무선통신에서의 머신러닝 기반 재밍 공격 검출 및 분류에 대한 연구

홍석화, 김규영, 이시현*
한국과학기술원 전기및전자공학부
seokhwa@kaist.ac.kr, kimyou283@kaist.ac.kr *sihyeon@kaist.ac.kr

Machine Learning Based Jamming Detection and Classification for Wireless Communications

Seokhwa Hong, Kyuyeong Kim, Si-Hyeon Lee*
School of Electrical Engineering, KAIST

요 약

본 연구에서는 머신러닝 기반 분류 기법과 이상탐지 기법을 계층적으로 통합한 하이브리드 재밍 검출 및 분류 알고리즘을 제안하고자 한다. 제안 알고리즘은 일차적으로 의사결정나무 알고리즘을 활용하여 오용탐지 모델을 만들어, 정상과 각 공격 유형의 데이터를 말단 노드별로 분해한다. 이어서 말단 노드로 분해된 데이터를 활용하여 이상탐지 모델인 Isolation Forest를 생성한다. 이를 통해 아는 유형의 공격에 대해서는 분류를 할 수 있음과 동시에 모르는 유형의 공격에 대해서도 검출이 가능하다는 것이 본 알고리즘의 장점이다. 성능평가를 위해 실제 무선통신 환경에서 다양한 유형의 재밍 공격을 구현하여, 기존 알고리즘 대비 제안한 알고리즘의 우수함을 입증하였다.

Ⅰ. 서 론

재밍 공격은 다양한 무선통신 네트워크를 위협할 수 있는 공격으로 알려져 있다. IoT, V2X, UAV뿐만 아니라, 5G, 6G와 같은 차세대 통신에서도 재밍 공격에 취약함이 지적되고 있으며, 이를 해결하기 위해서 머신러닝 기반의 재밍 검출 연구가 활발히 이루어지고 있다. 기존 재밍 검출 기술은 크게 오용탐지 기법과 이상탐지 기법으로 나뉜다. 오용탐지는 아는 유형의 공격은 높은 정확도로 검출 및 분류를 할 수 있지만 모르는 유형의 공격에 취약하다. 한편, 이상탐지 기법은 모르는 유형의 공격도 검출할 수 있지만 오용탐지 기법 대비 낮은 검출 정확도와 공격 유형의 분류가 어려운 문제점을 가진다. 이를 해결하기 위해 유선 네트워크 상황에서의 침입탐지 분야에서 오용탐지 기법과 이상탐지 기법을 함께 사용한 하이브리드 구조의 알고리즘이 제안되었다. 아는 공격과 모르는 공격을 모두 높은 정확도로 검출하는 결과를 보였으나, 공격 유형의 분류는 고려하지 않았다[1]. 본 연구에서는 재밍 공격의 분류를 통해 해당 공격에 대한 적절한 대응을 할 수 있다는 점에서 착안하여, 아는 공격에 대한 분류와 모르는 공격에 대한 검출이 동시에 가능한 알고리즘을 제안하고자 한다. 제안한 알고리즘은 분류 기법과 이상탐지 기법을 계층적으로 통합한 하이브리드 방식으로, 실제 무선통신 모뎀과 다양한 재머를 활용한 실험을 통해 기존 기술 대비 큰 성능 개선을 확인하였다.

Ⅱ. 본론

1. 모델

실제 무선통신 환경에서 통신지표를 바탕으로 성능을 평가하기 위하여 5,120MHz 대역에서 통신하는 송수신 모뎀을 활용하였다. 통신 모뎀은 TDMA 변조 방식을 활용하여 고정된 상황에서는 -25dBm의 송신 파워로 통신하고, 이동통신 상황에서는 -10dBm의 송신 파워로 통신한다.

통신 지표: 재밍 판단을 위해 수신단에서 얻어지는 지표들을 사용하였으며, 활용한 지표는 각각 *Dst id, PER, SNR, RSSI*로 정의한다. *Dst id*는 초당 감지되는 패킷의 개수이며, *PER*은 초당 발생하는 에러 패킷의 개수이다. *SNR*은 신호 대 잡음비이며, *RSSI*는 신호의 수신 감도를 의미한다.

재머: 다양한 유형의 공격에 대한 평가를 위하여 4가지 재머를 생성하였다. 통신 대역 내 하나의 주파수를 공격하는 톤 재머, 통신 대역폭 이상의 넓은 주파수 대역에 노이즈를 발생시키는 가우시안 재머, 시간적으로 온/오프가 반복되는 펄스 재머, 그리고 특정 주기로 주파수 하한부터 상한까지 변화해가며 공격하는 스위프 재머이다. 재머 생성을 위해서 벡터 신호 발생기 Eligent E4438C를 사용하였다.

