

Article

Not peer-reviewed version

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

[Xiaokai Liu](#) , [Fangmin Xu](#) ^{*} , LiNang Ning , Chenglin Zhao , Hao XIA

Posted Date: 13 May 2024

doi: 10.20944/preprints202405.0789.v1

Keywords: Industrial Internet of Things ; Physical Layer Security ; Wireless Communication ; Spatial Secrecy Outage Probability



Preprints.org is a free multidiscipline platform providing preprint service that is dedicated to making early versions of research outputs permanently available and citable. Preprints posted at Preprints.org appear in Web of Science, Crossref, Google Scholar, Scilit, Europe PMC.

Copyright: This is an open access article distributed under the Creative Commons Attribution License which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Article

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

Xiaokai Liu, Fangmin Xu *, LiNa Ning, Chenglin Zhao, Hao Xia

¹ Beijing Information Science and Technology University, Beijing, 100101, China

² Beijing University of Posts and Telecommunications, Beijing, 100876, China

³ China Mobile Group Design Institute Co., Ltd, Beijing, 100036, China

* 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 the physical layer security challenges, which is crucial for the reliable transmission of messages interconnected devices and sensors. Focus on the enhancing the physical layer security in the IIoT communication, this paper proposed a mechanism of Spatial Secrecy Outage Probability (SSOP) to ensure the secure transmission of data. The SSOP algorithm assumes that the location of legitimate device is known, while eavesdropper on the random distribution of device locations, forming the SSOP model related to device locations from the perspective of insecure regions (ISR) and secure regions (SR), and deduce the closed-form expression for its upper bound. Subsequently under the constraint of SSOP conditions, establish an optimization model with the objective of system throughput maximization based on Spatial Secrecy Outage Probability (SRM-SSOP). By optimizing the transmission rate of legitimate channels or controlling the transmission power, the maximization of system throughput can be achieved, thus reducing the consumption of communication resources. Through sophisticated modeling and simulation in the MATLAB, we verified the accuracy of the definition and derived upper bound of SSOP. The experimental results also show that 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. These performance are 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

1. Introduction

The cybersecurity in the Industrial Internet of Things (IIoT) plays a crucial role in overall network security protection. The Industrial Internet connects various industrial equipment and systems, such as factory production lines, warehousing systems, and logistics systems. The security of these devices and systems is key factors 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 generates vast amounts of data, including production data, equipment status data, and supply chain data. This data is vital for business decision-making and operational efficiency. Cybersecurity measures protect the confidentiality, integrity, and availability of this 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 systems and data, ensuring stable and reliable production operations.

Typically, the architecture of IIoT is divided into three basic layers [6]: application layer, network layer and perception layer. The application layer It is also known as the business layer, is implemented as the top layer in IIoT architecture [7]. The application layer receives the data transmitted from network layer and uses the data to provide required services or operations. The perception layer is also

known as the sensor layer, is implemented as the bottom layer in IIoT architecture [8]. The perception layer interacts with physical devices and components through smart devices (RFID, sensors, actuators, etc.). The network layer is also known as the transmission layer, is implemented as the middle layer in IoT architecture [9]. The network layer is used to receive the processed information provided by perception layer and determine the routes to transmit the data and information to the IIoT hub, devices, and applications via integrated networks. The network layer is the most important layer in IoT architecture, because various devices, and various communication technologies (Bluetooth, Wi-Fi, long-term evolution, etc.) are integrated in this layer. The network layer should transmit data to or from different things or applications, through interfaces or gateways among heterogeneous networks, and using various communication technologies and protocols. In the Three-Layer Architectures, the Physical Layer is usually involved in the network layer. The Physical Layer is responsible for handling the physical characteristics related to the transmission medium, such as modulation of electrical signals, utilization of the spectrum, and control of transmission power. The physical layer security prevents 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 the impact of such attacks [10–13]. This paper focus on how to design 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 security [14,15]. This is because physical layer security involves the security of infrastructure such as network devices, sensors, and controllers. These infrastructure are the foundation of industrial Internet operations, and once they are threatened or attacked, it may have a serious impact on the entire network [16,17]. 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 related equipment and facilities. By implementing effective authentication mechanisms and access control policies, the risk of unauthorized access can be greatly reduced [18–20]. 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 [21–23]. For example, by using the beam-forming technology [24], the legitimate device can get a better secrecy rate, even if the legitimate channel quality is worse than that of an eavesdropper device [25–27].

