이 일 구 교수 지도
석사학위 청구논문

재밍 공격 탐지 및 회피를 위한 머신러닝 기반 협력적 클러스터링 기법

2023

성신여자대학교 대학원
미래융합기술공학과
전 소 은

재밍 공격 탐지 및 회피를 위한 머신러닝 기반 협력적 클러스터링 기법

이 일 구 교수 지도

이 논문을 석사학위논문으로 제출함

2022년 11월

성신여자대학교 대학원

미래융합기술공학과

전 소 은

인 준 서

전소은의 석사학위 논문으로 인준함

2022년 11월

심사위원장 김 성 민 (서명 또는 인)

심 사 위 원 김 경 진 (서명 또는 인)

심 사 위 원 이 일 구 (서명 또는 인)

성신여자대학교 대학원

논 문 개 요

초고속, 초저지연, 초밀집의 5G 무선 네트워크 기술이 보편화되면서 무선 통신 장치를 대상으로 한 재밍 공격의 피해가 증가하고 있다. 특히 3GPP NR에서 핵심 후보 기술로 논의되고 있는 스마트 리피터는 Beyond 5G 네트워크 환경에서 스마트 인프라의 역할을 수행하게 되므로 모바일 재머와 같은 지능형 재머 공격에 쉽게 노출된다. 그러나 종래의 재밍 대응 기술은 단편적이고 지엽적인 정보에 의존한 탐지 방법이어서 정교한 재밍 공격에 대응하기 어렵다. 그리고 최근 기계학습 기반의 탐지 방법이 연구되고 있으나, 특정 노드에 학습이 과중되는 문제가 있으며, 로컬 탐지 결과에 의존하기 때문에 전역적으로 최적의 대응을 하기 어렵다. 본 연구에서는 스마트 리피터와 같이 고정된 노드 환경에서 협력적 재머 탐지를 통해 효율적으로 재머를 회피하는 머신러닝 기반 협력적 클러스터링 (Machine Learning-based Cooperative Clustering, MLCC) 기법을 제안한다. MLCC는 스마트 리피터와 AP의 로드밸런싱을 통해 재머를 협력적으로 검출하고, 이를 기반으로 에너지 소비를 최소화 할 수 있는 최적의 경로를 선택해 재머 탐지 성능과 네트워크 성능을 최적화한다. 평가 결과에 따르면 MLCC 기법을 적용하면 종래 방법 대비 재머 탐지 정확도가 최대 5.5%, 평균 1.9% 향상되었다. 또한, 재머의 이동속도에 따른 성능을 평가했을 때 MLCC는 random model 대비 처리율은 최대 35.77%, 평균 17.49% 향상되었고, 에너지 소모량은 최대 43.4%, 평균 41.09% 감소되었으며, 지연 시간은 최대 6.67%, 평균 4.97% 감소되었다. 제안하는 MLCC는 beyond-5G 스마트 리피터 네트워크 환경에서 재밍 공격에 효과적인 대응을 위해 적용될 수 있다.

목 차

표 차 례

그 림 차 례

Ⅰ. 서 론

최근 사물인터넷(IoT, Internet of Things), 클라우드, 인공지능(AI, Artificial Intelligence) 기술이 적용된 스마트 통신 인프라를 지원하기 위한 무선 네트워크 기술이 급속도로 발전하고 있다 [1]. 이러한 무선 통신 기술은 사용자에게 서비스를 제공하는 것뿐만 아니라, 다양한 응용 서비스와 공공 인프라로 활용 영역이 확장되고 있다 [2]. 특히, 5G 통신 인프라는 미션 크리티컬 (Mission Critical) 애플리케이션의 초고속, 초저지연, 초연결성을 보장하는 것을 목표로 하고 있다. 하지만, 무선 통신 기술은 유선 통신 대비 악의적인 공격자가 쉽게 네트워크에 접근할 수 있고, 그 중에서도 무선 네트워크는 공유 매체를 통해 통신하기 때문에 재밍이나 전파 간섭을 일으키기 쉽다 [1]. 이와 같이 간섭의 수준이 높을수록 수신기가 수신한 신호를 복원하기 어려워서 무선 네트워크의 성능이 저하된다 [3]. 공격자는 이러한 무선 통신 취약성을 악용하여 공격 대상의 무선 채널에 의도적인 간섭을 유발하고 합법적인 통신을 방해하기 위해 재밍 공격을 수행한다.

재밍 신호는 무선 매체에서 간섭, 충돌의 발생으로 인해 통신 환경을 파괴하는 비의도적 간섭과 공격자가 의도적으로 시스템의 가용성을 파괴하기 위해 공격을 수행하는 의도적 간섭으로 나누어 볼 수 있다. 의도적 재밍 공격은 서비스 거부 공격(DoS, Denial of Service)의 유형으로, 공격자가 통신을 방해하기 위해 악의적으로 높은 범위의 신호를 방출하는 공격 유형이다 [4]. 유럽 ENISA Threat Landscape Report 2018 report에 따르면, 대표적인 전파 방해 공격인 분산 서비스 거부 공격(DDoS, Distributed Denial of Service)의 공격 용량이 지속적으로 커지고 있으며, 공격 규모가 최대 1.7TB급으로 매우 커지고 있다 [5]. 특히 4G 대비 20배 빠른 통신 속

도와 10배 이상의 IoT 기기가 접속 가능한 5G 환경에서는 전파 방해 공격의 파급력이 매우 크다. 빠른 통신 속도와 많은 연결 장치 수를 지원하는 방향으로 현재 논의되고 있는 3GPP (3rd-generation partnership project) New Radio (NR)에서는 이러한 전파 방해 공격으로 인한 피해가 매우 커질 것으로 예상하고 있다. 따라서 빠르게 변화하는 네트워크 상황을 고려한 재밍 공격의 대응 기법이 요구된다.

종래 재밍 공격 탐지 기법으로는 Packet Delivery Ratio (PDR), Received Signal Strength Indicator (RSSI), timestamp와 같이 네트워크 환경 변화에 민감하게 반응하고 신호 변동이 심한 단일 탐지 메트릭을 활용하거나 [6-10], 무작위로 주파수를 호핑하는 방법이 연구되어왔다 [11]. 하지만, 현실적인 재밍 공격의 환경은 재밍 신호 파워나 공격 주기가 일정하지 않으며, 방대한 공격 패턴에 대응하기 어렵다는 문제가 있다.

현재 3GPP NR에서 스마트 리피터의 활용이 논의되고 있으며 [12], 스마트 리피터는 종래 Radio Frequency (RF) 리피터와 달리 단말의 위치와 전파 방향을 고려하여 신호를 전송한다는 특징이 있다. 스마트 리피터는 고정된 장치이기 때문에 전파 간섭이 발생할 경우, 모바일 장치와 같이 물리적으로 회피할 수 없어서 재밍 공격에 의한 큰 피해가 예상된다. 또한, 방향성을 가지는 신호를 전송하는 스마트 리피터의 특성상 신호 간섭 공격으로 인한 데이터 전송 오류도 유발하기 쉽다. 하지만, 현재 스마트 리피터 환경에서의 재밍 공격과 관련된 논의가 이루어지지 않고 있다. 이에 따라 빠르게 발전하는 이동 통신 기술과 급증하는 트래픽 환경에서 대표적인 전파 방해 공격인 재밍 공격에 대한 적절한 대응 방안이 요구되고 있다 [13]. 특히, 스마트 리피터 및 access point (AP)와 같이 고정된 노드가 분산된 환경에서 모바일 재머의 지능적인 공격을 탐지하는 방안과 재머 탐지에서 나아가 재머를 효율적으로 회피하는 방안에 관한 연구가 필요하다.

따라서 본 연구에서는 네트워크 내 모바일 재머가 분포한 환경에서 재밍 공격 탐지 및 회피를 위한 머신러닝 기반 협력적 클러스터링 (Machine Learning-based Cooperative Clustering, MLCC) 기법을 제안한다. MLCC는 협력적 재머 탐지 결과를 기반으로 최적의 경로로 라우팅한다.

본 연구는 다음의 세 가지 측면에서 주요 기여점이 있다.

1) 스마트 리피터 노드로 구성된 분산 네트워크 환경에서 클러스터의 개념을 도입하여 머신러닝 기반 협력적 탐지를 통해 재머 탐지율을 개선하였다.

2) 클러스터 노드(Cluster node, CN)인 스마트 리피터와 클러스터 헤드(Cluster head, CH)인 AP의 로드밸런싱을 통해 재머 탐지 과정에서 소모되는 에너지의 양을 최소화하였다.

3) 지능형 모바일 재머가 공격하는 환경에서 종래 재머 탐지 및 회피 방식은 심각한 성능 열화가 발생하지만, 제안하는 방식을 적용하면 재머 탐지 정확도, 처리율, 에너지 소모량, 지연 시간 성능이 유지됨을 보였다. 또한, 네트워크 내 간섭 상황에 따라 적응적으로 재머를 회피할 수 있는 방안을 제안하고 현실적인 무선 통신 모델에서 성능을 평가했다.

본 논문의 구성은 다음과 같다. Ⅱ장에서는 종래 재머 탐지 및 회피 기법의 선행연구를 분석하고, Ⅲ장에서 본 논문에서 다루는 스마트 리피터에 관하여 서술한다. Ⅳ장에서는 본 연구에서 제안하는 MLCC의 동작 방식을 서술하고 Ⅴ장에서 MLCC의 성능을 입증하기 위한 실험 환경과 실험 결과를 분석하며, Ⅵ장에서는 결론을 맺는다.

Ⅱ. 관련 연구

본 장에서는 재머 탐지 및 회피 관련 선행연구를 분석한다. 재머 탐지 기법과 회피 기법으로 나누어 선행연구를 분석하였으며, 재머 탐지 기법은 단일 탐지 메트릭 기반, 기계학습 기반, 퍼지 논리, 지수 가중치 이동 평균 (Exponentially weighted moving average, EWMA), 채널 상태 정보 기반의 탐지 방법이 연구되고 있었다. 대부분의 재머 탐지 기법은 PDR, RSSI와 같은 단일 탐지 메트릭의 측정치와 임계치를 비교하여 탐지하는 연구가 주로 이루어지고 있었다. 하지만 단일 탐지 메트릭 기반의 탐지 방법은 다양한 공격 패턴으로 공격을 수행하는 지능형 공격자에 대응하기에 어렵다는 한계가 있다. 재머 회피 기법은 채널 측정, 주파수 호핑, 공간 회피 기반 재머 회피 기법이 연구되고 있었다. 하지만, 종래 재머 회피 기법은 에너지 효율성과 지연 시간을 고려하여 회피하는 방안에 관한 연구는 부족했으며, 대부분이 재머 탐지 기법에만 초점을 맞추고 있어서 스마트 리피터와 같이 고정된 노드 환경에서 재머를 회피하기 위한 대응 기술이 미흡한 실정이었다.

1. 재머 탐지 기법

재머를 탐지하기 위한 기법으로는 주로 단일 재머 탐지 메트릭을 활용하여 탐지하는 방법이 연구되고 있다. 또한, 노드가 분산된 환경에서 효율적으로 재머를 탐지하기 위해 클러스터의 개념을 도입한 연구가 많았다. Table I은 재머 탐지 기법에 관한 선행연구를 정리한 표로 클러스터링 기법을 적용한 선행연구를 표시하였다.

선행연구 [6-8]는 PDR과 RSSI 지표를 함께 활용하여, 두 지표가 임계치 이하이면 재머로 판별하는 기법을 제안하였다. 본 선행연구 [6-8]는 클러스터 환경에서 중앙의 CH가 패킷을 수신할 때마다 재머 여부를 판별한다. 선행연구 [9, 10]는 데이터 전송 후 응답 시간을 재머 탐지 메트릭으로 활용한다. Timestamp가 임계치 이상일 경우, 재머의 악의적인 방해 신호로 인한 것으로 가정한다. 하지만 현실적인 재밍 공격은 파워와 신호 주기가 유동적이므로 단일 탐지 메트릭으로 임계치와 비교하여 탐지하는 기법은 재머가 우회하기 쉽다.

선행연구 [8, 14-16]는 최근 재머 탐지 기법으로 많이 연구되고 있는 머신러닝 기반 탐지 방법이다. 이 선행연구 [8, 14-16]는 공통적으로 각 노드에서 수집되는 신호의 피처를 로컬 혹은 1개의 노드에서 기계학습을 통해 학습하여 재머를 탐지하는 모델을 제안하였다. 하지만 선행연구 [8]는 머신러닝 학습에 RSSI 단일 피처만 고려하고 있고, 선행연구 [14]에서는 학습 모델 별 성능만 비교했다는 것이 한계점이다. 선행연구 [15]는 정교한 전처리 방법을 통해 성능을 높이고자 했으나, 딥러닝 모델을 활용했음에도 24,000개의 비교적 적은 데이터셋 샘플로 평가하여 종래 연구보다 탐지 정확도가 낮았다. 또한, 선행연구 [16]는 다양한 유형의 재밍 공격을 분류할 수 있었지만, 네트워크 상황이 지속적으로 변화하는 현실적인 환경의 고려

가 미흡했다.

