sensors

MDPI

Article

On the Performance of Random Cognitive mmWave Sensor Networks

Yi Song [1,2,3,*], Weiwei Yang [2], Zhongwu Xiang [2], Biao Wang [4] and Yueming Cai [2]

1 School of Physics and Electronic Electrical Engineering, Huaiyin Normal University, Huai'an 223300, China
2 College of Communications Engineering, Army Engineering University of PLA, No. 88 Houbiaoying, Qinhuai District, Nanjing 210007, China
3 Jiangsu Province Key Construction Laboratory of Modern Measurement Technology and Intelligent System, Huai'an 223300, China
4 School of Electronic and Information, Jiangsu University of Science and Technology, Zhenjiang 212003, China
* Correspondence: sy@hytc.edu.cn; Tel.: +86-025-8082-9409

Received: 12 June 2019; Accepted: 16 July 2019; Published: 19 July 2019

Abstract: This paper investigates the secrecy performance of a cognitive millimeter wave (mmWave) wiretap sensor network, where the secondary transmitter (SU-Tx) intends to communicate with a secondary sensor node under the interference temperature constraint of the primary sensor node. We consider that the random-location eavesdroppers may reside in the signal beam of the secondary network, so that confidential information can still be intercepted. Also, the interference to the primary network is one of the critical issues when the signal beam of the secondary network is aligned with the primary sensor node. Key features of mmWave networks, such as large number of antennas, variable propagation law and sensitivity to blockages, are taken into consideration. Moreover, an eavesdropper-exclusion sector guard zone around SU-Tx is introduced to improve the secrecy performance of the secondary network. By using stochastic geometry, closed-form expression for secrecy throughput (ST) achieved by the secondary sensor node is obtained to investigate secrecy performance. We also carry out the asymptotic analysis to facilitate the performance evaluation in the high transmit power region. Numerical results demonstrate that the interference temperature constraint of the primary sensor node enables us to balance secrecy performance of the secondary network, and provides interesting insights into how the system performance of the secondary network that is influenced by various system parameters: eavesdropper density, antenna gain and sector guard zone radius. Furthermore, blockages are beneficial to improve ST of the secondary sensor node under certain conditions.

Keywords: cognitive radio; millimeter wave; physical layer security; secrecy throughput

1. Introduction

Future communication will probably realize man–machine–object cooperative communication and ultra-densely connections to achieve full coverage, and higher spectral efficiency will become a key issue. Owing to the spectrum scarcity problem and the increasing data rate demand with different quality of service (QoS), new spectrum bands are needed to meet explosive traffic requirements. In order to improve spectrum utilization efficiency and avoid interference with other operational networks, it is necessary to enable cognitive radio characteristics in densely deployed future networks. On the other hand, as a promising candidate for future mobile networks, millimeter-wave (mmWave) communication [1] has attracted more and more attention because of its operating frequency ranging from 30 to 300 GHz. One of the significant features of mmWave signals is the small wavelength, which allows the transceivers to deploy large numbers of antenna arrays to achieve beamforming

gain to compensate path loss and establish links with a reasonable signal-to-interference-plus-noise ratio (SINR).

More recently, researchers have conducted some studies on cognitive mmWave networks, most of which focus on various techniques to dynamically avoid interference and lessen mutual interference. In order to minimize the mutual interference between cognitive users and other operational networks in fifth-generation (5G) networks, wavelet packet transform was applied to sparse code multiple access systems for spectrum sensing and multi-user access modulation in [2]. Using a similar method, [3] studied a joint wavelet-based spectrum sensing and filter bank multicarrier modulation for cognitive 5G heterogeneous networks in a mmWave spectrum band. Additionally, [4] showed that in mmWave cellular networks with a shared spectrum, especially when sharing spectrum with a high-power operator and density, it was necessary for inter-operator base station coordination to repress the resulting cross-operator interference. However, malicious devices may partake in spectrum sensing and access due to the open and dynamic characteristics of cognitive radio, which makes a cognitive radio more vulnerable to malicious attacks and eavesdropping [5]. For example, malicious attackers may mislead legitimate cognitive users and even cause them to fail to work properly by imitating the primary user sending information to the secondary user and informing the secondary user that the authorized spectrum has been occupied. Compared with malicious attacks, passive eavesdropping is more difficult to detect by users, resulting in more serious security threats. As a result, new security challenges from all aspects of network architecture are faced by a cognitive radio, such as spectrum sensing, spectrum access and spectrum management [6].

