Secure Visible Light Communication System via Cooperative Attack Detecting Techniques

SO-HYUN PARK, SOYOUNG JOO, AND IL-GU LEE
Department of Future Convergence Technology Engineering, Sungshin Women’s University, Seoul 02844, South Korea
Corresponding author: Il-Gu Lee (iglee@sungshin.ac.kr)

This work was supported in part by the National Research Foundation of Korea (NRF) Grant by the Korean Government through the Ministry of Science and ICT (MSIT) under Grant 2020R1F1A1061107, and in part by the Korea Institute for Advancement of Technology (KIAT) Grant by the Korean Government through the Ministry of Trade, Industry and Energy (MOTIE) (The Competency Development Program for Industry Specialist) under Grant P0008703.

ABSTRACT 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.

INDEX TERMS Cooperative attack detection, jamming, visible light communication (VLC), light-emitting diode (LED), security.

I. INTRODUCTION Visible light communication (VLC) uses a wider frequency band than radio frequency (RF), enabling rapid transmission of vast amounts of data and solving RF spectrum crunch [1]. Because VLC simultaneously supports communication functions using lighting devices, the VLC system is simplified and ecofriendly with an improvement in energy efficiency [2]. In addition, unlike RF radio waves that can easily diffract and transmit, they are secure because of their radio wave characteristics that cannot pass through the wall [3]. Light-emitting diodes (LEDs) and laser diodes (LDs) can be used as light sources for VLC systems. In indoor VLC systems, LEDs are the main light source because of their low vision protection restrictions. On the other hand, LD can transmit data faster and farther outdoors but has limitations because of energy efficiency, performance, cost, and vision protection issues [4]. Recently, LED and LD-based VCLs have been installed in smart cities, smart homes, underwater communication, and intelligent transport systems (ITS) [5].

VLC is known for high-level security owing to its straightness and transparency of radio waves, which prevent data leakage and manipulation out of the space where data are being transmitted [3]. Fast data transmission speed is an advantage of VLC systems using smart LEDs in smart-office environments [8]. In a dense mesh network environment to build a constant intelligent information system, there is a problem that it is vulnerable to attacks such as eavesdropping and jamming because of broadcasting and superposition characteristics. Users can easily remotely control the power and spectrum of the light sources of smart LEDs to improve energy efficiency, convenience, and security. However, it can also be manipulated as a jammer that infringes on the availability of adjacent LEDs [9]. Jammer sabotages the transmission by increasing the bit error rate (BER) and retransmission rate of data. This degrades the effective data rate and consumes more energy, resulting in the deterioration of the energy efficiency (EE). There are...
several types of jammers: illumination, disguised, and noise jammers [10], and all of them emit jamming signals toward the legitimate receivers. The type of jammer used in this study is the illumination jammer.

This study proposes a jamming attack detection method for a VLC system and a security method capable of responding thereto. In a smart-office environment using VLC, it can be assumed that the influence of LEDs is always identical because LEDs are fixed at a specific location. In this study, a method of detecting and responding to jamming attacks was proposed through a cooperative communication performance comparison between adjacent LEDs. As the cooperative detection method use the performance degradation pattern, it can be extended and applied to other types of jammer scenario.

The main contributions of the study are listed as follows.
- A jamming attack system was modeled in a smart LED-based VLC environment. Using the line of sight (LOS) characteristics of LEDs, the performance degradation patterns of each VLC link because of jamming attacks were analyzed and categorized.
- A jamming attack detection method through cooperation between LEDs was proposed, and the performance of the cooperative detection method was evaluated by measuring the attack detection rate.
- We proposed a method that can effectively respond to jamming attacks using LED cooperative transmission techniques. The most efficient attack response technique was analyzed by comparing the effective data rate and EE of each response technique.

The remainder of this study is organized as follows. Section II introduces related research, and Section III introduces the VLC system model assumed in this study. In Section IV, the VLC attack detection algorithm and response techniques are described. The performance of attack detection and response simulations are evaluated in Section V. Finally, Section VI concludes the study.

II. RELATED WORKS
In this section, related studies on VLC security are analyzed. Table 1 summarizes the previous studies on VLC security.

Most of the existing studies related to VLC security are related to eavesdropping, and there are only a few studies on jamming attacks. Jamming attacks correspond to intercell interference in the VLC system, and many studies have mitigated the interference in improving the performance of the VLC system. However, although existing studies suggest a variety of ways to respond to attacks such as jamming and eavesdropping in VLC systems, few studies have suggested methods to effectively detect attacks. This study proposes a technique for detecting and preventing jamming attacks using the characteristics of the VLC system.

A. VLC INTERFERENCE MITIGATION
Interference that may occur in the VLC system can be classified as intracell interference and intercell interference (ICI). Cochannel interference (CCI), renowned for in-cell interference, is a congestion that occurs when other devices approach the same channel, resulting in longer latency. A countermeasure for reducing CCI includes color shift keying. Several studies have been conducted on optimizing the field of view (FOV) of an angle diversity receiver (ADR) as a technique for reducing CCI [11]–[14]. Elddeeb et al. reduced CCI interference by proposing a constructed field-of-view angular college receiver (CFOV-ADR) that complements conventional ADR [11]. CFOV-ADR is a method of effectively separating LOS signals from adjacent transmitters by optimizing the FOV angle of the photodetector (PD). Through simulations, CFOV-ADR was proven to be superior to conventional ADR at all locations, and an optimized angle for removing CCI was suggested. Hosney et al. proposed a method for limiting the FOV of ADR as a solution to CCI. The FOV was optimized to achieve a low BER by simulating various positions of the multi-input multi-output (MIMO) system [12]. Hosney et al. proposed a management technique through CFOV-ADR of a VLC MIMO system for performance degradation caused by CCI [13]. This article proposes a scheme that uses CFOV-ADR to reduce the number of interference signals and eliminate interference signals using a maximum likelihood equalizer and least square channel estimation. Improved performance was demonstrated by comparing the BER of the time division multiple access technique. Eldeeb et al. proposed CFOV-ADR, which significantly reduces CCI, which limits the performance of VLC downlinks [14]. The photodetector, which applies the zero-forcing algorithm to conventional ADRs with an optimized FOV, helps to eliminate CCI. Simulation results show that the CFOV-ADR proposed in this study achieved a higher signal-to-interference-plus-noise ratio (SINR) than a single receiver and conventional ADR. Ibrahim et al. developed odd clipped optical orthogonal frequency-division multiplexing (OCO-OFDM) technology to propose a shared frequency reuse technology that can increase spectral efficiency while minimizing interference compared to conventional asymmetric clipped OFDM (ACO-ODM) technology [15]. Shared frequency reuse technology reduces interference by dividing the entire bandwidth into shared or reused bands and providing services by dividing the interference and noninterference areas.

