 노드들 사이에서만 ACK를 통한 공격 탐지가 이루어지기 때문에 경로 상에 존재하는 노드 이외의 이웃 노드들에 대한 공격탐지가 어렵다는 것이다.

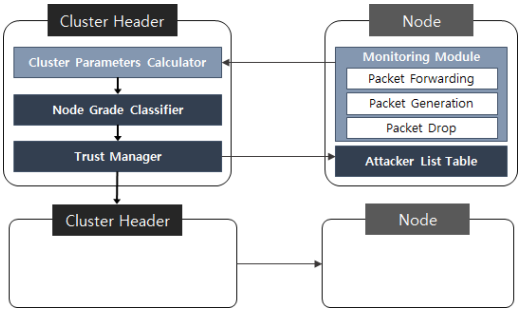
PCBHA(Prevention of a Co-operative Black Hole Attack) 기법은 경로 발견시 RREQ에 응답한 노드들 중 신뢰도가 가장 높은 노드를 선택하여 데이터 전송을 수행한다. 소스 노드가 목적 노드로부터 ACK 메시지를 수신하면 데이터 전송에 참여한 이웃 노드들의 신뢰도를 1 증가시키고, 그렇지 않다면 1을 감소시킨다. 이러한 방법으로 경로 상에 블랙홀 공격을 탐지하게 된다[11].

MA-IDS(Mobile Agent-IDS)는 mobile agent를 이용해 일정 범위내의 노드들에 대한 정보를 수집한다. 공격 탐지는 mobile agent에 탑재되어 있는 공격 탐지 알고리즘에 의해 수행된다. 이 기법은 에너지와 네트워크 오버헤드를 줄일 수 있는 장점을 가지고 있으나 큰 네트워크에 전송 범위가 좁다면 적용하기 어려운 단점이 있다[12].

Ⅲ. 제안한 기법

3.1 시스템 개요

본 논문에서는 동적 환경에서 악의적인 노드와 공격의 효율적인 탐지를 위하여 분산 침입탐지 기법을 제안하였다. 제안한 침입탐지 기법은 네트워크에 참여하는 모든 노드에서 1-hop 거리의 이웃 노드들에 대한 모니터링을 수행한다. 악의적인 노드 탐지를 위하여 다양한 매개변수를 활용하는데 이는 침입탐지 정확도 향상에 있어 중요한 요소가 된다. 그리고 매우 낮은 오탐율을 가지면서 동시에 여러 유형의 공격을 탐지할 수 있는 장점을 갖게 된다. 본 논문에서 제안한 분산 침입탐지는 클러스터 구조를 이용하였다. 즉 모든 노드에서 수집된 이웃 노드들에 대한 신뢰 정보를 관리하기 위해서이다. 각 클러스터네 클러스터 헤드는 노드들에 대한 신뢰 관리, 중앙 네트워크 관리, 노드 분류 역할을 담당한다. 네트워크에 참여하는 모든 노드들은 자신과 1-hop 떨어진 이웃 노드들의 트래픽을 감시한다. 이때 침입탐지를 위하여 패킷 포워딩 비율, 패킷 생성 비율, 패킷 폐기 비율을 측정하게 된다. 이렇게 측정된 값들은 자신의 클러스터 헤드에게 전달하게 된다. 클러스터 헤드에서는 자신의 관리하는 클러스터네 평균값과 비교하여 그 결과에 따라 해당 노드를 공격 노드, 경계 노드, 정상 노드로 분류하게 된다. 만약 공격 노드가 탐지된다면 해당 노드는 신뢰 관리자에서 등록을 하고 이웃 클러스터 헤드에게 해당 정보를 전송하여 공격 노드에 대한 정보를 신뢰 관리자에 등록하게 된다. 그리고 각 클러스터 헤드는 클러스터네 모든 노드들에게 정보를 전달하여 공격 노드로부터의 수신하는 모든 패킷은 모두 폐기하고 공격 노드로 패킷 전달도 모두 차단하게 된다. 클러스터 헤드들 간의 노드들에 대한 신뢰 정보나 공격 노드들에 대한 정보 교환 시 공격 노드들에 의한 데이터 변조를 차단하기 위하여 인증 기법을 적용하였다. 이때 서로에 대한 인증은 어떤 CA(Certificate Authority)의 도움 없이 서로간의 키 분배를 이용한 인증 방법을 사용하여 키 관리의 효율성을 향상시켰다. <그림 1>은 본 논문에서 제안한 분산된 침입탐지 기법의 구조를 보여주고 있다.



