韓國 컴퓨터情報學會 論文誌
第13卷 第2號, 2008. 3.

2008-13-2-3-3

무선랜을 위한 효율적인 침입탐지시스템 설계

우 성 희*

Design of Effective Intrusion Detection System for Wireless Local Area Network

Sung-Hee Woo *

요 약

무선랜은 물리적으로 근접한 거리의 공격자나 장비에 의해 공격이 행해질 수 있으며, STA와 AP상의 라디오링크에 접근하는 공격자가 부가적인 메시지를 투입시킴으로서 정보를 수정할 수 있기 때문에 유선랜과 비교해 볼 때, 같은 공격 유형에서도 그 위험이 끼치는 영향의 파급 정도는 더 클 수 있다. 따라서 무선랜의 인프라구조 내에 있다는 것만으로 충분히 공격이 가능해지는 무선랜의 취약점을 보완하기 위해서 효과적인 침입탐지시스템의 도입이 요구된다. 기존의 무선랜에서의 침입탐지기법들은 유선에서 활용되던 SVM을 이용한 방법론 등이 활용될 수 있으나, 이는 대용량의 무선 데이터셋의 이산형, 연속형 데이터 중에서, 중요한 침입여부 단서가 될 수 있는 연속형데이터는 활용할 수 없다는 단점을 가진다. 따라서 이 논문에서는 SVM과 데이터마이닝 기법을 혼합하여 무선랜을 위한 침입탐지시스템을 설계하고 이에 대한 실험결과를 통해 우수성을 입증하고자 한다.

Abstract

Most threats of WLAN are easily caused by attackers who access to the radio link between STA and AP, which involves some problems to intercept network communications or inject additional messages into them. In comparison with wired LAN, severity of wireless LAN against threats is bigger than the other networks. To make up for the vulnerability of wireless LAN, it needs to use the Intrusion Detection System using a powerful intrusion detection method as SVM. However, due to classification based on calculating values after having expressed input data in vector space by SVM, continuous data type can not be used as any input data. In this paper, therefore, we design the IDS system for WLAN by tuning with SVM and data-mining mechanism to defend the vulnerability on certain WLAN and then we demonstrate the superiority of our method.

▸ Keyword : Wireless LAN, IDS, IPS, IDPS

• 제1저자 : 우성희
• 접수일 : 2008. 2. 25, 심사일 : 2008. 3. 2, 심사완료일 : 2008. 3. 8.
* 충주대학교 전기전자 및 정보공학부 교수
※이 논문은 충주대학교 대학구조개혁지원사업비(교육인적자원부 지원)의 지원을 받아 수행한 연구임

Ⅰ. 서 론

무선랜(Local Area Network, LAN)은 일반적으로 사무실 빌딩이나 회사 캠퍼스와 같은 공평하게 제한된 구역 내에 장비들에 의해 사용되고 향상된 사용자 이동성을 제공하기 위해서 존재하는 유선 네트워크에 대한 확장으로 주로 활용된다[1]. 무선랜의 장비들은 전파 통신을 통해 데이터 교환이 가능하도록 제한된 지리적 범위 내의 무선 네트워크 노드들의 그룹으로 이루어지므로 유선 네트워크와 같이 물리적으로 접근을 제한하기가 상당히 어렵다. 따라서 보안 수준을 높은 단계로 끌어올리기 위해서는 물리적인 보안과 함께 침입을 탐지하기 위한 시스템의 도입이 필요하다. 무선랜용 침입탐지시스템을 위한 기술들은 유선랜에 방법론을 활용하고 있으며, 무선 데이터의 전처리 후에 룰에 기반한 필터링 또는 컨텐츠와 시그너처 등에 기반한 분류 등을 활용한다. 특히, 이진 분류 능력이 뛰어난 SVM(Support Vector Machines)을 이용한 방법 등이 효율적인 방법으로 행해지고 있으나, SVM은 입력 값을 벡터 공간에 나타낸 후 계산된 값을 근거로 분류를 수행하므로 벡터 값으로 표현이 불가능한 연속형데이터는 취급할 수 없다. 이 논문에서는 기존의 방법에 비해 효율적인 탐지율을 가지는 침입탐지시스템을 설계하였다. 제안한 침입탐지시스템은 AP를 거치는 무선 데이터를 센서를 통해 측정하고, 이 데이터를 이산형과 연속형으로 구분한 후 SVM과 데이터마이닝 기법을 혼합시켜 설계하였다. 논문의 구성은 다음과 같다. 2장에서는 관련연구를 다루고, 3장에서는 무선랜에서 필요한 보안요구사항을 기술한다. 4장에서는 이 논문에서 제안하는 SVM과 데이터마이닝 기법을 혼합하여 무선랜을 위한 침입탐지시스템을 기술하고 5장은 제안된 시스템에 대한 실험결과를 통해 우수성을 입증하고자 한다. 6장에서는 결론 및 향후 연구 방향을 제시한다.

