이 일 구 교수 지도

석사학위 청구논문

협력적인 공격 탐지 및 대응 기법을 통한 가시광 통신 보안 시스템

2022

성신여자대학교 대학원

미래융합기술공학과

박 소 현

협력적인 공격 탐지 및 대응 기법을 통한 가시광 통신 보안 시스템

이 일 구 교수 지도

이 논문을 석사학위논문으로 제출함

2021년 11월

성신여자대학교 대학원

미래융합기술공학과

박 소 현

인 준 서

박소현의 석사학위 논문으로 인준함

2021년 11월

심사위원장 김 성 민 (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

논문개요

최근 4차 산업 기술의 발전과 함께 초연결, 초저지연, 초실감 지능 정보 사회를 실현하기 위한 광대역 근거리 무선통신 시스템의 필요성이 대두되고 있다. 이러한 기술적 수요를 만족시킬 수 있는 차세대 통신 후보 기술 중 가시광 통신(VLC, visible light communication)은 조명 빛을 통신 광원으로 사용할 수 있는 기술로서 편리하고 환경친화적일 뿐 아니라, 에너지와 주파수 사용 효율성이 뛰어나다. 그리고 가시광 통신은 가시광의 직진성과 비투과성 때문에 높은 수준의 보안성을 가지지만, 밀집 메시 네트워크 환경의 가시광 통신 노드 중 일부 노드가 외부 공격에 의해 해킹되어 재밍 공격을 하는 경우 심각한 성능 열화를 초래할 수 있다. 그러나 종래에는 VLC 재밍 공격 가능성에 관한 연구들은 있었지만, 공격을 효과적으로 탐지하여 대응하는 방법은 거의 연구되지 않았다. 본 연구에서는 스마트 LED 기반 VLC 시스템에서 재밍 공격을 협력적으로 탐지하고 대응할 수 있는 방법을 제안한다. 본 연구의 실험 결과에 따르면 제안하는 협력 방식은 91%의 공격 탐지 정확도를 보였고, k-random 방식보다 1.82배 향상됨을 보였다. 제안하는 협력 방식은 장애물이 많은 환경에서도 84%의 최소 탐지율을 보이며 k-random 방식보다 1.68배 향상된 우수한 공격 탐지 성능을 증명했다.

목 차

표 차 례

그림 차례

Ⅰ. 서 론

가시광 통신(VLC, visible light communication)은 무선 주파수(RF, radio frequency)를 이용한 무선통신 기술보다 넓은 주파수 대역을 이용하기 때문에 방대한 양의 데이터를 빠르게 전송할 수 있고 RF spectrum crunch 문제점을 해결할 수 있다 [1]. VLC는 조명 장치를 이용해 통신 기능을 동시에 지원하기 때문에 시스템이 단순해지고 에너지 효율성이 향상되어 친환경적이다 [2]. 그리고 회절 및 투과를 잘하는 RF 전파와 다르게 벽을 통과할 수 없는 전파 특성 때문에 보안성이 뛰어나다 [3]. VLC의 광원으로는 LED(light-emitting diode)와 LD(laser diode) 등이 사용될 수 있다. 실내 VLC 시스템에서는 시력보호 제한이 적은 LED가 주로 사용되고 있으며, 실외에서는 더욱 빠르고 멀리 데이터를 전송할 수 있는 LD가 사용되고 있다. LD는 에너지 효율성, 성능, 비용, 시력보호 문제로 인해 적용 분야가 제한된다 [4]. 최근 LED와 LD 기반의 VLC는 스마트 시티, 스마트 홈을 비롯하여 수중 통신, 지능형 교통 시스템(ITS, intelligent transport system) 등에 사용되고 있다 [5].

VLC는 전파의 직진성과 비투과성 때문에 데이터 전송이 이루어지고 있는 공간 이외에서는 데이터의 유출과 조작이 어려워 보안성이 높다고 인식되고 있다[3]. 빠른 데이터 전송속도 이점으로 인하여 스마트 오피스 공간에서 스마트 LED를 이용하여 VLC 시스템을 구축할 수 있지만 [8], 끊임없는 지능정보 시스템을 구축하기 위한 밀집 메쉬 네트워크 환경에서 브로드캐스팅과 중첩 특성 때문에 도청, 재밍(jamming)과 같은 공격에 취약하다는 문제점이 있다 [6],[7]. 스마트 LED는 에너지 효율성과 편의성, 보안성 향상을 위해 광원의 세기와 스펙트럼 특성을 사용자가 쉽게 원격 제어할 수 있다. 이렇게 프로그래머블한 스마트 LED 시스템에 악의적인 조작을 가하여 인접 LED의

가용성을 침해하는 재머(jammer)로 사용할 수 있다 [9]. 재밍은 데이터의 정상적인 송신을 거부하여 비트 에러율(BER, bit error rate)을 증가시키고 데이터의 재전송률을 높인다. 이는 단위 시간 동안 성공적으로 전송되는 데이터의 양을 의미하는 스루풋(throughput) 저하의 원인이 되고, 더욱 많은 에너지를 소모하여 에너지 효율성(EE, energy efficiency)의 열화를 초래한다.

본 연구에서는 VLC 시스템에 대한 재밍 공격 탐지 방법과 이에 대응할 수 있는 보안 방법을 제안한다. VLC를 이용하는 스마트 오피스 환경에서 LED는 특정 위치에 고정되어 있기 때문에 LED의 영향은 항상 동일하다고 가정할 수 있다. 본 연구에서는 인접한 LED 간 협력적인 통신 성능 비교를 통하여 재밍 공격을 탐지 및 대응하는 방법을 제안하였다.

논문의 주요 기여점은 다음과 같다.

1) 스마트 LED 기반 VLC 환경에서 재밍 공격 시스템을 모델링하였다. LED의 LOS(line of sight) 특성을 이용하여 재밍 공격으로 인한 각 VLC 링크의 성능 열화 패턴을 분석 및 유형화하였다.

2) LED 간 협력을 통한 재밍 공격 탐지 방법을 제안하고, 공격 탐지율을 측정하여 협력 탐지 방법의 성능을 평가하였다.

3) LED 협력 송신 기법을 통해 재밍 공격에 효과적으로 대응할 수 있는 방법을 제안한다. 각 대응 기법의 Effective data rate과 EE를 비교하여 가장 효율적인 공격 대응 기법을 분석했다.

논문은 다음과 같이 구성된다. 2장에서는 관련 연구를 소개하고, 3장에서는 연구에서 가정한 VLC 시스템 모델을 소개한다. 4장에서는 VLC 공격 탐지를 위한 탐지 알고리즘을 설명하고, 재밍 공격에 대응할 수 있는 방법들을 소개한다. 5장에서는 시뮬레이션을 통해 공격 탐지 및 대응 시스템의 성능 및 효율성을 평가한다. 6장에서는 연구의 결론으로 논문을 마무리한다.

Ⅱ. 관련 연구

본 장에서는 VLC 보안과 관련된 선행 연구를 분석했다. Table I은 VLC 보안 관련 선행 연구를 정리한 표이다.

기존의 VLC 보안 관련 논문은 대부분 도청과 관련된 연구이고 재밍 공격에 대한 연구는 적다. 재밍 공격은 VLC 시스템의 셀간 간섭에 해당하는데 VLC 시스템의 성능 개선 측면에서 간섭을 완화하는 연구들은 다수 존재한다. 그러나, 기존 연구들은 VLC 시스템에서 재밍, 도청 등의 공격에 대응할 수 있는 다양한 방법들을 제안하지만, 공격을 효과적으로 탐지할 수 있는 방법을 제안하는 연구는 거의 없다. 본 연구는 VLC 시스템의 특성을 이용해 재밍 공격을 탐지, 대응하는 기법을 제안한다.

1. VLC 간섭 완화 기법

VLC 시스템에서 발생할 수 있는 간섭은 크게 셀내 간섭과 셀간 간섭(ICI, intercell interference)이 있다. 셀내 간섭은 동일 채널 간섭(CCI, cochannel interference)등의 간섭이 대표적이며 동일 채널 내 다른 장치의 채널 접근으로 대기 시간이 길어져 혼잡이 생기는 현상이다. CCI를 감소시키기 위한 대응 방안으로는 CSK(color shift keying) 등이 있다. CCI를 감소시키기 위한 기법으로 FOV(field of view)를 최적화하는 ADR(angle diversity receiver)에 대한 다수의 연구가 있다[10]-[13]. Eldeeb et al.은 기존 ADR을 보완하는 CFOV-ADR(constraint field of view angular diversity receiver) 를 제안하여 CCI 간섭을 감소시켰다 [10]. CFOV-ADR은 광검출기(PD, photodetector)의 FOV 각도를 최적화하여 인접 송신기로부터 오는 LOS 신호를 효과적으로 분리하는 방식이다. 시뮬레이션을 통해 모든 위치에서 기존 ADR보다 CFOV-ADR이 우수한 것을 증명하였고, CCI를 제거하기 위한 최적화된 각도를 제

TABLE I
Previous studies on VLC security

Previous studies	Performance / Security issues	Methods	Ref.	Main idea
VLC interference mitigation	Intracell interference	ADR	[10]-[13]	FOV를 최적화하는 ADR을 이용하여 ISI, CCI를 제거하여 셀내 간섭 완화
		OFDM	[14]	OFDM을 통해 스펙트럼 효율을 높이고 간섭 현상 최소화하는 공유 주파수 재사용 기술 제안
	Intercell interference (ICI)	ILIC	[15]	ILIC를 통해 다중 AP로 인한 통신 영역의 중첩으로 생기는 간섭 완화.
		ADR	[16]-[17]	ADR 최적화를 통한 ICI 완화
		Precoding	[18]-[19]	셀 조정, 프리코딩을 통한 ICI 완화
VLC PLS	Jamming	-	[9]	BER 평가지표를 이용해 악의적인 송신기에 의한 통신 중단 및 피해 분석.

		[20]	모든 수신 신호 중 재머의 신호를 간섭 신호로 처리하여 합법적인 신호 추출.
Eavesdropping	AN, Friendly jamming	[23]-[28]	도청자로 AN 또는 우호적 재밍 신호를 보내 데이터를 정상적으로 디코딩하지 못하게 함. 주로 AN, 우호적 재밍은 빔포밍과 함께 이용함.
	Beamforming	[29]-[31]	빔포밍 벡터를 최적화하여 정당한 사용자가 받게 되는 신호 파워를 최대화하고 도청자는 디코딩할 수 있는 충분한 신호를 받지 못하도록 함.
	LED selection	[32]-[34]	적절한 LED 링크를 선택하여 도청에 대응.
	Protected zone	[35]	도청자가 없는 영역을 보호구역으로 구축하여 정당한 사용자의 비밀률 향상.

시하였다. Hosney et al.은 CCI에 대한 해결책으로 ADR의 FOV를 제한하는 방식을 제안한다. 방 위치를 다르게 하여 VLC MIMO (Multi-Input Multi-O

utput) 시스템을 시뮬레이션하여 낮은 BER을 달성할 수 있도록 FOV를 최적화했다 [11]. Hosney et al.은 CCI로 인한 성능 저하에 대하여 VLC MIMO 시스템의 CFOV-ADR을 통한 관리 기법을 제안했다 [12]. CFOV-ADR를 활용하여 간섭 신호의 수를 감소시키고, 최대 우도법 이퀄라이저와 최소 제곱 채널 추정을 이용하여 간섭 신호를 해결하는 방식을 제안한다. 시분할 다중 접속 기법과 BER을 비교하여 향상된 성능을 증명하였다. Eldeeb et al.은 VLC 다운링크의 성능을 제한하는 CCI를 현저하게 감소시키는 CFOV-ADR을 제안했다 [13]. 광 검출기의 FOV를 최적화하고 제로포싱 알고리즘을 기존의 ADR에 적용하여 CCI를 제거하였다. 시뮬레이션 결과 해당 논문에서 제안하는 CFOV-ADR은 단일 수신기와 기존 ADR 대비 더 높은 SINR(Signal-to-Interference-plus-Noise Ratio)을 달성하는 것을 보여준다. Ibrahim et al.은 OCO-OFDM(Odd Clipped Optical Orthogonal Frequency-Devision Multiplexing) 기술을 개발하여 기존의 ACO-OFDM(Asymmetrical Clipped Optical OFDM)보다 스펙트럼 효율을 높이는 동시에 간섭 현상을 최소화할 수 있는 공유 주파수 재사용 기술을 제안했다 [14]. 공유 주파수 재사용 기술은 전체 대역폭을 공유 또는 재사용 대역으로 나누어 간섭 영역과 비간섭 영역을 구분하여 서비스를 제공하는 방식으로 간섭을 줄인다.