TABLE I

Previous studies on jammer detection

Metrics	Refs.	Clustering technique	Main features
PDR, RSSI, Timestamp	[6]-[8], [9],[10]	[6],[7], [9],[10]	· PDR, RSSI가 임계치 이하이면 재머로 판별 [6]-[8] · 수신한 데이터의 timestamp가 임계값을 초과할 경우, 재머로 판별 [9]-[10]
Machine learning	[8],[14]-[16]	[14]	· 각 노드에서 수집되는 피처를 머신러닝으로 학습하여 재머 판별
Fuzzy logic	[7],[17]	[7],[17]	· 퍼지 논리로 재머 탐지 메트릭의 최댓값을 계산하여 재머 탐지 메트릭을 최적화
EWMA	[18]	[18]	· 센서 노드로부터 수신한 패킷의 inter-arrival 피처를 사용하여 방해 공격 이벤트 강도의 비정상적인 변화를 검출하기 위해 EWMA 활용
Channel state information	[19],[20]	[20]	· 채널의 상태 정보를 기반으로 재머 검출 · 데이터 손실 및 위상 간섭 레벨을 고려

선행연구 [7, 17]는 퍼지 논리를 활용하여 종래 단일 재머 탐지 메트릭 기반의 탐지 기법을 발전시켰다. 두 선행연구는 퍼지 논리로 재머 탐지 메

트릭의 최댓값을 계산하여 최적화하였다. 하지만 두 선행연구 모두 모든 노드가 PDR 및 RSSI를 측정 및 평가하여 1차적으로 재머 여부를 판별한다는 점에서 노드의 개수가 증가할수록 CH의 작업이 과중된다는 한계가 있다.

선행연구 [18]는 재머를 탐지하기 위해 통계적 공정 관리 (Statistical process control, SPC) 기법 기반의 단계적 접근법을 제안했다. 센서 노드로부터 수신한 패킷의 inter-arrival time 피처를 사용하여 방해 공격 이벤트 강도의 비정상적인 변화를 검출하기 위해 EWMA을 활용하였다. 본 선행연구는 CH에서 재머 판별 및 검출이 모두 이루어지기 때문에 CH 노드의 오버헤드가 증가하고, CH 노드의 가용 자원이 매우 커야하는 문제가 있었다.

선행연구 [19, 20]는 채널의 상태 정보를 기반으로 재머를 검출하는 방법을 제안했다. 선행연구 [19]는 데이터의 전송 흐름이 끊긴 지점을 판별하여 데이터 손실이 발생한 재밍 영역을 검출하는 방식으로 재머를 탐지했다. 선행연구 [20]은 높은 위상 잡음 레벨을 가질수록 재머일 가능성이 높은 것으로 판별하고, signal-to-noise ratio (SNR)을 고려하여 탐지 성능을 높이는 방법을 제안했다. 하지만, 본 선행연구 역시 재밍 신호가 다양한 패턴으로 발생하는 현실 환경에서 대응이 어렵다.

2. 재머 회피 기법

재머를 회피하기 위한 대표적인 기법은 채널 측정 기반, 주파수 호핑 기반, 공간 회피 기반 회피 기법으로 나누어 볼 수 있다. Table II는 재머 회피 기법에 관한 선행연구를 정리한 표이다.

TABLE II

Previous studies on jammer avoidance

Metrics	Refs.	Main features
Channel measurement	[21],[22]	· 소스 노드에서 목적지 노드에 도달할 때까지 flooding request 패킷을 전송하여 PDR 측면에서 가장 효율적인 경로를 선택하여 재머 회피
Frequency hopping	[23]	· 재머의 행위를 확률적으로 모델링하는 최적의 결정 규칙을 통해 재머를 효율적으로 회피하기 위한 주파수 호핑 방안 제안
Spatial retreat	[24],[25]	· 재머가 탐지되면, 피해 노드를 물리적으로 이동시켜 재머를 공간적으로 회피

선행연구 [21, 22]은 소스 노드 (Source node, SN)부터 목적지 노드 (Destination node, DN)에 도달할 때까지 flooding request 패킷을 전송해 봄으로써 PDR 측면에서 가장 효율적인 경로를 선택하여 재머 회피하는 방법을 제안한다. 해당 선행연구는 flooding request 패킷을 인근에 모두 전송해보고 경로를 선택하기 때문에 최적의 경로를 선택할 수 있다는 이점이 있지만, 가능한 모든 경로에 패킷을 전송해보는 과정에서 트래픽 양이 매우 증가하는 것이 한계점이다.

선행연구 [23]은 재머의 행위를 확률적으로 모델링하는 최적의 결정 규

칙을 통해 재머를 회피하는 주파수 호핑 기법을 제안한다. 본 선행연구는 종래의 무작위로 주파수를 호핑하는 기법 [11]과 달리 재머의 행위를 확률적으로 모델링하여 사전에 대응할 수 있다는 점에서 기여점이 있지만, 전환되는 주파수가 서로 다른 두 개의 주파수에 한정하여 솔루션을 제공했다는 것이 한계점이다.

선행연구 [24, 25]는 재머가 탐지되면, 피해 노드를 물리적으로 이동시켜 공간적으로 재머를 회피하는 방안에 관하여 연구하였다. 하지만 공간적으로 이동하여 회피하는 방안은 무인 항공기(Unmanned Aerial vehicle, UAV)와 같이 이동형 장치에만 적용할 수 있다는 제약이 있다. 특히, 선행연구 [24]는 재밍 노드가 재밍 구역에서 벗어날 때까지 이동 방향을 무작위로 선택한다는 점에서 비효율적으로 소비하는 에너지가 크다.

종래 다수의 재밍 공격 관련 연구는 재머 탐지에 초점을 둔 연구가 주로 되어왔으며, 재머 회피를 위한 연구는 부족했다. 또한, 재머를 탐지하기 위한 기존의 연구는 다양한 신호 패턴으로 공격을 수행하는 정교한 재밍 공격에 대응이 어려웠다. 최근의 기계학습 기반 재머 탐지 연구도 로컬에서 학습이 이루어지기 때문에 탐지 정확도가 낮으며, 특정 노드에 연산이 과중되는 문제가 있었다.

Ⅲ. 스마트 리피터

1. 스마트 리피터 개요

본 장에서는 스마트 리피터의 개념을 서술한다. Fig. 1은 스마트 리피터와 RF 리피터의 개념도를 나타낸 것이다.

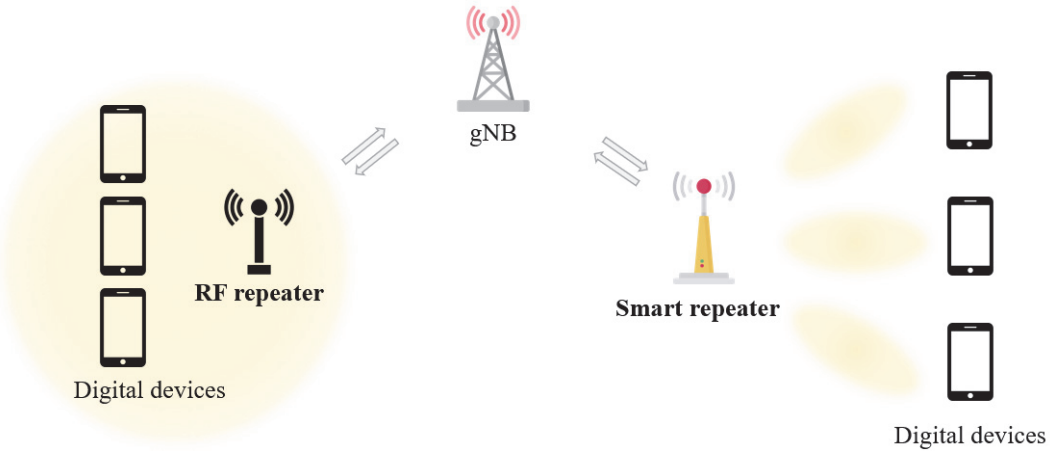


FIGURE 1. Schematic illustration of smart repeater and RF repeater

Fig. 1과 같이 리피터는 gNB(next generation node B)에 의해 제어된다. 스마트 리피터는 2G, 3G, 4G에서 활용되는 RF 리피터에서 개선된 리피터로 레귤러 메크로 셀 (Regular macro cell)의 커버리지 문제를 보완하기 위해 네트워크 제어 리피터 (Network-controlled repeater)의 명칭으로 3GPP Rel-18에 도입될 것으로 논의되고 있다 [26]. 종래의 RF 리피터는 비재생 릴레이 노드 (non-regenerative relay node)로 수신되는 모든 신호

를 증폭하고 전방향으로 신호를 송신한다 [27]. 또한, RF 리피터는 업링크와 다운링크를 구분하지 않는 전이중 통신을 수행한다 [27]. 따라서, RF 리피터는 단순한 방식으로 네트워크 커버리지를 개선할 수 있지만, 전방향으로 신호가 방사되는 특성상 간섭이 증가하는 문제가 있다. 이에 반해 스마트 리피터는 Fig. 1과 같이 유사한 이득으로 여러 방향으로 데이터를 송신할 수 있는 멀티빔 (multibeam) 안테나로 통신한다 [12]. 스마트 리피터는 단말의 위치와 전파 방향을 고려하여 업링크와 다운링크를 분리하여 신호를 송신하기 때문에 RF 리피터와 달리 비용 효율적이라는 장점이 있으며, 네트워크 커버리지를 빠르게 확장시킬 수 있다 [12]. 그러나 스마트 리피터 역시 네트워크 환경에서 의도적이거나 비의도적인 신호 간섭이 발생할 때 데이터가 잘못된 링크를 통해 전송될 수 있고, 스마트 리피터는 이동성이 없는 고정된 기기이기 때문에 물리적 간섭을 피하기 어렵다. 따라서 스마트 리피터 환경에서 재밍 공격에 대한 대응책이 필요하다.

2. 스마트 리피터의 보안성 분석

현재 3GPP NR에서 스마트 리피터의 도입이 활발히 논의되고 있으나, 보안 위협 측면의 보안성 분석은 부족한 실정이다. 본 장에서는 스마트 리피터의 통신 방식을 토대로 발생 가능한 보안 위협에 대해 분석한다.

스마트 리피터는 멀티빔 방식으로 통신하고, 업링크와 다운링크가 분리되어 단말의 위치와 전파 방향을 고려하여 신호를 송신한다는 특징이 있다. 멀티빔 안테나는 기지국에 설치된 한 개의 안테나로 동시에 다수개의 독립적인 무선 지향성 신호를 송출하여 네트워크 커버리지를 개선시킨다 [28]. 멀티빔 안테나는 대규모 multiple-input multiple-output (MIMO)를 가능케 하는 핵심 하드웨어 역할을 하며, 초기에는 물리적으로 부피가 크고 비용이 많이 소요되어서 레이더 시스템과 위성 통신에 주로 활용되었다 [28]. 하지만 최근 밀리미터파 웨이브 (Millimeter wave, MMW) 주파수 대역에서 더 짧은 파장으로 더 많은 안테나를 동일한 물리적 면적의 개구면 (Aperture)에 포함할 수 있게 되면서 높은 어레이(array) 이득과 작은 폼 팩터 (Form factor) 요건을 충족해야 하는 소형 장치에도 적용할 수 있게 되었다 [28]. 하지만 이러한 신호 특성이 다양한 보안 위협을 초래할 수 있다. Table III은 스마트 리피터에서 발생 가능한 보안 이슈를 정리한 것이다.

TABLE Ⅲ. Security issue of smart repeater

Security issue	Target service	Description
Eavesdropping [29]	Confidentiality	· 멀티 빔 특성상 여러 사용자에게 동시 서비스하므로 도청 위협이 큼 · 다수의 경로에 위치하는 도청자로부터 기밀 정보 유출 위협이 큼
Jamming (Intentional interference)	Availability	· 고정된 노드의 장치이기 때문에 재밍 공격을 수행하는 공격자로부터 물리적인 회피 불가
Physical interference (Unintentional interference)	Availability	· 고정된 노드의 장치이기 때문에 물리적인 공간 상 장애물로 인해 발생하는 간섭 회피 불가 · RF 리피터 대비 동시에 신호가 송신되는 경로가 많으므로 비의도적 간섭 발생 용이
Phase error [30]	Availability	· 입력 신호의 크기에 따라 출력 신호의 위상이 다른 값을 가질 수 있음 · 멀티빔 안테나 장치 내 구성요소의 부품이 서로 다른 크기로 제작되면서 신호의 크기 및 위상 변화가 발생할 수 있음 · 빔 형성 과정에서 안테나에 분배되는 신호 간 위상 및 진폭 오차가 발생할 수 있음

스마트 리피터는 다수의 독립적인 무선 신호를 송신하는 멀티빔 안테나를 활용하기 때문에 여러 합법적인 사용자에게 네트워크 내에서 동시 서비스하므로 도청 위협이 크다는 문제가 있다 [29]. 즉, 다수의 경로에 위치하는 도청자가 기밀 정보를 도청하여 유출할 가능성이 크다.

