electronics

MDPI

Article

A Novel Approach for the Enhancement of Security through Defining the Spatial Secrecy Outage Probability in the Industrial Internet of Things

Xiaokai Liu [1], Fangmin Xu [2,*], Lina Ning [2], Chenglin Zhao [2] and Hao Xia [3]

[1] School of Mechanical and Electrical Engineering, Beijing Information Science and Technology University, Beijing 100101, China; liu_xiaokai@bistu.edu.cn
[2] School of Information and Communication Engineering, Beijing University of Posts and Telecommunications, Beijing 100876, China; lnning@bupt.cn (L.N.); clzhao@bupt.edu.cn (C.Z.)
[3] China Mobile Group Design Institute Co., Ltd., Beijing 100036, China; xiahao@cmdi.chinamobile.com
* Correspondence: xufm@bupt.edu.cn

Abstract: The rapid development of the Industrial Internet of Things (IIoT) has brought enormous opportunities to the industrial environment, but has also posed significant challenges to network security, especially physical layer security, which is crucial for the reliable transmission of messages among interconnected devices and sensors. Focusing on enhancing the physical layer security in IIoT communication, this paper proposes a mechanism for the Spatial Secrecy Outage Probability (SSOP) to ensure the secure transmission of data. The SSOP algorithm assumes that the location of legitimate devices is known, while the eavesdropper devices have a random distribution of locations, forming the SSOP model related to the device locations from the perspective of insecure regions (ISRs) and secure regions (SRs), and the closed-form expression for its upper bound is derived. Subsequently, under the constraint of the SSOP conditions, we establish an optimization model with the objective of system throughput maximization based on the Spatial Secrecy Outage Probability (SRM-SSOP). By optimizing the transmission rate of legitimate channels or controlling the transmission power, the maximization of the system throughput can be achieved, thus reducing the consumption of communication resources. Through sophisticated modeling and simulation in MATLAB, we verified the accuracy of the definition and derived the upper bound of the SSOP. The experimental results also show that the SSOP algorithm gradually converges to a specific value as the number of antenna elements increases. In addition, we observed that, when the receiver device is aligned with the normal direction of the transmit antenna array, the SSOP reaches a minimum value. This performance is crucial for understanding and optimizing the security performance of IIoT communication systems.

Keywords: Industrial Internet of Things; physical layer security; wireless communication; spatial secrecy outage probability

check for updates

Citation: Liu, X.; Xu, F.; Ning, L.; Zhao, C.; Xia, H. A Novel Approach for the Enhancement of Security through Defining the Spatial Secrecy Outage Probability in the Industrial Internet of Things. *Electronics* **2024**, *13*, 2356. https://doi.org/10.3390/electronics13122356

Academic Editor: Floriano De Rango

Received: 10 May 2024
Revised: 9 June 2024
Accepted: 14 June 2024
Published: 16 June 2024

Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

Cybersecurity in the Industrial Internet of Things (IIoT) plays a crucial role in overall network security protection. The Industrial Internet of Things connects various industrial equipment and systems, such as factory production lines, warehousing systems, and logistics systems. The security of these devices and systems is a key factor for the stability and reliability of production operations. Cybersecurity measures can prevent malicious attacks or unauthorized access, ensuring that production equipment and systems remain intact and secure [1–3]. The Industrial Internet of Things generates vast amounts of data, including production data, equipment status data, and supply chain data. These data are vital for business decision-making and operational efficiency. Cybersecurity measures protect the confidentiality, integrity, and availability of these data, guarding against data breaches, tampering, or loss [4,5]. Overall, cybersecurity plays a critical role in the Industrial

Internet of Things. Enterprises should prioritize cybersecurity and implement effective measures to protect Industrial Internet of Things systems and data, ensuring stable and reliable production operations.

Typically, the architecture of the Industrial Internet of Things (IIoT) is divided into three fundamental layers: the application layer, the network layer, and the perception layer [6]. The application layer, also known as the business layer, is implemented as the top layer in the IIoT architecture [7]. It receives data transmitted from the network layer and utilizes these data to provide necessary services or operations. The perception layer, also referred to as the sensor layer, is implemented as the bottom layer in the IIoT architecture [8]. It interacts with physical devices and components through smart devices such as RFID tags, sensors, and actuators. The network layer, also known as the transmission layer, is implemented as the middle layer in the IIoT architecture [9]. This layer is responsible for receiving processed information from the perception layer, determining routes, and transmitting data and information to the IIoT hub, devices, and applications via integrated networks. The network layer is crucial in the IIoT architecture because it integrates various devices and communication technologies, such as Bluetooth, WiFi, and long-term evolution (LTE). It facilitates data transmission between different things or applications through interfaces or gateways among heterogeneous networks, using various communication technologies and protocols. In the three-layer architectures, the physical layer is usually involved in the network layer. The physical layer handles the physical characteristics related to the transmission medium, such as the modulation of electrical signals, spectrum utilization, and transmission power control. Physical layer security is essential to prevent direct physical attacks, such as damage, eavesdropping, and tampering with network devices or transmission media. Ensuring the security of the physical layer effectively protects the entire communication system from such attacks [10–12]. This paper focuses on designing physical layer communication mechanisms to reduce the risk of service interruptions caused by physical layer failures or attacks.

The physical layer security is regarded as the first line of defense for Industrial Internet of Things security [13,14]. This is because physical layer security involves the security of infrastructure such as network devices, sensors, and controllers. This infrastructure is the foundation of Industrial Internet of Things operations, and once they are threatened or attacked, it may have a serious impact on the entire network [3,15]. To ensure physical layer security, we need to take a series of measures. Strict control of physical access, protection of equipment, and hardware encryption are very important. This means we need to ensure that only authorized personnel can access and use the related equipment and facilities. By implementing effective authentication mechanisms and access control policies, the risk of unauthorized access can be greatly reduced [16–18]. In contrast, physical layer security, which exploits signal processing techniques to protect wireless transmissions from either passive or active attack from any adversary or malicious users, is becoming an important solution for secure communications [19–23]. For example, by using beamforming technology [24], a legitimate device can gain a better secrecy rate, even if the legitimate channel quality is worse than that of an eavesdropper device [25–27].

There has been much research work on physical layer security in wireless communications [28–37]. Reference [28] employs artificial noise technology (ANT) to assist in transmitting secure signals. By establishing an optimization model that minimizes the secrecy outage probability under the constraint of the secrecy rate, this Reference determines the optimal power allocation ratio between the transmitted signal and the artificial noise. Reference [29] investigates a physical layer security transmission scheme in a MISO system where the cooperative users assist (CUA) send interference. Under the condition that only the statistical information of the eavesdropping channel is known, the study establishes an optimization model with the secrecy rate as the constraint and the secrecy outage probability as the optimization objective. It also analyzes the impact of the quality of the legitimate channel and the number of eavesdroppers on the design of the transmission scheme. Reference [30] proposes an adaptive transmission scheme (ADP), which allows

the legitimate channel rate and secrecy rate to be adjusted dynamically according to the channel state information. This adaptive transmission mechanism maximizes the system's throughput under the constraint of the secrecy outage probability. Because the ADP algorithm can adjust the transmission rate and secrecy rate adaptively based on the channel state information, it achieves a higher system throughput. Overall, one of the effective methods is beamforming, which can achieve the secrecy capacity in multi-input, multi-output (MIMO) systems by enhancing energy in a particular direction and suppressing energy in other directions [38]. Previous works on physical layer security usually assumed the channel state information (CSI) of both the legitimate and eavesdropper channels or only the legitimate channel is perfectly known. In most cases, the eavesdropping user adopts the passive eavesdropping mode; the transmitter cannot attain the CSI or location information of the device Eve's channel. Therefore, many researchers use the security performance measurement index to analyze the security region (SR) or insecure region (ISR) of the system [39–41]. The SR means that Eve in this area cannot correctly decode the received confidential information, and the ISR means that the Eve in this area can correctly decode the received confidential information. The Secrecy Outage Region (SOR) was defined in [39]; it analyzes the geographical regions where secrecy outages may occur. The system security performance of the SOR was further studied by using artificial noise technology. In [40], the vulnerability region (VR) under a zero security rate in multi-hop networks is studied. By minimizing the VR, the number of eavesdropping users was reduced. The compromised secret region (CSR) is defined in [42], and it proposes a secure transmission strategy for the minimum CSR. By numerically approximating the CSR, the optimal location and allocated power of the jammer are calculated, and the minimum CSR under the constraint of the security outage probability is achieved.

