협력적 학습 기반의 효율적인 네트워크 공격 탐지 방법

조민지[1], 전소은[2], 이일구[3]

[1]성신여자대학교 융합보안공학과 학부생
[2]성신여자대학교 미래융합기술공학과 박사과정
[3]성신여자대학교 융합보안공학과, 미래융합기술공학과 교수

{20231114, 220237020,iglee}@sungshin.ac.kr

Cooperative Learning-Based Technique for Efficient Detection of Network Attacks

Min-Ji Cho[1], So-Eun Jeon[2], Il-Gu Lee[3]
*Dept. of Convergence Security Engineering, Sungshin Women's University
*Dept. of Future Convergence Technology Engineering, Sungshin Women's University

요 약

사물인터넷 기기 증가로 무선 네트워크에서 송수신 되는 데이터를 노린 악의적인 공격이 늘고 있다. 그러나 기존 탐지 방식은 낮은 탐지 성능과 높은 연산 부하를 가지는 한계가 있다. 본 논문은 자원이 충분한 access point (AP)와 경량 장치가 머신러닝 모델의 학습과 탐지를 분담하여 수행함으로써 탐지 성능과 효율성을 모두 개선할 수 있는 방법을 제안한다. 실험 결과에 따르면 종래 모델 대비 제안 모델의 탐지율은 평균적으로 약 38%, 데이터 전송 성공률은 약 17.75% 개선되었다.

1. 서론

사물인터넷과 모바일 기기의 사용이 보편화되면서 무선 네트워크 환경에 대한 의존도가 높아지고 있다. 무선 통신 기반의 사물인터넷 환경은 재밍이나 도청 등의 보안 위협에 취약하며, 간섭과 노이즈로 인해 급증하는 네트워크 상의 악의적인 공격을 탐지하기 어렵다 [1]. 이러한 문제를 해결하기 위해 네트워크 공격 탐지를 위한 다양한 연구개발이 진행되고 있으나, 기존의 머신러닝 기법 적용 방식은 연산 부담이 커서 경량 장치에 적용이 어렵고, 탐지 메커니즘을 단순화해 연산 부하를 줄이면 정확도가 낮아지는 트레이드오프 문제가 발생한다 [1]. 본 논문에서는 간섭이 존재하는 현실적인 네트워크 환경에서 access point (AP)와 경량 장치가 학습과 탐지를 분배하여 수행함으로써 탐지 성능과 효율성을 개선할 수 있는 방법을 제안한다.

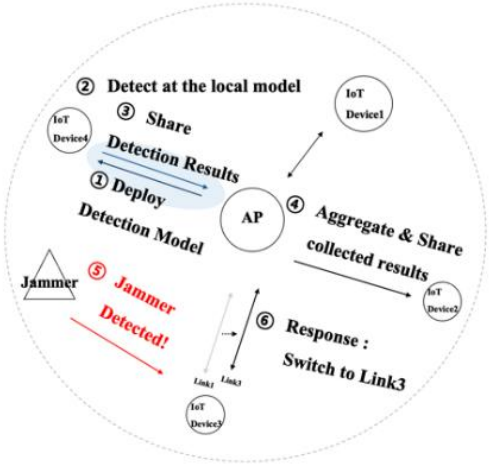
2. 선행연구

Hymlin Rose et al. [1]은 packet delivery ratio (PDR)이 기준값 이하이거나 timestamp가 일정 수준 이상일 경우 재밍으로 간주하고 received signal strength indicator(RSSI)를 보조 지표로 사용하였다. 그러나 신호 변화가 심하면 오탐 가능성이 증가하고 새로운 유형의 공격 탐지에는 한계가 있다.

S. Jeon et al. [2]은 로컬 노드의 탐지 결과로 글로벌 모델을 생성하고 스마트 리피터와 AP 간 협력으로 재밍 여부를 판단하는 머신러닝 기반 협력 클러스터링 기법을 제안하였다. 이 기법은 탐지율과 네트워크 성능을 향상시켰지만 로컬 장치 기반 학습하는 구조로 인해 자원이 제한된 환경에서는 한계가 있다.