또한, 이동성이 없는 고정된 기기인 스마트 리피터 환경은 가용성을 파괴하는 신호 간섭 공격이 발생하기 쉽다. 신호 간섭은 공격자가 의도적으로 간섭을 발생시키는 공격 유형인 재밍 공격과 비의도적 간섭인 물리적 간섭으로 나누어 볼 수 있다. 스마트 리피터는 다수의 지향성 신호를 송신함으로써 통신 효율과 성능은 높일 수 있지만, 신호 간섭이 발생할 때 신호 품질 성능이 급격하게 열화된다는 특징이 있다. 특히 모바일 장치와 달리 이동성이 없는 스마트 리피터 노드는 악의적인 재밍 신호나 구조 상 장애물로 인해 발생하는 간섭을 물리적으로 회피할 수 없고, RF 리피터 대비 동시에 신호가 송신되는 경로가 많으므로 비의도적인 간섭의 발생이 쉽다는 점에서 신호 간섭 문제에 취약하다.

스마트 리피터는 공격자의 의도적인 공격 외에도 위상 오류(Phase error)로 인해 신호 품질이 급격히 저하되는 가용성 측면의 취약점이 존재한다. 스마트 리피터의 증폭기가 비선형적이므로 입력 신호 크기에 따라 출력 신호의 위상이 다른 값을 가지게 될 수 있으며, 멀티빔 안테나 내 구성요소의 부품이 서로 다른 크기로 제작되면서 신호의 크기나 위상 변화가 발생할 수 있다 [30]. 또한, 빔 형성 과정에서 안테나에 분배되는 신호 간의 위상 및 진폭 오차가 발생할 수 있다 [30]. 이러한 위상 오류는 안테나의 송신 성능을 저하시켜 정상적인 통신 가용성을 파괴한다.

이와 같이 스마트 리피터 환경에서 발생 가능한 보안 위협이 다양하지만 보안성 분석에 대한 고려가 미흡하다. 특히 스마트 리피터는 다중 경로로 지향성 신호를 전송하기 때문에 종래 장치 대비 신호 간섭 문제로부터 취

약하다. 장애물로 인한 비의도적인 간섭에 대한 문제도 있지만, 지능적이고 악의적인 재밍 공격자가 이동하면서 전파 간섭을 발생시킬 경우, 스마트 리피터로 구성된 네트워크 시스템이 종래의 방법으로 재밍 공격을 탐지하거나 효과적으로 대응하기 어렵다. 따라서 본 논문에서는 스마트 리피터 환경에서 효율적으로 재밍 공격을 탐지 및 회피하기 위해 머신러닝 기반 협력적 클러스터링 기법을 도입한다.

Ⅳ. 재밍 공격 탐지 및 회피를 위한 머신러닝 기반 협력적 클러스터링 기법

본 장에서는 재밍 공격 탐지 및 회피를 위한 머신러닝 기반 협력적 클러스터링 기법의 동작 방법인 MLCC에 대해 서술한다.

1. MLCC 시스템 구조 및 메커니즘

MLCC는 위치가 고정된 스마트 리피터 노드들로 구성된 분산 네트워크 환경에서 효율적으로 재머를 탐지하기 위해 머신러닝 기반 협력적 클러스터링 기법을 적용한다. 클러스터는 클러스터 중심에 위치하는 CH와 네트워크에 분산된 CN의 구조로 구성된다. 본 논문에서 CH는 AP에 해당하고 CN은 스마트 리피터에 해당한다. AP가 통신 가능한 범위의 노드까지 1개의 클러스터에 포함하여 구성한다. Fig. 2는 MLCC의 시스템 구조도를 나타낸 것이다.

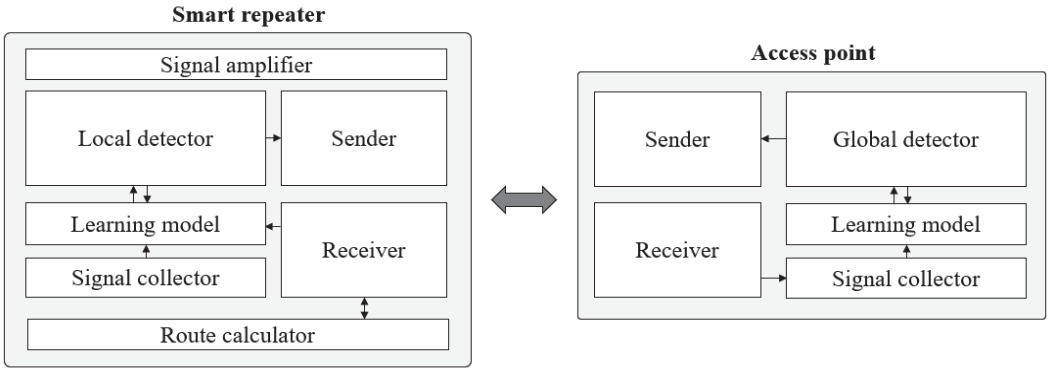


FIGURE 2. System architecture of the proposed MLCC

스마트 리피터 노드는 신호를 증폭시키는 신호 증폭부(Signal amplifier), 인근에서 비주기적으로 방출되는 신호를 수집하는 신호 수집부(Signal collector), 재머 여부를 판별하기 위해 수집한 신호를 학습하는 신호 학습부(Learning model), 생성된 학습 모델을 토대로 재머 여부를 로컬에서 판별하는 로컬 검출기(Local detector), 재머 판별 정보를 기반으로 최적의 데이터 전송 경로를 산출하는 경로 산출기(Route calculator), 데이터 및 신호를 송수신하는 송신부(Sender)와 수신부(Receiver)로 구성된다. 스마트 리피터는 인근에서 비주기적으로 방출되는 신호를 수집하여 판별한 결과를 송신부를 통해 AP로 전송한다. 여기서 판별 결과란, 인근 노드의 재머 여부와 재머 판별 정확도를 의미한다. CH 노드에 해당하는 AP는 수신한 재머 판별 정보를 취합하여 글로벌 검출기(Global detector)에서 판별 정확도의 평균치를 산출하여 최종적으로 재머의 위치를 추정하고, 추정한 재머의 위치를 토대로 학습 모델을 생성하여 글로벌 정보를 스마트 리피터 노드에 전송한다. 이를 수신한 스마트 리피터는 다수의 스마트 리피터 노드의 판별 결과가 반영된 재머 판별 모델로 업데이트하여 경로 산출기에서 최적의 경로를 산출한다.

2. MLCC 기반 재머 탐지 및 회피 기법

MLCC는 정상 스마트 리피터 노드(Smart repeater node, SR)와 재머 노드(Jammer node, JN)가 혼재한 환경에서 머신러닝 기반 노드 간 협업을 통해 재머를 효율적으로 탐지한다. 재머 탐지 메커니즘은 스마트 리피터의 학습 모델, 로컬 검출기와 AP의 글로벌 검출기를 통해 동작한다. Fig. 3은 MLCC의 협업 탐지 과정을 나타낸 것이다.

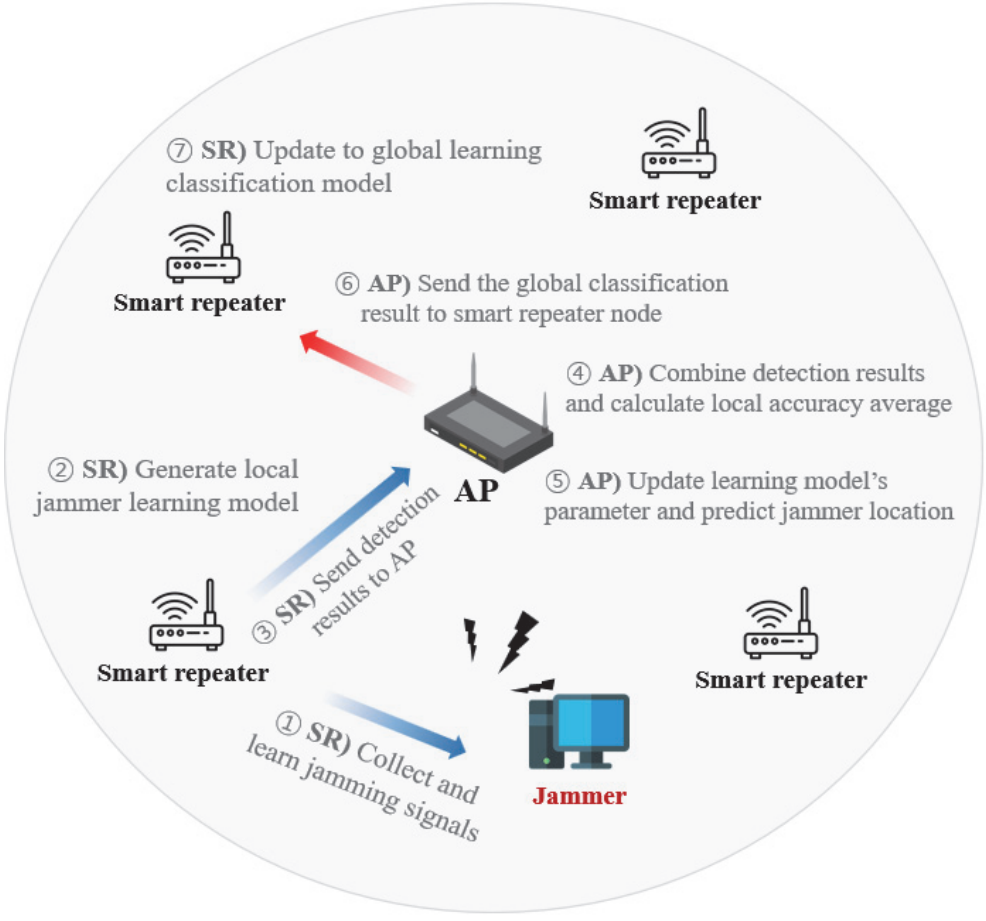


FIGURE 3. Flowchart for the machine-learning-based cooperative clustering approach used in this study

MLCC의 클러스터는 1개의 AP에 다수의 스마트 리피터가 연결된 네트워크 구조를 갖는다. MLCC는 학습 단계와 평가 단계를 거쳐 재머를 판별한다. 먼저 학습 단계에서 스마트 리피터는 인근 노드에서 비주기적으로 방출되는 신호를 수신부를 통해 수집한다. 이때 JN이 스마트 리피터 주변에 있을 때 스마트 리피터는 정상 스마트 리피터 노드와 JN의 신호를 함께 수집하여 정상 신호와 공격 신호를 학습할 수 있다. 본 연구에서 학습 모델로는 이진 분류를 위한 머신러닝 모델인 decision tree를 활용하였으며, 각 스마트 리피터는 축적된 인근 노드의 신호를 학습하여 재머 판별을 위한 머신러닝 모델을 생성한다. 이후 평가 단계에서 각 스마트 리피터는 생성된 머신러닝 기반 재머 학습 모델을 토대로 인근 노드의 재머 여부를 판단한다. 인근 노드에서 방출하는 신호가 재머인지 여부를 평가 정확도와 산출하게 되고, 각 로컬 노드에서 재머를 탐지한 결과를 AP로 전송한다. 이때 탐지 결과는 인근 노드의 재머 여부와 판별 정확도가 해당된다. AP는 이를 종합하여 글로벌 검출기를 통해 다수개의 스마트 리피터가 판별한 탐지 정확도의 평균치를 산출하여 네트워크 내 JN의 위치를 최종적으로 판별한다. 이때 MLCC는 분류의 확실성(Certainty of classification, CoC)을 기준으로 재머를 판별한다. CoC는 분류기에서 재머로 판별한 것에 대한 확실성의 정도를 의미한다. 요구되는 CoC 이상의 성능으로 재머를 탐지했을 경우, 재머로 판별하여 최종적인 JN의 위치를 특정한다. MLCC를 활용하면 협력적으로 재머의 위치를 인식할 수 있으므로 로컬 탐지 결과를 활용하는 종래 모델보다 정확하게 재머를 탐지할 수 있다. 이후 AP는 판별한 재머 정보를 토대로 학습 모델을 업데이트한 후, 산출한 재머 탐지 결과를 네트워크 내 스마트 리피터에 전송한다. 각 스마트 리피터는 로컬에 저장된 재머 학습 모델을 글로벌 재머 학습 모델로 업데이트함으로써 재머 탐지율을 높일 수 있다. 본 연구에서는 평가 모델의 단순성을 위해

로컬 학습 모델이 글로벌 학습 모델로 오류 없이 동일하게 업데이트된다고 가정하였다.