This paper mainly studies the classical passive eavesdropping system model in IIoT wireless communications, where the transmitter device (Alice) wishes to transmit to the legitimate device (Bob) in the presence of an eavesdropping device (Eve). Location information has been widely considered in wireless networks [43,44]. This paper mainly studies the scenario in which only Bob's location information is attained by Alice. In this paper, the spatial outage probability (SSOP) is defined as the physical region where uniformly distributed Eve devices cause secrecy outages during a legitimate transmission. Alice adopts beamforming to enlarge the signal-to-noise ratio (SNR) of the device Bob, and the SR created by beamforming is highly related to the location information and array parameters. The simulation results show that the SSOP can be reduced or the area of the SR can be increased by adjusting the antenna parameters or the position of the device Bob. The key contributions of the study are as follows: This paper presents a physical space model under the passive eavesdropping scenario. Based on this model, the spatial outage probability is introduced, and its upper bound closed-form expression is derived. Then, the system throughput with the spatial outage probability as a constraint is studied, and the optimal solution is analyzed. The simulation results indicate that, by defining the spatial outage probability, the security performance of the legitimate users communicating in different regions can be analyzed. Furthermore, the simulation results demonstrate that adjusting the transmission rate of legitimate channels can achieve maximum system throughput.

The remainder of this article is organized as follows. Section 2 provides the system and threat models and an overview of the secure transmission protocols in the IIoT situation. The spatial outage probability is introduced in Section 3. We provide a performance analysis, and the simulation results are discussed in Section 4. In Section 5, the conclusions are given.

Notations: Bold lowercase and uppercase letters represent vectors and matrices, respectively, i.e., $\mathbf{A}$. $(\cdot)^T$ and $(\cdot)^\dagger$ represent the transpose and Hermitian transpose, respectively. The Euclidean norm of a vector or a matrix is denoted by $\|\cdot\|$. The absolute value of a scalar is denoted by $|\cdot|$. $\mathbb{C}^{n\times m}$ represents a complex space of dimension $n \times m$, and $\mathbf{I}_{n\times n}$ denotes an n-by-n identity matrix. $\mathcal{CN}\left(0, \sigma^2\right)$ denotes the distribution of a circularly symmetric complex Gaussian (CSCG) random variable with mean zero and variance σ^2. The distribu-

tion of a Gaussian random variable with zero mean and variance σ^2 is denoted as $\mathcal{N}(0, \sigma^2)$. $P_r(\cdot)$ denotes the probability measure.

2. System Model

As shown in Figure 1, we considered a typical wireless network control system scenario, where a data transmitter controller, Alice, and the legitimate receiver, Bob, need to securely exchange data over wireless channels, while a single-antenna malicious node, Eve, attempts to acquire or disrupt the information transmitted between them via eavesdropping or active attacks. All nodes are assumed to be stationary or slow-moving and communicating in a static IIoT environment, which leads to infrequent variations in the wireless channels. Among these, the transmitter (Alice) is equipped with a uniform linear antenna array with N antennas, where the antenna spacing is the wavelength spacing, i.e., $d = 1/2\lambda$, and the legitimate devices (Bob) and the eavesdropper (Eve) are equipped with a single antenna, respectively. The paper adopts the polar coordinate system, where Alice's location is selected as the origin, Bob's location is denoted as (D_b, θ_b), and Eve's location is denoted as (D_e, θ_e). The paper assumes Alice knows the CSI and the location information of Bob, but the CSI and the location information of Eve are unknown to Alice or Bob. We assumed the legitimate channel (the channel between Alice and Bob) and the eavesdropping channel (the channel between Alice and Eve) are subject to quasi-static Rayleigh fading with an equal block length. As detailed below, the $1 \times N$ legitimate channel and the eavesdropping channel are denoted as follows.

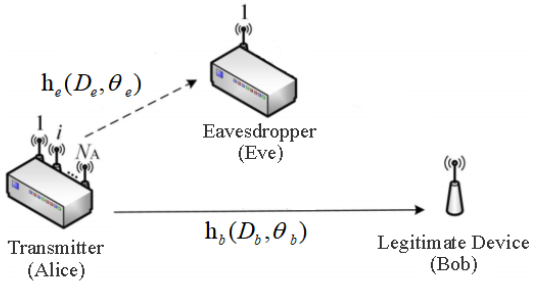

Figure 1. Illustration of IIoT scenario and the geometry of the transmitter, the legitimate device, and the eavesdropper.

$$\begin{aligned} \mathbf{h}_b &= D_b^{-\alpha/2} h_b \mathbf{a}(\theta_b), \\ \mathbf{h}_e &= D_e^{-\alpha/2} h_e \mathbf{a}(\theta_e), \end{aligned} \tag{1}$$

where $h_b \sim \mathcal{CN}(0,1)$, $h_e \sim \mathcal{CN}(0,1)$. α is the path loss exponent. $\mathbf{a}(\theta)$ denotes the array steering vectors, i.e., $\mathbf{a}(\theta) = \left[1, e^{-j2\pi d \sin\theta/\lambda}, \cdots, e^{-j2\pi(n_t-1)d\sin\theta/\lambda}\right]^T, \theta \in (0, 2\pi)$.

In this paper, Eve is a passive eavesdropper; hence, the location of Eve is unknown to Alice. In order to eavesdrop on the secret information, Eve cannot be too far from Alice. This inspired us to propose a circular eavesdropping model as in Figure 1. Eve's location follows a uniform distribution in the circular model [45]:

$$\begin{aligned} D_e^2 &\sim U(0, D_{\max}^2), \\ \theta_e &\sim U(0, 2\pi), \end{aligned} \tag{2}$$

where $U(:,:)$ denotes the uniform distribution and $D_{\max}$ denotes the maximum distance where Eve can eavesdrop on the secret information.

Alice adopts beamforming to transmit information s, and the received signals at Bob and Eve are, respectively, given by:

$$\begin{aligned} y_b &= \sqrt{P_A} D_b^{-\alpha/2} h_b \mathbf{a}^H(\theta_b) \mathbf{w} s + n_b, \\ y_e &= \sqrt{P_A} D_e^{-\alpha/2} h_e \mathbf{a}^H(\theta_e) \mathbf{w} s + n_e, \end{aligned} \tag{3}$$

where P_A is the power budget of Alice, $\mathbf{w} = \mathbf{a}(\theta_b) \Big/ \sqrt{N}$ denotes the beamforming vector, $\mathbb{E}\left[|s|^2\right] = 1$. n_b and n_e, respectively, denote the circularly symmetric complex Gaussian noise, i.e., $n_b \sim \mathcal{CN}\left(0, \sigma_n^2\right)$, $n_e \sim \mathcal{CN}\left(0, \sigma_e^2\right)$. The SNRs of the legitimate channel and eavesdropping channel are given by

$$\begin{aligned} \gamma_b &= \frac{NP_A D_b^{-\alpha} |h_b|^2}{\sigma_n^2}, \\ \gamma_e &= \frac{P_A D_e^{-\alpha} |h_e|^2 G^2(\theta_e, \theta_b)}{\sigma_e^2}, \end{aligned} \tag{4}$$

where $G(\theta_e, \theta_b) = \frac{1}{\sqrt{N}} \sum_{i=1}^{N} e^{j\pi(i-1)(\sin\theta_b - \sin\theta_e)}$.

