사이버전 피해평가 과정에서 비인가 무선 AP 공격 식별을 위한 기계학습을 이용한 데이타 분석

김도연, 김용현**, 김동화**, 신동규*, 신동일*
*세종대학교 컴퓨터공학과
**국방과학연구소
e-mail: rlaehdus2003@gce.sejong.ac.kr, { shindk, dshin}@sejong.ac.kr

Data analysis for detection of unauthorized AP using machine learning algorithm in the process of cyber war damage assessment

Doyeon Kim, Yonghyun Kim**, Donghwa Kim**, Dongkyoo Shin*, Dongil Shin*
*Dept of Computer Engineering, Se-jong University
**Agency for Defense Development

요 약

사이버전 피해평가에 있어서 유무선 통합 환경에 대한 공격의 탐지와 이에 대한 평가가 필요한 상황이다. 특히 회사, 정부 및 군 시설 등에서 인가되지 않은 AP를 사용하여 공격이 발생하는 경우 각종 바이러스 및 해킹 공격에 의한 피해가 발생한 가능성이 높다. 따라서 인가된 AP와 인가되지 않은 AP를 탐지해서 찾아 내야한다. 본 논문에서는 인가된 AP와 인가 되지 않은 AP를 탐지하기 위해 RTT(Round Trip Time)값을 데이터셋으로 만들고 각 기계학습 알고리즘 SVM(Support Vector Machine), J48(C4.5), KNN(K nearest neighbors), MLP(Multilayer Perceptron)의 결과를 비교해 성능의 차이를 밝히고 이를 통하여 공격을 탐지하여 피해평가에 연결이 되도록 한다.

1. 서론

사이버전에서의 피해평가는 다음 작전은 전개를 위하여 매우 중요한 과정이다. 사이버전에서의 피해평가를 위해서는 정보 자원을 포함하는 자산평가, 공격식별, 공격자의 의도 파악 및 이에따른 공격 유형 분류, 각 공격에 따른 피해평가의 과정의 구성이 필요하다[1],[2]. 기존의 사이버전 피해평가 연구는 유선환경에 치우쳐 왔다 [3],[4]. 그러나 근래에는 무선네트워크를 포함하는 유무선 통합 환경이 출현하였다.

무선 네트워크를 이용한 디바이스의 빠른 발전으로 인해 우리 삶에서는 WiFi 없는 곳을 찾아보기 힘들다. 회사는 물론 카페, 군 시설, 학교 및 공공기관에서도 쉽게 WiFi를 이용할 수 있다.

WiFi는 불특정 다수가 이용하기 때문에 접속자를 일일이 다 확인하기는 어렵다. 그리고 인가된 WiFi를 이용한 핫스팟 같은 테더링(Tethering) 경우에도 직접 AP 목록을 보고 설정을 자세히 보지 않는 이상 식별하기가 확실치 않다. 그러나 다양한 스마트 기기들로 인해 비인가 AP의 존재는 필수불가결한 존재가 되었다. 공공장소에는 물론이고 회사에서 핫스팟 같은 비인가 AP에 대한 규제나 제제가 없기 때문에 사용 또한 무분별하다. 이는 무선 네트워크에 매우 취약한 점을 제공한다. 비인가 AP에 접근한 다른 사용자들의 정보를 훔치거나 엿볼 수 있고, PC 또한 해킹이 가능하기 때문에 피해가 생길 수 있다.

특히나 정보 기관이나 군 시설에서 이러한 공격을 당한다면 국가적 피해로 이어질 수 있다. 2013년 6·25 사이버 테러로 인해 청와대가 공격받았고, 2014년 12월 17일 한수원 기밀 유출 사건이 일어났으며, 2017년 6월 26일 은행 세 곳과 금융결제원이 디도스(Ddos)공격을 받았다. 이처럼 사이버 공격은 정보 기관이나 군 시설에도 유·무선을 가리지 않고 일어날 수 있기 때문에 항상 대비를 갖추고 있어야한다.

대비를 갖추기 위해 4단계를 준비해야 한다. 우선 사이버전에서 발생 전 피해가 발생할 수 있는 자산을 조사하고 공격 식별을 하기 위해 탐지를 한다. 그리고 공격 유형을 나누어 각 공격에 대한 피해 평가를 해야 한다.

