情報保護學會論文誌
第 22 卷 第 1 號, 2012. 2

MANET에서 안정된 침입탐지에 관한 연구

양 환 석,† 양 정 모‡
중부대학교

A Study of Stable Intrusion Detection for MANET

Hwan-Seok Yang† , Jeong-Mo Yang‡
Joongbu University

요 약

이동 노드로만 구성된 MANET은 유비쿼터스 컴퓨팅 환경을 구축하기 위한 핵심 기술로 많은 관심을 받고 있다. 또한 중앙 기반 시설이 없기 때문에 보안에 더욱 취약하다. 따라서 악의적인 공격을 탐지해 낼 수 있는 침입탐지 시스템이 반드시 필요하다. 본 논문에서는 안정된 침입탐지를 위해 클러스터를 이용하였으며, 네트워크 문제인 것처럼 보이는 공격도 정확히 탐지할 수 있도록 다양한 공격에 대해 규칙을 정의하였다. 실험을 통해 본 논문에서 제안한 기법이 노드의 수가 증가하더라도 안정된 탐지율을 보이는 것을 확인하였다.

ABSTRACT

MANET composed of only moving nodes is concerned to core technology to construct ubiquitous computing environment. Also, it is a lack of security because of no middle infrastructure. So, it is necessary to intrusion detection system which can track malicious attack. In this study, cluster was used to stable intrusion detection, and rule about various attacks was defined to detect accurately attack that seems like network problem. Proposed method through experience was confirmed that stable detection rate was showed although number of nodes increase.

Keywords: MANET, Indrusion Detection System(IDS)

I. 서 론

MANET(Mobile Ad-hoc Network)은 이동 노드로만 구성된 네트워크로서 최근 유비쿼터스 컴퓨팅 환경을 구축하기 위한 핵심 기술로 많은 관심을 받고 있다. MANET은 네트워크를 구성하는 모든 노드들의 이동성으로 네트워크 위상이 수시로 변하며 중앙 관리체계가 없기 때문에 보안에 취약하다. 게다가 네트워크를 구성하는 모든 노드들이 라우터 기능을 수행해야 하므로 보안에 취약점을 갖고 있다[1].

MANET에서의 보안은 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[2]. 특히 유선환경에서는 라우터와 같은 패킷의 흐름이 집중되는 곳이 존재하기 때문에 그 위치에 침입탐지 시스템을 설치하지만 MANET은 이동 노드로만 구성되어 있기 때문에 침입탐지 시스템을 설치할 위치를 찾는 것이 매우 어려운 일이다[3]. 그리고 지역적 정보의 수집만으로 공격을 판단하는 일은 쉽지 않기 때문에 침입탐지에 관한 정보 교환과 상호 협력에 의

접수일(2011년 10월 5일), 게재확정일(2011년 12월 1일)
† 주저자, yanghs@joongbu.ac.kr
‡ 교신저자, jmyang@joongbu.ac.kr

해 공격을 판단하는 일은 반드시 필요하다.

본 논문에서는 MANET을 구성하는 노드들을 계층형 구조인 클러스터로 형성하였다. 그리고 클러스터를 관리하는 클러스터 헤드가 IDS의 역할을 수행한다. 그리고 네트워크 내의 모든 노드들은 자신이 패킷을 전송할 때, IDS에게 패킷 전송 정보를 송신한다. 이 정보를 기초로 하여 IDS는 침입탐지를 수행하게 된다.

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

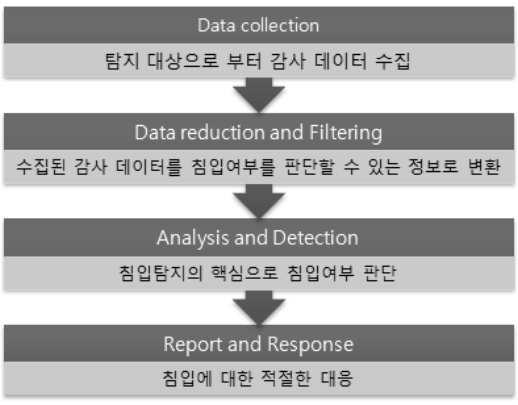
II. 관련연구

2.1 침입탐지 기법의 분류

침입탐지시스템은 목표 시스템에 대한 침입을 시도하거나, 비정상행위를 탐지하여 즉각적으로 적절한 대응을 할 수 있는 시스템을 말한다. 침입탐지시스템은 데이터 수집, 데이터의 가공, 침입 탐지 그리고 보고 단계로 이루어져 있다.

