electronics

MDPI

Article

Physical Layer Security for L-Band Digital Aeronautical Communication System with Interference Mitigation

Lei Qian [1,2,*], Henghao Xu [3], Lei Wang [4], Di Wang [1,2], Xin Liu [5] and Boya Shi [1,2]

[1] School of Electronic and Information Engieering, Tiangong Unversity, Tianjin 300387, China; wangdi@tiangong.edu.cn (D.W.); shiboya@tiangong.edu.cn (B.S.)
[2] Tianjin Key Laboratory of Optoelectronic Detection Technology and System, Tianjin 300387, China
[3] School of Telecommunications Engineering, Xidian University, Xi'an 710071, China; 1910920417@tiangong.edu.cn
[4] Tianjin Key Lab for Advanced Signal Processing, Civil Aviation University of China, Tianjin 300300, China; wanglei@mail.cauc.edu.cn
[5] Information Application Department, Noncommissioned Officer Institute, Army Academy of Armored Forces, Changchun 130117, China; xliu15@mails.jlu.edu.cn
* Correspondence: qianlei@tiangong.edu.cn

Abstract: As one of the main candidates for future civil aviation communications systems, the L-band digital aeronautical communication system (L-DACS) is expected to achieve secure and reliable transmission. Due to the broadcasting nature of air–ground wireless links, the L-DACS has the risk of being intercepted by malicious eavesdroppers, which negatively affects aviation communication security. In addition, because the spectrum of the L-DACS overlaps with the aviation distance measuring equipment (DME), the pulse interference caused by the DME signal may lead to the wireless link being more fragile and susceptible to wiretapping. In this paper, with a focus on enhancing wireless transmission security, we propose a comprehensive physical layer security (PLS) method for the L-DACS. The key to the proposed PLS method is restraining the transmission of the eavesdropper by injecting artificial noise into the transmitted signal while improving the transmission of the legitimate receiver through the adoption of pulse interference mitigation. First, to characterize the L-DACS in the secure scene, we derive the signal-to-interference-plus-noise ratio (SINR) of the legitimate receiver and any potential eavesdropper by constructing equivalent noise. Next, from the perspective of the information theory, we derive the closed form of the secrecy capacity of the L-DACS by employing the proposed PLS methods with three kinds of nonlinear interference mitigation: including ideal pulse blanking, peak threshold-based pulse blanking, and peak threshold-based pulse clipping. Finally, we compare and analyze different ways to enhance the secrecy capacity of the proposed PLS method using various interference mitigation methods.

Keywords: L-band digital aeronautical communication system; physical layer security; secrecy capacity; pulse interference mitigation

check for updates

Citation: Qian, L.; Xu, H.; Wang, L.; Wang, D.; Liu, X.; Shi, B. Physical Layer Security for L-Band Digital Aeronautical Communication System with Interference Mitigation. *Electronics* **2023**, *12*, 4591. https://doi.org/10.3390/electronics12224591

Academic Editor: Christos J. Bouras

Received: 18 September 2023
Revised: 1 November 2023
Accepted: 8 November 2023
Published: 10 November 2023

1. Introduction

Global air traffic is expected to reach 22 million flights per year by 2025, while the number of aircraft passengers is expected to approach 12 billion passengers per year by 2031 [1]. With the fast development of the civil aviation industry, the demand for secure civil aviation communications systems is increasing. In 2008, the International Civil Aviation Organization (ICAO) proposed several new generation aviation wireless communication system standards, among which the L-band digital aeronautical communication system (L-DACS) is considered one of the main candidates for future civil aviation communications infrastructure in the terminal area and high-altitude airway airspace [2]. In particular, mode 1 of L-DACS, i.e., L-DACS1, is the first-generation system for airport ground mobile communications, while mode 2 of L-DACS, i.e., L-DACS2, is the upgraded version for air traffic control [3].

Due to the broadcasting nature of air-ground wireless links, L-DACS has a risk of being intercepted by malicious eavesdroppers. The leakage of aviation management and control information may affect aviation communication security and lead to serious security incidents [4]. To ensure information security, cryptography-based security technologies such as data encryption, data integrity, and key authentication protocols were implemented in the upper layers of the L-DACS in [5] based on the existing protocol stack. In addition, through the FACTS2 simulation platform, the impact of cryptography-based security technologies on the information security was verified in [6] and the additional signaling overhead was evaluated. The results of these studies show that although cryptography-based security technologies can improve security performance, they come at the expense of a large amount of bandwidth resources and throughput. Hence, cryptography-based security technologies are not optimal solutions for L-DACS due to its scarce bandwidth resources and the high-capacity requirements of aviation communications.

Considering the stress imposed by spectrum scarcity, the ICAO has deployed the L-DACS system in the aeronautical radio navigation L-band, i.e., 960 MHz–1164 MHz. However, this frequency band is already occupied by other systems, including aeronautical navigation distance measuring equipment (DME). To measure the distance between an aircraft and a ground navigation station, the DME transmitter sends a pulse signal to the ground navigation station; upon receiving this signal, the ground navigation station immediately transmits back a pulse signal of the same frequency. The distance between the aircraft and the ground navigation station can then be estimated according to the round-trip time difference of the pulse signal [7]. Because the spectrum used for L-DACS is embedded in the inter-channel of DME, it is susceptible to high-power DME pulse interference. Due to the large difference in the statistical characteristics of DME impulsive noise and additive white Gaussian noise (AWGN), the performance of L-DACS is significantly degraded on the impulsive noise channel, which may disable air–ground transmission links and affect the stability of the L-DACS [8]. Furthermore, serious DME pulse interference may make the wireless link more fragile, rendering it susceptible to wiretapping and threatening the security of civil aviation communications.

As a supplement to upper-layer security, physical layer security (PLS) (known elsewhere as information-theoretic security) can provide secure wireless transmission by exploiting the difference between legitimate channels and wiretap channels from the perspective of the information theory [9]. Without any extra delay due to encryption, PLS can achieve a lightweight security guarantee for aviation communications systems. As such, PLS-aided L-DACS has begun to attract attention due to the possibility of guaranteeing the privacy of civil aviation management and control information. However, the related research remains in the preliminary stages. In 2017, the wireless datalink security of L-DACS was first discussed in [10], where the authors pointed out that existing upper-layer security methods could not be directly applied to L-DACS because of its narrow frequency band and susceptibility to pulse interference. To prevent illegal third parties from eavesdropping and attacking, it is possible to increase the physical layer transmitting power of L-DACS; however, this high power may cause interference with DME systems. The authors of [10] proposed detecting the presence of illegal users through real-time monitoring of system states such as the packet loss rate, signal-to-noise ratio (SNR), and other indicators, then guaranteeing information security by switching the current transmission to duplicate links. However, this approach consumes extra bandwidth resources. To improve the throughput while simultaneously enhancing the security in an L-DACS-based aeronautical ad hoc network, a novel PLS method based on channel quality indicator (CQI)-mapped spatially modulated sparse code multiple access (SM-SCMA) was proposed in [11]. In this method, a physical-layer secret key is generated by varying the SM-SCMA mapping patterns based on the instantaneous CQI in the desired link. Because this secret key is not exchanged between the source aeroplane and its destination, the ergodic secrecy rates can be significantly improved. However, the impact of high-power DME pulse interference on L-DACS was not taken into account.

For wireless communication systems with pulse interference, e.g., the power line communication (PLC) system, one way to enhance security is to encode the transmitted information with the use of a secret key, as reported in [12–16]. To further quantitatively analyze the PLS performance, a mathematical impulsive noise model is needed. The authors characterized the time-domain impulsive noise model using three parameters, namely, the pulse amplitude, pulse width, and inter-arrival time. Based on time-domain channel impulse response (CIR) modeling, the ergodic achievable secrecy rate and secrecy outage probability were numerically evaluated with the use of a dataset [17,18] obtained from a measurement campaign involving an impulsive noise-added communications system. Further, the effective secrecy throughput and wiretap code rates have been analyzed for wireless communication systems with pulse interference under the presence of colluding eavesdroppers in [19]. In [20], a novel CIR-based multilevel quantization was proposed to improve PLS by reducing the error mismatch rate. The effect of the impulsive noise in the time domain is equivalent to additive colored Gaussian noise in the frequency-domain. Based on the colored Gaussian noise model, Ref. [21] analyzed the PLS of the power grid network with impulsive noise and with temporal artificial noise injection when the CSI of an eavesdropper is known to the legitimate user and when it is unknown. Further, an artificial noise-aided PLS solution for multiple input–multiple output (MIMO) power grid networks with a colored Gaussian noise model was proposed in [22] using in-band full-duplex technology. Because pulse interference affecting wireless communication systems such as PLC systems may include several types of impulsive noise, including synchronous cyclic periodic impulsive noise, asynchronous cyclic periodic impulsive noise, and aperiodic impulsive noise, the Middleton class-A noise model was proposed to depict the impulsive noise comprehensively, an approach that has found broad accepted in investigations of PLC systems [23,24]. As a special case of a Middleton class-A noise model, the Bernoulli–Gaussian (BG) model focuses on characterizing the randomness of impulsive noise. Based on the BG model, a chaos-based modulation scheme was proposed in [25] to provide secure communications against an eavesdropper in impulsive noise-added wireless communication scenarios. Further, based on BG-characterized impulsive noise, a log-normal correlated channel model was developed [26] and the PLS performance was analyzed for artificial noise-aided cooperative PLC networks.

