이 일 구 교수 지도
석사학위 청구논문

머신러닝 기반 재밍 공격 분류와 효과적인 방어 기법

2023

성신여자대학교 대학원
미래융합기술공학과
이 선 진

머신러닝 기반 재밍 공격 분류와 효과적인 방어 기법

이 일 구 교수 지도

이 논문을 석사학위논문으로 제출함

2022년 11월

성신여자대학교 대학원

미래융합기술공학과

이 선 진

인 준 서

이선진의 석사학위 논문으로 인준함

2022년 11월

심사위원장 김 경 진 (서명 또는 인)

심 사 위 원 이 일 구 (서명 또는 인)

심 사 위 원 임 연 섭 (서명 또는 인)

성신여자대학교 대학원

논 문 개 요

4차 산업의 발전과 함께 지능형 사물인터넷이 홈 네트워킹과 스마트 인프라에 널리 활용되고 있으며 무선 커넥티비티 기술은 전 산업과 일상생활에 필수적인 요소가 되었다. 무선통신 기술은 초고속, 초저지연 요구사항을 만족시키기 위해 진화를 거듭하며 발전하고 있다. 그러나, 주파수와 시간을 분할하여 다중 사용자가 채널을 공유하기 때문에 네트워크가 혼잡해지면 간섭 문제로 인해 서비스 품질 (QoS, Quality of Service)를 보장할 수 없다. 또한 악의적인 공격자는 재밍 공격 (jamming attack)으로 통신 가용성을 침해하거나 데이터의 무결성을 파괴하여 인간의 생명과 안전까지도 위협할 수 있다. 종래 재밍 공격의 탐지 및 대응 기술은 재머의 종류를 세부적으로 탐지하지 못하고 종류와 관계없이 대응하는 경우가 대부분이었으며, 이러한 방식은 지능적인 공격을 탐지하고 방어하는데 한계가 있다. 본 논문에서는 머신러닝 기반의 재밍 공격 유형 분류와 재밍 유형에 따른 차등적 대응이 가능한 재머 분류 및 효과적인 방어 (JCED, Jammer Classification and Effective Defense) 알고리즘을 제안한다. JCED는 재머 유형에 따라 단순 재전송부터 능동적인 배터리 소모 공격까지 다양한 대응 방식을 적응적으로 선택하여 조치할 수 있다. 실험 결과에 따르면 JCED는 재머에 대한 단일 대응만 가능한 대응 탐지 및 일관성 알고리즘 (CDCA, Countermeasure Detection and Consistency Algorithm)보다 24.9% 높은 유효 처리량 (effective throughput)과 23.4% 낮은 에너지 소모율을 보였다. 또한, 무결성 침해 공격이 존재하는 환경에서도 JCED는 CDCA 대비 유효 처리량을 평균 3.05배 향상할 수 있었다. 즉, JCED는 다양한 유형의 재밍 공격에 대한 효과적인 방어 메커니즘으로 작용하여 디지털 정보의 안전성과 높은 처리량을 보장했다.

목 차

표 차 례

그림 차례

Ⅰ. 서 론

정보가 사회와 경제의 중심이 되는 정보화 시대로 진입하면서, 와이파이(Wi-Fi) 기술은 사회 전 분야의 핵심 기반 기술로 자리잡고 있다. COVID-19 팬데믹으로 온라인 서비스 이용률이 급격하게 높아지고, 각 개인이 사용하는 디바이스가 증가하면서 와이파이를 활용하는 노드의 수도 증가하고 있다. MarketsandMarkets에서는 전 세계 와이파이 시장 규모가 2020년 94억 달러에서 2026년에는 252억 달러 규모로 매년 17.8% 성장한다고 전망한 바 있다 [1]. Wi-Fi는 액세스 포인트 (AP, Access Point) 신호가 닿는 범위 내에서 요금의 부담 없이 누구나 통신 서비스를 이용할 수 있다는 장점을 가진다. 그러나 네트워크 밀집도가 증가하고 무선 장치들이 넓은 대역폭을 사용할수록 서비스 품질 (QoS, Quality of Service)을 보장할 수 없다 [2]. 만약 공격자가 이러한 취약점을 악용하여 재밍 공격으로 의료 장치 간 통신 가용성을 침해한다면, 타겟 AP에 연결된 의료 장치들은 통신이 지연되어 서비스 품질이 열화되거나 생명과 안전 문제로 이어질 수 있다 [3]. 실제로 군 통신망과 기간망의 취약점을 파악해 분산 서비스 거부 공격 (DDoS, Distributed Denial of Service)을 실행하여 국가적 피해가 발생한 사례도 존재한다 [4].

종래의 재밍 공격 대응 기술은 재밍으로 인한 피해를 최소화하는 목적으로 연구되었다. 대표적인 재밍 공격 대응 기술로는 채널 및 주파수 호핑 (channel/frequency hopping) 방식 [5],[6], 라우팅 방식 [7], 재밍 특성 및 머신러닝 기반의 단일 재머 탐지/대응 방식 [14]-[21]이 있다. 단일 재머 탐지 방식은 재머의 타입과 상관없이 의심되는 공격을 재머로 분류한 후 그에 대한 대응을 하는 방식이며, channel hopping 및 라우팅 기술은 재머

의 공격 특성이 아닌 채널과 경로에 따라 대응하는 방식이다. Channel hopping에는 네트워크 내 모든 노드가 채널을 이동하는 능동 (proactive) 방식과 채널 상태가 변화했을 때만 채널 호핑이 일어나는 반응형 (reactive) 방식이 있으며 [8], 재머의 타입에 관계없이 간단한 대응이 가능하기 때문에 최근까지 연구되고 있다.

그러나 재밍 공격이 점차 지능형 공격으로 진화하면서 단일 재머 탐지 및 대응 방식만으로는 모든 재머를 탐지하는데 한계가 있으며 [9],[10], channel hopping에 사용되는 채널 자원도 제한되어 있으므로 종래의 대응 방식은 완전한 해결책이 될 수 없다. 또한, 여러 유형의 재머에 대해 일률적인 방어 방식을 적용한다면 통신 품질을 확연히 개선할 수 없다. 따라서 본 논문에서는 기본 서비스 셋 (BSS, Basic Service Set) 시큐어 컬러링 (secure coloring)을 통해 보안성을 유지한 상태에서 비의도적 간섭을 필터링하고 재전송과 능동적 공격(battery draining)을 통해 QoS를 개선하는 Jammer Classification and Effective Defense (JCED) 알고리즘을 제안한다.

논문의 주요 기여점은 다음과 같다.

1) 첫째, 재밍 공격별 차등적 대응을 위해 머신러닝 모델 기반으로 재밍 공격 유형을 정확하게 분류하는 JCED 기법을 제안했다.

2) 둘째, 재밍 공격 유형에 따른 재밍 패턴 회피, BSS secure coloring, 배터리 소모 공격과 같은 차등적 대응 기법을 적용하여 유효 처리량 (effective throughput), 재전송 횟수 (number of retransmission), 에너지 소모율 (energy consumption)을 향상했다.

3) 셋째, 네트워크 공격 트래픽 데이터셋을 활용하여 재밍 공격 및 대응 기법의 성능 평가를 위한 네트워크 시뮬레이션 프레임워크를 제안했다.

이 논문의 Ⅱ장에서는 재머 대응에 대한 선행연구를 분석한다. Ⅲ장에서는 대표적인 종래 재머 대응 방식을 분석하고 JCED 모델을 제안한다. Ⅳ장에서는 실험 환경을 설정하고, Ⅴ장에서는 다양한 평가 지표를 통해 JCED의 성능을 비교 분석한다. Ⅵ장에서 결론으로 마무리한다.

Ⅱ. 관련 연구

일반적으로 재밍 공격은 지속형 (constant), 무작위형 (random), 기만형 (deceptive), 반응형 (reactive) 공격으로 나눌 수 있다 [11]. Constant 재밍 공격은 반송파 감지 다중 접속 (CSMA, carrier sense multiple access) 프로토콜에 상관없이 지속적인 신호를 전송하여 대역폭을 마비시킨다. Constant 재머는 구현 및 실행이 간편하지만, 신호를 쉬지 않고 보내기 때문에 공격자의 에너지 소모 측면에서 비효율적이며, 탐지되기 쉽다는 한계가 있다 [12]. Random 재머는 임의의 기간 (period) 동안만 방해 비트를 보내고, 나머지 시간은 절전 (power-saving)을 하는 공격 방식이다. Random 재머는 constant 재머보다 적은 에너지를 사용하므로 공격자 관점에서 비용 효율적이지만, power-saving 시간에 따라 공격 수준이 낮아지므로 공격 성공 측면에서는 비효율적이다. Deceptive 재머는 일반 패킷을 지속적으로 전송하여 정상 통신임을 가장해 공격한다. Deceptive 재머는 일반 패킷을 활용하기 때문에 공격자를 탐지하기 어렵지만, 공격자의 에너지 사용 측면에서 비효율적이다. Reactive 재머는 채널 상태를 확인하여 정상 패킷 통신이 감지될 때 신호를 보낸다. Reactive 재머를 이용하기 위해서는 네트워크 상태를 실시간으로 확인하기 위한 센싱 회로가 필요하지만, 데이터 전송 과정이 감지될 때에만 공격을 발생시키기 때문에 공격 탐지 가능성을 줄일 수 있으며 적은 에너지만으로도 효율적으로 공격할 수 있다 [13].

최근에는 탐지가 어려운 deceptive 재머와 reactive 재머를 활용해 채널 점유를 시도하는 공격과 재머 탐지를 우회하는 지능형 재밍 공격이 함께 증가하고 있으며 이러한 공격을 탐지 및 대응하는 기술도 연구되었다.

Table 1은 재머 탐지 및 대응과 관련된 선행연구를 정리한 것이다. 이때 대응 능력 (defense capability)란 재밍 탐지 후 대응 여부를 의미한다. 전체 재머에 대한 대응이 가능한 경우 strong, 일부 재머에 대한 대응만 가능한 경우 weak, 재머에 대한 대응이 부재한 경우 inability로 나타냈다.

Table 1.
Analysis of existing studies on jammer detection and response methods

Existing study	Ref	Method	Limitation	Defense Capability
Feature-based Detection	[14]	▪ 신호 강도 및 노드 위치 일관성 분석을 통해 재밍 공격 판단 ▪ 채널이 idle 되는 시점을 모니터링하고, 일반 트래픽 시간과 다르면 공격으로 판단	▪ Reactive 재머에 대한 대응만 가능 ▪ 지능형 재밍 공격에서는 탐지 어려움	Weak
	[15]	▪ 네트워크의 더미 사용자를 방해 전파의 허니팟으로 만듦 ▪ Fake 메커니즘을 활용하여 공격자를 함정에 빠트려 대역폭 효율성을 최대 1.7배로 향상	▪ 지능형 방해 전파가 이 패턴을 학습할 경우의 대응이 고려되어 있지 않음 ▪ 일부 재머만 탐지와 대응 가능	Weak
	[16]	▪ Stackelberg 게임 이론을 사용하여	▪ 재머의 종류에 따른	Weak

		스마트 재머가 존재하는 환경에서의 전력 제어 방식 성능 평가 ▪ 재밍 카운터 측정 반복 알고리즘을 통해 공격 방어	대응은 없음	
ML-based Detection	[17]	▪ Cloud Radio Access Network (C-RAN)에서 4가지 유형의 재밍 공격을 감지하고 분류	▪ 통신 환경을 설계하지 않고 데이터셋만 활용 ▪ 탐지만 가능하고, 대응 기술은 없음	Inability
	[18]	▪ Constant, Reactive, Random 재머에 대한 기계학습 기반 분류 방법 제안	▪ 실제 통신 환경에서의 대응 기술 없음 ▪ Deceptive 재머에 대한 대응 없음	Inability
	[19]	▪ 재밍 신호의 유형을 조사하고, 매개변수를 활용하여 대규모 데이터셋 생성 ▪ Random Forest, SVM, Neural Network (NN)에 적용하여 성능 평가	▪ 재밍 공격의 탐지만 가능하고, 대응 기술은 없음 ▪ 재머 유형 분류 불가	Inability

[20]	▪ 패턴을 인식하는 지능형 방해 전파 탐지 및 대응 방식 제안 ▪ 실시간으로 원시 스펙트럼 정보를 얻어 데이터셋을 생성하고 강화 학습하여 대응	▪ 패턴을 고려했으나 대응 방식은 일관되게 적용됨 (채널 스위칭 활용)	Weak
[21]	▪ Double Deep Q Network (Double DQN) 기반의 안티 재밍 (Anti Jamming) 기술 제안 ▪ Sweep 재밍, Random 재밍, Sensing-based 재밍 공격에 대응함	▪ 대응 방식이 채널 스위칭으로 일관됨 ▪ 다른 유형의 재머에 대한 성능 평가 없음	Weak

Table 1에 따르면 재머 탐지 기법은 특성 (feature) 기반 탐지와 머신러닝 기반 탐지로 나눌 수 있다. Fadele et al. [14]은 reactive 재머를 탐지하기 위해 대응 탐지 및 일관성 알고리즘 (CDCA, Countermeasure Detection and Consistency Algorithm)를 제안했다. CDCA는 임계값을 제어하여 공격을 탐지하고 위치 기반 인증을 통해 노드 위치의 일관성을 판단한다. 실험 결과에 따르면 CDCA의 스루풋은 종래 reactive 재머 대응 방식보다 10% 향상된 86%의 성능을 보였으며, 에너지 소모량을 3%로 낮췄다. 그러나 CDCA는 reactive 재머에 대한 방어만 가능하므로 다른 유형에 재밍 공격이 발생하면 그에 대응할 수 없다. Ibrahim et al. [15]은 방해 전파 탐지를 위한 더미 사용자 (PSU, Pseudo Secondary User)를 생성하

고 공격자를 유인해 가두는 트랩 (trap)형 대응 방식을 제안하였다. 실험 결과에 따르면 PSU가 있는 모델의 대역폭 효율성이 종래 모델 대비 1.7배 높았다. 그러나 일부 재머 유형에 대해서만 탐지 및 대응이 가능하며, 지능형 재머의 우회 공격에 대응할 수 없다. Su et al. [16]은 스마트 재머의 통신을 억제하기 위해 슈타켈베르크 (Stackelberg) 게임 이론을 이용하여 재밍 카운터 측정 알고리즘을 평가하였다. 그러나 이 연구 또한 재머 종류에 대한 맞춤형 대응보다는 일관적인 대응 기술만을 활용해 방어한다는 한계가 있다.