제안하는 MLCC 모델은 노드 간 협력적 탐지를 통해 특정한 재머의 위치 정보를 토대로 효율적인 데이터 전송 경로를 선정한다. 스마트 리피터는 고정된 노드 환경이기 때문에 노드들은 서로의 위치를 인지하고 있는 환경이다. 따라서, 정확도 높은 재머 분류 모델을 기반으로 최소 홉으로 이동 가능한 최적의 재머 회피 경로를 경로 산출기를 통해 선출한다. 효율적으로 경로를 선정하기 위해 스마트 리피터의 통신 범위에 따라 섹터화하여 최적의 경로를 선출할 수 있다.

Ⅴ. 성능 평가

1. 실험 환경

본 논문에서는 제안하는 MLCC 모델의 개념을 증명하고 성능을 평가하기 위해 복잡한 네트워크 구성을 추상 레벨로 모델링하여 단순화한 MLCC 네트워크 시뮬레이터를 구현했다. Fig. 4는 본 실험에서 활용한 클러스터 기반 네트워크의 노드 배치도를 나타낸 것이다.

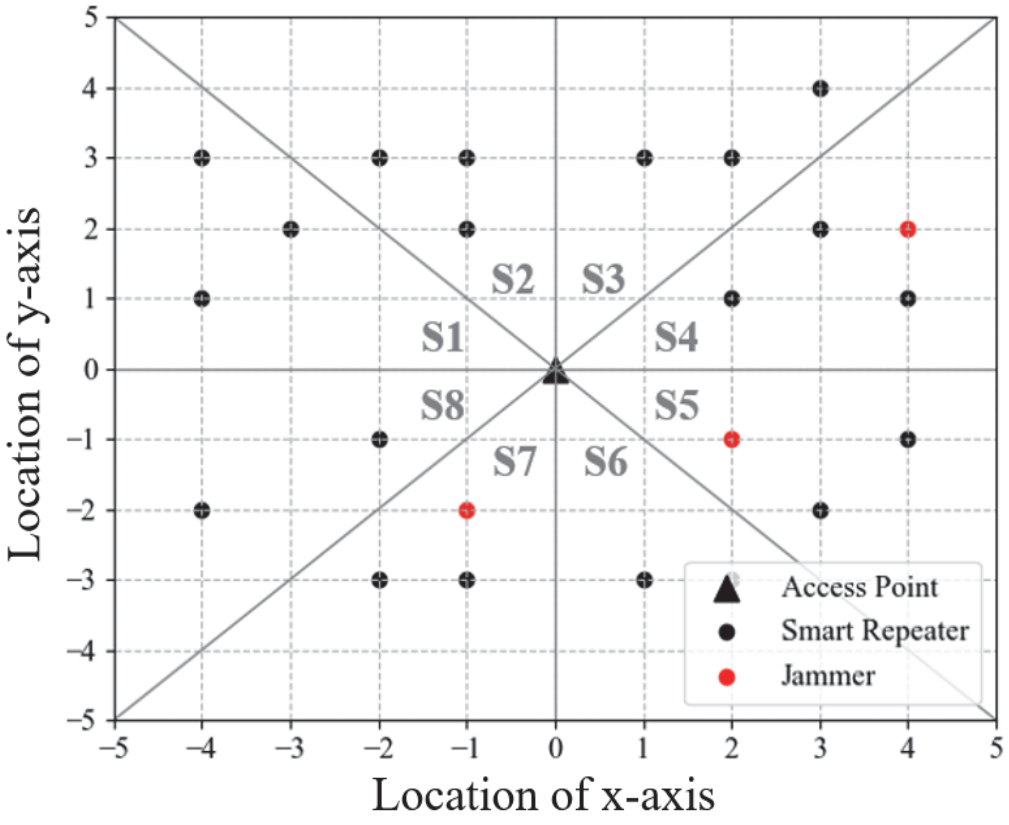


FIGURE 4. Deployment by node types in cluster

Fig. 4는 네트워크의 무선 장치의 배치를 단순화하여 xy 평면에 나타낸 것이다. ▲는 AP 노드, ●는 스마트 리피터 노드, 🔴는 Jammer 노드의 위치를 나타낸 것이고, S1부터 S8은 8개의 sector를 표현한 것이다. 실험 환경은 1개의 AP에 20개의 정상 스마트 리피터가 연결된 구조로 구현하였고, 선행연구와 동일한 조건에서 효율적으로 재머를 탐지 및 회피하기 위해 클러스터 내 공간을 S1부터 S8까지 8개의 섹터로 나누어 평가하였다 [31]. 또한, AP와 스마트 리피터 노드는 고정된 노드로 서로의 위치를 인지하고 있는 환경이고, 재머는 설정한 주기에 따라 물리적으로 이동하는 모바일 노드이다. 각 스마트 리피터는 양쪽으로 2개의 클러스터 내 노드까지 통신이 가능한 환경으로 가정하였다. 예를 들면 Fig. 4의 S2 섹터에서 (-1, 3)의 좌표의 정상 노드는 S8 섹터의 (-2, -1)와 S4 섹터의 (2, 1) 좌표의 CN까지 통신할 수 있다. 또한, JN의 개수와 이동 속도는 설정한 파라미터에 따라 동작한다. 본 실험에서 JN의 비율(γ)은 정상 노드 대비 JN의 개수로 표현하였으며, Eq. (1)에 따라 계산되었다.

$$\gamma = \frac{number\,of\,jammer\,node}{number\,of\,normal\,node} \times 100 \tag{1}$$

MLCC의 성능을 검증하기 위한 비교 모델은 flooding model(FM), pilot signal model(PM), random model(RM)을 선정하였다. FM은 선행연구 [20, 21]에서 활용한 라우팅 방법으로 DN에 도달할 때까지 인근 노드에 flooding request 패킷을 모두 전송해본 뒤에 간섭 레벨이 가장 낮은 라우팅 경로를 선택하는 모델이다. 본 연구에서 FM은 머신러닝 기반 탐지 과정 없이 flooding 패킷을 전송하면서 재머의 위치를 추정한다. PM은 특정 노드에서 재머 탐지를 담당하는 로컬 탐지 방법 [14, 15]의 탐지 방식을 활용하고, 이를 기반으로 재머를 회피하기 위한 라우팅 경로를 선정한다.

PM은 FM의 에너지 소모 문제를 일부 개선한 모델로, n개의 랜덤 경로를 선출하여 파일럿 신호 (Pilot signal)를 전송해본 뒤에 전송 성공률이 가장 큰 경로 1개를 선택하여 데이터를 전송하는 모델이다. 본 실험에서 PM의 n 값은 3으로 설정하였다. 마지막으로 RM은 앞선 두 비교 모델과 달리 경로 선출 과정 없이 무작위로 1개의 경로를 선정하여 바로 데이터를 전송하는 모델이다.

본 실험에서는 64 Quadrature Amplitude Modulation (QAM) 변조 방식을 사용해 21Mbps의 속도로 데이터를 전송한다. Fig. 5는 본 실험 환경에서 전송하는 데이터의 프레임 구조와 데이터 크기를 나타낸 것이다.

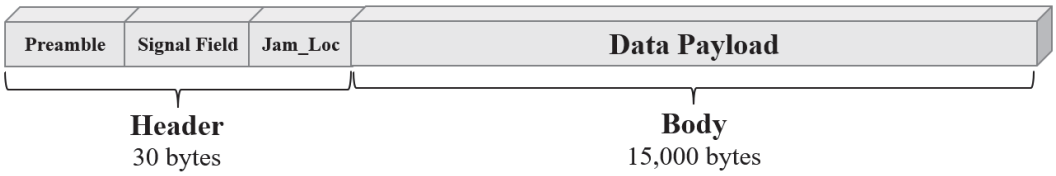


FIGURE 5. Structure of the packet frame used in this study

데이터 페이로드의 크기는 15,000byte로 고정하였고, 헤더는 30byte인 데이터를 전송하는 환경이다. 헤더는 Preamble, Signal Field와 AP로부터 공유 받은 재머의 위치를 저장하는 Jam_Loc으로 구성된다. 재밍 지역은 재머가 위치하는 1개의 섹터 범위로 가정하였다. 재밍 지역에 도달할 경우, 전송한 데이터 페이로드에 충돌이 발생하고, 해당 프레임이 재전송되면서 오버헤드가 증가하는 구조이다. 이때 재전송 허용 횟수는 8회로 제한하였다. 또한, 모바일 재머는 설정한 이동 속도 파라미터에 따라 8개의 섹터 중에서 랜덤으로 이동한다. 또한, 탐지 알고리즘이 동작하는 시간 간격보다 재머의 이동 속도가 빠를 때, 재머가 빠르게 이동하는 환경으로 가정하였

고, 탐지 간격보다 재머의 이동 속도가 느릴 때, 재머가 느리게 이동하는 환경으로 가정하였다. 시뮬레이션 반복 횟수는 300,000회로 설정하여 평균치를 산출하였다.

MLCC의 성능을 검증하기 위한 평가 지표는 탐지 정확도 성능 지표로 재머 탐지 정확도를 활용하였다. 재머 탐지 정확도는 JN을 JN으로 정확하게 판별한 true positive 비율을 의미한다. 본 연구에서 재머 탐지 성능을 측정하는데 활용한 데이터셋은 WSN-DS (Wireless Sensor Networks DataSet) [32]이다. Table Ⅳ는 WSN-DS 데이터셋의 피처 정보를 나타낸 것이다.

TABLE Ⅳ. Feature information of WSN-DS datatset [32]

Feature	Type	Description
ID	Integer	· 노드를 구분하는 고유 ID
Time	Integer	· 노드의 시뮬레이션 시간
is_CH	Integer	· 클러스터 헤드와 클러스터 노드를 구분하는 플래그
Who_CH	Integer	· 클러스터 헤드의 ID
Dist_to_CH	Float	· 클러스터 노드와 클러스터 헤드 사이의 거리
ADV_S	Integer	· 노드에 전송된 클러스터 헤드의 브로드캐스트 advertise 메시지 수
ADV_R	Integer	· 클러스터 헤드로부터 수신한 advertise 메시지 수
JOIN_S	Integer	· 노드에서 클러스터 헤드로 보낸 join request 메시지 수
JOIN_R	Integer	· 클러스터 헤드가 노드로부터 수신한 join request 메시지 수

SCH_S	Integer	· 노드에 전송된 advertise TDMA 스케줄 브로드캐스트 메시지 수
SCH_R	Integer	· 클러스터 헤드로부터 수신한 TDMA 스케줄 메시지 개수
Rank	Integer	· TDMA 스케줄 내 순서
DATA_S	Integer	· 클러스터 노드에서 클러스터 헤드로 전송된 데이터 패킷 수
DATA_R	Integer	· 클러스터 헤드로부터 수신한 데이터 패킷 수
Data_Sent_To_BS	Integer	· BS(Base station)로 전송된 데이터 패킷 수
dist_CH_To_BS	Float	· 클러스터 헤드와 BS 사이의 거리
send_code	Integer	· 클러스터 sending code
Consumed_Energy	Float	· 이전 라운드에서 노드가 소모한 에너지 양
Attack type	String	· 일반 노드와 공격 노드가 혼재하는 노드의 유형

WSN-DS 데이터셋은 Table Ⅳ와 같이 'id', 'Time', 'is_CH', 'Who_CH', 'Dist_to_CH', 'ADV_S', 'ADV_R', 'JOIN_S', 'JOIN_R', 'SCH_S', 'SCH_R', 'Rank', 'DATA_S', 'DATA_R', 'Data_Sent_To_BS', 'dist_CH_To_BS', 'send_code', 'Consumed_Energy', 'Attack type'의 19개의 피처로 구성된다. 이 데이터셋은 무선 센서 네트워크 내 서비스 거부 공격을 탐지하기 위한 데이터셋으로 Normal, Blackhole, Grayhole, Flooding, Scheduling attack 5개의 라벨로 구성된다. Normal 라벨을 제외한 공격에 해당하는 라벨은 모두 재밍 라벨로 통일하였고[32], 지도학습 모델인 Decision tree를 활용하였다. 학습 모델을 선정하기 위해서 빠르고 단순한 학습에 특화된 머신러닝 모델의 재머 분류 성능을 비교하였다. WSN-DS 데이터셋 환경에서

SVM(Support vector machine), Decision tree, Naive Bayesian, KNN(K-Nearest Neighbor) 모델의 분류 성능을 평가하였고 그 결과, 피처 간의 관계 식별에 특화된 decision tree가 97.7% 대의 최적의 분류 성능을 보였다. Table V는 데이터 불균형 문제를 해결하기 위해 데이터 밸런싱을 수행하기 전과 후의 라벨 별 데이터셋 개수를 나타낸 표이다.

