electronics

MDPI

Article

Secrecy Enhancement for SSK-Based Visible Light Communication Systems

Wangzhaoqi Xie [1], Bao Li [2], Yuyang Peng [1,*], Han Zhu [1], Fawaz AL-Hazemi [3] and Mohammad Meraj Mirza [4]

[1] Faculty of Information Technology, Macau University of Science and Technology, Macau SAR, China; 1909853gii20009@student.must.edu.mo (W.X.); 19098533ii20001@student.must.edu.mo (H.Z.)
[2] School of Mechatronic Engineering, Changchun University of Technology, Changchun 130012, China; libao12356897@ccut.edu.cn
[3] Department of Computer and Network Engineering, University of Jeddah, Jeddah 21959, Saudi Arabia; fmalhazemi@uj.edu.sa
[4] Department of Computer Science, College of Computers and Information Technology, Taif University, P.O. Box 11099, Taif 21944, Saudi Arabia; mmmirza@tu.edu.sa
* Correspondence: yypeng@must.edu.mo

Abstract: Visible light communication (VLC) is a technology that uses unlicensed light spectrum resources and high spatial reuse rates for communication. Because it does not occupy any resource allocation in wireless communication, it has fully alleviated the problem of spectrum scarcity in radio frequency (RF) communication and gradually become a new development direction. However, owing to the inherent broadcasting nature of the VLC channel, the VLC link is vulnerable to eavesdropping by unexpected or unauthorized users in spacious public places. Therefore, enhancing the security of the VLC system has attracted extensive attention. This paper studies the security optimization scheme of the VLC system based on the space shift keying (SSK) technology in the free space optical environment called the SSK-VLC system. The antenna selection (AS) technology and artificial noise (AN) cancellation method are adopted to enhance the confidentiality of the SSK-VLC system. In this paper, we presume that the SSK-VLC system includes three parts: a transmitter containing multiple light-emitting diodes, a legitimate receiver, and an eavesdropper, respectively. By using the designed AS and AN method, the transmitted valid information can be demodulated at the legitimate receiver, and at the same time, the received information by the eavesdropper will be disturbed. The simulation results prove that the proposed optimization scheme can further improve the security performance, including the secrecy rate (SR) and the bit error ratio (BER), compared with the traditional SSK-VLC scheme.

Keywords: visible light communication; space shift keying; antenna selection; artificial noise; security performance

Citation: Xie, W.; Li, B.; Peng, Y.; Zhu, H.; AL-Hazemi, F.; Mirza, M.M. Secrecy Enhancement for SSK-Based Visible Light Communication Systems. *Electronics* **2022**, *11*, 1150. https://doi.org/10.3390/electronics11071150

Academic Editor: Paulo Monteiro

Received: 5 March 2022
Accepted: 29 March 2022
Published: 6 April 2022

1. Introduction

1.1. Background

With the rapid development of modern science and technology, the amount of new knowledge and information has increased, which makes the limited radio frequency (RF) spectrum resources even scarcer. Therefore, increasing the communication speed and spreading the communication spectrum has become an effective way to solve the problem. Meanwhile, the visible light communication (VLC) technology is discussed as the indoor access method of the fifth-generation mobile communication system, which has 400 THz available bandwidth and can greatly compensate for the spectrum resources [1]. Both VLC and RF communications use electromagnetic waves for wireless communications. However, compared to the existing RF communication technology, the VLC system can provide higher speeds. Because the VLC system works under the line-of-sight (LoS) environment between the source and receiver, there are certain advantages in preventing eavesdropping.

In addition, the VLC system can be used in electromagnetically sensitive areas and can also be deployed in the places where it is difficult to deploy optical fibers, such as operating rooms. In the VLC system, the transmitter loads the bit sequence that has carried information on the light-emitting diode (LED) by the drive circuit and uses the visible light band as a medium to transmit the information to the free space in the form of light intensity. At the receiver, the received optical signal is converted into an electrical signal by a photodetector (PD), and the original signal is recovered by demodulation and remapping [2]. Compared with RF channels, VLC has unique advantages such as rich spectrum resources, lighting, and communications functions. In addition, the VLC link provides better signal constraints and reduces the probability of interception caused by LoS propagation and the constraints of light waves on opaque surfaces. However, due to the inherent broadcast nature of the VLC channel, the transmitted information is vulnerable to eavesdropping by unintentional or unauthorized users [3], especially in physical areas where multiple users can access or share the transmitter's illumination, such as classrooms, meeting rooms, public libraries, airplanes, etc. Moreover, even if the eavesdroppers are not allowed to access the designated area, they can still intercept information through the structure of the physical environment, such as small gaps (keyholes) and transparent materials (windows). Therefore, the security of VLC is as important as the security of RF communication. The existing security technologies are mainly based on traditional upper-layer encryption, which requires complex algorithms to cope with the increase of mobile terminals. As mobile device's computing capability and cracking ability improve, the traditional complex algorithms will face severe challenges. Compared with the traditional upper-layer encryption security technology, physical layer security (PLS) can provide the first line of defense by using the wireless channel's uniqueness, difference, reciprocity, and other physical layer characteristics to ensure communication security. Therefore, the research on PLS for the VLC system has shown greater significance. The common PLS technologies of VLC mainly include precoding schemes, the antenna selection (AS) method, artificial noise (AN) technology, and the establishment of security protection areas, which can effectively improve the transmission security of information.

With the advent of the big data era, the use of conventional diversity technology and smart antenna technology can no longer meet communication requirements. The multiple-input multiple-output (MIMO) technology can greatly improve the space resource utilization of the system and increase the transmission rate and transmission capacity without increasing the system bandwidth. However, MIMO technology needs to achieve synchronization between the transmitters, which increases the cost of the actual system. Moreover, the transmitter transmits signals with the same frequency, which may easily cause channel interference. As the number of antennas increases, the system implementation's difficulty increases accordingly. However, limiting the number of deployed antennas will limit the advantages of the MIMO technique. Therefore, the spatial modulation (SM) technology based on MIMO technology was proposed in [4]. The core idea of SM is to transmit data by activating only one antenna at the transmitter in each time slot, which can effectively avoid channel interference and synchronization problems in the multi-antenna transceiver technology. VLC is a technology that combines lighting and communication, and it usually uses multiple LED light sources in an indoor lighting environment. The introduction of SM into the VLC system makes full use of the spatial dimensions provided by multiple LEDs to transmit information, which not only maintains the advantages of VLC, such as its low cost, no electromagnetic radiation, and high safety performance, but also further improves the spectrum utilization of the communication system.

