가시광 통신 채널의 취약성 및 공격 방법

박소현 · 주소영 · 이일구*

성신여자대학교

Vulnerabilities and Attack Methods in Visible Light Communications Channel

So-Hyun Park · Soyoung Joo · Il-Gu Lee*

Sungshin Women's University

E-mail : 220206035@sungshin.ac.kr / 220216032@sungshin.ac.kr / iglee@sungshin.ac.kr

요 약

무선 통신 기술이 방대한 양의 데이터를 빠른 속도로 높은 정확도와 안전성을 보장하여 전송하는 방식에 초점을 맞추어 발전하면서 기존의 무선 주파수(RF, Radio Frequency)를 이용한 무선 통신 기술의 대안으로 가시광 통신(VLC, Visible Light Communication) 기술의 연구개발이 가속화되었다. RF 무선 통신의 전파 스펙트럼이 더욱 혼잡해지고, 대역폭에 대한 수요가 지속적으로 증가함에 따라 규제되지 않은 대역폭을 사용할 수 있는 VLC가 해결책으로 제시되고 있다. 하지만, VLC 채널은 LOS(Line of Sight) 전파 특성으로 중간자 공격(MITM, Man-In-The-Middle)에 취약하고 도청과 재밍 공격에 쉽게 노출될 수 있다는 문제점이 있다. 이러한 VLC 채널에 대한 공격은 통신 링크 및 데이터의 기밀성, 무결성 및 가용성을 훼손하고, 데이터 재전송률이 높아져 스루풋이 감소하고 전력 소모량이 증가하여 데이터 전송 효율성이 낮아지는 문제점이 있다. 본 연구에서는 취약한 VLC 채널을 모델링하여 악의적인 재머에 의한 공격 영향과 통신 취약성을 분석한다.

ABSTRACT

As wireless communication technology advances to ensure high accuracy and safety at high speeds, research and development of Visible Light Communication (VLC) technology has been accelerated as an alternative to traditional radio frequency (RF) technology. As the radio spectrum of RF communication becomes more congested and demand for bandwidth continues to increase, VLCs that can use unlicensed frequency band are proposed as a solution. However, VLC channels have broadcasting characteristics that make them easily exposed to eavesdropping and jamming attacks, and are vulnerable to MITM (Man-In-The-Middle) due to their line of sight (LOS) propagation characteristics. These attacks on VLC channels compromise the confidentiality, integrity, and availability of communications links and data, resulting in higher data retransmission rates, reducing throughput and increasing power consumption, resulting in lower data transmission efficiency. In this work, we model vulnerable VLC channels to analyze the impact of attacks and communications vulnerabilities by malicious jammers.

키워드

Jamming attack, Visible Light Communication (VLC), Vulnerabilities, Eavesdropping, Jamming

Ⅰ. 서 론

가시광 통신(VLC, Visible Light Communication)은 무선 주파수(RF, Radio Frequency)를 이용하는 기존의 무선통신보다 더 넓은 비면허 주파수 대역을 이용하며 빠른 전송속도를 보장하기 때문에 차세대 무선통신 기술로 주목받고 있다 [1]. 하지만, VLC의 LOS (Line of Sight) 특성으로 인하여 재밍(jamming), 도청, 중간자 공격 등에 취약하다 [2].

* corresponding author

본 논문에서는 VLC 채널에 대한 재밍 공격의 영향과 통신 취약성을 분석한다.

II. VLC 시스템 모델

VLC 시스템의 구성 요소는 LED (Light Emitting Diode) 송신기, 광검출기가 있고 각 파라미터는 표 1과 같다. LED는 IM/DD (Intensity Modulation/Direct Detection) 광전송방식을 사용하고, 각 LED의 링크는 SISO (Single Input Single Output)로 가정한다. 시스템 구성도는 그림1과 같고, LED의 위치는 각각 (2,2), (2,4), (2,6), (4,2), (4,4), (4,6), (6,2), (6,4)이다. 재머는 (6,6)에 위치하며 주변 LED 링크에 재밍 공격을 하여 통신 성능을 열화시킨다.