<그림 1 > 제안한 침입탐지 구조

3.2 분산 침입탐지 기법

네트워크네 악의적인 노드에 의한 공격을 보다 효율적으로 탐지하기 위하여 본 논문에서는 네트워크에 참여하는 모든 노드에서 자신과 1-hop 거리에 있는 이웃 노드들에 대한 트래픽을 감시하게 된다. 특히 침입탐지의 정확도 향상을 위하여 패킷 포워딩 비율(P_f), 패킷 생성 비율(P_g), 패킷 폐기 비율(P_d)을 매개변수로 사용하였다. 자신과 1-hop 거리의 각각의 이웃 노드들에 대한 매개변수 값을 측정하여 속성 집합으로 저장하게 된다. 노드 N_i의 속성 집합은 식 (1)과 같이 표현된다.

$$S_{N_i} = \{P_f, P_g, P_d\} \tag{1}$$

이와 같이 이웃 노드들에 대한 활동을 감시하고 그 속성들에 대한 값들을 다차원 벡터로 저장한 후 그 값을 클러스터 헤드에게 전달하게 된다. 본 논문에서 공격 여부를 판단하기 위해 사용되는 매개변수들은 다음과 같이 측정이 이루어진다. 먼저, 첫 번째 패킷 생성 비율은 일정 시간동안 노드 k가 자신의 이웃 노드 n에 생성한 제어 패킷의 양을 측정한 값을 의미한다. 그리고 노드 n이 속한 클러스터 k의 제어 패킷 평균값은 식 (2)에 의해 측정된다.

$$C_k(Avg(P_g)) = \sum_{i=1}^{n} P_g(N_i)/n \tag{2}$$

만약 노드 n에서 생성한 제어 패킷의 양이 클러스터 내 평균값보다 훨씬 큰 값을 갖는다면 해당 노드는 플러딩 공격을 의심할 수 있다. 다중 홉 환경에서 데이터 전달은 모든 노드에서 반드시 이루어져 한다. 두 번째 패킷 포워딩 비율은 목적 노드를 향해 이웃 노드가 패킷을 전송한 비율을 의미하며, 다른 노드들에 비해 이 비율이 상당히 크다면 해당 노드는 선택적 공격으로 의심할 수 있다. 따라서 일정 시간동안 노드 k가 자신의 이웃 노드 n에 대해 성공적으로 포워딩된 패킷 비율을 다음 식 (3)에 의해 계산한다.

$$P_f = \sum_{t=1}^{n} \left(\frac{P_f(N_d)}{P_r(N_d)}\right) \tag{3}$$

여기서 $P_f(N_k)$는 노드 n이 목적 노드 d에게 포워딩한 패킷의 양이고 $P_r(N_d)$는 노드 n이 수신한 패킷 중 목적 노드가 d인 패킷의 양이다. 그리고 식 (2)와 같은 방법으로 클러스터내 패킷 포워딩 평균값을 계산한다. 세 번째 패킷 폐기 비율은 이웃 노드 n이 수신한 전체 패킷 중 다른 이웃 노드로 패킷을 포워딩 한 비율을 측정한 값이다. 만약 이 값이 높게 나타난다면 해당 노드는 이기적인 행동을 하는 노드로 의심할 수 있다. 이 값은 식 (4)로 계산된다.

$$P_d = \sum_{t=1}^{n} \left(\frac{P_f(total)}{P_r(total)}\right) \tag{4}$$

이렇게 측정된 세 개의 매개변수 값은 클러스터 헤드에서 측정한 클러스터 내 평균값들과 비교한 후 정상(1), 의심(0), 공격(-1)의 플래그 값을 설정한다. 노드 등급 분류기에서는 세 개의 매개변수 중 공격(-1) 플래그를 하나라도 갖게 되면 해당 노드는 공격 노드로 분류가 되고, 의심(0)이 두 개 이상이면 경계 노드로 분류하게 된다. 공격 노드로 판정되면 해당 노드에 대한 정보는 이웃 클러스터 헤드에게 방송하