Hachimi et al. [17]은 무선 센서 네트워크 데이터셋 (WSN-DS, Wireless Sensor Networks Dataset) [28]을 활용하여 머신러닝에서의 다중 분류 성능을 평가하였다. 다층 퍼셉트론 (MLP, Multi-Layer Perceptron)와 Kernelized Support Vector Machine (KSVM) 모델을 활용해 평가한 결과, 약 94%의 정확도로 random 재머, constant 재머, reactive 재머, deceptive 재머, normal을 분류했다. 그러나 실제 네트워크 상황을 모델링하지 않았으며, 공격을 분류한 후 대응에 대한 고려는 없었다. Kasturi et al. [18]은 에드혹 (Ad-hoc) 네트워크에서의 재머 분류를 제안하기 위해 Network Simulator (NS)-3 시뮬레이터를 활용하여 재밍 공격 환경을 구성하고, 학습 데이터셋을 만들었다. MLP, K-최근접 이웃 알고리즘 (KNN, K-Nearest Neighbor), 의사결정 나무 (DT, Decision Tree), 랜덤 포레스트 (RF, Random Forest) 모델을 활용해 constant 재머, reactive 재머, random 재머를 분류하였으며, 그라디언트 부스팅 (Gradient Boosting) 모델을 통해 평가한 결과 최대 94.9%의 정확도를 보였다. 본 연구에서는 직접 데이터셋을 구축했다는 기여점이 있지만, 이 또한 대응 조치는 제안하고 있지 않으며, deceptive 재머는 탐지할 수 없다. Arjoune et al. [19]도 자체 데이터셋을 구축하여 분류 모델을 평가하였으며, RF 모델에서 96.6%

의 정확도로 스마트 재머를 분류하였다. 그러나 대응 방법에 대한 고려는 없으며, 재머의 유형을 분류하지 못했다. Liu et al. [20]은 재밍 공격에 대응하기 위해 재머의 사전 정보가 필요하다는 점에 착안하여 공격 방식이 변화해도 공격에 대응할 수 있는 패턴 인식 기반 지능형 방해 전파 대응 방식을 제안하였다. 외부 환경 변화를 고려한 다양한 종류의 전파 방해 패턴을 식별하여 태깅한 후 강화학습을 활용해 모델을 학습하였다. 랜덤 스위칭 (random switching) 환경에서 실험한 결과에 따르면 실험 초반에는 단일 학습보다 처리율이 낮지만, 점차 처리 성능이 향상됨을 보였다. 이 논문은 재머의 패턴으로 분류한다는 점에서 기여점이 있으나, 대응 방식은 일관된 형태를 보였다. Xu [21]는 로우 (raw) 형태의 스펙트럼 데이터를 활용한 마르코프 (markov) 결정 프로세스 모델인 Double Deep Q Network (DQN)을 설계하여 스위핑 (sweeping) 재밍, random 재밍, 센서 기반 (sensing-based) 재밍과 같은 전형적인 채널 재밍 공격을 탐지하고, 이를 방어하는 안티 재밍을 제안하였다. 또한 Double DQN은 기존 합성곱 신경망 (CNN, Convolutional Neural Networks) 형식의 Q 네트워크보다 방해 전파 공격을 방어하는데 효과적임을 밝혔다. 이 논문은 여러 대응 방식을 모델링했다는 점에서 의의가 있지만, 통신 과정에서 재머 유형을 하나로만 분류하여 단일 대응책으로 동작하기 때문에, reactive, deceptive 재머에 대한 탐지 및 대응 방법은 고려하지 못했다.

이처럼 재머 탐지와 관련된 종래 연구들은 주로 단일 재머 탐지에 초점이 맞춰져 있었고, 단편적인 대응으로 인해 모든 재머에 대한 대응 커버리지를 갖추지 못했다. 또한 재머 유형을 분류하더라도, 탐지에 성공한 유형 정보를 대응에 직접적으로 활용하는 연구는 없었다.

Ⅲ. JCED 메커니즘

본 논문에서는 Wi-Fi 통신 환경에서 재밍 공격이 발생했을 때, 머신러닝 모델로 재밍 공격 유형을 분류하고 적응적으로 (adaptive) 대응하는 JCED 알고리즘을 제안한다. 본 연구의 위협 모델 (threat model)은 네트워크 자원 소모 공격과 데이터 위변조 공격이다. 공격자는 자원 소모 공격을 통해 네트워크 가용성을 침해할 수 있고, 데이터 위변조 공격을 통해 데이터의 무결성을 파괴할 수 있다. 네트워크 자원 소모 공격에서 공격자는 일반 사용자와 같이 네트워크에 접근하여 통신할 수 있는 능력을 가지고 있다. 일반 사용자와는 달리 공격자는 악의적인 목적을 가지고 피해자의 시스템을 마비시키고, 정상적인 통신을 어렵게 한다. 따라서 네트워크 자원 소모 공격에서 시스템은 정상 사용자가 통신 서비스를 이용할 수 있도록 보장할 뿐만 아니라, 자원 처리 방식을 유동적으로 제어하여 네트워크의 자원 소비를 최소화해야 한다. 데이터 위변조 공격의 경우, 공격자는 일반 사용자로 위장하기 위해 패킷을 위변조할 수 있다. 만약 시스템에서 패킷의 무결성을 인식하지 못한다면 일반 사용자로 인식하여 공격자를 받아들이게 되며, 공격자는 이를 통해 시스템을 장악하고 시스템의 자원을 유출할 수 있다. 따라서 데이터 위변조 공격에서 시스템은 패킷의 무결성을 상시 확인하여 공격자를 발견하는 즉시 차단하고 그에 대해 대응해야 한다. 따라서 JCED 메커니즘은 재머 유형별 대응을 통해 가용성 침해 공격을 방어한다. 그리고 BSS secure coloring을 통해 무결성 파괴 공격을 탐지한다.

3.1 네트워크 구성

JCED의 네트워크 구성은 Fig. 1과 같다. 밀집 네트워크 환경에서는 AP 커버리지가 겹치는 중첩된 BSS (OBSS, Overlapped Basic Service Set) 구역이 존재한다 [22]. OBSS에 위치한 STA은 자신의 BSS에 있는 STA에서 송신하는 패킷 외에도 주변 BSS (neighbor BSS)의 패킷을 수신하게 된다. 반송파 감지 다중 액세스 및 충돌 회피 (CSMA/CA, Carrier sense multiple access with collision avoidance)를 사용하는 무선랜 장치들은 회선이 비어 있는지 확인(carrier sensing)함으로써 충돌을 회피한다. 만약 전송한 패킷이 충돌하면 랜덤 백오프 (random backoff)만큼 대기하며 무선매체가 계속 회선을 사용하고 있을 경우 대기 시간을 늘린다. 그리고 회선이 미사용되는 시점에 데이터를 전송한다. 따라서 밀집 네트워크에서 STA의 밀집도가 증가할수록 충돌 확률이 증가해 QoS가 저하된다. Wi-Fi 6 (802.11ax)에서는 BSS coloring 기법을 적용하여 밀집 네트워크에서의 효율적인 스펙트럼 사용을 지원한다 [23]. 송신 STA은 본인의 BSS를 알 수 있는 BSS coloring 정보를 프레임에 실어서 주변 BSS의 비의도적인 간섭을 필터링한다. 이 과정에서 데이터 처리율이 개선된다. 그러나 종래의 BSS coloring은 헤더에 평문으로 추가되는 정보이므로 공격자가 위변조하기 쉽다는 문제가 있다.

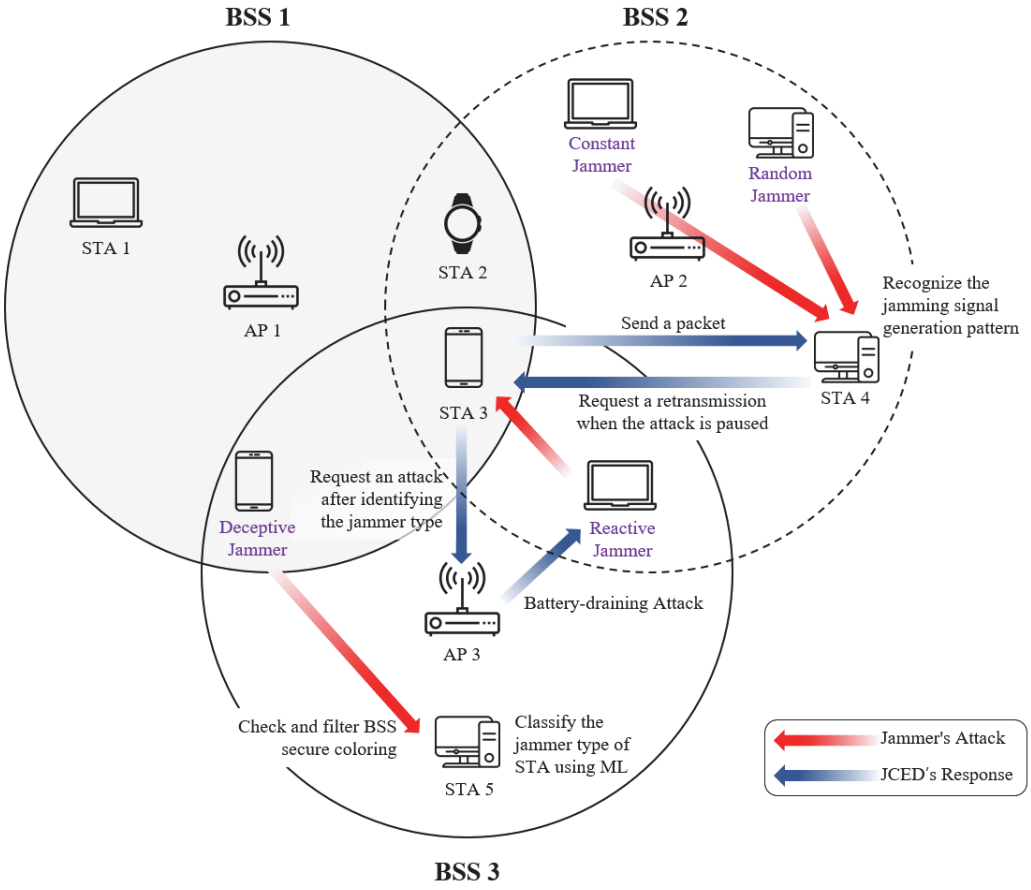

Figure 1. Network configuration of the JCED mechanism

반면 JCED는 STA이 패킷을 수신했을 때 BSS coloring을 확인함으로써 (STA 5) 비의도적인 간섭을 사전에 필터링한다. 또한 BSS secure coloring을 프레임 body에 추가로 삽입하여 deceptive 재머의 데이터 위변조 공격을 방지한다. 그리고 머신러닝 모델을 활용하여 재머 유형을 분류한다. 만약 constant 재머나 random 재머처럼 지속적인 신호를 발생시키는 공격 노드가 있을 경우, STA은 재머의 공격 패턴을 파악한다. 이후, 공격이 멈추는 시점에 처리하지 못한 정상 패킷의 재전송을 요청하고 처리한다 (STA 4). 또한 지능적으로 공격하는 reactive 재머를 탐지했을 경우, STA

은 AP에 재머 판별 정보를 송신하여 (STA 3), AP에게 공격을 요청한다. AP는 능동적인 공격(battery draining attack)을 수행해 reactive 재머의 공격을 무력화한다.