1.2. Related Work

Some studies about VLC systems with MIMO or multiple-input single-output (MISO) channels have been investigated in [5–14]. In [5], Kumar et al. proposed an indoor communication scheme that combines VLC and RF at the same time to improve the confidentiality rate. In the indoor communication system, VLC technology is the main implementation

scheme, and RF technology is used to make up for the shortcomings of VLC technology in terms of the imposed limit of secrecy rate (SR). Then, a novel selection mechanism was proposed to make the best technical choice based on the knowledge of channel state information (CSI). The proposed system not only prevents eavesdropping attacks, but also reduces the security outage probability (SOP). In [6], the movements of users were considered in the systems and an optimization scheme about dynamically allocating power was proposed to boost the PLS of the VLC network, which is based on non-orthogonal multiple access (NOMA). In this work, multiple optical allocations were designed, and optimization theory is used to find the optimal solution to the power allocation and the joint secure communication issues. In [7], Su et al., designed a multi-dimensional lattice design technique for a multi-user generalized space shift keying system (MU-GSSK) to improve the PLS of the MIMO VLC communication system, which is used to serve the multi-user. With properly designed precoding of the transmitter, all available LEDs can be used simultaneously to transmit information to each user with higher spectral efficiency and without any multi-user interference (MUI). The MU-GSSK scheme generates friendly interference signals by randomly switching LEDs to prevent any meaningful confidential information from leaking to the eavesdropper. Therefore, bit error ratio (BER) performance of the multi-user is improved. However, this system requires high command LED array, appropriate beamforming technology, and perfect CSI. In [8], two methods were designed to improve the PLS of VLC systems under the condition that multiple illegal users try to eavesdrop the legitimate users. Both methods are used to optimize the total transmitted power of senders such that the PLS could be improved. When the CSI of illegal users can not be known to the sender of systems, the power saving problem can be solved by letting the AN reside in the null space of channel of the legitimate user. Then, when the CSI is available, the author proposed two approaches named as concave convex procedure (CCP) and semidefinite relaxation (SDR) to find the suboptimal solutions of the non-convex power saving problem. In [9], Qian et al. combined the intelligent reflecting surfaces (IRS) technique with the single-input single-output (SISO)-VLC systems. First, the authors derived the lower bound of SR and the channel gain of IRS. Then, in order to find the optimal orientations of mirrors, the authors solved the optimization problem to enhance the IRS channel gain of the legitimate user while the IRS channel gain of the illegal user can be constrained by a particle swarm optimization (PSO) algorithm. Since the optimal orientations have been chosen to aid the VLC systems, the SR performance of the system can be enhanced by enlarging the difference of channel gain between a legitimate user and an illegal user. In [10], Ma et al. designed beam formers to improve the secrecy of MISO-VLC systems when the CSI between transmitter and eavesdropper is known. Moreover, the authors further expanded the scope of application of these beam formers by using imperfect CSI knowledge. When the wiretap CSI is perfect, the design of optimal safe beamforming is used. When the wiretap CSI is not perfect, the design of robust beamforming is used. In [11], Xiao et al. combined the reinforcement learning (RL) technique with the VLC systems based on the MISO scenario. Based on the MISO-VLC system, an RL-based intelligent beamforming framework and RL-based MISO-VLC beamforming algorithm were proposed. The optimal beamforming strategy could be realized after a sufficient number of learning iterations. The utility and confidentiality of the MISO- VLC system were further improved. Compared with the existing benchmarks, the BER of the legal receiver was significantly reduced. In [12], compared with the traditional zero-forcing precoding scheme, Arfaoui et al., proposed a new precoding strategy to boost the PLS performance of the MISO-VLC systems which serves the multi-user. However, the complexity of the proposed scheme was increased. The trade-off between the PLS performance and complexity of the proposed scheme can be further optimized. In [13], the SR performance of MIMO-VLC systems was studied under the wiretap channel. Arfaoui et al. proposed a low complexity precoding strategy which is based on the generalized singular value decomposition of the main channel to enhance the PLS of the systems. In [14], Chaaban et al. considered friendly

jamming to enhance the SR performance of the MISO-VLC system. The friendly jamming can cause interference to illegal users while it can be eliminated at the legitimate receiver.

However, the above papers have not fully considered the PLS of VLC based on the space shift keying (SSK) system. SSK modulation is a special mode of SM. Since it does not use the traditional digital baseband modulation technology, it has the advantages of low hardware cost and low detection complexity while ensuring system reliability. As in RF communication, the concept of SSK can also be applied in the VLC area by using the appropriate channel model and transmitter, such as LED. Applying SSK modulation technology to the VLC system has become an effective way to improve the system's ability to transmit data. In order to further reduce the complexity of the modulation and demodulation process, Jeganathan et al. proposed a simplified version of SM called SSK in [15], which only uses the spatial dimension to transmit information. This modulation scheme activates only one transmitting antenna to represent information at each transmission time, and other transmitting antennas do not work. In [16], to improve the data transmission rate, Bao et al., proposed a new generalized SM scheme based on the indoor VLC system. In [17], Wang et al., used the minimax criterion to select LEDs of GSSK-VLC systems for optical communication. Experiments showed that the average mutual information (AMI) between Bob and Eve can be further improved. Thus, the PLS security of SSK-VLC systems should be considered. In [5], two techniques were introduced to improve the PLS of VLC systems which use GSSK modulation. In the first technique, the authors applied the spatial constellation design (SCD) to boost the BER performance of Bob and reduce the BER performance of Eve. For the second technique, the authors combined the appropriate beamforming vectors at the relay with NOMA to enhance the PLS of the VLC system. In [18], Ben et al. considered the AN to enhance the PLS performance of the indoor MISO VLC system and derived the upper bound and the lower bound of SR. In the system, the minimum mean squared error (MMSE) equalizer is adapted to detect the receiving signals from the multi-user. Compared with the systems without AN, the SR performance can be improved with the help of the AN. Then, the SR performance is further improved by setting the appropriate power of AN. In [19], an optical jamming strategy was proposed to enhance the PLS for GSSK-VLC systems. In the system, the sender is designed to transmit the effective signal alone with the optical jamming which obeys the appropriate power constraint. Results showed that the PLS of the system can be enhanced in terms of achievable SR. However, the impact of atmospheric turbulence on VLC is not considered.

The atmospheric turbulence effect leads to the random fluctuation of the wavefront of the transmitted beam, resulting in spot drift and intensity fluctuation (flicker), which seriously reduces the quality of the transmitted beam. It further reduces the system performance of the free space optical communication system, such as increasing the BER, reducing the channel capacity, and increasing the interrupting probability. Therefore, it seriously affects the stability and reliability of the communication system. In order to find the influence of atmospheric turbulence on free space optical communication, researchers have proposed various atmospheric turbulence channel models, such as the lognormal distribution, the K-distributed turbulence, the exponential distribution, the I-K distribution, the Gamma-Gamma distribution, etc. Among these atmospheric turbulence channel models, the lognormal model is suitable for weak turbulence conditions, which can satisfy the smaller refractive index structure constant and other beam parameters. In [20], Kiasaleh et al. studied the performance of free space optical communication, which was based on differential phase shift keying (DPSK) modulation by using the K-distribution model. The K-distribution is suitable for medium distance propagation (close to 1 km). Specifically, when the scintillation index is in the range of (2, 3), the K-distribution is a reliable atmospheric turbulence model. In [21], Popoola et al. used the exponential distribution model to study the performance of free space optical communication. In [22], the Gamma-Gamma distribution model with actual test data for medium-strong turbulence was used to study the coding error rate of the free space VLC system. In [23], the error rate of the free space optical communication system was analyzed. In [24], Gappmair et al.,

used pulse position modulation to analyze the free space VLC system performance. In [25], the closed average channel capacity and expression of interrupting probability of the free space VLC system were derived. In the case of medium-strong turbulence, the Gamma-Gamma distribution model is consistent with the actual test data. To the best of our knowledge, there is no work considering SSK technology by considering Gamma-Gamma distribution model in the VLC system for single-user secure communication.

