sensors

MDPI

Article

Defending Against Randomly Located Eavesdroppers by Establishing a Protecting Region

Tao Li [1], Chaozheng Xue [1,*], Yongzhao Li [1] and Octavia A. Dobre [2]

[1] State Key Laboratory of Integrated Service Network, Xidian University, Xi'an 710071, China; taoli@xidian.edu.cn (T.L.); yzli@mail.xidian.edu.cn (Y.L.)

[2] Department of Electrical and Computer Engineering, Memorial University, St. John's, NL A1B 3X5, Canada; odobre@mun.ca

* Correspondence: chaozhengxue@gmail.com

Received: 13 November 2019; Accepted: 8 January 2020; Published: 13 January 2020

Abstract: The security problem in wireless sensor networks faces severe challenges, due to the openness of the sensor network channel and the mobility and diversity of the terminals. When facing randomly located eavesdroppers, the situation is much more complex. This paper studies the security performance of a wireless sensor network where randomly located passive and active eavesdroppers are both considered. Compared to a passive eavesdropper, an active eavesdropper can perform both eavesdropping and malicious jamming simultaneously in a wireless sensor network. Based on beamforming and artificial noise (AN), we propose a practical way to defend against the eavesdropper by establishing a protecting region. An appropriate metric, the hybrid outage probability, which takes both the transmission outage probability and the secrecy outage probability into consideration, is utilized to evaluate the security performance. In addition, the concept of safe transmission range is defined to evaluate the security performance. Simulation results are provided to depict the insecure region and verify the harm of the active eavesdropper to the transmission in the wireless sensor network.

Keywords: physical layer security; eavesdropper; outage probability; insecure region

1. Introduction

Along with the emergence of numerous wireless devices and various wireless services, wireless security has become a critical design issue in the implementation and operation of wireless sensor networks [1–4]. Against this background, physical layer security (PLS) has been receiving great research attention [5]. Compared to traditional key-based cryptographic techniques applied to upper layers which can be deciphered, PLS which exploits the channel characters to enhance security, can safeguard wireless data transmissions without requiring secret keys and complex algorithms [6–8]. The main design goal of PLS is to increase the performance difference between the link of the legitimate receiver and that of the eavesdropper by using well-designed transmission schemes in the wireless sensor networks [9]. In particular, beamforming and artificial noise (AN) are exploited to improve the security performance [10–13]. Most works assume that eavesdroppers work with a passive way in the wireless sensor networks. However, there are also active eavesdroppers who can eavesdrop information in a more "smart" way. An active eavesdropper, which can perform both eavesdropping and malicious jamming simultaneously, brings an intractable challenging security problem [14–24].

One of the active eavesdropping methods is pilot contamination in a wireless sensor network. The eavesdropper attacked the training phase to cause pilot contamination in wireless communication to improve its eavesdropping performance [14–16]. Another active eavesdropping method is jamming. In the presence of an active eavesdropper, the authors in [17,18] calculated an optimal power allocation

to improve the security performance of transmission. In [19,20], the properties of the game equilibrium were exploited to design a transmission strategy and a jamming strategy, where the eavesdropper took action first as the leader and the legitimate user acts as the follower in the wireless network. In [21], a three-stage Stackelberg game approach was proposed to improve the security performance under the competitions among the transmitter, relays and active eavesdropper. Finding the Stackelberg equilibrium of the scheme, and the legitimate users can achieve cooperative communication to improve the secrecy capacity and to defend against full-duplex active eavesdropping attacks. A novel transmission outage constrained scheme for both reliability and security was proposed to evaluate the secrecy performance and to gain valuable design insights in [22]. An optimal relay selection scheme was developed to improve the security performance with an active eavesdropper in cooperative wireless networks in [23,24].

These works mainly focused on adjusting the transmission strategies to obtain a better performance under the effect of self interference at the active eavesdropper and neglected the location of the eavesdropper in the wireless sensor networks. However, in practice, the location of the eavesdropper is unknown and this can change its location to cause severe interference for the transmission with small power. In this case, the above transmission strategies do not work well, which brings an intractable challenge for the transmission. Hence, the location of the active eavesdropper, as a vital parameter, has to be considered.

Under the assumption that the eavesdropper is passive, the authors in [25,26] revealed that the uncertainty on the location of the eavesdropper should be seriously taken into account for deploying a wireless sensor network system. A piecewise function was proposed to approximate the line-of-sight (LoS) probability for the air-to-ground links, which provides a better approximation than using the existing sigmoid-based fitting under randomly located unmanned aerial vehicle eavesdroppers [27]. The secrecy outage analysis of the randomly located eavesdroppers, which act independently and collude to intercept the transmitted message, was studied in [28]. The insecure region refers to a geographical area where certain security metrics such as average secrecy capacity and secrecy outage probability are not satisfied [29–34]. In [29], both the legitimate receiver and transmitter generated AN to impair the eavesdropper's channel, and the insecure region was defined by the average secrecy capacity to characterise the security performance when the eavesdropper's channel was unknown. A concept of outage secrecy region to evaluate the secrecy performance from a geometrical perspective was proposed in [30], where the legitimate receiver generated AN to impair the eavesdropper's channel. However, the approximate secrecy capacity was not accurate to define the insecure region. Then, outage probability, as a more appropriate metric, was exploited to determine the insecure region [31–34]. Authors examined the impact of the unmanned aerial vehicle jamming power and its three-dimensional spatial deployment on the outage probability of the legitimate receiver and the intercept probability of the eavesdropper. The security region was defined by the intercept probability [31]. In [32], one relay node in the sensor networks can improve the security by decreasing the area in which the eavesdropper can reside and listen to the information transmitted to the destination. This region was called vulnerability region with its characterization. In [33,34], with the design of AN, high outage performance around the around the transmitter was achieved.

Inspired by the above works, we propose a practical way to defend against an active eavesdropper by establishing a protecting region to restrict the location of an active eavesdropper in a wireless sensor network. Since the eavesdropper is able to emit a jamming signal to interfere with the transmission, the traditional metrics are not appropriate in this case, and a new metric, namely hybrid outage probability, is exploited to evaluate the security performance. Specifically, we derive the expression of the hybrid outage probability which takes both the transmission outage probability and the secrecy outage probability into consideration both for active and passive eavesdropper. Based on it, the insecure region is defined to confront the eavesdropper. And the concept safe transmission range, as a valuable indicator, is proposed. In our system, the AN is generated from receiver. This method has the following advantages. (a) The CSI is not needed by Alice, so there is no feedback channel and thus the bandwidth

resource is saved; (b) The AN can be generated by either multiple antennas or a single antenna, which is more practical than the existing AN methods which need multiple antennas at the transmitter; (c) It is particularly useful when the receiver has a stronger ability than the transmitter; (d) It is efficient if Eves are located around Bob [29,30,35]. Our analysis can be used in various practical sensor networks to provide valuable basis for establishing the protecting region and achieve secure transmission.