이 중 공격 식별을 위한 공격 탐지 단계에서 무선 환경(ex WiFi)을 통한 공격에 대해서 탐지가 미흡한 상황이다. 탐지를 통해서는 피해 평가에도 활용이 가능하기 때문

에 연구가 필요한 부분이라고 할 수 있다.
이러한 공격을 감지하기 위해서는 보다 정확도 높은 불법 AP의 판별이 필요한 상황이다. 그리고 높은 정확도의 판별을 위해서는 다양한 알고리즘의 대한 실험이 필요하다.
이 논문에서는 RTT(Round Trip Time)값을 이용해 데이터셋을 만들었다. 이렇게 구성한 데이터셋으로 기계학습 알고리즘에 적용해 결과값을 얻었고, 그 후 얻은 결과값들을 비교해 어느 알고리즘이 정확도가 높은지를 보인다. 2장에서는 관련연구 및 기존의 비인가 AP 분류를 위한 방법을 살펴보고, 3장에서는 실험 구성 소개와 데이터셋에서 쓰인 속성값의 관계들을 살펴본다. 4장에서는 실험을 통해 나온 결과를 분석하고 5장에서는 결론과 향후 발전 방향에 대해서 정리한다.

2. 관련 연구

인가된 AP와 비인가 AP(비인가된 AP)의 구성은 [그림1]과 [그림2]와 같다. 인가된 AP의 구성은 해당 AP의 무선 신호를 잡아서 기기를 사용하는 것이다. 반면, 비인가된 AP의 구성은 기존 인가된 AP의 신호를 중간에 다른 기기가 받고 그 신호를 이용해서 새로운 AP를 만들어 다른 사용자들이 이용 할 수 있도록 구성하는 것이다. [그림2]처럼 새로운 AP는 무선랜카드 2개를 가지고 있어야 하며 하나의 랜 카드로는 정상적인 AP의 신호를 수신하고, 다른 하나로는 받은 신호를 기반으로 새로운 AP를 만들어 신호를 보낸다. [5]

그림 1 인가 AP

[그림2]의 중계 AP 구조로 인해 인가된 AP와의 RTT 차이가 발생한다.

그림 2 비인가 AP

이 RTT값의 차이를 이용해 AP를 탐지하는 논문 중 H.Han과 B.Sheng의 [6]에서 쓰인 방법은 RTT값의 차이와 표준편차 값을 이용해 직선의 방적식에 적용해 직석을 만드는 것이다. 이 직석을 데이터 분포에 적용해 분류한다. 하지만 이 실험에서 분류를 위해 구하는 직선의 방정식의 α값과 β값이 고정된 상수를 이용함으로써 유연한 분류를 보여주지 못 한다. 이에 논문에서는 예정되지 못한 상황에서도 탐지가 가능한 알고리즘을 찾기 위해 여러 가지 알고리즘을 적용해서 분류하려고 한다.
RTT값들에 대한 특징점을 선정하는 방법으로는 각각의 인가된 AP와 비인가된 AP의 지연시간들의 차이와 평균과 분산값, 표준편차를 사용하였다.[7][8]

3. 실험 구성 및 데이터셋 추출

본 실험에서 Lenovo ideaPad Z400 touch 기기를 말단 PC로서 비인가PC를 이용하는 용도로 사용했으며, 인가된 AP로 쓰인 공유기는 Netgear GS608 이다. 비인가된 AP는 LG XNOTE P210-GE30P 와 이 노트북에 연결된 iptime N500을 이용해 새로운 AP를 구축했다.

각 데이터들은 window10 환경에서 tracert.exe를 이용해 교내 DNS서버와 AP까지의 RTT값을 측정해서 축적했으며, 측정이 되지 않는 홉을 제외하고 측정이 되는 홉만의 수치를 모아 관찰했다.
또한, 네트워크 실험에서 쓰일 프로토콜은 어느 것을 쓰냐에 따라 결과에 영향을 미칠 수 있다. 프로토콜마다 통신 규약의 큰 차이가 있을 수도 있으며 대역폭과 채널 또한