Physical layer security (PLS) attempts to protect wireless networks from wiretapping by utilizing randomness of wireless medium at the physical layer [7,8]. Therefore, PLS has been identified as a promising strategy to implement secure communication, which has received extensive attention in research community [9–15]. To elaborate, PLS has been considered in cognitive networks [16–18]. Specifically, for the cognitive networks with a random distribution of eavesdropping nodes, the authors designed four different transmission schemes to achieve secure transmission under the interference constraint of the primary receiver [16]. Also, for random cognitive radio networks, a simple and decentralized secure transmission scheme combining the secrecy guard zone and artificial noise was proposed to enhance the secure information transmission of secondary networks [17]. Moreover, the authors investigated the PLS of a multi-user multi-eavesdropper cognitive radio system [18]. Furthermore, for dual phase amplify-and-forward large wireless sensor networks, a new security cooperative protocol was studied [19].

On the other hand, PLS in mmWave systems has aroused interest with enthusiasm [20–23]. The features of the mmWave communication system, such as large antenna array, directionality and short range transmission, may provide stronger PLS for mmWave system. Using analog beamforming in the mmWave base station, the authors analyzed the secrecy throughput from the perspectives of delay-limited and delay-tolerant transmissions [24]. Under the stochastic geometry framework, the secrecy performance was studied in the artificial-noise-assisted and the noise-limited mmWave networks [25], the network-wide PLS performance of the downlink transmission in an mmWave cellular network was comprehensively studied. Considering a large-scale mmWave ad hoc network, the authors examined the impact of artificial noise on the secrecy rate; the results showed that it was necessary to carefully determine the power allocation between artificial noise and information signals to improve secrecy performance [26]. In addition, combined with unmanned aerial vehicle (UAV) networks, the secure transmission of mmWave simultaneous wireless information and power transfer UAV relay networks was studied [27]. Considering unique characteristics of air-to-ground channels and practical constraints of UAV deployment, [28] studied the secrecy performance of millimeter-wave unmanned aerial vehicle networks.

All the above works were either focused on the PLS of traditional microwave cognitive wireless networks or on the analysis of the secrecy performance of mmWave networks, but were rarely investigated on the PLS for cognitive mmWave wireless networks. In addition, as mentioned earlier,

future communications will probably be ultra-densely heterogeneous networks, where communication networks can be built with a combination of macro cells and small cells. The existing macro cells guarantee coverage and mobility in the ultra high frequency band, while small cells are needed in order to achieve gigabit rates over the mmWave range of 30–300 GHz. Effective utilization of small cell spectrum bands is one of the ways to improve the obtainable capacity and data rate of heterogeneous networks. It is a challenging task that could be accomplished through the spectrum sensing capability of cognitive radio [2]. Therefore, the design of future communication networks requires us to embed cognitive features including the ability of sensing interference power to take advantage of the available spectrum bands. Furthermore, because of the remarkable characteristics of the mmWave channel, for instance, the mmWave signals are more sensitive to blocking effects, and the fading statistics of the line-of-sight (LOS) link and the non-line-of-sight (NLOS) link are completely different [29], the secrecy performance of cognitive mmWave sensor networks will be very different from that of traditional cognitive microwave networks, which needs to be re-evaluated. Besides, considering that random-location eavesdroppers may reside in the signal beam of the secondary network, so that confidential information can still be intercepted. Also, the interference with the primary network is one of the critical issues when the signal beam of the secondary network is aligned with the primary network. To the best of our knowledge, the research on the secrecy performance of cognitive mmWave wiretap sensor networks has not yet been addressed, which motivates our work.

This paper studies the PLS in cognitive mmWave wiretap sensor networks. Our analysis considers the key characteristics of the mmWave channel and blockage density and the effects of different antenna arrays gains. In particular, the main contributions of this paper in specific terms are

- By using stochastic geometry approaches, we model the cognitive mmWave wiretap sensor networks to characterize the random spatial locations of primary and secondary nodes, as well as the eavesdroppers. Taking into account the effect of blockage, the links are either LOS or NLOS. A sector secrecy guard zone, synonymously referred to as the eavesdropper-exclusion area, is invoked around the secondary transmitter (SU-Tx) for improving the PLS.
- Considering that the random-location of both eavesdroppers and the primary sensor node may reside in the signal beam of the secondary network, we derive analytical expressions of secrecy throughput (ST) for the secondary sensor node to measure secrecy performance of the system with arbitrary system parameters. Subsequently, an asymptotic expression is proposed to gain additional insight into the performance evaluation and design for the proposed system.
- The results show that the interference temperature constraint of the primary sensor node can be used to balance secrecy performance of the secondary network, which indicates losing the interference temperature constraint of the primary node would worsen secrecy performance. Increasing the radius of the sector guard zone can improve ST. Furthermore, it is also shown that increasing the transmit power or antenna gain of the secondary network does not necessarily lead to the improvement of ST, and sometimes deteriorate ST. Besides, blockages can also be used to improve ST of SU-Rx under certain conditions.