The channel capacity of Bob and Eve can be given by

$$\begin{aligned} C_b &= \log_2(1 + \gamma_b) = \log_2\left(1 + \frac{NP_A D_b^{-\alpha} |h_b|^2}{\sigma_n^2}\right), \\ C_e &= \log_2(1 + \gamma_e) = \log_2\left(1 + \frac{P_A D_e^{-\alpha} |h_e|^2 G^2(\theta_e, \theta_b)}{\sigma_e^2}\right). \end{aligned} \tag{5}$$

3. Algorithm Design and Implementation

3.1. Spatial Secrecy Outage Probability

When the channel rate of the eavesdropping channel R_e is greater than the channel capacity of the eavesdropping channel C_e, Eve can receive the confidential information and decode it. At this time, the confidential information is leaked to Eve, which is called the secrecy outage. It can be seen that C_e relies on the location of Eve and small-scale fading $\mathbf{h}_e$ from (5); when C_e is higher than a certain threshold, the secrecy outage event can happen. The probability of the secrecy outage event is called the secrecy outage probability (SOP). In this paper, we adopted the insecure region Θ to illustrate the secrecy outage event for the uniformly distributed Eve. Θ is defined by the geometric region where Eve causes the secrecy outage event, as shown in Figure 2. Inside the red dotted lines stands for the insecure region, and outside the region is the secure region. The insecure region Θ can be denoted by

$$\Theta = \{z : C_e > R_b - R_s\}. \tag{6}$$

Substituting (5) into (6), Θ can be further denoted by $\Theta = \{z = (D_e, \theta_e) : D_e < D(\theta_e)\}$, where $D(\theta_e) \leq D_{\max}$ is given by

$$D(\theta_e) = \left[\frac{P_A |h_e|^2 G^2(\theta_e, \theta_b)}{(2^{R_b - R_s} - 1)\sigma_e^2}\right]^{\frac{1}{\alpha}}. \tag{7}$$

Let A be the area of the insecure region. According to the polar coordinate curve area formula, the area of insecure region A can be denoted by

$$\begin{aligned} A &= \frac{1}{2} \int_0^{2\pi} D^2(\theta) d\theta_e \\ &= \frac{1}{2} \int_0^{2\pi} \left[\frac{PG^2(\theta_e, \theta_b)|h_e|^2}{\sigma_e^2(2^{R_b - R_s} - 1)}\right]^{\frac{2}{\alpha}} d\theta_e \\ &= \frac{1}{2} \left[\frac{P|h_e|^2}{\sigma_e^2(2^{R_b - R_s} - 1)}\right]^{\frac{2}{\alpha}} \int_0^{2\pi} \left(G^2(\theta_e, \theta_b)\right)^{\frac{2}{\alpha}} d\theta_e. \end{aligned} \tag{8}$$

A depends on $\left(G^2(\theta_e,\theta_b)\right)^{\frac{2}{\alpha}}$ and $|h_e|^2$. The SSOP can be defined by the probability that Eve is located in Θ on the premise of guaranteeing Bob's reliable transmission. The SSOP, denoted by p_{ssop}, can be given by

$$p_{ssop} = \frac{1}{2\pi D_{\max}^2}\left[\frac{P_A|h_e|^2}{\sigma_e^2(2^{R_b-R_s}-1)}\right]^{\frac{2}{\alpha}} \int_0^{2\pi}\left(G^2(\theta_e,\theta_b)\right)^{\frac{2}{\alpha}} d\theta_e \tag{9}$$

p_{ssop} depends on the equivalent channel factor h_e from (9), and h_e is the random channel fading; hence, we are more interested in the expectation of p_{ssop}. The expectation of p_{ssop} can be denoted by $\bar{p}_{ssop}$ and can be given by

$$\begin{aligned}\bar{p}_{ssop} =& \mathbb{E}_{|h_e|}(p_{ssop}) = \frac{1}{2\pi D_{\max}^2}\left[\frac{P_A\mathbb{E}_{|h_e|}\left[|h_e|^2\right]}{\sigma_e^2(2^{R_b-R_s}-1)}\right]^{\frac{2}{\alpha}} \\ & \int_0^{2\pi}\left(G^2(\theta_e,\theta_b)\right)^{\frac{2}{\alpha}} d\theta_e.\end{aligned} \tag{10}$$

$\bar{p}_{ssop}$ can be further calculated by

$$\begin{aligned}\bar{p}_{ssop} =& \frac{1}{D_{\max}^2}\left[\frac{P_A}{\sigma_e^2(2^{R_b-R_s}-1)}\right]^{\frac{2}{\alpha}} \int_0^{2\pi}\frac{1}{2\pi}\left(G^2(\theta_e,\theta_b)\right)^{\frac{2}{\alpha}} d\theta_e \\ & \int_{-\infty}^{+\infty}|h_e|^{\frac{4}{\alpha}} f\left(|h_e|^2\right) d|h_e|^2.\end{aligned} \tag{11}$$

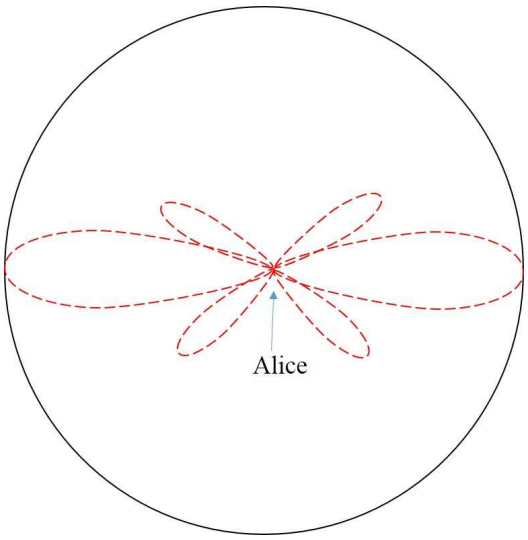

Figure 2. Illustration of the insecure region.

From (11), $\bar{p}_{ssop}$ can be obtained by numerical calculation. But, the closed-form expression cannot be obtained except for the path loss exponent $\alpha = 2$. Therefore, this paper analyzes its upper bound expression $\bar{p}_{ssop}^{up}$. There are two major obstacles to obtain the upper bound expression of $\bar{p}_{ssop}$. The first obstacle is $B_1 = \int_0^{2\pi}\frac{1}{2\pi}\left(G^2(\theta_e,\theta_b)\right)^{\frac{2}{\alpha}} d\theta_e$; the

second obstacle is $B_2 = \int_{-\infty}^{+\infty} |h_e|^{\frac{4}{\alpha}} f\left(|h_e|^2\right) d|h_e|^2$. This paper uses Jensen's Inequality to overcome the two obstacles. Jensen's Inequality is given by

$$\mathbb{E}\left[X^{\frac{2}{\alpha}}\right] \leq (\mathbb{E}[X])^{\frac{2}{\alpha}}. \tag{12}$$

Equality holds when $\alpha = 2$ for any X.