3.2 JCED 흐름도

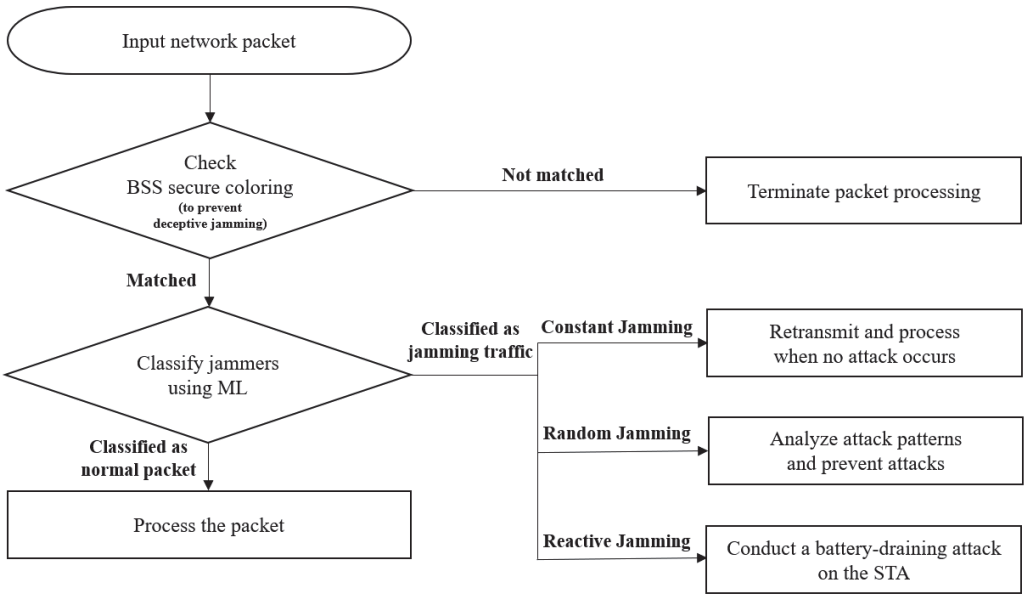

Figure 2. Flowchart of the JCED mechanism

JCED의 세부 동작 flow는 Fig. 2와 같다. Fig. 2에 따르면 하나의 STA이 다른 STA에게 패킷을 송신할 때, 수신 측에서는 BSS coloring을 확인하여 OBSS에서 발생하는 불필요한 신호를 필터링한다. 만약 다른 BSS coloring을 가진 패킷이 입력되었을 경우, STA은 해당 패킷을 간섭으로 분류하고 처리하지 않는다. 또한 이 과정은 공격자가 보내는 패킷을 필터링할 수 있으므로 deceptive 재머에 대한 사전 예방 기술이기도 하다.

또한 지능형 재머가 BSS coloring을 위조할 때 JCED에서는 프레임 바디에 암호화된 BSS secure coloring으로 데이터의 무결성을 검증한다. JCED의 Wi-Fi 패킷 프레임 구조는 Fig. 3과 같다.

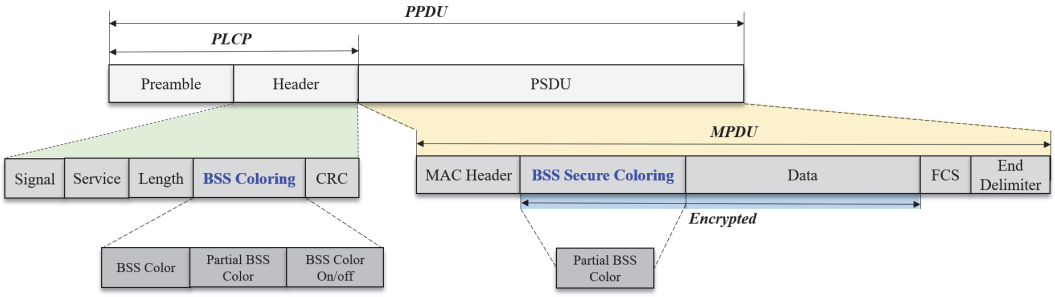

Figure 3. Wi-Fi packet frame structure

물리 계층의 프로토콜 데이터 단위 (PPDU, Physical Protocol Data Unit)은 물리 계층 수렴 처리 (PLCP, Physical Layer Convergence Protocol)와 PLCP Service Data Unit (PSDU)로 구성되어 있다 [24]. 또한 PLCP는 시그널 (signal), 서비스 (service), 길이 (length), 순환 중복 검사 (CRC, Cyclic Redundancy Code)를 포함하며, PSDU는 MAC (매체 접근 제어, Media Access Control) header, 데이터 (Data), 프레임 검사 시퀀스 (FCS, Frame Check Sequence), 끝 구분 기호 (End delimiter)로 이루어져 있다. 수신기에서는 PLCP preamble과 header 값을 통해 프레임의 예상 지속시간을 계산하여 채널을 감지한다(CCA, Clear Channel Assessment). 802.11ax에서는 PLCP 내 header에 BSS color가 입력되며, BSS coloring은 BSS color, partial BSS color, BSS color disabled로 구성된다 [25]. JCED에서는 header에 평문 형식의 BSS coloring을 입력할 뿐 아니라 PSDU에 암호화된 BSS secure coloring 값을 삽입한다. 암호화 과정에서 높은 안정성과 속도를 보장하는 AES (Advanced Encryption Standard) 알고리즘을 사용하였다. AES는 대표적인 대칭형 알고리즘으로, 128 비트의 암호화 블록과 128, 192, 256 비트의 키 길이를 지원한다. 연산 리소스가 제한된 장치에서 암호 알고리즘을 적용할 경우, AES를 경량 암호로 변경하여 소모

자원을 최소화할 수 있다. BSS coloring을 사용하여 1차 검증이 진행된 후 BSS secure coloring을 복호화해 BSS coloring과 대조하는 2차 검증 과정을 통해 정확한 BSS coloring을 확인하고 패킷의 무결성을 검증할 수 있다. 이때 BSS secure coloring에는 partial BSS coloring만 포함되어 일부 데이터만으로 BSS coloring을 파악할 수 있다. 즉 프레임 header 내 BSS coloring 값을 통해 처리 대상 패킷만을 신속히 결정하여 처리 효율을 높이고 body 내 암호화되어 있는 BSS secure coloring 값을 교차 검증하여 BSS coloring 위 변조 공격에 대응한다.

이후, JCED에서는 머신러닝 모델을 활용하여 패킷의 공격 여부, 공격 유형을 파악한다. 이때 공격 유형은 constant, random, deceptive, reactive 재머로 분류할 수 있다. Constant 재밍 공격이 발생하면, STA은 공격이 진행되지 않은 시점을 파악하고 해당 시점에 패킷을 처리해 공격을 회피한다. 공격 패킷의 형태가 random 재밍으로 분류될 경우 공격 패턴이 있는지 확인한다. 이때 시계열 데이터를 수집하고 백그라운드에서 동작하고 있는 인공지능 모델에 입력으로 넣어 패턴을 학습한다. 그리고 공격이 중단되는 시점을 예측하여 패킷 재처리를 시도해 공격을 회피한다. 만약 패턴이 발견되지 않는다면, STA의 에너지 효율성을 고려하며 재전송을 시도한다.

Reactive 재밍 공격이 발생하면, STA은 reactive 재머에 대해 배터리 소모 (battery draining) 공격을 수행한다. battery draining 공격을 받은 reactive 재머는 더 이상 패킷을 송신할 수 없게 된다. 이때 battery draining 공격이란 STA이 power saving (PS) 모드로 전환되지 않도록 다량의 패킷을 보내 STA의 가용 자원을 소모하는 기술이다 [26]. 일반적으로 battery draining 공격은 공격자가 대상 노드의 가용성을 파괴하기 위한 공격이다. 그러나 JCED에서는 지능형 공격을 발생시키는 노드에 대한 능

동적인 대응 조치로 battery draining 공격을 역이용한다. STA에서 머신러닝 모델로 reactive 재머를 탐지한 경우, STA은 전원이 연결되어 있는 AP에 battery draining 공격을 요청한다. AP는 reactive jammer를 draining 시킬 수 있는 시그널을 생성하여 reactive jammer의 정상적인 통신이 불가능해질 때까지 시그널을 지속적으로 송신한다. 이러한 대응을 통해 reactive 재머를 빠르게 차단할 수 있으며, 재밍 공격으로 인한 피해를 최소화할 수 있다. STA은 reactive 재머로부터 오는 비정상 패킷을 처리하는 시간을 줄일 수 있으며, 절약한 시간 동안 나머지 정상 패킷을 처리할 수 있다.

Ⅳ. 실험 환경

4.1 JCED 블록 다이어그램

JCED의 성능을 검증하기 위해 ad-hoc network의 가상 AP (virtual AP) 환경에서 STA 간 패킷 송수신 환경을 구축했다. 본 연구에서의 재머는 일반적인 모바일 기기의 배터리 용량인 1000mAh로 가정했다. 정상 STA은 전원이 계속 공급되는 노드와 배터리 전원으로만 동작하는 노드가 혼재되어 있으며, 재머와 STA은 특정 BSS 범위 내에서 BSS coloring이 할당되므로 재머와 STA의 BSS coloring은 서로 같거나 다를 수 있다. STA별 최대 처리량은 32Mbps으로 설정하였다. 실험 환경은 Intel(R) Core(TM) i9-10850K 3.60 GHz CPU, 32.0 GB RAM에서 python으로 구현했으며, JCED의 블록 다이어그램은 Fig. 4와 같다.

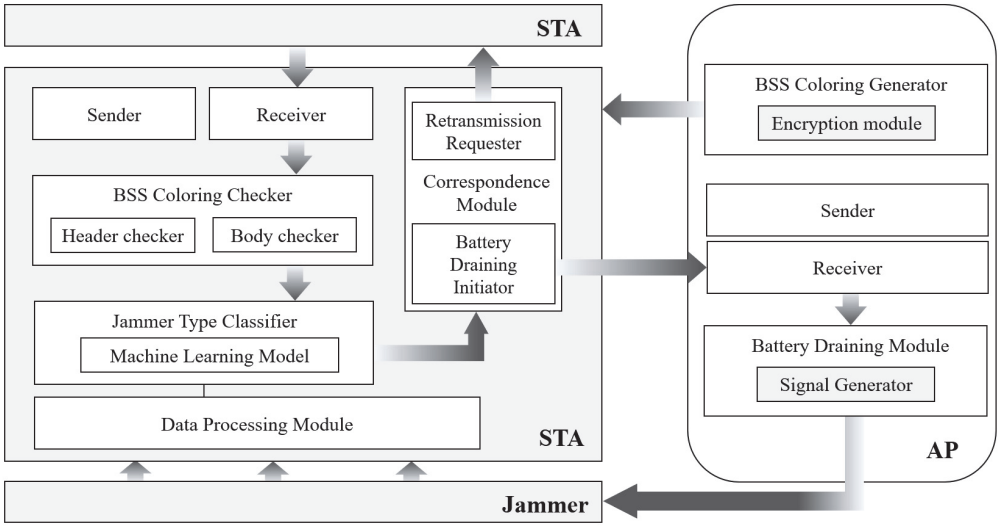

Figure 4. Block diagram of the simulation

STA은 송신기(sender), 수신기(receiver), BSS coloring checker, jammer type classifier, data processing module, defense module로 구성된다. BSS coloring checker는 패킷 프레임 내 BSS coloring와 BSS secure coloring를 확인하는 header 및 body checker를 각각 포함한다. BSS coloring을 확인한 후, jammer type classifier를 통해 머신러닝 모델 기반 다중 분류를 진행한다. 정상 패킷으로 분류한 경우 패킷을 처리하고, 정상 패킷이 아닌 경우 대응 모듈 (correspondence module)을 통해 대응한다. Correspondence module은 재전송 컨트롤러 (retransmission requester)를 이용해 재머 패턴을 고려하여 정상 노드에 재전송을 요청한다. 또한 battery draining initiator 정보를 AP에 전달하여 재머에 능동적으로 대처한다. AP도 STA과 동일하게 sender와 receiver를 가지며 STA에 BSS coloring을 전달한다. 만약 STA으로부터 battery draining 정보를 전달받으면, 신호 생성기 (signal generator)를 통해 공격 신호를 생성한 후 타겟 노드에 battery draining 공격을 수행한다.