2. System Model

We consider a multiple-input single-output (MISO) system in the presence of a full-duplex active eavesdropper (We assume that the distribution of location of eavesdropper is a homogeneous Poisson point process, and the eavesdropper works independently. In this case, an eavesdropper with changeable location can be popularized to multiple randomly located eavesdroppers.), as shown in Figure 1. Alice with N_a uniform linear array (ULA) antennas aims to transmit a confidential signal to Bob. In order to enhance the secrecy performance, beamforming is utilized at Alice. Bob and randomly located Eve are both equipped with one receiving antenna and one transmitting antenna [17,18]. Bob simultaneously receives the signal from Alice and emits the AN signal omnidirectionally to confuse the potential eavesdropper, while Eve simultaneously eavesdrops the signal from Alice and transmits jamming signal to interfere with the transmission. Since the full duplex capability at Bob, we assume the cancellation is not perfect. h_{bb} is the residual self interference after the self-interference cancellation. It is often assumed that the self-interference can be significantly suppressed [36], so that h_{bb} can be regarded as an independent Rayleigh distributed variable [37]; and $\rho \in [0, 1]$ is the linear residual self-interference coefficient. As for Eve, since the legitimate users cannot obtain the information of Eve, the worst case that Eve's self-interference can be eliminated perfectly is considered for the robust design.

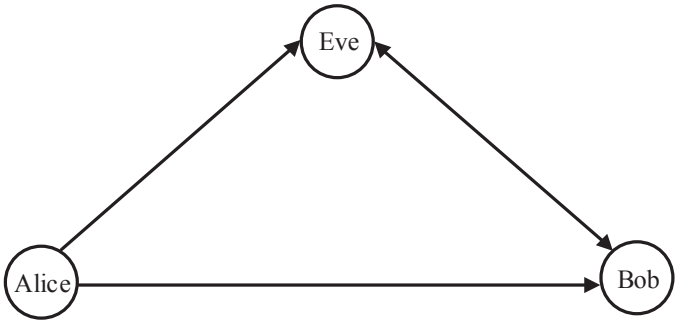

Figure 1. System model.

The main channel and the wiretap channel can be expressed as $1 \times N_a$ vector $\mathbf{h}_{ab}$ and $\mathbf{h}_{ae}$, respectively. Besides, the scalar h_{be} and h_{eb} represent the channels from Bob to Eve and Eve to Bob, respectively. All channels are assumed to be the flat Rayleigh fading. We assume that the Eve's CSI and location are unknown to both Alice and Bob and the full CSI of Bob is available for Alice. The received signals at Bob and Eve are respectively expressed as

$$y_b^{\text{act}} = \sqrt{\phi P}\mathbf{h}_{ab}\mathbf{w}_a x_a + \sqrt{P_e}h_{eb}x_e + \sqrt{\rho\left(1-\phi\right)P}h_{bb}x_b + n_b \tag{1}$$

and

$$y_e = \sqrt{\phi P}\mathbf{h}_{ae}\mathbf{w}_a x_a + \sqrt{\left(1-\phi\right)P}h_{be}x_b + n_e, \tag{2}$$

where $\mathbf{w}_a$ represents the $N_a \times 1$ beamforming vector at Alice, and the superscript $[\cdot]^{\text{H}}$ represents Hermitian conjugate. Under the assumption that perfect CSI of Bob is assumed to be known for Alice, the optimal beamforming is designed as $\mathbf{w}_a = \mathbf{h}_{ab}^{\text{H}}/\|\mathbf{h}_{ab}\|$ to enhance the receiving performance of Bob [38]. The confidential signal from Alice, the AN from Bob, and the jamming signal from Eve are

respectively denoted by scalar x_a, x_b, and x_e with unit power, i.e., $\mathbb{E}\left[|x_a|^2\right] = \mathbb{E}\left[|x_b|^2\right] = \mathbb{E}\left[|x_e|^2\right] = 1$. The total transmission power is denoted by P, which includes the confidential signal power from Alice and the AN power from Bob; and ϕ is the power allocation factor between the confidential signal from Alice and the AN signal from Bob. The jamming signal power from Eve is denoted by P_e. n_b and n_e are additive white Gaussian noises with powers σ_b^2 and σ_e^2, respectively. As our system model is also compatible with the passive Eve, i.e., when $P_e = 0$, Eve becomes passive. Then, the received signal at Bob is

$$y_b^{\text{pas}} = \sqrt{\phi P}\mathbf{h}_{ab}\mathbf{w}_a x_a + \sqrt{\rho\left(1-\phi\right)P}h_{bb}x_b + n_b. \tag{3}$$

3. Insecure Region Analysis

In this section, the correctness of the hybrid outage probability for active Eve is verified firstly. Subsequently, the expression of the hybrid outage probability is derived. Based on it, the insecure region and safe transmission range are defined to evaluate the security performance.

3.1. Hybrid Outage Probability

From (1) and (2), the signal-to-interference-noise ratio (SINR) at Bob and active Eve can be respectively calculated as (This paper aims to establish the insecure region to defend against the active eavesdropper and achieve a higher security performance. The self-interference is beyond our main focus. This is modeled as a variable depending on the ability of Bob, according to [18,22]. The value of self-interference is changed with ρ.)

$$\gamma_b^{\text{act}} = \frac{\phi P_a \lambda d_{ab}^{-\beta}\left\|\mathbf{h}_{ab}\mathbf{w}_a\right\|^2}{P_e\lambda d_{be}^{-\beta}\left|h_{eb}\right|^2 + \rho\left(1-\phi\right)P + \sigma_b^2} \tag{4}$$

and

$$\gamma_e = \frac{\phi P \lambda d_{ae}^{-\beta}\left\|\mathbf{h}_{ae}\mathbf{w}_a\right\|^2}{\left(1-\phi\right)P\lambda d_{be}^{-\beta}\left|h_{be}\right|^2 + \sigma_e^2}, \tag{5}$$

where $\|\cdot\|$ denotes the Euclidean norm, d_{ab}, d_{ae}, and d_{be} represent the distances between Alice and Bob, Alice and Eve, Bob and Eve, respectively, λ is a constant which depends on the propagation model and carrier frequency, $\beta \geq 2$ is the path-loss exponent. When Eve is passive, from (3), the SINR at Bob is

$$\gamma_b^{\text{pas}} = \frac{\phi P_a \lambda d_{ab}^{-\beta}\left\|\mathbf{h}_{ab}\mathbf{w}_a\right\|^2}{\rho\left(1-\phi\right)P + \sigma_b^2}. \tag{6}$$