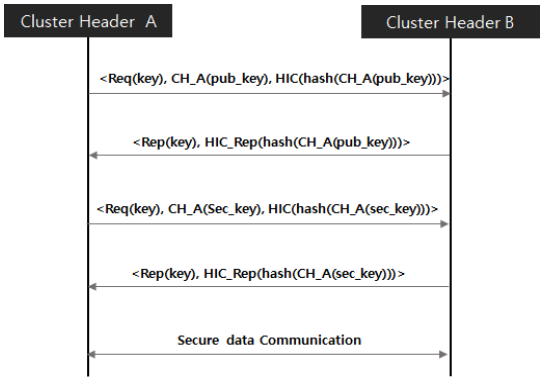
여 모든 노드들의 공격 노드 리스트에 공격 노드 정보를 등록하여 해당 노드로 부터의 모든 패킷을 폐기하여 네트워크 참여를 배제시킨다. 그리고 경계 노드의 경우 모니터링 간격을 증가시켜 활동 감시 횟수를 증가시킨다. <그림 2>는 클러스터 헤드에서 실행되는 침입탐지 과정 중 매개변수의 특징 계산에 대한 코드 일부를 보여주고 있다.

```
private void calParm(double pf, double pg, double pd) {
    for(i=0; i=n; i++) {
        this.pf += pf;
        this.pg += pg;
        this.pd += pd;
    }
    avgPf = this.pf / n;
    avgPg = this.pf / n;
    avgPd = this.pf / n;
    nodeClassfier(avgPf, avgPg, avgPd);
}
private void nodeClassfier(double avgPf, double avgPg, double avgPd)
{
    if(N[i].Pf >= (avgPf + (avgPf * 0.2)) {
        N[i].f = -1;
        sendTo(N[i].info());
    }
    else if(N[i].Pf > avgPf) {
        N[i].f = 0;
        sendTo(N[i].info());
    }
    else {
        N[i].f = 1;
        update(N[i]);
    }
}
```

<그림 2> 침입탐지를 위한 매개변수 특징 계산

3.3 클러스터 간 인증 기법

클러스터 헤드는 클러스터내 노드들에 대한 신뢰 정보 및 노드 유형 정보를 관리하고 공격 노드들에 대한 정보를 서로 교환하여 공격 노드의 네트워크 참여를 차단하게 된다. 따라서 클러스터 헤드 사이에 이러한 중요한 정보를 전송하는데 무결성이 보장된 안전한 데이터 전송을 위하여 키 교환 인증 기법을 적용하였다. 클러스터 헤드간의 인증을 위하여 CA 존재 없이 클러스터 헤드 간의 키 교환만을 통해서 이루어지기 때문에 키 관리의 효율성과 신속한 보안 기능을 제공해준다. 클러스터 헤드들간 키 교환 과정은 다음과 같다. 첫 번째 단계는 소스 클러스터 헤드는 자신의 공개키와 공개키 인증 서명을 송신한다. 두 번째 단계는 패킷을 수신한 목적 클러스터 헤드는 공개키와 공개키의 해시 검사 코드(HIC: Hash Inspection Code)를 포함하는 응답 메시지를 전송한다. 세 번째 단계는 소스 클러스터 헤드는 공유키를 생성하여 목적 클러스터 헤드의 공개키로 암호화하여 전송한다. 네 번째 단계는 공유키를 이용하여 전송하고자 하는 데이터를 암호화하여 전송한다. 위와 같은 방법으로 클러스터 헤드간의 안전하고 신속한 인증 기법을 제공하고 클러스터 헤드들의 정보 전송에 무결성을 높이게 된다. 그리고 서로간의 키 관리의 효율성을 높일 수 있다. 위에서 설명한 인증과정을 <그림 3>에서 보여주고 있다.



<그림 3> 클러스터 헤드간 인증 과정

IV. 성능분석

4.1 실험 환경

본 논문에서 제안한 공격탐지의 성능평가를 위하여 MANET을 실험할 수 있는 NS-2 시뮬레이터를 이용하였으며 <표 1>에서 제시한 다양한 매개변수를 이용하였다. 실험에서 사용한 공격은 블랙홀 공

격과 플러딩 공격을 발생시켰으며 이때 네트워크의 성능을 측정하였다.