There has been a lot of research work on physical layer security in the wireless communications [28–34], one of the effective methods is beamforming. It can achieve the secrecy capacity in multi-input-multi-output (MISO) systems by enhancing energy in a particular direction and suppressing energy in other directions [35]. Previous works on physical layer security usually assume the channel state information (CSI) of both legitimate and eavesdropper channel, 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 [36–38]. 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 [36], it analyzes the geographical regions where secrecy outages may occur. Besides, it further studies the system security performance of the SOR by using the artificial noise technology. In [37], the vulnerability region (VR) under zero security rate in multi hop networks was studied. By minimizing the VR, the number of eavesdropping users was reduced. The compromised secret region (CSR) was defined in [39] and it proposed a secure transmission strategy of 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 security outage probability is achieved.

This paper mainly studies the classical passive eavesdropping system model in the IIoT wireless communications, where the transmitter device (Alice) wishes to transmit to the legitimate device (Bob) in presence of eavesdropping device (Eve). Location information has been widely concerned in wireless networks [40,41]. This paper mainly studies the scenario that only Bob's location information is attained by Alice. In this paper, the spatial outage probability (SSOP) is defined by the physical region where uniformly distributed Eve causes secrecy outage to the legitimate transmission. Alice adopts beamforming to enlarge the signal to noise ratio (SNR) of the device Bob, 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 device Bob.

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

Notations: Bold lowercase and uppercase letters represent vectors and matrixes, respectively, i.e., $\mathbf{a}$ and $\mathbf{A}$. $(\cdot)^T$ 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 the dimension $n \times m$, and $\mathbf{I}_{n \times n}$ denotes an n -by- n identity matrix. $\mathcal{CN}(0, \sigma^2)$ denotes the distribution of a circularly symmetric complex Gaussian (CSCG) random variable with mean zero and variance σ^2 . The distribution 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 consider a typical wireless networked control systems 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 wireless channels. Among of this, the transmitter (Alice) is equipped with a uniform linear antenna array with N antennas where the antenna spacing is wavelength spacing, i.e., $d = 1/2\lambda$, 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) , Eve's location is denoted as (D_e, θ_e) . The paper assumes Alice has known the CSI and the location information of Bob, but the CSI and the location information of Eve are unknown to Alice or Bob. We assume 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 equal block length. As detailed below, the $1 \times N$ legitimate channel and the eavesdropping channel are denoted as follows:

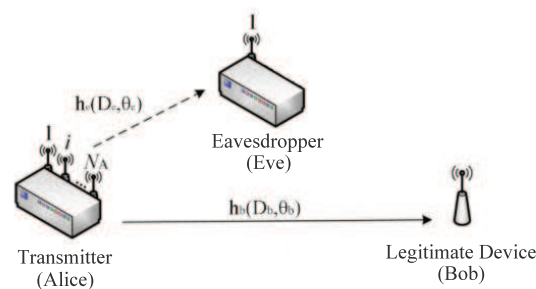


Figure 1. Illustration of IIoT scenario and the geometry of the transmitter, the legitimate device, and the eavesdropper.

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

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., $\mathbf{a}(\theta) = [1, e^{-j2\pi d \sin \theta / \lambda}, \dots, e^{-j2\pi(n_t-1)d \sin \theta / \lambda}]^T$, $\theta \in (0, 2\pi)$.

