Spatial Secrecy Outage Probability Design Under Nakagami-m Wiretap Channel in the Industrial Internet of Things

Xiaokai Liu , Fangmin Xu , Lina Ning * , Qiguang Li , Chenglin Zhao

Posted Date: 24 January 2025

doi: 10.20944/preprints202501.1851.v1

Keywords: Industrial Internet of Things; Physical-Layer Security; Spatial Secrecy Outage Probability; Nakagami-m Wiretap Channel; System Secrecy Throughput; Multiple Eavesdroppers

Article

Spatial Secrecy Outage Probability Design Under Nakagami-m Wiretap Channel in the Industrial Internet of Things

Xiaokai Liu [1,†], Fangmin Xu [2,†], Lina Ning [3,*], Qiguang Li [2] and Chenglin Zhao [2]

[1] School of Mechanical and Electrical Engineering, Beijing Information Science and Technology University,Bejing 102206, China; liu_xiaokai@bistu.edu.cn
[2] School of Information and Communication Engineering, Beijing University of Posts and Telecommunications,Beijing 100876, China; xufm@bupt.edu.cn; clzhao@bupt.edu.cn
[3] Academy of Military Sciences, Beijing 100097, China; lnning@bupt.cn
* Correspondence: lnning@bupt.cn
† These authors contributed equally to this work and should be considered co-first authors. This research was funded by Beijing Information Science and Technology University Research Fund.(Grant Number:2023XJJ02)

Abstract: The rapid evolution of the Industrial Internet of Things (IIoT) has created significant opportunities for industrial transformation, while simultaneously presenting substantial challenges to network security. Among these challenges, physical layer security emerges as a critical factor in ensuring the integrity and reliability of message transmission across interconnected devices and sensors within complex industrial environments. In our previous work [1], we proposed a mechanism for assessing the Spatial Secrecy Outage Probability (SSOP) in a Rayleigh Channel with a single eavesdropper, achieving promising simulation results. This paper focuses on the Nakagami-m Wiretap Channel and multiple eavesdroppers assuming that the location of legitimate devices is known, while the eavesdropper devices have a spatially homogeneous Poisson point process distribution of locations, forming the SSOP models 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 constraints imposed by SSOP conditions, we establish an optimization model aimed at maximizing system secrecy throughput. Finally,we analyze ISRs and SRs based on geographical location information through the lens of Secrecy Outage Probability (SOP), evaluating the security performance of our system. Through advanced modeling and simulation in MATLAB, we validated the accuracy of the proposed definition and derived the upper bound for the SSOP under Nakagami-m Channel. The experimental results further demonstrate the deep relationship between Secrecy Rate and Throughput. Additionally, it was observed that as the secrecy rate increases, the secrecy outage probability also rises, necessitating careful consideration of the trade-off. These insights are crucial for understanding and enhancing the security performance of IIoT communication systems.

Keywords: Industrial Internet of Things; Physical-Layer Security; Spatial Secrecy Outage Probability; Nakagami-m Wiretap Channel; System Secrecy Throughput; Multiple Eavesdroppers

1. Introduction

With the rapid development of the Industrial Internet of Things (IIoT), more and more IIoT-based sensors and devices are deployed in various scenarios, such as smart manufacturing, intelligent transportation, smart healthcare, and industrial control[2–6]. For many IIoT applications, the devices generate vast amounts of data, including production data, equipment status data, and supply chain data, which is vital for business decision-making and operational efficiency. For these applications, wireless communication has become the predominant method for devices to transmit data to centralized data centers. These centers serve as the backbone of decision-making processes, where transmitted data is analyzed and processed to drive operational efficiency and optimize industrial

 doi:10.20944/preprints202501.1851.v1

workflows. However, the reliance on wireless transmission introduces significant security challenges, as the open nature of wireless channels makes them vulnerable to eavesdropping, data interception, and unauthorized access by malicious entities. Ensuring the security and integrity of data during transmission has become a critical requirement to safeguard sensitive industrial information and maintain the trustworthiness of decision-making outcomes[7–11]. To address these concerns, robust network security mechanisms have become a focal point of research in the Industrial Internet domain. Advanced encryption techniques, secure communication protocols, and intrusion detection systems are being developed to mitigate risks associated with data transmission[12–16]. Additionally, innovations such as physical layer security and blockchain technology are being explored to enhance the resilience of industrial communication networks[17,18]. As industrial systems become increasingly interconnected, the role of secure data transmission continues to grow in importance, making network security a cornerstone for realizing the full potential of the Industrial Internet.

It is widely recognized that the architecture of the IIoT comprises three fundamental layers: the application layer, the network layer, and the perception layer[19]. The physical layer is usually involved in the network layer, which 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[20–25]. Physical layer security is recognized as the foundational defense mechanism for the IIoT, safeguarding critical infrastructure such as network devices, sensors, and controllers. These components are integral to the functionality of IIoT systems, and any compromise or attack targeting them can result in significant disruptions across the entire network[26,27]. To mitigate such risks, robust measures including stringent physical access control, equipment protection, and hardware-based encryption are imperative[28]. Ensuring that only authorized personnel have access to the physical infrastructure and implementing advanced authentication and access control policies, the risk of unauthorized access can be substantially minimized[29–31]. Additionally, advanced signal processing techniques have emerged as a pivotal approach to enhancing physical layer security[32–34]. These techniques provide robust protection against both passive and active attacks by adversaries or malicious users. For example, beamforming technology enables legitimate devices to achieve superior secrecy rates, even when the legitimate channel is of lower quality compared to that of an eavesdropper[35]. Such innovations highlight the critical role of physical layer security in ensuring secure and resilient communication in IIoT environments, solidifying its importance in the broader framework of IIoT security strategies[36–40]. This paper focuses on designing physical layer communication mechanisms to reduce the risk of service interruptions caused by physical layer failures or attacks.

There has been a great deal of research work on physical layer security in wireless communications[41–50], Reference[41] 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 [42] investigates a physical layer security transmission scheme in an 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 [43] 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)

 doi:10.20944/preprints202501.1851.v1

systems by enhancing energy in a particular direction and suppressing energy in other directions [44–49]. 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 [51–53]. The SR means that Eve in this area cannot correctly decode the received confidential information, and the ISR means that Eve in this area can correctly decode the received confidential information. The Secrecy Outage Region (SOR) was defined in [51]; 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 [52], 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 [53], 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. In [54], the proposed Layered Physical Layer Security (LPLS) scheme divides information into different security levels based on practical application scenarios. Under the constraint of ensuring the secrecy rate of the lowest-level information, the scheme achieves the maximization of the secrecy rate for the highest-level information. In[55], the study investigates a communication scenario in a MISO system with multiple eavesdropping users. The research employs artificial noise (AN) techniques for signal transmission and jointly optimizes the beamforming vectors of the transmitted signal and artificial noise. This optimization is performed under the constraints that the signal-to-noise ratio (SNR) at legitimate users and the SNR at eavesdropping users meet certain threshold conditions. In[56], the study explores transmission schemes in multi-user systems and proposes two interference-assisted multi-user scheduling schemes. The first is an optimal interference-assisted multi-user scheduling scheme, assuming the eavesdropping channel state information (CSI) is known. The second is a random interference selection-based multi-user scheduling scheme, relying only on the statistical information of the eavesdropping channel. The optimal power allocation ratio between the transmitted signal and the interference signal is derived by maximizing the secrecy capacity. In [57], A Coding Per Sub-channel scheme is proposed for a three-node eavesdropping system model, where multiple parallel sub-channels use distinct coding schemes. A novel expression for the outage probability is introduced, defined as the ratio of the sum of the outage secrecy rates of all sub-channels to the total secrecy rate of all sub-channels. Based on this, a secure transmission scheme is developed, which maximizes the secrecy rate under the constraint of secrecy outage probability.