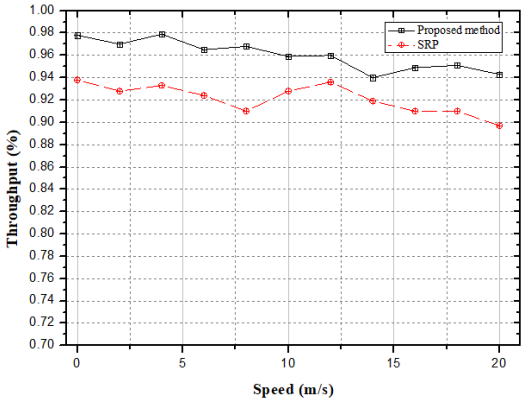
<표 1> 실험에 사용한 환경 변수

Parameter	Value
Network Size	1000 × 1000
Number of Nodes	50
Number of Malicious Nodes	10
Routing Protocol	AODV
Pause Time(Sec)	20
Attack Type	Blackhole, Flooding
Simulation Time	60
Traffic Pattern	CBR
MAC Layer	IEEE 802.11

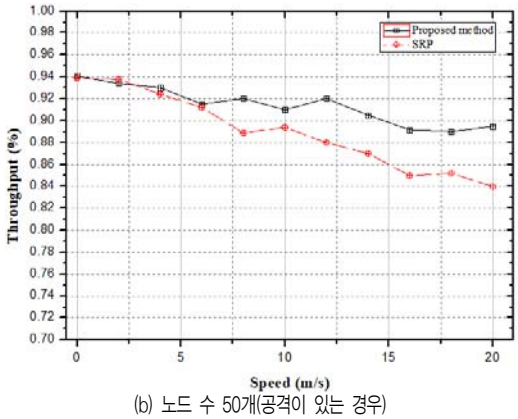
4.2 성능 평가

이 장에서는 본 논문에서 제안한 공격탐지 기법의 성능 측정 결과에 대하여 설명하며, 성능 평가 기준은 공격 유무에 따른 처리율, 종단 간 지연, 패킷 손실률, 오탐률로 설정하였다. 그리고 본 논문에서 제안한 클러스터 헤드간 인증 기법에 대한 성능 평가는 키 교환에 의해 중요 정보가 위변조 없이 정확하게 교환이 이루어지면 앞서 언급한 평가 기준들에 대한 성능이 우수하게 나타나기 때문에 이로 대체한다. 성능 측정은 SRP 기법과 비교 실험하였다.

<그림 4>는 단위 시간동안에 목적 노드에 성공적으로 전송된 패킷들의 평균 비율을 측정한 결과를 보여주고 있다. SRP 기법은 소스 노드와 목적 노드 사이의 패킷 양의 검사를 통해 공격 탐지가 이루어지기 때문에 처리율에서는 좋은 결과를 보여주었다. 제안한 기법도 노드들에 생성된 패킷 생성, 폐기, 포워딩 비율을 측정하여 공격을 탐지하기 때문에 공격이 존재하는 상황에서도 우수한 결과를 보여주었다.



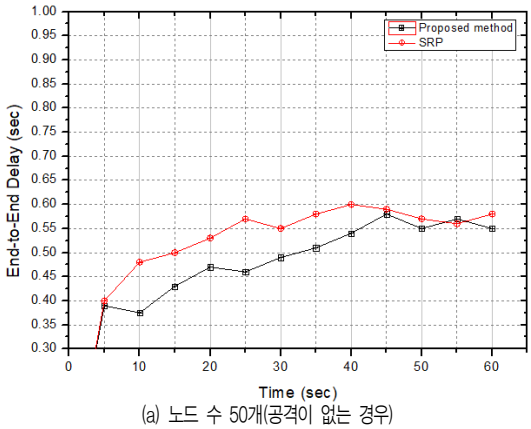
(a) 노드 수 50개(공격이 없는 경우)



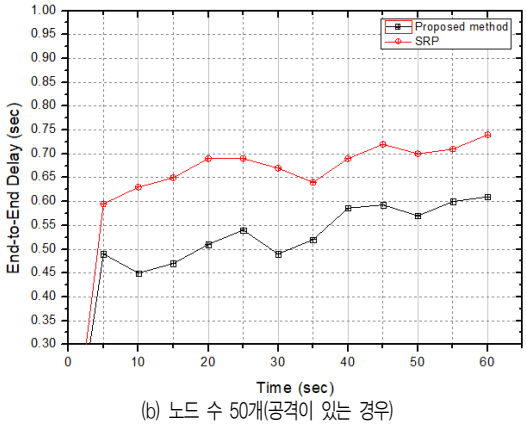
(b) 노드 수 50개(공격이 있는 경우)

<그림 4> 처리율

<그림 5>에서는 소스 노드에서 생성한 데이터 패킷이 목적 노드에 완전하게 도착한 시간을 측정한 결과를 보여주고 있다. SRP 기법은 소스 노드와 목적 노드 사이에 설정된 경로상의 공격외 이웃 노드에 의한 공격 탐지 성능이 낮기 때문에 공격 발생시 지연시간이 다소 높은 결과를 보여주었다. 그러나 제안한 기법은 모든 노드에서 자신의 이웃 노드들에 대한 공격 감시가 이루어지기 때문에 공격 발생 시에도 좋은 결과를 보여주었다.