Ⅱ. 관련연구

무선 랜의 경우 유선 네트워크와 같이 물리적 제한을 통해 침입을 탐지하고 방지하기가 상당히 어렵다. 일반적으로 War Drivers, 가짜 AP에 의한 공격, DoS 공격, MAC 주소 위조 공격 등이 있을 수 있다. 그 밖에도 무선랜에 대한 특수한 공격 방법으로는 멍키 잭(Monkey Jack)이나 키스메트(KISMET), 웰른라이터(wellenreiter), 보이드(Void) 11, 에어잭(AirJack), 호스트 AP(Host AP), ASLEAP, Ttcp Wifi, Associate Flood, AuthFlood, De-auth Flood FakeAp Flood 등이 공격방법이라고 할 수 있다[2][3].

무선랜에 침입탐지를 하기 위해서는 일반적으로 무선랜용 침입탐지시스템을 설치하거나, 또는 AP의 설치위치를 조정하는 방법 등을 활용할 수 있다.

무선랜용 침입탐지시스템은 그림 1과 같이 AP 혹은 이에 준하는 무선 RF 센서들을 설치해 실시간으로 무선 환경과 허가받지 않은 사용자나 AP를 탐지하고 무선랜을 통한 공격 시도를 탐지하는 시스템이다. 이러한 시스템은 일반적으로 센서부와 관제부로 나뉘어 지며 센서부의 탐지 결과를 관제부에서 넘겨받아 분석해 관리자에게 필요한 정보를 줄 수 있도록 되어 있다. 무선랜 침입탐지시스템의 경우 가능하면 인증 서버와 연동해 실시간으로 허가된 사용자와 허가된 AP, 그리고 사용자별 접근 제어 정책까지 연동되면 강력한 성능을 발휘할 수 있다. 또한 무선랜을 이용한 공격 시 공격자의 위치 추적은 사실상 어려웠으나 촘촘하게 설치된 센서를 이용하면 어느 정도의 오차 범위 내에서 위치 추적도 가능하므로 이러한 기능을 이용해 보는 것도 보안 레벨을 높이는 방법 중 하나다.