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 many eavesdropping devices (Eves) under the Nakagami-m Wiretap Channel. In wireless communication systems, the more information the transmitter has about the eavesdropping channel, the more effectively it can employ reliable techniques to reduce information leakage and enhance system security. However, when an eavesdropping user remains silent during the channel estimation phase, it becomes challenging for the transmitter to obtain details about the eavesdropping channel. Furthermore, the geographical location of the eavesdropping user significantly impacts the system's security performance. Recent studies have proposed the concepts of secure and insecure regions based on user location as performance metrics for physical layer security. When the eavesdropping user is within the secure region, security metrics such as secrecy capacity and secrecy outage probability meet the requirements for secure communication, making it difficult for the eavesdropper to intercept useful information. Conversely, when the eavesdropping user is located in insecure region, there is a higher likelihood of successful interception of confidential information. Research on secure regions helps minimize the consumption of communication resources within these areas, while studies

 doi:10.20944/preprints202501.1851.v1

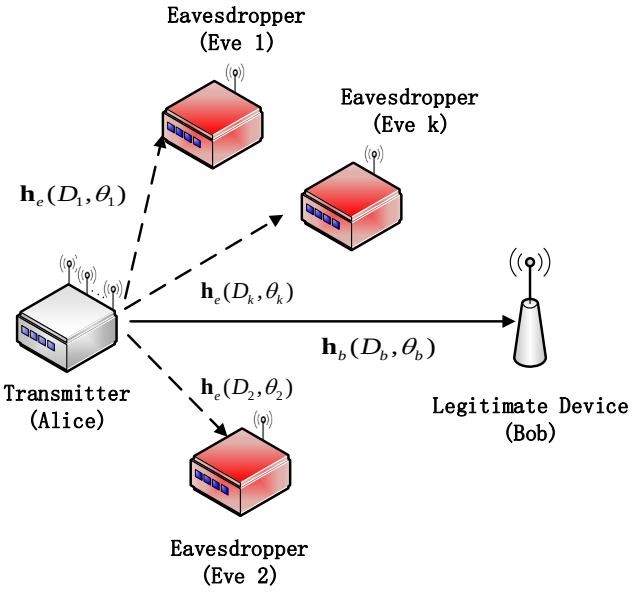

Figure 1. Illustration of IIoT scenario with multiple eavesdroppers.

on insecure regions facilitate the rapid identification of eavesdroppers' locations. This enables the transmitter to promptly implement effective countermeasures, such as artificial noise and cooperative jamming, to disrupt eavesdropping attempts in insecure regions. Consequently, this approach holds significant practical value in real-world engineering applications. The main contributions of this article are briefly summarized as follows.

1. Focusing on the scenario in MISO systems with multiple eavesdropping users, the paper models the locations of eavesdroppers using a Poisson point process. It analyzes the spatial outage probability under Nakagami-m channel fading and derives a closed-form expression for its upper bound.
2. After deriving the spatial outage probability, this paper investigates and analyzes the relationship between secrecy rate and secrecy throughput in the given scenario. With the optimization objective of maximizing the minimum average secrecy rate and under the constraint of secrecy outage probability, the system's secrecy throughput is validated.
3. In this channel environment, the paper also explores the issues of secure and non-secure regions under the constraint of secrecy outage probability. It analyzes the system's security performance, providing theoretical guidance for practical applications.

The remainder of this article is structured as follows. Section II presents a detailed description of the system model. In this section, we derive the SSOP expression under the Nakagami-m Wiretap Channel, along with its upper bound. Furthermore, Sections III focus on analyzing system throughput based on SSOP and examining the secure region of the system. Numerical results are provided in Section IV to support our findings. Finally, we conclude our work in Section V.

2. SYSTEM MODEL

As shown in Figure 1, this paper considers a time-division duplex MISO system scenario involving multiple non-cooperative single-antenna eavesdroppers. The system consists of a multi-antenna transmitter (Alice), a single-antenna legitimate user (Bob), and k single-antenna eavesdroppers $\text{Eve}_k(k = 1, 2, \ldots, K)$. The system is modeled using polar coordinates, where Alice is located at the origin. Alice is equipped with n_t antennas uniformly distributed along the y axis, with an inter-antenna spacing Δd equal to half the wavelength $\Delta d = \lambda/2$. The locations of the legitimate user and the eavesdropper are denoted as (D_b, θ_b) and (D_k, θ_k), respectively. D_b and D_k represent the distances of the users from the origin, while θ_b and θ_k denote the angles between the users and the origin. The

 doi:10.20944/preprints202501.1851.v1

legitimate channel is denoted as $\mathbf{h}_b = D_b^{-\alpha/2} h_b \mathbf{a}(\theta_b)$, the eavesdropping channel is represented as $\mathbf{h}_k = D_k^{-\alpha/2} h_k \mathbf{a}(\theta_k), k = 1, \ldots, K$, Both h_b and h_k follow independent Nakagami-m distributions, where parameter m indicates the severity of channel fading. The Probability Density Function (PDF) of $h_i (i = b, k)$ can be described as :

$$f(x) = \frac{2 {m_i}^{m_i} x^{2m_i - 1}}{{\Omega_i}^{m_i} \Gamma(m_i)} \exp\left(-\frac{m_i}{\Omega_i} x^2\right), x \geq 0 \tag{1}$$

where m_i is the form factor, indicating the severity of fading, and Ω_i represents the average power of h_i. $|h_i|^2$ follows a gamma distribution with fading parameter m_i and mean Ω_i, $|h_i|^2 \sim Ga(m_i, m_i/\Omega_i)$, the PDF can be further rewritten:

$$f\left(|h_i|^2\right) = \left[\frac{m_i}{\Omega_i}\right]^{m_i} \frac{\left(|h_i|^2\right)^{m_i - 1}}{\Gamma(m_i)} e^{-\frac{m_i}{\Omega_i}|h_i|^2} \tag{2}$$

where $\Gamma(x) = \int_0^\infty t^{x-1} \exp(-t) dt$ is gamma function. When Alice sends a signal, the signal noise of Bob and Eve receives the signal is shown below:

$$\begin{aligned} \gamma_b &= \frac{n_t P_A D_b^{-\alpha} |h_b|^2}{\sigma_n^2} \\ \gamma_k &= \frac{P_A D_k^{-\alpha} |h_k|^2 G^2(\theta_k, \theta_b)}{\sigma_k^2} \end{aligned} \tag{3}$$

where $G(\theta_k, \theta_b) = \mathbf{a}^H(\theta_b)\mathbf{a}(\theta_k)$, σ_n^2 and σ_k^2 are the variances of the noise signal received by a legitimate client and an eavesdropping client. The channel capacity of an eavesdropping user can be expressed as:

$$C_k = \log_2(1 + \gamma_k) = \log_2\left(1 + P_A D_k^{-\alpha} |h_k|^2 G^2(\theta_k, \theta_b) \Big/ \sigma_k^2\right) \tag{4}$$

3. Algorithm Design and Implementation

3.1. Analysis of Spatial Secrecy Outage Probability under Nakagami-m Channel Fading

It is well known that, the Nakagami-m channel is characterized by its ability to model different fading severities. It has a parameter m that indicates the fading level. The channel fading can range from mild to severe, affecting signal transmission and reception in wireless communication systems. Suppose R_b and R_s represent the transmission rate of the legitimate channel and the secrecy rate of the system, respectively. When Alice sends a confidential signal to Bob, the specific results can be divided into the following three situations:

1. $C_b < R_b$: in this situation, the secrecy capacity C_b of the legitimate channel is less than R_b, resulting that Transmission errors or distortions are inevitable in the transmitted information, and transmission interruption occurs.
2. $C_b > R_b$: for this scenario, If the channel capacity C_e of Eve is greater than $R_b - R_s$, at this time Eve can eavesdrop on the confidential information and the system will experience a secrecy outage.
3. $C_b > R_b$ and $C_s > R_s$: under this circumstance, the system is able to achieve the secure and confidential transmission of data.