TABLE V. Number of dataset after data balancing

Type	Before balancing	After balancing
Normal	340,066	34,595
Attack	34,595	34,595

기존 데이터셋은 Normal 데이터가 340,066개로 공격 데이터 대비 Normal 데이터가 매우 불균형한 환경이었기 때문에 두 타입의 라벨을 각각 34,595개로 데이터를 밸런싱하여 학습을 수행하였다.

네트워크 성능 지표로는 처리율, 에너지 소모량, 지연 시간을 평가하였고, 네트워크 내 전체 평균치를 계산하였다. 처리율은 DN이 성공적으로 수신한 데이터의 개수, 에너지 소모량은 데이터를 전송하는데 스마트 리피터가 소모하는 에너지의 양, 지연 시간은 1개의 정상 스마트 리피터 노드가 모든 데이터를 전송하는데 소요되는 시간을 의미한다.

처리율 평가지표는 다음의 Eq. (2)에 따라 계산하였다.

$$Throughput\,(Mbps) = \frac{Number\,of\ successfully\,received\,data}{Transmission\,time} \qquad (2)$$

Eq. (2)에 따라, 데이터를 전송하는데 소요된 총 시간 동안 재전송된 데이터를 포함하여 성공적으로 수신한 데이터의 개수를 계산하였다. 에너지

소모량은 유한 상태 기계(Finite state machine, FSM)를 정의하여 네트워크 내 정상 노드의 상태(state)에 따라 소모된 에너지의 양을 누적하여 측정하였다.

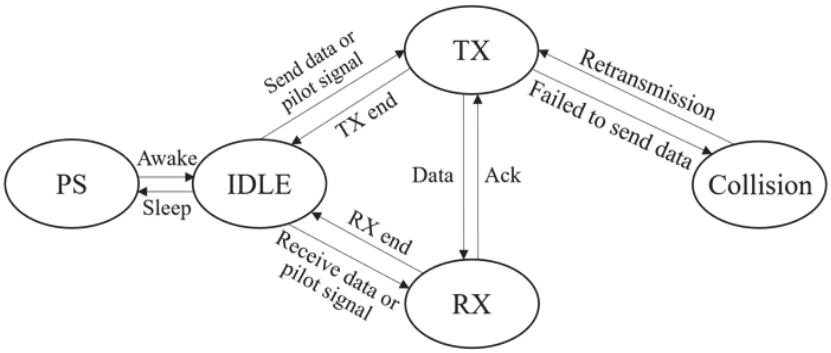


FIGURE 6. FSM utilized in this study

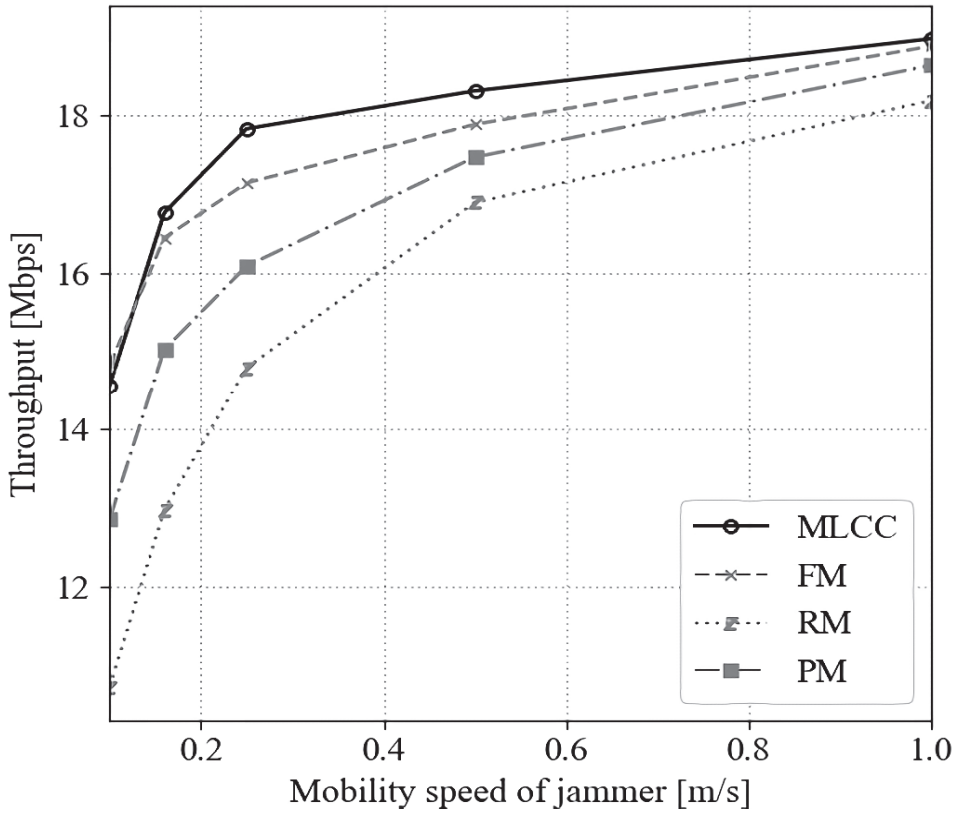
Fig. 6은 본 논문에서 활용한 FSM 구조를 나타낸 것이다 [33]. State은 TX, RX, IDLE, power saving (PS), collision 5가지로 정의하였다. PS는 sleep mode에서 비주기적으로 방출되는 신호를 수집하는 상태이고, IDLE은 PS에서 awake 된 상태를 의미한다. TX는 데이터 혹은 파일럿 신호를 전송하는 상태이며, RX는 데이터 혹은 파일럿 신호를 수신하는 상태이다. 또한, Collision은 재머로 인해 데이터 충돌이 발생하는 상태이다. 데이터를 전송 및 수신하는 과정에서는 각각 100.20mW, 25.05mW의 에너지를 소모하고, 헤더만 해당하는 파일럿 신호를 전송 및 수신할 때는 데이터 크기 비율에 따라 500배 적은 수치인 0.20mW, 0.05mW를 소모하도록 모델링하였다[34]. 또한, IDLE은 0.05mW, Power Saving은 0.01mW를 소모하도록 하고, 재밍 신호로 인한 데이터 충돌 발생 시 100mW의 오버헤드가 발생하는 환경으로 설정하였다 [34].

2. 실험 결과 및 분석

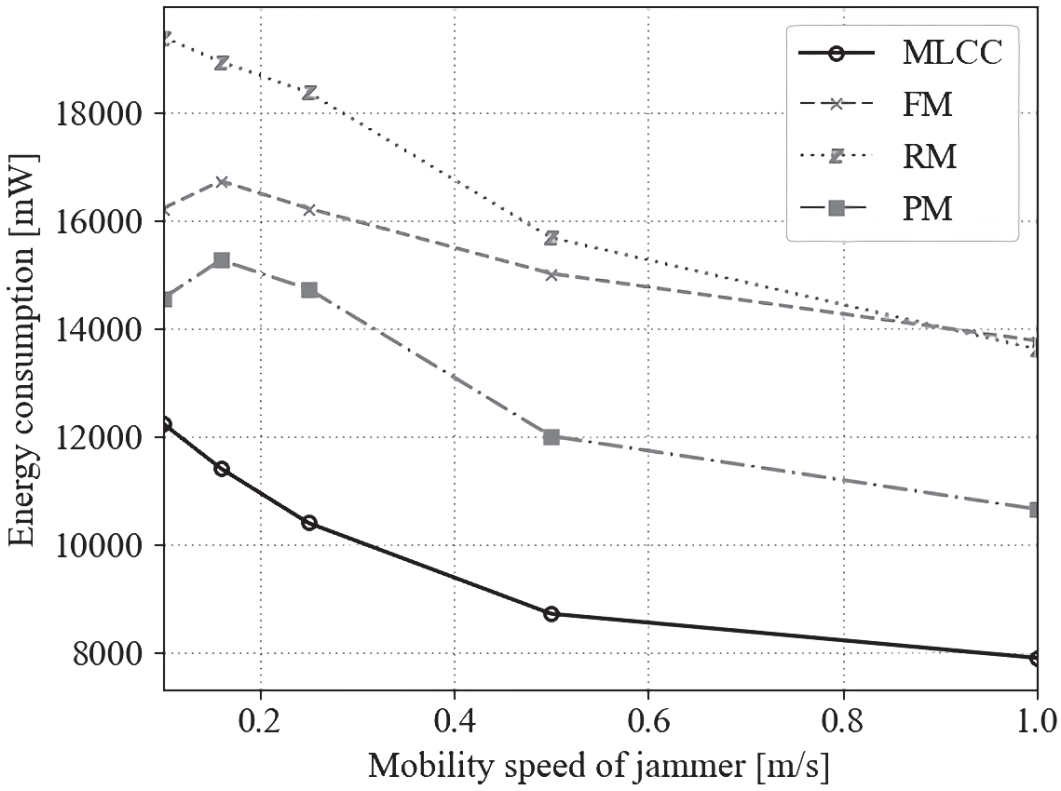
(1) 네트워크 성능 비교 분석

본 장에서는 네트워크 평가 지표인 처리율, 에너지 소모량, 지연 시간에 따른 MLCC의 성능을 평가한다. 본 실험은 20개의 스마트 리피터와 1개의 AP가 분포하는 환경에서 성능을 평가하였으며, 각 평가 지표는 노드들의 평균치를 측정하였다. Fig. 7과 Fig. 8은 재머의 이동 속도와 네트워크 내 재머의 비율에 따른 성능을 확인한 결과이다.

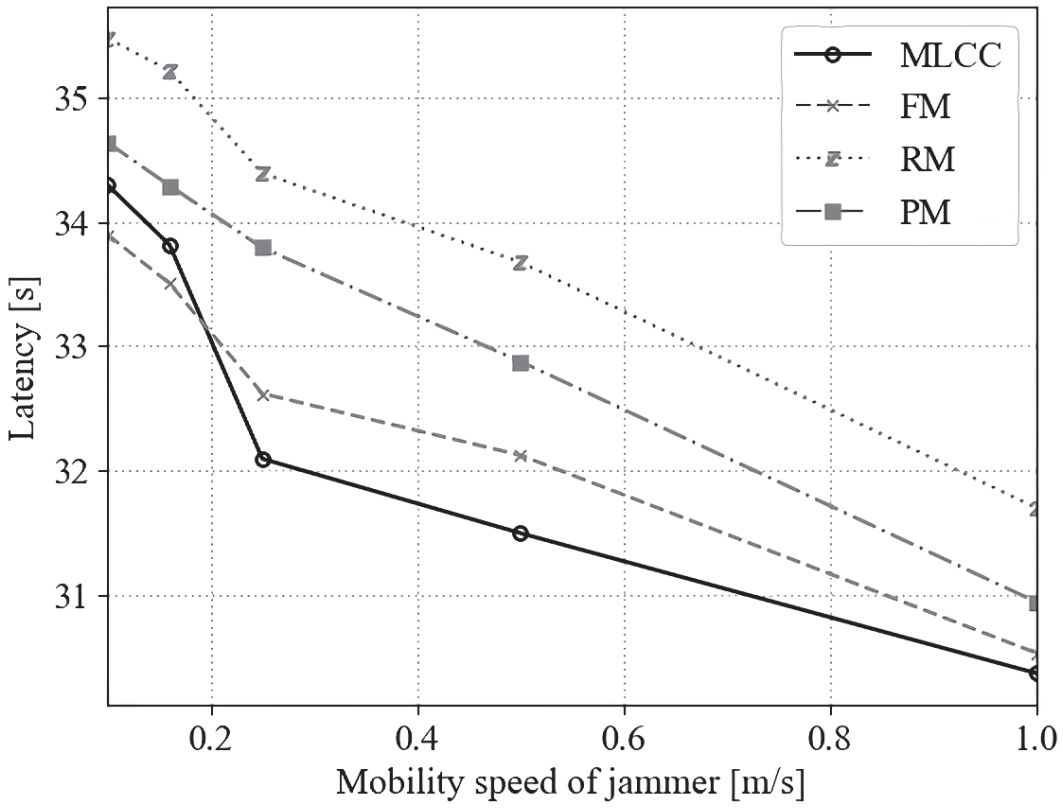
Fig. 7은 재머의 이동 속도가 증가함에 따른 네트워크 성능을 나타낸 결과로, γ는 15%, CoC는 70%, 탐지 간격은 5초로 고정하였다.