ICI는 다중 AP(access point)로 인한 통신 영역의 중첩으로 생기는 간섭 현상으로, 다양한 대응 방안이 존재한다. Kim et al.은 다중셀 VLC 시스템에서 발생할 수 있는 셀 간 간섭을 제거하기 위해 ILIC(inter-lighting interference cancellation)를 제안했다[15]. MISO(multi-input single-output) 가시광 통신 시스템과 같이 여러 개의 LED를 광원으로 사용하는 환경에서 전송 용량을 높이려면 각 LED에서 다른 데이터를 동시에 전송해야 한다. 이러한 경우에 수신 전력이 가장 높은 신호만 감지할 수 있는 문제점이 존재한다. ILIC 방식은 전체 신호 중 수신 전력이 가장 높은 신호를 간섭 신호로

설정하고 전체 수신 신호에서 제거하여 상대적으로 낮은 수신 전력 신호를 검출하는 방식으로 전체 평균 비트 오류율과 처리량을 향상할 수 있다. 또한, ICI를 완화하는 방법으로 ADR을 최적화하는 방식이 사용되기도 한다 [16]-[17]. Chen et al.은 일반적인 ADR의 측면 감지기 기울기의 각도를 최적화하여 기존 주파수 할당 기반의 ICI 완화 기법보다 셀 용량과 SINR 변동성을 개선했다 [16]. Játiva et al.은 시스템의 ICI를 완화하기 위한 피라미드형 ADR을 제안했다 [17]. 해당 연구에서는 select best combining, equal gain combining, maximum ratio combining(MRC) 방식을 비교 분석하여 MRC 방식이 ADR과 결합했을 때 가장 좋은 성능을 내는 것을 증명했다. 그리고 다수의 논문이 ICI를 줄이기 위한 방식으로 협력 또는 프리코딩 방식을 채택했다 [18]-[19]. Pham et al.에 따르면, 셀 내 간섭은 underlaying precoding 방식으로 처리할 수 있지만 ICI는 처리하기 어렵기 때문에 간섭을 완화하기 위한 셀 조정/협력 프리코딩 설계를 제안했다 [18]. 이 방법은 간섭 신호에 의한 채널 용량 열화 정도를 측정하여 제로포싱 기반의 프리코딩 기술을 활용한 간섭 완화 기법이다. 시뮬레이션을 통해 부분 협력 프리코딩 방식이 가장 우수한 성능 개선을 갖는 것을 보였다. [19]에서 Pham et al.은 ICI를 완화시킬 수 있는 제로포싱 프리코딩 방식을 제안했다. 셀 내의 LED 배열이 다른 셀의 LED 배열과 협력할 수 있도록 하여 조정된 프리코딩 방식을 설계하였다. 해당 방식은 사용자의 sum rate을 최대화시키며 송신 전력이 증가할수록 더욱 증가한다.

2. VLC 물리계층 보안

VLC에서 간섭은 의도와 상관없이 결과적으로 링크의 원활한 통신을 저해하는 재밍 공격이 될 수 있다. Blinowski et al.은 악의적인 송신기가 있는 경우 정상적인 통신이 방해받는 정도를 BER 평가 지표를 통해 측정하여 통신 중단 및 피해를 분석했다 [9]. 이 논문의 저자들은 악의적인 송신기가 있는 다양한 환경을 캐드 도구로 설계하고 각각의 환경에서 재머의 영향을 받는 영역을 계산하여 악의적인 송신기의 방해 범위를 분석했다. 시뮬레이션을 통해 악의적인 재머가 있는 환경에서 최대 75%의 영역의 전송을 방해할 수 있음을 증명했고, 송신기의 semi-angle이 증가함에 따라 재밍 영역이 증가하는 것을 입증했다. Ijaz et al.은 VLC 시스템에 설치된 악성 송신기의 적극적 공격에 대한 취약성을 보이고 스푸핑 공격과 재밍 공격을 막을 수 있는 방법을 제시했다 [20]. VLC 채널이 OMA(Orthogonal Multiple Access)인 경우와 NOMA(Non-orthogonal Multiple Access)인 경우를 구분하여 더 효과적인 인증 방법을 비교했다. 재밍 공격의 경우, 수신기는 악의적인 공격 노드의 신호와 합법적인 신호를 모두 수신하고, 합법적인 신호를 추출하기 위해 재머의 신호를 간섭 신호로 처리했다.

VLC PLS(physical layer security)에서 재밍과 관련된 연구는 매우 적고, 대부분의 VLC PLS 연구는 VLC의 도청 가능성을 토대로 WYNER's wiretap model 기반의 보안 채널 용량(secrecy capacity)을 이용한 채널 보안성 평가 및 도청 완화 방법을 제안했다 [21]. 보안 채널 용량이란 전체 채널 용량 중 도청되지 않고 안전하게 전달될 수 있는 데이터의 양을 의미한다. 도청에 대한 주요 해결 방법은 크게 인공 잡음 (AN, artificial noise) 및 우호적 재밍, 빔포밍, 그리고 LED 선택 기법이 있다.

AN은 원래의 수신자로 향하는 송신 신호를 도청자가 디코딩하지 못하도록 임의의 노이즈를 추가하는 도청 방지 기법이다 [22]. 대표적인 AN 방법은

우호적 재밍이 있다 [23]-[27]. VLC 시스템에서 우호적 재밍은 인접한 LED가 도청자로 재밍 신호를 보내 정당한 사용자가 수신해야 하는 데이터를 정상적으로 수신하지 못하게 하는 방법이다. Tian et al.은 jamming LED를 활용하여 다중 LED가 존재하는 실내 VLC 시스템의 비밀률(secrecy rate)을 분석했다 [23]. 정당한 사용자와 도청자가 모두 존재하는 다중 LED VLC 시스템에서 방해 신호를 활용하여 기밀성을 보장하는 방법을 제시하였다. 이 연구에서 저자들은 정당한 정보 송신자와 재머 간의 비율의 영향을 비교하여 평균 비밀률이 최대화되는 비율을 증명했다. 정당한 수신자는 우호적 재밍 신호를 탐지하고 무시할 수 있으며 도청자는 재밍 신호를 감지할 수 없다고 가정한다. 우호적 재밍 신호는 도청자의 SNR(Signal-to-Noise Ratio)을 떨어뜨려 시스템의 비밀률을 보장하는 방법을 통해 보안성을 향상시킨다. 송신 LED 개수의 절반이 정보를 포함하는 신호를 전송하고 나머지가 재밍 신호를 전송할 때, 결론적으로 평균 비밀률이 최대화되는 것을 보여준다. AN과 빔포밍은 주로 함께 이용되는데, Mostafa et al.은 권한이 없는 수신자에게서 VLC 통신 정보를 숨기고 안전한 통신을 보장하는 방법으로써 빔포밍과 우호적 재밍을 비롯한 대규모 LED 배열의 패턴 합성, 비밀률의 제한 등을 소개했다 [24]. 대규모 LED 배열의 패턴 합성은 대규모 LED가 설치된 방에서는 합법적인 수신기를 향한 빔이 임의의 방사선 패턴을 형성하게 되어 안전한 전송을 가능하게 하는 것을 의미한다. Cho et al.은 도청자가 랜덤하게 위치할 때 빔포밍과 재밍을 동시에 활용한 물리계층 보안을 고려했다 [25]. 랜덤한 재밍 신호가 섞여 있는 송신 신호는 원래의 데이터만을 추출하여 디코딩하기 어렵기 때문에 도청 방지에 효율적이다. 해당 논문에서는 빔포밍과 동시에 재밍 신호를 이용하여 랜덤한 도청자의 위치에 대한 통계 정보를 얻고 이를 통해 평균 비밀률을 극대화할 수 있음을 시뮬레이션을 통해 증명하였다. Arfaoui et al. 은 MISO VLC 도청 채널에서 AN 기반 빔포밍을 이용

했을 때의 보안 성능을 평가했다 [26]. 해당 연구에서는 도청자의 위치를 알지 못하여 완전하지 못한 채널 상태 정보 (CSI, channel state information)를 가지고 있을 경우 빔포밍을 최적화하는 방법을 제안했다. Al-Khori et al.은 RF/VLC 하이브리드 시스템에서의 브로드캐스팅 특성으로 인한 정보 기밀성 손상을 해결할 수 있는 우호적 재밍 기능과 빔포밍 설계를 제안했다 [27]. 이 논문의 저자들은 재밍 기능이 있는 다수의 릴레이를 활용한 하이브리드 RF/VLC 네트워크의 도청 공격 대응 방안의 효과를 시뮬레이션을 통해 비밀률을 측정하여 입증했다. 또한, 보안 채널 용량을 최대화할 수 있는 VLC의 빔포밍 설계를 제안했다. Pham et al.은 기존의 AN 기반 프리코딩에서 EE 이슈를 고려했다 [28]. VLC는 조명과 데이터 송신에 에너지가 소모되는데, 조명에 필요한 에너지는 고정된 상황에서 데이터 송신을 위한 에너지는 최적화될 필요가 있기 때문에 AN 기반 프리코딩에도 EE가 고려되어야 한다. 그 밖에도, 빔포밍만을 이용하여 VLC 도청에 대응하는 연구도 많이 이루어졌다 [29]-[31]. Xiao et al.은 MISO VLC 도청 채널에서 스마트 빔포밍을 통한 강화학습 기반 도청방지 프레임워크를 제안했다 [29]. Liang et al.은 안전구역에 있는 정당한 사용자가 수신하게 되는 신호 파워를 최대화하고 비 안전구역에 있는 도청자는 디코딩할 수 있는 충분한 신호를 받지 못하도록 빔포밍을 최적화하는 방법을 제안했다 [30]. Cho et al.은 기존의 빔포밍 연구들에서 능동적인 도청자 또는 수동적인 도청자 중 하나의 도청자 종류만 고려한 것과 달리 두 종류의 도청자에 대해 제로포싱 빔포밍을 통해 VLC 송신을 보호할 수 있는 제로포싱 빔포밍 벡터 최적화 문제를 해결했다 [31].

적절한 LED 선택을 통해 VLC 도청에 대응할 수 있다 [32] - [34]. Garg et al.은 [32]와 [33] 에서 두 개의 LED 요소로 이루어진 송신기를 이용하여 두 개의 LED 링크 중 비밀률이 더 높은 링크를 선택해 전송하는 방식으로 도청에 대응하는 방법을 제안했다. [33]에서는 파일럿 신호를 이용해 CSI를 측

정하는 방법도 설명하였다. 결론적으로 하나의 LED만 이용하는 것보다 두 개의 LED 요소 중 비밀률이 더 좋은 링크를 선택하는 방법을 선택했을 때 도청에 대응하는 성능이 더 우수했다. Cho et al.은 [34] 에서 단일 사용자 VLC 시스템에서 가장 근처에 있는 LED를 선택하는 기존의 연구에서 더 나아가, 다중 사용자 VLC 시스템에서 적절한 다수의 LED를 선택하는 최적화된 방법을 제안했다. 너무 많은 LED가 선택되면 정당한 사용자뿐만 아니라 도청자까지 신호를 수신할 수 있게 되고, 너무 적은 LED를 선택하면 정당한 사용자가 충분한 신호를 받지 못하는 문제점이 생기기 때문에 최적의 LED 세트를 선택하는 것이 중요하다.

Liang et al.은 다중 사용자가 존재하는 VLC 네트워크에서 이웃하는 AP끼리의 협력을 통해 비밀률을 향상시킬 수 있으며, 도청자가 없는 영역을 보호구역으로 구축하면 합법적인 사용자의 비밀률을 크게 향상시킬 수 있다는 것을 증명했다 [35]. 이 논문의 저자들은 비밀률을 향상시킬 수 있는 PLS 방식을 활용하여 높은 보안 요구사항을 가진 VLC 시스템을 구축할 수 있는 가능성을 입증했다.