1.3. Contribution

Based on the above analysis, a VLC system based on SSK technology was established. In the proposed system, the transmitter is equipped with multiple LEDs for wireless data transmission, and a legitimate receiver is equipped with single antenna for receiving data. In addition, there is an eavesdropper equipped with one antenna to eavesdrop the information data. In the system, AS technology and the AN elimination method are used to enhance the SR and BER performances of the SSK-VLC system. The BER and the SR results prove that the proposed scheme can improve the security performance compared with the traditional SSK-VLC scheme.

The rest of the paper is organized as follows. In Section 2, the system model of the scheme is introduced. In Section 3, the design method is described. Section 4 introduces the system analysis and the simulation results. Finally, the conclusion is given in Section 5.

2. System Model

SSK is a relatively simple modulation method in SM technology [26,27]. Because there are many similarities between VLC technology and RF communication, some modulation technologies in RF communication can also be applied to VLC. In this paper, SSK modulation technology is used for modulation and LED is used as antenna. There is only modulation in the spatial domain and no modulation in the signal domain in SSK modulation. In any transmission time slot, only one LED index conveys bit information, and the light intensity of the transmitted signal is fixed and does not carry bit information. It can effectively use the spatial domain and improve system performance. As shown in Figure 1, the system contains a signal transmitter named Alice, a legitimate receiver named Bob of the SSK system, and an eavesdropper named Eve. The transmitter Alice is configured with N_a LEDs and Bob as a legitimate receiver with a PD in the system model. In addition, Eve works as an eavesdropper in this system. The CSI of the legitimate channel is assumed to be perfectly known.

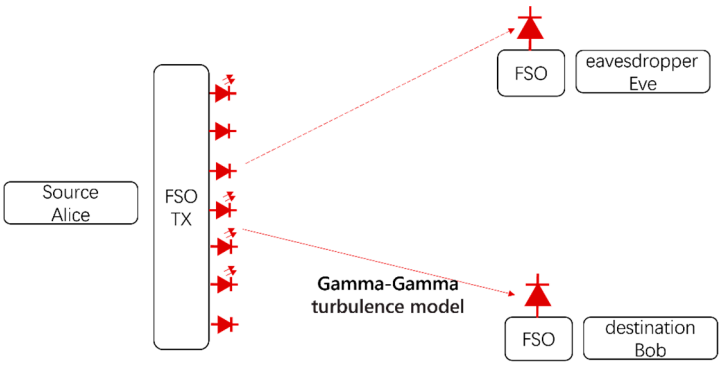

Figure 1. System model of SSK-VLC channel.

In the system, the antenna of the transmitter Alice consists of two parts. One part consists of N_t antennas selected from the N_a antennas to perform the SSK function. The reason of selection is that the number of transmit antennas N_a usually is not the power of 2, which cannot meet the SSK mechanism. Therefore, to meet the requirements of SSK transmission, the N_t antennas from the N_a antennas are selected where N_t is the power of 2. Among N_t antennas, one antenna is selected as the active antenna to convey the information through

the antenna index and transmit the first designed AN. At the same time, the other part of $N_a - N_t$ antennas choose one antenna to send the second designed AN.

The value of selecting the combination of N_t antennas from N_a antennas is $P = \begin{pmatrix} N_a \\ N_t \end{pmatrix}$. In each time slot, the transmitter Alice selects one of the P combinations as the first part of the antenna [28]. Therefore, the transmitted signal vector from the transmitter Alice can be represented by:

$$x(k) = e_j = [0 \cdots \underset{j\text{-th}}{0} \cdots 1 \cdots 0 \cdots 0]^T \tag{1}$$

The VLC channel gain is determined by the transmit LED and the location of the receiving PD. In order to adjust the illumination level of the LED, the identical bias current is used to drive the emission LED [17], which is represented by $I_{DC} \in R^+$. To ensure safety, keep linear current conversion, save power, and avoiding clip distortion, the total current of $I_{DC} + x(k)$ was restricted to the range of $[(1-\alpha)I_{DC}, (1+\alpha)I_{DC}]$, with $\alpha \in [0, 1]$ [17]. Additionally, assume that all LEDs and PDs have the same parameter. The instantaneous intensity can be modeled after electro-optic conversion as $P_T(k) = \eta[I_{DC} + x(k)]$, where η denotes the LEDs' current-to-light conversion efficiency. The optical power received by the legitimate receiver from the first LED can be expressed as $P_R(k) = GP_T(k)$, where G denotes the path gain between the first LED and the receiver. The path gain G is represented when the broad Lambertian emission mode is considered, as shown in [3]. When the generalized Lambertian emission pattern is considered, the path gain G can be represented by:

$$G = \begin{cases} \frac{1}{2\pi d^2}(m+1)A_R cos^m(\phi)cos\psi, & |\psi| \le \psi_{FoV} \\ 0, & |\psi| > \psi_{FoV} \end{cases} \tag{2}$$

where d denotes the LoS distance between the receiver's PD and the LED, A_R means the effective detection area of the PD, and ϕ means the angle of irradiance from the LED. All LED antennas are assumed to have same irradiance. Referring to (2), ψ is the angle of incidence of the i-th optical link, $m = -1/\log_2(cos\phi_{1/2})$ is the Lambertian emission order, with $\phi_{1/2}$ denoting the half irradiance angle, and ψ_{FoV} denoting the receiver' field-of-view (FoV) semi-angle. Based on [17], the detection area of the PD can be represented by:

$$A_R = \frac{\beta^2}{sin^2(\psi_{FoV})} A_{PD}, \tag{3}$$

where A_{PD} represents the PDs' area and β is the refractive index of the optical concentrator. Given the response R for the PD, the incident light power is converted into a current of $P_R(k)$. After removing the direct current (DC) bias I_{DC} in $x(k)$ contaminated by the noise, a transimpedance amplifier with a gain of T amplifies the received signal to produce a voltage of $q(k) \in R$, which is scaled by the combination of the transmitted signals. In other words, when the j-th LED lamp is activated to send a signal, the input-output relationship of the VLC channel between the N_t LEDs and a PD can be modeled as:

$$q(k) = h\, x(k) + w(k),\ k = 1, 2, \ldots \tag{4}$$

where $h = TRG\eta$ denotes the channel gain and $w(k) \sim N\left(0, \sigma^2\right)$ indicates the Gaussian noise. The three components of noise are weighted, including the shot noise, thermal noise, and intensity-dependent noise caused by the ambient light. The additive white Gaussian noise (AWGN) with zero mean can be used to model the sum of these noise components [29].