Theorem 1. *$\bar{p}_{ssop}^{up}$ can be derived using (12) and is expressed by*

$$\bar{p}_{ssop}^{up} = \frac{1}{D_{\max}^2}\left[\frac{P_A}{\sigma_e^2(2^{R_b-R_s}-1)}\left(1+2\sum_{n=1}^{n_t-1}\frac{n_t-n}{n_t}J_0(\pi n)\cos(\pi n \sin\theta_b)\right)\right]^{\frac{2}{\alpha}}, \tag{13}$$

where $J_0(\pi n)$ is the Bessel function of the first kind with order zero.

Proof. (1) The first obstacle $B_1 = \int_0^{2\pi} \frac{1}{2\pi}\left(G^2(\theta_e,\theta_b)\right)^{\frac{2}{\alpha}} d\theta_e$.

In the expression B_1, θ_e follows a uniform distribution, i.e., $\theta_e \sim U(0,2\pi)$. The probability density function (PDF) of θ_e is $f(\theta_e) = \frac{1}{2\pi}$. B_1 can be further expressed as

$$B_1 = \int_0^{2\pi} \frac{1}{2\pi}\left(G^2(\theta_e,\theta_b)\right)^{\frac{2}{\alpha}} d\theta_e = \mathbb{E}_{\theta_e}\left[\left(G^2(\theta_e,\theta_b)\right)^{\frac{2}{\alpha}}\right]. \tag{14}$$

According to (12),

$$B_1 \leq \left(\mathbb{E}_{\theta_e}\left[G^2(\theta_e,\theta_b)\right]\right)^{\frac{2}{\alpha}} = \left(\int_0^{2\pi}\frac{1}{2\pi}G^2(\theta_e,\theta_b)d\theta_e\right)^{\frac{2}{\alpha}}. \tag{15}$$

For the inequality, the equality holds when $\alpha = 2$.

For a uniform linear array, the closed-form expression of $\int_0^{2\pi}\frac{1}{2\pi}G^2(\theta_e,\theta_b)d\theta_e$ can be derived by

$$\begin{aligned}
&\int_0^{2\pi}\frac{1}{2\pi}G^2(\theta_e,\theta_b)d\theta_e \\
=&\int_0^{2\pi}\frac{1}{2\pi N}\left(\sum_{i=1}^{n_t} e^{j\pi(i-1)(\sin\theta_b-\sin\theta_e)}\right)^2 d\theta_e \\
=&\int_0^{2\pi}\frac{1}{2\pi N}\sum_{i,j} e^{j\pi(i-j)(\sin\theta_b-\sin\theta_e)}d\theta_e \\
=&\frac{1}{2\pi N}\sum_{i,j} e^{j\pi(i-j)\sin\theta_b}\int_0^{2\pi} e^{-j\pi(i-j)\sin\theta_e}d\theta_e.
\end{aligned} \tag{16}$$

According to the Bessel function of the first kind, i.e., $J_n(x) = \frac{1}{2\pi}\int_{-\pi}^{\pi} e^{j(n\tau - x\sin\tau)}d\tau$, (16) can be further denoted by

$$\int_0^{2\pi}\frac{1}{2\pi}G^2(\theta_e,\theta_b)d\theta_e = \frac{1}{n_t}\sum_{i,j} e^{j\pi(i-j)\sin\theta_b}J_0(\pi(i-j)). \tag{17}$$

According to the relationship between the trigonometric function and exponential function, as well as $J_0(-x) = J_0(x)$, (17) can be further derived as

$$\int_0^{2\pi} \frac{1}{2\pi} G^2(\theta_e, \theta_b) d\theta_e = 1 + 2 \sum_{n=1}^{n_t-1} \frac{n_t - n}{n_t} J_0(\pi n) \cos(\pi n \sin \theta_b). \tag{18}$$

Hence, the upper bound of B_1 is

$$B_1 \leq \left(1 + 2 \sum_{n=1}^{n_t-1} \frac{n_t - n}{n_t} J_0(\pi n) \cos(\pi n \sin \theta_b) \right)^{\frac{2}{\alpha}}. \tag{19}$$

(2) The second obstacle $B_2 = \int_{-\infty}^{+\infty} |h_e|^{\frac{4}{\alpha}} f\left(|h_e|^2\right) d|h_e|^2$.

According to (12), B_2 can be denoted by

$$B_2 = \mathbb{E}\left[\left(|h_e|^2 \right)^{\frac{2}{\alpha}} \right] \leq \left(\mathbb{E}\left[|h_e|^2 \right] \right)^{\frac{2}{\alpha}}. \tag{20}$$

$|h_e|^2$ follows the exponential distribution with parameter 1; therefore, $\mathbb{E}\left[|h_e|^2\right] = 1$. Substituting the results into (18), $B_2 \leq 1$, the equality holds when $\alpha = 2$.

According to the above analysis, the upper bound of the expectation of the SSOP is (13) and $\bar{p}_{ssop} = \bar{p}_{ssop}^{up}$ when $\alpha = 2$.

Thus, the proof is completed. □

3.2. Architectural Design for Maximum Throughput

In a passive eavesdropping system, Alice cannot obtain the channel state information (CSI) of the eavesdropping channel. To prevent the leakage of confidential information, an appropriate transmission scheme needs to be designed. In this paper, we designed a secure transmission scheme with the optimization objective of maximizing the system throughput. In this paper, we study secure transmission schemes under non-adaptive coding transmission, which refers to a communication method where the coding scheme used for data transmission is fixed and does not change in response to varying conditions of the communication channel. The system throughput η can be described as:

$$\eta = p_{tx} \times R_s \tag{21}$$

where p_{tx} is the legitimate channel transmission probability and R_s is the secrecy rate; for the non-adaptive coding transmission, we set R_b as the legitimate channel transmission rate, and we need to find the best R_b to obtain the maximum system throughput. To ensure the reliability of data transmission over the legitimate channel, p_{tx} is defined as:

$$p_{tx}(\mu) = P_r(\gamma_b \geq \mu) = \exp(-\mu/\gamma_b) \tag{22}$$

where μ is the receiver signal-to-noise ratio threshold. To achieve reliable data transmission, $p_{tx}(\mu)$ needs to be greater than a certain threshold δ, that is $p_{tx}(\mu) \geq \delta$. To prevent confidential information from being eavesdropped, $\bar{p}_{ssop}(R_b, R_s) \leq \varepsilon$; to achieve secure transmission, the secrecy rate needs to be greater than 0, $R_s \geq 0$, and we can find the best η as follows:

$$\begin{aligned} &\underset{R_b, R_s, \mu}{MAX} \quad \eta \\ &s.t. C_1 : C_b \geq R_b \\ &\quad C_2 : p_{tx}(\mu) \geq \delta \\ &\quad C_3 : \bar{p}_{ssop}(R_b, R_s) \leq \varepsilon \\ &\quad C_4 : R_s \geq 0 \end{aligned} \tag{23}$$

Based on the above analysis, the optimization objective function η is converted into a single-variable function.

$$\eta = \left(R_b - \log_2(1 + \frac{P_A}{\sigma_e^2}(\frac{B_1}{D_{\max}^2})^{\frac{\alpha}{2}}) \right) \exp(-(2^{R_b} - 1)/\gamma_b) \quad (24)$$

where $B_1 = \left(1 + 2\sum_{n=1}^{n_t-1} \frac{n_t - n}{n_t} J_0(\pi n) \cos(\pi n \sin\theta_b)\right)^{\frac{2}{\alpha}}$

4. Simulation Results

In this section, we further provide numerical results to validate our theoretical analysis. Without loss of generality, the simulation parameters were set as follows in MATLAB R2020b for WIN10. The Computer Configuration was as follows: the Processor (CPU) was an Intel(R) Core(TM) i7-10750H CPU @ 2.60 GHz; the Clock Speed was 2.59 GHz; the Memory (RAM) was 1024 GB with an NVIDIA GeForce GTX 1650 Ti. We set the path loss index α to be 2, and the simulation results were derived from 10,000 Monte Carlo experiments. The power budget P_A at Alice was 30 dBm, and the number of antennas was 8, i.e., $N = 8$. D_b is the distance between Alice and Bob, the default value being 10 m; $D_{\max}$ is the maximum distance between Alice and Eve, set to 50 m; R_b is the legal channel transmission rate, and the initial value was 4 bits/s/Hz; ε is the SSOP threshold, and the setpoint was 0.1; δ is the legitimate user reception probability threshold, set to 0.9; θ_b is the incident angle, and initial value was 0°; simultaneously, the noise power σ_b^2 was 30 dBm; η stands for the system throughput.