In this paper, Eve is a passive eavesdropper, hence the location of Eve is unknown to Alice. In order to eavesdropping the secrecy 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 [42]:

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

where $U(\cdot, \cdot)$ denotes the uniform distribution, $D_{\max}$ denotes the maximum distance where Eve can eavesdrop the secrecy information.

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

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

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

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

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

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

3. 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 secrecy outage. It can be seen 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 could be happen. The probability of the secrecy outage event called secrecy outage probability (SOP). In this paper, we adopt 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. The insecure region Θ can be denoted by

$$\Theta = \{z : C_e > R_b - R_s\}. \quad (6)$$

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

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

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

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

A is measured in m^2 , and it depends on $(G^2(\theta_e, \theta_b))^{\frac{2}{\alpha}}$ 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

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

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

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

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

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

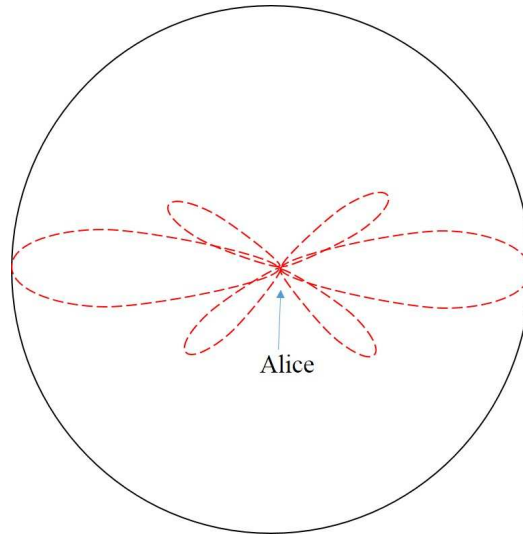


Figure 2. Illustration of the insecure region.

From (11), $\bar{p}_{ssop}$ can be obtained by numerical calculation. But the closed form expression can not 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 $B_1 = \int_0^{2\pi} \frac{1}{2\pi} (G^2(\theta_e, \theta_b))^{\frac{2}{\alpha}} d\theta_e$, the second obstacle is $B_2 = \int_{-\infty}^{+\infty} |h_e|^{\frac{4}{\alpha}} f(|h_e|^2) d|h_e|^2$. This paper uses Jensens Inequality to overcome the two obstacles. The Jensens Inequality is given by

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

The equality holds when $\alpha = 2$ for any X .

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

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

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

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

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

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

According to (12),

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

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

For 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 first kind of the Bessel function, 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 trigonometric function and exponential function, and $J_0(-x) = J_0(x)$, (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 $B_2 = \int_{-\infty}^{+\infty} |h_e|^{\frac{4}{\alpha}} f(|h_e|^2) d|h_e|^2$.

According to (12), B_2 can be denoted by

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

$|h_e|^2$ follows the exponential distribution with parameter 1, therefor $\mathbb{E} [|h_e|^2] = 1$. 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 SSOP is (13) and $\bar{p}_{ssop} = \bar{p}_{ssop}^{up}$ when $\alpha = 2$.

Thus, the proof is completed.

4. Simulation Results

In this section, we further provide numerical results to validate our theoretical analysis. Without losing generality, simulation parameters are set as follows in the MATLAB. we set the path loss index α to be 2, the simulation results are derived from 10000 Monte-Carlo experiments. The power budgets P_A at Alice is 30dBm and the number of antennas is 8, i.e., $N = 8$. D_b is the distance between Alice and Bob, the default value is 10 m, $D_{\max}$ is the maximum distance between Alice and Eve, to be set 50 m, R_b is the legal channel transmission rate, The initial value is 4bits/s/Hz, ε is the SSOP threshold, the setpoint is 0.1, δ is the legitimate user reception probability threshold, to be set 0.9, θ_b is the

incident angle, initial value is 0° , simultaneously, the noise power σ_b^2 is 30dBm, η stands for the system throughput.