4.2 평가 데이터셋 및 비교 모델

패킷 프레임의 header와 body 내 데이터 페이로드를 구성하기 위해 WSN-DS [28]을 활용하였다. WSN-DS 데이터셋은 무선 센서 네트워크 환경에서 널리 사용되는 데이터셋으로, 정상 (normal), 블랙홀 (blackhole), 그레이홀 (grayhole), 플로딩 (flooding), 스케줄링 (scheduling) 공격으로 구성된다 [29]. 이때, blackhole 공격은 random 재머의 특성을 가진다. Grayhole 공격은 일부 패킷을 지속적으로 드랍 (drop)하는 점에서 constant 재머와 유사하다. Flooding 공격은 채널 결정에 혼란을 주어 에너지를 소모하게 하는 공격으로 reactive 재머와 비슷한 속성을 가지며, Scheduling 공격은 deceptive 재머의 특성을 보인다 [15]. 본 연구에서는 WSN-DS 라벨을 각각 random, constant, reactive, deceptive 재머로 라벨링하여 실험하였다. WSN-DS 데이터셋의 feature는 Table 2와 같다 [28].

또한 JCED의 성능을 효과적으로 비교하기 위해 CDCA [14]를 종래모델로 사용했다. CDCA는 reactive 재머의 특성을 정의하고, 특성을 기반으로 공격 여부를 판단하는 feature 기반의 탐지 방법이며. 탐지 이후 대응 조치를 포함한다.

Table 2. Features of the WSN-DS dataset

Feature	Description
Node ID	노드 식별자
Time	노드의 현재 시간
Is CH?	노드의 CH (Cluster Head) 여부
Who CH?	CH의 ID
RSSI	수신된 신호 강도

Distance to CH	CH와 노드 사이의 거리
Max distance to CH	CH와 노드 사이의 최대 거리
Average distance to CH	CH와 노드 사이의 평균 거리
Current energy	노드의 현재 에너지
Energy consumption	이전 라운드에서 소비한 에너지 양
ADV_CH send	노드로 보낸 Advertise CH의 브로드캐스트 메시지 수
ADV_CH receives	CH에서 수신한 Advertise CH 메시지 수
Join_REQ send	참여 요청 메시지 수
Join_REQ receive	CH가 노드로부터 수신한 참여 요청 메시지 수
ADV_SCH send	노드에 전송된 Advertise TDMA 스케줄 broadcast의 수
ADV_SCH receives	CH로부터 수신된 TDMA 스케줄 메시지 수
Rank	TDMA 스케줄 내에서 노드의 순위
Data sent	센서에서 채널로 전송된 데이터 패킷 수
Data received	CH에서 수신한 데이터 패킷 수
Data sent to BS	BS (Base Station)에서 전송된 데이터 패킷 수
Distance CH to BS	CH와 BS 사이의 거리
Send Code	클러스터 전송 코드
Attack Type	노드의 유형

4.3 평가 지표

실험에서 활용한 평가 지표는 탐지 정확도 (detection accuracy), 유효 처리량 (effective throughput), 재전송 횟수 (number of retransmissions), 에너지 소모율 (energy consumption)이다. 이때 detection accuracy는 Eq. (1)로 정의된다.

$$Detection\ Accuracy(\%) = \frac{Number\ of\ nodes\ that\ correctly\ classified\ jammer\ types}{Number\ of\ total\ nodes} \times 100. \quad (1)$$

Detection accuracy는 전체 STA 개수 중 정상 STA을 정상으로 분류한 경우와 공격 STA을 공격으로 분류한 경우의 비율을 구한 것이다. CDCA에서는 재머의 특성에 따른 임계치와 위치 일관성 평가를 통해 노드의 유형을 분류한다. 반면 JCED에서는 머신러닝 모델을 활용해 노드의 유형을 분류한다.

$$Throughput(bps) = \frac{The\ amount\ of\ data\ transmitted\ successfully\ (bits)}{Time\ taken\ to\ transmit\ the\ entire\ packet\ (second)}. \quad (2)$$

$$Effective\ Throughput(bps) = \frac{The\ amount\ of\ normal\ data\ transmitted\ successfully\ (bits)}{Time\ taken\ to\ transmit\ the\ entire\ packet\ (second)}. \quad (3)$$

Throughput과 effective throughput은 각각 Eq. (2)와 (3)으로 정의된다. Throughput은 성공적으로 전송한 모든 데이터를 측정한다. 그러므로 정상 STA에서 보낸 패킷 외에도 재머가 송신한 패킷이 일부 throughput에 합산된다. 그에 반해 본 논문에서 제안한 effective throughput은 정상 STA

에서 보낸 패킷의 전송률만을 고려하여 실제 시스템 스루풋을 파악할 수 있다. 재전송 횟수는 패킷을 처리하기 위해 필요한 재전송 횟수의 평균을 측정하였다. Wi-Fi 환경에서 STA은 최대 8회까지의 재전송을 허용하므로, 실험에서도 최대 8회의 재전송을 모델링했다. Energy consumption은 각 STA이 패킷 송수신할 때의 사용한 에너지와, 데이터 처리 과정에서 소모하는 에너지량을 측정하였다. 소모한 에너지의 크기는 유한 상태 기계(FSM, Finite State Machine)에 따라 Table 3과 같이 정의하였다.

Table 3. Energy consumption value for each state

State	Value
TX	100mW
RX	25mW
IDLE	5mW

Table 3에 따르면 JCED의 state는 TX, RX, IDLE로 정의할 수 있다. TX는 STA이 다른 STA으로 패킷을 전송하는 상태이다. RX는 패킷을 수신하고 처리하는 상태를 의미한다. IDLE은 STA에서 송수신을 위해 대기하는 상태를 뜻한다. 일반적인 패킷의 TX power는 100mW, RX power는 25mW, IDLE Power는 5mW로 가정하였다. BSS coloring 및 BSS secure coloring 모델에서는 BSS coloring과 BSS secure coloring indicator 송신을 위해 각각 1mW와 2mW를 추가적으로 소모한다. 만약 패킷이 다른 BSS coloring을 가지고 있다면 패킷의 일부만 확인하고 처리하지 않기 때문에 5mW만을 사용한다.

Ⅴ. 성능 평가

본 장에서는 네트워크 트래픽 데이터셋 기반의 시뮬레이션 프레임워크에서의 JCED 성능을 평가한다. 먼저 STA 개수 변화에 따라 CDCA와 JCED의 성능을 비교한다. 그리고 단일 유형 대응과 다중 유형 대응에서의 JCED 성능을 평가한다. 마지막으로 공격 시도율 (AAR, Attack Attempt Rate)이 변화할 때 BSS coloring을 사용하지 않는 CDCA와 일반적인 802.11ax 표준의 BSS coloring, 제안하는 BSS secure coloring를 사용하는 JCED의 성능을 비교 분석한다. 모든 결과는 시뮬레이션을 10,000회 반복하여 평균값으로 비교하였다.

5.1 노드 증가에 따른 효율성

STA 개수 변화에 따른 평가에서는 STA이 5개부터 최대 50개까지 5개씩 증가할 때 CDCA와 JCED의 성능을 비교한다. Jammer to STA ratio (JSR)에 따라 JSR(Low), JSR(Med), JSR(High)로 구분해 실험하였으며, 각각 20%, 50%, 80%로 설정했다. 이때 재머의 세부 유형은 고르게 분포한다고 가정했으며, 각 STA은 동일한 traffic rate으로 패킷을 송수신한다. 이때 traffic rate이란 통신 과정에서 보내는 패킷의 개수를 의미한다. 또한 모든 재머는 동일한 AAR을 가진다고 가정한다.

실험에서 JCED는 RF 모델을 활용해 각 타입의 데이터를 동일하게 샘플링한 상태에서 이진분류 정확도를 측정하였다.

RF 알고리즘은 다수의 decision tree를 생성하고 이를 학습하는 앙상블

학습 방법으로, 의사 결정에 쓰이는 특성들을 랜덤하게 선택하는 모델이다. RF 모델은 분류와 회귀 문제에 활용되며, 대용량 데이터를 처리하기에 용이하다. 또한 중요한 특징을 선정하여 분류 성능을 최적화할 수 있다. 본 실험에서는 RF의 파라미터 중 n_estimator와 max_depth 값을 세팅하였다. n_estimator는 숲에 있는 나무의 수를 의미하며 50으로 설정하였고, 트리의 최대 깊이를 의미하는 max_depth는 0으로 설정했다. 또한, 학습 데이터와 평가 데이터의 비율을 7:3으로 나누었다.

CDCA도 JCED와 동일한 환경에서 reactive 재머 탐지 정확도를 측정했다. JSR에 따른 CDCA과 JCED의 탐지 정확도는 Fig. 5와 같다.

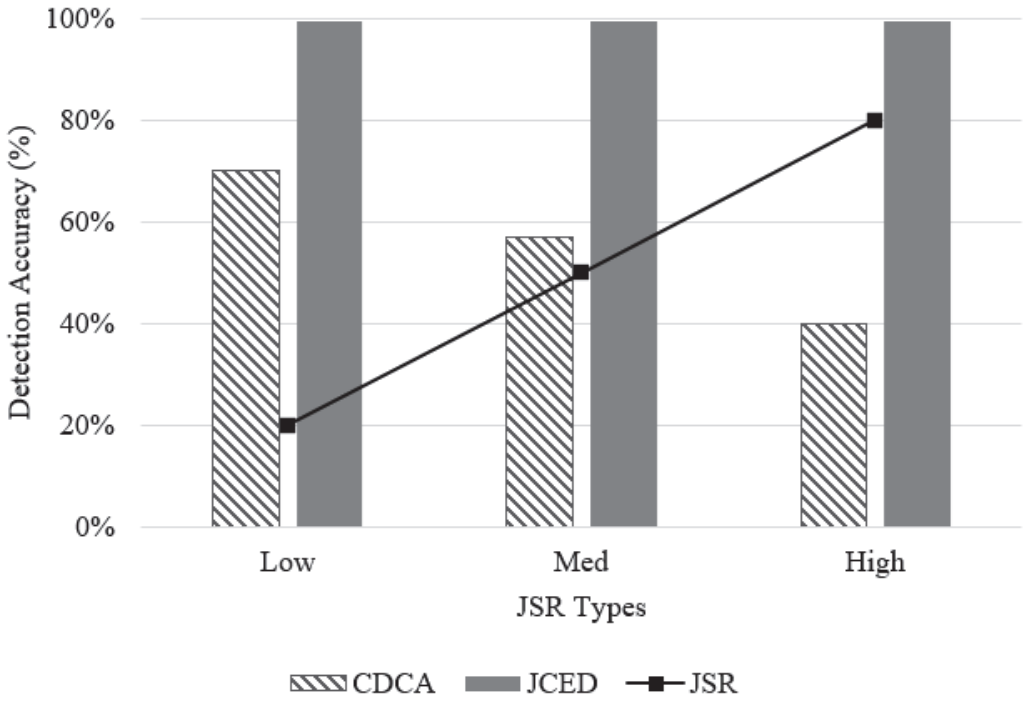

Figure 5. Detection accuracies of the CDCA and JCED algorithm

CDCA는 reactive 재머의 고유한 feature를 활용해 공격을 탐지하고 대응

한다. 그러므로 재머의 비율이 높아질수록 탐지하지 못하는 공격의 수가 증가하게 되고 정확도는 점차 낮아진다. 그러나 JCED는 random forest 모델에서 공격 여부를 정확하게 판단할 수 있고, 재머 유형도 98.16%의 정확도로 분류할 수 있다.

CDCA와 JCED의 시간 복잡도는 Table 4와 같다. 다양한 트래픽 환경에서 CDCA와 JCED의 시간 복잡도를 평가하기 위해 트래픽 크기에 따른 지연 시간을 측정하고, 각 트래픽 사이즈의 이름을 Low (13MB), Med (26MB), High (39MB)로 설정했다.