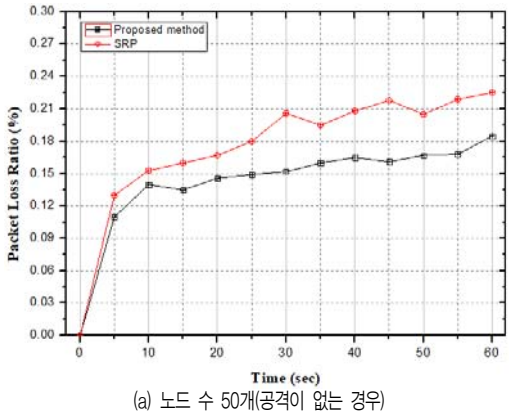


(a) 노드 수 50개(공격이 없는 경우)

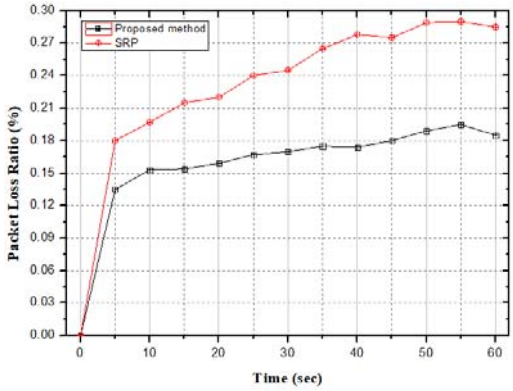


(b) 노드 수 50개(공격이 있는 경우)

<그림 5> 종단간 지연 시간



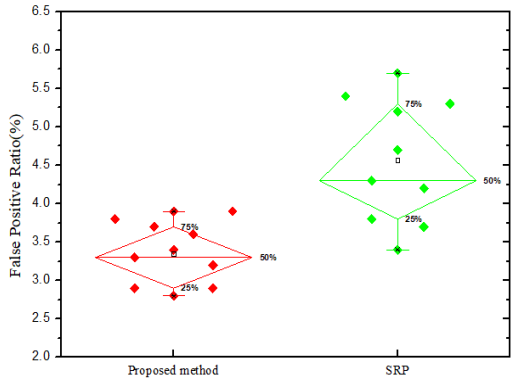
(a) 노드 수 50개(공격이 없는 경우)



(b) 노드 수 50개(공격이 있는 경우)

<그림 6> 패킷 손실율

<그림 6>은 패킷 손실율에 대한 실험 결과를 보여주고 있다. 이 평가 기준은 공격 발생시 공격 노드를 얼마나 빨리 탐지하여 목적 노드로의 패킷 손실이 덜 발생하게 하는 중요한 요소라고 할 수 있다. SRP는 노드의 이동에 따른 경로 재설정 그리고 이웃 노드에 대한 탐지 성능 저하로 인해 이동 속도가 증가할수록 패킷 손실율을 급격히 증가하는 모습을 보여주었으며, 제안한 기법도 노드들의 이동 속도에 따라 패킷 손실율이 다소 높게는 나타났으나 공격의 존재 유무에는 큰 영향을 받지 않았음을 확인할 수 있었으며 이는 공격 탐지의 성능이 우수하다는 것을 알 수 있는 요소이다.



<그림 7> 평균 오탐율

오탐률은 침입탐지의 가장 중요한 성능 평가 요

소 중의 하나이다. <그림 7>은 실험에서 사용한 블랙홀 공격과 플러딩 공격에 대한 10회 반복 실험한 결과의 평균값을 보여주고 있다. 그림에서 확인할 수 있듯이 제안한 기법은 모든 노드에서 1-hop 거리의 이웃 노드들에 대한 감시에 이에 대한 정보 관리가 이루어지기 때문에 오탐율이 상당이 낮은 결과를 얻을 수 있었다.