ICI is the interference caused by overlapping communication areas with multiple access points (APs), and various countermeasures have been studied. Kim et al. proposed interleaving interference (ILIC) to eliminate possible ICI in multicell VLC systems [16]. In an environment where multiple LEDs are used as light sources, such as multi-input single-output (MISO) visible light communication systems, different data must be transmitted simultaneously from each LED to increase the transmission capacity. In this case, there is a problem in that only the signal with the highest received power may be sensed. The ILIC method can improve the overall average BER and throughput by setting the signal with the highest received power as an interference signal.
TABLE 1. Previous studies on VLC security.

| Previous studies | Performance / Security issues | Methods | Ref. | Main idea |
|------------------|-------------------------------|---------|------|-----------|
| VLC interference mitigation | Intra-cell interference | ADR | [10]-[13] | Optimizing the FOV of an ADR as a technique for reducing CCI, ISI to mitigate intra-cell interference |
| | Inter-cell interference (ICI) | OFDM | [14] | Using OFDM technology to propose a shared frequency reuse technology that can increase spectral efficiency while minimizing interference |
| | | ILIC | [15] | ILIC to eliminate possible ICI in multi-cell VLC systems. |
| | | ADR | [16]-[17] | Optimizing ADR as a method to mitigate ICI |
| | | Precoding | [18]-[19] | Cell coordination/Precoding methods to mitigate ICI |
| VLC PLS | Jamming | | [9] | Analyzed communication interruption and damage when malicious transmitter exists by measuring BER |
| | | Eavesdropping | AN, Friendly jamming | [23]-[28] | Add AN or friendly jamming signal with the transmission signal to prevent eavesdroppers from decoding original data. AN, friendly jamming is mainly used with beamforming. |
| | | Beamforming | | [29]-[31] | Optimizing beamforming vector to maximize the received signal and prevent eavesdroppers get enough signals to decode the original data |
| | | LED selection | | [32]-[34] | Selecting an appropriate LED link to respond to eavesdroppers. |
| | | Protected zone | | [35] | Establishing eavesdropping-free zone as protected areas to improve the confidentiality of legitimate users |

and removing it from the entire received signal to detect a relatively low received power signal. Furthermore, a method of optimizing ADRs is also used to mitigate ICI [17], [18]. Chen et al. optimized the angle of the lateral detector slope of typical ADRs, improving cell capacity and SINR volatility over conventional frequency allocation-based ICI mitigation techniques [17]. Játiva et al. proposed a pyramid ADR to mitigate the ICI of the system [18]. This study compared and analyzed the selected best combining, equal gain combining, and maximum ratio combining (MRC) schemes, proving that the MRC scheme performs best when combined with ADR. Several studies have adopted a cooperative or precoding method to reduce ICI [19]–[20]. According to Pham and Pham, intracell interference can be handled using an underlying precoding technique, but ICI is difficult to process [19]. This study proposes a cell coordination/cooperative precoding design to mitigate interference. This method is an interference mitigation technique that uses zero-forcing-based precoding technology by measuring the degree of channel capacity degradation because of interference signals. Through simulation, it was proven that the partial cooperative precoding method has the best performance improvement. Pham et al. proposed a zero-forcing precoding method that can alleviate ICIs [20]. An adjusted precoding method was designed such that the LED array in the cell could cooperate with the LED array of other cells. This method maximizes the user’s sum rate, which further increases when the transmission power increases.

B. VLC PHYSICAL LAYER SECURITY

In VLC, regardless of intention, interference can be assumed as a jamming attack that hinders the secure communication of links. Blinowski et al. measured the BER and analyzed communication interruption and damage when normal communication was disturbed in the presence of a malicious transmitter [9]. In this study, a variety of environments with malicious transmitters were designed using computer-aided design tools, and the influence range of malicious transmitters was analyzed by calculating the areas affected by the jammer in each environment. The study demonstrated that a transmission range of up to 75% may be hindered in environments with a malicious jammer, and jamming areas increase when the semiangle of the transmitters increases. Ijaz et al. analyzed vulnerability to active attacks by malicious transmitters installed in the VLC system and suggested defensive methods to prevent spoofing and jamming attacks [21]. This study compared the orthogonal multiple access (OMA) VLC channel and nonorthogonal multiple access (NOMA) VLC channels to find more effective authentication methods by distinguishing between the cases. In the case of jamming...
attacks, the receiver receives signals from both malicious attack nodes and legitimate nodes, and processed jammer signals as interference signals to extract legitimate signals.

Few studies have been conducted on jamming in VLC physical layer security (PLS), and most VLC PLS studies have proposed a method of evaluating channel security and mitigating eavesdropping using WYNER’s Wiretap model-based secrecy capacity on the possibility of eavesdropping in VLC [22]. Secrecy capacity refers to the amount of data that can be safely transmitted without eavesdropping out of the total channel capacity. The main solutions to eavesdropping are artificial noise (AN), friendly jamming, beamforming, and LED selection techniques.