이러한 침입탐지시스템은 탐지 방식에 따라 오용 탐지(Misuse Detection)와 비정상행위(Anomaly Detection)로 분류할 수 있다[4]. [표 1]은 탐지 방식에 따른 기법들을 보여주고 있다.

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



[그림 1] 침입탐지 단계

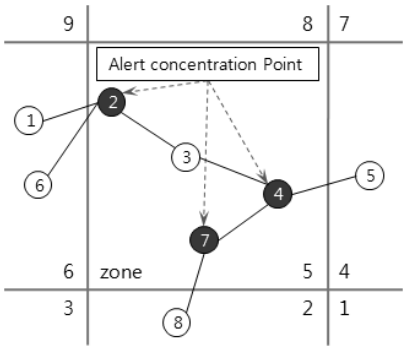
[표 1] 침입탐지 기법의 종류

분류	기법	방법
오용 탐지	조건부 확률	확률을 공식에 의해 계산 후 탐지.
	전문가 시스템	침입행위를 발견시 IF - THEN 규칙에 따라 처리함.
	상태전이분석	침입을 특정 시스템의 상태 전이의 순서로 표현하여 탐지.
	패턴 매칭	침입 시나리오로 설정된 패턴들과 비교하여 탐지.
비정상 행위	통계적 접근	행위에 대한 프로파일 생성 후 통계적 이상 여부에 따라 처리.
	특징 추출	침입의 패턴을 추출하여 침입을 예측하고 분류하는 기법
	신경망	명령을 학습시킨 후 다음실행 명령을 예측하는 기법

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[6].

2.2 영역 기반 침입탐지 기법

ZBIDS는 네트워크가 중복되지 않는 지역(zone)으로 분할하여 브로드캐스트에 의한 오버헤드를 줄이고, 침입탐지 효율을 높이기 위해 지역의 경계 지점에 위치한 게이트웨이 노드들이 지역 내에서 브로드캐스트된 정보를 통합하여 최종적인 침입탐지 정보를 생성하는 접근 방식을 가지고 있다[7]. 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



〔그림 2〕 ZBIDS 구조

감소시키고 침입탐지 시스템의 성능향상을 위한 침입탐지 정보 통합 알고리즘을 이용하였다는 점이다. 〔그림 2〕는 ZBIDS의 구조를 보여주고 있다.

III. 제안한 방법

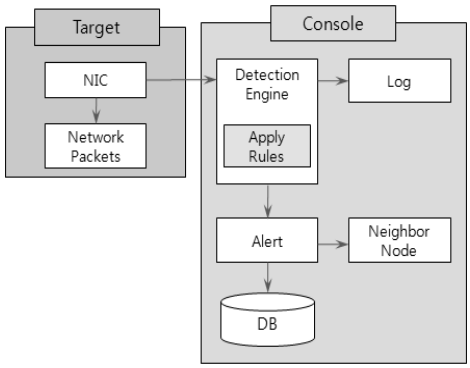
3.1 노드의 초기화 및 클러스터 구성

MANET의 안정된 침입탐지를 위하여 먼저 네트워크에 존재하는 노드들을 계층구조인 클러스터로 구성하였다. 그리고 클러스터를 관리하는 클러스터 헤드를 선출하기 위해 각 노드들은 자신의 링크 수와 신뢰도 값을 방송한다. 이 두 개의 값을 조합하여 클러스터 헤드를 선출한다. 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 있다. 이렇게 선출된 클러스터 헤드는 IDS의 역할을 수행하게 된다.

3.2 침입탐지 과정

본 논문에서 제안한 침입탐지 알고리즘의 침입탐지 과정은 〔그림 3〕에서 보여주고 있다.

클러스터를 관리하는 클러스터 헤드가 IDS 역할을 수행한다. 〔그림 3〕에서 보듯이 IDS는 이웃 노드로부터 자신들이 전송한 패킷의 전송 정보를 수신한다. 이렇게 수신한 패킷의 정보를 감시하다가 의심스러운 정보가 발견되면 이 정보를 저장한다. IDS의 제한된 자원을 고려하여 저장된 정보는 일정 시간이 지나면 삭제되도록 하였다. 이렇게 수집된 패킷에 이미 정의되