4.1. The Impact of Different Parameters on the Averaged SSOP

4.1.1. The Impact of the Averaged SSOP versus Bob's Different Values of θ_b

In Figure 3, we analyze the relationship between Bob's different values of θ_b and $\bar{p}_{ssop}$; from the simulation result, we can conclude that there is a slight oscillation at the beginning; the underlying reason lies in the influence of Alice's signal. With the increase of θ_b, the overall trend of $\bar{p}_{ssop}$ also increases. Therefore, when Bob is located in the normal direction of the antenna array being the direction of Alice, the results work perfectly. The root cause is when $\theta_b = 0°$. The antenna array has the narrowest beam width; at this point, the leakage of information is minimized, also making $\bar{p}_{ssop}$ minimal. Therefore, when the azimuth angle of legitimate users is known, the system's security performance can be improved by adjusting the direction of the antenna array. The Figure 3 shows the theoretical analysis results and numerical simulation results plotted on a curve graph, from which it can be observed that the two curves exhibit a good level of alignment. Furthermore, it further substantiates the theoretical analysis of results mentioned earlier.

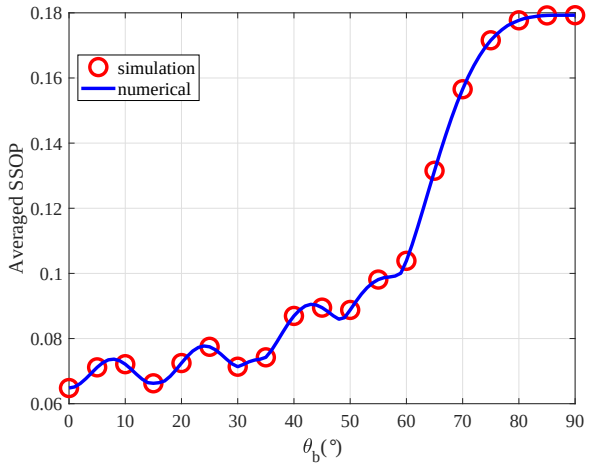

Figure 3. The impact of the averaged SSOP versus Bob's different values of θ_b.

4.1.2. The Averaged SSOP $\bar{p}_{ssop}$ versus the Different Value of N

In Figure 4, we plot the averaged SSOP, $\bar{p}_{ssop}$, versus different values of N for various $\theta_b = 0°, 30°, 60°$ for $D_b = 20$ m, $D_{max} = 50$ m. It can be seen from the figure that, for different θ_b, $\bar{p}_{ssop}$ fluctuates at a different rate. This fluctuation is caused by $B_1 = \left(1 + 2\sum_{n=1}^{n_t-1} \frac{n_t-n}{n_t} J_0(\pi n) \cos(\pi n \sin\theta_b)\right)^{\frac{2}{\alpha}}$. With the increase of N, $\bar{p}_{ssop}$ approaches a fixed value. Therefore, we can conclude that the system security performance does not always increase with the increase of the number of antennas. From this figure, the SSOP is minimum when $\theta_b = 0°$; this is because, when Bob is in the normal direction of the antenna array, more confidential information will be in the main lobe range of the transmitting beam. In practical communication systems, if the direction of the antenna array is adjustable, we can adjust the antenna array to align with Bob's normal direction. At this point, the system's security performance is optimized.

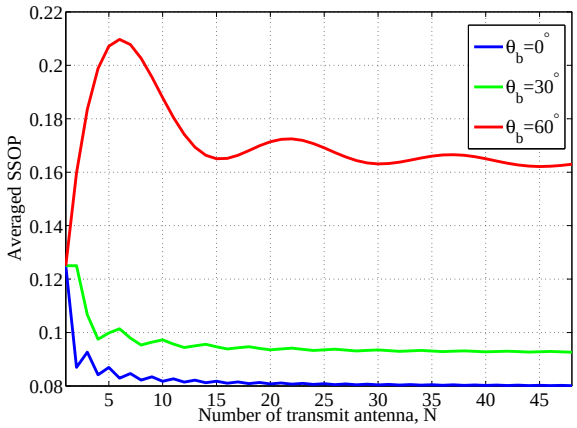

Figure 4. The averaged SSOP $\bar{p}_{ssop}$ versus different values of N.

4.1.3. The Averaged SSOP $\bar{p}_{ssop}$ versus Different Values of θ_b and D_b

In Figure 5, we plot the averaged SSOP, $\bar{p}_{ssop}$, versus different values of θ_b and D_b for $D_{max} = 50$ m. From the three-dimensional figure, we can see $\bar{p}_{ssop}$ when Bob is located in different places on the premise of Alice's location being selected as the origin. The region can be divided into three areas: the absolutely safe zone ($\bar{p}_{ssop} = 0$), the relatively safe zone ($\bar{p}_{ssop} < \varepsilon$), and the danger zone ($\bar{p}_{ssop} > \varepsilon$), where ε denotes a predefined probability value. From this figure, $\bar{p}_{ssop}$ grows with the increase of θ_b and D_b. When Bob is in the normal vector direction of the antenna array, the safety performance of the system is the best.

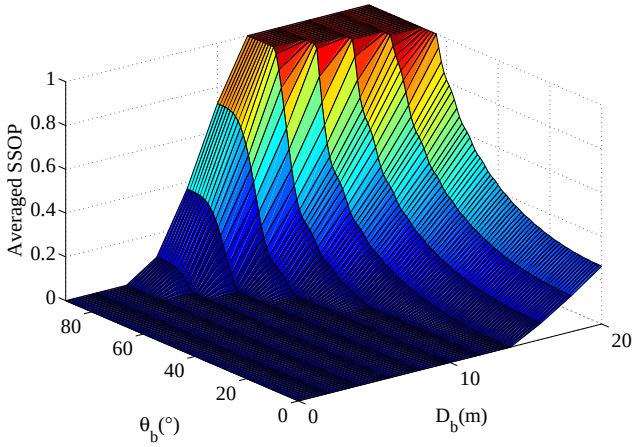

Figure 5. The averaged SSOP $\bar{p}_{ssop}$ versus different values of θ_b and D_b.

4.1.4. The Averaged SSOP $\bar{p}_{ssop}$ versus Different Values of θ_b and R_b

In Figure 6, we plot the averaged SSOP, $\bar{p}_{ssop}$, versus different values of θ_b and R_b for $D_{max} = 50$ m, $D_b = 50$ m. It can be seen from the figure that, when Bob is located in the normal direction of the transmitting antenna array, a larger legal channel rate R_b can be obtained under the same spatial outage probability constraint. Therefore, in the actual environment, the direction of the antenna array can be adjusted to Bob's normal direction to improve the safety performance of the system.