(a)


MLCC
FM
RM
PM
Energy consumption [mW]
18000
16000
14000
12000
10000
8000
0.2
0.4
0.6
0.8
1.0
Mobility speed of jammer [m/s]

(b)



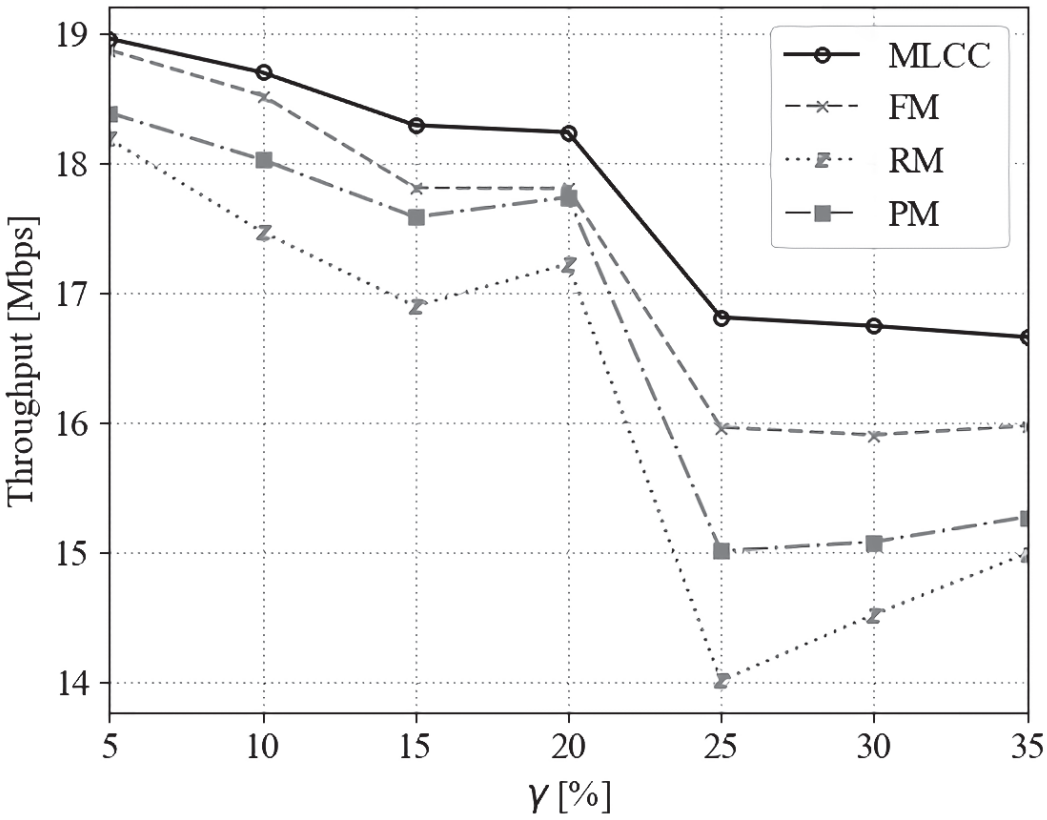
(c)

FIGURE 7. Network performance by mobility speed of jammer: (a) Throughput; (b) Energy Consumption; (c) Latency

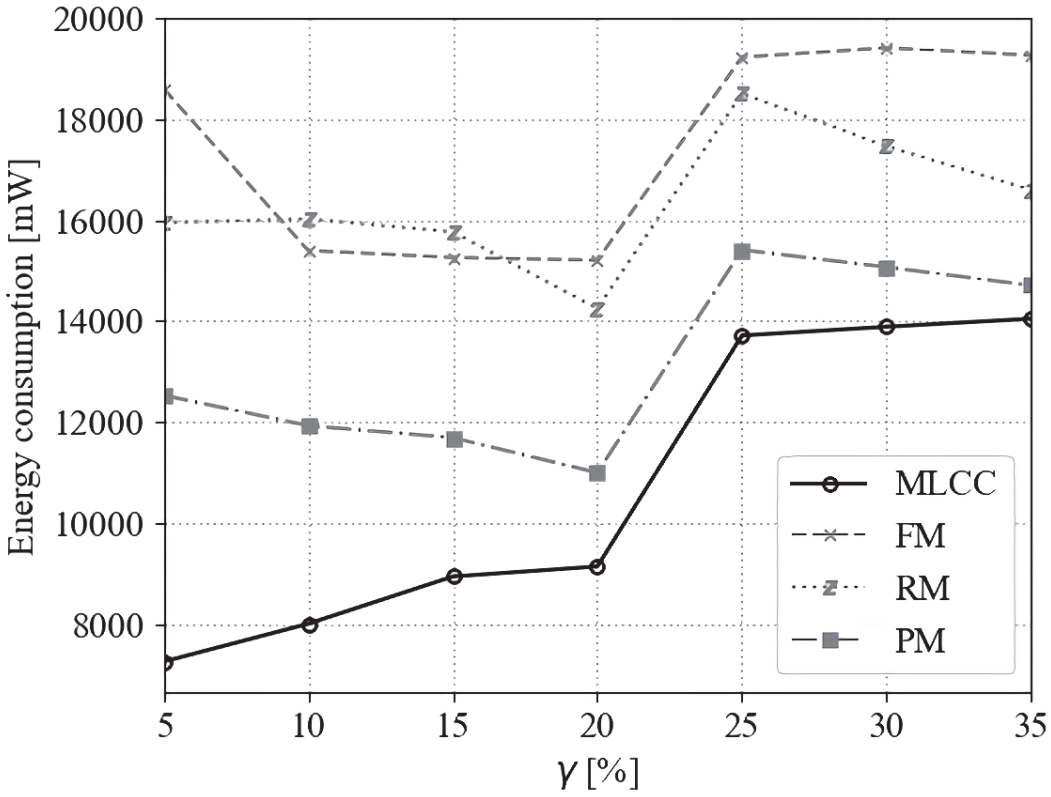
실험 결과에 따르면, 전반적으로 재머의 이동속도가 빠를수록 네트워크 성능이 좋아지는 결과를 보였다. 재머의 이동속도가 느릴 경우에는 재머가 특정 섹터에 머물게 되는 시간이 길어지게 되면서 재머의 공격에 대한 영향력이 커지기 때문에 충돌 횟수가 증가하여 성능의 열화 정도가 크다. 또한, 재머의 이동 속도가 탐지 속도보다 빠른 환경에서는 MLCC가 가장 효율적이었지만, 재머의 이동속도가 비교적 느린 0.25m/s 이하인 환경에서는 FM과 MLCC의 격차가 좁아진다. 이것은 재머의 위치를 기반으로 탐지를

수행하는 FM이 재머가 위치하는 섹터와 가장 멀리 위치하는 낮은 간섭 레벨의 섹터로 데이터를 전송하기 때문에 재머의 이동속도가 느릴수록 FM의 효율성이 높아지는 것이다. 또한, 처리율과 지연 시간은 RM, PM, FM 순으로 성능이 안 좋았고, 에너지 소모량은 RM, FM, PM 순으로 성능이 안 좋았다. RM은 최소 홉으로 이동하는 것을 고려하지 않고 무작위로 1개의 경로를 선정하기 때문에 가장 비효율적인 경로를 선정한다. 또한, FM은 데이터를 인근 섹터들에 무작위로 전송 시도하여 최적의 경로를 선정하지만, 데이터를 여러 번 전송하는 과정에서 에너지 소모량이 크다. 본 실험에서 PM은 null data packet을 3개의 랜덤 경로에 전송해본 뒤 최적의 경로를 선정하기 때문에 FM에 비하면 소모되는 에너지량은 적지만, 후보 경로 3개를 무작위로 선정한다는 점에서 FM보다 비효율적인 경로를 선정한다.

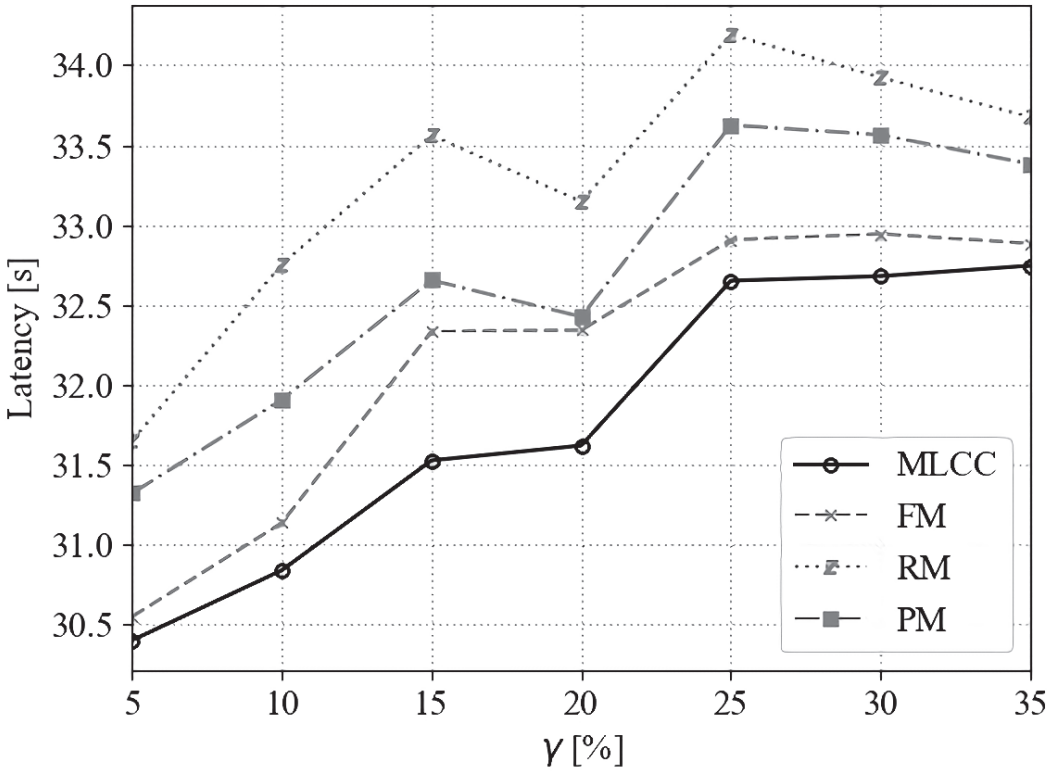
Fig. 8은 정상 스마트 리피터 노드 대비 JN의 비율인 γ가 증가함에 따른 네트워크 성능을 비교한 결과로, CoC는 70%, 재머 탐지를 수행하는 탐지 간격은 4초, 재머의 이동 속도는 0.5m/s로 고정한 환경에서의 결과이다.


MLCC
FM
RM
PM
Throughput [Mbps]
19
18
17
16
15
14
5
10
15
20
25
30
35
γ [%]

(a)


20000
18000
16000
14000
12000
10000
8000
Energy consumption [mW]
5
10
15
20
25
30
35
γ [%]
MLCC
FM
RM
PM

(b)



(c)

FIGURE 8. Network performance by rate of jammer node: (a) Throughput; (b) Energy Consumption; (c) Latency

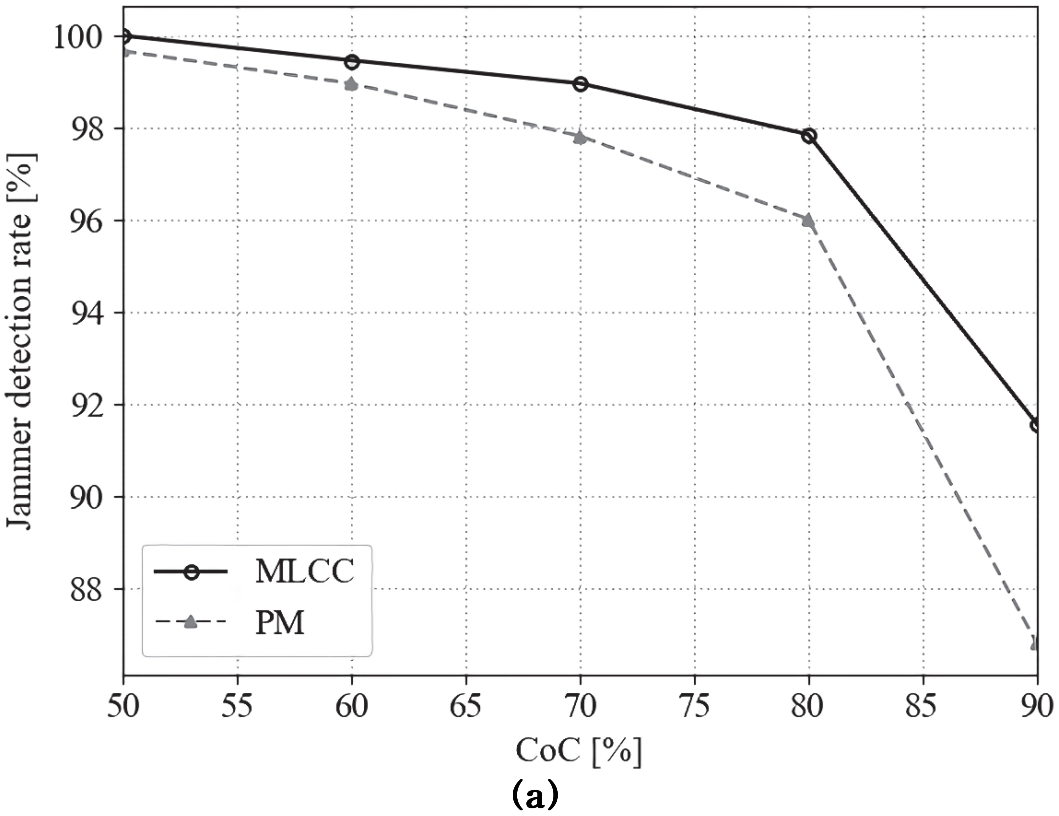
전반적으로 재머의 비율이 증가함에 따라, 처리율은 감소하고 에너지 소모량과 지연 시간은 증가하였다. 이는 네트워크 내 분포하는 재머의 비율이 높을수록 데이터를 전송하는 과정에서 재머가 위치하는 섹터를 홉으로 거칠 확률이 높으므로 전체적으로 네트워크 성능이 저하되는 것이다. 또한, 재머가 0.5m/s로 비교적 빠르게 이동하는 환경이기 때문에 MLCC가 재머 비율의 변화와 상관없이 가장 효율적인 결과를 보였다. 이는 본 연구에서 제안한 머신러닝 기반의 협업 탐지 및 회피 방법이 네트워크 간섭 상황에 신속하게 대처할 수 있음을 보였다.