According to the above assumptions and relying on the VLC channel model of Equation (4), the received signals of the legitimate receiver and the eavesdropper can be represented as:

$$y(k) = \boldsymbol{h_B} x(k) + w_B(k), \tag{5}$$

$$z(k) = \boldsymbol{h_E} x(k) + w_E(k), \tag{6}$$

where $\boldsymbol{h_E}$ and $\boldsymbol{h_B}$ are the Gamma-Gamma fading channels from Alice to Eve and Alice to Bob, respectively. After applying AS technology, the received signals can be re-expressed as:

$$y(k) = \boldsymbol{h}_B \boldsymbol{T}_k x(k) + w_B(k), \tag{7}$$

$$z(k) = \boldsymbol{h}_E \boldsymbol{T}_k x(k) + w_E(k), \tag{8}$$

where $\boldsymbol{T}_k$ is the N_t columns of identity matrix $\boldsymbol{I}_{N_a}$ which means the selected matrix of effective transmit antenna for $k \in \{1, 2, \ldots, P\}$. If we jointly consider AS and designed AN, and assume the eavesdropper knows nothing about the knowledge of the legal channel, it is difficult for Eve to eliminate the designed AN. Therefore, any vector of $\boldsymbol{h}_B$ cannot be represented by $\boldsymbol{h}_E$, and the received signals at Bob and Eve can be respectively represented as:

$$y(k) = \boldsymbol{h}_B \boldsymbol{T}_k x(k)(1 + \alpha_1 v) + \boldsymbol{h}_B \boldsymbol{T}_q x(k)(\alpha_2 v) + w_B(k), \tag{9}$$

$$z(k) = \boldsymbol{h}_E \boldsymbol{T}_k x(k)(1 + \alpha_1 v) + \boldsymbol{h}_E \boldsymbol{T}_q x(k)(\alpha_2 v) + w_E(k), \tag{10}$$

where $\boldsymbol{T}_q$ is a single column matrix selected from submatrix $\boldsymbol{I'}_{N_a}$, which means the selected matrix of the effective transmit antenna for $q \in \{1, 2, \ldots, N_a - N_t\}$. After adding the designed AN and AS, the signal received by Bob and Eve can be expressed as:

$$\begin{aligned} y_b &= h_{Bj}(1 + \alpha_1 v) + h_{Bi}(\alpha_2 v) + w_B(k) \\ &= h_{Bj} + h_{Bj}\, \alpha_1 v + h_{Bi} \alpha_2 v + w_B(k), \end{aligned} \tag{11}$$

$$\begin{aligned} y_e &= h_{Ej}(1 + \alpha_1 v) + h_{Ei}(\alpha_2 v) + w_E(k) \\ &= h_{Ej} + h_{Ej}\, \alpha_1 v + h_{Ei} \alpha_2 v + w_E(k), \end{aligned} \tag{12}$$

where h_{Bj} is the j-th entry of $\boldsymbol{h}_B$ and h_{Ej} is the j-th entry of $\boldsymbol{h}_E$, h_{Bi} is the i-th entry of $\boldsymbol{h}_B$, h_{Ei} is the i-th entry of $\boldsymbol{h}_E$, v denotes the complex Gaussian AN with zero mean and variance (value is less than 1), and α_1 and α_2 are the designed parameters for processing AN.

2.1. Attenuation Model of Atmospheric Turbulence Channel

When the beam spreads in the atmosphere, it is highly susceptible to atmospheric turbulence, which causes the decline of beam propagation quality, spot drift, and light intensity fluctuation, increases the error rate of VLC in free space, and affects the stability and reliability of VLC. As a result of the refractive index fluctuation, the strength of the light wave fluctuates when it transmits in atmospheric turbulence. In order to evaluate the effectiveness of corresponding countermeasures and assess the influence of atmospheric turbulence, it is important to model the fading distribution accurately. The lognormal distribution is usually used to simulate weak turbulence conditions, and the K-distribution is suitable for medium distance propagation. But the Gamma-Gamma distribution model is chosen to model the signal attenuation. The reason is that the Gamma-Gamma fading model is very consistent with the measured data of various turbulence conditions from weak to strong.

The Gamma-Gamma fading model is one of the commonly used turbulence channel models, which can mathematically express the intensity and phase fluctuation of received signals. The probability density function (PDF) of the Gamma-Gamma fading model is given as:

$$p(h) = \frac{2(ab)^{\frac{a+b}{2}}}{\Gamma(a)\Gamma(b)} h^{\frac{a+b}{2}-1} K_{a-b}\left(2\sqrt{abh}\right),\ h > 0 \tag{13}$$

where a and b respectively denote the small-scale and large-scale atmospheric turbulence coefficients, $\Gamma(\cdot)$ represents the Gamma function, and $K_n(\cdot)$ stands for the modified Bessel

function of the second kind of the n-th order. In the plane wave case, the a and the b are respectively represented as:

$$a = \left\{ exp\left[\frac{0.49\sigma^2}{\left(1 + 1.11\sigma^{\frac{12}{5}}\right)^{\frac{7}{6}}} \right] - 1 \right\}^{-1}, \tag{14}$$

$$b = \left\{ exp\left[\frac{0.51\sigma^2}{\left(1 + 0.69\sigma^{\frac{12}{5}}\right)^{\frac{5}{6}}} \right] - 1 \right\}^{-1}, \tag{15}$$

where $\sigma^2 = 1.23 C_n^2 k^{\frac{7}{6}} L^{\frac{11}{6}}$ as Rytov variance with k is the wavenumber, L is the transmission distance, and C_n^2 is the atmospheric refractive index structure constant. The a and b are the order of the modified Bessel function of the second kind. Only in the case of plane waves can a and b be expressed as Equations (14) and (15). These two parameters affect the number of large-scale and small-scale turbulent vortices in the atmosphere, thus affecting the light intensity and optical communication quality.

2.2. Artificial Noise Cancellation

The AN is designed by using the main CSI. The interference signal only acts on the eavesdropper for obtaining effective security capacity. Its basic idea is to interfere with the eavesdropper's reception by sending specific AN without affecting the legitimate receiver as much as possible. To improve the system's security performance, AN cannot affect the confidentiality of the legitimate receiver Bob. Specifically, since the CSI of the eavesdropping channel and the legal channel are independent, the interference of legal receiver Bob can be eliminated when the eavesdropper Eve interference is retained. So, when AN at Bob is eliminated, the interference term of Bob is zero, which can be expressed as:

$$h_{Bj}\, \alpha_1 v + h_{Bi} \alpha_2 v = 0. \tag{16}$$

The eavesdropper should suffer the interference after disturbing and this interference should not be eliminated. Therefore, the interference term of the eavesdropper Eve should not be zero, which means:

$$h_{Ej}\, \alpha_1 v + h_{Ei} \alpha_2 v \neq 0\,, \tag{17}$$

where the parameters α_1 and α_2 should be set as:

$$\begin{cases} \alpha_1 = h_{Bi} \\ \alpha_2 = -h_{Bj} \end{cases} or \begin{cases} \alpha_1 = -h_{Bi} \\ \alpha_2 = h_{Bj} \end{cases}. \tag{18}$$

When $h_{Ej} \neq h_{Bj}$ and $h_{Ei} \neq h_{Bi}$, Equations (16) and (17) can be guaranteed. In other words, the eavesdropper receives AN, but Bob's AN is eliminated.