〔그림 3〕 침입탐지 과정

어 있는 규칙을 적용한다. 이 과정에서 공격자의 의도에 의해 마치 네트워크 문제인 것처럼 보이는 공격들도 정확하게 탐지해 낼 수 있도록 IDS에 침입탐지 규칙을 정의 하였다. 만약 수집한 패킷에 침입이 탐지되었다면 IDS는 주변의 이웃 노드들에게 이 정보를 방송하고 공격에 대한 정보를 데이터베이스에 저장하게 한다. 이렇게 함으로써 다양한 공격을 보다 안정되게 탐지해 낼 수 있게 된다. 하지만 수집한 패킷의 정보가 어떤 유형의 공격 규칙과도 일치하지 않는다면 실패 카운터 값을 증가시키고 패킷 정보를 삭제한다. 불필요한 데이터 삭제는 무선 노드들의 자원 소모, 규칙 검색, 공격 탐지 시간을 줄일 수 있다. 〔그림 4〕는 침입탐지를 위한 pseudo 코드를 보여주고 있다. IDS의 이웃 노드로 부터 수신한 정보를 분석하여 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 조합하여 기대 값을 갱신한 후 IDS가 값을 저장한다.

```
att_Detect(netFail, expFail)
{
   while(all neighbor)
   {
      if(netFail > expFail) then
         alert attack;
      else
         update expFail value by combining
         it with netFail value;
   }
}
```

〔그림 4〕 침입탐지 pseudo code

3.3 침입탐지 규칙

IDS 역할을 수행하는 클러스터 헤드는 수집된 패킷에서 침입을 탐지하기 위해 정의된 규칙과 비교한다. 본 논문에서 침입탐지를 위해 사용한 규칙들에 대해 정의한 것이다. 첫 번째로 선택적 포워딩과 블랙홀 공격을 탐지해 낼 수 있는 retransmission 규칙이다. 이 규칙은 자신이 수신한 패킷을 이웃 노드들에게 전달하는지 감시한다. 두 번째로 delay 규칙은 이웃 노드들에게서 수신한 패킷을 정의된 시간 안에 전송해야 한다. 그렇지 않으면 공격으로 검출된다. 세 번째로 jamming 규칙은 송신 패킷의 충돌 횟수를 감시한다. 만약 충돌 횟수가 네트워크 내의 기대 값보다 적어야 한다. 네트워크 안에 잡음을 만들고 통신 채널을 왜곡시킬 수 있는 jamming 공격은 이 규칙에 의해 검출될 수 있다. 네 번째로 integrity 규칙은 수신된 메시지의 내용을 수정하는 공격을 검출하기 위한 것이다. 다섯 번째로 Interval 규칙은 패킷의 전송 시간이 제한된 시간보다 짧거나 긴 경우 실패가 발생한다. 이웃 노드에 의해 생성된 패킷을 송신하지 않는 공격과 반대로 이웃 노드들의 에너지 소모량을 증가시킬 목적으로 메시지 송신 비율을 증가시키는 공격을 이 규칙에 의해 탐지할 수 있다. 마지막으로 repetition 규칙은 같은 패킷을 똑같은 이웃에게 제한된 횟수만큼 재전송할 수 있다는 것이다. 이 규칙은 공격자가 어디서 똑같은 패킷을 얼마나 송신했는지 검출할 수 있기 때문에 서비스거부 공격에 대응할 수 있다.

IV. 실험 및 결과

4.1 실험 환경

본 논문에서 제안한 침입탐지 기법의 성능 분석을 위해 ZBIDS 기법과 비교 실험 하였다. 실험에 사용한 노드는 사용자가 자유롭게 움직일 수 있다는 개방된 환경 하에서 이동한다고 가정하였고, 정지 시간은 30초로 하였다. 패킷의 크기는 64 바이트, 데이터 전송 범위는 150m로 하였다. 실험에 사용한 노드의 수는 10~100개이고 각 실험 시간은 600초로 하였으며 10번 반복 실험하였다. 그리고 〔표 2〕는 실험에 사용한 변수 값이다.