The secrecy capacity is expressed as [29,30]

$$C_s = \begin{cases} C_b - C_e, & \textit{under } C_b > C_e; \\ 0, & \textit{under } C_b \leq C_e, \end{cases} \tag{7}$$

where $C_b = \log_2\left(1+\gamma_b\right)$ is the main channel capacity between Alice and Bob. $C_e = \log_2\left(1+\gamma_e\right)$ is the wiretap channel capacity between Alice and Eve. Since the CSI of the wiretap channel is unavailable, the instantaneous secrecy capacity is unobtainable. Thus, the outage probability is a more suitable metric for our system.

If the secrecy transmission rate is assumed to be R_s, the entire event space of communication can be divided into three mutually exclusive events [39]:

- Transmission outage event occurs when $C_b \leq R_s$. In this case, we find $C_e = C_b - R_s < 0$, which conflicts with the fact that $C_e > 0$. As such, R_s is not supported by the main channel and Alice can not transmit a signal.

- Secrecy outage event occurs when $C_s < R_s$ and $C_b > R_s$. In this case, as some information on the confidential signal can be known by Eve, perfect secrecy cannot be achieved.
- Secure transmission event occurs when $C_s \geq R_s$. In this case, perfect secrecy can be guaranteed.

In the conventional scenario where Eve is passive, the main performance metric is secrecy outage probability. However, in our system, Eve can emit malicious interference to destroy the transmission, which causes the transmission outage event. In this case, the secrecy outage probability cannot evaluate the performance comprehensively. Hence, we adopt the hybrid outage probability as performance metric, as follows

$$P_{\text{ho}}\left(\theta, d_{ae}, d_{be}\right) = P_{\text{to}}\left(\theta, d_{ae}, d_{be}\right) + P_{\text{so}}\left(\theta, d_{ae}, d_{be}\right), \tag{8}$$

where $P_{\text{to}}\left(\theta, d_{ae}, d_{be}\right)$ represents the transmission outage probability and $P_{\text{so}}\left(\theta, d_{ae}, d_{be}\right)$ represents the secrecy outage probability. Meanwhile, the hybrid outage probability is also applicable to passive Eve.

In order to obtain the expressions of the outage probabilities, we present the statistics of γ_b^{act} and γ_e. From the right hand side of (4), we find the numerator follows a chisquared distribution since $\|\mathbf{h}_{ab}\|^2$ is a sum of the squares of N_a independent Gaussian random variables; and the denominator follows an exponential distribution. Meanwhile, as the numerator and denominator are independent, we apply

$$F_{\frac{X}{Y+1}}\left(\gamma\right) = \Pr\left(\frac{x}{y+1} < \gamma\right) = \int_0^\infty \left(y+1\right) f_X\left(\gamma\left(y+1\right)\right) f_Y\left(y\right) dy \tag{9}$$

to obtain the cumulative distribution functions (CDF) of γ_b^{act} as

$$F_{\gamma_b}^{\text{act}}\left(\gamma\right) = 1 - \frac{1}{k_2}\exp\left(-\frac{\gamma}{k_1}\right)\sum_{n=1}^{N_a}\frac{1}{(n-1)!}\left(\frac{\gamma}{k_1}\right)^{n-1}\sum_{m=0}^{n-1}\frac{(n-1)!}{(n-m-1)!}\left(\frac{1}{k_2}+\frac{\gamma}{k_1}\right)^{-(m+1)}, \tag{10}$$

where

$$k_1 = \frac{\lambda d_{ab}^{-\beta}\phi P}{\rho\left(1-\phi\right)P + \sigma_b^2}$$

and

$$k_2 = \frac{\lambda d_{be}^{-\beta} P_e}{\rho\left(1-\phi\right)P + \sigma_b^2}.$$

We now derive the CDF of γ_e. Due to the fact that the beamforming vector $\mathbf{w}_a$ at Alice is independent from eavesdropper's channel $\mathbf{h}_{ae}$, the denominator follows exponentially distributed; and the numerator is also exponentially distributed. Similarly, the numerator and denominator are independent. With the help of (9), the CDF of γ_e is

$$F_{\gamma_e}\left(\gamma\right) = 1 - \frac{k_3}{k_4\gamma + k_3}\exp\left(-\frac{\gamma}{k_3}\right), \tag{11}$$

where

$$k_3 = \frac{\lambda d_{ae}^{-\beta}\phi P}{\sigma_e^2}$$

and

$$k_4 = \frac{\lambda d_{be}^{-\beta}\left(1-\phi\right)P}{\sigma_e^2}.$$

According to the definition of the transmission outage event with active Eve, we have

$$\begin{aligned} &P_{\text{to}}^{\text{act}}\left(\theta, d_{ae}, d_{be}\right) = \Pr\left(0 < C_b \leq R_s\right) = \Pr\left(0 < \gamma \leq 2^{R_s}-1\right) = F_{\gamma_b}^{\text{act}}\left(2^{R_s}-1\right) \\ &= 1 - \tfrac{1}{k_2}\exp\left(-\tfrac{2^{R_s}-1}{k_1}\right)\sum_{n=1}^{N_a}\tfrac{1}{(n-1)!}\left(\tfrac{2^{R_s}-1}{k_1}\right)^{n-1}\sum_{m=0}^{n-1}\tfrac{(n-1)!}{(n-m-1)!}\left(\tfrac{1}{k_2}+\tfrac{2^{R_s}-1}{k_1}\right)^{-(m+1)}. \end{aligned} \tag{12}$$