The research in this paper analyzes the Spatial Secrecy Outage Probability of the system under the prerequisite that Bob can correctly receive the confidential information, mainly including the following steps: 1) Determine the insecure region; 2) Construct the Spatial Secrecy Outage Probability based on the number of eavesdropping users in the insecure region; 3) Analyze the closed-form solution of the Spatial Secrecy Outage Probability. The specific implementation process is as follows:

 doi:10.20944/preprints202501.1851.v1

3.1.1. Determine the Insecure Region

This paper describes the outage event from the perspective of geometric figures. Define Θ as the insecure region, and the insecure region means that the eavesdropping user located in this region can eavesdrop on confidential information. In this study, the eavesdropping users follow a Poisson distribution. When any Eve_k is located within the region Θ, the secrecy outage event occurs. Therefore, Θ can be expressed as $\Theta = \{\text{Eve}_k : C_k > R_b - R_s\}$. Substituting γ_k into the above formula, the expression form of the insecure region regarding the location information of Eve_k can be obtained, as shown below:

$$\Theta=\{\text{Eve}_k : D_k < D(\theta_k)\} \tag{5}$$

where

$$D(\theta_k) = \left[\frac{P_A G^2(\theta_k,\theta_b)|h_k|^2}{\sigma_k^2(2^{R_b-R_s}-1)}\right]^{\frac{1}{\alpha}} \tag{6}$$

According to the formula for the area of a polar coordinate curve, the area of the insecure region A is obtained as:

$$\begin{aligned} A &= \tfrac{1}{2}\int_0^{2\pi} D^2(\theta_k)d\theta_k \\ &= \tfrac{1}{2}\int_0^{2\pi}\left[\frac{P_A G^2(\theta_k,\theta_b)|h_k|^2}{\sigma_n^2(2^{R_b-R_s}-1)}\right]^{\frac{2}{\alpha}} d\theta_k \\ &= \tfrac{1}{2}T\left(|h_k|^2\right)^{\frac{2}{\alpha}}\int_0^{2\pi}\left(G^2(\theta_k,\theta_b)\right)^{\frac{2}{\alpha}} d\theta_k \end{aligned} \tag{7}$$

where

$$T = \left[\frac{P_A}{\sigma_n^2(2^{R_b-R_s}-1)}\right]^{\frac{2}{\alpha}} \tag{8}$$

3.1.2. Construct the SSOP Based on the Number of Eavesdropping Users in the Insecure Region

From the paper[58], We can obtain that the spatial point process that meets the following two conditions is called a homogeneous Poisson point process.

a: If the number of points per unit area follows a Poisson distribution with density λ, then the number $N(B)$ of points in any finite region B in space follows a Poisson distribution with mean $\lambda v(B)$, where $v(B)$ represents the area of the bounded region B . The probability that there are m points in region B is as follows:

$$p\{N(B)=m\} = (\lambda v(B))^m \exp\left(\frac{-\lambda v(B)}{m!}\right) \tag{9}$$

b: For spatially bounded regions $B_1, B_2, \ldots, B_n$ that are disjoint from each other, the corresponding numbers of points $N(B_1), N(B_2), \ldots, N(B_n)$ are independent of each other. From the definition of the insecure region Θ , as long as there is one Eve_k located within region Θ, a secrecy outage event will occur. That is, when the secrecy capacity of Eve_k meets the condition $C_k > R_b - R_s$, a secrecy outage occurs in the system communication. This paper describes the spatial outage probability as the probability that $k(k \geq 1)$, Eves are located in the insecure region Θ , and the distribution density of eavesdropping users in region Θ is $\lambda_e A$. Therefore, according to the definition of the homogeneous Poisson point process, the Spatial Secrecy Outage Probability p_{ssop} is:

$$\begin{aligned} p_{ssop} &= \Pr\{m \text{ Eves in } \Theta\} \\ &= 1 - \Pr\{0 \text{ Eves in } \Theta\} \\ &= 1 - e^{-\lambda_e A} \end{aligned} \tag{10}$$

 doi:10.20944/preprints202501.1851.v1

3.1.3. Closed-Form Solution of SSOP

From Eq.10, we can conclude that the spatial outage probability is related to the area A of the insecure region and the distribution density λ_e of eavesdropping users. The smaller the area of the insecure region or the smaller the distribution density of eavesdropping users, the smaller p_{ssop} is and the safer the system becomes. From Eq.10 and Eq.9, we found that there is a relationship between p_{ssop} and h_k. h_k is subject to the Nakagami-m distributed random fading. Therefore, here we consider the average spatial outage probability $\bar{p}_{ssop}$. That is:

$$\bar{p}_{ssop}=\mathrm{E}_{|h_k|}\left[p_{ssop}\right]=1-E_{|h_k|}\left[e^{-\lambda_e A}\right] \tag{11}$$

The expanded expression of $\bar{p}_{ssop}$ is as follows:

$$\begin{aligned}\bar{p}_{ssop}&=1-E_{|h_k|}\left[e^{-\lambda_e A}\right]\\&=1-\int_{-\infty}^{+\infty}\exp\left(-\frac{\lambda_e}{2\pi}T\left(|h_k|^2\right)^{\frac{2}{\alpha}}\int_0^{2\pi}\left(G^2(\theta_k,\theta_b)\right)^{\frac{2}{c}}d\theta_k\right)f\left(|h_k|^2\right)d|h_k|^2\\&=1-\int_{-\infty}^{+\infty}\exp\left(-\frac{\lambda_e}{2\pi}T\left(|h_k|^2\right)^{\frac{2}{\alpha}}\int_0^{2\pi}\left(G^2(\theta_k,\theta_b)\right)^{\frac{2}{\alpha}}d\theta\right)\\&\quad*\left[\frac{m_k}{\Omega_k}\right]^{m_k}\frac{\left(|h_k|^2\right)^{m_k-1}}{\Gamma(m_k)}e^{-\frac{m_k}{\Omega_k}|h_k|^2}d|h_k|^2\end{aligned} \tag{12}$$

From the Eq.12, It is difficult to obtain the closed-form solution of $\bar{p}_{ssop}$. Therefore, in this section, we analyze the closed - form solution of the upper bound $\bar{p}^{up}_{ssop}$ of $\bar{p}_{ssop}$. From the Appendix.5, We can conclude that for the average spatial outage probability $\bar{p}_{ssop}$, the exact theoretical closed-form solution of its upper bound is:

$$\bar{p}^{up}_{ssop}=1-\exp\left[-\lambda_e\pi T(\Omega_k)^{\frac{2}{\alpha}}\left(\begin{array}{l}1+2\sum_{n=1}^{n_t-1}\frac{n_t-n}{n_t}J_0(\pi n)*\\\cos(\pi n\sin\theta_b)\end{array}\right)^{\frac{2}{\alpha}}\right] \tag{13}$$

When α=2, $\bar{p}_{ssop}$=$\bar{p}^{up}_{ssop}$. The range of values of the path loss exponent α is generally between 2 4 . To further analyze the physical meaning of $\bar{p}^{up}_{ssop}$, when taking $\alpha=2$, the expression of $\bar{p}^{up}_{ssop}$ is simplified to:

$$\bar{p}^{up}_{ssop}=1-\exp\left[-\frac{P_A/\sigma_n^2}{\gamma_k/\lambda_e\Omega_k}\left(\begin{array}{l}\pi+2\pi\sum_{n=1}^{n_t-1}\frac{n_t-n}{n_t}\\*J_0(\pi n)\cos(\pi n\sin\theta_b)\end{array}\right)\right] \tag{14}$$

From Eq.14, $\bar{p}^{up}_{ssop}$ is a function related to the signal-to-noise ratio P_A/σ_n^2 of legitimate users and the signal-to-noise ratio γ_k of eavesdropping users. When the distribution density λ_e of eavesdropping users is very small, the value of $\bar{p}^{up}_{ssop}$ is close to 0, which is consistent with the actual scenario. When the signal-to-noise ratio γ_k of a certain eavesdropping user is very large, $\bar{p}^{up}_{ssop}$ is close to 1, and at this time a secrecy outage occurs in communication.