Due to the non-negligible impact of DME pulse signals on the PLS performance of L-DACS, impulsive noise should be considered when designing a PLS method for L-DACS. In this paper, instead of the traditional channel capacity, we derive the secrecy capacity as a metric to characterize PLS performance for L-DACS. The secrecy capacity is the maximum transmission rate that can be achieved without leaking any information to an eavesdropper. A comprehensive PLS method is proposed for L-DACS to restrain the transmission of the eavesdropper by injecting artificial noise into the transmitted signal while improving the transmission of the legitimate receiver by adopting pulse interference mitigation. Our contributions are summarized as follows:

- We jointly consider a potential illegal eavesdropper at any position and high-powered DME pulse interference of practical L-DACS. We propose a PLS method including anisotropic, uniformly distributed artificial noise, and nonlinear interference mitigation.
- To analyze the PLS performance of the proposed method in different cases from the perspective of information theory, we derive the closed-form expressions of the secrecy capacity for practical artificial noise-aided L-DACS with three kinds of nonlinear pulse interference mitigation methods: ideal pulse blanking, peak threshold-based pulse blanking, and peak threshold-based pulse clipping.
- We compare and analyze the secrecy capacity for the proposed PLS method with various interference mitigation methods. Our simulation results show that it is necessary to consider eavesdropping alleviation and pulse interference mitigation jointly

in the secure L-DACS scene. Our proposed method can significantly improve PLS performance for L-DACS.

2. System Model

The system model of the secure L-DACS is illustrated in Figure 1; it includes a transmitter, a legitimate receiver, and an eavesdropper. The three parties are usually referred to as Alice, Bob, and Eve, respectively.

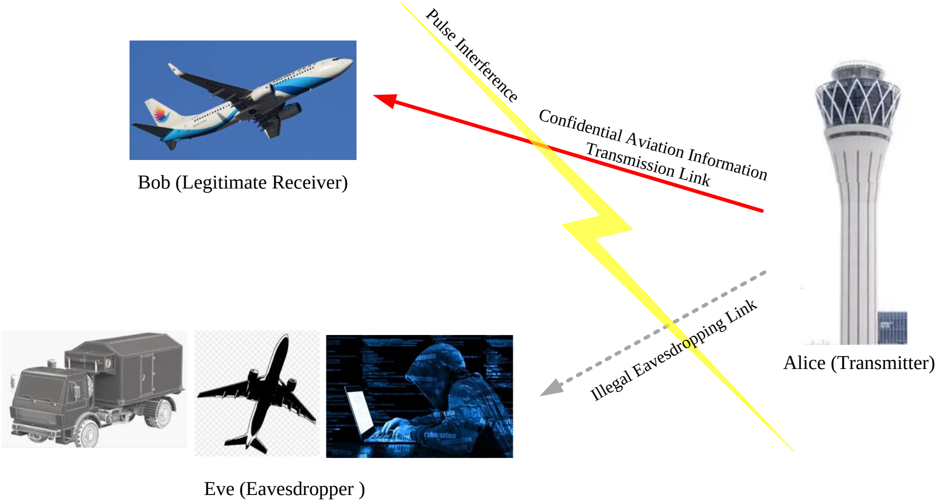
Pulse Interference
Confidential Aviation Information Transmission Link
Bob (Legitimate Receiver)
Illegal Eavesdropping Link
Alice (Transmitter)
Eve (Eavesdropper)

Figure 1. Secure scene of the L-DACS.

In this paper, the L-DACS transmitter has multiple antennas, the number of which is N_t. The legitimate receiver (Bob) and the eavesdropper (Eve) deploy a single antenna. The downlink received signals of Bob and Eve contain three parts (the transmitted signal, AWGN and pulse interference), which are expressed as

$$y_\mathrm{b} = \mathbf{h}_\mathrm{b}^T \mathbf{s} + n_\mathrm{b} + I_\mathrm{b} \tag{1}$$

and

$$y_\mathrm{e} = \mathbf{h}_\mathrm{e}^T \mathbf{s} + n_\mathrm{e} + I_\mathrm{e}, \tag{2}$$

respectively, where $\mathbf{s} \in \mathbb{C}^{N_\mathrm{t}\times 1}$ denotes the transmitted signal vector, $\mathbf{h}_\mathrm{b} \in \mathbb{C}^{N_\mathrm{t}\times 1}$ and $\mathbf{h}_\mathrm{e} \in \mathbb{C}^{N_\mathrm{t}\times 1}$ denote the channel gain vectors of Bob and Eve, respectively, $n_\mathrm{b} \sim CN(0, \sigma_{n_\mathrm{b}}^2)$ and $n_\mathrm{e} \sim CN(0, \sigma_{n_\mathrm{e}}^2)$ are the AWGNs of the channels of Bob and Eve, respectively (where $\sigma_{n_\mathrm{b}}^2$ and $\sigma_{n_\mathrm{e}}^2$ represent the variance of AWGNs), and I_b and I_e denote the impulsive noise suffered by Bob and Eve, respectively. In this paper, Rician fading channels are considered and the channel state information is assumed to be known to the L-DACS transmitter. According to the BG impulsive noise model, we have $I_\mathrm{b} = \beta_\mathrm{b} g_\mathrm{b}$ and $I_\mathrm{e} = \beta_\mathrm{e} g_\mathrm{e}$, where β_b and β_e are modeled as Bernoulli random variables, while g_b and g_e denote the impulsive noise. In detail, $\beta_\mathrm{b} = 1$ indicates the presence of impulsive noise in Bob's channel, and its corresponding probability is p_b. In contrast, $\beta_\mathrm{b} = 0$ indicates that the impulsive noise does not exist, for which the corresponding probability is $(1 - p_\mathrm{b})$. Here, g_b and g_e follow complex Gaussian distributions, i.e., $g_\mathrm{b} \sim CN(0, \sigma_{g_\mathrm{b}}^2)$ and $g_\mathrm{e} \sim CN(0, \sigma_{g_\mathrm{e}}^2)$, respectively, where $\sigma_{g_\mathrm{b}}^2$ and $\sigma_{g_\mathrm{e}}^2$ represent the variance of the corresponding impulsive noise.

3. Secrecy Capacity of L-DACS with the Proposed Comprehensive PLS Method

In this section, jointly considering a potential illegal eavesdropper at any position and high-powered DME pulse interference with the L-DACS, we propose the comprehensive PLS method summarized in Table 1. More particularly, in order to prevent confidential information from being acquired by the eavesdropper, we inject artificial noise into the transmitted signal of the L-DACS. Simultaneously, we utilize three typical nonlinear interference mitigation methods to consider the impact of high-power pulse interference: ideal pulse blanking, peak threshold-based pulse blanking, and peak threshold-based pulse clipping. For each interference mitigation-aided PLS method, we derive the closed-form of secrecy capacity for the L-DACS.

Table 1. Summary of the proposed comprehensive PLS method.

Step 1: Determine the system parameters of the L-DACS.
Step 2: At the transmitter, inject the artificial noise into the transmitted L-DACS signal.
Step 3: At the legitimate receiver, adopt different nonlinear interference mitigation methods (ideal pulse blanking, peak threshold-based pulse blanking, and peak threshold-based pulse clipping).
Step 4: Calculate the secrecy capacity for L-DACS employing the proposed PLS methods.

3.1. Secrecy Capacity for Artificial Noise-Aided L-DACS without Interference Mitigation

To enhance secrecy performance, the artificial noise-based PLS method is introduced into L-DACS to intentionally interfere with the received signal of the eavesdropper. Considering that the channel state information of the eavesdropping channel is always unavailable to the transmitter, the artificial noise is designed anisotropically and uniformly distributed in the nullspace of the legitimate channel. In other words, the transmitted signal is divided into the useful signal and jamming signal, which is described as

$$\mathbf{s} = \sqrt{\phi P_{\mathrm{t}}}\mathbf{w}s_{\mathrm{u}} + \sqrt{(1-\phi)P_{\mathrm{t}}/(N_{\mathrm{t}}-1)}\mathbf{T}\mathbf{s}_{\mathrm{a}}, \tag{3}$$

where P_{t} is the transmit power and $\phi \in [0,1]$ is the power separation factor. The useful signal is denoted by s_{u}, which follows a complex Gaussian distribution, i.e., $s_{\mathrm{u}} \sim CN(0, \sigma_{s_{\mathrm{u}}}^2)$, and we assume the power of s_{u} to be $E\left[|s_{\mathrm{u}}|^2\right] = 1$. In addition, $\mathbf{w}$ is the normalized precoding vector of the useful signal, and has dimension $N_{\mathrm{t}} \times 1$. To enhance the useful signal, $\mathbf{w}$ is determined in this paper using the maximum ratio transmission (MRT) principle. Therefore, $\mathbf{w}$ is obtained by $\mathbf{w} = \mathbf{h}_{\mathrm{b}}/\|\mathbf{h}_{\mathrm{b}}\|_2$ while satisfying $\|\mathbf{w}\|_2 = 1$. Moreover, the artificial noise vector and the artificial noise beamforming vector are denoted by $\mathbf{s}_{\mathrm{a}} \in \mathbb{C}^{(N_{\mathrm{t}}-1)\times 1}$ and $\mathbf{T} \in \mathbb{C}^{N_{\mathrm{t}}\times(N_{\mathrm{t}}-1)}$, respectively. To guarantee that the jamming signals are transmitted in the nullspace of the channel of the legitimate user, we define $\mathbf{T}$ as a matrix with columns $\mathbf{T}_1, \mathbf{T}_2, \cdots \mathbf{T}_{N_{\mathrm{t}}-1}$ that constitute a basis for the nullspace of $\mathbf{h}_{\mathrm{b}}^T$ and are normalized such that $\|\mathbf{T}_l\|_2 = 1, \forall l \in \{1, 2, \ldots, N_{\mathrm{t}}-1\}$. Furthermore, in order to be fair to each potential eavesdropping channel, the power of the artificial noise is divided equally among the available $N_{\mathrm{t}}-1$ nullspace directions, which is shown as the second term of Equation (3).