AN is an eavesdropping technique that adds noise to prevent eavesdroppers from decoding transmission signals directed to the original receiver [23]. A typical AN method is friendly jamming [24]–[28]. In the VLC system, friendly jamming is a method in which adjacent LEDs send jamming signals to eavesdroppers to prevent legitimate users from receiving data normally. Tian et al. analyzed the secrecy rate of indoor VLC systems with multiple LEDs using jamming [24]. In a multi-LED-VLC system in which both legitimate users and eavesdroppers exist, a method for ensuring confidentiality by utilizing interfering signals is suggested. In this study, the authors compared the effect when differentiating the ratio between legitimate information sender and jammer to prove the rate at which the average confidentiality is maximized. It is assumed that a legitimate receiver can detect and ignore a friendly jamming signal, and the eavesdropper cannot. Friendly jamming signals improve security by ensuring the confidentiality of the system by lowering the signal-to-noise ratio (SNR) of the eavesdropper. When half of the transmitting LEDs transmit signals containing information and the rest transmit jamming signals, the average secrecy rate is ultimately maximized. AN and beamforming are mainly used together, Mostafa and Lampe introduced pattern synthesis of large LED arrays, including beamforming and friendly jamming, and restrictions on secrecy capacity as a way to hide VLC communication data and ensure secure communication from unauthorized receivers [25]. The pattern synthesis of large-scale LED arrays means that in rooms with large-scale LEDs, beams toward legitimate receivers form arbitrary radiation patterns, enabling safe transmission. Cho et al. considered PLS using both beamforming and jamming when an eavesdropper is randomly located [26]. The transmission signal in which the random jamming signal is mixed is efficient in preventing eavesdropping because it is difficult to extract and decode only the original data. In this study, statistical information on the location of random eavesdroppers was obtained using jamming signals at the same time as beamforming, and it was proved through simulation that the average secrecy rate could be maximized. Arfaoui et al. evaluated the security performance of AN-based beamforming on MISO VLC eavesdropping channels [27]. This study proposes a method to optimize beamforming when there is no information about the location of eavesdroppers and when there is incomplete channel state information (CSI). Al-Khor et al. proposed a friendly jamming function and beamforming design that can address a violation of information confidentiality because of broadcasting characteristics in RF/VLC hybrid systems [28]. This study demonstrated the effectiveness of the eavesdropping attack response plan for hybrid RF/VLC networks using several relays with jamming capabilities. In addition, a beamforming design for a VLC capable of maximizing the secrecy capacity was proposed. Pham and Pham considered the EE issue in conventional AN-based precoding [29]. VLC consumes energy for lighting and data transmission, and as energy for data transmission needs to be optimized in fixed situations, EE must be considered for AN-based precoding. In addition, many studies have been conducted to correspond to VLC eavesdropping using only beamforming [30]–[32]. Xiao et al. proposed a reinforcement learning-based eavesdropping prevention framework through smart beamforming on MISO VLC eavesdropping channels [30]. Liang et al. proposed a method to maximize the signal power received by legitimate users in the secure zone and optimize beamforming to prevent eavesdroppers in the secure zone does not receive sufficient signals to decode [31]. Riurean solved the problem of optimizing VLC transmission through zero-forcing beamforming, which is distinct from conventional beamforming studies that considered only the type of active eavesdropper (AED) or passive eavesdropper (PED) [32].

One of the response methods of VLC eavesdropping is to select an appropriate LED [33]–[35]. Gargetal. proposed a way to respond to eavesdropping by selecting and transmitting higher links between two LED links using transmitters consisting of two LED elements [33] and [34]. In [34], a method for measuring CSI using a pilot signal was also described. When the secrecy rate of the two LED elements chose a better link than using only one LED, the performance corresponding to eavesdropping was better. Cho et al. proposed an optimized method for selecting a suitable number of LEDs in a multiuser VLC system, developing an existing study [35] that selects the nearest LED in a single-user VLC system. If many LEDs are selected, not only legitimate users but also eavesdroppers can receive signals, and if fewer LEDs are selected, legitimate users would not receive enough signals; therefore, it is important to select an optimal LED set.

Yin and Haas demonstrated that the cooperation between neighboring APs in a multiuser VLC network can improve the confidentiality of legitimate users and that establishing an eavesdropping-free zone as protected areas can significantly improve the confidentiality of legitimate users [36]. This study demonstrated the possibility of building a VLC system with high security requirements by utilizing PLS methods that improve confidentiality.

III. VLC SYSTEM MODEL

The smart LED-VLC system model is illustrated in Fig. 1. The components of the VLC system include a smart LED transmitter and PD. The smart LED transmitter is an LED

20476
on the ceiling, and the PD is located on the receiver plane. In Fig. 1, x, y, and z represent the location of the room in which the LED-VLC system is installed, and h is the vertical distance between the LED and the receiver plane. The signal transmitted from the backbone network is transmitted through optical fibers to modulate the light signal to the LED transmitter for communication. We assume that the LED uses an intensity modulation/direct detection (IM/DD) optical transmission method and is set up as a MISO environment from the LED to the user. With the IM/DD modulation scheme, the optical intensity is modulated directly in proportion to the driving current magnitude and is detected as a current magnitude directly in proportion to the received optical signal intensity. In indoor VLC systems, because LOS elements are stronger than NLOS (Non-LOS), only LOS propagation models were considered for VLC channels [36].

Fig. 2 shows the SNR distribution diagram according to the VLC system model environment, as shown in Fig. 1. As VLC has straightness, the SNR in the area just below each LED is the highest, and the farther away from the LED, the lower the SNR. The propagation characteristics of LED-based VLC systems can be verified through the SNR distribution diagram, and the pattern of jamming attacks on LED-based VLC systems can be categorized using the straightness of the VLC system. Table 2 lists the system parameters of the VLC components, such as the rooms, transmitters, and receivers. Nine LEDs were installed on the ceiling at uniform intervals, and the half-angle of full width at half maximum was set to 45°. The transmission power of one LED was 10 mW, and the jammer LED was transmitted at 50 mW. One LED consisted of an arrangement of 30 × 30. The receiver plane where the PD is located is 0.85 m away from the ground, the active area of the PD is 1 cm², and the half-angle of the FOV is 70°.