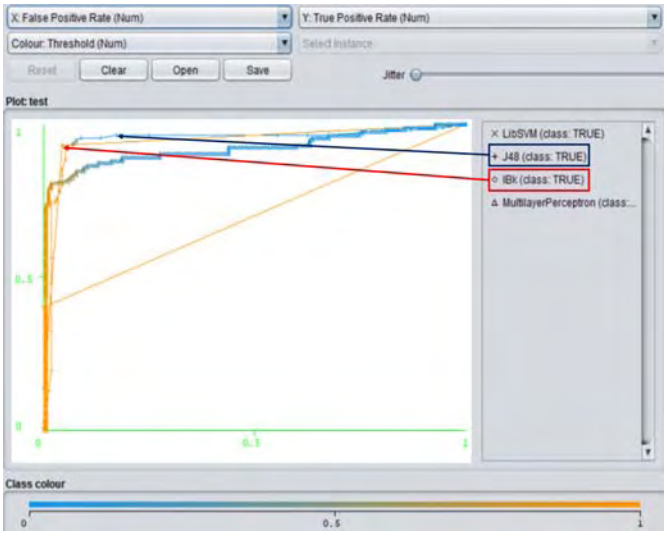

그림 3 실험 결과 시각화

실험에 오차를 일으킬 수 있다. 이에 본 논문에서는 현재 가장 많이 쓰이는 802.11n을 사용하여 실험을 진행하였다. 데이터의 양은 인가된 AP와 비인가된 AP 각각에서 2300개씩의 데이터 측정을 했으며, 측정된 데이터 중 상위 20%(460개) 값은 제외시키고 나머지 80%(1840개)의 데이터만을 사용했다. 그리고 측정된 RTTprobe (인가된 AP까지의 RTT) 값, RTTDNS (DNS까지의 RTT)값, RTTDNS - RTTprobe 의 값, 분산값, 표준편차를 구해 데이터를 분류하는데 속성값으로 사용했다.

4. 실험결과

실험에서 비교할 알고리즘은 기계학습 알고리즘들 중 분류 관련 알고리즘들을 선택했다. 해당 알고리즘들은 SVM(Support Vector Machine), J48(C4.5), KNN(K nearest neighbors), MLP(Multilayer Perceptron)이다. 각 알고리즘에 대한 실험 결과는 [표1]과 같다.

표 1 알고리즘 결과

알고리즘 / 정확도	SVM	J48	KNN	MLP
TP	40	92.9	92.9	84.5
FP	0	9.1	8.5	8.4
TC	70	92.9	94.1	88

TP : True Positive(%), FP : False Positive(%), TC : Total Correctness(%)

각 알고리즘의 결과를 보면 TP(True Positive)부분에서는 J48(C4.5) 와 KNN 알고리즘이 가장 정확도가 높았으며, FP(False Positive)에서는 SVM이 가장 높은 정확도를 보여줬다.

[그림 3]은 실험 결과를 weka 툴의 시각화 기능을 이용해 그래프로 비교해 본 그림이다. ㄱ 자의 형태에 가까울수록 가장 이상적인 결과라고 할 수 있다. [그림3]에서도 보시다시피 KNN 알고리즘이 이 형태에 가장 가깝고 그 다음으로 J48이 이상적인 모양을 띄고 있다.
결과적으로는 전체적인 정확도를 봤을 때는 KNN이 가장 높은 정확도를 보여줬다.

5. 결론

본 논문에서 인가된 AP와 비인가 AP의 차이는 기계학습을 통해 분류 가능하며 아직 정확도 면에서는 불안정한 부분이 있는 것을 확인 할 수 있었다. 그러나 이 문제에 있어서 실험에서 쓰인 데이터셋의 양과 속성값도 관련이 있기 때문에 향후에 많은 양의 데이터셋을 축적하고 속성값 또한 보충을 해서 견고한 실험을 할 필요가 있다. 그리고 이를 이용해 AP를 분별하는 프로그램의 개발 또한 필요한 부분이라고 생각한다.

ACKNOWLEDGMENT

본 연구는 방위사업청과 국방과학연구소의 지원으로 수행되었습니다(UD160066BD)

참 고 문 헌

[1] Ostler, Ryan. Defensive cyber battle damage assessment through attack methodology modeling. No. AFIT/GCO/ENG/11-11. AIR FORCE INST OF TECH WRIGHT-PATTERSON AFB OH GRADUATE SCHOOL OF ENGINEERING AND MANAGEMENT, 2011.
[2] Fortson Jr, Larry W. Towards the development of a defensive cyber damage and mission impact methodology. No. AFIT/GIR/ENV/07-M9. AIR FORCE INST OF TECH WRIGHT-PATTERSON AFB OH SCHOOL OF ENGINEERING AND MANAGEMENT, 2007.
[3] Tadda, George P. "Measuring performance of cyber situation awareness systems." Information Fusion, 2008 11th International Conference on. IEEE, 2008.
[4] Musman, Scott, et al. "Evaluating the impact of cyber attacks on missions." International Conference on Cyber Warfare and Security. Academic Conferences International Limited, 2010.
[5] 장룡호, et al. 비인증 AP 의 하드웨어 성능에 따른 시간 측정 기반의비인증 AP 탐색 기법의 분석. 한국통신학회논문지, 40.3: 551-558, 2015.
[6] Han, Hao, et al. "A timing-based scheme for rogue AP detection." IEEE Transactions on parallel and distributed Systems 22.11 (2011): 1912-1925.
[7] 이재욱; 이시영; 문종섭. k-SVM 을 이용한 Rogue AP 탐지 기법 연구. 정보보호학회논문지, 24.1: 87-95, 2014.
[8] 강성배, 양대헌, 최진춘, 이석준. "SVM을 이용한 중계 로그 AP 탐지 기법." 정보보호학회논문지, 23.3 (2013.6): 431-444.