3.2. Analysis of Secrecy Throughput

The secure throughput is defined as the product of the secure transmission rate R_s and the probability of secure information transmission $(1-p_{out}(R_s))$, as shown below:

$$\xi=R_s(1-p_{out}(R_s)) \tag{15}$$

In this chapter, we analyze the spatial outage probability of the system from the user location information. Therefore, we define the secure throughput as the product of R_s and $\left(1-\bar{p}_{ssop}(R_s)\right)$, that is:

$$\xi=R_s\left(1-\bar{p}_{ssop}(R_s)\right) \tag{16}$$

 doi:10.20944/preprints202501.1851.v1

The specific expression of ξ is as follows:

$$\begin{aligned}\xi{=}R_s \int_{-\infty}^{+\infty} \exp\left(-\frac{\lambda_e}{2\pi} T\left(|h_k|^2\right)^{\frac{2}{\alpha}} \int_0^{2\pi} \left(G^2(\theta_k,\theta_b)\right)^{\frac{2}{\alpha}} d\theta\right) \\ * \left[\frac{m_k}{\Omega_k}\right]^m \frac{\left(|h_k|^2\right)^{m_k-1}}{\Gamma(m_k)} e^{-\frac{m_k}{\Omega_k}|h_k|^2} d|h_k|^2\end{aligned} \tag{17}$$

It is difficult to obtain the closed-form solution of ξ from formula Eq.17. Under normal circumstances, when taking $\alpha = 2$, at this time $\bar{p}_{ssop}{=}\bar{p}^{up}_{ssop}$, the closed-form solution of ξ can be obtained as:

$$\xi{=}R_s \exp\left[\begin{array}{l} -\frac{\lambda_e \pi \Omega_k P_A}{\sigma_n^2\left(2^{R_b-R_s}-1\right)} \\ *\left(1{+}2\sum_{n=1}^{n_t-1} \frac{n_t-n}{n_t} J_0(\pi n)\cos(\pi n \sin\theta_b)\right)\end{array}\right] \tag{18}$$

As can be seen from formula Eq.18, ξ is a convex function of R_s. Therefore, the maximum throughput of the system can be analyzed.

3.3. Analysis of Secure Region Based on Secrecy Outage Probability

In this section, we assume that there is only one eavesdropping user, Eve, in the eavesdropping system model. The secrecy outage probability is more suitable than the secrecy capacity for describing the secure region when the eavesdropping channel is unknown. In this section, we analyze the secure region of this scenario based on the secrecy outage probability. The definition of the secrecy outage probability is as follows:

$$\begin{aligned} p_{out}(\theta_b,\theta_e,D_b,D_e) &= \Pr(C_s < R_s | C_b > R_s) \\ &= \frac{\Pr(C_s<R_s, C_b>R_s)}{\Pr(C_b>R_s)}\end{aligned} \tag{19}$$

Let p_s denote $\Pr(C_s < R_s, C_b > R_s)$, then

$$\begin{aligned} p_s &= \Pr(C_s < R_s, C_b > R_s) \\ &= \Pr\left\{\log_2\left(\frac{1+\gamma_b}{1+\gamma_e}\right) < R_s, \log_2(1+\gamma_b) > R_s\right\} \\ &= \Pr\left\{\gamma_e > \frac{\gamma_b - 2^{R_s}+1}{2^{R_s}}, \gamma_b > 2^{R_s}-1\right\}\end{aligned} \tag{20}$$

From $|h_i|^2 \sim Ga(m_i, m_i/\Omega_i)$, we have $\gamma_b \sim Ga(\alpha_b,\beta_b)$,$\gamma_e \sim Ga(\alpha_e,\beta_e)$, The parameters of γ_b and γ_e are as follows:

$$\begin{cases} \alpha_b = m_b \\ \beta_b = \frac{\sigma_n^2 m_b}{n_t P_A D_b^{-\alpha} \Omega_b}\end{cases} \tag{21}$$

$$\begin{cases} \alpha_e = m_e \\ \beta_e = \frac{\sigma_e^2 m_e}{P_A D_e^{-\alpha} G^2(\theta_e,\theta_b)\Omega_e}\end{cases} \tag{22}$$

From the [58], We can obtain that the distribution function of the gamma distribution is as follows:

$$F_X(x) = \frac{\gamma(\alpha_j,\beta_j x)}{\Gamma(\alpha_j)} = 1 - e^{-\beta_j x}\sum_{i=0}^{\alpha_j-1}\frac{1}{i!}(\beta_j x)^i \tag{23}$$

Among them, the random variable $X \in \{\gamma_b,\gamma_e\}, j \in \{b,e\}$, $\gamma(\cdot,\cdot)$ represents the lower incomplete gamma function, and $\Gamma(\cdot,\cdot)$ represents the upper incomplete gamma function. Let $Z = 2^{R_s}-1$, then

 doi:10.20944/preprints202501.1851.v1

$$\begin{aligned} p_s &= \int_{\mathrm{Z}}^{\infty} \int_{\frac{\gamma_b-\mathrm{Z}}{\mathrm{Z}+1}}^{\infty} f_{\gamma_e}(x_e) f_{\gamma_b}(x_b) dx_e dx_b \\ &= \int_{\mathrm{Z}}^{\infty} \left(1 - F_{\mathrm{X}_e}\left(\tfrac{x_b-\mathrm{Z}}{\mathrm{Z}+1}\right)\right) f_{\gamma_b}(x_b) dx_e dx_b \\ &= \int_{\mathrm{Z}}^{\infty} \left(1 - F_{\mathrm{X}_e}\left(\tfrac{x_b-\mathrm{Z}}{\mathrm{Z}+1}\right)\right) f_{\gamma_b}(x_b) dx_e dx_b \\ &= \int_{\mathrm{Z}}^{\infty} \left(e^{-\beta_e\left(\frac{x_b-\mathrm{Z}}{\mathrm{Z}+1}\right)} \sum_{i=0}^{\alpha_b-1} \frac{1}{i!} \left(\beta_e \tfrac{x_b-\mathrm{Z}}{\mathrm{Z}+1}\right)^i \right) {\beta_b}^{\alpha_b} \tfrac{{x_b}^{\alpha_b-1}}{\Gamma(\alpha_b)} e^{-\beta_b x_b} dx_b \end{aligned} \tag{24}$$

According to Reference [58], there is the following equation relationship:

$$(a+x)^n = \sum_{i=0}^{n} \binom{n}{i} x^i a^{n-i} \tag{25}$$

Based on Eq.24, and by interchanging the order of summation and integration in Eq.23, the closed-form expression of p_s can be obtained as follows:

$$\begin{aligned} p_s = &\sum_{i=0}^{\alpha_b-1} \frac{1}{i!} \left(\frac{\beta_e}{\mathrm{Z}+1}\right)^i \frac{{\beta_b}^{\alpha_b}}{\Gamma(\alpha_b)} \sum_{j=0}^{i} \binom{i}{j} (-\mathrm{Z})^{i-j} e^{-\frac{\beta_e \mathrm{Z}}{\mathrm{Z}+1}} \left(\frac{\mathrm{Z}+1}{\beta_e+(\mathrm{Z}+1)\beta_b}\right)^{\alpha_b+j} \\ &\times \Gamma\left(\alpha_b + j, \tfrac{\beta_e+(\mathrm{Z}+1)\beta_b}{\mathrm{Z}+1}\right) \end{aligned} \tag{26}$$

The expression of the secure transmission probability $\Pr(C_b > R_s)$ is as follows:

$$\Pr(C_b > R_s) = e^{-\beta_b \mathrm{Z}} \sum_{i=0}^{\alpha_b-1} \frac{1}{i!} (\beta_b \mathrm{Z})^i \tag{27}$$