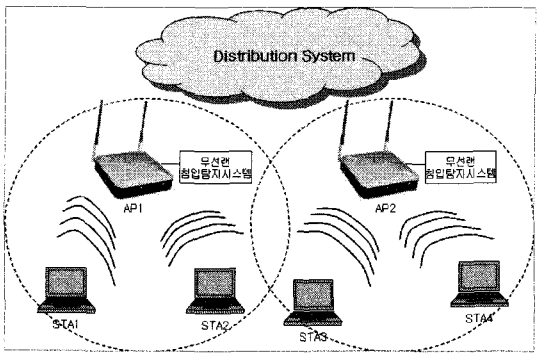

그림 1. 무선랜 컴포넌트
Fig 1. Wirelss LAN component

반면, AP의 설치 위치 조정을 통해 물리적 접근을 제어할 수 있다. 일반적으로 AP의 경우 높은 위치에 설치되는 경우가 대부분이다. AP의 위치가 공격자가 물리적으로 접근할 수 있는 위치에 있다면 공격자가 AP를 직접적으로 공격할 수도 있다. 또한 분실 등의 위험도 있으므로 AP의 설치 위치는 무선 전파 구간의 음영 지역의 최소화를 위한 셀의 설계와 더불어 물리적인 접근이 쉽지 않도록 설치하는 방법도 고려해야 한다. 만약 공격자가 AP를 제거하고 AP에 연결돼 있던 이더넷을 PC로 바로 연결하게 되면 내부 네트워크는 직접적으로 공격을 받을 수도 있다. 따라서 AP의 설치 위치나 설치 방법

등은 가능한 한 접근이 어렵도록 해야 한다.

III. 무선랜을 위한 보안요구사항

무선랜에서 침입탐지 및 기능을 추가하기 위해서는 여러 가지 보안 기능들을 제공해야 한다. 여기서는 보안 기능의 유형을 정보 수집, 로깅, 탐지, 방지 등으로 나누어 기술한다.

3.1 정보 수집 기능

무선 LAN에서의 공격 유형을 알기 위해서는 무선 장치 상의 정보를 수집해야 한다. 수집하는 정보의 예는 다음과 같다.

- 무선 LAN에 포함된 장치 식별 정보
- 무선 LAN의 SSID 식별 정보

3.2 로깅 기능

일반적으로 감지된 이벤트와 관련하여 데이터의 광범위한 로깅을 수행해야 한다. 무선 LAN을 위한 탐지 및 방지에 의해 일반적으로 로그화된 데이터 필드는 다음을 포함한다.

- 타임스탬프(보통 날짜와 시간)
- 이벤트나 경고 유형
- 우선순위 및 심각도 등급
- 출발지 MAC 주소
- 채널 번호
- 이벤트를 관찰했던 센서의 ID
- 수행된 방지 행동

3.3 탐지 기능

일반적으로 공격 및 잘못 구성된 환경 설정, 무선 LAN 프로토콜 레벨에 대한 정책 위반, 주로 검사하는 IEEE 802.11a,b,g와 프로토콜 통신 등을 탐지할 수 있다. 다음은 탐지해야 하는 기능들이다.

- 탐지된 이벤트의 유형
- 탐지 정확성
- 튜닝 및 고객화
- 기술 제약사항

3.4 방지 기능

무선 LAN에서 침입을 방지하기 위해서는 다음의 두 가지 기능들을 제공한다.

- 무선: 어떤 센서들은 잘못 환경 설정된 STA와 인증된 AP 사이, 공중에서 또는 인증된 STA와 잘못 구성된 AP 사이에 연결을 종결함으로 방지할 수 있다.
- 유선: 어떤 센서들은 특수한 STA나 장치의 MAC 주소를 기반하는 AP 혹은 스위치 포트를 포함하는 네트워크 행위를 막기 위해서 유선 네트워크 상에 하나의 스위치에게 지시할 수 있다.

중요한 고려사항으로는 방지 기능을 수행할 때 모니터링하는 센서들이 갖는 효과들이다. 예를 들어, 만약 하나의 센서가 연결을 종결하는 시그널을 보낸다면 이는 방지행위가 완료되기 전까지 다른 통신들을 모니터링하도록 채널 스캐닝을 수행할 수 없도록 하기도 한다. 이러한 점을 완화시키기 위해 센서들은 2개의 라디오(radio)를 가지는데, 하나는 모니터링과 탐지를 위한 것이고 다른 하나는 방지 행동을 수행하기 위한 것이다. 센서를 선택할 때, 조직은 무슨 방지 행동이 수행될 필요가 있는지 어떻게 그 센서의 탐지 능력들이 방지 행동을 수행하는지 영향을 끼칠 수 있는지를 고려해야 한다.