Ⅲ. VLC 시스템 모델

스마트 LED-VLC 시스템 모델은 Fig. 1과 같다. VLC 시스템의 구성 요소는 스마트 LED 송신기, PD가 있다. 스마트 LED 송신기는 천장의 LED이고, PD는 수신면(receiver plane) 위에 위치한다. Fig. 1에서 x, y, z는 LED-VLC 시스템이 설치된 방의 위치를 나타내고, h는 LED와 수신면 사이의 수직 거리이다. 백본망으로부터 전달된 신호를 광섬유를 통해 전달하여 LED 송신기로 빛 신호를 변조하여 통신하게 된다. LED는 IM/DD(intensity modulation/direct detection) 광 전송방식을 사용하고, LED에서 사용자로의 MISO 환경을 가정한다. 실내 VLC 시스템에서는 LOS 요소가 NLOS (Non-LOS) 보다 강하기 때문에 VLC 채널은 LOS 전파 모델만 고

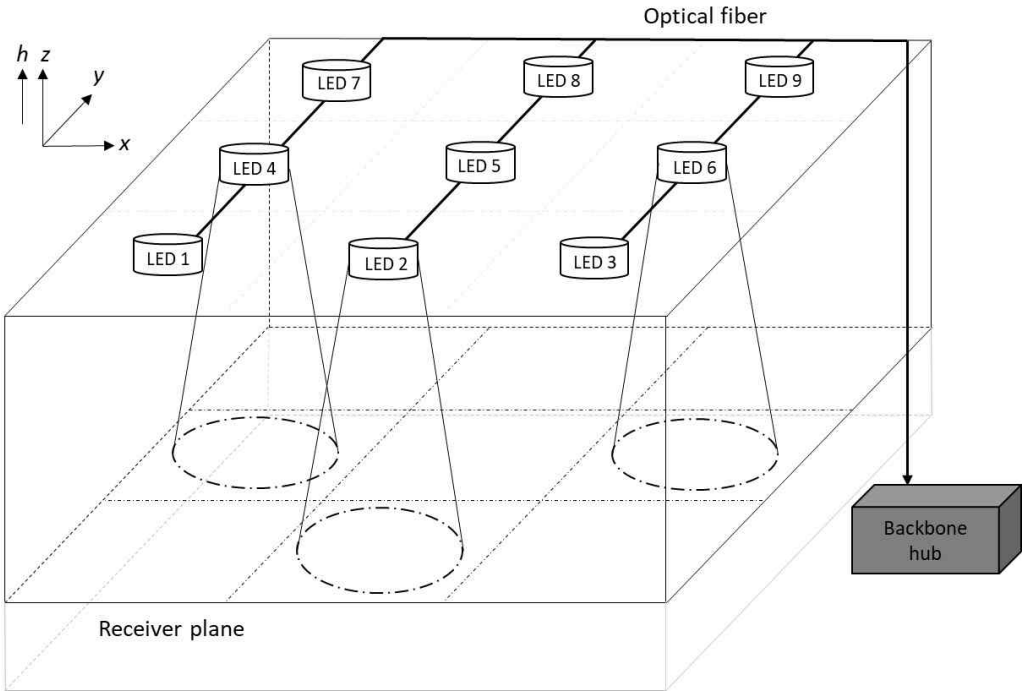

FIGURE 1. VLC system model

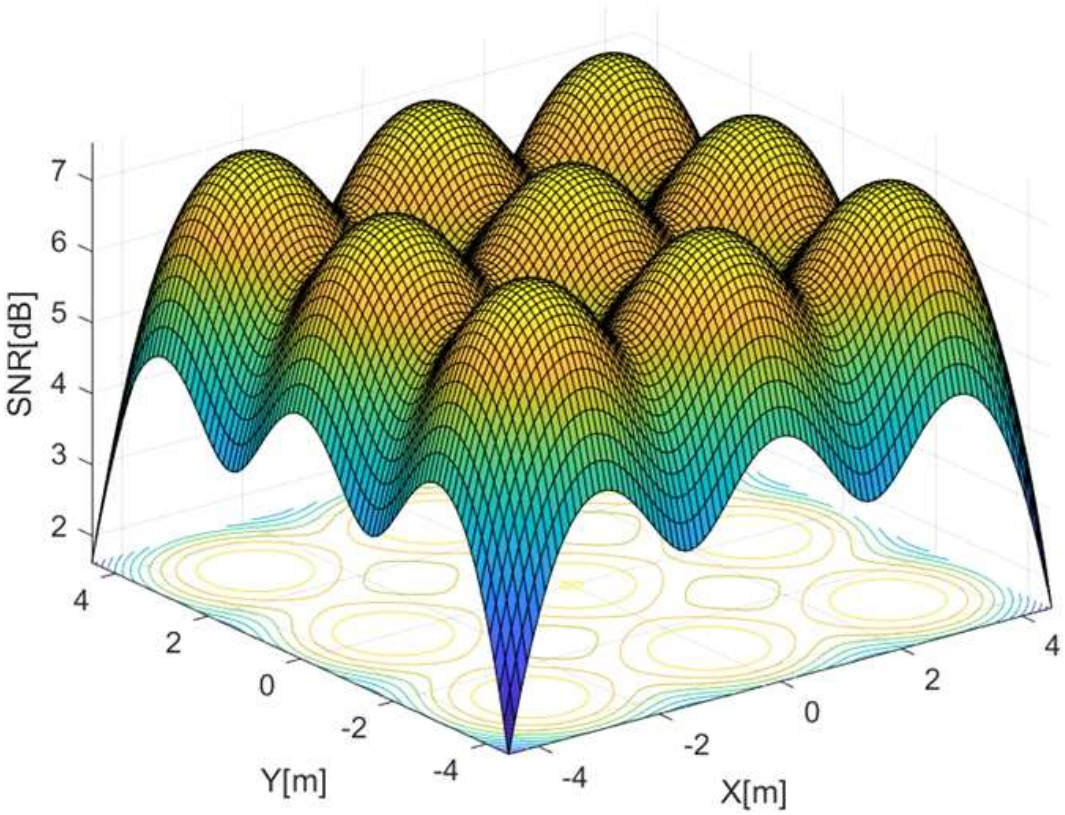

FIGURE 2. SNR[dB] of VLC system

려하였다 [35].

Fig. 2는 Fig. 1의 VLC 시스템 모델 환경에 따른 SNR 분포도이다. VLC는 직진성을 가지기 때문에 각 LED의 바로 밑에 있는 구역에서의 SNR이 가장 높고 LED와 멀어질수록 SNR이 낮아진다. SNR 분포도를 통해 LED 기반 VLC 시스템의 전파 특성을 확인할 수 있고, 본 논문에서는 이러한 VLC의 직진성을 이용하여 LED 기반 VLC 시스템에 대한 재밍 공격의 패턴을 유형화할 수 있었다. Table II는 VLC 구성요소인 방, 송신기, 수신기의 시스템 파라미터를 나타낸다. LED는 천장에 균일한 간격으로 9개가 설치되어 있고, 반치전폭의 반각은 45°로 설정했다. LED 하나의 송신 파워는

TABLE II
Parameters for VLC system components

Components	Parameters	Values
Room	Size (m^3)	$9 \times 9 \times 3$
Source	Location (LED 1~9)	(1.5, 1.5, 3), (4.5, 1.5, 3), (7.5, 1.5, 3), (1.5, 4.5, 3), (4.5, 4.5, 3), (7.5, 4.5, 3), (1.5, 7.5, 3), (4.5, 7.5, 3), (7.5, 7.5, 3)
	Semi angle at half power (deg)	45
	Transmitted power (per LED) (mW)	10
	Transmitted power (jammer) (mW)	50
	Number of LEDs per array	30×30 (900)
Receiver	Receiver plane above the floor (m)	0.85
	Active area (cm^2)	1
	Half-angle FOV (deg)	70

10mW이며, 재머 LED는 50mW로 송신한다. 하나의 LED는 30×30의 배열로 이루어져 있다. PD가 위치한 수신 평면은 지면에서 0.85m 떨어져있고, PD의 활성 영역은 $1cm^2$이며, FOV의 반각은 70°이다.

1. VLC 재밍 시스템

재밍 공격의 영향을 분석하기 위한 평가 지표로 BER을 사용하였다. IM/DD 변조 기법을 사용했을 때 BER과 SINR은 다음과 같이 구할 수 있다 [9], [36].

$$BER = Q(SINR), \tag{1}$$

$$SINR = \frac{(R \bullet P_{rx})^2}{N + (P_{rj})^2}, \tag{2}$$

where

$$N = \sigma_{shot}^2 + \sigma_{thermal}^2, \tag{3}$$

$$\sigma_{shot}^2 = 2qRP_{rx}B + 2qI_BI_2B, \tag{4}$$

이때 R은 PD의 반응성이고 1로 설정하였으며, P_{rx}는 수신 파워, N은 노이즈 분산, 그리고 P_{rj}는 재머로부터 수신된 파워이다. 즉, P_{rj}가 간섭으로 작용하여 P_{rj}가 증가할수록 전체적인 SINR이 감소하여 BER이 증가한다. 노이즈는 푸아송 잡음(σ_{shot}^2)과 열 잡음($\sigma_{thermal}^2$)으로 구성되는데, 푸아송 잡음만 고려하여 VLC 시스템을 모델링했다 [9]. q는 기본 전하(elementary charge), B[Hz]는 PD의 대역폭, I_B는 기저 방사선으로 인한 광전류, $I_2 = 0.562$는 잡음 대역폭 인자이다.

Fig. 3은 Fig. 1의 VLC 시스템의 조명 파라미터이다. LED가 램버시안 방출 패턴을 가진다고 할 때, 램버트 방출의 차수 m_l은 다음과 같이 정의된다.

$$m_l = \frac{\ln(2)}{\ln(\cos\phi_{1/2})} \tag{5}$$

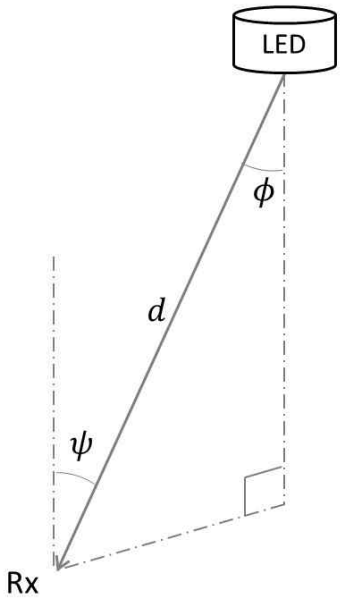

FIGURE 3. Illumination of VLC system

이때 $\phi_{1/2}$는 LED 반치전폭의 반각을 의미한다.