4.1. The Impact for the Averaged SSOP versus Bob's Different Value of θ_b

In Figure 3, we analyzed the relationship between Bob's different value of θ_b and the $\bar{p}_{ssop}$, from the simulation result, we can conclude there is a slight oscillation at the beginning, the underlying reason lies in the Alice signal influence. With the increase of the θ_b , the $\bar{p}_{ssop}$ overall trend also increases. Therefore, when Bob located in the normal direction of the antenna array as the Alice direction, the results work perfectly. The root cause is when $\theta_b=0^\circ$, The antenna array has the narrowest beam width, at this point, the leakage of information is minimized also make the $\bar{p}_{ssop}$ to be 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 FIG.3 shows the theoretical analysis results and numerical simulation results plotted on a curve graph which can be observed that the two curves exhibit a good level of alignment. Furthermore, it further substantiates the theoretical analysis results mentioned earlier.

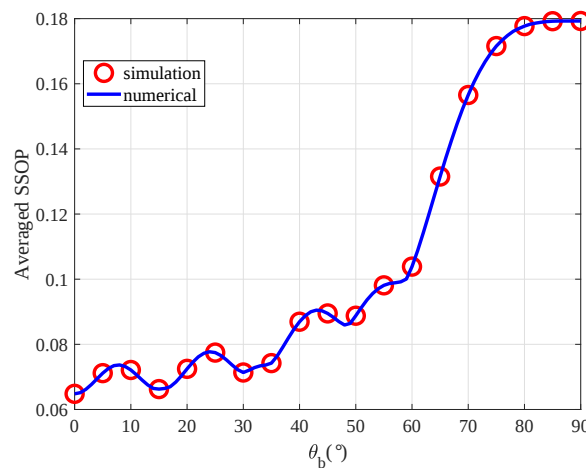


Figure 3. The Impact for the averaged SSOP versus Bob's different value of θ_b .

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

In Figure 4, we plot the averaged SSOP, $\bar{p}_{ssop}$, versus different value of N for various $\theta_b = 0^\circ, 30^\circ, 60^\circ$ for $D_b = 20\text{m}$, $D_{max} = 50\text{m}$. It can be seen from figure that for different θ_b , $\bar{p}_{ssop}$ fluctuates at different rate. The fluctuates 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 increasing of N , $\bar{p}_{ssop}$ approaches to 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 the minimum when $\theta_b = 0^\circ$, 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.

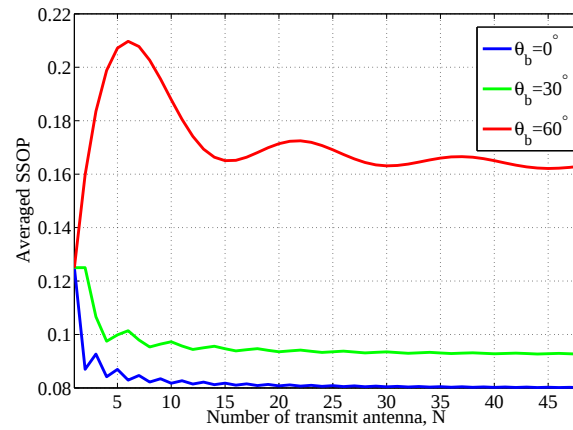


Figure 4. The averaged SSOP $\bar{p}_{ssop}$ versus different value of N .

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

In Figure 5, we plot the averaged SSOP, $\bar{p}_{ssop}$, versus different value of θ_b and D_b for $D_{max} = 50\text{m}$. From the three dimensional figure we can see $\bar{p}_{ssop}$ when Bob located in different places on the premise of Alices location is selected as the origin. The region can be divided into 3 areas, the absolute safety zone ($\bar{p}_{ssop} = 0$), relatively safe zone ($\bar{p}_{ssop} < \epsilon$) and danger zone ($\bar{p}_{ssop} > \epsilon$), ϵ denoted a predefined probability value. From this figure, $\bar{p}_{ssop}$ grows with the increasing 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.