IV. 무선랜을 위한 침입탐지시스템 제안

무선랜을 위한 침입탐지시스템을 제안하기 위해서 전체 시스템의 개요를 명시하고, 각 모듈별 기능과 알고리즘을 명세한다.

4.1 전체 시스템 개요

이 논문에서 제안하는 무선랜을 위한 침입탐지모델의 프레임워크는 그림 2와 같다. 무선랜을 위한 침입탐지를 위해서는 보안 기능을 위한 컴포넌트들이 요구된다. 여기서는 데이터 수집을 위한 센서를 AP에 번들시켜 위치시키고, Audit 정보를 보관하는 Audit DB, 그 DB의 정보를 받아 데이터마이닝 기법에 의해 데이터에 대한 분석을 실시할 관리 서버 등을 이용하도록 한다. 번들된 AP는 네트워크 엑세스를 제공하는 것과 다중의 채널이나 고의적인 행위를 위한 밴드(band)를 모니터링하는 사이의 시간을 나누는 것이 요구된다. 만일 오직 단일의 밴드와 채널을 모니터링하는 것이 필요하다면 번들된 솔루션은 적절한 보안과 네트워크 가용성을 제공할지도 모른다. 또한 무선랜을 위한 다른 보안 컴포넌트들은 트래픽을 샘플링하면서 모니터링하는 네트워크에서의 모든 패킷들을 볼 수 있도록 한다. 두 가지 모니터링 주파수 대역으로