VLC 채널의 직류 이득인 H와 수신기에서 수신한 파워 P_{rx}는 다음과 같이 구할 수 있다.

$$H = \frac{(m_l + 1) \cdot A}{2\pi d^2} \cos^{m_l}(\varnothing) \cdot \cos(\psi), \tag{6}$$

$$P_{rx} = P_{tx} \cdot H \cdot T_s(\psi) \cdot g(\psi), 0 \le \psi \le \psi_{con}, \tag{7}$$

이때 P_{tx}는 송신 파워, A는 PD의 물리적 영역, ψ는 수신 평면에 수직인

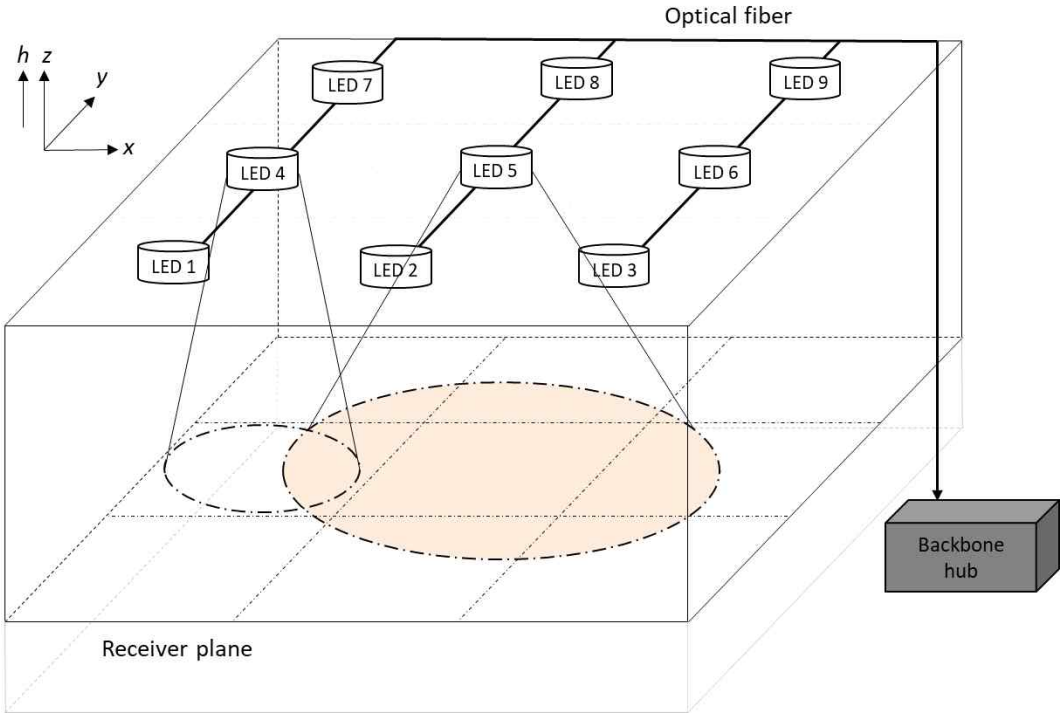

FIGURE 4. Example of jamming attack in VLC system (when LED5 is a jammer)

축에 대한 입사각, $T_s(\psi)$는 필터 이득(1로 설정함), $g(\psi)$는 집중기 이득, ψ_{con}는 FOV, d는 LED와 검출기 사이의 거리를 의미한다. 수신기에서 집중기 이득은 다음과 같이 정의된다.

$$g(\psi) = \begin{cases} \dfrac{n^2}{\sin^2 \psi_{con}}, & 0 \le \psi \le \psi_{con} \\ 0, & 0 \ge \psi_{con} \end{cases} \tag{8}$$

이때 n은 PD 렌즈의 굴절률을 의미하고, 1.5로 설정했다. 본 논문에서는 LED와 재머 LED의 파워에 따른 성능 열화를 BER을 이용해 분석하였다.

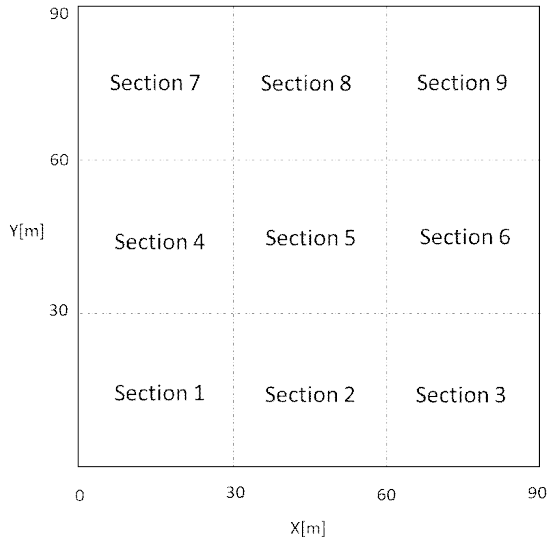

FIGURE 5. The receiver plane is divided into 9 equal sections.

스마트 LED는 광원의 세기, 빔 폭 등을 조절할 수 있기 때문에 LED 중 하나가 재머로 악용될 수 있다 [9]. 해당 논문에서는 LED 세트가 공격자에 의해 모두 작동된다는 가정으로 재밍 시스템을 구성하였고, 재머의 개수를 늘려가며 여러 재밍 환경을 비교하였다. 본 연구에서는 재머의 개수를 한 개로 고정하였고, Fig. 4는 9개의 LED 중 LED5가 재머인 경우를 나타낸다. 재머의 강한 신호는 주변 LED의 링크에 상당한 간섭으로 작용하여 링크 성능을 열화시킬 수 있다. 재머의 파워를 높이거나 빔 폭을 넓게 하여 주변 LED 링크에 간섭을 증가시킬 수 있다.

본 연구에서는 재머의 송신 파워를 증가시켜서 재밍 공격을 시도하였다. 재밍 공격의 영향을 분석하기 위하여 수신면을 Fig. 5와 같이 9등분하여 LED의 번호와 동일하게 Section1부터 Section9로 표현하였다.

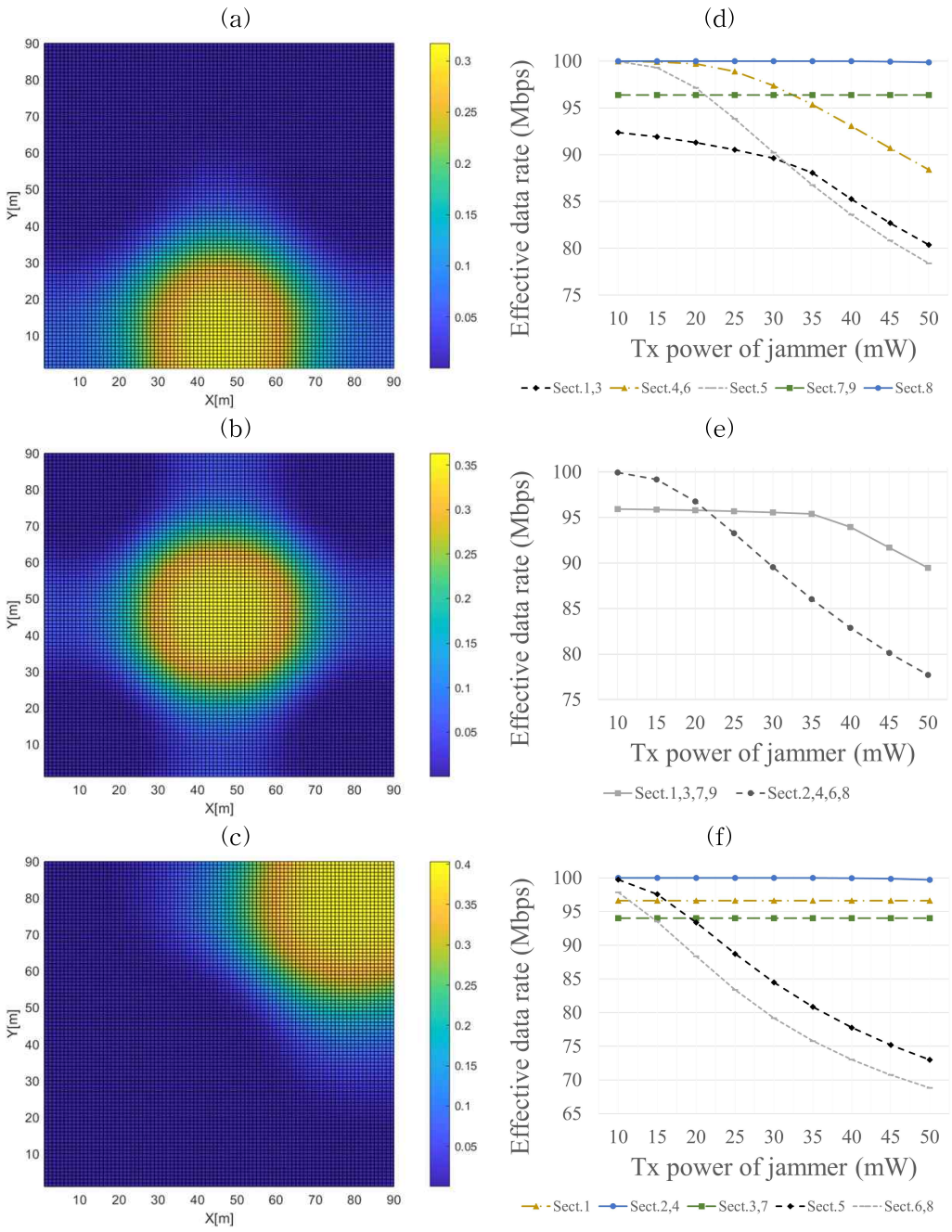

FIGURE 6. BER under jamming attack when the jammer is (a) LED2, (b) LED5, (c) LED9; Effective data rate vs. Tx power of jammer when the jammer is (d) LED2, (e) LED5, and (f) LED9.

Fig. 6(a)-(c)는 각각 LED2, LED5, LED9가 재머일 때 수신자의 위치에 따른 BER을 나타낸 것이다. 재머의 빔 폭($\phi_{1/2}$)은 동일하고 송신 파워만 10mW에서 50mW로 증가시켜 재밍 공격을 실시했다. LED2와 LED4, LED6, LED8은 BER의 양상이 동일하기 때문에 LED2만 분석하였고, 마찬가지로 LED1, LED3, LED7, LED9의 BER 양상이 동일하기 때문에 LED9로 대표하였다. 따라서, LED2, LED5, LED9의 BER이 전체 LED의 BER 양상을 대표할 수 있다. Fig. 6(a)-(c)에서 재머와 인접한 LED 링크의 BER이 증가하여 Effective data rate이 감소한 것을 알 수 있다.

재밍의 영향으로 인하여 재머와 인접한 링크의 성능이 재머의 위치에 따라 일정한 규칙을 가지며 변하는 것을 확인할 수 있었다. Fig. 6(d)-(f)는 재머가 각각 LED2, LED5, LED9일 때 재머의 송신 파워에 따른 각 섹션의 BER을 이용해 Effective data rate을 계산하여 나타낸 그래프이고, Fig. 7은 Fig. 6(d)-(f)의 결과를 정리한 표이다. Effective data rate은 오류 없이 전송 가능한 데이터의 양을 의미하고, VLC 시스템의 data rate은 100Mbps로 설정했다. Effective data rate은 다음 식으로 계산할 수 있다.

$$Effective\,Data\,Rate = Data\,Rate(1-BER) \tag{9}$$

LED2가 재머일 경우 Section5의 BER이 가장 높았고, Section1과 3, Section4와 6, Section7과 9의 BER이 각각 동일했다. LED5가 재머일 경우 Section1, 3, 7, 9의 BER이 동일했고, 마찬가지로 Section2, 4, 6, 8의 BER이 동일했다. 마지막으로, LED9가 재머일 경우, LED9와 가장 인접한 Section6과 8의 BER이 동일하게 가장 높았고, Section3과 7, Section2와 4의 BER이 각각 동일하였다.

BER은 최대 50%의 값을 가지며, Fig. 8은 LED 5가 재머인 경우, 재머

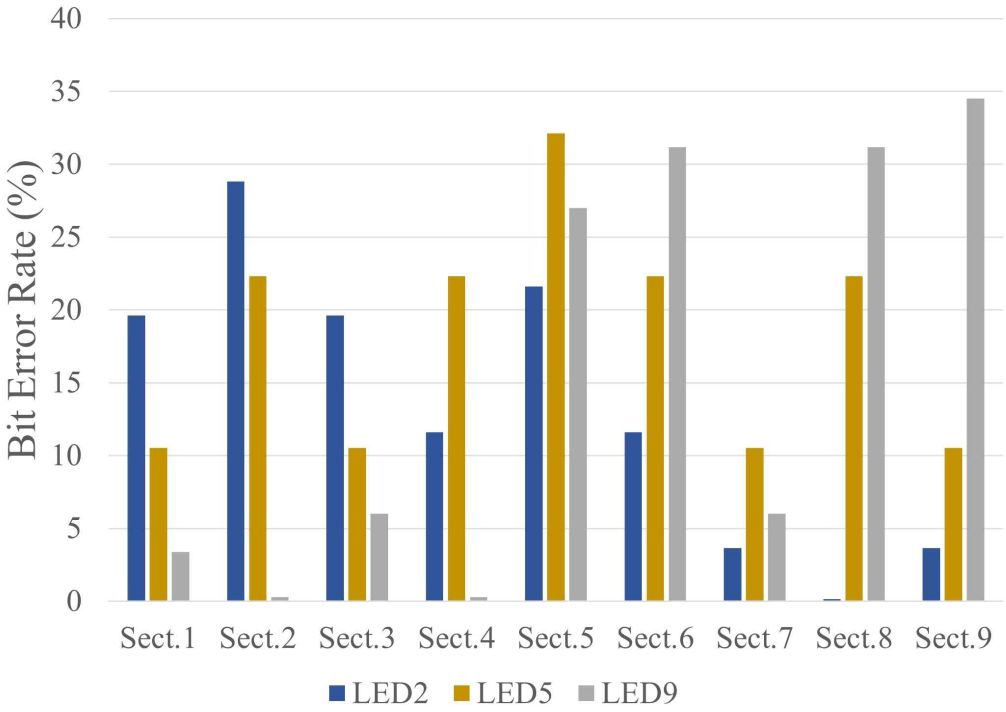

FIGURE 7. Effects of jamming attack for each section

의 Tx power가 2000mW에서 10000mW까지 증가할 때의 Effective data rate을 나타낸다. Effective data rate이 50Mbps에 수렴하면 BER이 50%이기 때문에 재밍 공격에 의해 링크가 셧다운되어 아예 사용할 수 없게 된다.