The hybrid outage probability in (8) can be re-expressed as

$$\begin{aligned} P_{\text{ho}}(\theta, d_{ae}, d_{be}) &= P_{\text{to}}(\theta, d_{ae}, d_{be}) + P_{\text{so}}(\theta, d_{ae}, d_{be}) \\ &= \Pr(C_b \le R_s) + \Pr(C_b < R_s + C_e, C_b > R_s) \\ &= \Pr(0 < C_b < R_s + C_e) \\ &= \Pr\left(0 < \gamma_b < 2^{R_s}(1+\gamma_e) - 1\right) \\ &= \int_0^{\infty} \int_0^{2^{R_s}(1+\gamma_e)-1} f_{\gamma_b}(\gamma_b) f_{\gamma_e}(\gamma_e)\, \mathrm{d}\gamma_b \mathrm{d}\gamma_e \\ &= \int_0^{\infty} f_{\gamma_e}(\gamma_e) F_{\gamma_b}\left(2^{R_s}(1+\gamma_e) - 1\right) \mathrm{d}\gamma_e. \end{aligned} \tag{13}$$

Then, from (11), the probability density function (PDF) of γ_e can be derived as

$$f_{\gamma_e}(\gamma) = \left(\frac{k_3 k_4}{(k_3 + k_4\gamma)^2} + \frac{1}{k_3 + k_4\gamma}\right) \exp\left(-\frac{\gamma}{k_3}\right). \tag{14}$$

By substituting (9) and (13) into (12), the hybrid outage probability in the presence of an active Eve is derived as

$$\begin{aligned} P_{\text{ho}}^{\text{act}}(\theta, d_{ae}, d_{be}) = \; & 1 - \tfrac{1}{k_2} \int_0^{\infty} \exp\left(-\left(\tfrac{\gamma_e}{k_3} + \tfrac{2^{R_s}(1+\gamma_e)-1}{k_1}\right)\right) \\ & \sum_{n=1}^{N_a} \left(\tfrac{2^{R_s}(1+\gamma_e)-1}{k_1}\right)^{n-1} \sum_{m=0}^{n-1} \tfrac{1}{(n-m-1)!} \left(\tfrac{1}{k_2} + \tfrac{2^{R_s}(1+\gamma_e)-1}{k_1}\right)^{-(m+1)} \\ & \left(\tfrac{k_3 k_4}{(k_4\gamma_e + k_3)^2} + \tfrac{1}{k_4\gamma_e + k_3}\right) d\gamma_e. \end{aligned} \tag{15}$$

It is clear that the secrecy outage probability can be calculated through (15) and (12) with the help of (8).

From (6), $\|\mathbf{h}_{ab}\|^2$ is a sum of the squares of N_a independent Gaussian random variables, the CDF of γ_b^{pas} is

$$F_{\gamma_b}^{\text{pas}}(\gamma) = 1 - \exp\left(-\frac{\gamma}{k_1}\right) \sum_{n=0}^{N_a-1} \frac{1}{n!} \left(\frac{\gamma}{k_1}\right)^n \tag{16}$$

The analysis of the outage probability expressions with passive Eve are similar. The transmission outage probability and the hybrid outage probability are derived, as follows

$$P_{\text{to}}^{\text{pas}}(\theta, d_{ae}, d_{be}) = 1 - \exp\left(-\frac{2^{R_s} - 1}{k_1}\right) \sum_{n=0}^{N_a-1} \frac{1}{n!} \left(\frac{2^{R_s} - 1}{k_1}\right)^n \tag{17}$$

and

$$\begin{aligned} P_{\text{ho}}^{\text{pas}}(\theta, d_{ae}, d_{be}) = \; & 1 - \int_0^{\infty} \exp\left(-\left(\tfrac{\gamma_e}{k_3} + \tfrac{2^{R_s}(1+\gamma_e)-1}{k_1}\right)\right) \\ & \left(\tfrac{k_3 k_4}{(k_4\gamma_e + k_3)^2} + \tfrac{1}{k_4\gamma_e + k_3}\right) \sum_{n=0}^{N_a-1} \tfrac{1}{n!} \left(\tfrac{2^{R_s}(1+\gamma_e)-1}{k_1}\right)^n d\gamma_e \end{aligned} \tag{18}$$

where $\text{Ei}(\cdot)$ is the exponential integral function [40].

3.2. Insecure Region and Safe Transmission Range

As mentioned above, the insecure region Ω is the set of the eavesdropper's locations where the hybrid outage probability is larger than a given threshold denoted by $0 < \varepsilon < 1$; this is expressed as

$$\Omega = \left\{(\theta, d_{ae}, d_{be}) \,|P_{\text{ho}}(\theta, d_{ae}, d_{be}) > \varepsilon\right\}. \tag{19}$$

According to the definition of insecure region, we can establish the protecting region, where Eve is not allowed to enter to achieve secure transmission in a real communication scenario.

Eve emitting a jamming signal also brings the risk of being detected. We assume that if the jamming power from Eve increases to a certain threshold P_e^{th}, it will be exposed. When Eve is located near Alice, it can intercept the confidential signal easily; when Eve is located near Bob, it can damage the legitimate transmission with small power. Hence, not only the region around Alice but also around Bob is insecure. When the jamming signal power from Eve P_e equals P_e^{th}, the boundary of the insecure region can be obtained.

In addition, for the worst case that Eve appears on the line between Alice and Bob, it can also obtain the power gain from Alice's beamforming. The safe transmission range is defined by $P_{\text{ho}} < \varepsilon$, as shown in Figure 2. This range is denoted by d_s, and helps delineating the circular protecting region around Alice and Bob.

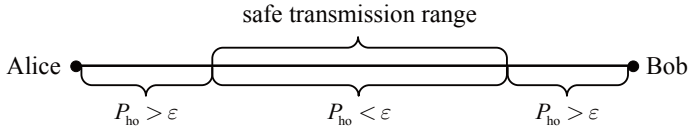

Figure 2. Safe transmission range.

4. Numerical Results

Simulation results are conducted to show the insecure region defined by the hybrid outage probability. Unless otherwise mentioned, the default simulation parameters are as listed in Table 1. All channels experience Rayleigh fading, i.e, $\lambda = 1$. The boundary of the insecure region is obtained when the jamming signal power $P_e = P_e^{\text{th}}$. The outage probabilities are calculated over 1000 trials of Monte Carlo simulations.

Table 1. Simulation Parameters.