According to the design of our jamming signals, we have $\mathbf{h}_{\mathrm{b}}^T\mathbf{T} = 0$. To show the effect of the artificial noise on the received signals, we can substitute Equation (3) into Equation (1) and obtain the received signals of Bob as follows:

$$y_{\mathrm{b}} = \begin{cases} \sqrt{\phi P_{\mathrm{t}}}\mathbf{h}_{\mathrm{b}}^T\mathbf{w}s_{\mathrm{u}} + n_{\mathrm{b}} + g_{\mathrm{b}}, & \text{if } \beta_{\mathrm{b}} = 1, \\ \sqrt{\phi P_{\mathrm{t}}}\mathbf{h}_{\mathrm{b}}^T\mathbf{w}s_{\mathrm{u}} + n_{\mathrm{b}}, & \text{if } \beta_{\mathrm{b}} = 0. \end{cases} \tag{4}$$

Similarly, by substituting Equation (3) into Equation (2), we can obtain the received signals of Eve as follows:

$$y_{\mathrm{e}} = \begin{cases} \sqrt{\phi P_{\mathrm{t}}}\mathbf{h}_{\mathrm{e}}^T\mathbf{w}s_{\mathrm{u}} + \sqrt{(1-\phi)P_{\mathrm{t}}/(N_{\mathrm{t}}-1)}\mathbf{h}_{\mathrm{e}}^T\mathbf{T}\mathbf{s}_{\mathrm{a}} + n_{\mathrm{e}} + g_{\mathrm{e}}, & \text{if } \beta_{\mathrm{b}} = 1, \\ \sqrt{\phi P_{\mathrm{t}}}\mathbf{h}_{\mathrm{e}}^T\mathbf{w}s_{\mathrm{u}} + \sqrt{(1-\phi)P_{\mathrm{t}}/(N_{\mathrm{t}}-1)}\mathbf{h}_{\mathrm{e}}^T\mathbf{T}\mathbf{s}_{\mathrm{a}} + n_{\mathrm{e}}, & \text{if } \beta_{\mathrm{b}} = 0. \end{cases} \tag{5}$$

Based on Equation (4), the signal-to-interference-plus-noise ratio (SINR) of Bob can be expressed as

$$\gamma_{\mathrm{b}} = \frac{\phi P_{\mathrm{t}}(\mathbf{h}_{\mathrm{b}}^T\mathbf{w})^T(\mathbf{h}_{\mathrm{b}}^T\mathbf{w})}{p_{\mathrm{b}}\sigma_{g_{\mathrm{b}}}^2 + \sigma_{n_{\mathrm{b}}}^2}. \tag{6}$$

Further, according to the Shannon's theorem, the channel capacity of Bob can be derived as

$$C_{\mathrm{b}} = B\log_2(1 + \frac{\phi P_{\mathrm{t}}(\mathbf{h}_{\mathrm{b}}^T\mathbf{w})^T(\mathbf{h}_{\mathrm{b}}^T\mathbf{w})}{p_{\mathrm{b}}\sigma_{g_{\mathrm{b}}}^2 + \sigma_{n_{\mathrm{b}}}^2}). \tag{7}$$

Similarly, based on Equation (5), the SINR and channel capacity of Eve can be derived as

$$\gamma_{\mathrm{e}} = \frac{\phi P_{\mathrm{t}}(\mathbf{h}_{\mathrm{e}}^T\mathbf{w})^T(\mathbf{h}_{\mathrm{e}}^T\mathbf{w})}{[(1-\phi)P_{\mathrm{t}}/(N_{\mathrm{t}}-1)](\mathbf{h}_{\mathrm{e}}^T\mathbf{T})^T(\mathbf{h}_{\mathrm{e}}^T\mathbf{T}) + p_{\mathrm{e}}\sigma_{g_{\mathrm{e}}}^2 + \sigma_{n_{\mathrm{e}}}^2} \tag{8}$$

and

$$C_{\mathrm{e}} = B\log_2(1 + \frac{\phi P_{\mathrm{t}}(\mathbf{h}_{\mathrm{e}}^T\mathbf{w})^T(\mathbf{h}_{\mathrm{e}}^T\mathbf{w})}{[(1-\phi)P_{\mathrm{t}}/(N_{\mathrm{t}}-1)](\mathbf{h}_{\mathrm{e}}^T\mathbf{T})^T(\mathbf{h}_{\mathrm{e}}^T\mathbf{T}) + p_{\mathrm{e}}\sigma_{g_{\mathrm{e}}}^2 + \sigma_{n_{\mathrm{e}}}^2}), \tag{9}$$

respectively.

According to the information theory, the secrecy capacity is defined as

$$R_{\mathrm{sec}} = [C_{\mathrm{b}} - C_{\mathrm{e}}]^+. \tag{10}$$

Therefore, the secrecy capacity of the artificial noise-aided L-DACS without interference mitigation can be expressed as

$$\begin{aligned} R_{\mathrm{sec}} = \Bigg[& B\log_2(1 + \frac{\phi P_{\mathrm{t}}(\mathbf{h}_{\mathrm{b}}^T\mathbf{w})^T(\mathbf{h}_{\mathrm{b}}^T\mathbf{w})}{p_{\mathrm{b}}\sigma_{g_{\mathrm{b}}}^2 + \sigma_{n_{\mathrm{b}}}^2}) \\ & - B\log_2(1 + \frac{\phi P_{\mathrm{t}}(\mathbf{h}_{\mathrm{e}}^T\mathbf{w})^T(\mathbf{h}_{\mathrm{e}}^T\mathbf{w})}{[(1-\phi)P_{\mathrm{t}}/(N_{\mathrm{t}}-1)](\mathbf{h}_{\mathrm{e}}^T\mathbf{T})^T(\mathbf{h}_{\mathrm{e}}^T\mathbf{T}) + p_{\mathrm{e}}\sigma_{g_{\mathrm{e}}}^2 + \sigma_{n_{\mathrm{e}}}^2}) \Bigg]^+. \end{aligned} \tag{11}$$

3.2. Secrecy Capacity for Artificial Noise-Aided L-DACS with Ideal Pulse Blanking

To alleviate the impact of high-power pulse interference, the ideal pulse blanking method is developed for the legitimate user in L-DACS; in this subsection, the ideal pulse blanking-aided PLS method is proposed and analyzed. We assume that the legitimate user can precisely estimate the positions of the impulsive noise, then the impulsive noise is blanked by multiplying the pulse blanking factor on the received signal. To eliminate the received signal to zero at the position where the pulses exist while maintaining the same at other positions, the pulse blanking factor of the ideal pulse blanking method is designed as

$$d^{\mathrm{IB}} = \begin{cases} 0, & \text{if } \beta_{\mathrm{b}} = 1, \\ 1, & \text{if } \beta_{\mathrm{b}} = 0. \end{cases} \tag{12}$$

Combining Equations (4) and (12), the received signal of Bob in the adopted L-DACS ideal pulse blanking-aided PLS method can be obtained as follows:

$$y_{\mathrm{b}}^{\mathrm{IB}} = y_{\mathrm{b}} d^{\mathrm{IB}} = \begin{cases} 0, & \text{if } \beta_{\mathrm{b}} = 1, \\ \sqrt{\phi P_{\mathrm{t}}}\mathbf{h}_{\mathrm{b}}^T\mathbf{w}s_{\mathrm{u}} + n_{\mathrm{b}}, & \text{if } \beta_{\mathrm{b}} = 0. \end{cases} \tag{13}$$

For the sake of analysis, we can try to transform the received signal after ideal pulse blanking processing into a universal form by constructing an equivalent noise. The transformed received signal is expressed as

$$y_{\mathrm{b}}^{\mathrm{IB}} = \sqrt{\phi P_{\mathrm{t}}}\mathbf{h}_{\mathrm{b}}^T\mathbf{w}s_{\mathrm{u}} + n_{\mathrm{b}}^{\mathrm{IB}}, \tag{14}$$

where $n_{\mathrm{b}}^{\mathrm{IB}}$ denotes the equivalent noise of the ideal pulse blanking method, which is described as follows:

$$n_{\mathrm{b}}^{\mathrm{IB}} = \begin{cases} -\sqrt{\phi P_{\mathrm{t}}}\mathbf{h}_{\mathrm{b}}^{T}\mathbf{w}s_{\mathrm{u}}, & \text{if } \beta_{\mathrm{b}} = 1, \\ n_{\mathrm{b}}, & \text{if } \beta_{\mathrm{b}} = 0. \end{cases} \tag{15}$$

Equation (15) indicates that at the position of the impulsive noise, i.e., $\beta_{\mathrm{b}} = 1$, the receiver performs ideal pulse blanking, which results in the whole received signal being blanked to zero. Therefore, in this case the equivalent noise satisfies $n_{\mathrm{b}}^{\mathrm{IB}} = -\sqrt{\phi P_{\mathrm{t}}}\mathbf{h}_{\mathrm{b}}^{T}\mathbf{w}s_{\mathrm{u}}$. By contrast, for positions without impulsive noise, i.e., $\beta_{\mathrm{b}} = 0$, only AWGN exists in the channel; hence, the equivalent noise satisfies $n_{\mathrm{b}}^{\mathrm{IB}} = n_{\mathrm{b}}$.

According to Equation (14), the SINR and channel capacity of Bob in the adopted L-DACS ideal pulse blanking-aided PLS method can be derived as

$$\begin{aligned} \gamma_{\mathrm{b}}^{\mathrm{IB}} &= p_{\mathrm{b}}\frac{\phi P_{\mathrm{t}}\|\mathbf{h}_{\mathrm{b}}\|_2^2}{\phi P_{\mathrm{t}}\|\mathbf{h}_{\mathrm{b}}\|_2^2} + (1-p_{\mathrm{b}})\frac{\phi P_{\mathrm{t}}\|\mathbf{h}_{\mathrm{b}}\|_2^2}{\sigma_{n_{\mathrm{b}}}^2} \\ &= p_{\mathrm{b}} + (1-p_{\mathrm{b}})\frac{\phi P_{\mathrm{t}}\|\mathbf{h}_{\mathrm{b}}\|_2^2}{\sigma_{n_{\mathrm{b}}}^2}, \end{aligned} \tag{16}$$

and

$$C_{\mathrm{b}}^{\mathrm{IB}} = B\log_2\left[1 + p_{\mathrm{b}} + (1-p_{\mathrm{b}})\frac{\phi P_{\mathrm{t}}\|\mathbf{h}_{\mathrm{b}}\|_2^2}{\sigma_{n_{\mathrm{b}}}^2}\right]. \tag{17}$$

Because the illegal eavesdropper does not know the information of the impulsive noise, we assume that the receiver at eavesdropper do not adopt any interference mitigation. Therefore, the SINR and channel capacity of Eve in this subsection are the same as in Equations (8) and (9) in Section 3.1.