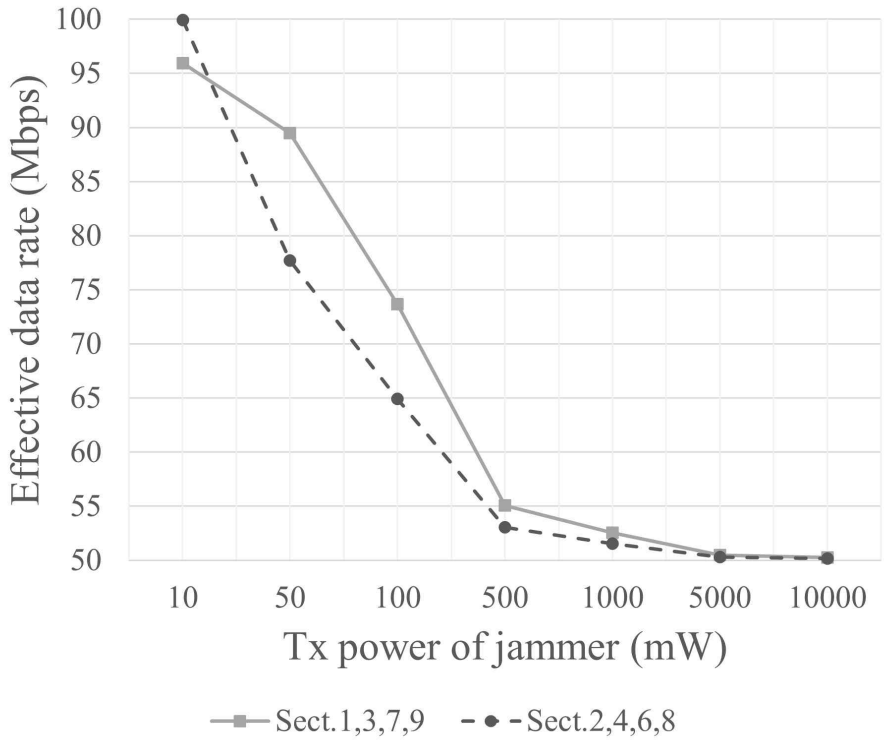

FIGURE 8. The LED link shuts down as Tx power of jammer increases.

Ⅳ. 공격 탐지 및 대응 시스템

1. 분류 알고리즘

재밍 공격을 탐지하는 것은 통신성능 열화의 원인이 공격인지 아닌지를 구분하는 분류 문제에 해당한다. 성능 열화, 즉 SINR 감소의 원인은 재밍 공격뿐만 아니라 송신 링크를 가로막는 장애물에 의해 발생할 수 있다. 본 연구에서는 주변 LED 또는 광원으로부터의 신호는 간섭으로 고려하지 않았고, LED와 수신자 사이의 직접적인 링크를 방해하는 물체를 장애물로 정의하였다. 재밍 공격에서 장애물에 의해 성능이 저하되었을 때의 SINR은 다음과 같이 구할 수 있다.

$$SINR = \begin{cases} \dfrac{(P_{rx})^2}{N + (P_{rj})^2} & (P_{rx}^{(s,t)} \neq 0) \\ 0 & (P_{rx}^{(s,t)} = 0) \end{cases} \tag{10}$$

이때, $P_{rx}^{(s,t)} (0 < s < S, 0 < t < T, S = 90, T = 90)$는 수신 평면에서 수신자의 좌표인 (s,t)에서의 수신 신호 파워를 의미하고, S와 T는 각각 수신 평면의 X, Y축에 위치할 수 있는 수신자의 최대값을 의미한다. $P_{rx}^{(s,t)} = 0$은 수신자와 수직 거리에 장애물이 위치하여 수신 신호 파워가 0이 된 경우이다.

재밍 공격 탐지 모델은 BER을 평가 지표로 이용하여 공격과 장애물을 구분하고 분류 성능, 즉 탐지율을 오차 행렬로 평가한다. Fig. 7의 BER 값에 따라 패턴을 분석하여 공격과 장애물을 분류할 수 있는 특징(feature)을 추출하여 Table III의 탐지 조건을 만들었다. Table III은 탐지 조건, 재머의 위치, 그리고 재머의 Tx power가 50mW일 때의 BER을 나타낸다. BER의 패턴은

TABLE III
Conditions for jamming detection

Conditions		Jammers	BER
BER1	BER1(1)	LED2	Section1 = Section3
	BER1(2)		Section4 = Section6
	BER1(3)		Section7 = Section9
BER2	BER2(1)	LED5	Section1 = Section3 = Section7 = Section9
	BER2(2)		Section2 = Section4 = Section6 = Section8
BER3	BER3(1)	LED9	Section2 = Section4
	BER3(2)		Section3 = Section7
	BER3(3)		Section6 = Section8
Rel-BER1		LED2	BER1(3) < BER1(2) < BER1(1)
Rel-BER2		LED5	BER2(1) < BER2(2)
Rel-BER3		LED9	BER3(1) < BER3(2) < BER3(3)

재머의 영향을 동일하게 받는 section 간 BER의 값이 동일하다는 것과, 재머와 가까울수록 BER이 커진다는 두 가지의 특징이 있다. 예를 들어, LED2가 재머인 경우 Section1과 3, Section4와 6, 그리고 Section7과 9의 BER이 동일하고(BER1), Section1과 3의 BER이 항상 Section4와 6의 BER보다 높고, 마찬가지로 Section4와 6의 BER이 Section7과 9의 BER보다 항상 크다는 특징이 있다(Rel-BER1). 탐지 알고리즘은 Table III을 이용하여 성능 열화를 탐지한 후 스마트 LED 간의 협력을 통해 성능 열화의 원인이 재밍 공격인지 장애물에 의한 것인지를 분류하는 것이다. 성능 열화가 발생하였지만, Table III의 탐지 조건대로 성능이 저하되지 않았다면 장애물에 의한 성능 열화로 판단하고, 성능 저하 패턴이 탐지 조건과 일치하였다면 재밍 공격이라고 판단한다. Table III의 탐지 조건은 LED2, LED5, LED9가 재머일 때의 탐지 조건을 보여주지만, LED2와 LED9의 케이스는 동일한 방식으로 LED4, LED6,

LED8, 그리고 LED1, LED3, LED7이 재머일 경우에도 탐지 조건을 정할 수 있다.

협력 탐지 모델의 성능을 평가하기 위하여 k-random 탐지 모델을 도입하여 함께 탐지 성능을 비교하였다. k-random 탐지 모델은 협력 탐지 조건을 적용하지 않고 전체 섹션 중 k개 이상의 섹션에서 성능이 저하될 경우 공격이라고 판단한다 [37], [38].

2. Ground truth 수집

공격 탐지를 위하여 공격과 장애물에 의한 성능 열화 데이터를 각각 수집하였다. Ground truth는 각 LED 링크의 성능 열화를 평가할 수 있는 데이터인 각 섹션의 BER이다. 각 섹션의 BER을 탐지 알고리즘에 입력하여 공격과 공격이 아닌 상황을 분류한다.

협력 탐지 모델의 성능을 평가하기 위하여 재밍 공격 상황에도 장애물을 함께 모델링하여 재밍과 장애물에 의한 성능 열화가 동시에 발생하도록 하였다. 장애물은 각 섹션에 하나씩 발생할 수 있기 때문에 전체적으로 최소 0개에서 최대 9개까지 발생할 수 있다. 장애물은 한 섹션의 1/4를 차지하도록 설정하였고, 장애물이 있는 곳은 수신 파워가 0이 된다. 재밍 공격으로 인한 성능 열화와 장애물로 인한 성능 열화가 중첩하여 발생하더라도 협력 탐지 모델을 이용한다면 인접 LED간 성능 열화 패턴 비교를 통해 공격을 탐지할 수 있다. 예를 들어, BER1의 경우 장애물로 인하여 Section1과 Section3의 BER이 달라지게 되더라도 나머지 탐지 조건인 Section4와 Section6, Section7과 Section9의 BER 값을 비교하여 탐지할 수 있다.

3. 공격 탐지 시스템

Fig. 9는 공격 탐지 시스템의 파이프라인이다. 공격 탐지 시스템은 공격 전과 후에 수집한 ground truth를 분류 알고리즘에 입력하여 탐지 조건 비교를 통해 공격을 탐지한다. 재밍 공격 전 각 섹션의 BER을 먼저 수집한 다음 성능 열화가 발생한 이후의 BER을 수집하고, 탐지 조건을 통해 협력 공격 탐지를 수행한다. k-random 모델의 경우에는 BER을 비교하여 전체 섹션 중 k개 이상의 섹션에서 성능이 저하될 경우 공격이라고 판단한다.

공격을 올바르게 탐지하고, 공격이 아닌 것을 공격이 아니라고 판단하는 공격 탐지율을 평가하기 위하여 오차 행렬을 이용해 정밀도, 재현률, 정확도, f1 score를 도출하였다. 오차 행렬은 분류 성능을 평가하기 위하여 실제 값과 예측값을 비교하는 표이다. True positive(TP)는 실제 공격을 탐지 모델이 공격으로 분류하는 경우, false negative(FN)는 실제 공격을 탐지 모델이 공격이 아니라고 분류하는 경우, false positive(FP)는 실제로 공격이 아닌데 탐지 모델이 공격으로 분류하는 경우, true negative(TN)는 실제로 공격이 아니고 탐지 모델이 공격이 아니라고 분류하는 경우이다. TP, FN, FP, TN을 이용하여 정밀도, 재현율, 정확도, f1 score을 도출할 수 있다. 정밀도는 탐지 모델이 공격이라고 분류한 것 중 실제로 공격인 것의 비율이고, 재

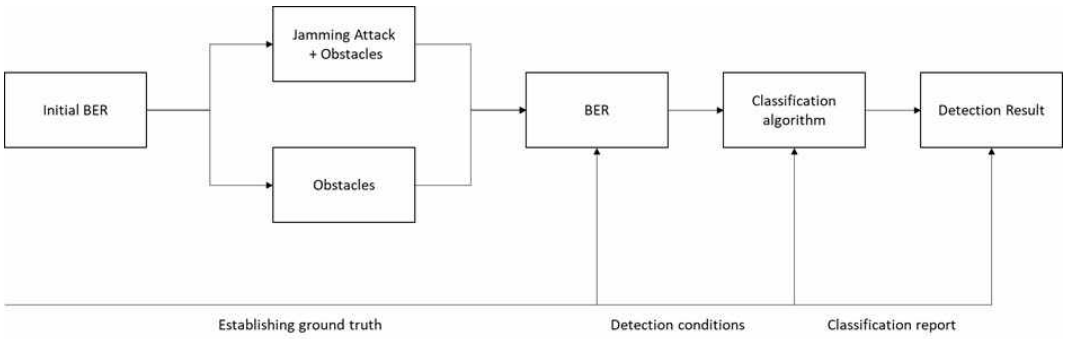

FIGURE 9. The attack detection system pipeline.

현율은 실제 공격 중 탐지 모델이 공격이라고 분류한 것의 비율, 정확도는 공격을 공격이라고 탐지한 경우와 공격이 아닌 것을 공격이 아니라고 탐지한 경우를 모두 포함한 비율, f1 score는 정밀도와 재현율의 조화평균이다.

k-random 탐지 모델의 경우 k개 이상의 섹션에서 성능 열화가 발생하면 모두 공격이라고 판단하기 때문에 공격이 아닌 성능 열화까지 공격이라고 분류할 확률이 높을 것을 예상할 수 있다.