2.3. Antenna Selection

In recent years, some scholars have begun to consider using legitimate user AS to improve the safe interrupting capacity of the system [30]. By selecting some antennas from all antennas for signal processing, AS technology can obtain system performance while saving hardware costs and reducing system complexity. We consider both the legal channel and the eavesdropping channel and design AS and AN together, which can improve the channel capacity of the legal user and reduce the channel capacity of eavesdropping to increase the security capacity of the legal channel significantly. In this part, the selection of antenna and the standard of AS are discussed. The power of the received signal at the legitimate receiver is $||\boldsymbol{h}_B \boldsymbol{T}_k x(k)||^2$ and $||\boldsymbol{h}_E \boldsymbol{T}_k x(k)||^2$ is the power of the received signal at the eavesdropper. To ensure the communication performance of Bob, $||\boldsymbol{h}_B \boldsymbol{T}_k x(k)||^2$

demands to be larger than $||\boldsymbol{h}_E \boldsymbol{T}_k x(k)||^2 + \sigma^2$ with σ^2 being AWGN power. In order to achieve the above requirement, the signal to leakage noise ratio (SLNR) for the j-th channel in the k-th combination is expressed as:

$$\varphi_j(\boldsymbol{T}_k) = \frac{||\boldsymbol{h}_B \boldsymbol{T}_k x(k)||^2}{||\boldsymbol{h}_E \boldsymbol{T}_k x(k)||^2 + \sigma^2}. \tag{19}$$

The purpose is to select the optimal $\boldsymbol{T}_k$ value by the maximum SLNR value. If all transmit antennas are assumed to be irrelevant, the SLNR of each transmit antenna is different and can be represented as:

$$\varphi_l = \frac{||h_{Bl}||^2}{||h_{El}||^2 + \sigma^2}\,, \tag{20}$$

where h_{Bl} and h_{El} is the l-th column of the channel $\boldsymbol{h}_B$ and $\boldsymbol{h}_E$ with l being the index of the selected antenna ($l \in \{1, 2, \ldots, N_a\}$). After calculating the SLNR values of all transmitter antennas, the SLNR values are arranged in a descending order as follows:

$$\varphi_{\pi_1} \geq \varphi_{\pi_2} \geq \cdots \geq \varphi_{\pi_{N_t}} \geq \cdots \geq \varphi_{\pi_{N_a}}\,, \tag{21}$$

where $\{\pi_1, \pi_2, \cdots, \pi_{N_a}\}$ is an ordered permutation set of $\{1, 2, \cdots, N_a\}$. Therefore, the best condition is to select the first N_t SLNR values from Equation (21). Based on the selected SLNR, the corresponding N_t antenna can be obtained. The larger the SLNR value, the more significant the difference between the eavesdropping channel and the legitimate channel. Compared with the non-antenna selection scheme, the system performance is improved. The complexity of the method based on SLNR is divided into two parts. The first part of the operation is to calculate the N_t SLNR values, and the second part is the sorting operation [31]. Therefore, the complexity of the AS method based on SLNR can be expressed as $O(N_a) + O(N_a \log_2 N_a) \approx O(N_a \log_2 N_a)$.

3. SSK-VLC System Analysis

This section discusses the SR performance of the VLC-SSK scheme. The scheme eliminates the AN at the legitimate receiver and retains the AN for the eavesdropper. Therefore, the signals received at the legitimate receiver Bob and the eavesdropper Eve are expressed as:

$$y_b = h_{Bj} + w_B(k)\,, \tag{22}$$

and

$$\begin{aligned} y_e &= h_{Ej}(1 + \alpha_1 v) + h_{Ei}(\alpha_2 v) + w_E(k) \\ &= h_{Ej} + h_{Ej}\,\alpha_1 v + h_{Ei}\alpha_2 v + w_E(k). \end{aligned} \tag{23}$$

After the AS, the probability of choosing an antenna from N_t antennas equal $1/\ N_t$, so the likelihood of receiving the signal follows complex Gaussian distribution at the legitimate receiver Bob, which can be expressed as:

$$P(y_b|h_{Bj}) = \frac{1}{\pi\sigma^2} exp\left(-\frac{|y_b - h_{Bj}|^2}{\sigma^2}\right), \tag{24}$$

$$P(y_b) = \frac{1}{N_t}\sum_{j=1}^{N_t} \frac{1}{\pi\sigma^2} exp\left(-\frac{|y_b - h_{Bj}|^2}{\sigma^2}\right). \tag{25}$$

Between Alice and Bob, the mutual information can be represented by:

$$\begin{aligned} I(y_b;h_{Bj}) &= \int \sum_{j=1}^{N_t} P(y_b,h_{Bj}) \log_2 \frac{P(y_b,h_{Bj})}{P(y_b)P(h_{Bj})} dy_b \\ &= \tfrac{1}{N_t} \int \sum_{j=1}^{N_t} P(y_b|h_{Bj}) \log_2 \frac{P(y_b|h_{Bj})}{P(y_b)} dy_b \\ = \tfrac{1}{N_t} \int \sum_{j=1}^{N_t} \tfrac{1}{\pi\sigma^2} exp\left(-\tfrac{|y_b-h_{Bj}|^2}{\sigma^2}\right) &\times \log_2 \frac{\tfrac{1}{\pi\sigma^2} exp\left(-\tfrac{|y_b-h_{Bj}|^2}{\sigma^2}\right)}{\tfrac{1}{N_t}\sum_{j'=1}^{N_t} \tfrac{1}{\pi\sigma^2} exp\left(-\tfrac{|y_b-h_{Bj}|^2}{\sigma^2}\right)} dy_b \\ = \log_2 N_t - \tfrac{1}{N_t} \sum_{j=1}^{N_t} E_{w_B(k)} &\left[\log_2 \left(\sum_{j'=1}^{N_t} exp\left(-\frac{|h_{Bj}-h_{Bj'}+w_B(k)|^2 - |w_B(k)|^2}{\sigma^2} \right) \right) \right]. \end{aligned} \tag{26}$$

According to Equation (23), including two designed ANs at Eve and AWGN, the noise part is represented as:

$$w'_E(k) = +h_{Ej}\,\alpha_1 v + h_{Ei}\alpha_2 v + w_E(k). \tag{27}$$

In the design, both the AN and the AWGN follow the complex Gaussian distribution; therefore, $w'_E(k)$ is Gaussian colored noise, and its variance can be represented by:

$$W_e = E\left[w'_E(k)\left(w'_E(k)\right)^H\right]. \tag{28}$$

In order to calculate the mutual information of the eavesdropper Eve, the necessity for linear whitening transform function Q multiplying the received signal of the eavesdropper is recognized, which is expressed as:

$$Q = \sigma W_e^{-1/2}. \tag{29}$$

According to Equations (23), (27) and (29), the received signal at the eavesdropper Eve can be represented by:

$$y'_e = Q_{\boldsymbol{h}_{Ej}} + Q_{w'_E(k)} = \overline{h}_{Ej} + \overline{w}_E(k). \tag{30}$$