Parameters	Values
Number of antennas in Alice N_a	4
Distance between Alice and Bob d_{ab}	100 m
Total transmission power P	10 W
Power allocation factor ϕ	0.1
Jamming signal power P_e^{th}	15 dBm
Secrecy transmission rate R_s	0.3 bps/Hz
Threshold ε	0.2
Path loss exponent β	2
Linear residual coefficient ρ	10^{-8}

Figures 3–7 show the insecure regions with active Eve and passive Eve, respectively. The region represents the secure region where $P_{\text{ho}} < \varepsilon$, while the yellow region represents the insecure region where $P_{\text{ho}} > \varepsilon$. Compared with the passive Eve in Figure 7, one can see that the active Eve increases the insecure region, and the region around Bob is also insecure. Since the jamming signal from Eve can interfere with Bob, which makes the insecure region also look approximately like a disc around Bob. On the other hand, the confidential signal is transmitted from Alice, Eve appears around Alice can eavesdrop the confidential signal, which makes the insecure region look approximately like a disc around Alice. As for the active Eve in Figures 3 and 4, when a large number of antennas are applied in Alice, the size of insecure region will diminish. Because the multi-antenna gain makes Bob receive the confidential signal more easily. Although it also benefits to the eavesdropper to eavesdrop the confidential signal, the gain from beamforming increases the performance difference between the link of the legitimate receiver and that of the eavesdropper, and from Figures 3 and 5, when P_e^{th} increases, the insecure region enlarges, since Eve can interfere with the transmission at a further location. It is

noted that the insecure region enlarges when ρ increases from Figures 3 and 6 since that the AN from Bob effects itself much more. When the insecure region is determined, the secure transmission can be achieved by protecting the insecure region, which is easy to conduct due to its regular circular shape.

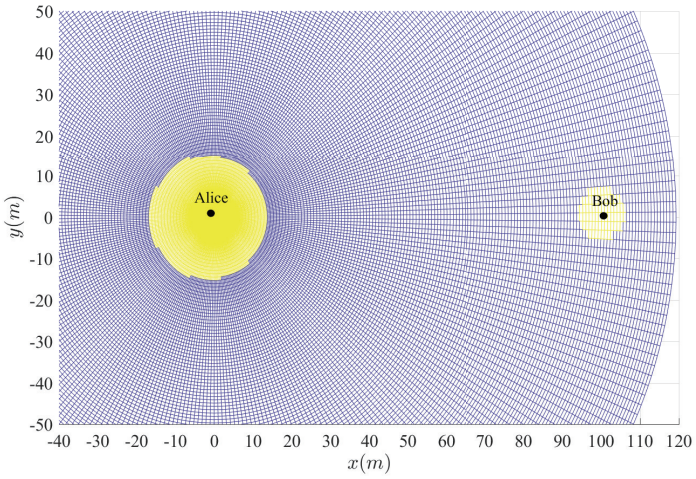

Figure 3. Insecure region with $P_e^{\text{th}} = 15$ dBm, $N_a = 4$ and $\rho = 10^{-8}$.

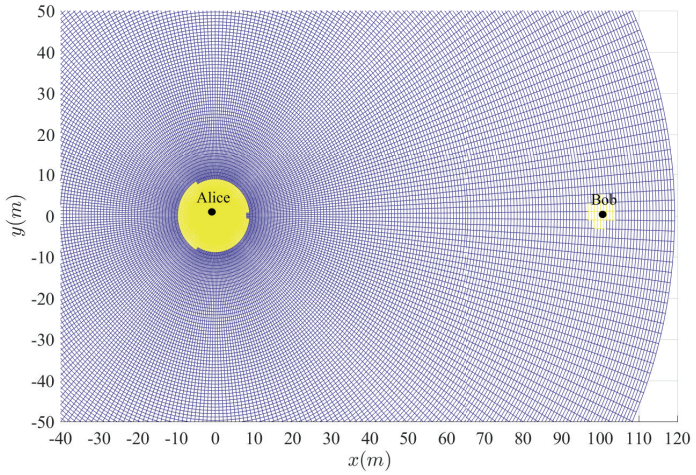

Figure 4. Insecure region with $P_e^{\text{th}} = 15$ dBm, $N_a = 10$ and $\rho = 10^{-8}$.

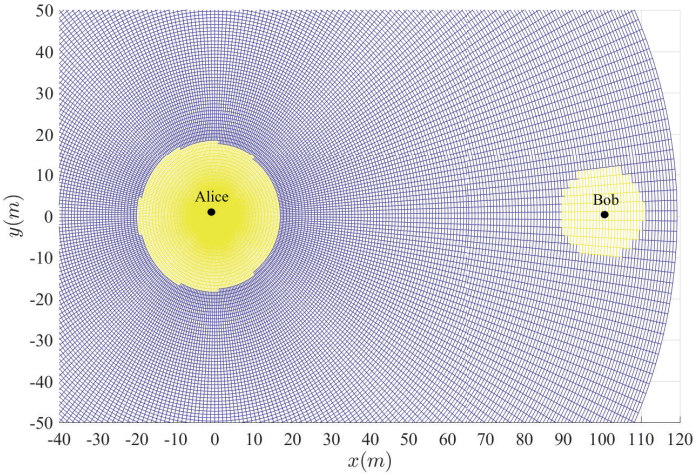

Figure 5. Insecure region with $P_e^{\text{th}} = 20$ dBm, $N_a = 4$ and $\rho = 10^{-8}$.

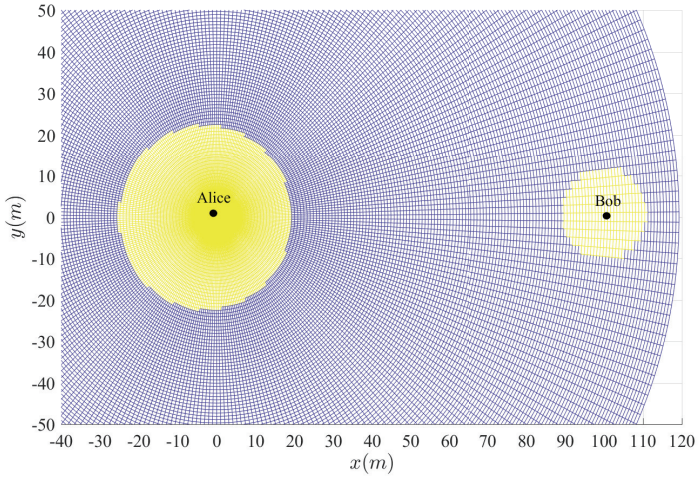

Figure 6. Insecure region with $P_e^{\text{th}} = 20$ dBm, $N_a = 4$ and $\rho = 10^{-6}$.