4. 공격 대응 시스템

재밍 공격의 영향을 최소화하는 대표적인 방법은 협력적인 전송 방법을 이용하여 송신 효율성을 높이는 것이다. 협력적인 전송은 여러 개의 송신기에서 동일한 신호를 전송하므로 수신되는 신호 이득이 증가하여 재밍 간섭의 영향을 줄이고 SINR을 개선할 수 있다.

본 연구의 다중 LED 기반의 VLC 시스템은 여러 LED에서 보내는 신호가 중첩되어 하나의 사용자에게 보내지는 MISO 채널이기 때문에 이미 협력적인 전송 방법에 의한 효과를 얻고 있는 상황이다. 본 절에서는 재밍 공격에 의해 영향을 받는 링크의 effective data rate과 전력효율을 높이는 방법을 평가하기 위하여 Table V의 세 가지의 협력적 전송 방법을 비교하였다. Single LED는 재밍 공격의 영향을 받는 LED의 송신 파워를 증가시키는 방법이고, dual LEDs는 재밍 공격의 영향을 받는 LED와 가장 인접하고 재머와 가장 먼 LED의 송신 파워를 함께 증가시키는 방법이고, Octuple LEDs는 모든 LED의 송신 파워를 증가시키는 방법이다. single LED의 VLC 시스템 모델 환경은 LED와 재머 LED가 각각 하나만 존재하고, dual LEDs는 공격받는 LED 하나와 재머 LED, 인접 LED 하나가 존재하고,

TABLE V
Cooperative transmission techniques

Cooperative Transmission	Explanation
Single LED	Increase Tx power of LED affected by jamming attack
Dual LEDs	Increase Tx power of both LED affected by jamming attack and LED closest to the affected LED and farthest from jammer
Octuple LEDs	Increase Tx power of all LEDs

Octuple LEDs는 8개의 LED와 1개의 재머 LED가 존재하는 상황이다.

협력적 전송의 효과를 평가하기 위해서 EE와 BER을 지표로 사용하였다. 협력적 전송은 송신 이득을 개선하여 재밍 공격의 영향을 줄일 수는 있지만 EE 열화가 발생한다. EE (Mbps/J)는 effective data rate를 파워 소모량으로 나눠서 다음의 수식과 같이 구할 수 있다.

$$EE = \frac{Effective\,data\,rate}{total\,power\,consumption} \tag{11}$$

LED의 송신 파워 증가량에 따라서 EE와 BER을 측정하여 협력 송신 기법의 효율성을 평가하였다. 협력 송신 기법으로 인하여 증가한 송신 파워는 다음과 같이 계산한다.

$$Total\ Tx\,power = \sum_{i=1}^{L} \frac{(Tx\,power\,of\,\mathrm{sin}gle\ link)}{L} \tag{12}$$

이때, L은 협력하는 LED의 개수이다. single LED 방법에서 L=1이고, dual LEDs 방법에서는 L=2, 그리고 Octuple LEDs에서는 L=8이다. LED 하나의 Tx 파워는 Octuple LEDs 방법으로 파워를 증가시켰을 때를 기준으로 각 방법마다 하나의 LED가 다른 파워로 송신하도록 설정했다. 즉, single LED의 경우에는 하나의 LED가 80mW, dual LEDs의 경우에는 하나의 LED가 40mW, 그리고 Octuple LEDs는 하나의 LED가 10mW씩 Tx power가 증가하게 된다.

Ⅴ. 성능 평가

1. 실험 환경

재밍 탐지 시스템과 공격 탐지 시뮬레이션은 MATLAB으로 구현하였다. Ground truth는 재머가 있는 경우 3개의 재머에 대해 각 100개의 ground truth와, 재머가 없는 경우 300개의 ground truth, 총 600개의 ground truth를 매번 랜덤하게 생성하였고, 시뮬레이션은 100회 반복하였다. k-random의 경우 k=2개 이상의 섹션의 성능이 저하될 경우 공격이라고 판단하도록 설정했다. k값의 변화에 따른 k-random 모델의 탐지 성능도 비교하였다. 장애물은 전체 LED 섹션 중 1군데 이상 5군데 이하로 랜덤한 위치에 발생하도록 설정하였다. Fig. 10은 장애물이 3개 있을 때 수신 파워의 예시이다. 장

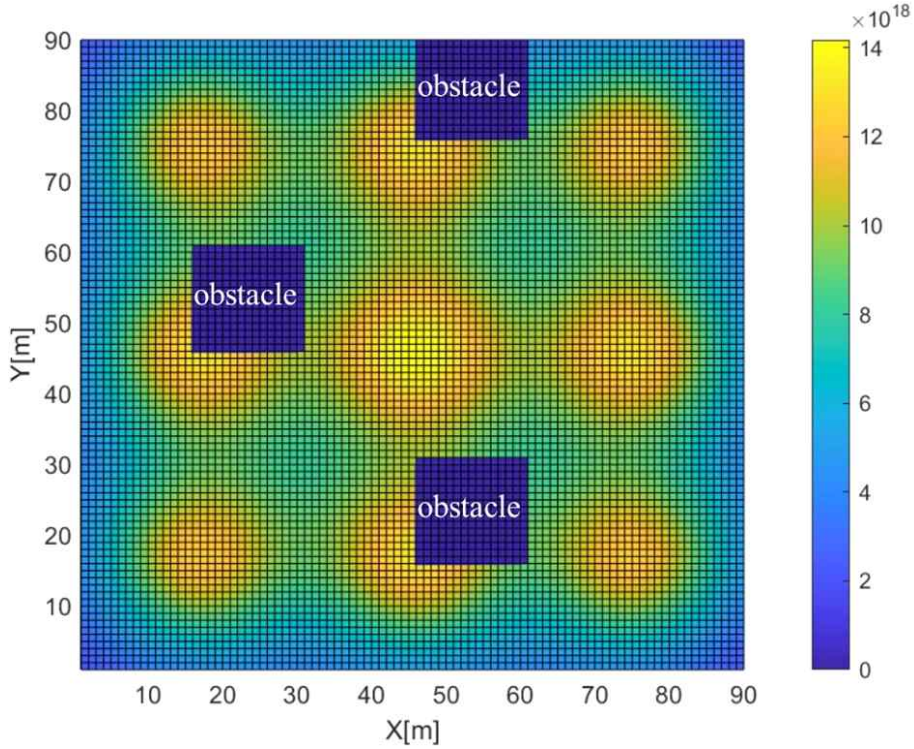

FIGURE 10. Example of received power with obstacles

TABLE IV
Final detection condition for classification algorithm

Conditions	Operations
Final condition	BERC AND Rel-BER
BERC	BER1 OR BER2 OR BER3
Rel-BER	Rel-BER1 OR Rel-BER2 OR Rel-BER3
BER1	BER1(1) OR BER1(2) OR BER1(3)
BER2	BER2(1) OR BER2(2)
BER3	BER3(1) OR BER3(2) OR BER3(3)

애물이 있는 부분의 수신 파워($P_{rx}^{(s,t)}$)는 0으로 설정했다.

또한, 장애물의 개수와 k 값의 변화에 따른 탐지율도 측정했다. 장애물이 1개에서 9개까지 증가할 때의 k-random 모델과 협력 모델의 탐지율 변화를 비교했다. 이를 통해 장애물이 있는 상황에서 더 효과적인 탐지 모델을 평가할 수 있다. k-random 모델은 탐지율이 k 값에 따라 영향을 많이 받을 것이기 때문에, k의 값을 2부터 9까지 증가시키면서 탐지율을 평가했다. 이때 장애물의 개수는 5개로 고정하고 k 값만 변화시키면서 측정하였다.

분류 알고리즘은 최종 탐지 조건으로 BERC와 Rel-BER을 모두 만족할 경우 공격이라고 판단하도록 했다. BERC는 특정 섹션끼리 재밍 공격으로 인해 BER이 같아지는 특징, Rel-BER은 BER의 상대적인 크기가 재머와 가까울수록 커지는 특징을 이용한 탐지 조건이다. 분류 알고리즘을 위한 최종 탐지 조건은 Table IV와 같이 설정하였다. BERC와 Rel-BER은 각각의 세부 조건들을 모두 OR 연산한 결과이다. 연산은 여러 경우의 수가 있을 수 있지만 본 연구에서는 Table IV를 기준으로 실험을 하였다.

2. 실험 결과 및 분석

Fig. 11은 k-random 모델과 협력 모델의 재밍 공격 탐지 결과를 비교한 그래프이다. 주목할 만한 점은, k-random 모델의 재현율이 더 높게 나왔다는 것이다. k-random 모델은 k(k=2)개 이상의 LED 섹션에서 성능 열화가 생기면 모두 공격이라고 판단하기 때문에 모든 공격을 탐지할 수 있었다. 하지만, 정확도가 낮은 이유는 공격이 아닌 성능 열화까지 공격이라고 판단하였기 때문이다. 따라서 정밀도와 정확도가 50%로 나타났고, 공격이라고 판단한 것 중에서 절반은 공격이 아니라는 것을 의미한다.

반대로 협력 탐지 모델의 경우 정밀도가 100%로 나왔고, 이는 탐지모델이 공격이라고 판단한 모든 성능 열화가 공격이 맞았다는 것을 의미한다. 협력 모델의 재현율은 82%, 정확도는 91%로 나타났고, 정밀도를 제외한 모든 평