The transform function's purpose is to make the noise distribution of the eavesdropper Eve's ANs and AWGN obey the Gaussian distribution with zero mean and variance σ^2. Consequently, the overall received signal follows the complex Gaussian distribution, which can be shown as:

$$P\left(y_e\middle|\overline{h}_{Ej}\right) = \frac{1}{\pi\sigma^2} exp\left(-\frac{\left|y'_e-\overline{h}_{Ej}\right|^2}{\sigma^2}\right). \tag{31}$$

After taking into consideration the probability of selecting the specific antenna, (31) is derived as:

$$P(y'_e) = \frac{1}{N_t}\sum_{j=1}^{N_t} \frac{1}{\pi\sigma^2} exp\left(-\frac{\left|y_e-\overline{h}_{Ej}\right|^2}{\sigma^2}\right). \tag{32}$$

The mutual information between the transmitter Alice and the eavesdropper Eve can be expressed as:

$$\begin{aligned} &I(y_e;h_{Ej}) = I\left(y'_e;\overline{h}_{Ej}\right) \\ &= \log_2 N_t - \tfrac{1}{N_t}\sum_{j=1}^{N_t} E_{\overline{w_E(k)}} \left[\log_2 \left(\sum_{j'=1}^{N_t} exp\left(-\frac{\left|Q\left(h_{Ej}-h_{Ej'}\right)+\overline{w_E(k)}\right|^2 - \left|\overline{w_E(k)}\right|^2}{\sigma^2} \right) \right) \right]. \end{aligned} \tag{33}$$

The mutual information expression of the wiretap channel and the legitimate channel is known, and the calculation formula of SR is [32]:

$$R_s = max\{0, I(y_b; h_{Bj}) - I(y_e; h_{Ej})\}. \quad (34)$$

where $I(y_b; h_{Bj})$ and $I(y_e; h_{Ej})$ can be expressed as Equations (35) and (36) according to (24):

$$I(y_b; h_{Bj}) = H(y_b) - H(y_b|h_{Bj}), \quad (35)$$

$$I(y_e; h_{Ej}) = H(y_e) - H(y_e|h_{Ej}), \quad (36)$$

where $H(\cdot)$ is the entropy of the discrete random variable. The optimal antenna is selected to indicate the valid signal and transmit the AN. The absolute value difference of the CSI coefficient is more significant than the absolute value difference of the scheme without AS between the wiretap channel and legitimate channel. Obviously, the AS scheme can improve the security of VLC.

4. Analytical and Simulation Results

To evaluate the performance of the proposed VLC-SSK system, the simulation is carried out in MATLAB. In the simulation, a quasi-stationary flat-fading channel is assumed with the equal probability distribution of input bits and AWGN. To better evaluate the performance of the proposed VLC-SSK system, the results of the SR and the BER values under different SNR variables are shown in Figures 2–6. In these figures, the proposed AS scheme is called the SLNR scheme, and the existing scheme is called the random selection scheme.

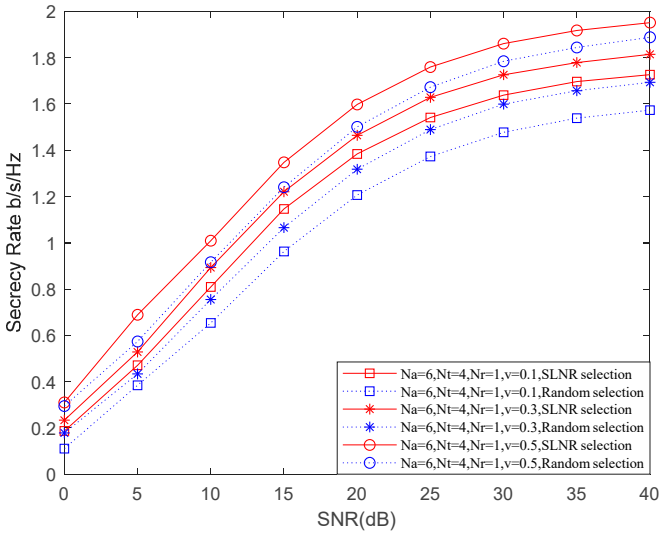

Figure 2. SR over SNR under different schemes for different v.

Figure 2 shows the relation between the SR value and the SNR value for different schemes under v values (v = 0.1, 0.3, and 0.5). In the simulation, $N_r = 1$ at the receiver, $N_a = 6$, and $N_t = 4$ at transmitter are assumed. The SR values of all the schemes increase as the SNR values increase. In addition, as the v value increases, the SR values of all the schemes increase because as the v value increases, the interference of AN on the eavesdropper also increases, which leads to higher SR. Furthermore, the SR values of SLNR schemes outperform the SR values of random selection schemes. Figure 3 shows the relation between the SR value and the SNR value for different schemes under different (N_a, N_t) situations. Specifically, (5, 2), (6, 4), and (10, 8) pairs are considered. In Figure 3, SR values of all schemes increase with the increase of SNR value and tend toward the saturation point. Among all the different (N_a, N_t) situations, the schemes with the (10, 8) pair achieve the best SR performance. Figure 4 shows the relation between the BER values

and the SNR values of Bob and Eve for different schemes under the (6, 4) pair situation. As shown in the figure, the BER values of all the schemes decrease as the SNR values increase and the BER values of Bob are lower than the BER values of Eve in all the schemes. In addition, the BER value of Bob in the SLNR scheme is lower than the BER value of Bob in the random selection scheme while the BER values of Eve in all the SLNR and random selection schemes are similar. Therefore, it can be concluded that the BER performance of the SLNR scheme is better than the one of the random selection scheme. Figure 5 shows the relation between the BER values and the SNR values of Bob and Eve for the SLNR scheme under the (6, 4) pair situation and different v values (v = 0.3, 0.5, and 0.8). As shown in the figure, the BER values of all situations decrease as the SNR values increase and the BER values of Bob are lower than the BER values of Eve in all situations. In addition, as the v value increases, the BER value of Bob decreases and the BER value of Eve increases. Therefore, we can conclude that the bigger v value can bring the better performance for the proposed scheme. Therefore, a higher v value can be set to decrease the BER of Bob and increase the BER of Eve to improve the security performance of the system. Figure 6 shows the relation between the BER values and SNR values of Bob and Eve for different schemes under different (N_a, N_t) situations. As shown in the figure, the BER values of all schemes in all situations decrease as the SNR values increase and the BER values of Bob are lower than the BER values of Eve in all schemes in all situations. In addition, among all the different (N_a, N_t) situations, the schemes with the (5, 2) pair achieve the lowest values of BER for Bob and Eve.

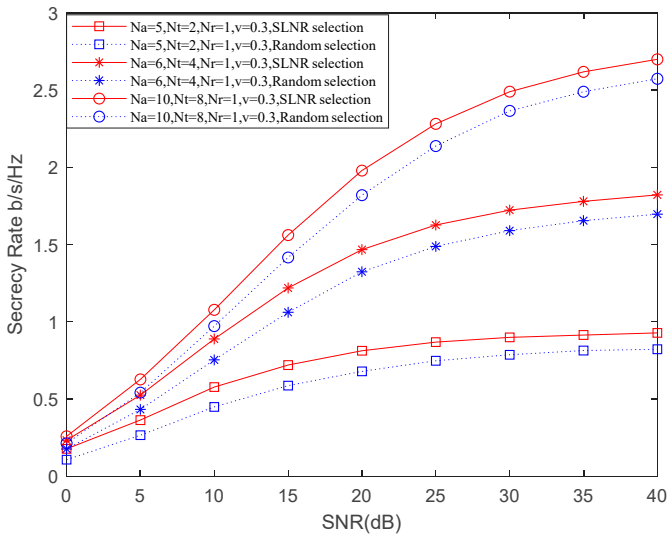

Figure 3. SR over SNR under different schemes for different N_a and N_t.