The rest of the paper is organized as follows. The system model and mmWave channel characteristics are provided in Section 2. Secrecy performance analysis is evaluated in Section 3. Then, in Section 4, numerical and simulation results are given. Finally, conclusions are drawn in Section 5.

2. System Model

2.1. Network Topology

As shown in Figure 1, we consider an underlay cognitive mmWave wiretap sensor network, where the SU-Tx is equipped multiple antennas to utilize directional beamforming to communicate with a secondary sensor node in the presence of a primary sensor node. Multiple eavesdroppers

intercept confidential information sent from the SU-Tx. The spatial distribution of all eavesdroppers is modeled using a homogeneous Poisson point processes (HPPP), which is denoted by Φ_E and it is associated with the density λ_E. Also, the locations of primary and secondary sensor nodes are randomly distributed, and both of them and each eavesdropper is equipped with one receive antenna.

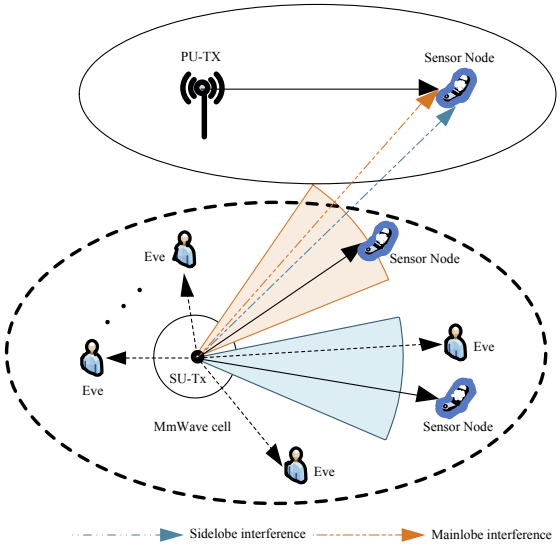

Figure 1. Illustration of the system model.

2.2. Directional Beamforming

For mathematical tractability, the antenna pattern is assumed to be a sectorial model [25,26,30]. Consequently, the SU-Tx antenna gain pattern about a generic angle θ is given by

$$G_S(\theta) = \begin{cases} M_S, & \text{if } |\theta| \leq \theta_S \\ m_S, & \text{Otherwise} \end{cases}, \tag{1}$$

where M_S and m_S are the main lobe and side lobe gain, respectively; $\theta \in [0, 2\pi)$ is the angle of boresight direction; θ_S is the main lobe beam width. Assuming that the perfect channel state information (CSI) of the secondary sensor node can be obtained by the SU-Tx, then it could adjust its antenna steering orientation array to the secondary sensor node to maximize the directional gain. It should be pointed out that we neglect the channel estimation error and also ignore the error of time and carrier frequency synchronization. In practical, it may be a nontrivial task to estimate the CSI, an upper bound on achievable secrecy performance is actually provided in our work. The estimation of mmWave channel is more in line with the actual communication system, but it is beyond the scope of this paper. Furthermore, supposing that the eavesdroppers can be detected as long as they are close enough to SU-Tx. Therefore, a sector guard zone with central angle θ_S and radius r around the SU-Tx is introduced, where eavesdroppers are not allowed to roam. Similar security mechanisms have been used in the literature [22,31,32].