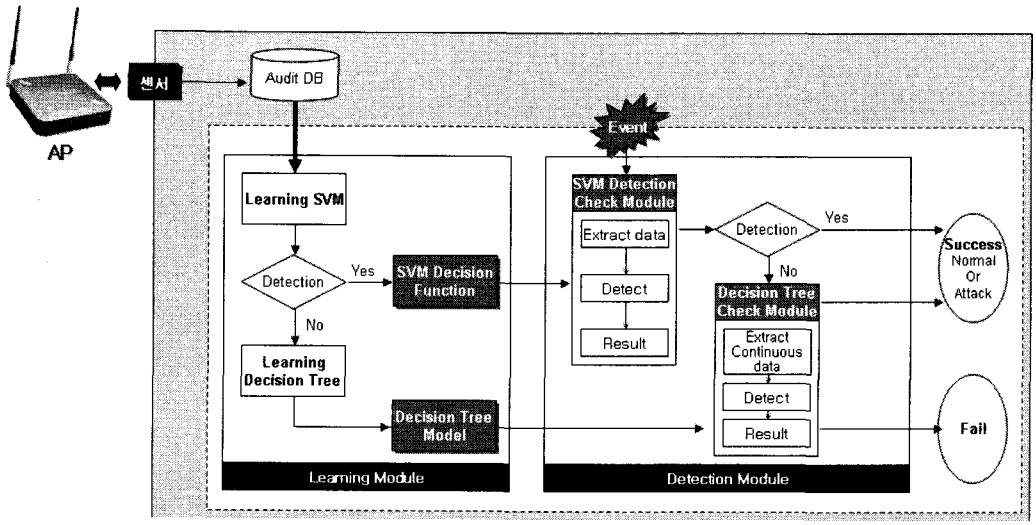

그림 2. 무선랜을 위한 침입탐지시스템
Fig 2. Intrusion Detection System for Wirless LAN

2.4GHz와 5GHz을 들 수 있으며, 각 대역폭은 채널로 나뉘어진다. 하나의 센서로 대역폭의 모든 트래픽을 동시적으로 모니터링 하는 것은 현재로써는 불가능하며 그 센서가 다른 채널을 모니터링하려고 준비할 때, 그 센서는 그것의 전파를 끄고, 채널을 바꾼 후에, 전파를 켜야 한다. 하나의 채널이 더 길게 모니터링 할수록 그 센서는 다른 채널 상에서 발생하는 고의적인 행위를 더 놓칠 수도 있다. 이러한 문제점을 피하기 위해 센서들은 채널을 빈번하게 바꾸는 채널 스캐닝(channel scanning)을 1초에 여러번 각 채널들을 모니터함으로써 할 수 있다. 채널 스캐닝을 줄이고 없애기 위해서, 특수화된 센서가 각 서로 다른 채널들을 모니터링하고 있는 각 전파 및 안테나 쌍들을 가지고 여러 개의 전파와 높은 파워 안테나를 사용하는 것이 가능하다. 어떤 경우는, 각 센서가 더 많은 채널을 모니터링하게 하기 위해서 오버래핑(overlapping)하는 범위를 가지고 센서들 간의 스캐닝 패턴을 도울 수 있다.

4.2 모듈별 기능

제안모델의 프레임워크는 크게 탐지모듈과 학습모듈로 나누어진다. 학습모듈에서는 침입감사데이터를 이용하여 SVM과 의사결정트리 학습이 이루어지고 탐지 모듈에서는 학습 모듈의 학습 결과를 바탕으로 침입 탐지를 수행한다[5][6][7]. SVM의 특성상 이산형 데이터는 SVM에 적용할 수 없고, 적용한다 하더라도 학습 결과에는 영향을 미치지 않기 때문이다. 연속형 데이터와 이산형 데이터는 다음과 같이 구분된다[8][9].

- 연속형 데이터: 가능한 측정 결과를 셀 수 없는 경우
- 이산형 데이터: 측정 결과를 셀 수 있는 경우

SVM을 이용한 침입 탐지 실험에 이용하지 못한 이산형 데이터들도 침입 탐지 결과에 충분히 영향을 미칠 수 있으므로 이들을 실험에서 배제하여서는 안 된다. 이산형 데이터 중, 다음 항목들은 침입 탐지 판정에 유용한 정보를 제공한다.

- 타임스탬프(보통 날짜와 시간)
- 이벤트나 경고 유형
- 우선순위 및 심각도 등급
- 출발지 MAC 주소
- 채널 번호 , 이벤트를 관찰했던 센서의 ID

또한 연속형 데이터는 다음과 같다.

- 무선 LAN에 포함된 장치 식별 정보
- 무선 LAN의 SSID 식별하는 연속형 정보
- 수행된 방지 행동

따라서 SVM을 이용한 침입 탐지 실험에서 미처 탐지하지 못한 연결들은 그들의 이산형 데이터를 추출, 의사결정트리 방법을 적용하여 재 탐지 하는 방안을 제안한다. 제안 모델은 크게 학습 모듈과 탐지 모듈로 구성되어 있다. 학습 모듈은 침입 감사 데이터를 SVM과 의사결정트리에 적용시켜 학습 모델과 결정함수를 생성한다. 탐지 모듈은 IDS로부터 수집된

이벤트들을 SVM 결정함수와 의사결정트리 모델로 탐지 실험을 하여 침입을 판정한다.

4.3 학습 모듈

4.3.1 SVM 학습 모듈

SVM 학습은 침입과 정상을 구분할 수 있는 서포터 벡터와 가중치 벡터 값으로 이루어지는 결정함수를 구하는 과정이다. 학습과정을 통해 입력 벡터 값에 따라 고차원 공간에 침입과 정상을 구분할 수 있는 최대 마진을 가지는 결정면을 가진다.

① 침입 감사 데이터 셋으로 부터 학습을 위한 데이터 셋 추출
② 추출된 데이터 셋을 SVM 머신의 입력 포맷에 맞게 변환
③ 커널을 사용하여 SVM학습
④ 학습 후 결정함수 생성

4.3.2 의사결정 트리 학습 모듈

의사결정트리는 많은 컴퓨팅 작업 없이 분류과정을 형성하며 이산형 변수와 연속형 변수에 모두 사용할 수 있다. 때문에 SVM 학습 결과 탐지하지 못한 데이터의 이산형 데이터 부분만을 추출하여 의사결정트리 방법을 적용한다. 의사결정트리의 학습 과정은 다음과 같다.