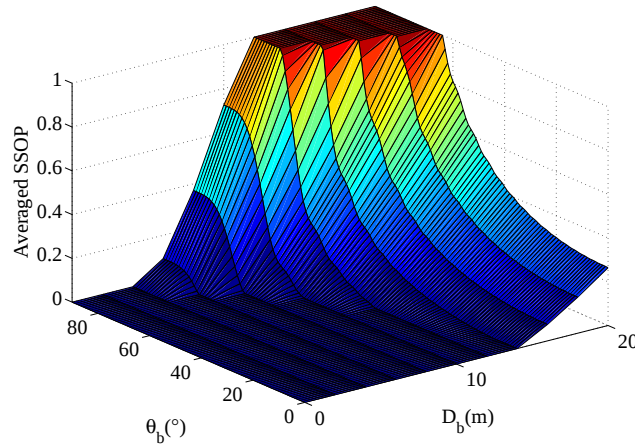


Figure 5. The averaged SSOP $\bar{p}_{ssop}$ versus different value of θ_b and D_b .

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

In Figure 6, we plot the averaged SSOP, $\bar{p}_{ssop}$, versus different value of θ_b and R_b for $D_{max} = 50\text{m}$, $D_b = 50\text{m}$. 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.

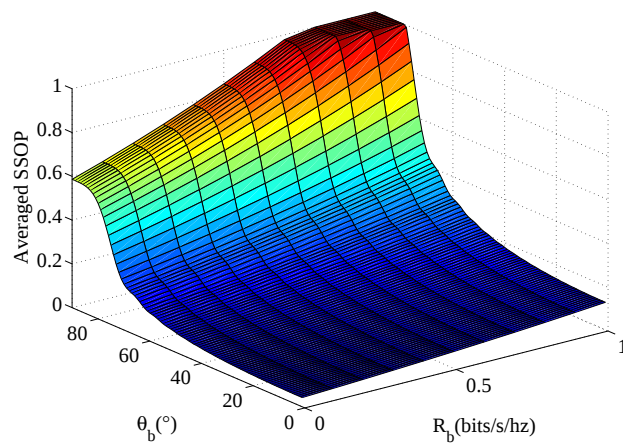


Figure 6. the averaged SSOP $\bar{p}_{ssop}$ versus different value of θ_b and R_b .

4.5. 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 theoretical analysis. Given our knowledge of the channel information for the legitimate channel in practical communication scenarios, 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 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.

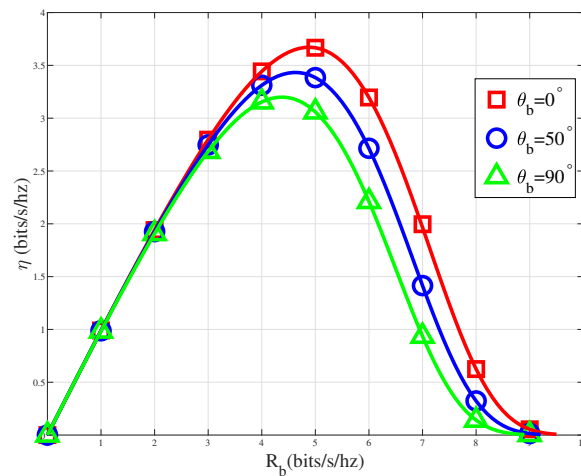


Figure 7. The system throughput η versus the legitimate channel transmission rate R_b .

4.6. 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 Throughput Maximization based on Spatial Secrecy Outage Probability, SRM-SSOP algorithm conditions and the adaptive transmission mechanism (ADP) based on the [43]. 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 transmission rate and secrecy rate according to channel state information, the ADP algorithm can achieve higher system throughput. From the simulated data, it is apparent that under strict outage probability constraints ($\epsilon = 0.1$), the presented approach in this paper exhibits superior performance compared to the optimization scheme based on ADP at elevated transmit power levels ($P_A > 50\text{dBm}$). While, in scenarios with lower transmit power, the system performance based on SRM-SSOP may be suboptimal compared to ADP, it is noteworthy that ADP constantly adjusts the coding length to adapt to dynamic transmission rates, introducing heightened complexity in coding and modulation. In contrast, the proposed approach maintains a fixed transmission rate, rendering it more suitable for practical engineering applications.