Furthermore, by substituting Equations (17) and (9) into Equation (10), the secrecy capacity of the adopted L-DACS ideal pulse blanking-aided PLS method is as follows:

$$\begin{aligned} R_{\mathrm{sec}}^{\mathrm{IB}} = \Bigg\{ & B\log_2\left[1 + p_{\mathrm{b}} + (1-p_{\mathrm{b}})\frac{\phi P_{\mathrm{t}}\|\mathbf{h}_{\mathrm{b}}\|_2^2}{\sigma_{n_{\mathrm{b}}}^2}\right] \\ & -B\log_2(1 + \frac{\phi P_{\mathrm{t}}(\mathbf{h}_{\mathrm{e}}^{T}\mathbf{w})^{T}(\mathbf{h}_{\mathrm{e}}^{T}\mathbf{w})}{[(1-\phi)P_{\mathrm{t}}/(N_{\mathrm{t}}-1)](\mathbf{h}_{\mathrm{e}}^{T}\mathbf{T})^{T}(\mathbf{h}_{\mathrm{e}}^{T}\mathbf{T}) + p_{\mathrm{e}}\sigma_{g_{\mathrm{e}}}^2 + \sigma_{n_{\mathrm{e}}}^2}) \Bigg\}^{+}. \end{aligned} \tag{18}$$

3.3. Secrecy Capacity for Artificial Noise-Aided L-DACS with Peak Threshold-Based Pulse Blanking

Considering the estimation error of impulsive noise in the practical L-DACS, finding the precise position of impulsive noise incurs a high cost. In this subsection, we develop a peak threshold-based pulse blanking method to mitigate interference at the legitimate receiver without using the ideal estimation assumption. Unlike ideal pulse blanking, we design the pulse blanking factor for the peak threshold-based pulse blanking method according to the amplitude of the received signal, which is easier to estimate than the position of impulsive noise. By multiplying the pulse blanking factor on the received signal, the received signal is blanked to zero if the amplitude of the received signal is larger than the pulse blanking threshold; otherwise, the received signal remains the same. The designed pulse blanking factor d^{PB} can be expressed as

$$d^{\mathrm{PB}} = \begin{cases} 0, & \text{if } |y_{\mathrm{b}}| \geqslant T_{\mathrm{th}}, \\ 1, & \text{if } |y_{\mathrm{b}}| < T_{\mathrm{th}}, \end{cases} \tag{19}$$

where $|y_{\mathrm{b}}|$ denotes the amplitude of the received signal and T_{th} denotes the peak threshold.

Multiplying Equation (19) with Equation (4), the received signal of Bob in the adopted L-DACS peak threshold-based pulse blanking-aided PLS method can be expressed as

$$y_{\mathrm{b}}^{\mathrm{PB}} = y_{\mathrm{b}} d^{\mathrm{PB}} = \begin{cases} 0, & \text{if } |y_{\mathrm{b}}| \geqslant T_{\mathrm{th}}, \\ \sqrt{\phi P_{\mathrm{t}}} \mathbf{h}_{\mathrm{b}}^{T} \mathbf{w} s_{\mathrm{u}} + n_{\mathrm{b}} + I_{\mathrm{b}}, & \text{if } |y_{\mathrm{b}}| < T_{\mathrm{th}}. \end{cases} \tag{20}$$

Using the same analytical method as in Section 3.1, we construct an equivalent noise for peak threshold-based pulse blanking, and transform the received signal as follows:

$$y_{\mathrm{b}}^{\mathrm{PB}} = \sqrt{\phi P_{\mathrm{t}}} \mathbf{h}_{\mathrm{b}}^{T} \mathbf{w} s_{\mathrm{u}} + n_{\mathrm{b}}^{\mathrm{PB}}, \tag{21}$$

where $n_{\mathrm{b}}^{\mathrm{PB}}$ denotes the equivalent noise, which is described as follows:

$$n_{\mathrm{b}}^{\mathrm{PB}} = \begin{cases} -\sqrt{\phi P_{\mathrm{t}}} \mathbf{h}_{\mathrm{b}}^{T} \mathbf{w} s_{\mathrm{u}}, & \text{if } \beta_{\mathrm{b}} = 1 \text{ and } |y_{\mathrm{b}}| \geqslant T_{\mathrm{th}}, \\ n_{\mathrm{b}} + g_{\mathrm{b}}, & \text{if } \beta_{\mathrm{b}} = 1 \text{ and } |y_{\mathrm{b}}| < T_{\mathrm{th}}, \\ -\sqrt{\phi P_{\mathrm{t}}} \mathbf{h}_{\mathrm{b}}^{T} \mathbf{w} s_{\mathrm{u}}, & \text{if } \beta_{\mathrm{b}} = 0 \text{ and } |y_{\mathrm{b}}| \geqslant T_{\mathrm{th}}, \\ n_{\mathrm{b}}, & \text{if } \beta_{\mathrm{b}} = 0 \text{ and } |y_{\mathrm{b}}| < T_{\mathrm{th}}. \end{cases} \tag{22}$$

As shown in Equation (22), there are four cases. First, when the pulse interference exists and the received signal is larger than or equal to the peak threshold, the legitimate receiver performs pulse blanking, which results in the whole received signal being blanked to zero; hence, the equivalent noise satisfies $n_{\mathrm{b}}^{\mathrm{PB}} = -\sqrt{\phi P_{\mathrm{t}}} \mathbf{h}_{\mathrm{b}}^{T} \mathbf{w} s_{\mathrm{u}}$. Second, when the pulse interference exists and the amplitude of the received signal does not reach the threshold, according to the principle of peak threshold-based pulse blanking, the receiver does not perform pulse blanking; therefore, we have $n_{\mathrm{b}}^{\mathrm{PB}} = n_{\mathrm{b}} + g_{\mathrm{b}}$. Third, in the case that the amplitude of the received signal is larger than or equal to the threshold even though there is no pulse interference, the whole received signal is blanked to zero and we have $n_{\mathrm{b}}^{\mathrm{PB}} = -\sqrt{\phi P_{\mathrm{t}}} \mathbf{h}_{\mathrm{b}}^{T} \mathbf{w} s_{\mathrm{u}}$. Finally, in the case that the pulse interference does not exist and the received signal is less than the threshold, only AWGN exists in the channel, and the equivalent noise degrades to $n_{\mathrm{b}}^{\mathrm{PB}} = n_{\mathrm{b}}$.

To obtain the SINR and channel capacity of Bob in Equation (21), we need to derive the probability and the corresponding conditional variance of the equivalent noise for each case in Equation (22) by following the approach proposed in [27]. Then, the SINR of Bob in the adopted L-DACS peak threshold-based pulse blanking-aided PLS method is expressed as

$$\begin{aligned} \gamma_{\mathrm{b}}^{\mathrm{PB}} = {} & p_{\mathrm{b}} \alpha \frac{\|\mathbf{h}_{\mathrm{b}}\|_2^2}{\left(2 + T_{\mathrm{th}}^2 \middle/ \left(\sigma_A^2\right)^2\right)} + p_{\mathrm{b}} (1-\alpha) \frac{\phi P_{\mathrm{t}} \|\mathbf{h}_{\mathrm{b}}\|_2^2}{2\left(\sigma_{n_{\mathrm{b}}}^2 + \sigma_{g_{\mathrm{b}}}^2\right) \left(1 - \frac{\left(\sigma_{n_{\mathrm{b}}}^2 + \sigma_{g_{\mathrm{b}}}^2\right) T_{\mathrm{th}}^2}{2\left(\sigma_A^2\right)^2 \left(\alpha^{-1} - 1\right)}\right)} \\ & + (1-p_{\mathrm{b}}) \beta \frac{\|\mathbf{h}_{\mathrm{b}}\|_2^2}{\left(2 + T_{\mathrm{th}}^2 \middle/ \left(\sigma_B^2\right)^2\right)} + (1-p_{\mathrm{b}})(1-\beta) \frac{\phi P_{\mathrm{t}} \|\mathbf{h}_{\mathrm{b}}\|_2^2}{2\sigma_{n_{\mathrm{b}}}^2 \left(1 - \frac{\sigma_{n_{\mathrm{b}}}^2 T_{\mathrm{th}}^2}{2\left(\sigma_B^2\right)^2 \left(\beta^{-1} - 1\right)}\right)}, \end{aligned} \tag{23}$$

where $\alpha = e^{-T_{\mathrm{th}}^2 / 2\sigma_A^2}$, $\beta = e^{-T_{\mathrm{th}}^2 / 2\sigma_B^2}$, $\sigma_A^2 = \sigma_{\mathbf{h}_{\mathrm{b}}}^2 + \sigma_{n_{\mathrm{b}}}^2 + \sigma_{g_{\mathrm{b}}}^2$, $\sigma_A^2 = \sigma_{\mathbf{h}_{\mathrm{b}}}^2 + \sigma_{n_{\mathrm{b}}}^2 + \sigma_{g_{\mathrm{b}}}^2$, $\sigma_B^2 = \sigma_{n_{\mathrm{b}}}^2 + \sigma_{g_{\mathrm{b}}}^2$.