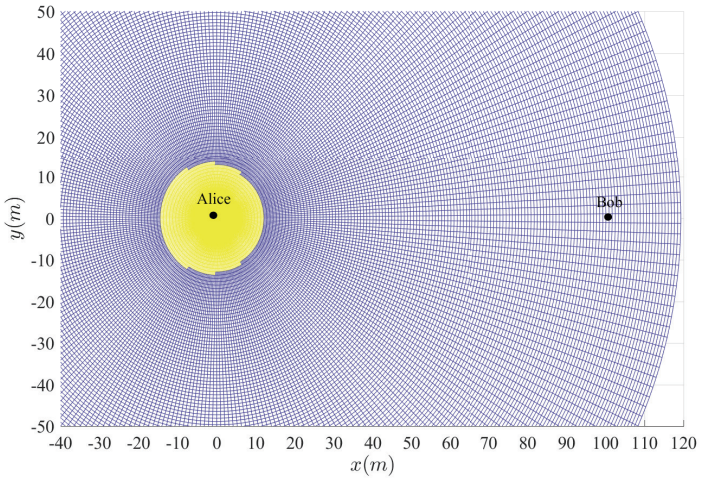

Figure 7. Insecure region with passive Eve and $N_a = 4$ and $\rho = 10^{-8}$.

In the following, we consider that Eve is located on the line between Alice and Bob, and the change trend between Alice and Bob is analyzed.

Figure 8 presents the hybrid outage probability P_{ho} and the transmission outage probability P_{to} versus d_{ae} with different P_e^{th}. For passive Eve, $P_{\text{ho}}^{\text{pas}}$ decreases with the increase of d_{ae}, due to the fact that the power of the received confidential signal decreases and the power of the received AN from Bob increases. On the other hand, $P_{\text{to}}^{\text{pas}}$ is a constant, which is easily verified from (17). For active Eve, when increasing d_{ae}, the significant difference of $P_{\text{ho}}^{\text{act}}$ from passive Eve $P_{\text{ho}}^{\text{pas}}$ is the change around Bob. The main reason is that $P_{\text{to}}^{\text{act}}$ dramatically increases around Bob, since the jamming signal from Eve causes significant damage to Bob. When P_e^{th} decreases, one notices that the width of the peak around Bob decreases, which means that the insecure region around Bob diminishes, and the safe transmission range d_s increases. According to the safe transmission range, the circular protecting region around Alice and Bob can be conducted.

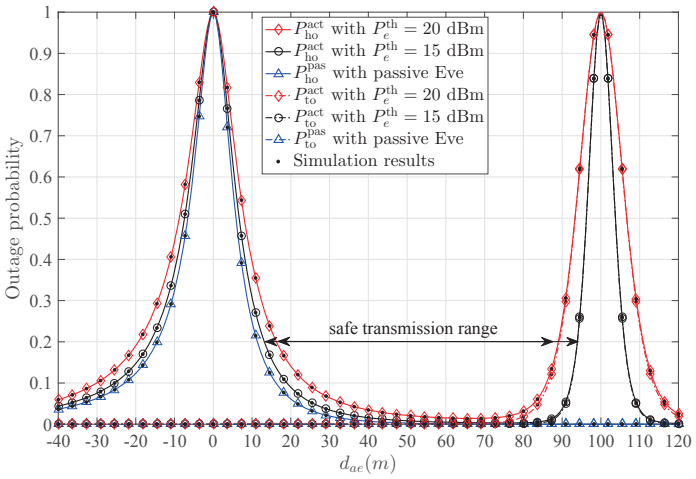

Figure 8. The influence of P_e^{th} on the outage probability.

Figure 9 depicts the transmission outage probability P_{to} and the secrecy outage probability P_{so} versus d_{ae} with different ϕ. As ϕ increases, P_{so} increases while P_{to} decreases; this is because increasing the power of the confidential signal is beneficial to the establishment of transmission between Alice and Bob, but also increases the risk of eavesdropping. Note that P_{to} represents the reliability of the transmission. Thus, a reasonable trade-off between transmission reliability and security should be considered. Meanwhile, the variation trend of P_{so} is the same for both active and passive Eve, which means that the active Eve mainly interferes with the establishment of the legitimate transmission link between Alice and Bob, and it can dramatically increase $P_{\text{to}}^{\text{act}}$ by moving around Bob.

Figure 10 shows the influence of β, R_s, and ρ on the hybrid outage probability, respectively. It is clear that when β increases, the security performance decreases, since the communication condition is worse. When R_s decreases, the security performance increases, as more power can be used to transmit the AN signal. As ρ increases, the security performance decreases, since the self-interference at Bob causes more damage to the transmission. It is worth noting that numerical results are consistent with the simulation results.

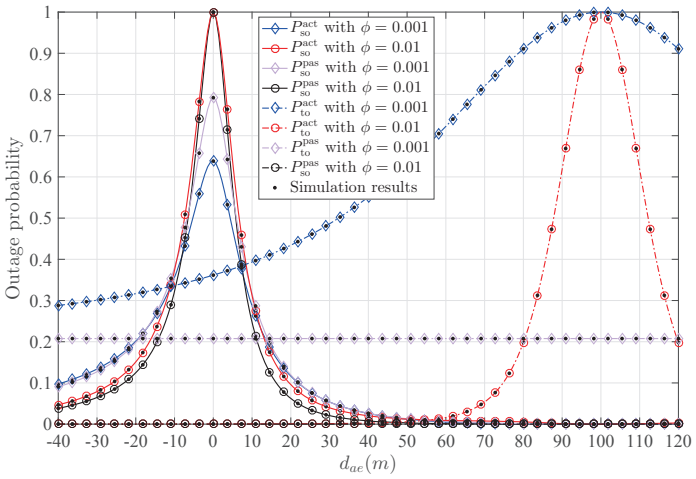

Figure 9. The influence of ϕ on the outage probability.

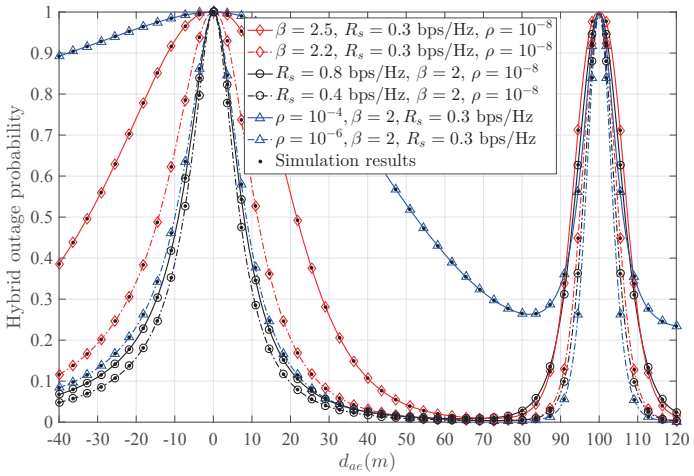

Figure 10. The influence of R_s, β, and ρ on the hybrid outage probability $P_{\text{ho}}^{\text{act}}$.