A. JAMMING ATTACK

The BER was used as an evaluation index to analyze the impact of jamming attacks. With the IM/DD modulation technique, the SINR with BER can be obtained as follows [9]:

\[
BER = Q(SINR),
\]

\[
SINR = \frac{(R \cdot P_{rx})^2}{N + (P_{rj})^2},
\]

where

\[
N = \sigma_{shot}^2 + \sigma_{thermal}^2,
\]

\[
\sigma_{shot}^2 = 2qRP_{rx}B + 2qI_B \frac{B}{2}.
\]

A jamming system was constructed assuming that all LED sets were operated by attackers, and several jamming environments were compared while increasing the number of jammers. In this study, the number of jammers was fixed at one, and Fig. 3 shows the case when LED 5 is a jammer among the nine LEDs. R is the responsivity of the PD and is initialized to 1, \( P_{rx} \) is the received power, \( N \) is the total noise variance, and \( P_{rj} \) is the power received from the jammer. Specifically, \( P_{rj} \) acts as a temporary interference and increases, the overall SINR decreases, and the BER increases. Noise is composed of Poisson noise (\( \sigma_{shot}^2 \)) and thermal noise (\( \sigma_{thermal}^2 \)), but the VLC system was modeled considering only Poisson noise [9], where q is the elementary charge, B is the

| Components | Parameters | Values |
|------------|------------|--------|
| Room | Size (m³) | 9 × 9 × 3 |
| Source | Location (LED 1–9) | (1.5, 1.5, 31, (4.5, 1.5, 3), (7.5, 1.5, 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) |
| Modulation scheme | IM/DD |
| Receiver | Receiver plane above the floor (m) | 0.85 |
| Active area (cm²) | 1 |
| Half-angle FOV (deg) | 70 |
FIGURE 3. Example of jamming attack in VLC system (when LED 5 is a jammer).

FIGURE 4. Illumination of VLC system.

bandwidth of the PD in units of Hz, I_B is the photocurrent because of background radiation, and I_2 = 0.562 is the noise bandwidth factor.

Fig. 4 shows the illumination and parameters of the VLC system, as shown in Fig. 1. Assuming that an LED has a Lambertian radiation pattern, the order of Lambertian m_l is defined as follows:

\[ m_l = \frac{\ln(2)}{\ln(\cos(\phi_{1/2}))} \] (5)

\( \phi_{1/2} \) means the half-angle of the full width of the LED.

The \( P_{rx} \), power received from the receiver, and \( H \), the direct current (DC) gain of the VLC channel, can be obtained as follows:

\[ H = \frac{(m_l + 1) \cdot A}{2\pi d^2} \cos^m(\theta) \cdot \cos(\psi) \] (6)

\[ P_{rx} = P_{tx} \cdot H \cdot T_s(\psi) \cdot g(\psi), \quad 0 \leq \psi \leq \psi_{con} \] (7)

In this case, \( P_{tx} \) represents the transmission power, \( A \) denotes the physical area of the PD, \( \psi \) is the incident angle related to the vertical axis to the reception plane, \( T_s(\psi) \) is the filter gain (set to 1), \( g(\psi) \) denotes the concentrator gain, \( \psi_{con} \) denotes FOV, and \( d \) is the distance between the LED and the detector. The concentrator gain in the receiver is defined as follows:

\[ g(\psi) = \begin{cases} \frac{n^2}{\sin^2(\psi_{con})}, & 0 \leq \psi \leq \psi_{con} \\ 0, & 0 \geq \psi_{con} \end{cases} \] (8)

\( n \) is the refractive index of the PD lens and is set to 1.5. In this study, performance degradation according to the power of the LED and jammer LED was analyzed using the BER.

Because the smart LED can adjust the intensity, beam width, etc. of the light source, one of the LEDs can be used as a jammer [9]. Fig. 4 shows the case where LED 5 is a jammer among the nine LEDs. Jammer’s strong signal can significantly interfere with the link of the peripheral LEDs, which can degrade the link performance. Interference with peripheral LED links may be increased by increasing the power of the jammer or increasing the beamwidth.

In this study, jamming attacks were attempted by increasing the transmit power of the jammer. To analyze the impact of the jamming attack, it is divided into nine equal parts and expressed as Section 1 to Section 9 in the same way as the number of LEDs, as shown in Fig. 5.

Fig. 6(a)–(c) show the BER according to the location of the receiver when LED2, LED5, and LED9 are jammers, respectively. Jammer’s beam width is fixed (\( \phi_{1/2} \)), and the transmit power is increased from 10 to 50 mW to carry out a jamming attack. LED2, LED4, LED6, and LED8 analyzed only LED2 because the BER patterns were identical, and LED1, LED3, LED7, and LED9 were represented by LED9 because of the identical BER patterns. Accordingly, the BERs of LED2, LED5, and LED9 may represent the BER pattern of the entire LED. In Fig. 6(a)–(c), it can be observed that the effective data rate decreased owing to the increase in the BER of the LED link adjacent to the jammer.

Because of the influence of jamming, it was confirmed that the performance of the link adjacent to the jammer changed with a certain rule depending on the location of the jammer. Fig. 6(d)–(f) show the effective data rate calculated using the BER of each section according to the transmission power of the jammer when the jammer is LED2, LED5, and LED9, respectively. Fig. 7 is a graph summarizing the results of Fig. 6(d)–(f). The effective data rate refers to the amount of data that can be transmitted without errors, and the data rate of the VLC system is set to 100 Mbps. The effective data rate was calculated using the following equation:

\[ \text{Effective Data Rate} = \text{Data Rate}(1 - \text{BER}) \] (9)
When LED2 was jammer, the BER of Section 5 was the highest, whereas Sections 1 and 3, Sections 4 and 6, and Sections 7 and 9 were identical, respectively. When LED5 was the jammer, the BER of Sections 1, 3, 7, and 9 were identical, and likewise, the BERs of Sections 2, 4, 6, and 8 were identical. Lastly, if LED9 was a jammer, the BER of Sections 6 and 8, which are closest to LED9, were the highest and identical, and the BERs of Sections 3 and 7, and Sections 2 and 4 were identical.

BER has a maximum value of 50%, and Fig. 8 shows the effective data rate when the Tx power of the jammer increases from 2000 to 10000 mW when LED 5 is a jammer. If the effective data rate reaches 50 Mbps, the BER becomes 50%, which shuts down the links and violates the availability.