이와 같이 지능형 모바일 재머가 분포하는 환경에서도 제안하는 MLCC 성능이 처리율, 에너지 소모량, 지연 시간 측면에서 종래 FM, RM, PM 대비 우수하였다. FM은 실제 재머 신호를 토대로 라우팅 경로를 설정하기 때문에 처리율과 지연 시간 측면에서 우수했지만, 에너지 소모량 측면에서 가장 비효율적인 결과를 보였고, RM은 탐지 결과와 상관없이 랜덤으로 경로를 설정하기 때문에 재머를 적절히 회피하지 못하여 모든 성능 지표에서 비효율적인 결과를 보였다. 그에 반해 여러 개의 경로 중 재머와 가장 충돌이 적은 경로를 선정하는 PM은 비교적 전반적인 성능 지표에서 효율적인 결과를 보였다.

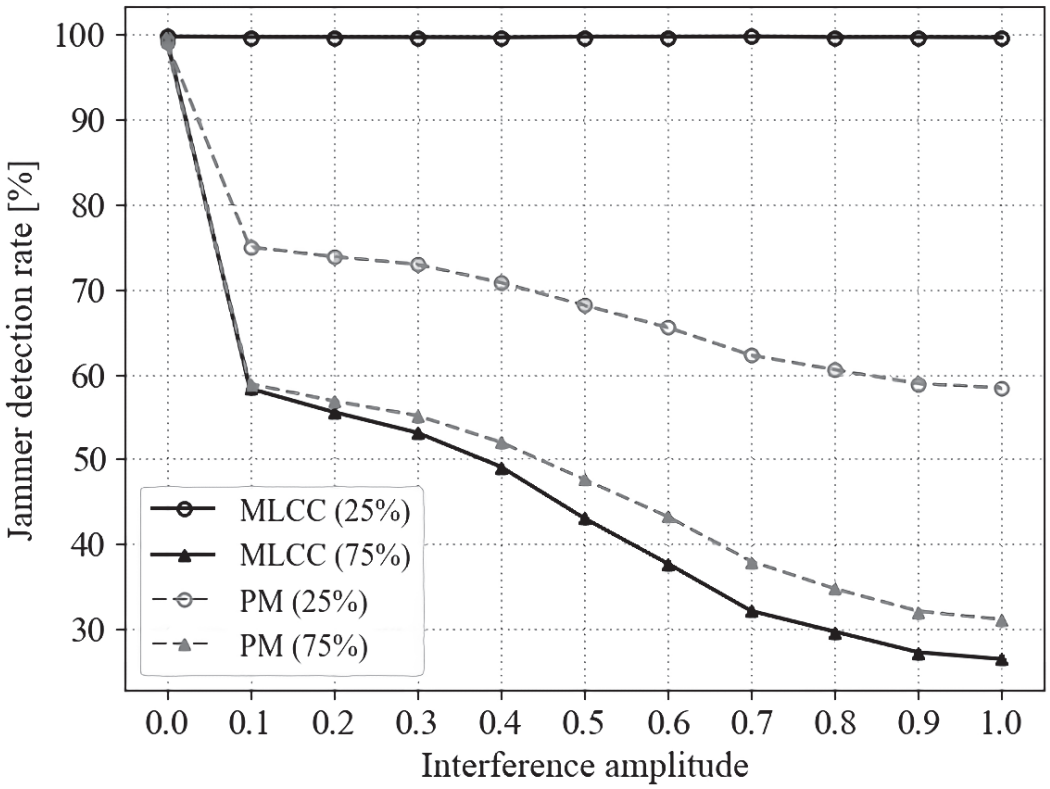
(2) 재머 탐지 정확도 성능 비교 분석

본 장에서는 MLCC의 재머 탐지 정확도 지표 성능을 검증한다. 앞선 실험 결과를 토대로, 모바일 장치에서 중요하게 고려되어야 하는 에너지 소모량과 처리율 측면에서 우수한 PM과 성능 비교를 수행한다.

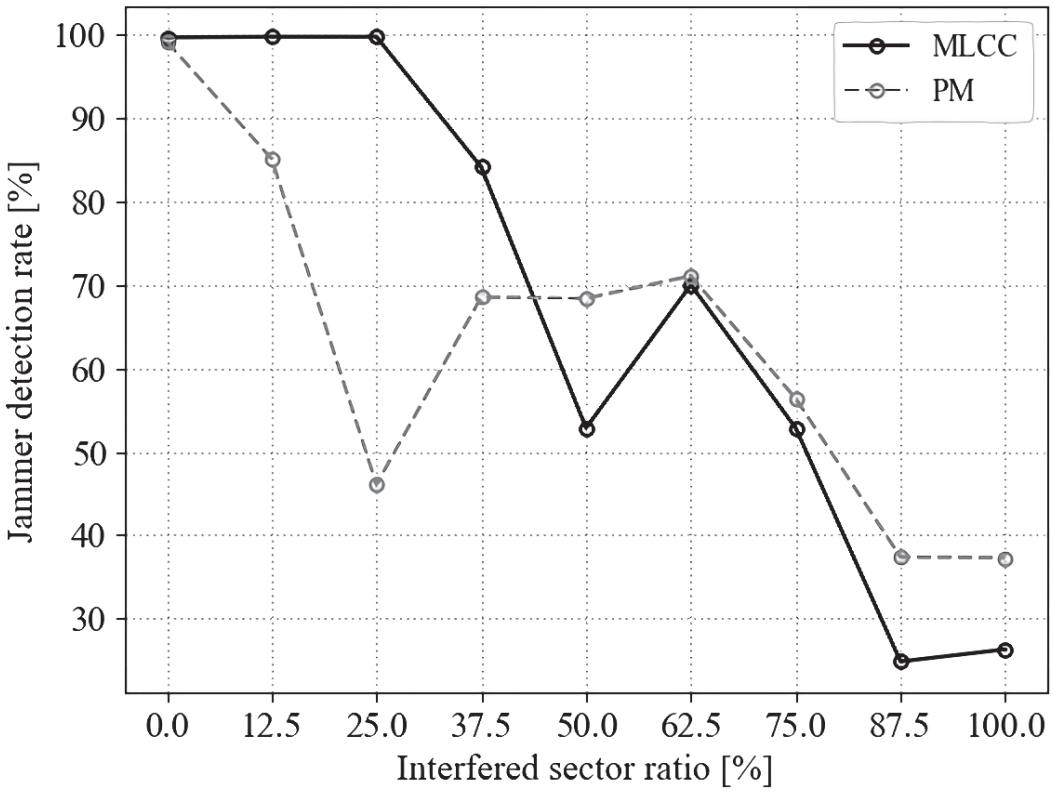
Fig. 9는 재머 탐지 성능을 비교한 결과이다. Fig. 9(a)는 CoC가 증가함에 따른 PM의 종래 로컬 기반 재머 탐지 방식과 MLCC의 협력 탐지 방식의 탐지 정확도 성능을 비교한 결과로 γ은 15%로 고정하고, CoC를 변경하며 성능을 평가했다. Fig. 9(b), (c)는 비의도적 간섭이 포함된 네트워크 환경에서 MLCC와 PM의 탐지 성능을 비교한 결과로 γ를 25%로, CoC를 0.7로 고정하여 실험했다.



(a)


Jammer detection rate [%]
100
90
80
70
60
50
40
30
0.0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
0.9
1.0
Interference amplitude
MLCC (25%)
MLCC (75%)
PM (25%)
PM (75%)

(b)



(c)

FIGURE 9. Performance of jammer detection accuracy: (a) CoC; (b) Interference amplitude; (c) Interfered sector ratio

Fig. 9(a)의 실험 결과에 따르면, 재머의 간섭 외에 비의도적인 간섭이 없는 환경에서는 MLCC의 탐지 성능이 PM보다 좋은 결과를 보였다. 또한, 재머 탐지 CoC가 높아질수록 재머 탐지 정확도는 저하되었다. 이는 탐지 기준이 높아지는 것이기 때문이다. 특히 CoC가 가장 큰 90%일 때 PM 대비 MLCC의 재머 탐지 정확도가 최대 4.77%만큼 개선되었다. 이는 MLCC가 다수개의 노드에서 취합한 결과로 정확도 평균치를 산출하여 재머 여부를 판별했기 때문에 1개의 노드에서만 판별한 결과 대비 정확도가 높게 도출되었다.

Fig. 9(b)는 재머를 탐지하는 과정에서 클러스터 내의 간섭 소스의 간섭 크기를 의미하는 Interference amplitude에 따른 탐지 성능을 비교한 결과이고, 범례는 모델명과 Interfered sector ratio를 가리킨다. Interfered sector ratio는 전체 클러스터 내 간섭 소스를 포함하는 섹터의 비율을 의미한다. 예를 들어, Interfered sector ratio가 25%일 때는 8개의 섹터 중 2개의 섹터에 간섭이 포함된 환경이며, 75%일 때는 8개의 섹터 중 6개의 섹터에 간섭이 포함된 환경을 의미한다. 전체적으로 Interference amplitude가 증가할수록 탐지 성능이 급격하게 저하되는 결과를 보였다. 또한, 클러스터 내 간섭이 포함된 섹터가 많은 환경인 75%일 때 탐지 성능이 더 낮아지는 모습을 보였고, 간섭이 포함된 섹터가 적은 환경인 25%일 때는 MLCC의 탐지 성능은 유지되지만, PM의 성능은 급격히 저하되는 것을 확인할 수 있다. 이는 클러스터 내 간섭이 적게 포함되어 있을 때, 전체 클러스터에 공유되는 글로벌 정보에 영향을 거의 미치지 않은 것으로 MLCC가 평균 99.72%로 높은 탐지율이 유지되었다. 그에 반해 PM은 MLCC보다 간섭의 영향을 즉각적으로 받게 되는 노드의 비율이 높기 때문에 간섭이 조금만 포함되어도 탐지율이 급격히 떨어진다. 간섭이 75% 포함된 환경에서는 PM이 MLCC보다 성능이 높은 모습을 보였다. 이는 전체 스마트 리피터 노드에서 재머 여부를 판별한 결과를 취합하여 탐지하는 MLCC가 간섭으로 인해 전체 섹터에 미치는 영향이 매우 커진다는 점에서 탐지율이 급격하게 저하된다.

Fig. 9(c)는 네트워크 내 간섭 소스를 포함하는 섹터의 비율에 따른 탐지율 성능을 비교한 결과로, Interference amplitude는 0.5로 고정하여 결과를 비교했다. 네트워크 내 1개의 클러스터 내에서 간섭이 37.5% 이하로 포함될 때 MLCC가 더 효과적인 결과를 보였고, 25% 이상의 간섭이 포함되는 시점부터 MLCC의 탐지율이 급격하게 저하되면서 PM이 더 효율적인 결

과를 보였다. 이에 따라 클러스터 내 섹터에 간섭의 포함 정도가 커지는 환경에서는 글로벌 정보를 활용하는 MLCC가 비효율적인 결과를 보였다.

Ⅵ. 결론 및 향후 연구

무선 네트워크 기술이 급속도로 발전함에 따라, 네트워크 속도 및 연결성 측면에서 개선된 통신 성능을 제공한다는 이점이 있지만, 여러 보안성 문제도 함께 대두되고 있다. 특히 초고속, 초저지연, 초밀접의 5G 무선 네트워크 기술이 보편화되면서 네트워크 통신량이 급증하였고, 스마트 인프라의 무선 통신을 방해하는 재밍 공격의 위험성이 커지고 있다.