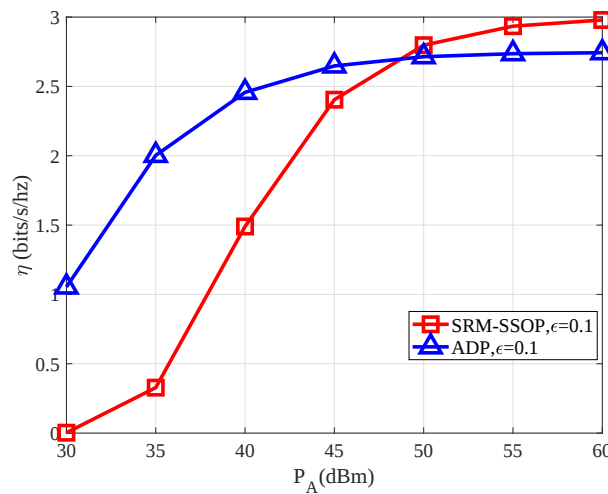


Figure 8. The system throughput η versus the different transmission power levels P_A .

4.7. The Relationship between System Throughput versus Bob's Azimuth Angle

In the Figure 9, we analyzed 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. At this configuration, the main lobe beam is the narrowest, leading to minimal information leakage. Consequently, with the flexibility of adjustable antenna direction, optimizing system throughput can be achieved by aligning the antenna array direction when Bob's position is known.

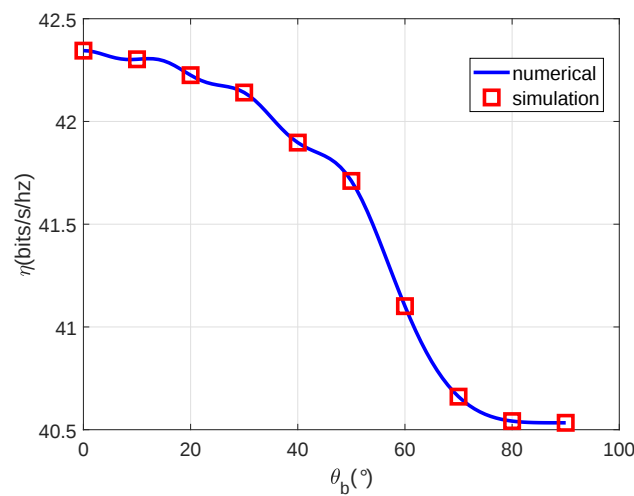


Figure 9. The system throughput η versus Bob's different value of θ_b .

5. Conclusions

In this article, we designed a wireless protocol called SSOP in the IIoT situation to judge the security performance of the system whereby Alice communicates to Bob in the presence of uniformly distributed Eve. First we defined the insecure region from the perspective of mathematical based on the secrecy outage event. Secondly, The SSOP is defined according to analyze the insecure region and the upper bound of SSOP was derived based. Performance analysis was provided to highlight the advantages of our proposed scheme over other benchmarks in terms of system throughput and secure transmission rate, and the robustness of our scheme to eavesdropping and active attacks. Numerical simulations verified the correctness of our analysis and illustrated the impacts of a wide range of system parameters on the security performance. we can conclude Spatial Secrecy Outage Probability is an important indicator for evaluating the security performance of wireless communication systems in the industrial Internet of Things environment, providing us with opportunities to gain insight into the security performance of communication systems. By studying the variation patterns and influencing factors of SSOP, we can better guide the design and optimization of communication systems and improve system security.