실험 시나리오: 송신 모뎀의 움직임에 따라, 고정 시나리오와 이동 시나리오로 나누었다. 고정 시나리오는 그림 1(a) 와 같이 송수신 모뎀이 5m 거리의 고정된 위치에서 통신한다. 재머 거리 5m에서 정상과 4가지 재머에 대하여 각 300개씩 총 1,500개의 데이터를 수집하였고, 재머 거리가 가까울 때(3m)와 멀 때(7m)도 같은 방식으로 수집하였다. 이동 시나리오는 그림 1(b)와 같이 송신 모뎀이 원형 이동과 수직 이동하는 경우로 나누었다. 두 경우 모두, 재머 거리 4.5m에서 정상과 4가지 재머에 대하여 각 350개씩 총 1,750개의 데이터를 수집하였으며, 재머 거리가 가까울 때(4.5m)와 멀 때(6m)도 같은 방식으로 수집하였다.

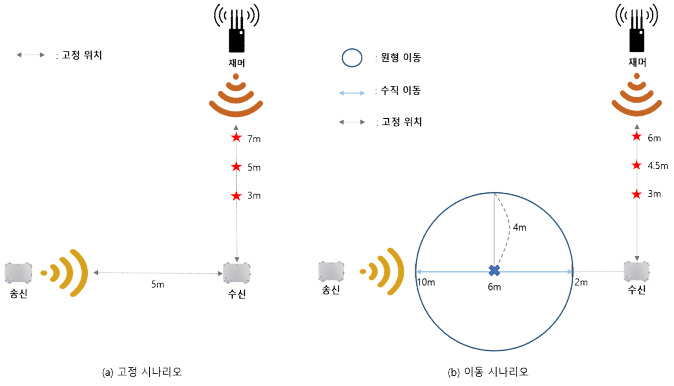

그림 1. 고정 시나리오 및 이동 시나리오

2. 제안 알고리즘

본 논문에서 재밍 여부를 판단하는 것을 재밍 검출, 재머의 유형을 분류하는 것을 재밍 분류라고 정의한다. 제안하는 하이브리드 재밍 검출 및 분류 알고리즘은 다음과 같이 동작한다. 첫 번째로, 오용탐지의 대표적인 기법인 의사결정나무(CART)[2]를 학습 데이터를 활용해 형성한다. 의사결정나무는 학습 과정에 활용된 아는 공격은 잘 검출 및 분류하지만, 학습에 활용되지 않은 모르는 공격에는 취약하다. 학습 데이터로 형성된 의사결정나무의 각 말단 노드들은 정상과 여러 유형의 공격 데이터들이 분해된 형태로 이루어진다. 각 말단 노드 데이터를 활용하여 노드별로 이상탐지 기법인 Isolation Forest(IF) [3]를 학습한다. IF는 예상과 다른 패턴을 찾는 알고리즘으로, 학습 데이터에 이용된 데이터와 다른 특성을 보이는 데이터를 비정상으로 판단한다. 이를 활용하여 의사결정나무에서 정상이라고 판단한 노드에 대하여, IF를 이용해 정상인지 모르는 유형의 공격인지 판단한다. 그리고 의사결정나무에서 아는 유형의 공격이라고 판단한 노드에 대하여 아는 공격인지 모르는 유형의 공격인지 판단한다. 이러한 구조의 모델을 병렬처리가 가능한 앙상블 기법을 이용하여 다수결 결정을 통해 성능을 향상하였다. 주어진 데이터만을 활용해 결정경계를 정하는 의사결정나무의 특성상 모르는 공격이 정상 혹은 아는 유형의 공격으로 잘못 판별되는 문제를 해결하여, 아는 공격을 분류할 수 있음과 동시에 모르는 공격의 검출이 가능하다.