〔표 2〕 실험에 사용한 환경 변수

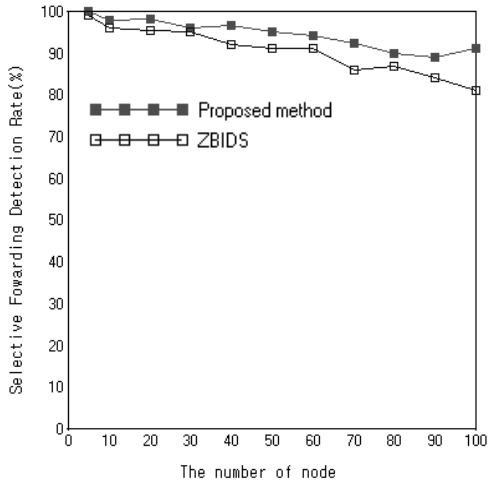
라우팅 프로토콜	AODV
MAC 프로토콜	IEEE 802.11 DCF
이동 모델	Random waypoint model
네트워크 크기	1000 × 1000
이동 속도	0~10m/s

4.2 실험 결과

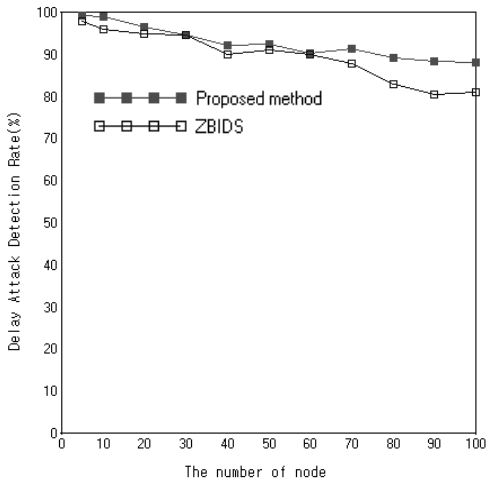
본 논문에서 제안한 침입탐지의 효율성을 평가하기 위하여 선택적 포워딩, 지연 공격, 클러스터 헤드의 메모리 사용량 측정을 평가 기준으로 하였다. 그리고 FNR(False Negative Ratio), FPR(Flase Positive Ratio)를 측정하여 제안한 침입탐지시스템의 안정성을 확인 하였다. 각 공격은 임의로 발생시켰으며 실험 시간 동안 50번 발생시켰다. 실험에서 클러스터 헤드는 수집된 데이터를 정의된 규칙에 적용하여 침입탐지 및 공격의 유형을 탐지하게 된다.

〔그림 5〕에서 보여주는 선택적 포워딩 공격은 클러스터 헤드에 의해서 이웃 노드의 행동을 파악하고 있기 때문에 높은 탐지율을 보여주고 있다. 그러나 네트워크에 노드의 수가 많아지고 이동 속도가 빨라질수록 전송 지연 시간이 발생함에 따라 탐지율이 떨어졌다. ZBIDS도 마찬가지로 노드들의 수가 많아짐에 따라 탐지율이 떨어지는 것을 확인할 수 있었다. 클러스터 헤드가 주변의 이웃 노드의 행동을 파악하고 있기 때문에 선택적 포워딩 공격의 탐지율도 노드의 수에 크게 영향을 받지 않고 안정되게 탐지 하였다.

지연 공격은 자신이 수신한 패킷을 정의된 시간 안에 이웃 노드에게 전송해야만 한다. 만약 그렇지 않다



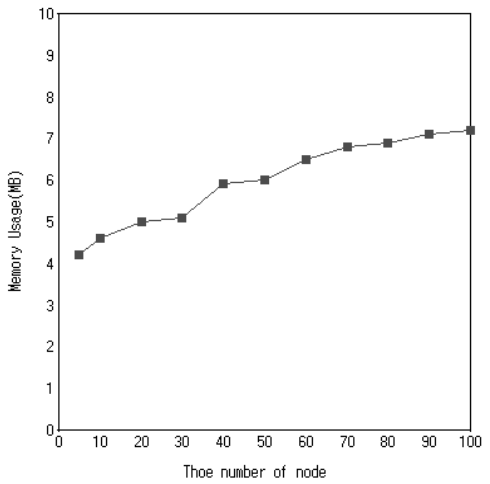
〔그림 5〕 선택적 포워딩 공격 탐지율



〔그림 7〕 지연 공격 탐지율

면 이를 공격으로 간주한다. 〔그림 6〕에서 보듯이 제안한 침입탐지시스템이 ZBIDS에 비해 좋은 결과를 보였다. 〔그림 6〕에서 나타나듯이 노드의 수가 많아지고 이동이 증가할수록 제어 패킷의 양의 증가로 네트워크의 성능이 다소 떨어짐으로써 자연스러운 지연 현상으로 공격으로 잘못 탐지하는 비율이 다소 높아졌다.