Table 4. Comparison of time complexity for jammer detection steps

Time / Model	Traffic Size (MB)	Data Loading & Preprocessing (sec)	Model Training (sec)	Model Inference (sec)
CDCA	Low (13MB)	0.1457	-	0.7228
	Med (26MB)	0.2690	-	1.4810
	High (39MB)	0.4152	-	2.2403
JCED	Low (13MB)	0.2059	4.3571	0.2611
	Med (26MB)	0.3712	9.9088	0.5509
	High (39MB)	0.5725	16.7505	0.8955

Table 4에 따르면, 데이터 로딩 시간은 CDCA가 JCED보다 약 1.4배 빠르다. 그 이유는 머신러닝을 위한 전처리 과정을 따로 포함하고 있지 않기 때문이다. 또한 CDCA는 학습 과정도 필요하지 않다. 그에 비해 JCED는

전처리 과정과 학습 과정이 포함되면서 분류까지의 총 시간은 늘어난다. 그러나 학습 과정은 백그라운드에서 진행되기 때문에 실제 환경에서는 큰 영향을 받지 않는다. 뿐만 아니라, CDCA는 inference 단계에서 관리자가 사전에 설정한 룰셋과 임계치에 따라 비교해야 하지만, JCED는 학습된 모델을 활용해 분류하기 때문에 더 짧은 탐지 시간을 가지며, 재머 분류 정확도도 더 높다. 즉 CDCA를 사용하는 것보다 JCED를 사용하는 것이 모든 트래픽 환경에서 권장된다.

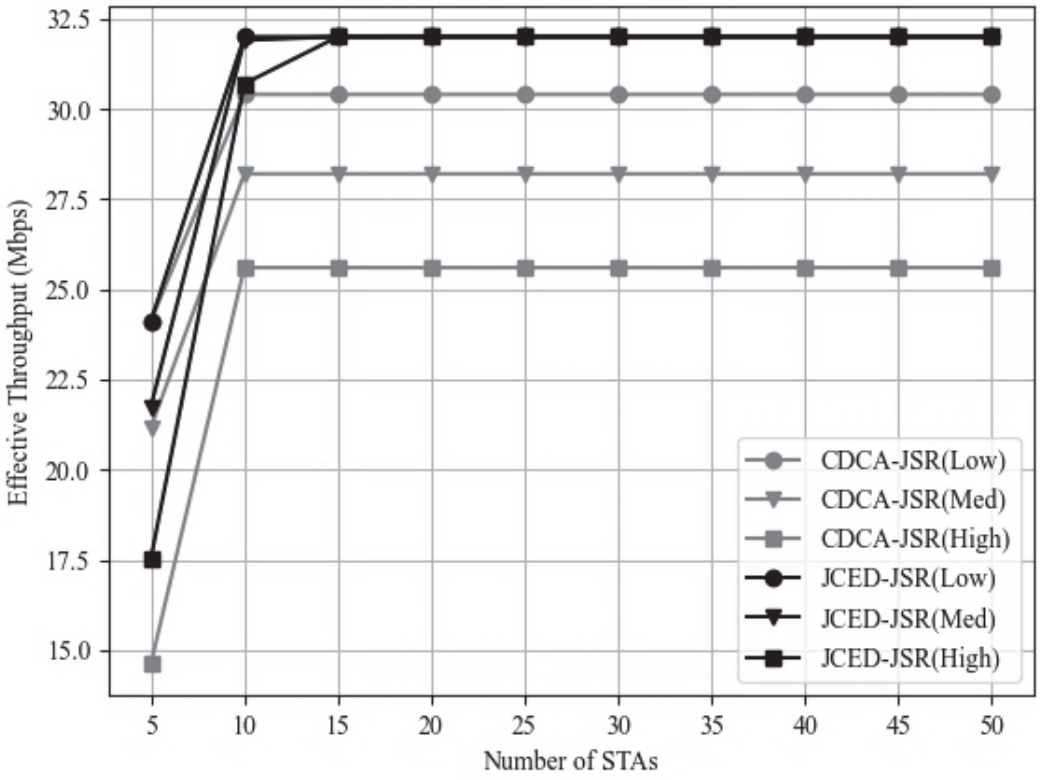

Figure 6. Performance evaluation results of effective throughput

Fig. 6은 STA 개수 변화에 따른 effective throughput을 나타낸 것이다.

일반적인 네트워크 throughput 지표에서는 재밍 신호를 처리했어도 정상 패킷과 동일하게 측정된다. 그렇기 때문에 CDCA의 공격 탐지 성능이 낮아도 스루풋이 좋은 것처럼 보인다. 그러나 effective throughput에서는 측정 지표에서 비정상 패킷을 제외하기 때문에 정상 패킷에 대한 스루풋이 측정된다. 따라서 CDCA의 경우 최댓값보다 낮은 지점에 effective throughput이 고정된다. 또한 JSR이 클수록 더 낮은 값을 가진다. 그에 반해 JCED에서는 공격을 정확히 판단해 회피 및 대응하기 때문에 JSR과 관계없이 effective throughput이 일정한 처리율로 수렴하며, 정상 패킷을 올바르게 처리하므로 CDCA보다 스루풋이 높다.

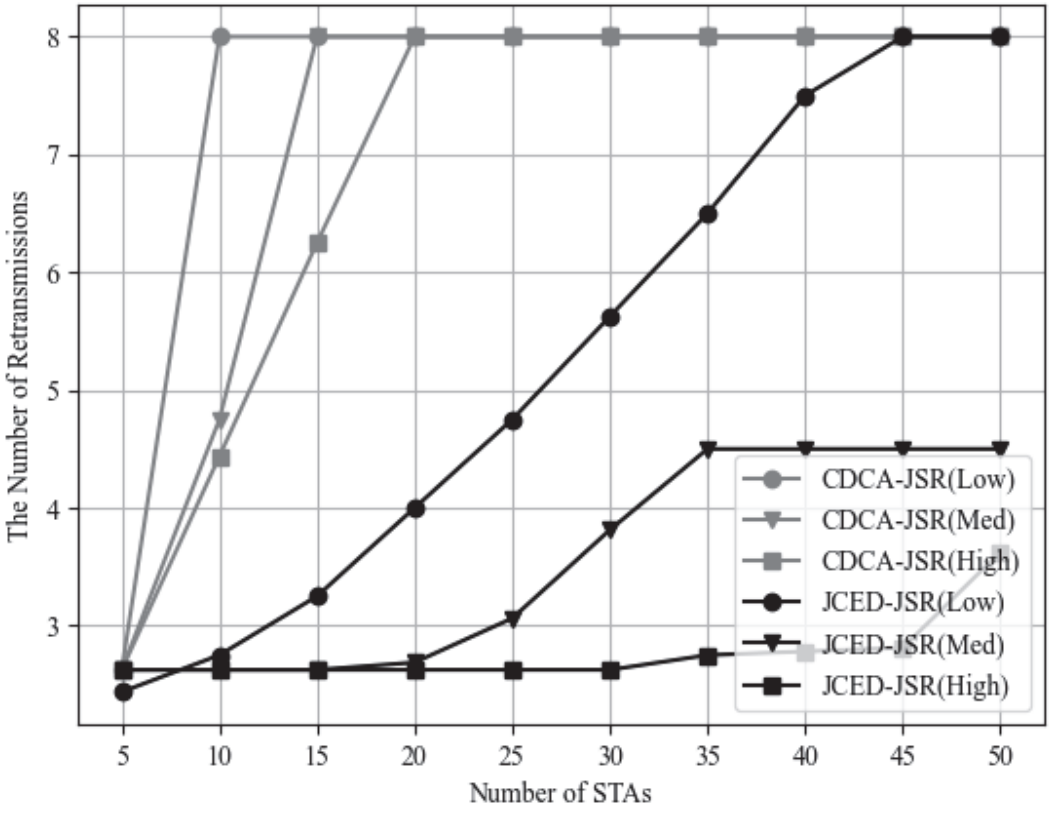

Figure 7. Performance evaluation results of retransmission

Fig. 7은 STA 개수 증가에 따른 재전송 횟수를 측정한 것이다. Fig. 7에 따르면 JSR이 낮을수록 상대적으로 정상 노드의 수가 많아지기 때문에 JSR(Low) 환경에서 재전송 횟수가 증가한다. 기본적으로 STA 수가 많아지면 normal STA들의 contention과 collision이 많아져서 재전송으로 인한 delay가 커진다. 이 시뮬레이션 조건에서는 재머가 많아지면 normal STA 수가 상대적으로 작아지는 효과와 JCED의 defense 효과가 나타난 것이다. 그러므로 JSR(Low)일 때가 JSR(High) 보다 재전송 횟수가 높아 delay가 더 크다. CDCA에서는 재머의 개수가 증가함에 따라 Low, Med, High 환경에서 모두 재전송 횟수가 급격하게 증가하는 형태를 띄지만, JCED는 재머의 개수가 증가해도 CDCA 대비 재전송 횟수가 천천히 증가한다.

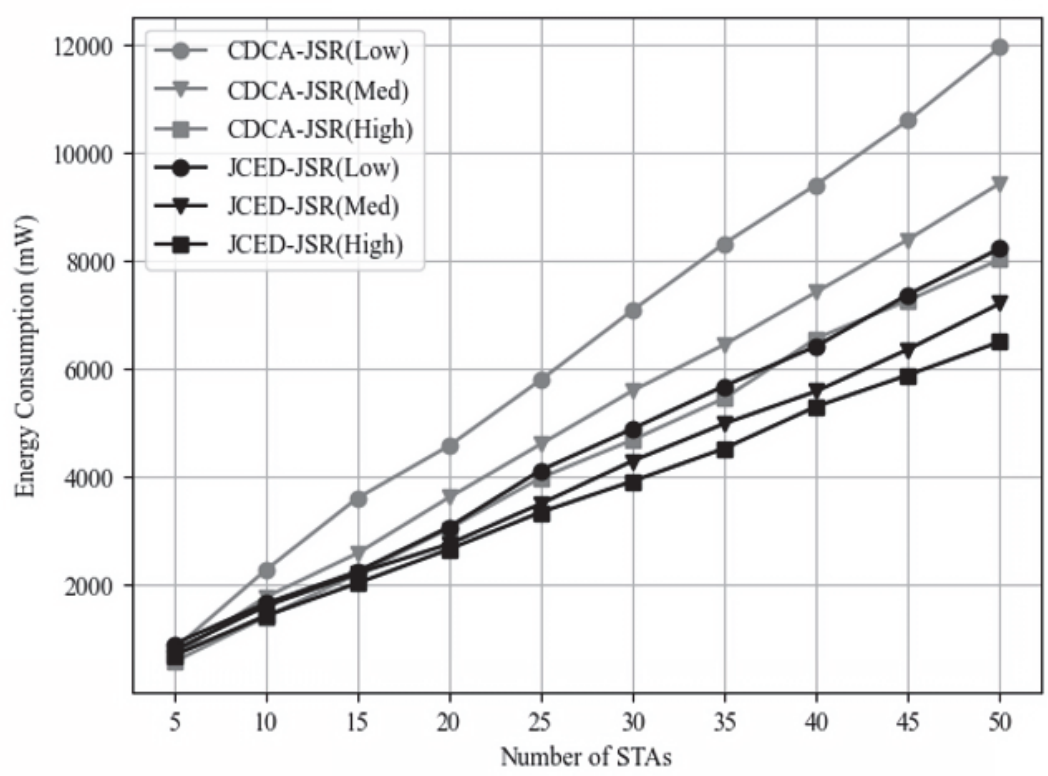

Figure 8. Performance evaluation results of energy consumption

Fig. 8은 STA 개수 증가에 따른 energy consumption을 측정한 것이다. Fig. 8에 따르면 CDCA는 패킷을 처리하는 과정에서 오탐율 증가로 인해 RX 파워 소모량이 증가한다. 따라서 전체 에너지 소모량이 커지고, 특히 재전송이 많은 JSR(Low)에서의 에너지 소모량이 높다. JCED는 BSS coloring을 확인하는 과정에서 오버헤드가 발생한다. 또한, reactive 재머를 battery draining 시킬 때 하나의 노드 당 최대 1000mAh의 에너지를 소모하기 때문에 일부 환경에서는 CDCA보다 높은 에너지 소모율을 보인다. 그러나 JCED는 비정상 패킷을 필터링하기 때문에 RX 소모량이 줄어들어 전반적인 에너지 소모량은 종래 모델보다 작은 형태를 띈다. 또한 CDCA

와 JCED 모두 JSR이 높을수록 정상 노드의 비율이 줄어들기 때문에 High에서 에너지 소모량이 가장 작다. 즉 effective throughput, retransmission, energy consumption 관점에서 JCED의 성능이 CDCA보다 개선되었으며, JSR(Low), JSR(Med), JSR(high) 환경에서 모두 나은 성능을 보였다.

5.2 TL 변화에 따른 효율성

트래픽 부하 (TL, Traffic Load) 변화에 따른 효율성 평가에서는 TL이 증가할 때 CDCA와 JCED의 성능을 분석한다. Table 5는 802.11ax 환경에서 단일 공간 스트림에 대한 변조 및 코딩 체계를 나타낸 표이다 [27].