① SVM 탐지 결과를 바탕으로 학습을 위한 데이터 셋 추출
② 추출된 데이터 셋을 의사결정 트리 알고리즘을 사용하여 학습
③ 학습 후 의사결정트리 모델 생성

4.4 탐지 모듈

4.4.1 SVM 탐지 모듈

SVM 탐지 모듈은 SVM 학습을 통해 생성된 결정함수에 침입 감사 데이터를 적용하여 침입 여부를 판정하는 모듈로 탐지 과정은 다음과 같다.

① 실험 데이터 셋을 SVM 입력 포맷에 맞게 변환
② 실험 데이터 셋을 SVM 학습으로 얻은 결정함수에 적용
③ 침입인지 정상인지 판정

4.4.2 의사결정트리 탐지 모듈

의사결정트리 탐지 모듈은 의사결정트리 학습을 통해 생성된 모델에 SVM 탐지 모듈에서 탐지하지 못한 데이터만을 적용하여 침입을 판정하는 모듈로 탐지 과정은 다음과 같다.

① SVM 탐지 모듈에서 미탐지된 데이터 셋을 추출
② 추출된 데이터 셋을 의사결정트리 학습으로 얻은 의사결정트리 모델에 적용
③ 침입인지 정상인지 판정하며, 다음의 정보를 추가하여 관리자가 보고
■ 탐지된 이벤트의 유형
■ 탐지 정확성
■ 기술 제약사항

V. 실험 및 평가

5.1 실험 환경

제안모델은 SVMChen2.0과 Clementine7.0을 이용하여 실험되었으며 실험에 사용한 침입 감사 데이터는 무선 트래픽을 이용한 데이터셋으로 표 1과 같이 구성하였으며, 각각의 연결기록은 40개의 독립적인 속성과 공격 유형 레이블로 이루어져 있다.

표 1. 무선 데이터 셋의 구성
Table 1. Wireless Data Set

항 목		개 수
총 데이터 수		320,000
총 속성의 수	이산형	7
	연속형	33
	공격 유형 레이블	1
	합계	41
공격유형 클래스		4
총 공격 유형		38

침입탐지시스템은 탐지대상으로부터 생성되는 시스템 사용 내역, 컴퓨터 통신에 사용되는 패킷 등과 같은 데이터를 수집하는 침입 감사 데이터(Audit Data) 수집 과정을 거친 후에 수집된 침입 감사 데이터는 침입 판정이 가능할 수 있도록 데이터 가공 및 축약(Data Reduction and Filtering) 과정을 거쳐 의미 있는 정보로 전환된다. 이러한 과정을 통해 생성된 침입 감사 데이터는 SVM에 입력되기 전에 SVM 머신의 표준 입력 형식에 합당하도록 포맷을 변환하여야 한다.

데이터 포맷 변환은 각 연결들의 앞부분에 정상일 경우 '1', 공격일 경우 '-1'을 레이블링 한 뒤, 40개의 속성마다 'No:속성 값'과 같이 넘버링 함으로써 얻어진다.

5.2 성능 평가 기준

제안 방법의 성능을 평가하기 위한 항목으로 탐지율과 False Positive 오판율, False Negative 오판율을 사용하며 계산방법은 다음과 같다.

$$\text{탐지율} = \frac{\text{시스템에 의해 침입으로 판정된 침입 데이터의 개수}}{\text{전체 침입 데이터 개수}} \times 100 \quad (식1)$$

$$\text{F-P오류율} = \frac{\text{시스템에 의해 침입으로 오판된 정상 데이터의 개수}}{\text{전체 정상 데이터 개수}} \times 100 \quad (식2)$$

$$\text{F-N오류율} = \frac{\text{시스템에 의해 정상으로 오판된 침입 데이터의 개수}}{\text{전체 침입 데이터 개수}} \times 100 \quad (식3)$$