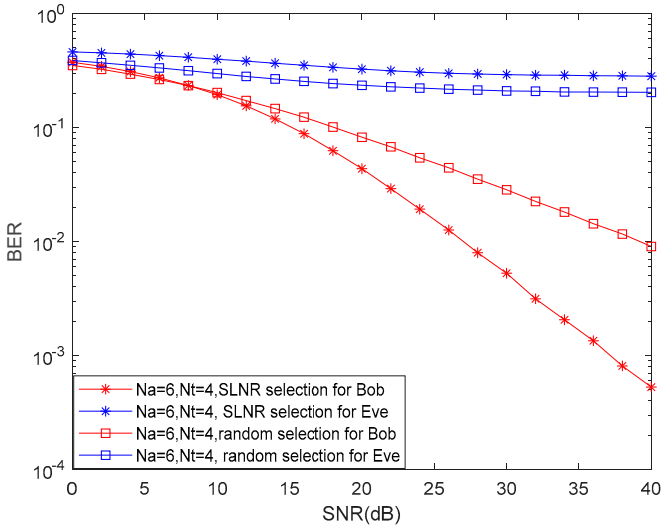

Figure 4. BER over SNR under different schemes for different schemes.

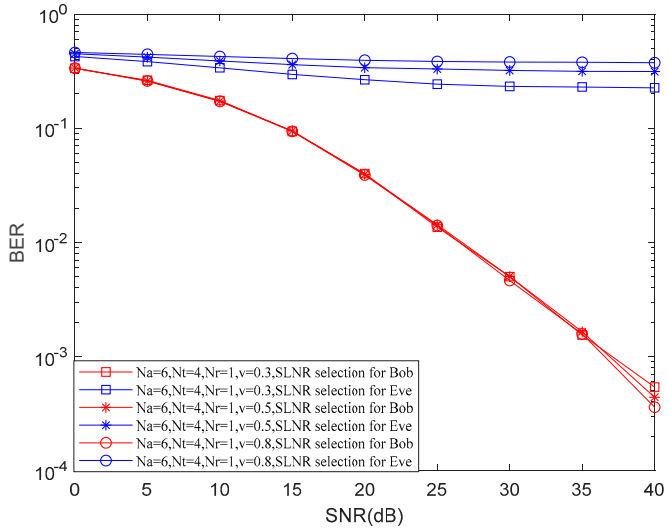

Figure 5. BER over SNR under different schemes for different v.

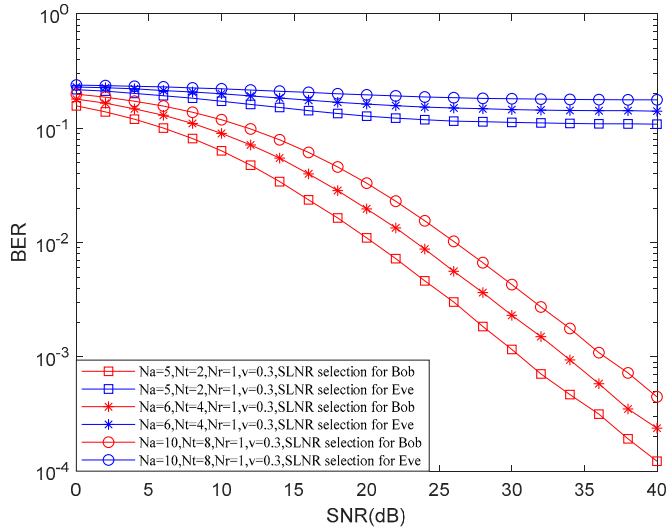

Figure 6. BER over SNR under different schemes for different N_a and N_t.

5. Conclusions

In this paper, a security enhancement scheme of the SSK system for VLC is proposed. In the proposed scheme, AS and AN technologies have been applied to the SSK system for VLC to improve the security performance of the system. Compared with the scheme without AS technology and AN cancellation method, the security performance of the system is proven. In the AN cancellation method, appropriate parameters are designed to eliminate the legitimate receiver's interference and maintain with the eavesdropper. In the AS, the antenna is selected according to the SLNR values for improving the system performance. The simulation results show that the security performance of the proposed SR enhancement scheme is better than the random selection scheme.

Author Contributions: Conceptualization, W.X. and Y.P.; methodology, W.X.; validation, W.X.; formal analysis, W.X. and H.Z.; investigation, W.X.; writing—original draft preparation, W.X. and Y.P.; writing—review and editing, W.X., B.L. and Y.P.; visualization, H.Z.; supervision, Y.P.; project administration, Y.P.; funding acquisition, Y.P., F.A.-H. and M.M.M. All authors have read and agreed to the published version of the manuscript.

Funding: This work is supported in part by The Science and Technology Development Fund, Macau SAR (0108/2020/A3), in part by The Science and Technology Development Fund, Macau SAR (0005/2021/ITP), and in part by Taif University Researchers Supporting Project number (TURSP-2020/329), Taif University, Taif, Saudi Arabia.

Acknowledgments: The authors are grateful for the support of Taif University Researchers Supporting Project number (TURSP-2020/329) Taif University, Taif, Saudi Arabia.

Conflicts of Interest: The authors declare that there are no conflict of interest regarding the publication of this paper.