Table 5. 802.11ax modulation and coding schemes

MCS Index	Modulation Type	Coding Rate	Data Rate (Mbit/s)			
			20MHz Channels		40MHz Channels	
			1600 NS GI	800 NS GI	1600 NS G1	800 NS G1
0	BPSK	1/2	8	8.6	16	17.2
1	QPSK	1/2	16	17.2	33	34.4
2	QPSK	3/4	24	25.8	49	51.6
3	16-QAM	1/2	33	34.4	65	68.8
4	16-QAM	3/4	49	51.6	98	103.2
5	64-QAM	2/3	65	68.8	130	137.6
6	64-QAM	3/4	73	77.4	146	154.9
7	64-QAM	5/6	81	86.0	**163**	172.1

Table 5에 따르면 Wi-Fi 6 표준 내 40MHz 채널 (1600ns Guard Interval (GI)), 64-직교 진폭 변조 (QAM, Quadrature Amplitude Modulation), coding rate 5/6 환경에서의 최대 data rate은 163Mbit/s이다. 따라서 이 중 절반에 해당하는 80Mbps를 최대 TL로 설정했다. 정상 노드의 개수를 5개로 고정하고 JSR에 따라 재머의 개수를 늘려 실험하였으며,

JSR(Low)는 1개, JSR(Med)를 3개, JSR(High)를 5개로 설정했다. 5.1절과 동일하게 JCED는 random forest 모델을 활용해 각 타입의 데이터를 동일하게 샘플링한 상태에서 이진분류 정확도를 측정하였다. CDCA도 동일한 환경에서 reactive 재머 탐지 정확도를 측정했다.

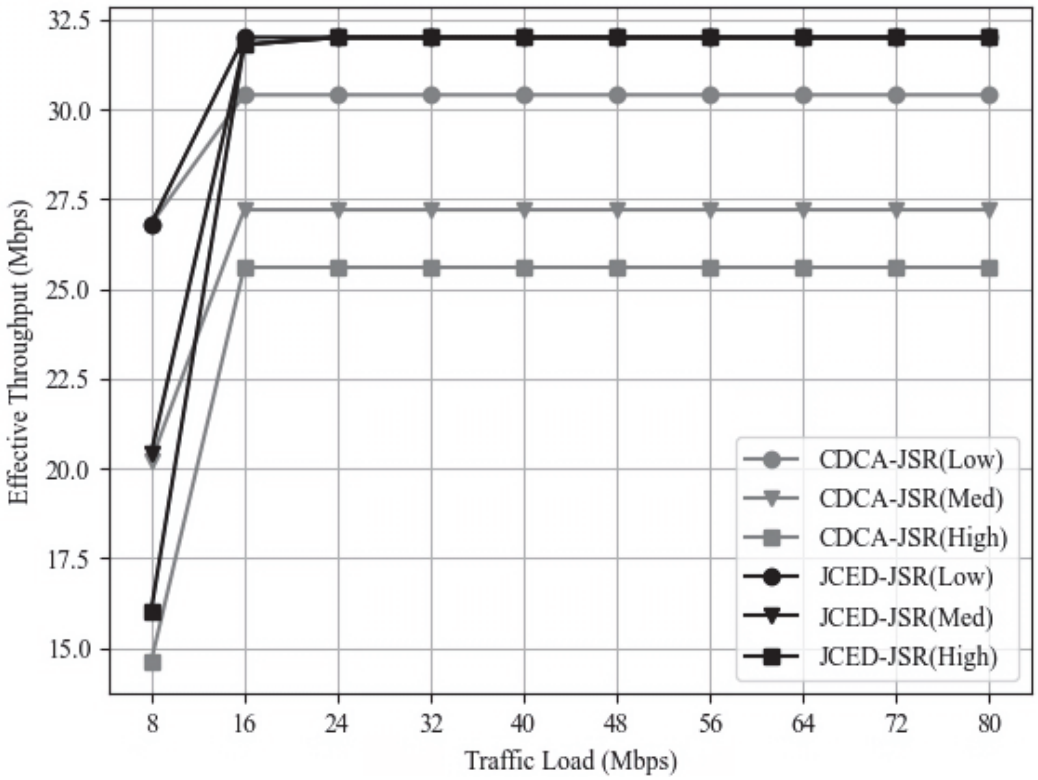

Figure 9. Performance evaluation results of effective throughput

Fig. 9는 TL 변화에 따른 effective throughput을 나타낸 그래프이다. TL이 증가함에 따라 CDCA와 JCED의 effective throughput은 특정 값으로 수렴하며, JSR이 낮을수록 높은 값을 가진다. JCED는 재머의 유형을 세부적으로 탐지하고, 적응적으로 대응하기 때문에 모든 JSR 환경에서

CDCA보다 높은 effective throughput을 가진다.

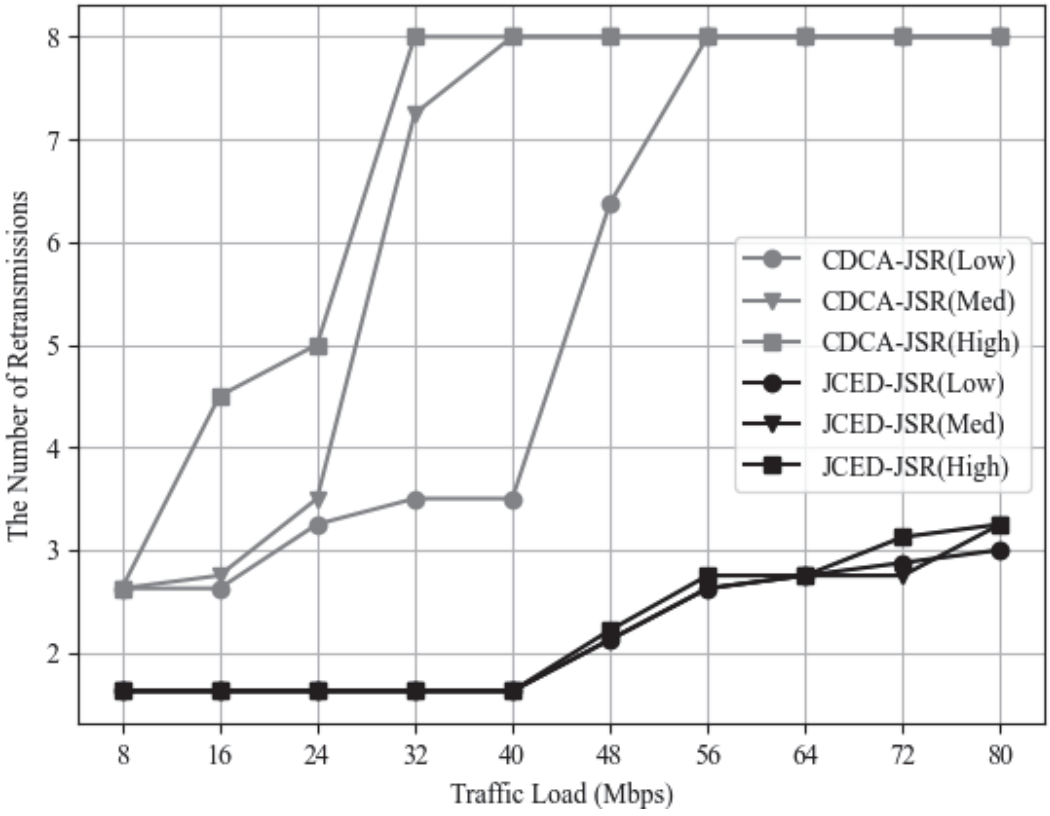

Figure 10. Performance evaluation results of retransmission

Fig. 10은 TL 변화에 따른 재전송 횟수를 나타낸 그래프이다. Fig. 10에 따르면 JSR이 높을수록 공격 노드의 수가 증가하기 때문에 JSR(High) 환경에서 재전송 횟수가 가장 높다. CDCA의 경우, JSR(Low) 환경에서도 reactive 재머만 탐지 및 대응할 수 있기 때문에 TL 증가에 따라 재전송 횟수 증가폭이 크다. 그러나 JCED를 활용하면 같은 TL에서 상대적으로 적은 재전송만으로도 패킷을 처리할 수 있다.

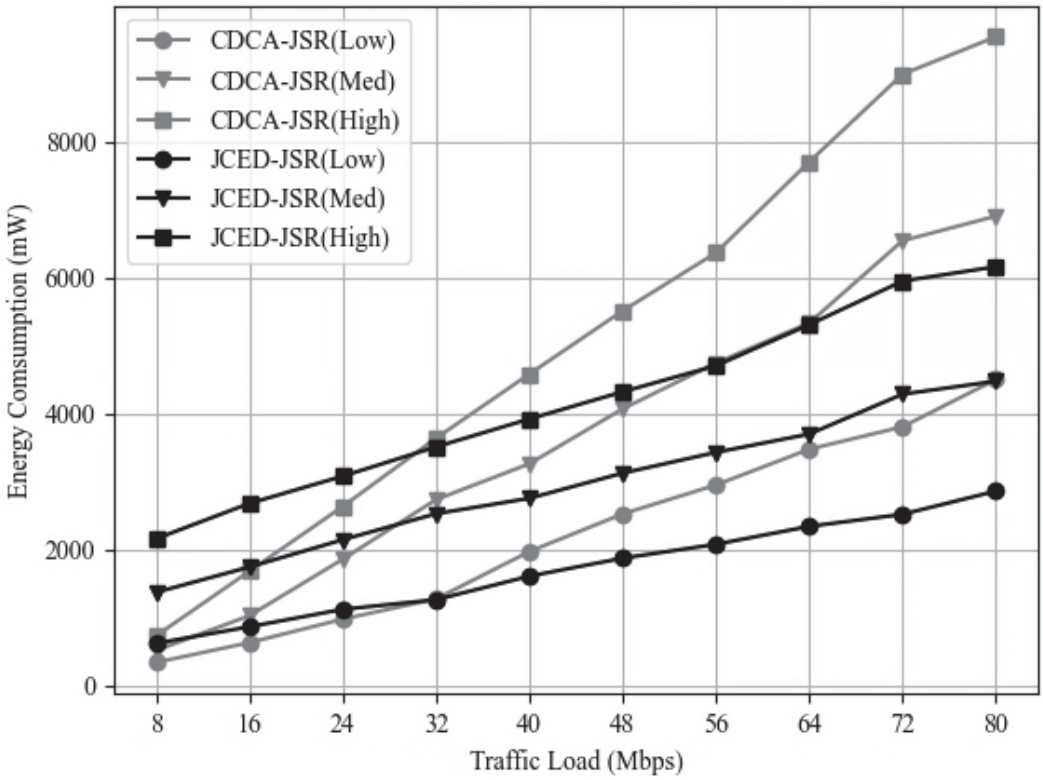

Figure 11. Performance evaluation results of energy consumption

Fig. 11은 TL 변화에 따른 energy consumption을 측정한 것이다. CDCA는 패킷을 처리할 때 공격 패킷을 정확히 분류하지 못하기 때문에 에너지 소모율이 증가하며, 재전송이 많은 JSR(High)에서 값이 가장 높다. JCED의 경우, battery draining과 같이 공격에 대응하는 과정에서 일부 에너지를 소모하지만, CDCA보다 적은 에너지만으로도 패킷을 처리할 수 있다.

즉 TL이 변화하는 환경에서도 JCED의 효율이 CDCA보다 개선되었으며, JSR(Low), JSR(Med), JSR(high) 환경에서 모두 나은 성능을 보였다.

5.3 재머 유형별 대응에 따른 효율성

JCED은 재머 유형별로 다른 대응 조치를 취한다. 단일 유형 대응 방식의 성능을 평가하기 위해 Table 6과 같이 케이스를 나누어 실험하였다.

Table 6. Detection and defense capability of countermeasure cases

Jammer Type	Detection and Defense Capability					
	CDCA	JCED (Constant)	JCED (Random)	JCED (Deceptive)	JCED (Reactive)	JCED (All)
Constant Jammer	X	O	X	X	X	O
Random Jammer	X	X	O	X	X	O
Deceptive Jammer	X	X	X	O	X	O
Reactive Jammer	O	X	X	X	O	O

CDCA는 reactive 재머만을 탐지하고, 해당 패킷을 필터링하는 방식이며, JCED(Constant), JCED(Random), JCED(Deceptive), JCED(Reactive)는 ML 기반으로 재머 유형을 탐지하지만, 특정 유형의 재머에 대해서만 대응하는 모델이다. JCED(All)는 ML 모델을 활용해 모든 재머 유형을 탐지하고, 유형별로 다르게 대응하는 제안 모델이다. 이때 최대 처리량은 50Mbps로 가정하였다. Figs. 12, 13은 각 케이스에서 STA 개수가 증가할 때 effective throughput과 energy consumption을 측정한 결과이다.