(식1)은 탐지율을 의미하며, 전체 침입 데이터 중 시스템에 의해 침입으로 정확히 판정된 데이터의 비율을 백분율로 나타낸 값이다. (식2)는 펄스 포지티브(False Positive)에 대한 오판율로써 전체 정상 데이터 중 시스템에 의해 침입으로 오 판정된 데이터의 비율을 백분율로 나타낸 값이며, (식3)은 펄스 네거티브(False Negative) 오판율로써 전체 침입 데이터 중 시스템에 의해 정상으로 잘못 판정된 데이터의 비율을 백분율로 나타낸 값이다.

5.3 실험방법

기존 방식 실험은 SVM 학습을 통해 생성된 결정함수에 침입 감사 데이터를 적용하여 침입 여부를 판단하는 과정이다. 기존 방식의 학습은 학습용 데이터 셋과 학습에 사용되는 내부 커널함수, 정규화 매개변수인 C값에 의존하며, 다음과 같은 과정을 거친다. 무선 데이터셋의 연결들 중 6만 건을 비례추출 하여 정상(1)/공격(-1)으로 레이블링 한 후 으로 나타내어지는 RBF커널(C=0)을 사용하여 학습시킴으로써 이진 분류를 수행할 수 있는 결정함수를 얻는다. 기존방식 학습 후 생성된 결정함수를 이용하여 침입 탐지 실험을 수행하기 위한 실험 데이터는 데이터 셋 중 10만 건을 랜덤 추출하여 생성하였다. SVM 탐지 실험 과정에서는 30만 건의 침입 감사 데이터를 모두 커버하기 위해 총 3번에 걸쳐 실험 데이터 셋을 추출하여 SVM 탐지 실험을 진행하였다. 기존 방식의 침입 탐지 과정에서는 학습 데이터를 추출하여 SVM 결정함수에 적용시켜 탐지를 수행하며 그 결과 생성된 결과 파일에는 탐지 여부가 기록된다.

제안 방식 실험은 의사결정트리 학습을 통해 생성된 모델에 침입 감사 데이터를 적용하여 침입 여부를 판단하는 과정이다. 기존 방식 실험 후, 탐지하지 못한 약 7천건의 연결 데이터를 추출하여 실험 데이터로 사용한다. 즉, 제안 방식의 침입 탐지 실험은 실험 데이터를 추출하여 제안 모델에 적용시켜 탐지 결과를 파일로 저장하게 된다. 텍스트 파일로 저장된 탐지 결과에는 탐지 여부와 정탐지 횟수를 카운트 한 내용이 기록된다.

5.4 평가

SVM 학습 후 생성된 결정함수로 기존 방식 실험을 수행한다. 표 2는 기존 방법과 제안 방법의 실험 결과이며, 그림 3은 SVM과 제안방식을 비교한 그래프이다.

표 2. 제안 방법과 기존 방법의 성능 비교
Table 2. Performance comparison between existed and proposed methods

평가 기준 / 방법	학습 소요시간	탐지 소요시간	탐지율	F-P 오류율	F-N 오류율
SVM	35분40초	25분 30초	91.50%	3.00%	9.05%
제안방법	35분55초	25분 38초	97.30%	2.80%	8.16%

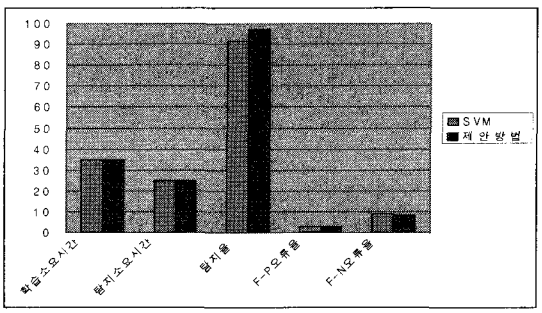

그림 3. 제안 방법과 기존 방법의 비교
Fig 3. Comparison between existed and proposed methods

기존의 SVM의 학습소요시간보다 제안방법의 소요시간은 15초 정도 길었으나, 탐지 소요시간은 기존 SVM에 비해 8초 정도 추가로 소요됨으로, 전체 학습 시간이 탐지시간에 미치는 영향은 미미하다. 탐지율의 경우는 연속형의 데이터를