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

References

1. Liu, Y.; Chi, C.; Zhang, Y.; Tang, T. Identification and Resolution for Industrial Internet: Architecture and Key Technology. *IEEE Internet of Things Journal* **2022**, *9*, 16780–16794.
2. Serror, M.; Hack, S.; Henze, M.; Schuba, M.; Wehrle, K. Challenges and Opportunities in Securing the Industrial Internet of Things. *IEEE Transactions on Industrial Informatics* **2021**, *17*, 2985–2996.
3. Mcginthy, J.M.; Michaels, A.J. Secure Industrial Internet of Things Critical Infrastructure Node Design. *IEEE Internet of Things Journal* **2019**, *6*, 8021–8037.
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 of Things Journal* **2024**, *11*, 11073–11086.
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 of Things Journal* **2023**, *10*, 2776–2783.
6. Yousuf, T.; Mahmoud, R.; Aloul, F.; Zualkernan, I. Internet of Things (IoT) Security: Current Status, Challenges and Countermeasures **2015**.

7. Al-Fuqaha, A.; Guizani, M.; Mohammadi, M.; Aledhari, M.; Ayyash, M. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE Communications Surveys and Tutorials* **2015**, *17*, 2347–2376.
8. Kokoris-Kogias, E.; Voutyras, O.; Varvarigou, T. TRM-SIoT: A scalable hybrid trust and reputation model for the social Internet of Things. *IEEE International Conference on Emerging Technologies and Factory Automation*, 2016.
9. Lin, J.; Yang, X.; Yu, W.; Fu, X. Towards Effective En-Route Filtering against Injected False Data in Wireless Sensor Networks. *Global Telecommunications Conference*, 2011.
10. Suo, H.; Wan, J.; Zou, C.; Liu, J. Security in the Internet of Things: A Review. *IEEE* **2012**.
11. Mukherjee, A. Physical-Layer Security in the Internet of Things: Sensing and Communication Confidentiality Under Resource Constraints. *Proceedings of the IEEE* **2015**, *103*, 1747–1761.
12. Mcginthy, J.M.; Michaels, A.J. Secure Industrial Internet of Things Critical Infrastructure Node Design. *IEEE Internet of Things Journal* **2019**, *6*, 8021–8037.
13. 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 of Things Journal* **2022**, *9*, 18392–18405.
14. 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. *Discover Internet of Things* **2023**, *3*, 16.
15. 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. *Concurrency and Computation: Practice and Experience* **2023**, *35*, e7826.
16. Chen, H.; Hu, M.; Yan, H.; Yu, P. Research on industrial internet of things security architecture and protection strategy. 2019 International conference on virtual reality and intelligent systems (ICVRIS). *IEEE*, 2019, pp. 365–368.
17. Mcginthy, J.M.; Michaels, A.J. Secure industrial Internet of Things critical infrastructure node design. *IEEE Internet of Things Journal* **2019**, *6*, 8021–8037.
18. Islam, S.N.; Baig, Z.; Zeadally, S. Physical layer security for the smart grid: Vulnerabilities, threats, and countermeasures. *IEEE Transactions on Industrial Informatics* **2019**, *15*, 6522–6530.
19. Xu, L. Secure transmission strategy of network communication layer relay based on satellite transmission. 2020 2nd International Conference on Information Technology and Computer Application (ITCA). *IEEE*, 2020, pp. 268–271.
20. 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.
21. Liu, M.; Liu, Z.; Lu, W.; Chen, Y.; Gao, X.; Zhao, N. Distributed few-shot learning for intelligent recognition of communication jamming. *IEEE Journal of Selected Topics in Signal Processing* **2021**, *16*, 395–405.
22. Liu, M.; Wang, J.; Zhao, N.; Chen, Y.; Song, H.; Yu, F.R. Radio frequency fingerprint collaborative intelligent identification using incremental learning. *IEEE Transactions on Network Science and Engineering* **2021**, *9*, 3222–3233.
23. 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 Communications* **2022**, *19*, 52–63.
24. Li, B.; Zhou, Z.; Zou, W.; Sun, X.; Du, G. On the efficient beam-forming training for 60GHz wireless personal area networks. *IEEE Transactions on Wireless Communications* **2013**, *12*, 504–515.
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. 2022 IEEE 3rd KhPI Week on Advanced Technology (KhPIWeek). *IEEE*, 2022, pp. 1–5.
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 Wireless Communications Letters* **2014**, *3*, 357–360.
27. Barb, G.; Oteteanu, M. Digital GoB-based Beamforming for 5G communication systems. 2020 international symposium on antennas and propagation (ISAP). *IEEE*, 2021, pp. 469–470.