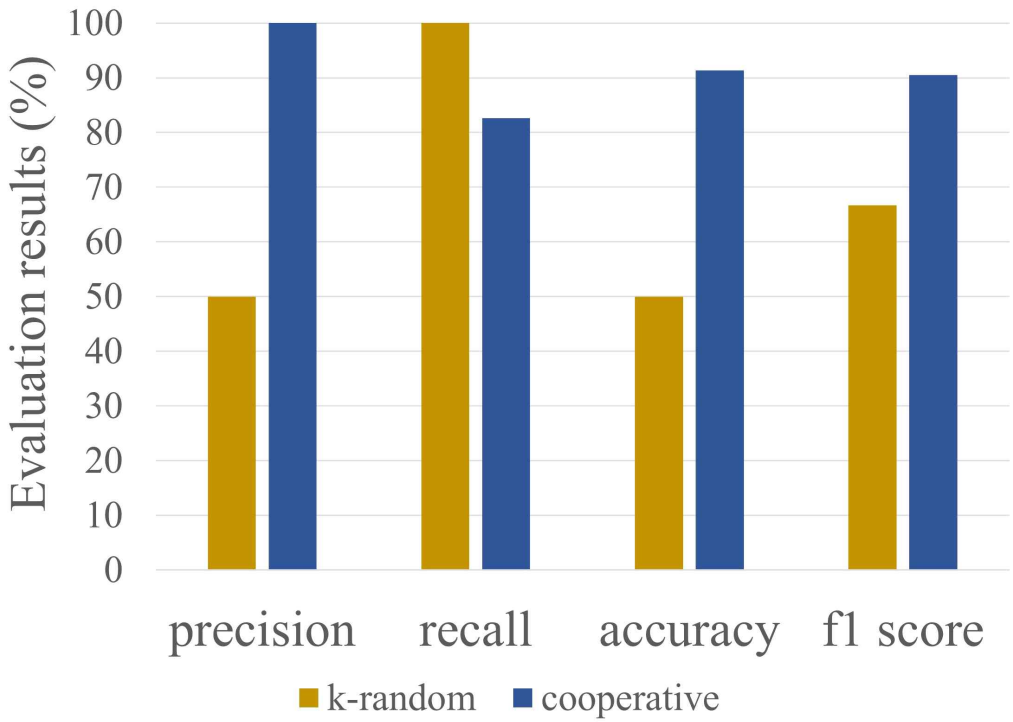

FIGURE 11. Results of attack detection simulation

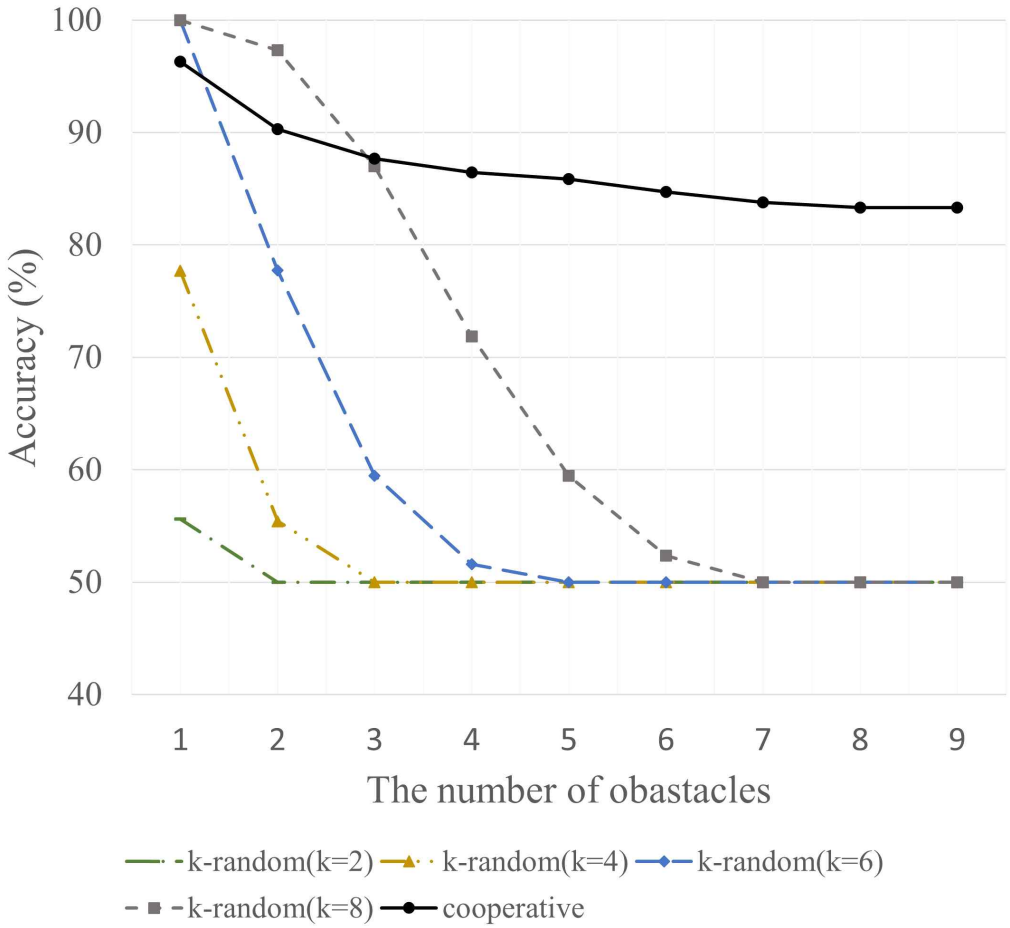

FIGURE 12. Accuracy vs. The number of obstacles

가 지표에서 협력 모델이 k-random 모델보다 성능이 우수하다는 것을 확인할 수 있었다. 협력 모델은 모든 공격 중 82%의 공격을 탐지할 수 있었고, 성능 열화의 원인이 공격이 아닌 것을 구분하는 성능이 100%에 달하기 때문에 매우 우수한 것을 알 수 있다.

Fig. 12는 장애물이 있는 LED 섹션 개수에 따른 각 모델의 탐지율의 정확도를 비교한 결과다. 전체적으로 장애물이 증가할수록 탐지율은 낮아지다가 일정 지점부터는 거의 변하지 않고 최소 탐지율을 유지하는 것을 확인할

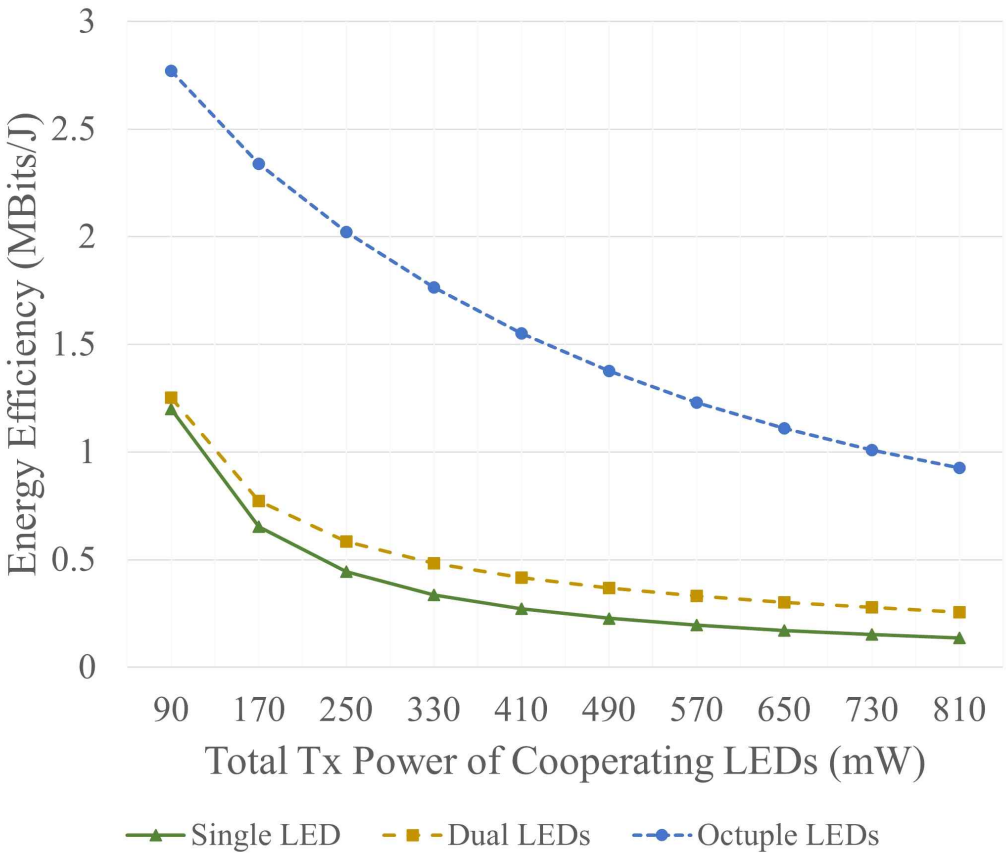

FIGURE 13. EE (Mbits/J) vs. Total Tx power of cooperating LEDs (mW)

수 있다. k-random 모델(k=2)의 경우 장애물의 개수가 k보다 작은 1개인 경우에는 탐지율이 67% 정도로 전체 k-random 모델(k=2)의 탐지율 중 가장 높았고, 장애물의 개수와 k 값이 동일한 시점부터는 50%의 탐지율을 계속 유지한다. 따라서 k-random 모델(k=2)의 최소 탐지율은 50%라는 것을 도출할 수 있다. k-random 모델의 분류 알고리즘에서 사용하는 k의 값을 k=4, k=6, k=8로 각각 증가시켰을 때의 탐지율도 비교하였다. 장애물의 개수가 k-1과 동일한 시점부터 50%의 탐지율을 유지한다. 즉, k의 개수와 무관하게 k-random 모델의 최소 탐지율은 50%이다.

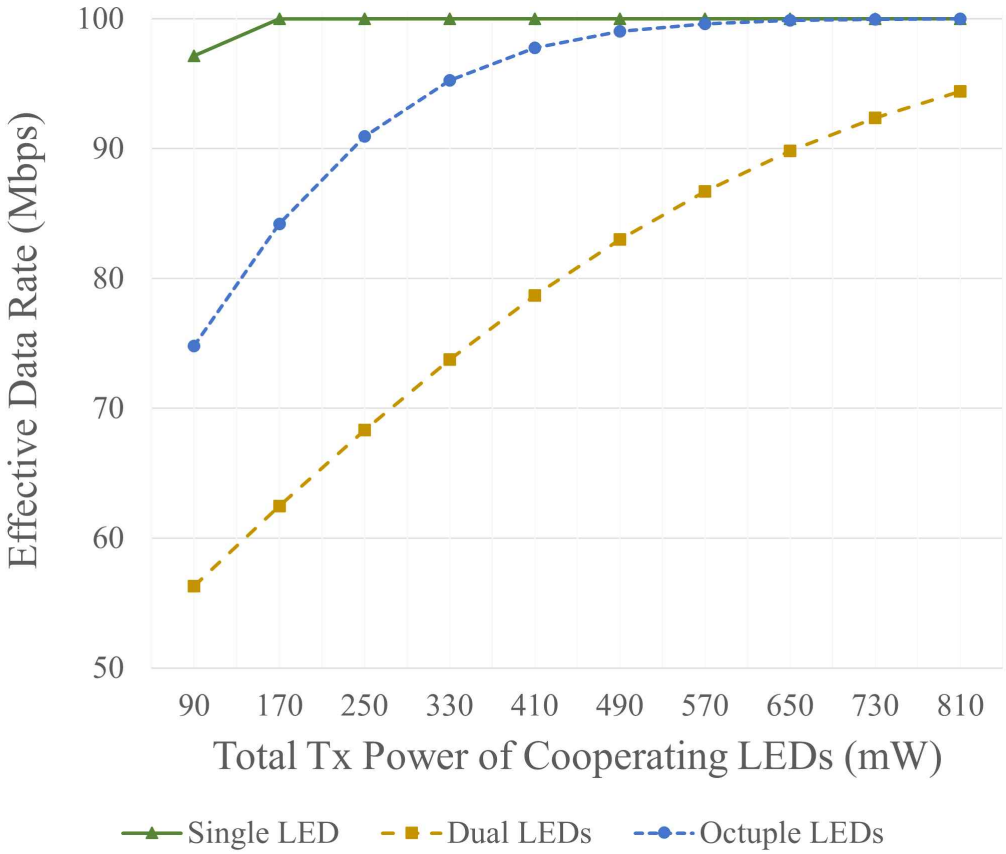

FIGURE 14. BER (%) vs. Total Tx power of cooperating LEDs (mW)

협력 모델의 경우에는 장애물의 개수에 따라 탐지율이 점차 낮아지다가 장애물이 5개 이상일 때부터 84%의 탐지율을 비슷하게 유지하는 것을 알 수 있다. 협력 모델의 최소 탐지율은 84%라는 것을 도출할 수 있고, 협력 모델이 k-random 모델보다 최소 탐지율이 약 1.68배 높다는 것을 알 수 있다. 간섭이 많은 상황에서도 k-random 모델보다는 협력모델의 최소 탐지율이 높기 때문에 협력 모델을 사용하는 것이 더욱 효과적이라는 것을 알 수 있다.

Fig. 13은 협력하는 LED의 총 송신 파워 증가에 따른 EE이다. EE만 고

려했을 때 모든 LED가 협력한 경우에 EE가 가장 높았고, 공격받는 하나의 LED만 파워를 높인 경우가 EE가 가장 낮았다.

Fig. 14는 협력하는 LED의 총 송신 파워 증가에 따른 effective data rate을 측정한 그래프이다. Effective data rate이 가장 많이 증가한 방법은 공격받는 하나의 LED만 파워를 높인 single LED의 경우이다. 인접한 LED 하나와 공격받는 LED만 협력한 dual LEDs의 경우에는 EE도 가장 낮고 effective data rate도 가장 적게 증가했다. 협력 LED의 총 송신 파워가 90mW일 때, Octuple LEDs의 effective data rate은 single LED의 77% 수준이지만, 총 송신 파워가 증가할수록 Octuple LEDs의 effective data rate도 점차 크게 증가하여 570mW부터는 Octuple LEDs의 경우 99.9% 이상, single LED의 경우 100%의 effective data rate을 확보할 수 있다.

총 Tx power가 570mW일 때 single LED의 EE는 0.19, Octuple LEDs의 EE는 1.23으로 Octuple LEDs의 EE가 6배 이상 높기 때문에, 최종적으로 EE와 BER의 절충 관계에 대해서 Octuple LEDs 방법을 사용하는 것이 가장 효율적이다. 다시 말해, 모든 LED가 협력하여 송신 파워를 증가시키는 방법으로 재밍 공격에 대응하는 것이 에너지 효율성과 effective data rate 확보 측면에서 가장 효율적이다.