Figure 11 shows the influence of P_e^{th} and ϕ on d_s. The top and bottom surfaces represent the positions of the right and left endpoints of the safe transmission range, respectively, with distance d_s between them. The insecure region around Bob corresponding to the top surface mainly depends on P_e^{th}, while the insecure region around Alice corresponding to the bottom surface mainly depends on ϕ. Furthermore, when P_e^{th} increases, Eve can interfere with Bob from a further location, which causes the decrease of d_s. The increase of ϕ makes it easier to intercept, which causes the decrease of d_s as well. Obviously, all simulation results show that the active Eve can cause a higher outage probability, and is more harmful to the secure transmission.

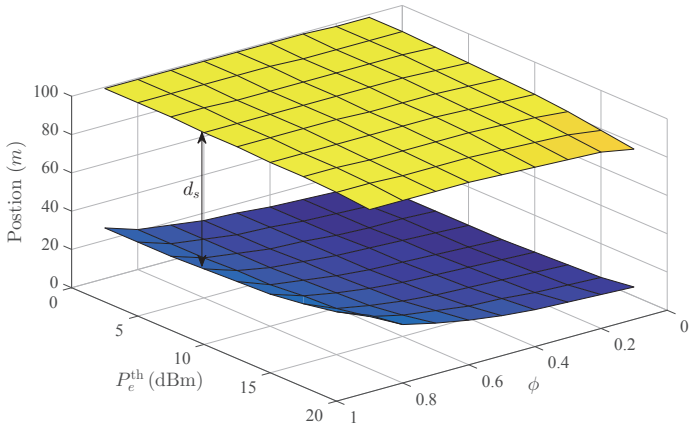

Figure 11. The influence of P_e^{th} and ϕ on d_s.

5. Conclusions

This paper has proposed a valuable way to defend against an eavesdropper by establishing the protecting region to prevent the eavesdropper from entering in the wireless sensor networks. We have analyzed the insecure region based on the metric of the hybrid outage probability which takes both the transmission outage probability and the secrecy outage probability into consideration, under the assumption that the eavesdropper is passive and active. Subsequently, the hybrid outage probability expressions have been derived to define the insecure region. The safe transmission range, as an effective indicator, has been defined to conduct the circular protecting region around transceiver. The analysis of the insecure region can also be integrated with existing transmission strategies to achieve a higher security performance in wireless sensor networks.

Author Contributions: T.L. and C.X. performed the simulation results and wrote the paper; Y.L. conceived the model; O.A.D. provided some suggestions and revised the paper. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported in part by the Postdoctoral Science Foundation of China under Grant 2019M663630, in part by the National Key R&D Program of China under Grant 2016YF-B1200202 and 254, in part by the National Natural Science Foundation of China under Grant 61771365, in part by the 111 Project under Grant B08038, in part by the Fundamental Research Funds for the Central Universities under Grant JBF180101.

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

References

1. Zheng, J.; Cai, Y.; Shen, X.; Zheng, Z.; Yang, W. Green energy optimization in energy harvesting wireless sensor networks. *IEEE Commun. Mag.* **2015**, *53*, 150–157. [CrossRef]
2. Zou, Y.; Zhu, J.; Wang, X.; Hanzo, L. A survey on wireless security: Technical challenges, recent advances, and future trends. *Proc. IEEE* **2016**, *104*, 1727–1765. [CrossRef]
3. Chen, G.; Gong, Y.; Xiao, P.; Chambers, J.A. Dual antenna selection in secure cognitive radio networks. *IEEE Trans. Veh. Technol.* **2016**, *65*, 7993–8002. [CrossRef]
4. Chen, G.; Coon, J.P.; Tajbakhsh, S.E. Secure routing for multihop Ad Hoc networks with inhomogeneous eavesdropper clusters. *IEEE Trans. Veh. Technol.* **2018**, *67*, 10660–10670. [CrossRef]
5. Hamamreh, J.M.; Furqan, H.M.; Arslan, H. Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 1773–1828. [CrossRef]
6. Hu, H.; Gao, Z.; Liao, X.; Leung, V.C.M. Secure communications in CIoT networks with a wireless energy harvesting untrusted relay. *Sensors* **2017**, *17*, 2023. [CrossRef] [PubMed]
7. Zhu, F.; Yao, M. Improving physical-layer security for CRNs using sinr-based cooperative beamforming. *IEEE Trans. Veh. Technol.* **2016**, *65*, 1835–1841. [CrossRef]
8. Lee, J. Full-duplex relay for enhancing physical layer security in multi-hop relaying systems. *IEEE Commun. Lett.* **2015**, *19*, 525–528. [CrossRef]
9. Wu, Y.; Khisti, A.; Xiao, C.; Caire, G.; Wong, K.; Gao, X. A survey of physical layer security techniques for 5G wireless networks and challenges ahead. *IEEE J. Sel. Areas Commun.* **2018**, *36*, 679–695. [CrossRef]
10. Son, W.; Jang, H.S.; Jung, B.C. A pseudo-random beamforming technique for improving physical-layer security of MIMO cellular networks. *Entropy* **2019**, *21*, 1038. [CrossRef]
11. Zeng, M.; Nguyen, N.; Dobre, O.A.; Poor, H.V. Securing downlink massive MIMO-NOMA networks with artificial noise. *IEEE J. Sel. Top. Signal Process.* **2019**, *13*, 685–699. [CrossRef]
12. Nguyen, V.; Nguyen, H.V.; Dobre, O.A.; Shin, O. A new design paradigm for secure full-duplex multiuser systems. *IEEE J. Sel. Areas Commun.* **2018**, *36*, 1480–1498. [CrossRef]
13. Lin, S.H.; Lu, R.R.; Fu, X.T.; Tong, A.L.; Wang, J.Y. Physical-layer security analysis over m-distributed fading channels. *Entropy* **2019**, *21*, 998. [CrossRef]
14. Tugnait, J.K. Self-contamination for detection of pilot contamination attack in multiple antenna systems. *IEEE Wirel. Commun. Lett.* **2015**, *4*, 525–528. [CrossRef]
15. Zhou, X.; Maham, B.; Hjorungnes, A. Pilot contamination for active eavesdropping. *IEEE Trans. Wirel. Commun.* **2012**, *11*, 903–907. [CrossRef]
16. Zhang, W.; Lin, H.; Zhang, R. Detection of pilot contamination attack based on uncoordinated frequency shifts. *IEEE Trans. Commun.* **2018**, *66*, 2658–2670. [CrossRef]
17. Liu, C.; Lee, J.; Quek, T.Q.S. Secure transmission in the presence of full-duplex active eavesdropper. In Proceedings of the 2017 IEEE Global Communications Conference (GLOBECOM), Singapore, 4–8 December 2017; pp. 1–6.
18. Liu, Z.; Li, N.; Tao, X.; Li, S.; Xu, J.; Zhang, B. Artificial-noise-aided secure communication with full-duplex active eavesdropper. In Proceedings of the 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Montreal, QC, Canada, 8–13 October 2017; pp. 1–7.
19. Tang, X.; Ren, P.; Han, Z. Power-efficient secure transmission against full-duplex active eavesdropper: A game-theoretic framework. *IEEE Access* **2017**, *5*, 24632–24645. [CrossRef]
20. Tang, X.; Ren, P.; Wang, Y.; Han, Z. Combating full-duplex active eavesdropper: A hierarchical game perspective. *IEEE Trans. Commun.* **2017**, *65*, 1379–1395. [CrossRef]