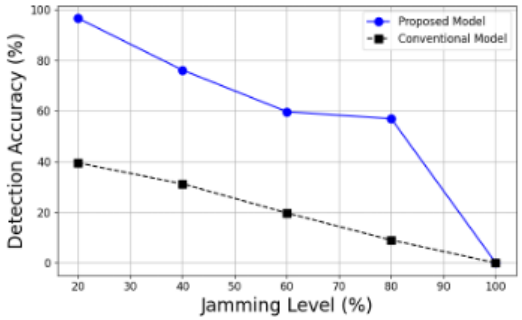
3. 협력적 학습 기반의 효율적인 네트워크 공격 탐지 및 대응 방법

본 장에서는 간섭이 혼재된 멀티 링크 환경에서 경량 장치가 효율적으로 네트워크 공격을 탐지 및 대응할 수 있는 제안 기법의 동작 메커니즘을 서술한다. 그림 1은 제안하는 모델의 동작 메커니즘을 나타낸다.

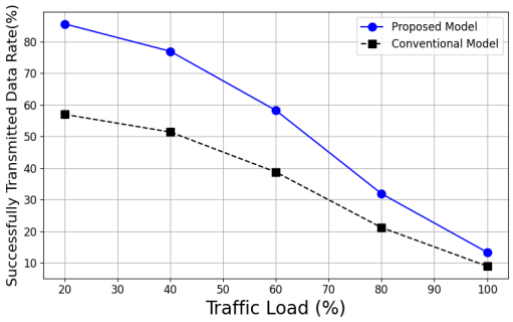


(그림 1) 제안 모델의 동작 메커니즘

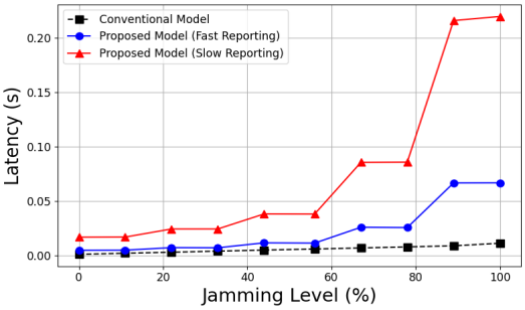
제안 모델은 경량 장치의 연산 부담을 낮추기 위해 AP에서 탐지 모델을 구축하고 주변 경량 장치로 배포하여 로컬 환경에서는 탐지만 수행하도록 한다. 각 장치는 공격 여부를 탐지한 후 일정 간격으로 AP에 탐지 결과를 보고하고, AP는 이를 취합하여 분석한다. 공격이 감지되면 간섭이 적고 공격이 발생하지 않는 링크로 이동하여 안정적인 통신 환경을 유지한다.



(그림 2) 제안과 종래 모델의 탐지율 비교



(그림 3) 제안 모델과 종래 모델의 전송 성공률 비교



(그림 4) 제안 모델과 종래 모델의 탐지 지연 시간 비교

4. 성능 평가

4.1 성능 평가 환경

본 실험에서는 탐지 모델 학습을 위해 악성 트래픽 데이터셋인 Wireless Sensor Network-Dataset (WSN-DS)을 사용하였다. 네트워크에 랜덤 노이즈가 포함된 환경에서 성능 평가했으며 Decision Tree 모델을 사용해서 데이터셋을 학습했다. 성능 비교를 위한 종래 모델로는 머신러닝 기반 로컬 탐지를 수행하는 모델을 선정하였다 [1]. 평가 지표로는 탐지율(Detection accuracy), 데이터 수신률(Successfully transmitted data rate), 탐지 지연 시간(Detection latency)을 사용하였다. 탐지율은 공격을 성공적으로 탐지한 비율을 의미하고, 데이터 수신률은 전송 데이터 중 성공적으로 수신된 비율을 의미한다. 탐지 지연 시간은 공격 탐지까지 걸린 시간을 의미한다. 탐지 지연 시간 실험에서는 제안 모델의 탐지 보고 주기에 따른 차이를 함께 비교하였다. Fast 모델은 공격 탐지 후 2 time unit 마다, slow 모델은 7 time unit 마다 AP에 보고하는 환경이다.