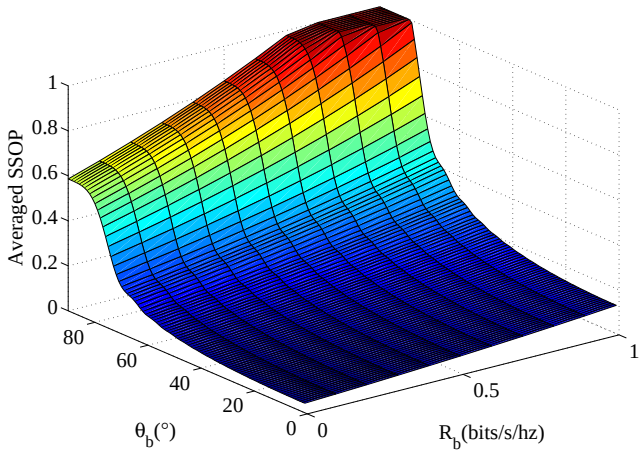

Figure 6. The averaged SSOP $\bar{p}_{ssop}$ versus different values of θ_b and R_b.

4.2. The Relationship Between System Throughput versus Different Parameters

4.2.1. The Relationship Between System Throughput versus the Legitimate Channel Transmission Rate

The relationship between system throughput η and the legitimate channel transmission rate R_b is excellently illustrated in Figure 7. In this experimental section, the present study posits the following assumptions: In this section, an exploration is conducted into a non-adaptive coding transmission scheme, wherein the transmission rate of the legitimate channel remains invariant throughout the data transmission process. The graphical representation reveals a non-linear relationship between system throughput η and the legitimate channel transmission rate R_b, exhibiting an initial ascent followed by a subsequent decline. This observed trend aligns with the anticipated variations derived from the theoretical analysis. In practical communication scenarios, if the legitimate users have knowledge of the channel information, it becomes possible to strategically design the optimal transmission rate based on theoretical insights, aiming to attain the highest achievable system throughput. The graphical representation illustrates that the maximum value η is attained when Bob is positioned along the normal direction of the antenna array. This observation serves as additional validation for the analytical findings concerning the Spatial Secrecy Outage Probability (SSOP). Specifically, it underscores that the system's security performance is optimized when Bob is aligned with the normal direction of the transmitting antenna array.

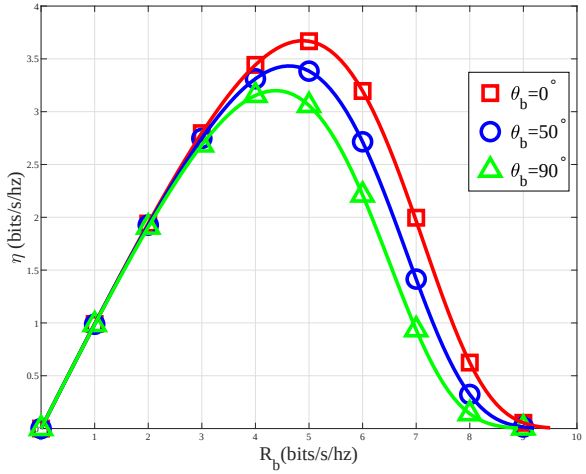

Figure 7. The system throughput η versus the legitimate channel transmission rate R_b.

4.2.2. The Relationship Between System Throughput versus Different Transmission Power Levels

Figure 8 examines the comparative performance of system throughput η under varying transmit power P_A conditions. The graphical representation indicates a positive correlation between increasing transmit power P_A and system throughput η, reaching a gradual convergence towards a stable value. Consequently, the findings suggest that transmit power is not a limiting factor impeding the augmentation of system throughput. The figure also analyzes the comparative relationship between the system-throughput-optimization scheme under the proposed system SRM-SSOP algorithm conditions and the other existing methods, the adaptive transmission mechanism (ADP) based on [30], artificial noise technology (ANT) [28], and cooperative users assist (CUA) [29]. We can conclude the following: 1. The CUA algorithm can obtain a better results when the power P_A is lower, because at lower power, through user cooperation, different users transmit the same signal to the receiver, effectively countering channel fading and improving transmission reliability and stability. User cooperation can increase the difficulty for eavesdroppers by using distributed transmission and encryption techniques, enhancing communication security. 2. The ADP transmission mechanism is an adaptive transmission scheme where the legitimate channel rate and secrecy rate can be dynamically adjusted based on channel state information. Operating under the constraint of secrecy outage probability, this mechanism aims to maximize system throughput. Due to the adaptive adjustment of the transmission rate and secrecy rate according to channel state information, the ADP algorithm can achieve higher system throughput. 3. The ANT algorithm also can obtain excellent results. Artificial noise can be used to interfere with eavesdroppers' reception, making it difficult for them to decode useful information, thus enhancing communication security. 4. From the simulated data, it is apparent that, under strict outage probability constraints ($\varepsilon = 0.1$), the presented approach in this paper exhibits superior performance compared to the optimization scheme based on other algorithms at elevated transmit power levels ($P_A > 50$ dBm), while in scenarios with lower transmit power, the system performance based on the SRM-SSOP may be suboptimal compared to the CUA, ADP, and ANT. 5. The complexity of the algorithms must be fully considered, and the one that is more suitable for different application scenarios should be chosen. Based on the analysis in the literature [28–30], we can conclude that the algorithm proposed in this paper is more suitable for practical engineering applications in terms of algorithm complexity.

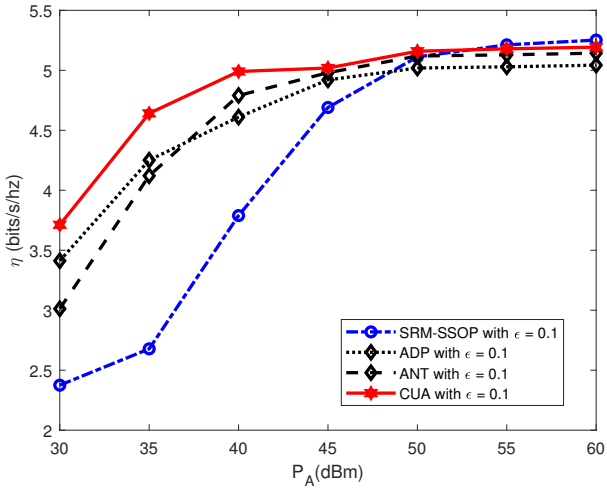

Figure 8. The system throughput η versus the different transmission power levels P_A.

4.2.3. The Relationship Between System Throughput versus Bob's Azimuth Angle

In Figure 9, we analyze the relationship between system throughput η and Bob's azimuth angle θ_b. Due to the symmetry of the function $G(\theta_e, \theta_b)$ with respect to angle $\pm(\theta_b \pm \pi)$, based on the uniform linear array's symmetry, we only investigate the case of $\theta_b \in [0, \pi/2]$. From the algorithmic analysis earlier, we can deduce that θ_b and η exhibit a decreasing trend. The graph illustrates a notable alignment between the simulation results and theoretical analysis, further affirming the correctness of the theoretical analysis. The graphical representation clearly indicates that the system throughput is maximized when $\theta_b = 0$, corresponding to Bob's alignment with the normal direction of the transmitting antenna array. In this configuration, the main lobe beam is the narrowest, leading to minimal information leakage. Consequently, with the flexibility of an adjustable antenna direction, optimizing system the throughput can be achieved by aligning the antenna array direction when Bob's position is known.