Substitute $\Pr(C_b > R_s)$ and $\Pr(C_s < R_s, C_b > R_s)$ into $p_{out}(\theta_b, \theta_e, D_b, D_e)$, so the closed-form solution of $p_{out}(\theta_b, \theta_e, D_b, D_e)$ is as follows:

$$\begin{aligned} p_{out}(\theta_b, \theta_e, D_b, D_e) = &\sum_{i=0}^{\alpha_b-1} \frac{1}{i!} \left(\frac{\beta_e}{\mathrm{Z}+1}\right)^i \frac{{\beta_b}^{\alpha_b}}{\Gamma(\alpha_b)} \sum_{j=0}^{i} \binom{i}{j} (-\mathrm{Z})^{i-j} e^{\frac{\mathrm{Z}}{\mathrm{Z}+1}((\mathrm{Z}+1)\beta_b-\beta_e)} \\ &\times \left(\frac{\mathrm{Z}+1}{\beta_e+(\mathrm{Z}+1)\beta_b}\right)^{\alpha_b+j} \Gamma\left(\alpha_b + j, \tfrac{\beta_e+(\mathrm{Z}+1)\beta_b}{\mathrm{Z}+1}\right) \Bigg/ \sum_{i=0}^{\alpha_b-1} \frac{1}{i!} (\beta_b \mathrm{Z})^i \end{aligned} \tag{28}$$

Define the secure region and the non-secure region according to $p_{out}(\theta_b, \theta_e, D_b, D_e)$. Here, the non-secure region Θ is defined as the geometric region when the secrecy outage probability is greater than the given threshold $\varepsilon (0 \le \varepsilon \le 1)$, as shown in the following formula:

$$\Theta = \{\theta_b, \theta_e, D_b, D_e | p_{out}(\theta_b, \theta_e, D_b, D_e) > \varepsilon\} \tag{29}$$

θ_b and D_b can be expressed in terms of θ_e and D_e. Therefore, when the positions of Alice and Bob are relatively fixed, the secure region refers to the range of movement of Eve. When Eve is within this range of movement, it does not affect the secrecy performance of the system. Thus, at this time, the transmitting end and the legitimate user can achieve secure data transmission without adopting other technical means. The worst-case scenario for the secrecy performance occurs when Eve is in the same direction as Bob, that is, when θ_b=θ_e=0.

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 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. In this section, we first use Monte Carlo simulation to study the relationship between the SSOP

 doi:10.20944/preprints202501.1851.v1

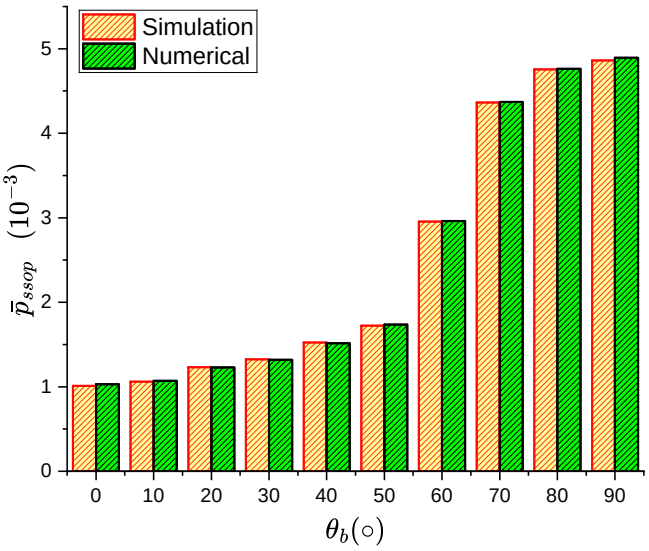

Figure 2. Comparison of Spatial Secrecy Outage Probability between Theoretical Analysis and Simulation Results With different θ_b

and its parameters. Secondly, we investigate the impact of the secrecy rate on the secure throughput. Finally, we analyze the secure region under the Nakagami-m channel. Unless otherwise specified, the simulation parameters are shown in Table.1.

Table 1. Simulation parameter settings

Parameters	Details	Setting Value
P_A	Transmit Power	40dBm
n_t	Number of Antennas	8
σ_n^2	Noise variance	30dBm
ε	Outage Probability Threshold	0.1
θ_b	Angle of Incidence	0°
m_b,Ω_b	Nakagami-m Distribution Parameter	1,1
m_e,Ω_e	Nakagami-m Distribution Parameter	1,1
R_s	Secrecy Rate	0.5bps/hz
λ_e	Poisson Distribution Parameter	0.001

4.1. Simulation and Analysis of Spatial Secrecy Outage Probability

Fig.2 depicts the influence of the angle θ_b of Bob relative to Alice on the average Spatial Secrecy Outage Probability under the condition of the channel fading exponent α=2. As can be seen from the figure, as the direction of Bob deviates from the normal direction of the antenna array at Alice's end, the average Spatial Secrecy Outage Probability $\bar{p}_{ssop}$ increases accordingly and tends towards a fixed value. It can be observed from the figure that during the variation of θ_b, the curve of $\bar{p}_{ssop}$ exhibits a small oscillatory characteristic. As can be seen from Eq.12, this is affected by the factor $\Delta = \sum_{n=1}^{n_t-1} \frac{n_t-n}{n_t} J_0(\pi n) \cos(\pi n \sin\theta_b)$. The figure also describes the fitting situation between the simulation results of the average Spatial Secrecy Outage Probability $\bar{p}_{ssop}$ and the theoretical analysis. It can be seen that the fitting effect is good, which further validates the theoretical analysis results of Eq.12. Fig.3 analyzes the impact of the number of transmit antennas n_t on the average spatial outage probability $\bar{p}_{ssop}$ and its upper bound $\bar{p}_{ssop}^{up}$ under the condition of the channel fading exponent α=3. As can be seen from the figure, with the increase of the number of antennas n_t, both the average spatial outage probability $\bar{p}_{ssop}$ and its upper bound $\bar{p}_{ssop}^{up}$ decrease. This is because as the number of antennas increases, the main lobe of the beam becomes narrower, and less information leaks, thus the outage probability decreases accordingly. From the expression of $\bar{p}_{ssop}$, it can be known that the number

 doi:10.20944/preprints202501.1851.v1

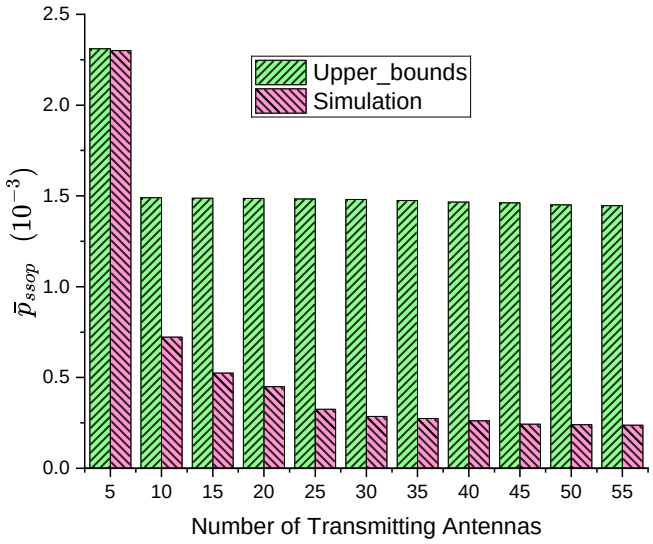

Figure 3. The Impact of Antenna Number n_t on the Average Spatial Secrecy Outage Probability and Its Upper Bound