**IV. ATTACK DETECTION AND RESPONSE SYSTEM**

**A. CLASSIFICATION ALGORITHM**

Detecting jamming attacks corresponds to a classification problem that distinguishes whether the cause of deterioration in communication performance is a jamming attack. The cause of performance degradation, that is, SINR reduction, can be caused by jamming attacks as well as obstacle blocking transmission links. In this study, signals from peripheral LEDs or light sources were not considered as interference, and objects that interfered with direct links between LEDs and receivers were defined as obstacles. The SINR when performance is degraded by an obstacle in a jamming attack...
can be obtained as follows:

\[
SINR = \begin{cases} 
\frac{(P_{rx})^2}{N + (P_{t,x})^2} & (P_{rx}^{(s,t)} \neq 0) \\ 0 & (P_{rx}^{(s,t)} = 0) \end{cases} \tag{10}
\]

\(P_{rx}^{(s,t)} (0 < s \leq S, 0 < t \leq T, S = 90, T = 90)\)

is the received signal power at the coordinates \((s, t)\) of the receiver plane, and \(S\) and \(T\) represent the maximum value of the receiver that may be located on the X and Y axes of the receiver plane, respectively. \(P_{rx}^{(s,t)} = 0\) is the case when the received signal power becomes zero, where an obstacle is located at a vertical distance from the receiver.

The jamming attack detection model uses BER as an evaluation index to distinguish between attacks and obstacles and evaluates classification performance, that is, detection rate, as a confusion matrix. The detection conditions listed in Table 3 were created by analyzing the pattern according to the BER value in Fig. 7. Feature extraction can be used to classify attacks and obstacles. Table 3 lists the detection conditions, the location of the jammer, and the BER when the Tx power of the jammer is 50 mW. The pattern of the BER is identical when the sections are equally affected by the jammer and the BER increases when the section is closer to the jammer. For example, when the LED2 is a jammer, the BERs of Sections 1 and 3, Sections 4 and 6, and Sections 7 and 9 are identical (BER1), Section1 and Section3 are always higher than the maximum BER of Section4 and Section6. In addition, the BER of Section6 is always greater than that of Sections 7 and 9 (Rel-BER1). Jamming detection was done by extracting the features and patterns of performance degradation. Likewise, the patterns of other types of jamming attack, e.g., disguised and noise jamming, can be extracted and utilized to detect corresponding attacks.

The detection algorithm detects performance degradation using Table 3 and classifies whether the cause of performance degradation is because of jamming attacks or obstacles through cooperation between smart LEDs. If performance degradation occurs but performance does not degrade according to the detection conditions in Table 3, it is regarded as performance degradation because of obstacles, and if the performance degradation pattern matches the detection conditions, it is considered as a jamming attack.

To evaluate the performance of the cooperative detection model, a k-random detection model was introduced, and the detection performance was compared. The k-random detection model does not apply cooperative detection conditions and determines that it is an attack if more than k LEDs out of all LEDs deteriorate [37], [38].

B. ESTABLISHING GROUND TRUTH

Data on performance degradation because of attacks and obstacles were collected for attack detection. The ground truth is the BER of each section, which is capable of evaluating the performance degradation of each LED link. Input the BER of each section into the detection algorithm to classify whether it is an attack or not.

To evaluate the performance of the cooperative detection model, obstacles were modeled together even in a jamming attack situation so that jamming and performance degradation because of obstacles occurred concurrently. Since obstacles can occur one by one in each section, they can occur from a minimum of 0 to a maximum of 9. Obstacles are set to account for 1/4 of a section, and where the obstacle is located, the received power becomes zero. Even if performance degradation is caused by jamming attacks and performance degradation caused by obstacle overlap, attacks can be detected by comparing the performance degradation patterns between adjacent LEDs. For example, in the case of BER1, even if the BER of Sections 1 and 3 varies owing to obstacles, the BER values of Sections 4, 6, 7, and 9 can be compared and detected.

C. ATTACK DETECTION SYSTEM

Fig. 9 shows the pipeline of the attack detection system. The attack detection system detects attacks by comparing the detection conditions by inputting the ground truth, collected before and after the attack, into the classification algorithm. The BER of each section is collected in advance of a jamming attack and collected afterward when performance degradation occurs, and cooperative attack detection is performed through detection conditions. For the k-random model, we compare the BER and determine that it is an attack if performance is poor in more than k LED sections of the entire LED [37], [38].

To properly detect an attack and evaluate the attack detection rate that distinguishes what is not an attack, precision, recall, accuracy, and f1 score were derived using a confusion matrix. The confusion matrix is a table comparing the actual and predicted values to evaluate the classification performance. True positive (TP) classifies an actual attack as an attack, false negative (FN) classifies an actual attack as not an attack, a false positive (FP) classifies a false attack as an attack, and a true negative (TN) classifies a false attack as a false attack. The precision, recall, accuracy, and f1 score may be derived using TP, FN, FP, and TN. Precision is the ratio...
of an actual attack from the detection model classified as an attack, recall is the ratio of the detection model classified as an attack from an actual attack, and accuracy is the unified average of both detection of attacks and nonattack.

In the k-random detection model, if performance degradation occurs in more than k sections, it is considered to be an attack, so it can be expected that even performance degradation rather than a jamming attack will be classified as an attack.

D. ATTACK RESPONSE SYSTEM

A typical way to minimize the impact of jamming attacks is to increase the transmission efficiency using cooperative transmission methods. Because the cooperative transmission transmits the same signal from multiple transmitters, it increases the received signal gain, reduces the influence of jamming interference, and improves the SINR.

As our study uses the MISO channel, a multi-LED-based VLC system in which signals from multiple LEDs overlap and are sent to one user, it is already being effective by cooperative transmission methods. In this section, three cooperative transmission methods listed in Table 4 were compared to evaluate the effective data rate of the link affected by the jammer and suggest a method to increase the power efficiency. Using a single LED as a cooperating transmission method is a way to increase the Tx power of LED affected by jamming attack, using dual LEDs is a way to increase the Tx power of both LED affected by jamming attack and LED closest to the affected LED and farthest from jammer, and using Octuple LEDs is a way to increase the Tx power of all LEDs. There is only one LED and a jammer LED in the single LED-VLC system model, dual LEDs VLC system which has one victim LED, one jammer LED, and one adjacent LED. The Octuple LED-VLC system model has eight LEDs and one jammer LED.