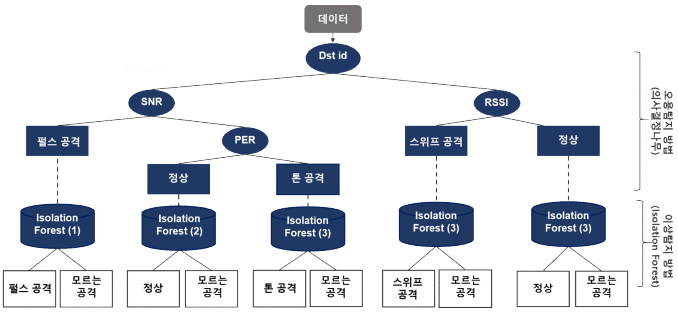

그림 2. 의사결정나무와 IF의 하이브리드 구조

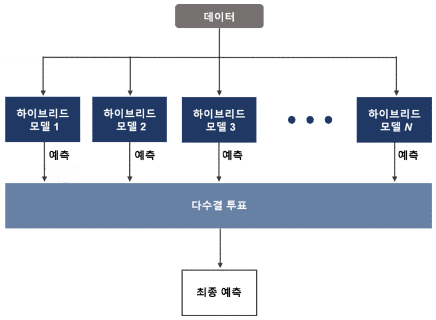

그림 3. 하이브리드 모델의 앙상블

3. 실험 결과

수집한 통신 지표를 바탕으로 여러 시나리오에 대하여 제안한 알고리즘과 기존 알고리즘 [1]의 성능을 비교하였다. 학습에 이용된 재머와 이용되지 않은 재머에 대한 성능을 평가하기 위하여 1가지 재머를 알고 있는 경우, 2가지 재머를 알고 있는 경우, 그리고 3가지 재머를 알고 있는 경우로 나누어 실험을 진행하였다. 3가지 경우 모두 학습 단계에서 정상과 아는 유형의 재머를 학습하고, 테스트 단계에서는 아는 유형과 모르는 유형을 1:1 비율로 테스트하여 아는 유형의 분류와 모르는 유형의 검출 성능을 동등하게 평가하고자 하였다. 테스트 데이터는 학습 데이터에서 활용하지 않은 데이터를 사용하였다. 그림 4에서 확인할 수 있듯이 고정 및 2가지 이동 시나리오 모두 제안한 알고리즘이 기존 알고리즘 대비 좋은 성능을 보였다. 또한 재머가 가까울 때와 멀 때의 실험에서도 유사한 결과를 보여, 거리에 상관없이 알고리즘이 잘 동작하는 것을 알 수 있었다.

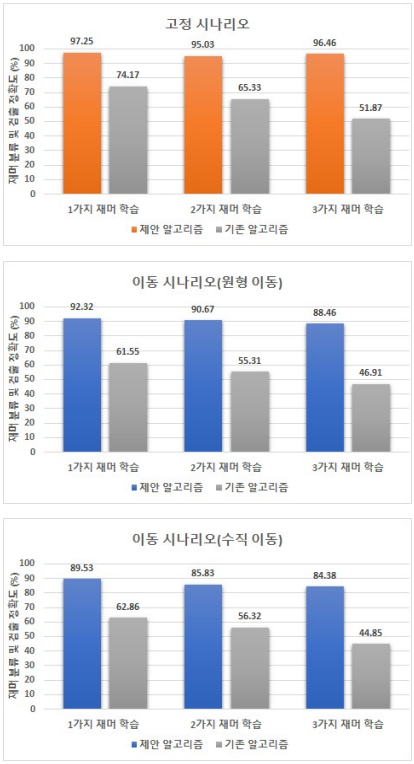

그림 4. 재밍 검출 및 분류 정확도

Ⅲ. 결론

본 논문에서는 머신러닝을 기반으로, 아는 유형의 재머를 분류할 수 있음과 동시에 모르는 유형의 재머도 검출할 수 있는 알고리즘을 제안하였다. 무선통신 모뎀에서 얻어진 실제 통신 지표와 4가지 유형의 재머를 바탕으로 성능을 평가하였다. 우리가 아는 한, 아는 재머의 분류와 모르는 재머의 검출이 동시에 가능한 알고리즘은 무선 재밍 검출 분야에서 최초이며, 우수한 성능과 함께 잠재적인 모든 재밍 공격의 검출 가능성을 보였다.

ACKNOWLEDGMENT

본 연구는 과학기술정보통신부의 재원으로 한국연구재단, 무인이동체원천기술개발사업단의 지원을 받아 무인이동체원천기술개발사업을 통해 수행되었음.(No.2020M3C1C1A01084524)

참 고 문 헌

[1] G. Kim, S. Lee, and S. Kim, “A novel hybrid intrusion detectionmethod integrating anomaly detection with misuse detection,”*Expert Syst. with Appl.*, vol. 41, no. 4, pp. 1690 - 1700, 2014.

[2] L. Breiman, J. Friedman, R. Olshen, and C. Stone. “Classification and Regression Trees,” Wadsworth, Belmont, CA, 1984.

[3] F. T. Liu, K. M. Ting, and Z.-H. Zhou, “Isolation forest,” in *Proc. 8th IEEE Int. Conf. Data Mining*, Dec. 2008, pp. 413 - 422.