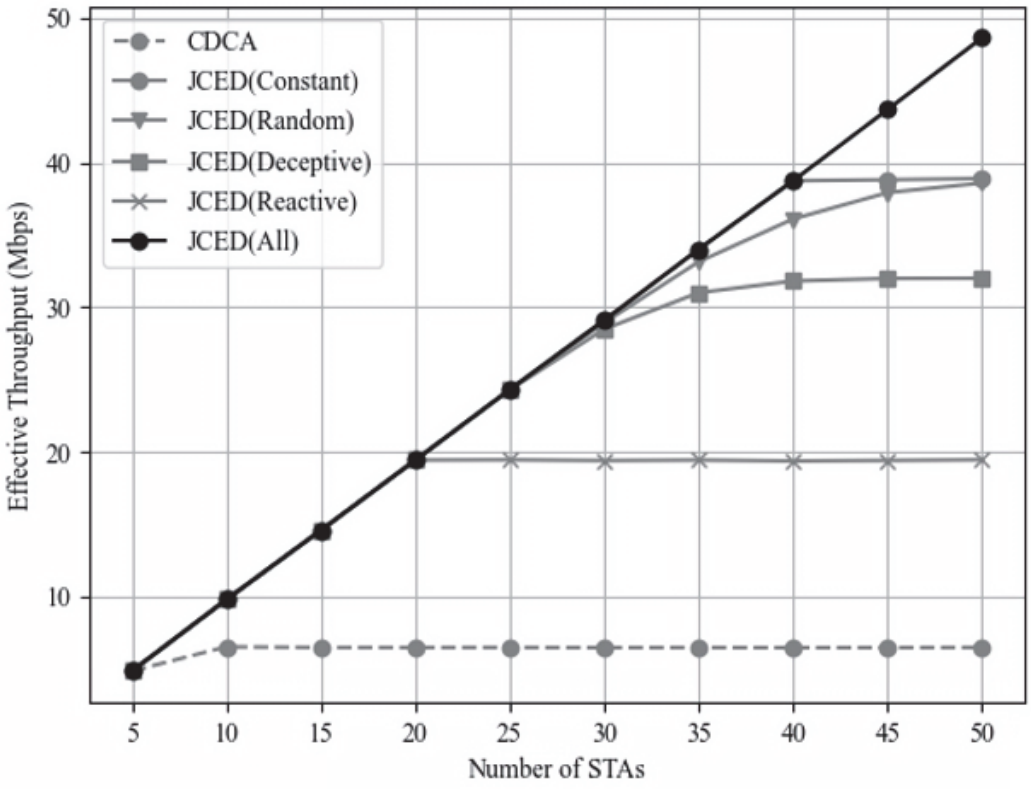

Figure 12. Performance evaluation results of effective throughput

Fig. 12에 따르면 CDCA에서는 reactive 재머만을 탐지하고 방어하는 전략을 취하기 때문에 STA 수가 증가하면 effective throughput이 특정 값으로 수렴한다. 또한 모든 대응 전략을 가지고 있는 JCED의 effective throughput이 가장 높았다. 한편 개별 대응 전략만을 가지고 있는 모델의 경우, 재전송이 가능한 JCED(Constant), JCED(Random)의 effective throughput이 가장 높았다. 그 외에는 BSS coloring으로 필터링이 가능한 JCED(Deceptive)와 battery draining 공격이 가능한 JCED(Reactive) 순으로 높았다.

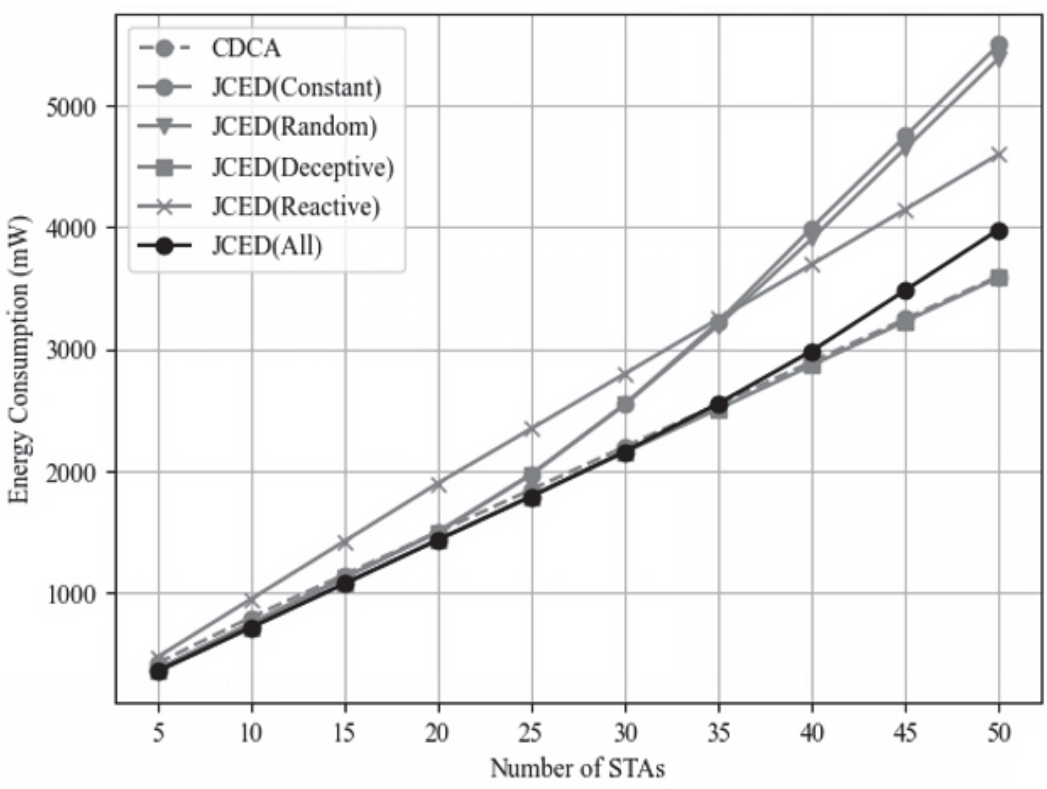

Figure 13. Performance evaluation results of energy consumption

Fig. 13에 의하면, CDCA는 프레임 header와 body에 BSS coloring과 BSS secure coloring 값이 없고, 그로 인한 처리 과정이 생략되기 때문에 적은 에너지 소모량을 보인다. JCED(Deceptive) 의 경우, BSS coloring으로 패킷 필터링이 가능하기 때문에 에너지 소모량이 상대적으로 적다. JCED(Constant) 와 JCED(Random)은 BSS coloring을 통한 필터링이 불가능하고, 재전송 과정에서 추가 에너지를 소모하기 때문에 에너지 소모량이 매우 높으며, JCED(Reactive)에서도 battery draining 공격을 수행하는 과정에서 다른 모델보다 에너지를 많이 소모한다. 즉, JCED가 CDCA뿐만 아니라, 제안모델의 단일 탐지 및 대응 방식과 비교했을 때도 개선된

effective throughput과 energy consumption을 가진다.

5.4 공격 환경에서 분류 및 대응의 효율성

패킷 무결성 공격이 발생했을 때 JCED의 성능을 측정하기 위해 10개의 STA이 존재할 때 AAR의 변화에 따른 effective throughput과 energy consumption을 측정하였으며, 각각 Figs. 14, 15로 시각화하였다.

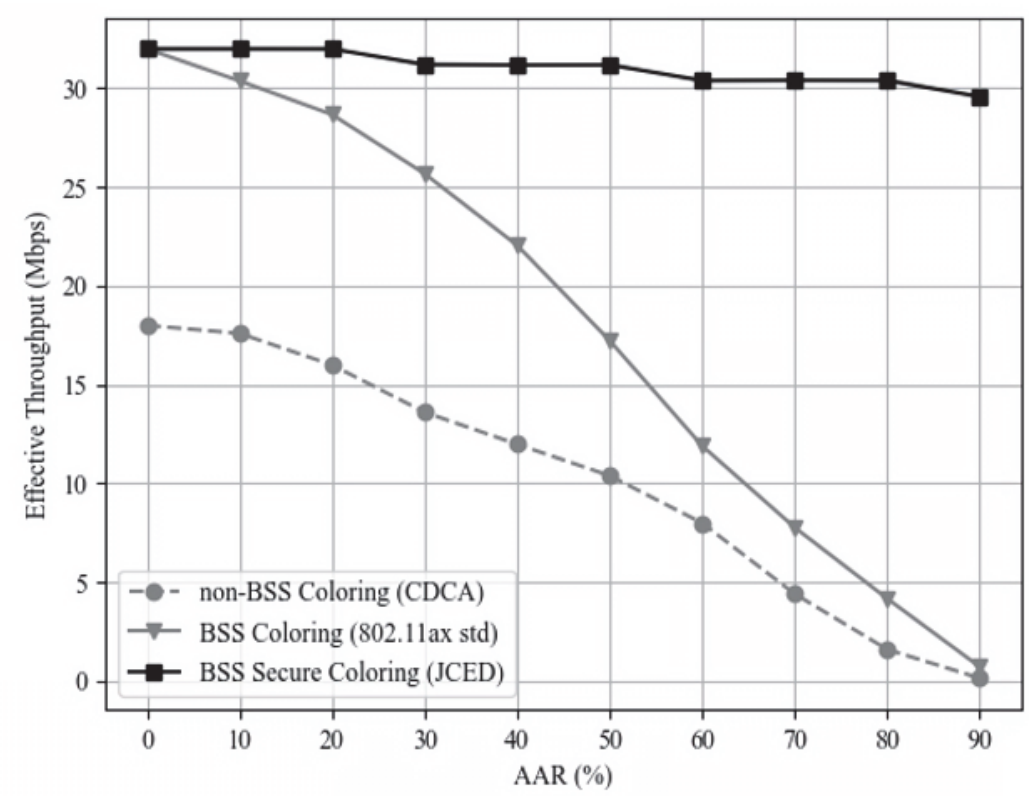

Figure 14. Performance evaluation results of effective throughput

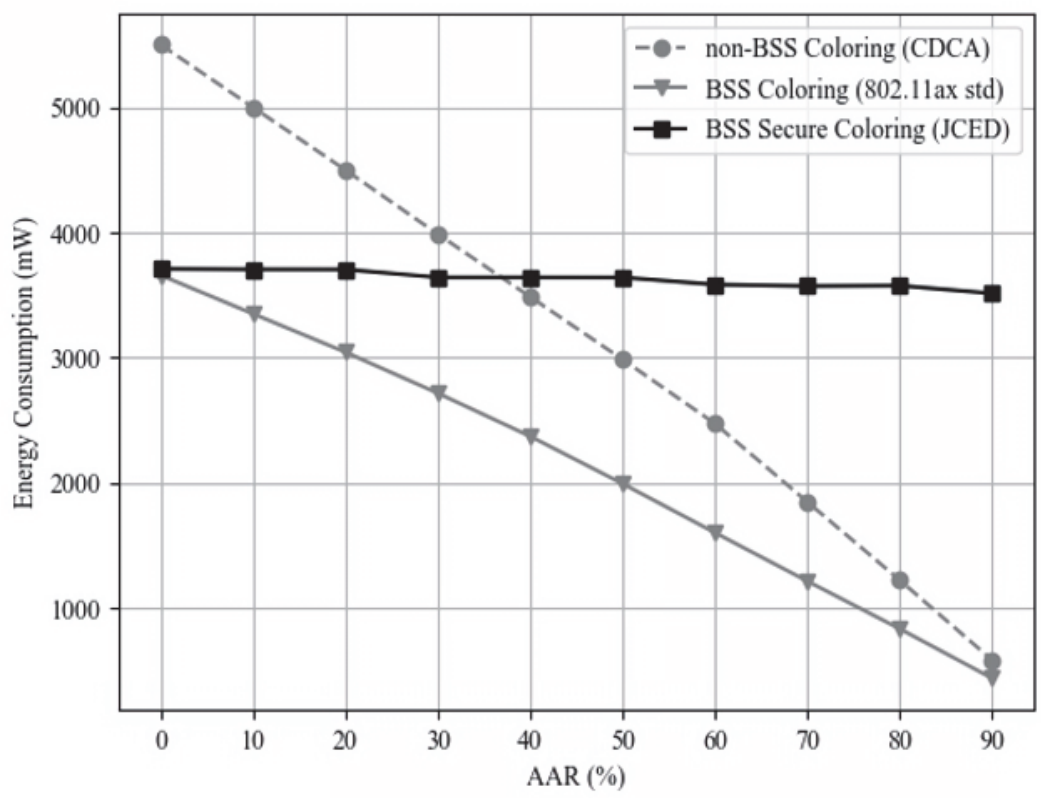

Figure 15. Performance evaluation results of energy consumption

AAR이란 공격 시도율 (Attack Attempt Rate)로 통신 환경에서 공격자가 패킷 무결성을 침해하는 공격을 수행할 확률을 의미한다. AAR은 0%부터 90%까지 변화하며, 0%일 때는 의도적 간섭이 발생하지 않고, 90%일 때 간섭이 가장 크다. AAR에 따른 공격 성공률은 50%의 확률로 가정하였다. STA 간 통신 중 오류가 없을 때의 최대 데이터 생성 속도는 32Mbps인 조건에서 실험했다. 통신 중 무결성 공격으로 패킷이 손상되었다면 정상 패킷으로 판단되어도 처리하지 않으며, effective throughput에 반영되지 않는다.