Ⅴ. 결론

본 논문에서는 공격 탐지의 효율성을 높이고 동시에 여러 공격을 탐지할 수 있는 능력을 갖추면서 오탐률 낮추는데 초점을 맞추었다. 이를 위하여 패킷 포워딩 비율, 패킷 생성 비율, 패킷 폐기 비율을 공격탐지의 매개변수로 결정하였다. 분산 탐지를 위해 네트워크에 참여하는 모든 노드에서 1-hop 거리의 이웃 노드들에 대한 트래픽을 감시를 통해 정보를 수집한다. 수집된 정보들의 효율적인 관리와 공격 여부 판단을 위해 클러스터 구조를 이용하였다. 클러스터 헤드는 노드에서 수집된 매개변수 속성 값들에 대해 탐지 알고리즘을 적용하여 공격 노드의 판단과 노드들의 신뢰 정보 관리 등 중앙 관리자 역할을 수행하게 된다. 그리고 클러스터 헤드들 간의 공격 노드 정보와 신뢰 정보 등을 교환 시 악의적인 노드들에 의해 전송 정보의 변조도 고려하지 않을 수 없다. 따라서 어떠한 CA가 존재하지 않은 상황에서 4단계로 이루어진 노드들 간의 키 교환만을 이용하여 신속하고 안전한 데이터 전송기법을 제안하였다. 이러한 과정으로 키 관리의 효율성을 높일 수 있으며, 공격 노드와 노드들의 신뢰 정보에 대한 무결성을 제공할 수 있게 되었다. 본 논문에서는 실험을 통해 노드 수와 공격 유무에 따른 처리율, 패킷 손실률, 종단간 지연, 오탐률을 성능평가 기준으로 하여 SRP 기법과 비교 실험하였다. 실험을 통해 제안한 기법의 우수한 성능을 확인할 수 있었다.

참고문헌

[1] Butun, I., Morgere, S.D., Sankar, R., “A survey of intrusion detection system in wireless sensor networks,” IEEE Communication System, Tutorials 16(1), 2014.

[2] Kaur, J., Lindskog, D., Zavarsky, P., “An algorithm to facilitate intrusion response in mobile ad hoc networks,” Proceedings of the 9th International Conference on Security of Information and Networks, 2016.

[3] 고장혁, 이동호, “네트워크 트래픽 수집 및 복원을 통한 내부자 행위 분석 프레임워크 연구,” 디지털산업정보학회지, 제13권, 제4호, 2017, pp. 125-135.

[4] Nguyen, H.L., Nguyen, U.T., “A study of different types of attacks in mobile adhoc networks,” 25th IEEE Canadian Conference on Electrical Computer Engineering(CCEC), 2012.

[5] 이세열, “자가적응모듈과 퍼지인식도가 적용된 하이브리드 침입시도탐지모델,” 디지털산업정보학회지, 제13권, 제3호, 2017, pp. 19-25.

[6] 석선우, 최승원, “Efficient and Security Enhanced Evolved Packet System Authentication and Key Agreement Protocol,” 디지털산업정보학회지, 제13권, 제1호, 2017, pp. 57-101.

[7] R. M. Chamudeeswari, P. Sumathi, “Security attacks on Routing protocols and Intrusion Detection in MANET,” International Journal of

Scientific Research and Management, Vol.5, 2015, pp. 7067-7073.

[8] Sahana, S., Saha, S., Das Gupta, S., " Weight based hierarchical clustering algorithm for mobile ad hoc networks," Procedia Eng., No. 38, 2012, pp. 1084–1093.

[9] Han-Chao Lee, Shin-Ming Cheng, Kuo-Ping Wu, "A responsive probing approach to detect dynamic intrusion in a MANET," IEEE, Vol. 3, No. 2, 2016, pp. 243–259.

[10] Badie, A.M., Lindskog, D., Zavarsky, P., "Responding to intrusions in mobile ad hoc networks," World Congress on Internet Security(WorldCIS-2013), 2013, pp. 30–34.

[11] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto, "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method," International Journal of Network Security, Vol.5, No.3, 2007, pp. 338–346.

[12] Latha Tamilselvan, V. Sankaranarayanan, "Prevention of Co-operative Black Hole Attack in MANET," International Journal of Networks, Vol. 3, No. 5, 2008, pp. 13-20.

■ 저자소개 ■

양 환 석
(Yang Hwanseok)

2011년 9월~현재
중부대학교 정보보호학과 조교수
2006년 2월~2011년 2월
호원대학교 사이버수사경찰학과 연구교수
2005년 2월 조선대학교 전산통계학과(이학박사)
1998년 2월 조선대학교 전산통계학과(이학석사)

관심분야 : 정보보호, 침입탐지시스템, MANET
E-mail : yanghs@joongbu.ac.kr

논문접수일 : 2018년 02월 20일
수 정 일 : 2018년 03월 07일
게재확정일 : 2018년 03월 12일