표 1. VLC 시스템 파라미터

Room	
Size	8×8×3 m^3
Reflection coefficient	0.8
Source	
Semiangle at half power	45 deg.
Transmitted power (per LED)	10 mW
Transmitted power (jammer)	50 mW
Number of LEDs per array	30 × 30
Receive	
Half-angle FOV	70 deg.
Receive plane above the floor	1 cm^2

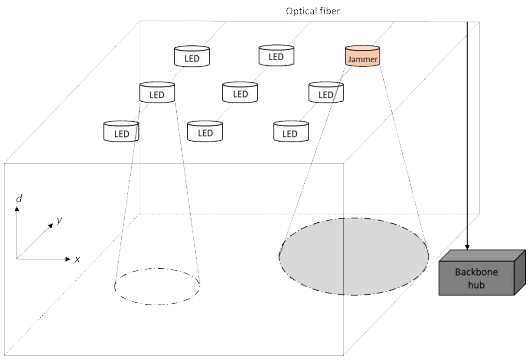

그림 1. VLC 시스템 구성도

III. VLC 공격 및 취약성 분석

재밍 공격의 영향을 분석하기 위한 평가 지표로 비트 에러율(BER, Bit Error Rate)을 사용하였다 (1). SINR(Signal-to-Interference-plus-Noise-Ratio)는 식 (2)를 이용하여 계산했다 [3]. 이때, R은 광검출기의 응답도, P_r은 수신 신호, σ_{shot}과 $\sigma_{thermal}$은 노이즈, P_j는 재밍 신호를 의미한다.

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

$$SINR = \frac{(RP_r)^2}{\sigma_{shot}^2 + \sigma_{thermal}^2 + P_j^2} \tag{2}$$

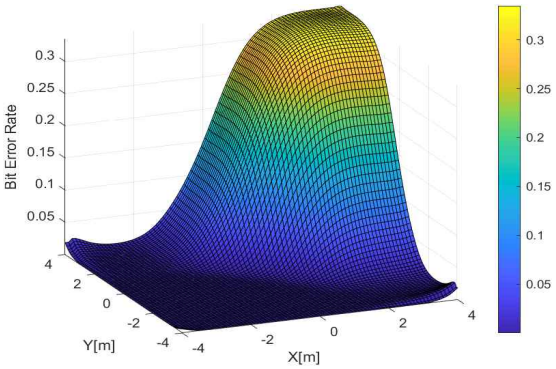

그림 2. VLC 채널 재밍 공격 시 비트 에러율

그림 2는 재밍 공격 시 VLC 채널의 BER을 보여준다. 재머와 인접한 구역은 BER이 30% 이상 증가하는 것을 확인하였다. BER이 높아지면 재전송되는 비트의 양이 증가하기 때문에 지정된 시간 안에 전송하는 정보의 처리량이 낮아지고, 소모되는 에너지가 증가하여 통신 성능이 나빠진다. 또한, 통신 데이터의 무결성과 가용성을 훼손하여 보안성이 낮아지게 된다.

IV. 결 론

본 논문에서는 VLC 링크에 대한 재밍 공격을 실시하였고, BER을 이용해 공격의 영향을 분석하였다. VLC는 넓은 주파수 대역을 사용하여 빠른 데이터 전송 속도를 가지지만, 재밍 공격, 도청 등에 취약한 문제점을 가지고 있기 때문에 이에 대한 물리계층 보안 기술이 요구된다. 향후 과제로는 악의적인 재머와 도청 공격의 영향 분석과 탐지 및 대응 방법을 연구할 계획이다.

Acknowledgement

이 논문은 2021년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원(No. 2020R1F1A1061107)과 2021년도 정부(산업통상자원부)의 재원으로 한국산업기술진흥원의 지원(P0008703, 2021년 산업혁신인재성장지원사업)을 받아 수행된 연구임.

References

[1] N. Chi, Y. Zhou, Y.Wei, and F.Hu, “Visible light communication in 6G: Advances, challenges, and prospects.” *IEEE Vehicular Technology Magazine* 15.4, 93-102, 2020.

[2] C. Rohner, S. Raza, and D. Puccinelli. “Security in visible light communication: Novel challenges and opportunities.” *Sensors & Transducers Journal* 192.9, 9-15, 2015.

[3] G. Blinowski. “The feasibility of launching physical layer attacks in visible light communication networks.” *arXiv preprint arXiv*:1608.07146, 2016.