EE and BER were used as indicators to evaluate the effectiveness of cooperative transmission. Cooperative transmission can improve transmission gains to reduce the impact of jamming attacks, but EE degradation occurs. EE (Mbps/J) is calculated by dividing the effective data rate by the power consumption using the following equation:

$$EE = \frac{\text{Effective data rate}}{\text{total power consumption}}$$  \hspace{1cm} (11)

The EE and BER were measured according to the transmission power increment of the LED to evaluate the efficiency of the cooperative transmission technique. The increased transmission power because of transmission diversity is calculated as follows:

$$\text{Total Tx power} = \sum_{i=1}^{L} \left( \frac{\text{Tx power of single LED}}{L} \right)$$  \hspace{1cm} (12)

$L$ in the equation represents the number of LEDs that cooperate with each other. $L = 1$ in the single LED method, $L = 2$ in the dual LEDs method, and $L = 8$ in the Octuple LEDs method. One of the LEDs’ Tx power is set to transmit a different power for each method based on the Octuple LEDs method. In other words, one LED increases its Tx power by 80 mW in a single LED method, one LED increases by 40 mW in the case of dual LEDs, and one LED increases by 10 mW in the case of the Octuple LEDs.

V. PERFORMANCE EVALUATION

A. SIMULATION ENVIRONMENT

The jamming detection system and attack detection simulation were implemented in MATLAB. A total of 100 ground truths for each of the three jammers if jammer exists, and 300 ground truths if jammers do not exist; as a result, a total of 600 ground truths were randomly generated while the simulation was repeated 100 times. In the case of k-random,
if the performance of two or more LEDs (k = 2) deteriorated, it was set to determine that it was an attack. The detection performance of the k-random model was compared based on the change in the k value. Obstacles were set to occur above one and five of the entire LED sections. Fig. 10 shows an example of the received power when there are three obstacles. The received power \( P_{rx}(s,t) \), where the obstacle exists, is set to zero.

In addition, the detection rate according to the change in the number of obstacles and the value of k was also measured. Changes in detection rates between the k-random model and the cooperative model were compared when the obstacles increased from 1 to 9. The comparison allows us to evaluate a more effective detection model in situations with obstacles. The detection rate of the k-random model would be greatly influenced by the value of k. Therefore, the k-random model was evaluated by changing only the value of k from 2 to 9, and the number of obstacles was fixed at 5.

The classification algorithm determined that it was an attack if both BERC and Rel-BER were satisfied with the final detection condition. BERC is a feature in which the BER becomes the same owing to jamming attacks between certain sections, and Rel-BER is a detection condition using features that always have different relative sizes of BER. The classification algorithm was set as shown in Table 5. BERC and Rel-BER are the results of the OR calculations for each detail. There may be several arithmetic operations, but the experiment was conducted based on Table 5.

### TABLE 5. 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) |

**FIGURE 10.** Example of received power with obstacles.

**FIGURE 11.** Results of attack detection simulation.

**B. EVALUATION RESULTS**

Fig. 11 shows a graph comparing the detection results of jamming attacks between the k-random and cooperative models. Notably, the recall of the random k model was higher. The k-random model detected all attacks because it assumed an attack when there was performance degradation in more than k (k = 2). However, the model could not distinguish between the jamming attack and performance degradation, which led to low accuracy. Therefore, precision and accumulation were found to be 50%, which means that half of those judged to be attacks were not actual attacks.

Conversely, in the case of the cooperative detection model, the precision was 100%, which means that all performance degradation that the detection model judged to be an attack was correct. The recall of the cooperative model was 82% and the accuracy was 91%, and it was proved that the cooperative model was better than the k-random model for all evaluation indicators except precision. The cooperative model was able to detect 82% of all attacks, and it can be considered as a superior model because 100% of the performance distinguishes that the cause of performance degradation is not an attack.

Fig. 12 compares the accuracy of the detection rate of each model according to the number of LED sections with obstacles. Overall, the detection rate decreased as the number of obstacles increased, but hardly changed from a certain point and maintained the minimum detection rate. In the k-random model (k = 2), when the number of obstacles was 1, less than k, the detection rate was 67%, the highest among the total k-random models (k = 2), and the detection rate remained at 50% from the time the number of obstacles and k value were identical. Therefore, from this research, we can determine that the minimum detection rate of the k-random model (k = 2) is 50%. We also compared the detection rates when the value of k used in the classification algorithm of the k-random model increased to k = 4, k = 6, and k = 8. The detection rate remained at 50% when the number of
obstacles was identical to k-1. Regardless of the number of k, the minimum detection rate of the k-random model was 50%.

On the other hand, in the case of the cooperative model, the detection rate gradually decreased according to the number of obstacles, and the detection rate of 84% remained similar when there were more than five obstacles. From the simulation, we can conclude that the minimum detection rate of the cooperative model is 84%, and it has a minimum detection rate of approximately 1.68 times higher than that of the k-random model. Even in situations where there is a lot of interference, it is more effective to use a cooperative model because the minimum detection rate is much higher than that of the k-random model.

Fig. 13 shows the EE according to the total transmission power increment of the cooperating LEDs. Considering only the EE factor, the highest EE was shown when all LEDs cooperated, and the lowest EE was observed when only one victim LED’s power was increased.

Fig. 14 shows a graph measuring the effective data rate according to the increase in the total transmission power of the cooperating LEDs. The method that increased the effective data rate the most was the single LED technique, which increased the power of only one LED under attack. In the case of dual LEDs, which cooperated with only one adjacent LED and only the victim LED, the EE was the lowest and the effective data rate increased the least. When the total Tx power of the cooperative LEDs is 90 mW, the effective data rate of Octuple LEDs is 77% of that of the single LED, but as the total transmission power increases, from 570 mW, the effective data rate of Octuple LEDs gradually increases by more than 99.9% for Octuple LEDs and 100% for single LEDs.