Then, according to Shannon's theorem, the channel capacity of Bob in the adopted L-DACS peak threshold-based pulse blanking-aided PLS method is derived as follows:

$$\begin{aligned} C_{\mathrm{b}}^{\mathrm{PB}} = B \log_2 \Bigg[& 1 + p_{\mathrm{b}} \alpha \frac{\|\mathbf{h}_{\mathrm{b}}\|_2^2}{\left(2 + T_{\mathrm{th}}^2 \middle/ \left(\sigma_A^2\right)^2\right)} + p_{\mathrm{b}} (1-\alpha) \frac{\phi P_{\mathrm{t}} \|\mathbf{h}_{\mathrm{b}}\|_2^2}{2\left(\sigma_{n_{\mathrm{b}}}^2 + \sigma_{g_{\mathrm{b}}}^2\right) \left(1 - \frac{\left(\sigma_{n_{\mathrm{b}}}^2 + \sigma_{g_{\mathrm{b}}}^2\right) T_{\mathrm{th}}^2}{2\left(\sigma_A^2\right)^2 \left(\alpha^{-1} - 1\right)}\right)} \\ & + (1-p_{\mathrm{b}}) \beta \frac{\|\mathbf{h}_{\mathrm{b}}\|_2^2}{\left(2 + T_{\mathrm{th}}^2 \middle/ \left(\sigma_B^2\right)^2\right)} + (1-p_{\mathrm{b}})(1-\beta) \frac{\phi P_{\mathrm{t}} \|\mathbf{h}_{\mathrm{b}}\|_2^2}{2\sigma_{n_{\mathrm{b}}}^2 \left(1 - \frac{\sigma_{n_{\mathrm{b}}}^2 T_{\mathrm{th}}^2}{2\left(\sigma_B^2\right)^2 \left(\beta^{-1} - 1\right)}\right)} \Bigg]. \end{aligned} \tag{24}$$

Considering that the illegal eavesdropper does not have sufficient knowledge about the impulsive noise, we assume that the receiver at the eavesdropper does not adopt any interference mitigation. Therefore, the SINR and channel capacity of Eve is the same as in Equations (8) and (9) in Section 3.1.

Furthermore, by substituting Equations (24) and (9) into Equation (10), the secrecy capacity in the adopted L-DACS peak threshold-based pulse blanking-aided PLS method can be provided by

$$\begin{aligned} R_{\mathrm{sec}}^{\mathrm{PB}} = \Bigg\{ B\log_2 \Bigg[1 + p_{\mathrm{b}}\alpha \frac{\|\mathbf{h}_{\mathrm{b}}\|_2^2}{\left(2 + T_{\mathrm{th}}^2 \Big/ \left(\sigma_A^2\right)^2\right)} + p_{\mathrm{b}}(1-\alpha) \frac{\phi P_{\mathrm{t}} \|\mathbf{h}_{\mathrm{b}}\|_2^2}{2\left(\sigma_{n_{\mathrm{b}}}^2 + \sigma_{g_{\mathrm{b}}}^2\right)\left(1 - \frac{\left(\sigma_{n_{\mathrm{b}}}^2 + \sigma_{g_{\mathrm{b}}}^2\right)T_{\mathrm{th}}^2}{2\left(\sigma_A^2\right)^2\left(\alpha^{-1}-1\right)}\right)} \\ + (1-p_{\mathrm{b}})\beta \frac{\|\mathbf{h}_{\mathrm{b}}\|_2^2}{\left(2 + T_{\mathrm{th}}^2 \Big/ \left(\sigma_B^2\right)^2\right)} + (1-p_{\mathrm{b}})(1-\beta) \frac{\phi P_{\mathrm{t}} \|\mathbf{h}_{\mathrm{b}}\|_2^2}{2\sigma_{n_{\mathrm{b}}}^2 \left(1 - \frac{\sigma_{n_{\mathrm{b}}}^2 T_{\mathrm{th}}^2}{2\left(\sigma_B^2\right)^2\left(\beta^{-1}-1\right)}\right)} \Bigg] \\ - B\log_2 (1 + \frac{\phi P_{\mathrm{t}} \left(\mathbf{h}_{\mathrm{e}}^T \mathbf{w}\right)^T \left(\mathbf{h}_{\mathrm{e}}^T \mathbf{w}\right)}{\left[(1-\phi)P_{\mathrm{t}}/(N_{\mathrm{t}}-1)\right] \left(\mathbf{h}_{\mathrm{e}}^T \mathbf{T}\right)^T \left(\mathbf{h}_{\mathrm{e}}^T \mathbf{T}\right) + p_{\mathrm{e}}\sigma_{g_{\mathrm{e}}}^2 + \sigma_{n_{\mathrm{e}}}^2}) \Bigg\}^{+}. \end{aligned} \tag{25}$$

3.4. Secrecy Capacity for Artificial Noise-Aided L-DACS with Peak Threshold-Based Pulse Clipping

Considering that the capacity of the legitimate user may be reduced when the received signal is totally blanked to zero, in this subsection we employ a peak threshold-based pulse clipping method to mitigate the pulse interference. Similar to the peak threshold-based pulse blanking method, we assume that the amplitude of the received signal is known by the legitimate receiver and is set as the pulse clipping threshold. When the amplitude of the received signal is larger than or equal to the threshold, instead of blanking, the amplitude of the received signal is clipped to the threshold; otherwise, the original amplitude of the signal is maintained. The received signal of Bob in the artificial noise-aided L-DACS after peak threshold-based pulse clipping can be modeled as follows:

$$y_{\mathrm{b}}^{\mathrm{PC}} = \begin{cases} T_{\mathrm{th}} e^{j\arg(y_{\mathrm{b}})}, & \text{if } |y_{\mathrm{b}}| \geqslant T_{\mathrm{th}}, \\ y_{\mathrm{b}}, & \text{if } |y_{\mathrm{b}}| < T_{\mathrm{th}}, \end{cases} \tag{26}$$

where $\arg(y_{\mathrm{b}})$ denotes the phase angle of the received signal.

Using the same analytical method as in Section 3.1, we construct an equivalent noise for peak threshold-based pulse clipping and transform the received signal into

$$y_{\mathrm{b}}^{\mathrm{PC}} = \sqrt{\phi P_{\mathrm{t}}} \mathbf{h}_{\mathrm{b}}^T \mathbf{w} s_{\mathrm{u}} + n_{\mathrm{b}}^{\mathrm{PC}}, \tag{27}$$

where $n_{\mathrm{b}}^{\mathrm{PC}}$ denotes the equivalent noise, which is described as follows:

$$n_{\mathrm{b}}^{\mathrm{PC}} = \begin{cases} T_{\mathrm{th}} e^{j\arg(y_{\mathrm{b}})} - \sqrt{\phi P_{\mathrm{t}}} \mathbf{h}_{\mathrm{b}}^T \mathbf{w} s_{\mathrm{u}}, & \text{if } \beta_{\mathrm{b}} = 1 \text{ and } |y_{\mathrm{b}}| \geqslant T_{\mathrm{th}}, \\ n_{\mathrm{b}} + g_{\mathrm{b}}, & \text{if } \beta_{\mathrm{b}} = 1 \text{ and } |y_{\mathrm{b}}| < T_{\mathrm{th}}, \\ T_{\mathrm{th}} e^{j\arg(y_{\mathrm{b}})} - \sqrt{\phi P_{t}} \mathbf{h}_{\mathrm{b}}^T \mathbf{w} s_{\mathrm{u}}, & \text{if } \beta_{\mathrm{b}} = 0 \text{ and } |y_{\mathrm{b}}| \geqslant T_{\mathrm{th}}, \\ n_{\mathrm{b}}, & \text{if } \beta_{\mathrm{b}} = 0 \text{ and } |y_{\mathrm{b}}| < T_{\mathrm{th}}. \end{cases} \tag{28}$$

Similar to the analysis of the peak threshold-based pulse blanking method, there are four cases in Equation (28). First, if the amplitude of the received signal is larger than or equal to the peak threshold at the position of the pulse interference, the legitimate receiver performs pulse clipping, which results in the amplitude of the received signal being limited to the threshold; hence, the equivalent noise satisfies $n_{\mathrm{b}}^{\mathrm{PC}} = T_{\mathrm{th}} e^{j\arg(y_{\mathrm{b}})} - \sqrt{\phi P_{\mathrm{t}}} \mathbf{h}_{\mathrm{b}}^T \mathbf{w} s_{\mathrm{u}}$. Second, if the amplitude of received signal does not reach the threshold at the position of pulse interference, the receiver does not perform pulse clipping, and then we have $n_{\mathrm{b}}^{\mathrm{PC}} = n_{\mathrm{b}} + g_{\mathrm{b}}$. Third, if the amplitude of received signal reaches the threshold without any pulse interference being present, the received signal is limited to T_{th} and we have $n_{\mathrm{b}}^{\mathrm{PC}} = T_{\mathrm{th}} e^{j\arg(y_{\mathrm{b}})} - \sqrt{\phi P_{\mathrm{t}}}\mathbf{h}_{\mathrm{b}}^{T}\mathbf{w}s_{\mathrm{u}}$. Finally, in the case that the pulse interference does not exist and the received signal is less than the threshold, only AWGN exists in the channel and the equivalent noise degrades to $n_{\mathrm{b}}^{\mathrm{PC}} = n_{\mathrm{b}}$.