본 연구에서는 3GPP NR에서 논의 중인 스마트 리피터 환경에서 모바일 재머를 탐지 및 회피하기 위한 MLCC 기법을 제안하였다. 종래 연구에서는 주로 PDR, RSSI와 같은 단일 탐지 메트릭을 기반으로 탐지하는 방안이 제안되었으며, 최근에는 기계학습 기반 탐지 방법이 연구되고 있지만, 특정 노드에 학습이 과중되는 한계점이 있다. 또한, 대부분의 재밍 대응 기술이 재머 탐지에만 초점을 맞추고 있고, 재머를 회피하기 위한 방안에 관한 연구는 미흡했다. MLCC는 분산된 고정 노드들이 머신러닝을 기반으로 협업하여 지능형 재머를 탐지함으로써 기존 로컬 탐지 방법 대비 탐지 성능을 높였다. CH인 AP가 CN인 스마트 리피터와 협업하여 판별한 재머의 위치를 네트워크에 공유하여 각 노드가 효율적인 라우팅 경로를 산정할 수 있다. 또한, 본 연구에서는 종래 연구에서는 고려되지 않았던 모바일 재머 환경에서 MLCC의 성능을 입증하였고, 지능형 재머 공격자의 대응 방법을 다룸으로써 고도화되어가는 지능형 위협에 대응할 수 있다. 실험 결과에 따르면 모바일 재머 환경에서도 종래 모델 대비, 재머 탐지 정확도, 처리율, 에너지 소모량, 지연 시간 측면에서 MLCC의 효율성을 입증하였다. 또한, 네트워크 내 간섭이 많이 포함된 환경에서는 로컬 탐지 기반의 파일럿 신호 기반 라우팅을 활용함으로써 적응적으로 재머를 회피하는 방안을 제

안하였다.

본 연구에서는 데이터셋 기반의 시뮬레이션 모델에서 제안한 방법과 종래의 방법을 성능 평가했지만, 향후 연구에서는 실제 테스트베드 환경에서 MLCC을 구현하여 성능을 검증할 계획이다. 또한, 스마트 리피터 환경에서 업링크와 다운링크를 타겟으로 하는 재밍 공격의 탐지 방법을 연구하고, 비의도적 간섭이 혼재하는 환경에서도 탐지 성능을 개선하는 연구를 진행할 예정이다.

참 고 문 헌

[1] X. Wei, T. Wang, C. Tang, J. Fan, Collaborative mobile jammer tracking in multi-hop wireless network, Future Gener. Comput. Syst. 78 (2018) 1027 - 1039. https://doi.org/10.1016/j.future.2016.11.032.

[2] J. Villain, V. Deniau, C. Gransart, A. Fleury, E.P. Simon, Characterization of IEEE 802.11 Communications and detection of low-power jamming attacks in noncontrolled environment based on a clustering study, IEEE Syst. J. 16 (2022) 683 - 692. https://doi.org/10.1109/JSYST.2020.3045365.

[3] Y. Arjoune, S. Faruque, Smart jamming attacks in 5-g new radio: A review, in: 2020 10th Annual Computing and Communication Workshop and Conference (CCWC), 2020, pp. 1010 - 1015. https://doi.org/10.1109/CCWC47524.2020.9031175.

[4] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, G. Pantziou, A survey on jamming attacks and countermeasures in wsns, IEEE Commun. Surv. Tutorials. 11 (2009) 42 - 56. https://doi.org/10.1109/SURV.2009.090404.

[5] M. Louis, S. Andreas, D. Cristos, M. Louis, L. Marco, R. Omid, “ENISA Threat Landscape Report 2018”, European Network and Information Security Agency, 2019, pp. 47 - 53.

[6] K.P. Vijayakumar, P. Ganeshkumar, M. Anandaraj, A novel jammer detection framework for cluster-based wireless sensor networks, J. Wirel. Netw. 35 (2016). https://doi.org/10.1186/s13638-016-0528-1 .

[7] K.P. Vijayakumar, P. Ganeshkumar, M. Anandaraj, K. Selvaraj, P. Sivakumar, Fuzzy logic-based jamming detection algorithm for cluster-based wireless sensor network, Int. J. Commun. Syst. 31 (2018). https://doi.org/10.1002/dac.3567.

[8] B. Upadhyaya, S. Sun, B. Sikdar, Machine learning based jamming detection in wireless IoT networks, in: IEEE VTS Asia Pacific Wireless Communications Symposium (APWCS), 2019, pp. 1 - 5. https://doi.org/10.1109/VTS-APWCS.2019.8851633.

[9] S.G. Hymlin Rose, T. Jayasree, Detection of jamming attack using timestamp for wsn, Ad Hoc Netw. 91 (2019) 101874. https://doi.org/10.1016/j.adhoc.2019.101874.

[10] N.F.A. AL-Shaihk, R. HassanpourN. AL Shaihk and R, Active Defense Strategy against Jamming Attack in Wireless Sensor Networks, IJCNIS. 11 (2019) 1 - 13. https://doi.org/10.5815/ijcnis.2019.11.01.

[11] S. Bag, B. Roy, Two channel hopping schemes for jamming resistant wireless communication, in: 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), IEEE Publications (2013) 659 - 666. https://doi.org/10.1016/j.comnet.2017.03.009.

[12] Qualcomm, RWS-210019: NR Smart Repeaters, 2021. [Online]. Available: https://www.3gpp.org/ftp/TSG_RAN/TSG_RAN/TSGR_AHs/2021_06_RAN_Rel18_WS/Docs/RWS-210019.zip

[13] The evolution of security in 5g, in: 5G Americas White Paper, 2019.

The Evolution of Security in 5G - 5G Americas. [Online]. Available: https://www.5gamericas.org/the-evolution-of-security-in-5g-2/

[14] M. Hachimi, G. Kaddoum, G. Gagnon, P. Illy, Multi-stage jamming attacks detection using deep learning combined with kernelized support vector machine in 5-g cloud radio access networks, in: 2020 International Symposium on Networks, Computers and Communications (ISNCC), 2020, pp. 1 - 5. https://doi.org/10.1109/ISNCC49221.2020.9297290.

[15] S. Gecgel, C. Goztepe, G. Karabulut Kurt, Jammer Detection Based on Artificial Neural Networks: A Measurement Study, Association for Computing Machinery, p. 2019. https://doi.org/10.1145/3324921.3328788.

[16] A. Jain, G.S. Kasturi, J. Singh, Detection and classification of radio frequency jamming attacks using machine learning, J. Wirel. Mob. Netw. Ubiquitous Comput. Depend. Appl. (JoWUA). 11 (2020) 49 - 62. https://doi.org/10.22667/JOWUA.2020.12.31.049.

[17] K.P. Vijayakumar, K.P. Pradeep Mohan Kumar, K. Kottilingam, T. Karthick, P. Vijayakumar, P. Ganeshkumar, An adaptive neuro-fuzzy logic based jamming detection system in WSN, Soft Comput., Berlin, Heidelberg. 23 (2019) 2655 - 2667. https://doi.org/10.1007/s00500-018-3636-5.

[18] O. Osanaiye, A.S. Alfa, G.P. Hancke, A statistical approach to detect jamming attacks in wireless sensor networks, Sensors (Basel). 18 (2018). https://doi.org/10.3390/s18061691.

[19] G. Han, L. Liu, W. Zhang, S. Chan, A Hierarchical Jammed-Area

Mapping Service for Ubiquitous Communication in Smart Communities, IEEE Commun. Mag. 56 (2018) 92 - 98. https://doi.org/10.1109/MCOM.2018.1700399.

[20] M.N. Mahdi Nouri, M.M. Mohsen Mivehchy, M.F.S. Mohamad Farzan Sabahi, Target recognition based on phase noise of received laser signal in lidar jammer, Chin. Opt. Lett. 15 (2017) 100302. https://doi.org/10.3788/COL201715.100302.

[21] J. Lee, J. Kang, S.S. Lee, Jamming-resilient adaptive network protocol in wireless networks, Lecture Notes in Electrical Engineering. 01 (2016) 3 - 9. https://doi.org/10.1007/978-981-10-0557-2_1.

[22] H. Bany Salameh, R. Derbas, M. Aloqaily, A. Boukerche, Secure Routing in Multi-hop iot-Based Cognitive Radio Networks Under Jamming Attacks, New York, New York. https://doi.org/10.1145/3345768.3355944, 2019.

[23] P. Bhavathankar, S. Sarkar, S. Misra, Optimal decision rule-based ex-ante frequency hopping for jamming avoidance in wireless sensor networks, Computer Networks. 128 (2017) 172 - 185. https://doi.org/10.1016/j.comnet.2017.03.009.

[24] B. Duan, D. Yin, Y. Cong, H. Zhou, X. Xiang, L. Shen, Antijamming path planning for unmanned aerial vehicles with imperfect jammer information, in: 2018 IEEE International Conference on Robotics and Biomimetics (ROBIO), 2018, pp. 729 - 735. https://doi.org/10.1109/ROBIO.2018.8665238.

[25] W. Xu, T. Wood, W. Trappe, Y. Zhang, Channel Surfing and Spatial

Retreats: Defenses Against Wireless Denial of Service, New York, New York, Association for Computing Machinery. https://doi.org/10.1145/1023646.1023661, 2004.

[26] R. Flamini, D. De Donno, J. Gambini, F. Giuppi, C. Mazzucco, A. Milani, L. Resteghini, Towards a heterogeneous smart electromagnetic environment for millimeter-wave communications: An industrial viewpoint, IEEE Trans. Antennas Propag. (2022) 1 - 1. https://doi.org/10.1109/TAP.2022.3151978.

[27] Qualcomm, RP-201140: Smart Repeaters-Motivation, 2020.

[28] W. Hong, Z. H. Jiang, C. Yu, J. Zhou, P. Chen, Z. Yu, H. Zhang, B. Yang, X. Pang, M. Jiang, Y. Cheng, M. K. T. Al-Nuaimi, Y. Zhang, J. Chen, S. He, Multibeam Antenna Technologies for 5G Wireless Communications, IEEE Transactions on Antennas and Propagation. 65 (2017) 6231-6249, 10.1109/TAP.2017.2712819.

[29] Xiao, Y., Liu, J., Quan, J., Shen, Y., Jiang, X., On Secrecy Performance of Multibeam Satellite System with Multiple Eavesdropped Users. in: International Conference on Mobile Ad-hoc and Sensor Networks, 2017, pp. 402-412. https://doi.org/10.1007/978-981-10-8890-2_30.

[30] S. Moon, M. Seok, I. Yeom, Multibeam anttena device and multibeam generating method, KR Patent, 10-2019-0076695, filed December 22, 2017, Issued July 02, 2019.

[31] B.N. Priyanka, R. Jayaparvathy, D. DivyaBharathi, Efficient and dynamic cluster head selection for improving network lifetime in WSN using whale optimization algorithm, Wireless Pers. Commun.

123 (2022) 1467 - 1481. https://doi.org/10.1007/s11277-021-09192-7.

[32] I. Almomani, B. Al-Kasasbeh, M. Al-Akhras, WSN-DS: A dataset for intrusion detection systems in wireless sensor networks, J. Sens. 2016 (2016) 1 - 16. https://doi.org/10.1155/2016/4731953.

[33] F. Wu, W. Yang, J. Ren, F. Lyu, P. Yang, Yaoxue Zhang, and Xuemin Shen. Named Data Networking Enabled Power Saving Mode Design for WLAN, IEEE Transactions on Vehicular Technology. 69 (2020) 901 - 913.

[34] MediaTek Inc., Comparison of Calibration Methodology for MAC, 2014-05-15, 2014. [Online]. Available: https://mentor.ieee.org/802.11/dcn/14/11-14-0677-00-00ax-mac -simulation -calibration-methodology-comparison.pptx

ABSTRACT

Machine learning-based cooperative clustering for jamming attack detection and avoidance in beyond-5G networks

So-Eun Jeon
Department of Future Convergence Technology Engineering
Graduate School of Sungshin University

High-throughput, low-latency, high-density 5G wireless network technologies have become commonplace, although the damage caused by jamming attacks on wireless communication networks has increased. In particular, the smart repeaters proposed as key candidate technologies in 3GPP New Radio (NR) and playing the role of smart infrastructure in beyond-5G network environments are increasingly vulnerable to intelligent attacks from mobile jammers. Conventional jamming defense technology is dependent on a detection method that relies on fragmentary and local information, making it difficult to respond to advanced jamming attacks. Although machine learning-based detection methods have recently been studied, learning is dependent on a specific node, and because it depends on local detection results, it cannot respond globally.

This study proposes a machine learning-based cooperative clustering (MLCC) technique that efficiently avoids jamming using cooperative detection techniques in smart repeaters for beyond-5G networks. This results demonstrate that the proposed MLCC technique improves detection accuracy by up to 5.5 % and an average of 1.9 %. In addition, when evaluating the performance according to the movement speed of the jammer, MLCC improved the throughput by up to 35.77 % and an average of 17.49 %, and decreased energy consumption by up to 43.4 %, and an average of 41.09 %, and latency by up to 6.67 % and an average of 4.97 % compared to random model. The proposed MLCC could be applied to beyond-5G smart repeater network environment for an efficient defense against jamming attacks.