2.3. Channel Model

In outdoor mmWave scenarios, a channel between SU-Tx and receiver may be LOS or NLOS link in the presence of blockages [26]. $P_L(r_d)$ represents the probability of a LOS with distance r_d, while the NLOS probability is $P_N(r_d)$, which is given as $P_L(r_d) = e^{-\beta r_d}$ or $P_N(r_d) = 1 - e^{-\beta r_d}$, where β is a parameter determined by the density of blockages. Considering independent Nakagami fading for each link [33], and the Nakagami fading parameter of the LOS (NLOS) link is $N_L(N_N)$. For simplicity, N_L and N_N are both assumed to be positive integers. The secondary sensor node and eavesdroppers received channel gains can be described as $M_S|h_{SU}|^2 L(r_{SU})$ and $M_S|h_{SE}|^2 L(r_E)$,

respectively, where both $|h_{SU}|^2$ and $|h_{SE}|^2$ are normalized Gamma random variable with following $\Gamma(N_L, 1/N_L)$ and $\Gamma(N_N, 1/N_N)$, the distance from the SU-Tx to the secondary sensor node is r_{SU} and the distance from the SU-Tx to the eavesdroppers is r_E. The path loss function of $L(r_{SU})$ and $L(r_E)$ are modeled as $L(r_j) = C_L r^{-\alpha_L}$ or $L(r_j) = C_N r^{-\alpha_N}$, $j \in \{SU, E\}$, α_L and α_N are path loss exponents of the LOS and NLOS, C_L and C_N are the constant depending on the LOS and NLOS.

2.4. Received SINR

To guarantee the interference temperature constraint of the primary network, the instantaneous interference power at the primary sensor node from the SU-Tx should lower than a given threshold I_w, then the transmit power of the SU-Tx is further constrained by $P_U = \min\left(\frac{I_w}{M_S|h_{SP}|^2 L(r_{SP})}, P_t\right)$, where P_t is the maximum transmit power of the SU-Tx. Moreover, it is assumed that the interference of primary transmitter on the secondary sensor node is not greater than δ_0. The variable δ_0 leaves for future research. $\sigma_\vartheta^2, \vartheta \in \{U, E\}$ is the noise power. Therefore, the SINR at the secondary sensor node is defined as

$$\gamma_U = \frac{M_S P_U |h_{SU}|^2 L(r_U)}{\sigma_U^2 + \delta_0}, \tag{2}$$

In this model, the eavesdroppers attempt to intercept the confidential information of the system, assuming that the SU-Tx do not know the instantaneous CSI of eavesdroppers. Non-colluding eavesdroppers are taken into account where eavesdroppers decode the information independently. For such case, the eavesdropper closest to SU-Tx is not necessarily the most detrimental, but the eavesdropper with the best channel to SU-Tx. In addition, we consider the worst-case scenario of cognitive mmWave wiretap sensor networks, in which the eavesdroppers are assumed to have powerful detection capabilities. In fact, this assumption overestimates the anti-jamming ability of the eavesdroppers. Then, the instantaneous SINR of detecting the information of the secondary sensor node at the most detrimental eavesdropper can be expressed as follows:

$$\gamma_E = \max_{E \in \phi_E} \left(\frac{M_S P_U |h_{SE}|^2 L(r_E)}{\sigma_E^2} \right). \tag{3}$$

Of particular note, we consider that the primary and secondary sensor nodes and eavesdroppers are located in the main lobe. This is because the main lobe has the greatest interference to the primary sensor node, which may cause the primary network performance to be deteriorated seriously. At the same time, the situation where the eavesdropper is located in the main lobe poses a serious threat to the security of the secondary sensor network. Thus, the considered scenario is the worst-case which have been widely adopted in mmWave systems with secrecy considerations; e.g., [25,34].

3. Secrecy Performance Analysis

In this section, we elaborate to evaluate the ST of secondary sensor node for the proposed cognitive mmWave wiretap sensor networks.

3.1. ST of the Secondary Sensor Node

The ST of the secondary sensor node can be expressed as

$$\begin{aligned} \eta^U &= R_{\mathrm{m}}^s \Pr\left(\gamma_E < 2^{(R_m - R_{\mathrm{m}}^s)} - 1, \gamma_U > 2^{R_m} - 1\right) \\ &= R_{\mathrm{m}}^s \Pr\left(\max_{E \in \phi_E} \left(\frac{M_S P_U |h_{SE}|^2 L(r_E)}{\sigma_E^2}\right) < \varepsilon_2, \frac{P_U M_S |h_{SU}|^2 L(r_U)}{\sigma_U^2 + \delta_0} > \varepsilon_1\right), \end{aligned} \tag{4}$$

where $\varepsilon_1 = 2^{R_m} - 1$, $\varepsilon_2 = 2^{(R_m - R_m^s)} - 1$. Substituting P_U in Equation (4) and using the properties of the joint distribution of two random variables in [35] we have:

$$\min\left(\frac{I_w}{M_S|h_{SP}|^2 L(r_{SP})}, P_t\right) = \begin{cases} \frac{I_w}{M_S|h_{SP}|^2 L(r_{SP})} & \text{if} \quad P_t > \frac{I_w}{M_S|h_{SP}|^2 L(r_{SP})} \\ P_t & \text{if} \quad P_t \le \frac{I_w}{M_S|h_{SP}|^2 L(r_{SP})} \end{cases}. \tag{5}$$