According to the probability and the corresponding conditional variance of the equivalent noise for each case derived in Section 3.3, the SINR and capacity of Bob in the L-DACS adopted peak threshold-based pulse clipping aided PLS method are respectively expressed as follows:

$$\begin{aligned}\gamma_{\mathrm{b}}^{\mathrm{PC}} = {} & p_{\mathrm{b}}\alpha \frac{\|\mathbf{h}_{\mathrm{b}}\|_2^2}{\left(T_{\mathrm{th}}^2 + 2 + T_{\mathrm{th}}^2 \big/ \left(\sigma_A^2\right)^2\right)} + p_{\mathrm{b}}(1-\alpha)\frac{\phi P_{\mathrm{t}}\|\mathbf{h}_{\mathrm{b}}\|_2^2}{2\left(\sigma_{n_{\mathrm{b}}}^2 + \sigma_{g_{\mathrm{b}}}^2\right)\left(1 - \frac{\left(\sigma_{n_{\mathrm{b}}}^2 + \sigma_{g_{\mathrm{b}}}^2\right)T_{\mathrm{th}}^2}{2\left(\sigma_A^2\right)^2\left(\alpha^{-1}-1\right)}\right)} \\ & + (1-p_{\mathrm{b}})\beta \frac{\|\mathbf{h}_{\mathrm{b}}\|_2^2}{\left(T_{\mathrm{th}}^2 + 2 + T_{\mathrm{th}}^2 \big/ \left(\sigma_B^2\right)^2\right)} + (1-p_{\mathrm{b}})(1-\beta)\frac{\phi P_{\mathrm{t}}\|\mathbf{h}_{\mathrm{b}}\|_2^2}{2\sigma_{n_{\mathrm{b}}}^2\left(1 - \frac{\sigma_{n_{\mathrm{b}}}^2 T_{\mathrm{th}}^2}{2\left(\sigma_B^2\right)^2\left(\beta^{-1}-1\right)}\right)},\end{aligned} \tag{29}$$

and

$$\begin{aligned}C_{\mathrm{b}}^{\mathrm{PC}} = B\log_2\Bigg[& 1 + p_{\mathrm{b}}\alpha \frac{\|\mathbf{h}_{\mathrm{b}}\|_2^2}{\left(T_{\mathrm{th}}^2 + 2 + T_{\mathrm{th}}^2 \big/ \left(\sigma_A^2\right)^2\right)} + p_{\mathrm{b}}(1-\alpha)\frac{\phi P_{\mathrm{t}}\|\mathbf{h}_{\mathrm{b}}\|_2^2}{2\left(\sigma_{n_{\mathrm{b}}}^2 + \sigma_{g_{\mathrm{b}}}^2\right)\left(1 - \frac{\left(\sigma_{n_{\mathrm{b}}}^2 + \sigma_{g_{\mathrm{b}}}^2\right)T_{\mathrm{th}}^2}{2\left(\sigma_A^2\right)^2\left(\alpha^{-1}-1\right)}\right)} \\ & + (1-p_{\mathrm{b}})\beta \frac{\|\mathbf{h}_{\mathrm{b}}\|_2^2}{\left(T_{\mathrm{th}}^2 + 2 + T_{\mathrm{th}}^2 \big/ \left(\sigma_B^2\right)^2\right)} + (1-p_{\mathrm{b}})(1-\beta)\frac{\phi P_{\mathrm{t}}\|\mathbf{h}_{\mathrm{b}}\|_2^2}{2\sigma_{n_{\mathrm{b}}}^2\left(1 - \frac{\sigma_{n_{\mathrm{b}}}^2 T_{\mathrm{th}}^2}{2\left(\sigma_B^2\right)^2\left(\beta^{-1}-1\right)}\right)}\Bigg].\end{aligned} \tag{30}$$

Because the received signal is not pulse-clipped, the SINR and channel capacity of Eve are the same as in Equations (8) and (9) in Section 3.1.

Furthermore, by substituting Equations (30) and (9) into Equation (10), the secrecy capacity in the adopted L-DACS peak threshold-based pulse clipping-aided PLS method can be provided by

$$\begin{aligned}R_{\mathrm{sec}}^{\mathrm{PC}} = \Bigg\{ B\log_2\Bigg[& 1 + p_{\mathrm{b}}\alpha \frac{\|\mathbf{h}_{\mathrm{b}}\|_2^2}{\left(T_{\mathrm{th}}^2 + 2 + T_{\mathrm{th}}^2 \big/ \left(\sigma_A^2\right)^2\right)} + p_{\mathrm{b}}(1-\alpha)\frac{\phi P_{\mathrm{t}}\|\mathbf{h}_{\mathrm{b}}\|_2^2}{2\left(\sigma_{n_{\mathrm{b}}}^2 + \sigma_{g_{\mathrm{b}}}^2\right)\left(1 - \frac{\left(\sigma_{n_{\mathrm{b}}}^2 + \sigma_{g_{\mathrm{b}}}^2\right)T_{\mathrm{th}}^2}{2\left(\sigma_A^2\right)^2\left(\alpha^{-1}-1\right)}\right)} \\ & + (1-p_{\mathrm{b}})\beta \frac{\|\mathbf{h}_{\mathrm{b}}\|_2^2}{\left(T_{\mathrm{th}}^2 + 2 + T_{\mathrm{th}}^2 \big/ \left(\sigma_B^2\right)^2\right)} + (1-p_{\mathrm{b}})(1-\beta)\frac{\phi P_{\mathrm{t}}\|\mathbf{h}_{\mathrm{b}}\|_2^2}{2\sigma_{n_{\mathrm{b}}}^2\left(1 - \frac{\sigma_{n_{\mathrm{b}}}^2 T_{\mathrm{th}}^2}{2\left(\sigma_B^2\right)^2\left(\beta^{-1}-1\right)}\right)}\Bigg] \\ & - B\log_2\left(1 + \frac{\phi P_{\mathrm{t}}\left(\mathbf{h}_{\mathrm{e}}^T\mathbf{w}\right)^T\left(\mathbf{h}_{\mathrm{e}}^T\mathbf{w}\right)}{\left[(1-\phi)P_{\mathrm{t}}/(N_{\mathrm{t}}-1)\right]\left(\mathbf{h}_{\mathrm{e}}^T\mathbf{T}\right)^T\left(\mathbf{h}_{\mathrm{e}}^T\mathbf{T}\right) + p_{\mathrm{e}}\sigma_{g_{\mathrm{e}}}^2 + \sigma_{n_{\mathrm{e}}}^2}\right)\Bigg\}^{+}.\end{aligned} \tag{31}$$

4. Simulation Results

In this section, based on the theoretical results, we present the results of our simulations evaluating the performance of the proposed comprehensive PLS method with various interference mitigation methods. The main parameters are summarized in Table 2.

First, to show the effects of pulse interference mitigation on L-DACS, we simulate the time domain signals of the system with the peak threshold-based pulse blanking method and peak threshold-based pulse clipping method, as shown in Figures 2 and 3, respectively. The original time domain signals were obtained using the official L-DACS simulation platform [28].

As shown in Figures 2 and 3, the original received L-DACS signal suffers pulse interference from DME, which appears as pulse pairs. With the peak threshold set as $T_{\mathrm{th}} = 3$, both the peak threshold-based pulse blanking method and the peak threshold-based pulse clipping method have significant effects on interference mitigation.

Further, to evaluate the secrecy performance of the L-DACS with the proposed comprehensive PLS method, we simulated the secrecy capacity of the system in the Rician fading channel with three kinds of interference mitigation methods, as shown in Figures 4–8. In each figure, there are five different curves to indicate the five cases. As a benchmark, the green curve with triangle markers indicates the secrecy capacity without any PLS method or any interference mitigation method [27]. To compare the jamming-like PLS method [22], the red curve with hexagram markers indicates the secrecy capacity of the artificial noise-aided L-DACS without interference mitigation, which is calculated according to Equation (11). The pink curve with asterisk markers indicates the secrecy capacity of the ideal pulse blanking-aided PLS method, which is calculated according to Equation (18). The blue curve with circle markers indicates the secrecy capacity of the peak threshold-based pulse blanking-aided PLS method, which is calculated according to Equation (25). The black curve with rhombus markers indicates the secrecy capacity of the peak threshold-based pulse clipping-aided PLS method, which is calculated according to Equation (31).

Table 2. Simulation parameters.

Name of Parameter	Value of Parameter
The number of transmitted antennas, N_t	4
Variance of AWGN of Bob, $\sigma_{n_{\mathrm{b}}}^2$	1
Variance of AWGN of Eve, $\sigma_{n_{\mathrm{e}}}^2$	1
Rician factor of Bob	10
Rician factor of Eve	10
Threshold of interference mitigation, T_{th}	3
Occurring probability of pulse interference of Bob, p_{b}	2×10^{-2}
Occurring probability of pulse interference of Eve, p_{e}	2×10^{-2}
Artificial noise power distribution factor, ϕ	0.5
signal-to-noise ratio, SNR	15 dB
signal-to-interference ratio, SIR	−15 dB

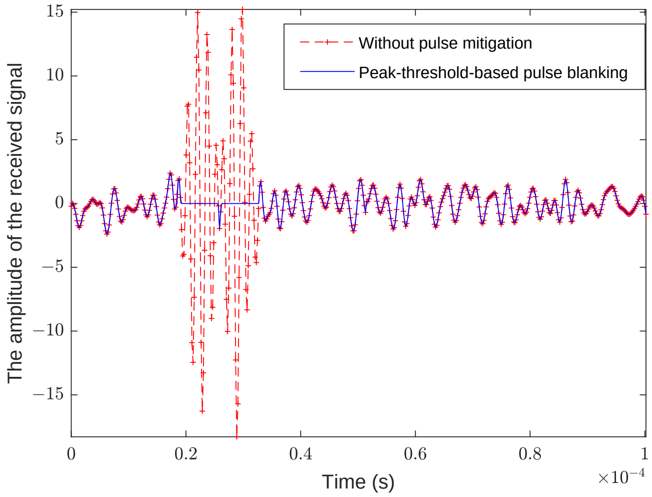

Figure 2. Time domain signal of L-DACS with peak threshold-based pulse blanking method.

Figure 4 shows the secrecy capacity for various SNRs. To depict the impulsive noise, the SIR in L-DACS was set as −15 dB. We assumed the probability of pulse interference occurring to be the same for the channel of the legitimate user and the channel of the eavesdropper, which we set as $p_{\mathrm{b}} = p_{\mathrm{e}} = 2 \times 10^{-2}$. When injecting artificial noise into the transmitted signal, the power distribution factor was $\phi = 0.5$, meaning that half of power is used for useful information transmission and half is used for jamming to achieve security. The threshold values used for the peak threshold-based pulse blanking method and peak threshold-based pulse clipping method were taken to be $T_{\text{th}} = 3$. As a benchmark, we first simulated the secrecy capacity of the L-DACS without artificial noise and without any interference mitigation method. As shown in Figure 4, the secrecy capacity is low for all SNRs, which means that confidential aviation information has a high risk of leakage. After injecting artificial noise into the transmitted signal, the secrecy capacity increases slightly with the increase in SNR, as shown in the right subfigure in Figure 4. To further increase the secrecy capacity by improving the transmission power of the legitimate user, the ideal pulse blanking, peak threshold-based pulse blanking, and peak threshold-based pulse clipping methods were adopted in our simulations. It can be seen that the secrecy capacity increases almost monotonically as the quality of the channel improves. More specifically, with perfect knowledge of the positions of the pulse interference, the ideal pulse blanking method performs best in terms of enhancing the secrecy capacity. For a unit bandwidth, i.e., 1 Hz, the peak threshold-based pulse clipping method performs slightly better than the peak threshold-based pulse blanking method, as the received signal is not totally blanked to zero and information remains for use in the clipping method, as shown in the left subfigure in Figure 4. With a large bandwidth, the advantages of clipping become more obvious.