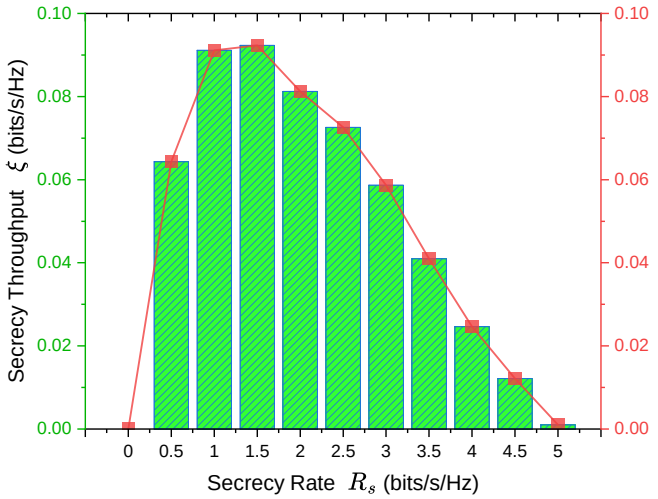

Figure 4. Relationship between Secrecy Rate and Secrecy Throughput

of antennas n_t and C are not in a proportional relationship. As can be seen from the figure, as the number of antennas increases, both $\bar{p}_{ssop}$ and $\bar{p}^{up}_{ssop}$ tend to stabilize. This indicates that the increase in the number of antennas cannot continuously improve $\bar{p}_{ssop}$, which is consistent with the theoretical analysis. It can also be observed from the figure that $\bar{p}_{ssop}$ converges more slowly compared to $\bar{p}^{up}_{ssop}$, resulting in an increasingly larger gap between the two.

4.2. Analysis of Secrecy Throughput

Fig.4 analyzes the relationship between the secrecy throughput and the change of the secrecy rate R_s. As R_s increases, the probability of secure transmission $1 - \bar{p}_{ssop}(R_s)$ decreases accordingly. At this time, R_s is dominant, and the secrecy throughput increases with the increase of R_s. When R_s increases to a certain extent, $1 - \bar{p}_{ssop}(R_s)$ becomes dominant, and the secrecy throughput decreases as R_s increases. When R_s is further increased, $1 - \bar{p}_{ssop}(R_s)$ decreases to 0, and at this time, the secrecy throughput also decreases to 0.

4.3. Analysis of Secure Area Based on Secrecy Outage Probability

Fig.5 analyzes the relationship between the secrecy outage probability p_{out} and the distance D_e between Alice and Eve under the condition that Bob's position remains unchanged ($D_e = 10m$) in the Nakagami-m fading channel. It can be seen from the curves in the figure that the secrecy outage

 doi:10.20944/preprints202501.1851.v1

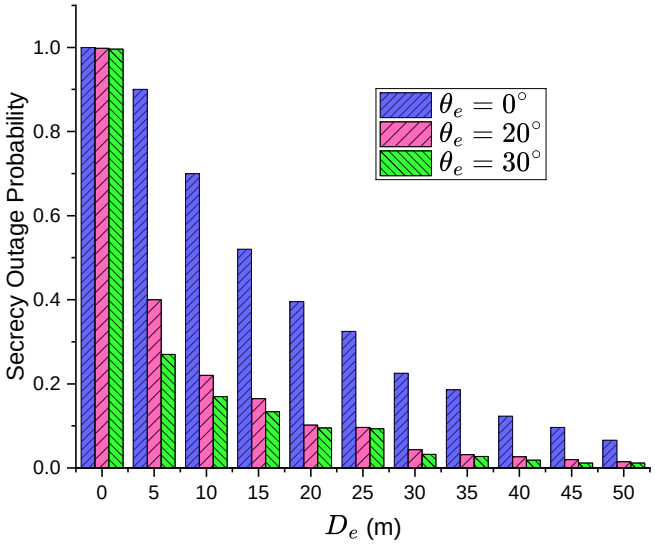

Figure 5. The Relationship between Secrecy Outage Probability and the Distance between Alice and Eve

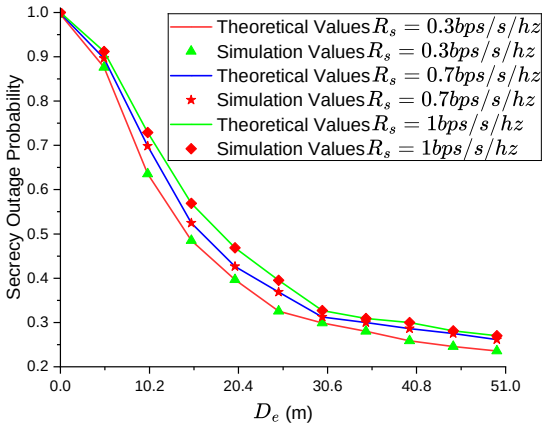

Figure 6. The Impact of Secrecy Rate on Secrecy Outage Probability under Different Values of the Distance between Alice and Eve

probability decreases as D_e increases. When the distance increases to a certain extent, the secrecy outage probability tends to 0, that is, Eve cannot overhear any information. The figure also analyzes the relationship between the secrecy outage probability and the incident angle of Eve relative to Alice. It can be seen from the figure that when $\theta_e = 0$, that is, when Eve is located on the line connecting Alice and Bob, the outage probability is the largest and the secrecy performance is the worst. At this time, Eve is within the main lobe coverage range of Alice's transmitting beam, so the amount of eavesdropped data is the largest. Therefore, when Bob's position is determined, the relationship $p_{out}(\theta_e, D_e) < \varepsilon$ between p_{out} and Eve's position can be used to set a non - secure area with a threshold value of ε. Eve is not allowed to enter the non-secure area, providing a theoretical guidance basis for practical applications. Fig.6 analyzes the relationship between the secrecy outage probability p_{out} and the secrecy rate R_s under the Nakagami-m fading channel, where $D_b = 10$m,θ_b=$\theta_e = 0$. As R_s increases, the secrecy outage probability p_{out} increases accordingly. Therefore, in practical systems, a trade-off between transmission efficiency and confidentiality is required to achieve secure transmission of the system. When $D_e = 0$, the received signal-to-noise ratio of the eavesdropping user tends to infinity, so a secrecy outage event must occur at this time. It can be seen from the figure that the secrecy outage probability is 1 when $D_e = 0$, and the theoretical analysis is consistent with the simulation results. The theoretical and simulation values of the secrecy outage probability are compared in the

 doi:10.20944/preprints202501.1851.v1

figure. It can be seen from the figure that the theoretical and simulation values agree well, further proving the correctness of the theoretical analysis.

5. Conclusions

This paper addresses the physical layer security of the Industrial Internet of Things (IIoT) within the context of a Nakagami-m wiretap channel featuring multiple eavesdroppers. By employing a Poisson point process to model the locations of these eavesdroppers, significant advancements have been made in enhancing both understanding and performance regarding secure communication in IIoT systems. Firstly, a closed-form expression for the upper bound of the Spatial Secrecy Outage Probability (SSOP) has been derived. Through theoretical analysis and simulation, it is demonstrated that factors such as the angle between the legitimate user and the transmitter, as well as the number of transmit antennas, significantly influence SSOP. As the legitimate user's direction deviates from the normal direction of the antenna array, the SSOP tends to increase and shows an oscillatory characteristic. With an increase in the number of antennas, the SSOP and its upper bound decrease and gradually stabilize, indicating that while increasing antennas can improve security to a certain extent, there is a limit. Secondly, the relationship between secrecy rate and secrecy throughput has been investigated. It has been found that as the secrecy rate initially increases, the secrecy throughput also increases. However, when the secrecy rate exceeds a certain value, the decrease in the probability of secure transmission dominates, causing the secrecy throughput to decline. This highlights the need for a trade-off between transmission efficiency and confidentiality in practical systems. Finally, the secure and non-secure regions were analyzed based on the secrecy outage probability. The secrecy outage probability decreases as the distance between the eavesdropper and the transmitter increases, and it reaches its maximum when the eavesdropper is in the same direction as the legitimate user. By defining the non-secure region based on the secrecy outage probability threshold, theoretical guidance for preventing eavesdropping has been provided. In summary, the research in this paper provides valuable theoretical and practical insights for enhancing the physical layer security of IIoT systems. Future work can focus on further optimizing the transmission scheme and security mechanism considering more complex channel models and practical application scenarios to meet the growing security requirements of the IIoT.