Therefore, further derivation of Equation (4) can be expressed as

$$\begin{aligned} \eta^U &= R_{\mathrm{m}}^s \Pr\left(\gamma_E < 2^{(R_m - R_{\mathrm{m}}^s)} - 1, \gamma_U > 2^{R_m} - 1\right) \\ &= R_{\mathrm{m}}^s \Pr\left(\max_{E\in\phi_E}\left(\frac{M_S P_t |h_{SE}|^2 L(r_E)}{\sigma_E^2}\right) < \varepsilon_2, \frac{P_t M_S |h_{SU}|^2 L(r_U)}{\sigma_U^2 + \delta_0} > \varepsilon_1, P_t \le \frac{I_w}{M_S|h_{SP}|^2 L(r_{SP})}\right) \\ &+ R_{\mathrm{m}}^s \Pr\left(\max_{E\in\phi_E}\left(\frac{\frac{I_w}{|h_{SP}|^2 L(r_{SP})}|h_{SE}|^2 L(r_E)}{\sigma_E^2}\right) < \varepsilon_2, \frac{\frac{I_w}{|h_{SP}|^2 L(r_{SP})}|h_{SU}|^2 L(r_U)}{\sigma_U^2 + \delta_0} > \varepsilon_1, P_t > \frac{I_w}{M_S|h_{SP}|^2 L(r_{SP})}\right) \\ &= \underbrace{R_{\mathrm{m}}^s \int_0^{\frac{I_w}{P_t M_S}} \Pr\left(\max_{E\in\phi_E}\left(\frac{M_S P_t |h_{SE}|^2 L(r_E)}{\sigma_E^2}\right) < \varepsilon_2, \frac{P_t M_S |h_{SU}|^2 L(r_U)}{\sigma_U^2 + \delta_0} > \varepsilon_1\right) f_k(x)\, dx}_{Q_1} \\ &+ \underbrace{R_{\mathrm{m}}^s \int_{\frac{I_w}{P_t M_S}}^{\infty} \Pr\left(\max_{E\in\phi_E}\left(\frac{\frac{I_w}{|h_{SP}|^2 L(r_{SP})}|h_{SE}|^2 L(r_E)}{\sigma_E^2}\right) < \varepsilon_2, \frac{\frac{I_w}{|h_{SP}|^2 L(r_{SP})}|h_{SU}|^2 L(r_U)}{\sigma_U^2 + \delta_0} > \varepsilon_1\right) f_k(x)\, dx}_{Q_2} \end{aligned}, \tag{6}$$

where $\kappa = |h_{SP}|^2 L(r_{SP})$, and the probability density function (PDF) of κ is represented by $f_\kappa(x)$, the cumulative distribution function (CDF) of κ is represented by $F_\kappa(x)$. We first derive the CDF of κ, which can be expressed as

$$\begin{aligned} F_k(x) &= \Pr\left(|h_{SP}|^2 L(r_{SP}) < x\right) = \Pr\left(|h_{SP}|^2 < \tfrac{x}{L(r_{SP})}\right) \\ &= \frac{2}{R_{SP}^2}\left(\int_0^{R_{SP}} \frac{\Upsilon\left(N_L, \frac{xN_L}{L(r_{SP})}\right)}{\Gamma(N_L)} e^{-\beta r_{SP}} r_{SP} dr_{SP} + \int_0^{R_{SP}} \frac{\Upsilon\left(N_N, \frac{xN_N}{L(r_{SP})}\right)}{\Gamma(N_N)} \left(1 - e^{-\beta r_{SP}}\right) r_{SP} dr_{SP}\right) \\ &= \frac{2}{R_{SP}^2}\left(\sum_{i=0}^{\infty} \frac{(-1)^i \left(\frac{N_L x}{C_L}\right)^{N_L+i}}{i!(N_L+i)\Gamma(N_L)} \times \frac{\Upsilon(\alpha_L(N_L+i)+2, \beta R_{SP})}{\beta^{\alpha_L(N_L+i)+2}} + \sum_{j=0}^{\infty} \frac{(-1)^j \left(\frac{N_N x}{C_N}\right)^{N_N+j}}{j!(N_N+j)\Gamma(N_N)} \left(\frac{(R_{SP})^{\alpha_N(N_N+j)+2}}{\alpha_N(N_N+j)+2} - \frac{\Upsilon(\alpha_N(N_N+j)+2, \beta R_{SP})}{\beta^{\alpha_N(N_N+j)+2}}\right)\right) \end{aligned}. \tag{7}$$