Ⅵ. 결 론

LED 기반 VLC 시스템은 LED의 브로드캐스팅 및 중첩 특성으로 인하여 재밍 공격에 취약하다. 하지만, 기존 VLC 물리계층보안 연구에서는 공격을 효과적으로 탐지하기 위한 연구는 거의 이루어지지 않았다. 본 연구에서는 LED 간 협력을 통해 VLC 시스템에 대한 재밍 공격을 탐지, 대응하는 방법을 제안하였다. 협력 탐지 모델의 성능을 평가하기 위하여 k-random 모델을 도입하여 함께 성능을 비교하였고, 동일한 조건에서 협력 탐지 모델의 공격 탐지 정확도는 91%로, k-random 모델의 정확도인 50%보다 1.82배 향상된 것을 확인하였다. 장애물이 많은 환경에서도 협력 모델은 84%의 최소 탐지율을 보이며 k-random 모델보다 1.68배 높은 탐지 성능을 보였다. 또한, LED간 협력 송신 기법을 이용하여 에너지 효율성을 고려하며 재밍 공격에 효율적으로 대응할 수 있었다. 하지만, 본 연구의 탐지 시뮬레이션은 LED의 위치, 간섭, 노이즈 조건이 제한된 환경에서 진행되었고, 탐지 조건의 연산 방법에 따라 실험 결과가 달라진다는 한계점이 있다. 향후 연구로는 공격으로 인한 성능 열화 패턴 학습을 통해 인공지능 기반 협력 모델을 구축하여 탐지 성능을 더욱 향상하고자 한다.

ACKNOWLEDGEMENTS

본 논문은 한국정보통신학회 학술대회에서 발표한 ‘가시광 통신 채널의 취약성 및 공격 방법 [39]’ 논문의 후속 연구로 수행되었습니다. 논문을 지도해주신 이일구 교수님과 공저자로서 함께 연구에 참여한 주소영 학생에게 감사드립니다.

참고문헌

[1] L. E. M. Matheus, A. B. Vieira, L. F. Vieira, M. A. Vieira, and O. Gnawali, “Visible light communication: concepts, applications and challenges,” *IEEE Communications Surveys & Tutorials*, vol. 21, no. 4, pp. 3204-3237, Apr. 2019.

[2] S. U. Rehman, S. Ullah, P. H. J. Chong, S. Yongchareon, and D. Komosny, “Visible light communication: a system perspective—overview and challenges,” *Sensors*, vol. 19, no. 5, p. 1153, Feb. 2019.

[3] A. Jovicic, J. Li, and T. Richardson, “Visible light communication: opportunities, challenges and the path to market,” *IEEE Communications Magazine*, vol. 51, no. 12, pp. 26-32, Dec. 2013.

[4] F. Zafar, M. Bakaul, and R. Parthiban, “Laser-diode-based visible light communication: Toward gigabit class communication,” *IEEE Communications Magazine*, vol. 55, no. 2, pp. 144-151, Feb. 2017.

[5] S. Ariyanti and M.Suryanegara, “Visible light communication (VLC) for 6G technology: The potency and research challenges,” presented at *2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4)*, London, UK, Jul. 27-28, 2020.

[6] G. Blinowski, “Security issues in visible light communication systems,” *IFAC-PapersOnLine*, vol. 48, no. 4, pp. 234-239, Sep. 2015.

[7] G. Blinowski, “Security of visible light communications systems - a survey,” *Physical Communication*, vol. 34, pp. 246-260, Jun. 2019.

[8] C. Medina, M. Zambrano, and K. Navarro, “Led based visible light co

mmunication: Technology, applications and challenges-a survey," *International Journal of Advances in Engineering & Technology*, vol. 8, no. 4, p. 482, Aug. 2015.

[9] G. Blinowski, "The feasibility of launching physical layer attacks in visible light communication networks," Aug. 2016.

[10] H. B. Eldeeb, H. A. Selmy, H. M. Elsayed, and R. I. Badr, "Co-channel interference cancellation using constraint field of view adr in VLC channel," presented at *2017 IEEE Photonics Conference (IPC) Part II*, Orlando, FL, USA, Oct.1-5, 2017.

[11] M. E. Hosney, H. A. Selmy, and K. M. Elsayed, "Co-channel interference reduction by optimizing field of view angle of angular diversity receiver in VLC systems," presented at *2020 22nd International Conference on Transparent Optical Networks (ICTON)*, Bari, Italy, Jul, 19-23, 2020.

[12] M. Hosney, H. A. Selmy, A. Srivastava, and K. M. Elsayed, "Interference mitigation using angular diversity receiver with efficient channel estimation in MIMO VLC," *IEEE Access*, vol. 8, pp. 54060-54073, Mar. 2020.

[13] H. B. Eldeeb, H. A. Selmy, H. M. Elsayed, and R. I. Badr, "Interference mitigation and capacity enhancement using constraint field of view ADR in downlink VLC channel," *IET Communications*, vol. 12, no. 16, pp. 1968-1978, May. 2018.

[14] A. Ibrahim, T. Ismail, K. F. Elsayed, M. S. Darweesh, and J. Prat, "Resource allocation and interference management techniques for OFDM-based VLC atto-cells," *IEEE Access*, vol. 8, pp. 127431-127439, Jul. 20

20.

[15] K. Kim, K. Lee, and K. Lee, “An inter-lighting interference cancellati on scheme for MISO-VLC systems,” *International Journal of Electronic s*, vol. 104, no. 8, pp.1377-1387, Mar. 2017.

[16] C. Chen, P. Du, H. Yang, W. D. Zhong, X. Deng, and Y. Yang, “De monstration of Inter-cell Interference mitigation in multi-cell VLC syste ms using optimized angle diversity receiver,” presented at *2019 IEEE 4 th Optoelectronics Global Conference (OGC)*, Shenzhen, China, Sep. 3-6, 2019.

[17] P. P. Játiva, C. A. Azurdia-Meza, M. R. Canizares, S. Céspedes, and S. Montejo-Sánchez, “Performance enhancement of VLC-based systems using diversity combining schemes in the receiver,” presented at *2019 I EEE Latin-American Conference on Communications (LATINCOM)*, S alvador, Brazil, Nov. 11-13, 2019.

[18] T. V. Pham, and A. T. Pham, “Coordination/cooperation strategies an d optimal zero-forcing precoding design for multi-user multi-cell VLC networks,” *IEEE Transactions on Communications*, vol. 67, no. 6, pp. 4 240-4251, Jun. 2019.

[19] T. V. Pham, H. Le Minh, and A. T. Pham, “Multi-cell VLC: Multi-u ser downlink capacity with coordinated precoding,” presented at *2017 IE EE International Conference on Communications Workshops (ICC Wor kshops)*, Paris, France, May. 21-25, 2017.

[20] A. Ijaz, M. M. U. Rahman, and O. A. Dobre, “On safeguarding visibl e light communication systems against attacks by active adversaries,” *I EEE Photonics Technology Letters*, vol. 32, no. 1, pp. 11-14, Nov. 201

9.

[21] M. Obeed, A. M. Salhab, M. S. Alouini, and S. A. Zummo, “Survey on physical layer security in optical wireless communication systems,” p resented at *2018 Seventh International Conference on Communications a nd Networking (ComNet)*, Hammamet, Tunisia, Nov. 1-3, 2018.

[22] R. Negi and S. Goel, “Secret communication using artificial noise,” pr esented at *IEEE vehicular technology conference*, Dallas, Tx, Sep. 2005.

[23] D. Tian, W. Zhang, J. Sun, and C. X. Wang, “Physical-layer security of visible light communications with jamming,” presented at *2019 IEEE /CIC International Conference on Communications in China (ICCC)*, Ch angchun, China, Aug. 11-13, 2019.

[24] A. Mostafa and L. Lampe, “Enhancing the security of VLC links: Ph ysical-layer approaches,” presented at *2015 IEEE Summer Topicals Me eting Series (SUM)*, Nassau, Bahamas, Jul. 13-15, 2015.

[25] S. Cho, G. Chen, and J. P. Coon, “Enhancement of physical layer sec urity with simultaneous beamforming and jamming for visible light com munication systems,” *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 10, pp. 2633-2648, Oct. 2019.

[26] M. A. Arfaoui, H. Zaid, Z. Rezki, A. Ghrayeb, A. Chaaban, and M. S. Alouini, “Artificial noise-based beamforming for the MISO VLC wire tap channel,” *IEEE Transactions on Communications*, vol.64, no. 4, pp. 2866-2879, Dec. 2018.

[27] J. Al-Khori, G. Nauryzbayev, M. M. Abdallah, and M. Hamdi, “Joint beamforming design and power minimization for friendly jamming relayi ng hybrid RF/VLC systems,” *IEEE Photonics Journal*, vol. 11, no. 2, p

p. 1-18, Mar. 2019.

[28] T. V. Pham and A. T. Pham, “Energy efficient artificial noise-aided precoding design for visible light communication systems,” presented at *2020 International Conference on Computing, Networking and Communications (ICNC)*, Big Island, HI, USA, Feb. 17-20, 2020.

[29] L. Xiao, G. Sheng, S. Liu, H. Dai, M. Peng, and J. Song, “Deep reinforcement learning-enabled secure visible light communication against eavesdropping,” *IEEE Transactions on Communications*, vol. 67, no. 10, pp. 6994-7005, Jul. 2019.

[30] S. Liang, Z. Fang, G. Sun, and J. Zhang, “A physical layer security approach based on optical beamforming for indoor visible light communication,” *IEEE Communications Letters*, vol. 24, no. 10, pp. 2109-2113, Jul. 2020.

[31] S. Riurean, “A study on the VLC security at the physical layer for two indoor scenarios,” presented at *MATEC Web of Conferences*. [Online]. Available: https://www.proquest.com/conference-papers-proceedings/study-on-vlc-security-at-physical-layer-two/docview/2557050093/se-2

[32] P. Garg, “Dual-element indoor VLC network with two-stage secure link adaptation scheme,” presented at *2019 5th International Conference on Signal Processing, Computing and Control (ISPCC)*, Solan, India, Oct. 10-12, 2019.

[33] P. Garg, P. K. Sharma, and A. Gupta, “Secure information broadcasting analysis in an indoor VLC system with imperfect CSI,” *IET Communications*, vol. 15, pp. 526-536, Nov. 2020.

[34] S. Cho, G. Chen, and J. P. Coon, “Physical layer security in multiuse

r VLC systems with a randomly located eavesdropper," presented at *2019 IEEE Global Communications Conference (GLOBECOM)*, Waikoloa, HI, USA, Dec. 9-13, 2019.

[35] L. Yin and H. Haas, "Physical-layer security in multiuser visible light communication networks," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 1, pp. 162-174, Nov. 2017.

[36] Z. Ghassemlooy, W. Popoola, and S. Rajbhandari, Optical wireless communications: system and channel modeling with Matlab®, CRC press, 2019.

[37] N. Rahman, "Fast and energy-efficient technique for jammed region mapping in wireless sensor networks," Jan. 2014.

[38] U. Pesovic, S. Djurasevic, V. Lukovic, and P. Planinsic, "Interference classification for IEEE 802.15.4 networks," presented at *2020 International Conference on Broadband Communications for Next Generation Networks and Multimedia Applications (CoBCom)*, Graz, Austria, Jul. 7-9, 2020.

[39] S. H. Park, S. Joo, and I. G. Lee, "Vulnerabilities and attack methods in visible light communications channel,"presented at *Proceedings of the Korean Institute of Information and Commucation Sciences Conference*, Gunsan, Korea, Oct. 28-30, 2021.

ABSTRACT

Secure Visible Light Communication System via Cooperative Attack Detecting Techniques

Sohyun Park
Department of Future Convergence Technology Engineering
Graduate School of
Sungshin University

With the recent development of fourth industrial technology, the need for a broadband short-range wireless communication system to realize an ultraconnected, ultra-low latency, and ultra-realistic intelligent information society has emerged. Among the next-generation communication network technologies that can fulfill the technical demands, visible light communication (VLC) is a promising technology that can use illuminated light as a communication light source, which is convenient and environmentally friendly and has high energy and frequency efficiency. However, although VLC has a high level of security owing to the straightness and transparency of visible light, if some of the VLC nodes in a dense mesh network environment are hacked by external attacks, there can be critical performance degradation by jamming attacks. Although several studies have suggested the possibility of VLC jamming attacks, only a few have studied how to effectively detect and respond to these attacks. This study proposes a method to collaboratively detect and respond to jamming attacks in smart LED-based VLC systems. According to the experimental results of this study, the proposed cooperative method

showed 91% attack detection accuracy and 1.82 times better than the k-random method. The proposed method showed a minimum detection rate of 84% even in an obstacle-rich environment, proving outstanding attack detection performance 1.68 times better than the k-random method.