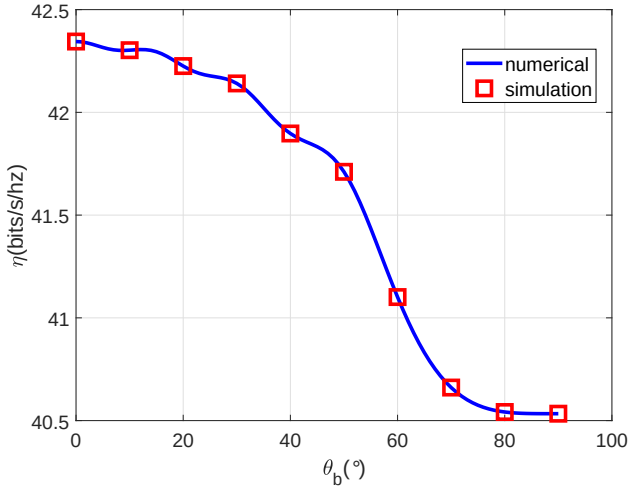

Figure 9. The system throughput η versus Bob's different values of θ_b.

5. Conclusions

In this article, we designed a wireless protocol called the Spatial Secrecy Outage Probability (SSOP) for the IIoT environment to assess the security performance of a system where Alice communicates with Bob in the presence of a uniformly distributed eavesdropper, Eve. First, we mathematically defined the insecure region based on the secrecy outage event.

Then, we defined the SSOP by analyzing this insecure region and derived its upper bound. We conducted a performance analysis to demonstrate the advantages of our proposed scheme over other benchmarks in terms of the system throughput, the secure transmission rate, and robustness against eavesdropping and active attacks. Numerical simulations confirmed the accuracy of our analysis and illustrated the impact of various system parameters on security performance. From our findings, we concluded that the Spatial Secrecy Outage Probability is a crucial indicator for evaluating the security performance of wireless communication systems in the Industrial Internet of Things environment. It provides valuable insights into the security performance of communication systems. By studying the variation patterns and influencing factors of the SSOP, we can better guide the design and optimization of communication systems, thereby enhancing system security.

Author Contributions: Validation, L.N.; Investigation, H.X.; Writing—original draft, X.L.; Writing—review and editing, F.X.; Supervision, C.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Beijing Information Science and Technology University Research Fund (Grant Number: 2023XJJ02).

Data Availability Statement: The data that support the findings of this study are available from the corresponding author upon reasonable request.

Conflicts of Interest: Author Hao Xia was employed by the company China Mobile Group Design Institute Co., Ltd. The remaining authors declare that they have no conflicts of interest related to this work. This research was funded by Beijing Information Science and Technology University Research Fund (Grant Number: 2023XJJ02). The decision to submit this report for publication was made solely by the authors, and the sponsors had no involvement in this decision-making process.

References

1. Liu, Y.; Chi, C.; Zhang, Y.; Tang, T. Identification and Resolution for Industrial Internet: Architecture and Key Technology. *IEEE Internet Things J.* **2022**, *9*, 16780–16794. [CrossRef]
2. Serror, M.; Hack, S.; Henze, M.; Schuba, M.; Wehrle, K. Challenges and Opportunities in Securing the Industrial Internet of Things. *IEEE Trans. Ind. Inform.* **2021**, *17*, 2985–2996. [CrossRef]
3. Mcginthy, J.M.; Michaels, A.J. Secure Industrial Internet of Things Critical Infrastructure Node Design. *IEEE Internet Things J.* **2019**, *6*, 8021–8037. [CrossRef]
4. Yao, P.; Yan, B.; Yang, T.; Wang, Y.; Yang, Q.; Wang, W. Security-Enhanced Operational Architecture for Decentralized Industrial Internet of Things: A Blockchain-Based Approach. *IEEE Internet Things J.* **2024**, *11*, 11073–11086. [CrossRef]
5. Ud Din, I.; Bano, A.; Awan, K.A.; Almogren, A.; Altameem, A.; Guizani, M. LightTrust: Lightweight Trust Management for Edge Devices in Industrial Internet of Things. *IEEE Internet Things J.* **2023**, *10*, 2776–2783. [CrossRef]
6. Yousuf, T.; Mahmoud, R.; Aloul, F.; Zualkernan, I. Internet of Things (IoT) Security: Current Status, Challenges and Countermeasures. *Int. J. Inf. Secur. Res. (IJISR)* **2015**, *5*, 608–616. [CrossRef]
7. Al-Fuqaha, A.; Guizani, M.; Mohammadi, M.; Aledhari, M.; Ayyash, M. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE Commun. Surv. Tutorials* **2015**, *17*, 2347–2376. [CrossRef]
8. Kokoris-Kogias, E.; Voutyras, O.; Varvarigou, T. TRM-SIoT: A scalable hybrid trust and reputation model for the social Internet of Things. In Proceedings of the IEEE International Conference on Emerging Technologies and Factory Automation, Berlin, Germany, 6–9 September 2016. [CrossRef]
9. Lin, J.; Yang, X.; Yu, W.; Fu, X. Towards Effective En-Route Filtering against Injected False Data in Wireless Sensor Networks. In Proceedings of the Global Telecommunications Conference, Houston, TX, USA, 5–9 December 2011. [CrossRef]
10. Suo, H.; Wan, J.; Zou, C.; Liu, J. Security in the Internet of Things: A Review. In Proceedings of the 2012 International Conference on Computer Science and Electronics Engineering, Hangzhou, China, 23–25 March 2012. [CrossRef]
11. Mukherjee, A. Physical-Layer Security in the Internet of Things: Sensing and Communication Confidentiality Under Resource Constraints. *Proc. IEEE* **2015**, *103*, 1747–1761. [CrossRef]
12. Ji, Z.; Yeoh, P.L.; Chen, G.; Zhang, J.; Zhang, Y.; He, Z.; Yin, H.; Li, Y. Physical-Layer-Based Secure Communications for Static and Low-Latency Industrial Internet of Things. *IEEE Internet Things J.* **2022**, *9*, 18392–18405. [CrossRef]
13. Lipps, C.; Herbst, J.; Klingel, S.; Franke, L.; Wolff, A.; Rüb, M.; Reddy, R.; Rahm, M.; Schotten, H.D. Connectivity in the era of the (I) IoT: About security, features and limiting factors of reconfigurable intelligent surfaces. *Discov. Internet Things* **2023**, *3*, 16. [CrossRef]
14. Yu, S.; Wu, F.; Chen, B.; Cao, R.; Yang, Z.; Li, K. A parallel game model-based intrusion response system for cross-layer security in industrial internet of things. *Concurr. Comput. Pract. Exp.* **2023**, *35*, e7826. [CrossRef]