Then, we solve the first derivative of CDF and obtain the PDF of κ, which is calculated as

$$\begin{aligned} f_k(x) = \frac{2}{R_{SP}^2}\Bigg(&\sum_{i=0}^{\infty} \frac{(-1)^i (x)^{N_L+i-1}}{\left(\frac{C_L}{N_L}\right)^{N_L+i} i!\Gamma(N_L)} \times \frac{\Upsilon(\alpha_L(N_L+i)+2, \beta R_{SP})}{\beta^{\alpha_L(N_L+i)+2}} \\ &+ \sum_{j=0}^{\infty} \frac{(-1)^j (x)^{N_N+j-1}}{\left(\frac{C_N}{N_N}\right)^{N_N+j} j!\Gamma(N_N)} \left(\frac{(R_{SP})^{\alpha_N(N_N+j)+2}}{\alpha_N(N_N+j)+2} - \frac{\Upsilon(\alpha_N(N_N+j)+2, \beta R_{SP})}{\beta^{\alpha_N(N_N+j)+2}}\right)\Bigg) \end{aligned}. \tag{8}$$

Now, we focus our attention on deriving the integrals Q_1 in Equation (6). Q_1 can be rewritten as

$$Q_1 = \int_0^{\frac{I_w}{P_t M_S}} F_y(\varepsilon_2)\left(1 - F_v(\varepsilon_1)\right) f_k(x)\, dx, \tag{9}$$

where

$$\begin{aligned} F_y(\varepsilon_2) &= \Pr\left\{\max_{E\in\phi_E}\left(\frac{M_S P |h_{SE}|^2 L(r_E)}{\sigma_E^2}\right) < \varepsilon_2\right\} \\ &= \underbrace{\Pr\left\{\max_{E\in\phi_E^L}\left(\frac{M_S P_t |h_{SE}|^2 L(r_E)}{\sigma_E^2}\right) < \varepsilon_2\right\}}_{\Psi_1} \times \underbrace{\Pr\left\{\max_{E\in\phi_E^N}\left(\frac{M_S P_t |h_{SE}|^2 L(r_E)}{\sigma_E^2}\right) < \varepsilon_2\right\}}_{\Psi_2}, \end{aligned} \tag{10}$$

$$F_v(\varepsilon_1) = \Pr\left\{\frac{P_t M_S |h_{SU}|^2 L(r_U)}{\sigma_U^2 + \delta_0} < \varepsilon_1\right\}. \tag{11}$$

$F_y(\varepsilon_2)$ and $F_v(\varepsilon_1)$ can be obtained after some mathematical manipulations. However, for the sake of completeness, we presented a sketch of the proof, as given in Appendix A.