When the total Tx power is 570 mW, the EE of single LEDs is 0.19, and the EE of the Octuple LEDs is 1.23, which is six times greater than that of using a single LED. Therefore, the use of the Octuple LEDs method is more efficient for the trade-off relationship between EE and BER. In other words, a method in which all LEDs cooperate to increase transmission power is the most efficient way to respond to jamming attacks in EE and ensuring effective data rates.

VI. CONCLUSION

The broadcasting and superposition features of LEDs in LED-based VLC systems are vulnerable to jamming attacks. However, there are only a few studies on existing VLC PLS studies that examine effective detection methods for jamming attacks. In this study, we propose a detection method that uses the cooperation between LEDs to effectively detect jamming attacks on a VLC system. To evaluate the performance of the cooperation detection model, a k-random model was implemented and compared. The accuracy of the cooperation detection model was 91%, which is 1.82 times higher than that of the k-random model with an accuracy of 50%. Even in an environment with many obstacles, the cooperative model showed a minimum detection rate of 84%,
which was 1.68 times higher detection performance than that of the k-random model. In addition, using the cooperative transmission technique allows an efficient response to jamming attacks while considering EE. However, experimental conditions such as the LED’s location, interference, and noise were limited in our detection model. In addition, there is a limitation in that the experimental results vary depending on the calculation method of the detection conditions. Future research aims to improve detection performance by establishing an artificial intelligence-based cooperative model through learning patterns of performance degradation because of attacks. It is possible to consider varying the type, location, or the number of the LED and the receiver.