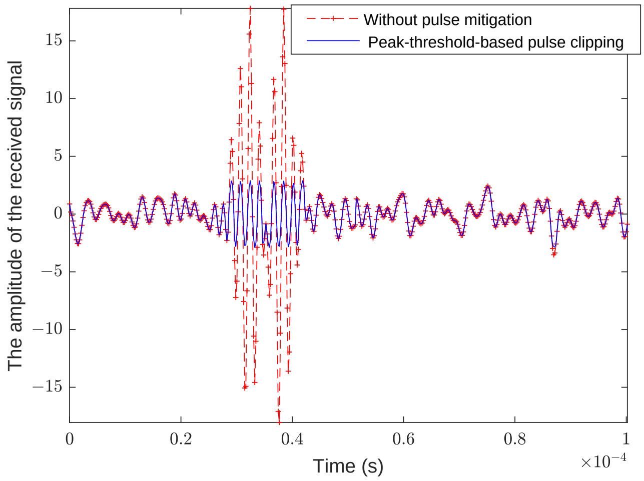

Figure 3. Time domain signal of L-DACS with peak threshold-based pulse clipping method.

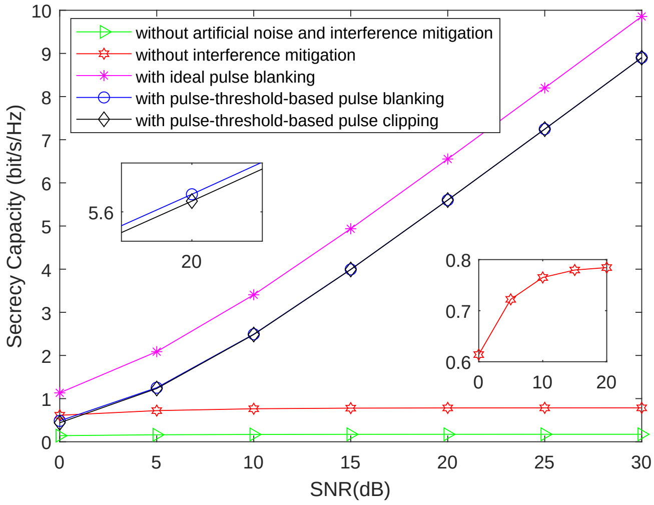

Figure 4. The secrecy capacity obtained by different interference mitigation methods for various SNRs.

Figure 5 shows the effect of the threshold T_{th} on the secrecy capacity. For the case with no pulse interference mitigation and ideal pulse blanking, a change in the threshold has no effect on the secrecy capacity, which is in line with the theoretical analysis in Section 3. In the case where the legitimate receiver adopts peak threshold-based pulse blanking and peak threshold-based pulse clipping, the secrecy capacity is a convex function about the threshold. In detail, as the threshold increases, the secrecy capacity first increases and then decreases, with the secrecy capacity reaching the maximum when the threshold is optimal. In this case, the optimal threshold is 3, which we used in the simulations shown in the subsequent Figures 6–8. in this paper.

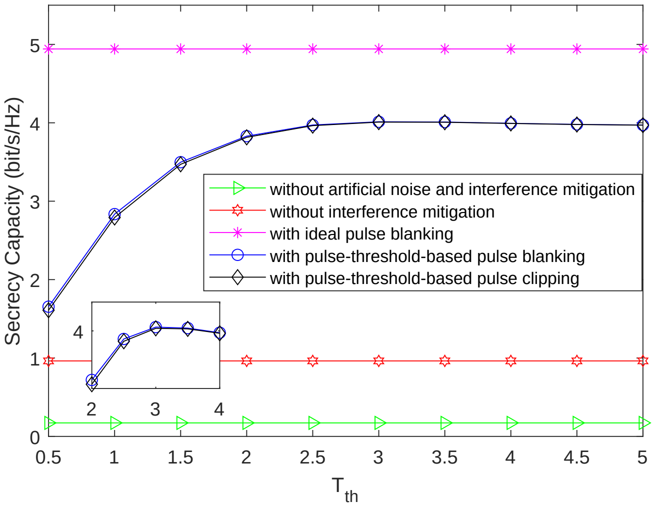

Figure 5. The secrecy capacity obtained withby different interference mitigation methods for various threshold values.

In exploring the effect of different pulse interference levels on the secrecy capacity, we obtained Figures 6 and 7, which respectively present the secrecy capacity for various intensities and various probabilities of pulse interference. In addition, the probability of pulse interference in Figure 6 is $p_{\text{b}} = p_{\text{e}} = 2 \times 10^{-2}$ and the SIR in Figure 7 is -15 dB.

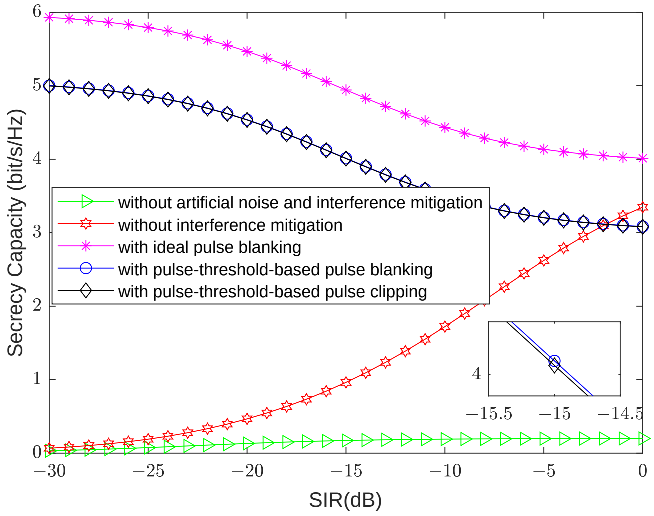

Figure 6. The secrecy capacity obtained with different interference mitigation methods for various SIRs.

As shown in Figures 6 and 7, if no interference mitigation method is used in the artificial noise-aided L-DACS, then the secrecy capacity increases when the SIR increases or when the probability decreases. The reason for this is that for a fixed transmitting power, the pulse interference level decreases either when the SIR increases or when the probability decreases, which provides a relatively good transmission environment. Because the legitimate user is unaffected by the artificial noise, the improvement in the transmission environment has a more obvious effect on Bob's transmission than on Eve's, which helps to enhance the secrecy capacity.

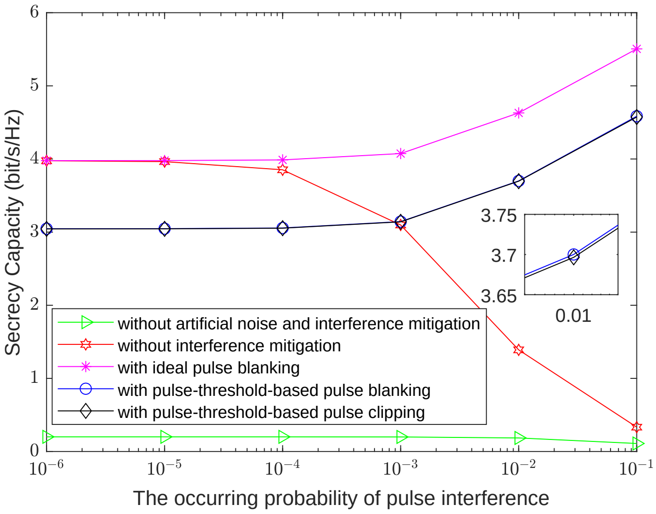

Figure 7. The secrecy capacity obtained with different interference mitigation methods for various probabilities of pulse interference.

Further, when interference mitigation methods are adopted by the legitimate user, the secrecy capacity decreases as the pulse interference level decreases. The reason behind this is that the effect of adopting pulse interference mitigation methods is more obvious when the legitimate receiver suffers serious pulse interference, which corresponds to a smaller SIR and a larger probability of pulse interference. Because the capacity of the legitimate user is improved by interference mitigation while the capacity of the eavesdropper remains the same, an obvious pulse mitigation effect results in a large improvement in the secrecy capacity. In Figures 6 and 7, we find an interesting result in that when the pulse interference level is low enough, the secrecy capacity obtained by peak threshold-based pulse mitigation is smaller than the secrecy capacity without any pulse interference mitigation method. This result is reasonable because in this case the pulse interference is weak and the amplitude of the pulse interference is even smaller than the amplitude of the received signal. When adopting peak threshold-based pulse mitigation, the useful signal of Bob may be blanked or clipped, which has a negative effect on the secrecy capacity. However, this negative effect does not occur in the case where ideal pulse blanking is used, as the receiver with ideal pulse blanking can mitigate the pulse interference precisely without threshold judgment.

Figure 8 demonstrates the secrecy capacity for various artificial noise power distribution factors. As expected, the secrecy capacity is significantly improved by jointly adopting artificial noise and pulse interference mitigation methods. Furthermore, the secrecy capacity obtained by using the ideal pulse blanking method is superior to the secrecy capacity using peak threshold-based mitigation methods. As shown in Figure 8, the secrecy capacity is a convex function of the artificial noise power distribution factor ϕ. In other words, the secrecy capacity first increases and then decreases with an increasing proportion of the jamming power with respect to the total transmitted power. The reason for this is that if the jamming signal is too small, it cannot provide a sufficient guarantee against eavesdropping for the legitimate user, which reduces the secrecy capacity. In contrast, if the jamming signal is too large, it wastes of power resources, which likewise harms the secrecy capacity. The secrecy capacity reaches its maximum when the artificial noise power distribution factor ϕ is optimal, which is about 0.7. Figure 8 shows that the optimal power distribution factor is different when interference mitigation is considered. Hence, it is necessary to analyze the secrecy performance for the L-DACS with artificial noise and pulse interference mitigation jointly taken into consideration.