Appendix A Appendix A

Theorem A1. *For the average spatial outage probability $\bar{p}_{ssop}$, the exact theoretical closed-form solution of its upper bound is:*

$$\bar{p}_{ssop}^{up}=1-\exp\left[-\lambda_e \pi T(\Omega_k)^{\frac{2}{\alpha}}\left(\begin{array}{l}1+2\sum\limits_{n=1}^{n_t-1}\frac{n_t-n}{n_t}J_0(\pi n)* \\ \cos(\pi n\sin\theta_b)\end{array}\right)^{\frac{2}{\alpha}}\right]$$

When α=2, then $\bar{p}_{ssop}$=$\bar{p}_{ssop}^{up}$

Proof. From the Eq.12, we can conclude $\bar{p}_{ssop}$ can be obtained through numerical calculation, but it is difficult to derive its closed-form expression. Therefore, for the purpose of theoretical analysis, this section mainly derives the closed-form expression $\bar{p}_{ssop}^{up}$ of the upper bound of $\bar{p}_{ssop}$. It can be seen from Eq.12 that the difficulties in deriving the closed-form expression of $\bar{p}_{ssop}$ mainly include: 1. The area A of the non-secure region Θ , as known from Eq.9, A contains the integral of the antenna array factor. When $\alpha > 2$, the integral is difficult to obtain. 2.The expression of $E_{|h_k|}\left[e^{-\lambda_e A}\right]$ contains random variables of Nakagami-m fading. When $\alpha > 2$, the numerical solution is difficult to obtain.

 doi:10.20944/preprints202501.1851.v1

Appendix A.0.1 Solve for the area A of the non-secure region

From the paper[1] we have published, $B_1 = \int_0^{2\pi} \frac{1}{2\pi} \left(G^2(\theta_e, \theta_b)\right)^{\frac{2}{\alpha}} d\theta_e$, We can directly obtain the upper bound of A as follows When α=2.

$$A \leq \pi T \left(|h_k|^2\right)^{\frac{2}{\alpha}} \left(1+2 \sum_{n=1}^{n_t-1} \frac{n_t - n}{n_t} J_0(\pi n) \cos(\pi n \sin \theta_b)\right)^{\frac{2}{\alpha}}$$

Appendix A.0.2 Solve for $E_{|h_k|}\left[e^{-\lambda_e A}\right]$

According to Jensen's inequality $E\left(e^X\right) \geq e^{E(X)}$, to solve for the expected value $E_{|h_k|}\left[e^{-\lambda_e A}\right]$, where X is a random variable. The equality holds only when X is a deterministic value.According to Jensen's inequality, we can obtain:

$$\bar{p}_{ssop}=1 - E_{|h_k|}\left[e^{-\lambda_e A}\right] \leq 1 - e^{-\lambda_e E_{|h_k|}(A)}$$

From the Eq.13, The expected value of A is as follows:

$$E_{|h_k|}(A) \leq \pi T \left(1+2 \sum_{n=1}^{n_t-1} \frac{n_t - n}{n_t} J_0(\pi n) \cos(\pi n \sin \theta_b)\right)^{\frac{2}{\alpha}} E_{|h_k|}\left(\left(|h_k|^2\right)^{\frac{2}{\alpha}}\right)$$

According to Jensen's inequality for $E\left[X^{\frac{2}{\alpha}}\right] \leq (E[X])^{\frac{2}{\alpha}}$, then $E_{|h_k|}\left[\left(|h_k|^2\right)^{2/\alpha}\right] \leq \left(E_{|h_k|}\left[|h_k|^2\right]\right)^{2/\alpha}$. Since the average value of the Nakagami-m fading channel is Ω_k, thus $E_{|h_k|}\left[\left(|h_k|^2\right)^{2/\alpha}\right] \leq (\Omega_k)^{2/\alpha}$. Therefore, the expression for the upper bound of the expected value of A is as follows:

$$\bar{p}^{up}_{ssop}=1 - \exp\left[-\lambda_e \pi T (\Omega_k)^{\frac{2}{\alpha}} \left(1+2 \sum_{n=1}^{n_t-1} \frac{n_t - n}{n_t} J_0(\pi n) \cos(\pi n \sin \theta_b)\right)^{\frac{2}{\alpha}}\right]$$

When α=2, then $\bar{p}_{ssop}=\bar{p}^{up}_{ssop}$, thus the theorem is proved. □

References

1. Liu, X.; Xu, F.; Ning, L. A Novel Approach for the Enhancement of Security through Defining the Spatial Secrecy Outage Probability in the Industrial Internet of Things. *ELECTRONICS* **2024**, *13*.
2. Cai, J.; Wen, L.; Feng, H.; Fang, K.e. An Overview of Security Threats, Attack Detection and Defense for Large-Scale Multi-Agent Systems (LSMAS) in Internet of Things (IoT). *IEEE Transactions on Industrial Cyber-Physical Systems* **2025**, *3*, 70–81.
3. Saeidlou, S.; Ghadiminia, N.; Oti-Sarpong, K. Cyber-physical System Security for Manufacturing Industry 4.0 using LSTM-CNN Parallel Orchestration. *IEEE Access* **2025**, pp. 1–1.
4. Li, Y.; Feng, L.; Tang, C. A Vehicle Path Planning and Prediction Algorithm Based on Attention Mechanism for Complex Traffic Intersection Collaboration in Intelligent Transportation. *IEEE Transactions on Intelligent Transportation Systems* **2024**, pp. 1–12.
5. Houssein, E.H.; Othman, M.A.; Mohamed, W.M. Internet of Things in Smart Cities: Comprehensive Review, Open Issues, and Challenges. *IEEE Internet of Things Journal* **2024**, *11*, 34941–34952.
6. Chen, Y.; He, H.; Liu, S. Physical Layer Authentication for Industrial Control Based on Convolutional Denoising Autoencoder. *IEEE Internet of Things Journal* **2024**, *11*, 15633–15641.
7. Liu, Y.; Chi, C.; Zhang, Y. Identification and Resolution for Industrial Internet: Architecture and Key Technology. *IEEE Internet of Things Journal* **2022**, *9*, 16780–16794.
8. Serror, M.; Hack, S.; Henze, M. Challenges and Opportunities in Securing the Industrial Internet of Things. *IEEE Transactions on Industrial Informatics* **2021**, *17*, 2985–2996.
9. Mcginthy, J.M.; Michaels, A.J. Secure Industrial Internet of Things Critical Infrastructure Node Design. *IEEE Internet of Things Journal* **2019**, *6*, 8021–8037.