References

1. Yucek, T.; Arslan, H. A survey of spectrum sensing algorithms for cognitive radio applications. *IEEE Commun. Surv. Tutorial* **2009**, *11*, 116–130. [CrossRef]
2. Karunatilaka, D.; Zafar, F.; Kalavally, V.; Parthiban, R. LED Based Indoor Visible Light Communications: State of the Art. *IEEE Commun. Surv. Tutorials* **2015**, *17*, 1649–1678. [CrossRef]
3. Mostafa, A.; Lampe, L. Physical-Layer Security for MISO Visible Light Communication Channels. *IEEE J. Sel. Areas Commun.* **2015**, *33*, 1806–1818. [CrossRef]
4. Mesleh, R.Y.; Haas, H.; Sinanovic, S.; Ahn, C.W.; Yun, S. Spatial Modulation. *IEEE Trans. Veh. Technol.* **2008**, *57*, 2228–2241. [CrossRef]
5. Kumar, A.; Garg, P.; Gupta, A. PLS Analysis in an Indoor Heterogeneous VLC/RF Network Based on Known and Unknown CSI. *IEEE Syst. J.* **2021**, *15*, 68–76. [CrossRef]
6. Zhao, X.; Sun, J. Physical-Layer Security for Mobile Users in NOMA-Enabled Visible Light Communication Networks. *IEEE Access* **2020**, *8*, 205411–205423. [CrossRef]
7. Su, N.; Panayirci, E.; Koca, M.; Yesilkaya, A.; Poor, H.V.; Haas, H. Physical Layer Security for Multi-User MIMO Visible Light Communication Systems With Generalized Space Shift Keying. *IEEE Trans. Commun.* **2021**, *69*, 2585–2598. [CrossRef]
8. Pham, T.V.; Pham, A.T. Energy Efficient Artificial Noise-Aided Precoding Designs for Secured Visible Light Communication Systems. *IEEE Trans. Wirel. Commun.* **2021**, *20*, 653–666. [CrossRef]
9. Qian, L.; Chi, X.; Zhao, L.; Chaaban, A. Secure Visible Light Communications via Intelligent Reflecting Surfaces. In Proceedings of the ICC 2021—IEEE International Conference on Communications, Online, 14–23 June 2021; pp. 1–6.
10. Ma, S.; Dong, Z.; Li, H.; Lu, Z.; Li, S. Optimal and Robust Secure Beamformer for Indoor MISO Visible Light Communication. *J. Lightwave Technol.* **2016**, *34*, 4988–4998. [CrossRef]
11. Xiao, L.; Sheng, G.; Liu, S.; Dai, H.; Peng, M.; Song, J. Deep Reinforcement Learning-Enabled Secure Visible Light Communication against Eavesdropping. *IEEE Trans. Commun.* **2019**, *67*, 6994–7005. [CrossRef]
12. Arfaoui, M.A.; Ghrayeb, A.; Assi, C.M. Secrecy Performance of Multi-User MISO VLC Broadcast Channels with Confidential Messages. *IEEE Trans. Wirel. Commun.* **2018**, *17*, 7789–7800. [CrossRef]
13. Arfaoui, M.A.; Ghrayeb, A.; Assi, C.M. Secrecy Performance of the MIMO VLC Wiretap Channel with Randomly Located Eavesdropper. *IEEE Trans. Wirel. Commun.* **2020**, *19*, 265–278. [CrossRef]
14. Chaaban, A.; Rezki, Z.; Alouini, M.-S. Fundamental Limits of Parallel Optical Wireless Channels: Capacity Results and Outage Formulation. *IEEE Trans. Commun.* **2016**, *65*, 296–311. [CrossRef]
15. Jeganathan, J.; Ghrayeb, A.; Szczecinski, L.; Ceron, A. Space shift keying modulation for MIMO channels. *IEEE Trans. Wirel. Commun.* **2009**, *8*, 3692–3703. [CrossRef]

16. Bao, J.; Zhang, H. The Study of Generalized Spatial Modulation Based on MPAPM Signals in Indoor Visible Light Communication System. In Proceedings of the 2020 IEEE Eurasia Conference on IOT, Communication and Engineering, Yunlin, Taiwan, 23–25 October 2020; pp. 82–84.
17. Wang, F.; Liu, C.; Wang, Q.; Zhang, J.; Zhang, R.; Yang, L.-L.; Hanzo, L. Secrecy Analysis of Generalized Space-Shift Keying Aided Visible Light Communication. *IEEE Access* **2018**, *6*, 18310–18324. [CrossRef]
18. Ben, Y.; Chen, M.; Cao, B.; Yang, Z.; Li, Z.; Cang, Y.; Xu, Z. On Secrecy Sum-Rate of Artificial-Noise-Aided Multi-user Visible Light Communication Systems. In Proceedings of the 2021 IEEE International Conference on Communications Workshops (ICC Workshops), Montreal, QC, Canada, 14–23 June 2021; pp. 1–6.
19. Wang, F.; Liu, C.; Wang, Q.; Zhang, J.; Zhang, R.; Yang, L.-L.; Hanzo, L. Optical Jamming Enhances the Secrecy Performance of the Generalized Space-Shift-Keying-Aided Visible-Light Downlink. *IEEE Trans. Commun.* **2018**, *66*, 4087–4102. [CrossRef]
20. Kiasaleh, K. Performance of coherent DPSK free-space optical communication systems in K-distributed turbulence. *IEEE Trans. Commun.* **2006**, *54*, 604–607. [CrossRef]
21. Popoola, W.O.; Ghassemlooy, Z.; Allen, J. Performance of subcarrier modulated free-space optical communications. In Proceedings of the PGNET Annual Postgraduate Symposium on the Convergence of Telecommunications Networking & Broadcasting, Liverpool, UK, 23–24 July 2008; Volume 1, pp. 342–355.
22. Uysal, M.; Li, J.; Yu, M. Error rate performance analysis of coded free-space optical links over gamma-gamma atmospheric turbulence channels. *IEEE Trans. Wirel. Commun.* **2006**, *5*, 1229–1233. [CrossRef]
23. Bayaki, E.; Schober, R.; Mallik, R.K. Performance Analysis of Free-Space Optical Systems in Gamma-Gamma Fading. In Proceedings of the 2008 IEEE Global Telecommunications Conference, New Orleans, LA, USA, 30 November–4 December 2008; pp. 1–6.
24. Gappmair, W.; Muhammad, S.S. Error performance of PPM/Poisson channels in turbulent atmosphere with gamma-gamma distribution. *Electron. Lett.* **2007**, *43*, 880–882. [CrossRef]
25. Nistazakis, H.E.; Tsiftsis, T.A.; Tombras, G.S. Performance analysis of free-space optical communication systems over atmospheric turbulence channels. *IET Commun.* **2009**, *3*, 1402–1409. [CrossRef]
26. Peng, Y.; Peng, L. A cooperative transmission strategy for body-area networks in healthcare systems. *IEEE Access* **2017**, *4*, 9155–9162. [CrossRef]
27. Peng, Y.; Li, J.; Park, S.; Zhu, K.; Hassan, M.; Alsanad, A. Energy-efficient cooperative transmission for intelligent transportation systems. *Future Gener. Comput. Syst.* **2019**, *94*, 634–640. [CrossRef]
28. Huang, Z.; Peng, Y.; Li, J.; Tong, F.; Zhu, K.; Peng, L. Secrecy Enhancing of SSK Systems for IoT Applications in Smart Cities. *IEEE Internet Things J.* **2021**, *8*, 6385–6392. [CrossRef]
29. Zhu, H.; Peng, Y. Secrecy enhancing for SSK-based communications in the presence of imperfect CSI estimation. *IEEJ Trans. Electr. Electron. Eng.* **2021**, *16*, 1544–1546. [CrossRef]
30. Huang, Z.; Peng, Y.; Li, J.; Jiang, X.-Q. Secrecy Enhancing for Space Shift Keying Based Communication Systems. *IEEJ Trans. Electr. Electron. Eng.* **2020**, *15*, 771–772. [CrossRef]
31. Mehlhorn, K. *Data Structures and Algorithms: Sorting and Searching*; Springer: Berlin/Heidelberg, Germany, 1984.
32. Yu, W.; Zhang, K.; Shang, P.; Jiang, X.-Q.; Wen, M.; Li, J.; Hai, H. Security enhancing spatial modulation using antenna selection and artificial noise cancellation. In Proceedings of the 2019 International Conference on Computer Communication and the Internet, Honolulu, HI, USA, 18–21 February 2019; pp. 105–109.