고려한 제안방법이 단일 SVM 방식보다 6.8% 높게 측정되었으며, F-P 오류율과 F-N 오류율은 기존에 비해 0.2%, 0.89%가 낮은 실험 결과를 확인할 수 있다.

Ⅵ. 결론

한 조직 내의 무선 LAN에서 침입 탐지 및 방지를 위한 솔루션을 설치하기 위해서는 우선 어떤 조직 내의 어떤 침입과 위협이 있는지를 분석해야 할 것이다. 또한 일반적으로 알려진 유선 네트워크에서의 침입과는 달리 전파 통신을 한다는 점에서 유사한 침입 유형이라도 더 크거나 작은 영향력을 줄 수 있다는 점을 간과해서는 안 된다. 이 논문에서는 무선랜이 가지는 위협과 보안방안 등을 알아보고, 기존의 방법에 비해 효율적인 탐지율을 가지는 침입탐지시스템을 설계하였다. 제안한 침입탐지시스템 시스템은 AP를 거치는 무선 데이터를 센서를 통해 측정하고, 이 데이터를 이산형과 연속형으로 구분한 후 SVM과 데이터마이닝 기법을 혼합시켜 설계하였다. 그 결과, 기존의 SVM 방법만을 활용한 것보다 학습소요시간과 탐지소요시간은 더 길었으나, 탐지율과 F-P 오류율, F-N 오류율은 훨씬 향상됨을 알 수 있었다. 향후에는 제안한 기법에 추가적으로 들어가는 기능으로 공격 시그너처 등을 함께 활용하여 탐지소요시간을 줄이면서도 탐지율의 향상을 가져올 수 있는 구조를 연구하고자 한다.

참고문헌

[1] NIST, Special Publication 800-94, Guide to Intrusion Detection and Prevention Systems (IDPS).

[2] NIST, Special Publication 800-97, Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i.

[3] NIST, Special Publication 800-101, "Guidelines on Cell Phone Forensics".

[4] IEEE, IEEE 802.11a,b,g, http://standards.ieee.org/getieee802/download/

[5] N. Cristianini an, J. Shawe-Taylor, "An Introduction to Support Vector Machines and Other Kernel-Based Learning Methods", Cambridge University Press, 2000.

[6] Sung, A.H. Mukkamala, S., "Identifying important features for intrusion detection using support vector machines and neural networks", Applications and the Internet, 2003. Proceedings. 2003 Symposium on , 27-31 Jan. 2003.

[7] Ke Wang, Salvatore J. Stolfo, "One-Class Training for Masquerade Detection", CU Tech Report April 2003.

[8] Wenke Lee, Salvatore J. Stolfo, Kui Mok, "Data Mining Framework for Building Intrusion Detection Models", In Proceedings of the 1999 IEEE Symposium on Security and Privacy, Oakland, CA, May 1999.

[9] Zhi-Song Pan; Song-Can Chen; Gen-Bao Hu; Dao-Qiang Zhang, "Hybrid neural network and C4.5 for misuse detection", Machine Learning and Cybernetics, 2003 International Conference on , Volume: 4 , Pages:2463 - 2467, Vol.4 2-5 Nov. 2003.

저 자 소 개

우성희

1999년 2월 : 충북대학교 전자계산학 이학박사

1995년 9월~2006년 2월 : 청주과학대학 컴퓨터과학과 부교수

2006년 3월~현재 : 충주대학교 전기전자 및 정보공학부 컴퓨터 멀티미디어학과 교수

〈관심분야〉 네트워크 보안, 침입탐지시스템, 프로토콜 테스팅