10. Yao, P.; Yan, B.; Yang, T. Security-Enhanced Operational Architecture for Decentralized Industrial Internet of Things: A Blockchain-Based Approach. *IEEE Internet of Things Journal* **2024**, *11*, 11073–11086.
11. Ud Din, I.; Bano, A.; Awan, K.A. LightTrust: Lightweight Trust Management for Edge Devices in Industrial Internet of Things. *IEEE Internet of Things Journal* **2023**, *10*, 2776–2783.
12. Cheng, S.H.; Lee, M.H.; Wu, B.C. A Lightweight Power Side-Channel Attack Protection Technique With Minimized Overheads Using On-Demand Current Equalizer. *IEEE Transactions on Circuits and Systems II: Express Briefs* **2022**, *69*, 4008–4012.
13. Ding, Z.; He, D.; Qiao, Q. A Lightweight and Secure Communication Protocol for the IoT Environment. *IEEE Transactions on Dependable and Secure Computing* **2024**, *21*, 1050–1067.
14. Limbasiya, T.; Das, D.; Das, S.K. MComIoV: Secure and Energy-Efficient Message Communication Protocols for Internet of Vehicles. *IEEE/ACM Transactions on Networking* **2021**, *29*, 1349–1361.
15. Wei, N.; Yin, L.; Tan, J. An Autoencoder-Based Hybrid Detection Model for Intrusion Detection With Small-Sample Problem. *IEEE Transactions on Network and Service Management* **2024**, *21*, 2402–2412.
16. Djaidja, T.E.T.; Brik, B.; Senouci.etl, M. Early Network Intrusion Detection Enabled by Attention Mechanisms and RNNs. *IEEE Transactions on Information Forensics and Security* **2024**, *19*, 7783–7793.
17. Khan, R.; Mehmood, A.; Maple, C. Performance Analysis of Blockchain-Enabled Security and Privacy Algorithms in Connected and Autonomous Vehicles: A Comprehensive Review. *IEEE Transactions on Intelligent Transportation Systems* **2024**, *25*, 4773–4784.
18. Liu, Y.; Su, Z.; Wang, Y. Energy-Efficient and Physical-Layer Secure Computation Offloading in Blockchain-Empowered Internet of Things. *IEEE Internet of Things Journal* **2023**, *10*, 6598–6610.
19. Yousuf, T.; Mahmoud. Internet of Things (IoT) Security: Current Status, Challenges and Countermeasures. *International Journal for Information Security Research (IJISR)* **2015**, *5*.
20. Al-Fuqaha, A.; Guizani, M.; Mohammadi, M. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE Communications Surveys and Tutorials* **2015**, *17*, 2347–2376.
21. 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, **2016**.
22. 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, **2011**.
23. Suo, H.; Wan, J.; Zou, C. Security in the Internet of Things: A Review. *IEEE* **2012**.
24. 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.
25. Mcginthy, J.M.; Michaels, A.J. Secure Industrial Internet of Things Critical Infrastructure Node Design. *IEEE Internet of Things Journal* **2019**, *6*, 8021–8037.
26. Lipps, C.; Herbst, J.; Klingel, S. 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.
27. Yu, S.; Wu, F.; Chen, B. 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*, 7826.
28. Chen, H.; Hu, M.; Yan, H. 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). IEEE, **2019**, pp. 365–368.
29. 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.
30. 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). IEEE, **2020**, pp. 268–271.
31. Nguyen, H.N.; Nguyen, N.L.; Nguyen, N.T. Reliable and secure transmission in multiple antennas hybrid satellite-terrestrial cognitive networks relying on NOMA. *IEEE Access* **2020**, *8*, 215044–215056.
32. Liu, M.; Liu, Z.; Lu, W. Distributed few-shot learning for intelligent recognition of communication jamming. *IEEE Journal of Selected Topics in Signal Processing* **2021**, *16*, 395–405.
33. Liu, M.; Wang, J.; Zhao, N. Radio frequency fingerprint collaborative intelligent identification using incremental learning. *IEEE Transactions on Network Science and Engineering* **2021**, *9*, 3222–3233.
34. Liu, M.; Liu, C.; Li, M. Intelligent passive detection of aerial target in space-air-ground integrated networks. *China Communications* **2022**, *19*, 52–63.

35. Zhang, Y.; Woods, R.; Ko, Y. Security Optimization of Exposure Region-Based Beamforming With a Uniform Circular Array. *IEEE Transactions on Communications* **2018**, *66*, 2630–2641. https://doi.org/10.1109/TCOMM.2017.2768516.
36. Zhang, Y.; Ko, Y.; Woods, R. Defining Spatial Secrecy Outage Probability for Exposure Region-Based Beamforming. *IEEE Transactions on Wireless Communications* **2017**, *16*, 900–912. https://doi.org/10.1109/TWC.2016.2633351.
37. Li, B.; Zhou, Z.; Zhang, H. Efficient beamforming training for 60-GHz millimeter-wave communications: A novel numerical optimization framework. *IEEE Transactions on Vehicular Technology* **2013**, *63*, 703–717.
38. Bashar, B.S.; Rhazali, Z.; Elwi, T.A. Antenna Beam forming Technology Based Enhanced Metamaterial Superstrates. In Proceedings of the 2022 IEEE 3rd KhPI Week on Advanced Technology (KhPIWeek). IEEE, **2022**, pp. 1–5.
39. Xiong, Q.; Gong, Y.; Liang, Y.C. Achieving secrecy of MISO fading wiretap channels via jamming and precoding with imperfect channel state information. *IEEE Wireless Communications Letters* **2014**, *3*, 357–360.
40. Barb, G.; Otesteanu, M. Digital GoB-based Beamforming for 5G communication systems. In Proceedings of the 2020 international symposium on antennas and propagation (ISAP). IEEE, **2021**, pp. 469–470.
41. Wang, B.; Mu, P.; Li, Z. Artificial-Noise-Aided Beamforming Design in the MISOME Wiretap Channel Under the Secrecy Outage Probability Constraint. *IEEE Transactions on Wireless Communications* **2017**, *16*, 7207–7220.
42. Hu, L.; Wen, H.; Wu, B. Cooperative-Jamming-Aided Secrecy Enhancement in Wireless Networks With Passive Eavesdroppers. *IEEE Transactions on Vehicular Technology* **2018**, *67*, 2108–2117.
43. Li, Z.; Mu, P.; Li, Z. An Adaptive Transmission Scheme for Slow Fading Wiretap Channel with Channel Estimation Errors. In Proceedings of the IEEE Globecom 2016, **2016**.
44. 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.
45. 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). IEEE, **2022**, pp. 338–343.
46. Xie, R.; Tang, Q.; Liang, C. Dynamic computation offloading in IoT fog systems with imperfect channel-state information: A POMDP approach. *IEEE Internet of Things Journal* **2020**, *8*, 345–356.
47. 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.
48. Niu, H.; Xiao, Y.; Lei, X. 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). IEEE, **2022**, pp. 1–5.
49. Xia, G.; Lin, Y.; Liu, T. Transmit antenna selection and beamformer design for secure spatial modulation with rough CSI of Eve. *IEEE Transactions on Wireless Communications* **2020**, *19*, 4643–4656.
50. 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). IEEE, **2022**, pp. 1–5.
51. Wang, J.; Lee, J.; Wang, F. Jamming-aided secure communication in massive MIMO Rician channels. *IEEE Transactions on Wireless Communications* **2015**, *14*, 6854–6868.
52. Sarma, S.; Shukla, S.; Kuri, J. Joint scheduling & jamming for data secrecy in wireless networks. In Proceedings of the 2013 11th International Symposium and Workshops on Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks (WiOpt). IEEE, **2013**, pp. 248–255.
53. Li, H.; Wang, X.; Hou, W. Security enhancement in cooperative jamming using compromised secrecy region minimization. In Proceedings of the 2013 13th Canadian Workshop on Information Theory. IEEE, **2013**, pp. 214–218.
54. Zhang, W.; Chen, J.; Kuo, Y. Artificial-Noise-Aided Optimal Beamforming in Layered Physical Layer Security. *IEEE Communications Letters* **2019**, *23*, 72–75.
55. Liu, X.; Gao, Y.; Zang, G. Artificial-Noise-Aided Robust Beamforming for MISOME Wiretap Channels with Security QoS. *IEEE* **2019**.
56. Li, B.; Zou, Y.; Zhou, J. Secrecy Outage Probability Analysis of Friendly Jammer Selection Aided Multiuser Scheduling for Wireless Networks. *IEEE Transactions on Communications* **2019**, pp. 1–1.
57. Wang, X.; Mu, P.; Zhang.etl. Secrecy CPS transmission scheme for slow fading independent parallel wiretap channels with new SOP constraint. **2018**, pp. 1–6.

 doi:10.20944/preprints202501.1851.v1

58. Zhou, Y.; Yeoh, P.L.; Chen, H. Improving Physical Layer Security via a UAV Friendly Jammer for Unknown Eavesdropper Location. *IEEE Transactions on Vehicular Technology* **2018**, *67*, 11280–11284.