21. Fang, H.; Xu, L.; Zou, Y.; Wang, X.; Choo, K.R. Three-stage stackelberg game for defending against full-duplex active eavesdropping attacks in cooperative communication. *IEEE Trans. Veh. Technol.* **2018**, *67*, 10788–10799. [CrossRef]
22. Lv, L.; Ding, Z.; Chen, J.; Al-Dhahir, N. Design of secure NOMA against full-duplex proactive eavesdropping. *IEEE Wirel. Commun. Lett.* **2019**, *8*, 1090–1094. [CrossRef]
23. Zhou, H.; He, D.; Wang, H.; Yang, D. Optimal relay selection with a full-duplex active eavesdropper in cooperative wireless networks. In Proceedings of the 2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring), Kuala Lumpur, Malaysia, 28 April–1 May 2019; pp. 1–5.
24. Chen, G.; Gong, Y.; Xiao, P.; Chambers, J.A. Physical Layer Network Security in the Full-Duplex Relay System. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 574–583. [CrossRef]
25. Karas, D.S.; Boulogeorgos, A.A.; Karagiannidis, G.K. Physical layer security with uncertainty on the location of the eavesdropper. *IEEE Wirel. Commun. Lett.* **2016**, *5*, 540–543. [CrossRef]
26. Karas, D.S.; Boulogeorgos, A.A.; Karagiannidis, G.K.; Nallanathan, A. Physical Layer security in the presence of interference. *IEEE Wirel. Commun. Lett.* **2017**, *6*, 802–805. [CrossRef]
27. Tang, J.; Chen, G.; Coon, J.P. Secrecy performance analysis of wireless communications in the presence of uav jammer and randomly located uav eavesdroppers. *IEEE Trans. Inf. Forensics Secur.* **2019**, *14*, 3026–3041. [CrossRef]
28. Chen, G.; Coon, J.P.; Di Renzo, M. Secrecy outage analysis for downlink transmissions in the presence of randomly located eavesdroppers. *IEEE Trans. Inf. Forensics Secur.* **2017**, *12*, 1195–1206. [CrossRef]
29. Li, W.; Tang, Y.; Ghogho, M.; Wei, J.; Xiong, C. Secure communications via sending artificial noise by both transmitter and receiver: Optimum power allocation to minimise the insecure region. *IET Commun.* **2014**, *8*, 2858–2862. [CrossRef]
30. Li, W.; Ghogho, M.; Chen, B.; Xiong, C. Secure communication via sending artificial noise by the receiver: Outage secrecy capacity/region analysis. *IEEE Commun. Lett.* **2012**, *16*, 1628–1631. [CrossRef]
31. Zhou, Y.; Yeoh, P.L.; Chen, H.; Li, Y.; Schober, R.; Zhuo, L.; Vucetic, B. Improving physical layer security via a uav friendly jammer for unknown eavesdropper location. *IEEE Trans. Veh. Technol.* **2018**, *67*, 11280–11284. [CrossRef]
32. Marina, N.; Hjorungnes, A. Characterization of the secrecy region of a single relay cooperative system. In Proceedings of the 2010 IEEE Wireless Communication and Networking Conference (WCNC), Sydney, Australia, 18–21 April 2010; pp. 1–6.
33. Zheng, T.; Wang, H.; Yin, Q. On transmission secrecy outage of a multi-antenna system with randomly located eavesdroppers. *IEEE Commun. Lett.* **2014**, *18*, 1299–1302. [CrossRef]
34. Mao, L.; Li, Y.; Li, T.; Gao, M.; Zhang, H. Security region analysis with artificial noise based on secrecy outage probability. In Proceedings of the 2018 IEEE Military Communications Conference (MILCOM), Los Angeles, CA, USA, 29–31 October 2018; pp. 336–340.
35. Tugnait, J.K. Using artificial noise to improve detection performance for wireless user authentication in time-variant channels. *IEEE Wirel. Commun. Lett.* **2014**, *3*, 377–380. [CrossRef]
36. Ju, H.; Oh, E.; Hong, D. Improving efficiency of resource usage in two-hop full duplex relay systems based on resource sharing and interference cancellation. *IEEE Trans. Wirel. Commun.* **2009**, *8*, 3933–3938.
37. Krikidis, I.; Suraweera, H.A.; Smith, P.J.; Yuen, C. Full-Duplex Relay Selection for Amplify-and-Forward Cooperative Networks. *IEEE Trans. Wirel. Commun.* **2012**, *11*, 4381–4393. [CrossRef]
38. Gerbracht, S.; Scheunert, C.; Jorswieck, E.A. Secrecy outage in MISO systems with partial channel information. *IEEE Trans. Inf. Forensics Secur.* **2012**, *7*, 704–716. [CrossRef]
39. Yang, N.; Yan, S.; Yuan, J.; Malaney, R.; Subramanian, R.; Land, I. Artificial noise: Transmission optimization in multi-input single-output wiretap channels. *IEEE Trans. Commun.* **2015**, *63*, 1771–1783. [CrossRef]
40. Gradshteyn, I.S.; Ryzhik, I.M. *Tabel of Integrals, Series, and Products*, 7th ed.; Academic Press: Cambridge, MA, USA, 2007.