28. Talak, R.; Karaman, S.; Modiano, E. Improving age of information in wireless networks with perfect channel state information. *IEEE/ACM Transactions on Networking* **2020**, *28*, 1765–1778.
29. Shi, W.; Pang, S.; Zhang, W. Linear shrinkage receiver for slow fading channels under imperfect channel state information. 2022 IEEE Information Theory Workshop (ITW). IEEE, 2022, pp. 338–343.
30. 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 of Things Journal* **2020**, *8*, 345–356.
31. Yilmaz, B.B.; Prvulovic, M.; Zajić, A. Electromagnetic side channel information leakage created by execution of series of instructions in a computer processor. *IEEE Transactions on Information Forensics and Security* **2019**, *15*, 776–789.
32. 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? 2022 IEEE 96th Vehicular Technology Conference (VTC2022-Fall). IEEE, 2022, pp. 1–5.
33. 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 Transactions on Wireless Communications* **2020**, *19*, 4643–4656.
34. Chen, Y.; Zhu, G.; Xu, J. Over-the-air computation with imperfect channel state information. 2022 IEEE 23rd International Workshop on Signal Processing Advances in Wireless Communication (SPAWC). IEEE, 2022, pp. 1–5.
35. Mukherjee, A.; Fakoorian, S.A.A.; Huang, J.; Swindlehurst, A.L. Principles of Physical Layer Security in Multiuser Wireless Networks: A Survey. *IEEE Communications Surveys & Tutorials* **2014**, *16*, 1550–1573.
36. Wang, J.; Lee, J.; Wang, F.; Quek, T. Jamming-Aided Secure Communication in Massive MIMO Rician Channels. *IEEE Transactions on Wireless Communications* **2015**, *14*, 6854–6868.
37. Sarma, S.; Shukla, S.; Kuri, J. Joint scheduling & jamming for data secrecy in wireless networks. International Symposium on Modeling & Optimization in Mobile, 2013.
38. Zheng, T.X.; Wang, H.M.; Yin, Q. On Transmission Secrecy Outage of a Multi-Antenna System With Randomly Located Eavesdroppers. *IEEE Communications Letters* **2014**, *18*, 1299–1302.
39. Hao, L.; Wang, X.; Hou, W. Security enhancement in cooperative jamming using compromised secrecy region minimization. Information Theory, 2013.
40. Yan, S.; Malaney, R.; Nevat, I.; Peters, G.W. Optimal Information-Theoretic Wireless Location Verification. *Vehicular Technology IEEE Transactions on* **2014**, *63*, 3410–3422.
41. Yan, S.; Malaney, R.; Nevat, I.; Peters, G.W. Signal strength based wireless location verification under spatially correlated shadowing. 2014 IEEE International Conference on Communications (ICC). IEEE, 2014, pp. 2617–2623.
42. Yan, S.; Malaney, R. Line-of-sight based beamforming for security enhancements in wiretap channels. 2014 International Conference on IT Convergence and Security (ICITCS). IEEE, 2014, pp. 1–4.
43. Li, Z.; Mu, P.; Li, Z.; Zhang, W.; Zhang, Y. An Adaptive Transmission Scheme for Slow Fading Wiretap Channel with Channel Estimation Errors. *IEEE Globecom* 2016, 2016.

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.