Whereas, we can get Q_1 in Equation (6), which can be expressed as

$$\begin{aligned}
Q_1 = &\left(1 - \frac{2}{R_U^2}\left(\sum_{i=0}^{\infty}\frac{(-1)^i(A\varepsilon_1 N_L)^{N_L+i}}{i!(N_L+i)\Gamma(N_L)(P_t M_S C_L)^{N_L+i}} \times \frac{\Upsilon(\alpha_L(N_L+i)+2,\beta R_U)}{\beta^{\alpha_L(N_L+i)+2}}\right.\right.\\
&\left.\left. + \sum_{j=0}^{\infty}\frac{(-1)^j(A\varepsilon_1 N_N)^{N_N+j}}{j!(N_N+j)\Gamma(N_N)(P_t M_S C_N)^{N_N+j}}\left(\frac{(R_U)^{\alpha_N(N_N+j)+2}}{\alpha_N(N_N+j)+2} - \frac{\Upsilon(\alpha_N(N_N+j)+2,\beta R_U)}{\beta^{\alpha_N(N_N+j)+2}}\right)\right)\right)\\
&\times \frac{2}{R_{SP}^2}\left(\sum_{i=0}^{\infty}\frac{(-1)^i(N_L I_w)^{N_L+i}}{i!(N_L+i)\Gamma(N_L)(P_t M_S)^{N_L+i}} \times \frac{\Upsilon(\alpha_L(N_L+i)+2,\beta R_{SP})}{\beta^{\alpha_L(N_L+i)+2}}\right.\\
&\left. + \sum_{j=0}^{\infty}\frac{(-1)^j(N_N I_w)^{N_N+j}}{j!(N_N+j)\Gamma(N_N)(P_t M_S)^{N_N+i}}\left(\frac{(R_{SP})^{\alpha_N(N_N+j)+2}}{\alpha_N(N_N+j)+2} - \frac{\Upsilon(\alpha_N(N_N+j)+2,\beta R_{SP})}{\beta^{\alpha_N(N_N+j)+2}}\right)\right)\\
&\times \exp\left(-\theta_s\lambda_E\left(\left(\frac{(N_N-1)!}{\Gamma(N_N)}\right)\sum_{m=0}^{N_N-1}\frac{\left(\frac{\sigma_E^2\varepsilon_2 N_N}{P_t C_N M_S}\right)^m}{m!} \times \frac{\Gamma\left(\frac{m\alpha_N+2}{\alpha_N}, \frac{\sigma_E^2\varepsilon_2 r^{\alpha_N} N_N}{P_t C_N M_S}\right)}{\alpha_N\left(\frac{\sigma_E^2\varepsilon_2 N_N}{P_t C_N M_S}\right)^{\frac{m\alpha_N+2}{\alpha_N}}}\right.\right.\\
&\left.\left. + \sum_{n=0}^{\infty}\frac{(-1)^n\left(\frac{\sigma_E^2\varepsilon_2 N_N}{P_t C_N M_S}\right)^{N_N+n}}{n!(N_N+n)\Gamma(N_N)}\frac{\Gamma(\alpha_N(N_N+n)+2,\beta r)}{\beta^{\alpha_N(N_N+n)+2}} - \sum_{n=0}^{\infty}\frac{(-1)^n\left(\frac{\sigma_E^2\varepsilon_2 N_L}{P_t C_L M_S}\right)^{N_L+n}}{n!(N_L+n)\Gamma(N_L)}\frac{\Gamma(\alpha_L(N_L+n)+2,\beta r)}{\beta^{\alpha_L(N_L+n)+2}}\right)\right)
\end{aligned} \tag{12}$$

From the derivation of Q_1, we can see that when the radius of sector guard zone becomes larger or the SU-Tx uses a narrower beams, Q_1 increases. When $P_t \leq \frac{I_w}{M_S|h_{SP}|^2 L(r_{SP})}$, the larger R_{SP} is beneficial to the increasing of Q_1. In addition, it can be seen from the expression of Q_1 that it is related to λ_E and the blockage density β.

Let us now turn our attention to solving the integral Q_2 in Equation (6). Then Q_2 can be rewritten as

$$Q_2 = \int_{\frac{I_w}{P_t M_S}}^{\infty} F_z(\varepsilon_2)\left(1 - F_u(\varepsilon_1)\right) f_k(x)\, dx, \tag{13}$$

where

$$\begin{aligned}
F_z(\varepsilon_2) &= \Pr\left\{\max_{E\in\phi_E}\left(\frac{\frac{I_w}{|h_{SP}|^2 L(r_{SP})}|h_{SE}|^2 L(r_E)}{\sigma_E^2}\right) < \varepsilon_2\right\}\\
&= \underbrace{\Pr\left\{\max_{E\in\phi_E^L}\left(\frac{I_w|h_{SE}|^2 L(r_E)}{|h_{SP}|^2 L(r_{SP})\sigma_E^2}\right) < \varepsilon_2\right\}}_{\Psi_3} \times \underbrace{\Pr\left\{\max_{E\in\phi_E^N}\left(\frac{I_w|h_{SE}|^2 L(r_E)}{|h_{SP}|^2 L(r_{SP})\sigma_E^2}\right) < \varepsilon_2\right\}}_{\Psi_4},
\end{aligned} \tag{14}$$

$$F_u(\varepsilon_1) = \Pr\left\{\frac{I_w|h_{SU}|^2 L(r_U)}{A|h_{SP}|^2 L(r_{SP})} < \varepsilon_1\right\}. \tag{15}$$

$F_z(\varepsilon_2)$ and $F_u(\varepsilon_1)$ can be obtained after some mathematical manipulations. A sketch of this proof is given in Appendix B.