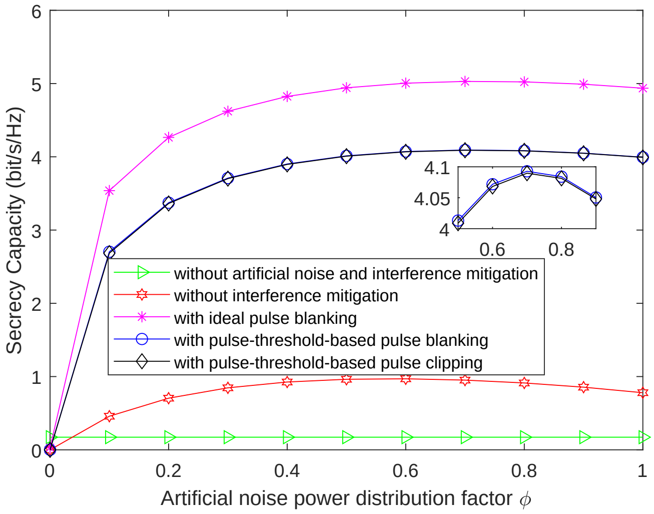

Figure 8. The secrecy capacity obtained by different interference mitigation methods for various artificial noise power distribution factors.

5. Conclusions

In this paper, while jointly considering the impact of potential illegal eavesdropping and high-powered pulse interference caused by DME, we propose a comprehensive PLS method for L-DACS by injecting artificial noise into the transmitted signal and adopting nonlinear interference mitigation. Based on the information theory, we derive the closed-form expressions of the secrecy capacity in four cases: artificial noise-aided L-DACS without interference mitigation, with ideal pulse blanking, with peak threshold-based pulse blanking, and woth peak threshold-based pulse clipping. In simulations, we compared the secrecy capacity in these four cases with various SNRs, threshold values, SIRs, probabilities of pulse interference, and artificial noise power distribution factors. Our simulation results verify that the proposed comprehensive PLS method can effectively improve the security performance of L-DACS, which provides theoretical support and technical reference for future practical aviation communications systems.

Author Contributions: Conceptualization, L.Q.; Methodology, L.Q.; Software, H.X.; Validation, L.W.; Resources, B.S.; Writing—Original draft, H.X.; Writing—Review and editing, L.Q.; Funding acquisition, D.W. and X.L. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded in part by the National Natural Science Foundation of China (62301359) and in part by the Multiple Input Foundation of Tianjin, China (21JCQNJC00770).

Data Availability Statement: Data are contained within the article.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Jacob, P.; Sirigina, R.P.; Madhukumar, A.; Prasad, V.A. Cognitive radio for aeronautical communications: A survey. *IEEE Access* **2016**, *4*, 3417–3443. [CrossRef]
2. Sajatovic, M.; Haindl, B.; Ehammer, M.; Gräupl, T.; Schnell, M.; Epple, U.; Brandes, S. LDACS1 system definition proposal. In *Eurocontrol Study*, 1st ed.; Eurocontrol: Brussels, Belgium, 2009; Volume 1.
3. Schnell, M.; Epple, U.; Shutin, D.; Schneckenburger, N. LDACS: Future aeronautical communications for air-traffic management. *IEEE Commun. Mag.* **2014**, *52*, 104–110. [CrossRef]
4. Sampigethaya, K.; Poovendran, R.; Shetty, S.; Davis, T.; Royalty, C. Future e-enabled aircraft communications and security: The next 20 years and beyond. *Proc. IEEE* **2011**, *99*, 2040–2055. [CrossRef]

5. Mäurer, N.; Bilzhause, A. A cybersecurity architecture for the L-band digital aeronautical communications system (LDACS). In Proceedings of the 2018 IEEE/AIAA 37th Digital Avionics Systems Conference (DASC), London, UK, 23–27 September 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 1–10.
6. Mäurer, N.; Gräupl, T.; Schmitt, C. Evaluation of the LDACS cybersecurity implementation. In Proceedings of the 2019 IEEE/AIAA 38th Digital Avionics Systems Conference (DASC), San Diego, CA, USA, 8–12 September 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 1–10.
7. Epple, U.; Schnell, M. Overview of legacy systems in L-band and its influence on the future aeronautical communication system LDACS1. *IEEE Aerosp. Electron. Syst. Mag.* **2014**, *29*, 31–37. [CrossRef]
8. Schnell, M.; Brandes, S.; Gligorevic, S.; Walter, M.; Rihacek, C.; Sajatovic, M.; Haindl, B. Interference mitigation for broadband L-DACS. In Proceedings of the 2008 IEEE/AIAA 27th Digital Avionics Systems Conference, St. Paul, MN, USA, 26–30 October 2008; IEEE: Piscataway, NJ, USA, 2008; pp. 2.B.2-1–2.B.2-12.
9. Liang, Y.; Poor, H.V.; Shamai, S. Information theoretic security. *Found. Trends® Commun. Inf. Theory* **2009**, *5*, 355–580. [CrossRef]
10. Bilzhause, A.; Belgacem, B.; Mostafa, M.; Graupl, T. Datalink security in the L-band digital aeronautical communications system (LDACS) for air traffic management. *IEEE Aerosp. Electron. Syst. Mag.* **2017**, *32*, 22–33. [CrossRef]
11. Liu, Y.; Yang, Y.; Yang, L.L.; Hanzo, L. Physical Layer Security of Spatially Modulated Sparse-Code Multiple Access in Aeronautical Ad-hoc Networking. *IEEE Trans. Veh. Technol.* **2021**, *70*, 2436–2447. [CrossRef]
12. Passerini, F.; Tonello, A.M. Secure PHY layer key generation in the asymmetric power line communication channel. *Electronics* **2020**, *9*, 605. [CrossRef]
13. Lee, K.; Klingensmith, N.; Banerjee, S.; Kim, Y. Voltkey: Continuous secret key generation based on power line noise for zero-involvement pairing and authentication. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* **2019**, *3*, 1–26. [CrossRef]
14. Yang, F.; Islam, M.A.; Ren, S. PowerKey: Generating secret keys from power line electromagnetic interferences. In Proceedings of the International Conference on Network and System Security, Melbourne, VIC, Australia, 25–27 November 2020; Springer: Berlin, Germany, 2020; pp. 354–370.
15. Henkel, W.; Turjman, A.M.; Kim, H.; Qanadilo, H.K. Common randomness for physical-layer key generation in power-line transmission. In Proceedings of the ICC 2020—2020 IEEE International Conference on Communications (ICC), Dublin, Ireland, 7–11 June 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 1–6.
16. Noura, H.N.; Melki, R.; Chehab, A.; Fernandez, J.H. Efficient and robust data availability solution for hybrid PLC/RF systems. *Comput. Netw.* **2021**, *185*, 107675. [CrossRef]
17. Camponogara, A.; Poor, H.V.; Ribeiro, M.V. Physical layer security of in-home PLC systems: Analysis based on a measurement campaign. *IEEE Syst. J.* **2020**, *15*, 617–628. [CrossRef]
18. Camponogara, Â.; Poor, H.V.; Ribeiro, M.V. PLC systems under the presence of a malicious wireless communication device: Physical layer security analyses. *IEEE Syst. J.* **2020**, *14*, 4901–4910. [CrossRef]
19. Camponogara, Â.; Souza, R.D.; Ribeiro, M.V. The Effective Secrecy Throughput of a Broadband Power Line Communication System Under the Presence of Colluding Wireless Eavesdroppers. *IEEE Access* **2022**, *10*, 85019–85029. [CrossRef]
20. Fernandez, J.H.; Omri, A.; Di Pietro, R. Channel Impulse Response Multilevel Quantization for Power Line Communications. *IEEE Access* **2022**, *10*, 66113–66126. [CrossRef]
21. ElSamadouny, A.; El Shafie, A.; Abdallah, M.; Al-Dhahir, N. Secure sum-rate-optimal MIMO multicasting over medium-voltage NB-PLC networks. *IEEE Trans. Smart Grid* **2016**, *9*, 2954–2963. [CrossRef]
22. Prasad, G.; Taghizadeh, O.; Lampe, L.; Mathar, R. Securing MIMO power line communications with full-duplex jamming receivers. In Proceedings of the 2019 IEEE International Symposium on Power Line Communications and its Applications (ISPLC), Prague, Czech Republic, 3–5 April 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 1–6.
23. Selim, B.; Alam, M.S.; Kaddoum, G.; AlKhodary, M.T.; Agba, B.L. A deep learning approach for the estimation of Middleton class-A Impulsive noise parameters. In Proceedings of the ICC 2020—2020 IEEE International Conference on Communications (ICC), Dublin, Ireland, 7–11 June 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 1–6.
24. Mathur, A.; Bhatnagar, M.R.; Panigrahi, B.K. Performance evaluation of PLC under the combined effect of background and impulsive noises. *IEEE Commun. Lett.* **2015**, *19*, 1117–1120. [CrossRef]
25. Mohan, V.; Mathur, A.; Kaddoum, G. Analyzing Physical-Layer Security of PLC Systems Using DCSK: A Copula-Based Approach. *IEEE Open J. Commun. Soc.* **2022**, *4*, 104–117. [CrossRef]
26. Salem, A.; Hamdi, K.A.; Alsusa, E. Physical Layer Security Over Correlated Log-Normal Cooperative Power Line Communication Channels. *IEEE Access* **2017**, *5*, 13909–13921. [CrossRef]
27. Liu, H.; Zhang, X.; Li, D.; Wang, L. *Interference Mitigation Methods and Performances for L-DACS1 System*; Science Press: Beijing, China, 2016.
28. Für Luft-und Raumfahrt (DLR) Institut für Kommunikation und Navigation, D.Z. Future Aeronautical Communications L-DACS1. Available online: www.ldacs.com (accessed on 30 September 2022).

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.