15. Chen, H.; Hu, M.; Yan, H.; Yu, P. Research on industrial internet of things security architecture and protection strategy. In Proceedings of the 2019 International Conference on Virtual Reality and Intelligent Systems (ICVRIS), Jishou, China, 14–15 September 2019; pp. 365–368. [CrossRef]
16. Islam, S.N.; Baig, Z.; Zeadally, S. Physical layer security for the smart grid: Vulnerabilities, threats, and countermeasures. *IEEE Trans. Ind. Inform.* **2019**, *15*, 6522–6530. [CrossRef]
17. Xu, L. Secure transmission strategy of network communication layer relay based on satellite transmission. In Proceedings of the 2020 2nd International Conference on Information Technology and Computer Application (ITCA), Guangzhou, China, 18–20 December 2020; pp. 268–271. [CrossRef]
18. Nguyen, H.N.; Nguyen, N.L.; Nguyen, N.T.; Le, A.T.; Ha, N.D.X.; Do, D.T.; Voznak, M. Reliable and secure transmission in multiple antennas hybrid satellite-terrestrial cognitive networks relying on NOMA. *IEEE Access* **2020**, *8*, 215044–215056. [CrossRef]
19. Liu, M.; Liu, Z.; Lu, W.; Chen, Y.; Gao, X.; Zhao, N. Distributed few-shot learning for intelligent recognition of communication jamming. *IEEE J. Sel. Top. Signal Process.* **2021**, *16*, 395–405. [CrossRef]
20. Liu, M.; Wang, J.; Zhao, N.; Chen, Y.; Song, H.; Yu, F.R. Radio frequency fingerprint collaborative intelligent identification using incremental learning. *IEEE Trans. Netw. Sci. Eng.* **2021**, *9*, 3222–3233. [CrossRef]
21. Liu, M.; Liu, C.; Li, M.; Chen, Y.; Zheng, S.; Zhao, N. Intelligent passive detection of aerial target in space-air-ground integrated networks. *China Commun.* **2022**, *19*, 52–63. [CrossRef]
22. Zhang, Y.; Woods, R.; Ko, Y.; Marshall, A.; Zhang, J. Security Optimization of Exposure Region-Based Beamforming with a Uniform Circular Array. *IEEE Trans. Commun.* **2018**, *66*, 2630–2641. [CrossRef]
23. Zhang, Y.; Ko, Y.; Woods, R.; Marshall, A. Defining Spatial Secrecy Outage Probability for Exposure Region-Based Beamforming. *IEEE Trans. Wirel. Commun.* **2017**, *16*, 900–912. [CrossRef]
24. Li, B.; Zhou, Z.; Zou, W.; Sun, X.; Du, G. On the efficient beam-forming training for 60GHz wireless personal area networks. *IEEE Trans. Wirel. Commun.* **2013**, *12*, 504–515. [CrossRef]
25. Bashar, B.S.; Rhazali, Z.; Elwi, T.A.; Misran, H.; Ismail, M.M.; Mahdi, M.; Alanssari, A.I. Antenna Beam forming Technology Based Enhanced Metamaterial Superstrates. In Proceedings of the 2022 IEEE 3rd KhPI Week on Advanced Technology (KhPIWeek), Kharkiv, Ukraine, 3–7 October 2022; pp. 1–5. [CrossRef]
26. Xiong, Q.; Gong, Y.; Liang, Y.C.; Li, K.H. Achieving secrecy of MISO fading wiretap channels via jamming and precoding with imperfect channel state information. *IEEE Wirel. Commun. Lett.* **2014**, *3*, 357–360. [CrossRef]
27. Barb, G.; Otesteanu, M. Digital GoB-based Beamforming for 5G communication systems. In Proceedings of the 2020 International Symposium on Antennas and Propagation (ISAP), Osaka, Japan, 25–28 January 2021; pp. 469–470. [CrossRef]
28. Wang, B.; Mu, P.; Li, Z. Artificial-Noise-Aided Beamforming Design in the MISOME Wiretap Channel Under the Secrecy Outage Probability Constraint. *IEEE Trans. Wirel. Commun.* **2017**, *16*, 7207–7220. [CrossRef]
29. Hu, L.; Wen, H.; Wu, B.; Tang, J.; Pan, F.; Liao, R.F. Cooperative-Jamming-Aided Secrecy Enhancement in Wireless Networks With Passive Eavesdroppers. *IEEE Trans. Veh. Technol.* **2018**, *67*, 2108–2117. [CrossRef]
30. Li, Z.; Mu, P.; Li, Z.; Zhang, W.; Zhang, Y. An Adaptive Transmission Scheme for Slow Fading Wiretap Channel with Channel Estimation Errors. In Proceedings of the IEEE Globecom 2016, Washington, DC, USA, 4–8 December 2016. [CrossRef]
31. Talak, R.; Karaman, S.; Modiano, E. Improving age of information in wireless networks with perfect channel state information. *IEEE/ACM Trans. Netw.* **2020**, *28*, 1765–1778. [CrossRef]
32. Shi, W.; Pang, S.; Zhang, W. Linear shrinkage receiver for slow fading channels under imperfect channel state information. In Proceedings of the 2022 IEEE Information Theory Workshop (ITW), Mumbai, India, 1–9 November 2022; pp. 338–343. [CrossRef]
33. Xie, R.; Tang, Q.; Liang, C.; Yu, F.R.; Huang, T. Dynamic computation offloading in IoT fog systems with imperfect channel-state information: A POMDP approach. *IEEE Internet Things J.* **2020**, *8*, 345–356. [CrossRef]
34. Yilmaz, B.B.; Prvulovic, M.; Zajić, A. Electromagnetic side channel information leakage created by execution of series of instructions in a computer processor. *IEEE Trans. Inf. Forensics Secur.* **2019**, *15*, 776–789. [CrossRef]
35. Niu, H.; Xiao, Y.; Lei, X.; Wang, G.; Xiao, M.; Mumtaz, S. When the CSI from Alice to Bob is Unavailable: What Can Eve Do to Eliminate the Artificial Noise? In Proceedings of the 2022 IEEE 96th Vehicular Technology Conference (VTC2022-Fall), London, UK, 26–29 September 2022; pp. 1–5. [CrossRef]
36. Xia, G.; Lin, Y.; Liu, T.; Shu, F.; Hanzo, L. Transmit antenna selection and beamformer design for secure spatial modulation with rough CSI of Eve. *IEEE Trans. Wirel. Commun.* **2020**, *19*, 4643–4656. [CrossRef]
37. Chen, Y.; Zhu, G.; Xu, J. Over-the-air computation with imperfect channel state information. In Proceedings of the 2022 IEEE 23rd International Workshop on Signal Processing Advances in Wireless Communication (SPAWC), Oulu, Finland, 4–6 July 2022; pp. 1–5. [CrossRef]
38. Mukherjee, A.; Fakoorian, S.A.A.; Huang, J.; Swindlehurst, A.L. Principles of Physical Layer Security in Multiuser Wireless Networks: A Survey. *IEEE Commun. Surv. Tutorials* **2014**, *16*, 1550–1573. [CrossRef]
39. Wang, J.; Lee, J.; Wang, F.; Quek, T. Jamming-Aided Secure Communication in Massive MIMO Rician Channels. *IEEE Trans. Wirel. Commun.* **2015**, *14*, 6854–6868. [CrossRef]
40. Sarma, S.; Shukla, S.; Kuri, J. Joint scheduling & jamming for data secrecy in wireless networks. In Proceedings of the International Symposium on Modeling & Optimization in Mobile, Tsukuba Science City, Japan, 13–17 May 2013.

41. Zheng, T.X.; Wang, H.M.; Yin, Q. On Transmission Secrecy Outage of a Multi-Antenna System with Randomly Located Eavesdroppers. *IEEE Commun. Lett.* **2014**, *18*, 1299–1302. [CrossRef]
42. Hao, L.; Wang, X.; Hou, W. Security enhancement in cooperative jamming using compromised secrecy region minimization. In Proceedings of the Information Theory, Toronto, ON, Canada, 18–21 June 2013. [CrossRef]
43. Yan, S.; Malaney, R.; Nevat, I.; Peters, G.W. Optimal Information-Theoretic Wireless Location Verification. *IEEE Trans. Veh. Technol.* **2014**, *63*, 3410–3422. [CrossRef]
44. Yan, S.; Malaney, R.; Nevat, I.; Peters, G.W. Signal strength based wireless location verification under spatially correlated shadowing. In Proceedings of the 2014 IEEE International Conference on Communications (ICC), Sydney, Australia, 10–14 June 2014; pp. 2617–2623. [CrossRef]
45. Yan, S.; Malaney, R. Line-of-sight based beamforming for security enhancements in wiretap channels. In Proceedings of the 2014 International Conference on IT Convergence and Security (ICITCS), Beijing, China, 28–30 October 2014; pp. 1–4. [CrossRef]

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.