제안한 침입탐지 기법은 클러스터 헤드가 이웃 노드들로부터 의심스러운 패킷에 대한 정보 수집 후 패턴을 검색한다. 노드 수의 증가에 따른 클러스터 헤드의 자원 고갈이 발생하게 된다면 침입탐지는 불가능하게 된다. 따라서 게이트웨이 노드들에 의해 정보를 수집



〔그림 7〕 클러스터 헤드 메모리 사용율

〔표 3〕 FNR과 FPR 측정

	Value(%)
FNR	3.7%
FPR	4.9%

하는 ZBIDS와는 비교 실험하지 않았으며, 제안한 기법에서 정보를 수집하는 클러스터 헤드의 메모리 사용량을 측정하였다. 〔그림 7〕에서 노드의 수가 많아질수록 자연스럽게 메모리의 사용량도 증가하긴 했지만 평균 5.5M 정도임을 확인할 수 있었다. 〔표 3〕은 실험을 통해 측정한 FNR과 FPR을 보여주고 있다. 본 논문에서 제안한 침입탐지시스템이 안정된 공격 탐지가 이루어지는 것을 보여주고 있다.

V. 결 론

본 논문에서는 네트워크 문제인 것처럼 보이는 공격을 정확히 탐지해내고 노드들의 이동에도 침입탐지를 안정되게 수행할 수 있는 침입탐지 시스템을 제안하였다. 네트워크를 구성하는 노드를 클러스터로 구성한 후 선출된 클러스터 헤드가 IDS 역할을 수행 하였다. 그리고 악의적인 의도의 공격에도 안정된 탐지를 하기위해 다양한 공격에 대해 규칙을 정의하였다. 네트워크에 노드들의 수가 증가하고 이동 속도가 증가하더라도 안정된 탐지율을 보이는 것을 실험에서 확인할 수 있었다. 그리고 클러스터 헤드의 메모리 사용량도 노드의 수가 증가하여도 크게 증가하지 않음을 확인할 수 있었다.

참고문헌

〔1〕 S. Corson and J. Macker, "Mobile ad hoc networking(MANET):routing protocol performance issues and evaluation considerations," IETF RFC2501, January 1999.

〔2〕 Y. Li and J. Wei, " Guidelines on Selecting Intrusion Detection Mothod in MANET," Proceedings of ISECON 2004, v 21 (NETWORK), pp. 1-17 , November 2004.

〔3〕 D. Sterne, P. Balasubramanyam, D. Carman, B. Wilson, R. Talpade, C. Ko, R. Balupari, C-Y. Tseng, T. Bowen, K.

Levitt and J. Rowe, "A General Cooperative Intrusion Detection Architecture for MANETs," Proceedings of the third IEEE International Workshop on Information Assurance, IWIA'05, pp. 57-70, March 2005.

〔4〕 H. Debar, M. Dacier, and A. Wespi, "A Revised Taxonomy for Intrusion Detection Systems," Annales des Telecommunications, Vol. 55, No.7-8, pp. 361-378, August 2000.

〔5〕 W. Stallings, Cryptography and Network Security - Principles and Practices, 3rd edition , Person Education, Aug. 2003.

〔6〕 A. Mishra, K. Nadkarni, amd A. Patcha, "Intrusion Detection in Wireless Ad Hoc Networks," IEEE Wireless Communications, Vol. 11, No.1, pp. 48-60, February 2004.

〔7〕 B. Sun, K.Wu, and U. W. Pooch. "Alert Aggregation in Mobile Ad Hoc Networks". The 2003 ACM Workshop on Wireless Security in conjuction with the 9th Annual International Conference on Mobile Computing and Networking (MobiCom'03), pp. 69-78, September 2003.

〈著者紹介〉

양 환 석 (Hwan-Seok Yang) 정회원
1996년 2월: 호원대학교 전자계산학과 이학사
1998년 2월: 조선대학교 대학원 전산통계학과 이학석사
2005년 2월: 조선대학교 대학원 전산통계학과 이학박사
2011년 9월~현재: 중부대학교 정보보호학과 전임강사
〈관심분야〉 정보보호, 침입탐지시스템, MANET

양 정 모 (Jeong-Mo Yang) 종신회원
1984년 2월: 동국대학교 사범대학 수학과 이학사
1989년 2월: 동국대학교 대학원 수학과 이학석사
1997년 2월: 단국대학교 대학원 수학과 이학박사
1997년 3월~현재: 중부대학교 정보보호학과 교수
〈관심분야〉 정보보호, 암호학, 암호수학