REFERENCES
[1] L. E. M. Matheus, A. B. Vieira, L. F. M. Vieira, M. A. M. Vieira, and O. Gnawali, “Visible light communication: Concepts, applications and challenges,” IEEE Commun. Surveys Tuts., vol. 21, no. 4, pp. 3204–3237, 4th Quart., 2019.
[2] S. Rehman, S. Ullah, P. Chong, S. Yongchareon, and D. Komosny, “Visible light communication: A system perspective—Overview and challenges,” Sensors, vol. 19, no. 5, p. 1153, Mar. 2019.
[3] A. Jovicic, J. Li, and T. Richardson, “Visible light communication: Opportunities, challenges and the path to market,” IEEE Commun. Mag., vol. 51, no. 12, pp. 32–36, Dec. 2013.
[4] F. Zufar, M. Bakaul, and R. Parthiban, “Laser-diode-based visible light communication: Toward gigabit class communication,” IEEE Commun. Mag., vol. 55, no. 2, pp. 144–151, Feb. 2017.
[5] S. Ariyantti and M. Suryanegara, “Visible light communication (VLC) for 6G technology: The potency and research challenges,” in Proc. 4th World Conf. Smart Trends Syst., Secur. Sustainability (WorldS4), London, U.K., Jul. 2020, pp. 490–493.
[6] G. Blinowski, “Security issues in visible light communication systems,” IFAC-PapersOnLine, vol. 48, no. 4, pp. 234–239, 2015.
[7] G. Blinowski, “Security of visible light communications systems—a survey,” Phys. Commun., vol. 34, pp. 246–260, Jun. 2019.
[8] C. Medina, M. Zambrano, and K. Navarro, “Led based visible light communication: Technology, applications and challenges—a survey,” Int. J. Adv. Eng. Technol., vol. 8, no. 4, pp. 482, Aug. 2015.
[9] G. Blinowski, “The feasibility of launching physical layer attacks in visible light communication networks,” 2016, arXiv:1608.07146.
[10] Y. M. Al-Moliki, M. T. Alresheedi, and Y. Al-Harthi, “Improving availability and confidentiality via hyperchaotic baseband frequency hopping based on optical OFDM in VLC networks,” IEEE Access, vol. 8, pp. 125013–125028, 2020.
[11] H. B. Eldeeb, H. A. I. Selmy, H. M. Elsayed, and R. I. Badr, “Co-channel interference cancellation using constraint field of view ADR in VLC channel,” in Proc. IEEE Photon. Conf. (IPC), Orlando, FL, USA, Oct. 2017, pp. 1–5.
[12] M. E. Hosney, H. A. I. Selmy, and K. M. F. Elsayed, “Co-channel interference reduction by optimizing field of view angle of angular diversity receiver in VLC systems,” in Proc. 22nd Int. Conf. Transparent Opt. Netw. (ICTON), Bari, Italy, Jul. 2020, pp. 19–23.
[13] 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, 2020.
[14] H. B. Eldeeb, H. A. I. Selmy, H. M. Elsayed, and R. I. Badr, “Interference mitigation and capacity enhancement using constraint field of view ADR in downlink VLC channel,” IET Commun., vol. 12, no. 16, pp. 1968–1978, Oct. 2018.
[15] A. Ibrahim, T. Ismail, K. F. Elsayed, S. M. Darweesh, and J. Prat, “Resource allocation and interference management techniques for OFDM-based VLC atto-cells,” IEEE Access, vol. 8, pp. 127431–127439, 2020.
[16] S. Kim, K. Lee, and K. Lee, “An inter-lighting interference cancellation scheme for MISO-VLC systems,” Int. J. Electron., vol. 104, no. 8, pp. 1377–1387, Mar. 2017.
[17] C. Chen, P. Du, H. Yang, W. D. Zhong, X. Deng, and Y. Yang, “Demonstration of Inter-cell Interference mitigation in multi-cell VLC systems using optimized angle diversity receiver,” in Proc. 4th Optoelectron. Global Conf. (OOGC), Shenzhen, China, Sep. 2019, pp. 36–39.
[18] C. A. Azurdia-Meza and M. R. Canizares, “Performance enhancement of VLC-based systems using diversity combining schemes in the receiver,” in Proc. IEEE Latin-Am. Conf. Commun. (LATICOM), Salvador, Brazil, Nov. 2019, pp. 1–6.
[19] T. V. Pham and A. T. Pham, “Coordination/Cooperation strategies and optimal zero-forcing precoding design for multi-user multi-cell VLC networks,” IEEE Trans. Commun., vol. 67, no. 6, pp. 4240–4241, Jun. 2019.
[20] T. V. Pham, H. Le Minh, and A. T. Pham, “Multi-cell VLC: Multi-user downlink capacity with coordinated precoding,” in Proc. IEEE Int. Conf. Commun. Workshops, Paris, France, May 2017, pp. 469–474.
[21] A. Ijaz, M. M. U. Rahman, and O. A. Dobre, “On safeguarding visible light communication systems against attacks by active adversaries,” IEEE Photon. Technol. Lett., vol. 32, no. 1, pp. 11–14, Jan. 1, 2020.
[22] M. Obied, A. M. Salhab, M. S. Alouini, and S. A. Zummo, “Survey on physical layer security in optical wireless communication systems,” in Proc. 7th Int. Conf. Commun. Netw. (ComNet), Hammamet, Tunisia, Nov. 2018, pp. 1–5.
[23] R. Negi and S. Goel, “Secret communication using artificial noise,” in Proc. Veh. Technol. Conf., Dallas, TX, USA, Sep. 2005, p. 1906.
[24] D. Tian, W. Zhang, J. Sun, and C.-X. Wang, “Physical-layer security of visible light communications with jamming,” in Proc. IEEE/CIC Int. Conf. Commun. China (ICCC), Changchun, China, Aug. 2019, pp. 512–517.
[25] A. Mostafa and L. Lampe, “Enhancing the security of VLC links: Physical-layer approaches,” in Proc. IEEE Summer Topicals Meeting Ser. (SUM), Nassau, Bahamas, Jul. 2015, pp. 39–40.
[26] S. Cho, G. Chen, and J. P. Coon, “Enhancement of physical layer security with simultaneous beamforming and jamming for visible light communication systems,” IEEE Trans. Inf. Forensics Secur. Commun., vol. 14, no. 10, pp. 2633–2648, Oct. 2019.
[27] M. A. Arfaoui, H. Zaid, Z. Rezki, A. Gharaieb, A. Chaaban, and M.-S. Alouini, “Artificial noise-based beamforming for the MISO VLC wiretap channel,” IEEE Trans. Commun., vol. 67, no. 4, pp. 2806–2879, Apr. 2019.
[28] J. Al-Khori, G. Nauryzbayev, M. M. Abdallah, and M. Hamdi, “Joint beamforming design and power minimization for friendly jamming relay- ing hybrid RF/VLC systems,” IEEE Photon. J., vol. 11, no. 2, pp. 1–18, Apr. 2019.
[29] T. V. Pham and A. T. Pham, “Energy efficient artificial noise-aided precoding design for visible light communication systems,” in Proc. Int. Conf. Comput., Netw. Commun. (ICNC), Big Island, HI, USA, Feb. 2020, pp. 507–512.
[30] L. Xiao, G. Sheng, S. Liu, H. Dai, M. Peng, and J. Song, “Deep reinforcement learning-enabled secure visible light communication against eavesdropping,” IEEE Trans. Commun., vol. 67, no. 10, pp. 6994–7005, Oct. 2019.
[31] S. Liang, Z. Fang, G. Sun, and J. Zhang, “A physical layer security approach based on optical beamforming for indoor visible light communication,” IEEE Commun. Lett., vol. 24, no. 10, pp. 2109–2113, Oct. 2020.
[32] S. Riurean, “A study on the VLC security at the physical layer for two indoor scenarios,” in Proc. MATEC Conf., 2021, pp. 1–5. [Online]. Available: https://www.proquest.com/conference-papers-proceedings-study-on-vlc-security-at-physical-layer-two/docview/2557050093/se-2
[33] Ambrish and P. Garg, “Dual-element indoor VLC network with two-stage secure link adaptation scheme,” in Proc. 5th Int. Conf. Signal Process., Comput. Control. (ISPPC), Solan, India, Oct. 2019, pp. 366–371.
[34] P. Garg, P. K. Sharma, and A. Gupta, “Secure information broadcasting analysis in an indoor VLC system with imperfect CSI,” IET Commun., vol. 15, pp. 526–532, Nov. 2020.
[35] S. Cho, G. Chen, and J. P. Coon, “Physical layer security in multiuser VLC systems with a randomly located eavesdropper,” in Proc. IEEE Global Commun. Conf. (GLOBECOM), Waikoloa, HI, USA, Dec. 2019, pp. 1–6.
[36] Y. Yin and H. Haas, “Physical-layer security in multiuser visible light communication networks,” IEEE J. Sel. Areas Commun., vol. 36, no. 1, pp. 162–174, Jan. 2018.
SO-HYUN PARK received the B.S. degree from the Department of Convergence Security, Sungshin Women’s University (SWU), Seoul, South Korea, in 2020, where she is currently pursuing the M.S. degree with the Department of Future Convergence Technology Engineering. Her current research interests include information security, wireless networks and communications, optical wireless communications, and artificial intelligence.

SOYOUNG JOO received the B.S. degree from the Department of Convergence Security Engineering, Sungshin Women’s University (SWU), in 2021, where she is currently pursuing the M.S. degree with the Department of Future Convergence Technology Engineering. Her current research interests include in the area of networks, security, and AI convergence technologies.

IL-GU LEE received the B.S. degree in electrical engineering from Sogang University, Seoul, South Korea, in 2003, the M.S. degree from the Department of Information and Communications Engineering, Korea Advanced Institute of Science and Technology (KAIST), Daejeon, South Korea, in 2005, and the Ph.D. degree from the Computer Science and Engineering Department, Graduate School of Information Security, KAIST, in 2016.

He is currently a Professor with the Department of Convergence Security Engineering, Sungshin Women’s University (SWU), Seoul. Before joining SWU in March 2017, he was with the Electronics and Telecommunications Research Institute (ETRI) as a Senior Researcher, from 2005 to 2017, and served as a Principal Architect and a Project Leader at Newratek (KR) and Newracom (USA), from 2014 to 2017. He has authored/coauthored more than 80 technical articles in the areas of information security, wireless networks, and communications, and holds about 160 patents. His current research interests include wireless/mobile networks, with an emphasis on information security, networks, wireless circuits, and systems.

Dr. Lee is an Active Participant and a Contributor to the IEEE 802.11 WLAN Standardization Committee.