4.2 성능 평가 결과 및 분석

그림 2는 네트워크 내에 혼재된 간섭 강도 변화에 따른 두 모델의 탐지 정확도를 비교한 결과이다. 실험 결과 간섭 수준이 증가할수록 두 모델 모두 탐지율이 저하되었다. 특히 종래 모델은 로컬 데이터를 기반으로 탐지를 수행하므로 학습 데이터가 한정되어 탐지 성능이 급격히 감소하였다. 반면 제안 모델은 AP가 주변 장치의 탐지 결과를 수집하고 이를 분석하여 판단하기 때문에 일부 장치의 결과가 누락되어도 전체 탐지율에는 큰 영향을 받지 않았다.

그림 3은 트래픽 부하 수준이 높아질수록 데이터 전송 성공률(%)을 비교한 결과이다. 트래픽 부하 수준이 증가함에 따라 두 모델 모두 전송 성공률이 감소하였다. 종래 모델은 공격이 탐지되더라도 별도의 대응을 수행하지 않기 때문에 전송 성공률이 급격히 하락하였다. 이에 반해 제안 모델은 공격이 탐지되었을 때 간섭이 적은 링크로 전환하여 통신하므로 높은 트래픽 환경에서도 안정적인 전송 성능을 유지하였다.

그림 4는 간섭 강도에 따른 전송 지연 시간을 나타낸다. 간섭이 심해질수록 전체 지연 시간이 증가하는 결과를 보였다. 종래 모델은 로컬 탐지 방식을 수행하기 때문에 낮은 탐지 성능 대신 탐지 시간은 가장 짧았다. 반면 탐지 결과를 AP와 공유하는 제안 모델은 공유 과정에서 지연이 더 증가하였다. 이때 탐지 결과를 AP에 더 자주 보고하는 Fast 모델이 지연시간이 더 적게 소요되었다.

5. 결론

자원이 제한된 경량 장치는 사물인터넷 환경에 내재된 간섭과 노이즈로 인해 네트워크 공격을 안정적으로 탐지하고 대응하는 데 한계가 있다. 이에 본 연구에서는 종래 기법의 높은 연산 부담과 낮은 탐지율 문제를 개선하고자 AP에서 탐지 모델을 학습 및 배포하여 경량 장치에서도 효율적으로 공격 탐지 및 대응이 가능한 모델을 제안하였다.

Acknowledgement

본 논문은 2025년도 과학기술정보통신부 및 정보통신기획평가원의 재원으로 중견연구 사업의 지원(No. RS-2025-00518150)과 ICT혁신인재4.0 사업의 연구결과로 수행되었음 (No. IITP-2022-RS-2022-00156310)

참고문헌

[1] S.G. Hymlin Rose, T. Jayasree,"Detection of jamming attack using timestamp for WSN", Ad Hoc Networks, Vol. 91, Aug. 2019

[2] S. Jeon, S. Lee, and I. Lee, “Machine Learning-Based Efficient Discovery of Software Vulnerability for Internet of Things,” Intelligent. Automation. Soft Computing., vol. 37, no. 2, pp. 2407–2419, 2023.

[3] S. Jeon, S, Keem Y. Lee, H. Yu, and I. Lee, “Machine Learning-Based Cooperative Clustering for Detecting and Mitigating Jamming Attacks in beyond 5G Networks,” Information System Frontiers, Aug. 2024.