Figs. 14, 15에 따르면, BSS coloring이 없는 모델(non-bss coloring)에서는 비의도적인 간섭 패킷까지 처리하기 때문에 실제 처리하는 패킷의 수는

점차 감소한다. BSS coloring을 적용하면 의도하지 않은 간섭을 필터링할 수 있지만, AAR의 변경으로 인해 무결성이 파괴된 패킷은 처리할 수 없다. 그러므로 effective throughput과 에너지 소모량이 점차 감소한다. BSS secure coloring 모델은 프레임 header 내 BSS coloring, body에서의 BSS secure coloring을 통해 무결성에 대한 교차 검증이 가능하다. 그러므로 AAR이 증가해도 effective throughput은 크게 감소하지 않으며, 위협에 강인한 특성을 가진다. 실제로 Non-BSS coloring와 비교했을 때 평균 3.05배 높은 effective throughput을 가지며, 에너지 소모량은 13.77%만 증가하였다. 또한 BSS coloring 스킴과 비교했을 때는 72.79% 개선된 effective throughput을 보인다. 즉 JCED를 적용했을 때, non-BSS coloring 스킴과 BSS coloring 스킴을 적용했을 때보다 effective throughput이 높아져 QoS를 개선할 수 있다.

Ⅵ. 결 론

무선 통신의 발전으로 인류는 다양한 서비스를 편리하게 이용할 수 있게 되었지만, 그에 따라 공격자의 공격 방식도 점차 고도화, 세밀화되었다. 특히 재밍 공격은 이용자의 통신을 방해할 뿐 아니라, 지능적인 공격으로 이용자의 시스템을 조종할 수 있다는 점에서 매우 위험하다. 그러나 단일 탐지나 channel 및 frequency hopping 기반의 종래 방식으로는 지능적인 공격을 올바르게 탐지하기 어렵다. 그리고 단일 대응 방식을 적용하기 때문에 효과를 보기 어렵다. 본 논문에서는 머신러닝 모델을 활용하여 재머의 종류를 분류하고, 재머 종류에 따라 다른 대응 방식을 적응적으로 적용하는 JCED를 제안한다. JCED는 일반적인 대응 방식인 회피 외에도 BSS secure coloring과 battery draining 공격을 활용해 대응한다. 따라서 jamming signal이 입력되었을 때 대응을 시작하는 종래 연구들과는 달리 능동적인 방어 기법 적용이 가능하다. 성능 평가 결과에 따르면 JCED는 effective throughput, retransmission, energy consumption 관점에서 CDCA 기법보다 개선된 성능을 보였으며, BSS secure coloring을 통해 deceptive 재밍 공격의 영향을 효과적으로 저감할 수 있었고 프레임 위변조 공격을 예방할 수 있었다. 본 연구에서는 자체 시뮬레이션 안에서 테스트했기 때문에 WSN-DS 데이터셋 내 재밍 공격에 한정하여 실험했다. 향후 연구에서는 실제 STA 간 통신 테스트베드를 구축해 BSS secure coloring 도입으로 인한 오버헤드를 정량적으로 측정하고 이를 최소화하는 방안을 연구할 계획이다. 또한 다양한 재밍 환경에서 JCED를 실험해 지능형 재머의 분류 및 대응 성능을 개선할 계획이다.

참 고 문 헌

[1] MarketsandMarkets, Wi-Fi Market by Component (Hardware, Solution, and Services), Density (High-density Wi-Fi and Enterprise-class Wi-Fi), Location Type (Indoor and Outdoor), Organization Size, Vertical (Education, Retail and eCommerce), and Region (2022 - 2026), https://www.marketsandmarkets.com/Market-Reports/global-wi-fi-market-994.html (accessed 31 August 2022)

[2] Priya, Bhanu, and Jyoteesh Malhotra. "QAAs: QoS provisioned artificial intelligence framework for AP selection in next-generation wireless networks." Telecommunication Systems 76.2 (2021): 233-249.

[3] Vlasios Tsiatsis, Stamatis Karnouskos, Jan Höller, David Boyle, and Catherine Mulligan, Chapter 6 - Security, Internet of Things (Second Edition), Academic Press, 2019, Pages 127-142, ISBN 9780128144350, https://doi.org/10.1016/B978-0-12-814435-0.00018-3.

[4] Vadlamani, Satish & Eksioglu, Burak & Medal, Hugh & Nandi, Apurba. (2016). Jamming attacks on wireless networks: A taxonomic survey. International Journal of Production Economics. 172. 76-94. 10.1016/j.ijpe.2015.11.008.

[5] Sirojiddin Djuraev, Jin-Ghoo Choi, Kyu-Seek Sohn, and Seung Yeob Nam, "Channel hopping scheme to mitigate jamming attacks in wireless LANs", EURASIP Journal on Wireless Communications and Networking." EURASIP Journal on Wireless Communications and Networking 11(2017)

[6] Liu, Yiming, et al. "Novel channel-hopping pattern-based wireless IoT

networks in smart cities for reducing multi-access interference and jamming attacks." EURASIP Journal on Wireless Communications and Networking 2021.1 (2021): 1-19.

[7] Kim, J., Biswas, P. K., Bohacek, S., Mackey, S. J., Samoohi, S., and Patel, M. P. (2021). Advanced protocols for the mitigation of friendly jamming in mobile ad-hoc networks. Journal of Network and Computer Applications, 181:103037.

[8] Yongcheol Kim. (2015). A channel jumping technique for improving fairness performance in a tactical WLAN jamming environment. Journal of the Korean Telecommunications Society, 40(11), 2188-2195.

[9] Il-Gu Lee and Myungchul Kim, "Persistent Jamming in Wireless Local Area Networks: Attack and Defense," Computer Networks, Vol. 109, No. 1, pp. 67-83, Jun. 2016.

[10] So-Hyun Park, Soyoung Joo, and Il-Gu Lee, "Secure Visible Light Communication System via Cooperative Attack Detection Techniques," IEEE Access, Vol.10, pp.20473-20485, Feb. 2022

[11] Pirayesh, Hossein, and Huacheng Zeng. "Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey." IEEE Communications Surveys & Tutorials (2022).

[12] Lall, S., Maharaj, B., and van Vuuren, P. J. (2016). Null-frequency jamming of a proactive routing protocol in wireless mesh networks. Journal of Network and Computer Applications, 61:133 - 141.

[13] Kanika Grover, Alvin Lim, and Qing Yang. 2014. Jamming and anti-jamming techniques in wireless networks: a survey. Int. J. Ad Hoc Ubiquitous Comput. 17, 4 (December 2014), 197 - 215. https://doi.org/10.15

04/IJAHUC.2014.066419

[14] Fadele, A.A., Othman, M., Hashem, I.A.T. et al. A novel countermeasure technique for reactive jamming attack in internet of things. Multimed Tools Appl 78, 29899 - 29920 (2019). https://doi.org/10.1007/s11042-018-6684-z

[15] Ibrahim, Khalid, et al. "Entice to Trap: Enhanced Protection against a Rate-Aware Intelligent Jammer in Cognitive Radio Networks." Sustainability 14.5 (2022): 2957.

[16] Z. Su et al., "Guarding legal communication with smart jammer: Stackelberg game based power control analysis," in China Communications, vol. 18, no. 4, pp. 126-136, April 2021, doi: 10.23919/JCC.2021.04.010.

[17] M. Hachimi, G. Kaddoum, G. Gagnon and P. Illy, "Multi-stage Jamming Attacks Detection using Deep Learning Combined with Kernelized Support Vector Machine in 5G Cloud Radio Access Networks," 2020 International Symposium on Networks, Computers and Communications (ISNCC), 2020, pp. 1-5, doi: 10.1109/ISNCC49221.2020.9297290.

[18] Kasturi, G. S., Ansh Jain, and Jagdeep Singh. "Detection and Classification of Radio Frequency Jamming Attacks using Machine learning." J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl. 11.4 (2020): 49-62.

[19] Arjoune, Youness & Salahdine, Fatima & Islam, Md & Ghribi, Elias & Kaabouch, Naima. (2020). A Novel Jamming Attacks Detection Approach Based on Machine Learning for Wireless Communication.

[20] Liu, Songyi, et al. "Pattern-aware intelligent anti-jamming communication: A sequential deep reinforcement learning approach." IEEE Access 7 (2019): 169204-169216.

[21] Xu, Jianliang, et al. "An intelligent anti-jamming scheme for cognitive radio based on deep reinforcement learning." IEEE Access 8 (2020): 202563-202572.

[22] Joshi, Sarthak, et al. "Dynamic Distributed Threshold Control for Spatial Reuse in IEEE 802.11 ax." 2022 National Conference on Communications (NCC). IEEE, 2022.

[23] Commscope, Wi-Fi 6 fundamentals: Basic Service Set Coloring (BSS Coloring),https://www.commscope.com/blog/2018/wi-fi-6-fundamentals-basic-service-set-coloring-bss-coloring/, 2018 (accessed 31 August 2022)

[24] ShareTechnote, Wi-Fi, http://sharetechnote.com/html/WLAN_FrameStructure.html (accessed 31 August 2022)

[25] Extreme Networks, Learn About BSS Color in 802.11ax: Background, Definition, Set-up, https://www.extremenetworks.com/extreme-networks-blog/what-is-bss-color-in-802-11ax/, 2021 (accessed 1 September 2022)

[26] Lee, Il-Gu, Kyungmin Go, and Jung Hoon Lee. "Battery draining attack and defense against power saving wireless lan devices." Sensors 20.7 (2020): 2043.

[27] Eletronicsnotes, Modulation Coding Schemes, MCS for IEEE 802.11ax, https://www.electronics-notes.com/articles/connectivity/wifi-ieee-802-11/802-11ax-modulation-coding.php (accessed 1 November 2022)

[28] (Dataset) Almomani, I.; Al-Kasasbeh, B.; AL-Akhras, M. WSN-DS: A

Dataset for Intrusion Detection Systems in Wireless Sensor Networks. J. Sens. 2016, 2016, 4731953, doi:10.1155/2016/4731953

[29] Tabbaa, Hiba, Samir Ifzarne, and Imad Hafidi. "An Online Ensemble Learning Model for Detecting Attacks in Wireless Sensor Networks." arXiv preprint arXiv:2204.13814 (2022).

ABSTRACT

Machine Learning-based Jamming Attack Classification and Effective Defense Technique

Sunjin Lee
Department of Future Convergence Technology Engineering
Graduate School of Sungshin University

The fourth industrial revolution has resulted in the intelligent Internet of Things being widely used for home networking applications and smart infrastructure. Consequently, wireless connectivity has become essential in both industrial and daily life applications. Wireless communication is a continuously evolving technology that satisfies the requirements of high speed and ultra-low latency. However, as multiple users utilize a single channel by sharing frequency and time, the quality of service cannot be ensured owing to the interference occurring from a congested network. Additionally, malicious attackers can compromise communication availability or destroy data integrity through jamming attacks, threatening human life and safety. Conventional jamming attack detection and response technology respond to attacks without detecting the type of jammer; therefore, this method exhibits certain limitations in detecting

and defending against an intelligent attack. In this study, we propose a novel jammer classification and effective defense (JCED) algorithm that can classify jamming attack types using machine learning and provide differential responses based on the jamming types. Depending on the jammer type, the JCED algorithm can adaptively select various response methods, ranging from simple retransmission to active battery-draining attacks. The experimental results verify that JCED exhibits 24.9% higher effective throughput and 23.4% lower energy consumption than the countermeasure detection and consistency algorithm (CDCA). Moreover, JCED can improve the effective throughput by an average of approximately three times in comparison with CDCA in an environment with integrity violation attacks. Thus, the JCED can serve as an effective defense mechanism against different types of jamming attacks, ensuring the safety and high throughput of digital information.