Consequently, we have Q_2, which can be expressed as

$$
\begin{aligned}
Q_2 = \int_{\frac{I_w}{P_t M_S}}^{\infty} & \left(1 - \frac{2}{R_U^2}\left(\sum_{i=0}^{\infty} \frac{(-1)^i (Ax\varepsilon_1 N_L)^{N_L+i}}{i!(N_L+i)\Gamma(N_L)(I_w C_L)^{N_L+i}} \times \frac{\Upsilon(\alpha_L(N_L+i)+2, \beta R_U)}{\beta^{\alpha_L(N_L+i)+2}}\right.\right. \\
& \left.\left. + \sum_{j=0}^{\infty} \frac{(-1)^j (Ax\varepsilon_1 N_N)^{N_N+j}}{j!(N_N+j)\Gamma(N_N)(I_w C_N)^{N_N+i}} \left(\frac{(R_U)^{\alpha_N(N_N+j)+2}}{\alpha_N(N_N+j)+2} - \frac{\Upsilon(\alpha_N(N_N+j)+2, \beta R_U)}{\beta^{\alpha_N(N_N+j)+2}}\right)\right)\right. \\
& \times \exp\left(-\theta_s \lambda_E \left(\left(\frac{(N_N-1)!}{\Gamma(N_N)}\right) \sum_{m=0}^{N_N-1} \frac{\left(\frac{\sigma_E^2 \varepsilon_2 x N_N}{I_w C_N}\right)^m}{m!} \times \frac{\Gamma\left(\frac{m\alpha_N+2}{\alpha_N}, \frac{\sigma_E^2 \varepsilon_2 x r^{\alpha_N} N_N}{I_w C_N}\right)}{\alpha_N \left(\frac{\sigma_E^2 \varepsilon_2 x N_N}{I_w C_N}\right)^{\frac{m\alpha_N+2}{\alpha_N}}}\right.\right. \\
& \left.\left. + \sum_{n=0}^{\infty} \frac{(-1)^n \left(\frac{\sigma_E^2 \varepsilon_2 x N_N}{I_w C_N}\right)^{N_N+n}}{n!(N_N+n)\Gamma(N_N)} \frac{\Gamma(\alpha_N(N_N+n)+2, \beta r)}{\beta^{\alpha_N(N_N+n)+2}} - \sum_{n=0}^{\infty} \frac{(-1)^n \left(\frac{\sigma_E^2 \varepsilon_2 x N_L}{I_w C_L}\right)^{N_L+n}}{n!(N_L+n)\Gamma(N_L)} \frac{\Gamma(\alpha_L(N_L+n)+2, \beta r)}{\beta^{\alpha_L(N_L+n)+2}}\right)\right) \\
& \times \frac{2}{R_{SP}^2}\left(\sum_{i_1=0}^{\infty} \frac{(-1)^{i_1} (N_L)^{N_L+i_1} (x)^{N_L+i_1-1}}{i_1!\Gamma(N_L)} \times \frac{\Upsilon(\alpha_L(N_L+i_1)+2, \beta R_{SP})}{\beta^{\alpha_L(N_L+i_1)+2}}\right. \\
& \left. + \sum_{j_1=0}^{\infty} \frac{(-1)^{j_1} (N_N)^{N_N+j_1} (x)^{N_N+j_1-1}}{j_1!\Gamma(N_N)} \left(\frac{(R_{SP})^{\alpha_N(N_N+j_1)+2}}{\alpha_N(N_N+j_1)+2} - \frac{\Upsilon(\alpha_N(N_N+j_1)+2, \beta R_{SP})}{\beta^{\alpha_N(N_N+j_1)+2}}\right)\right) \mathrm{d}x
\end{aligned} \tag{16}
$$

From Equation (16), we can know that the transmit power P_t, the main beam gain M_S, the the blockage density β and eavesdrop density λ_E have an important effects on Q_2.

Resultantly, the calculation for the ST of the secondary sensor node is complete. Then, η^U can be calculated as follows:

$$
\eta^U = R_{\mathrm{m}}^s \left(Q_1 + Q_2\right), \tag{17}
$$

where Q_1 can be obtained from Equation (12) and Q_2 follows from the Equation (16).

Remark 1. *According to Equation (17), η^U is an increasing function due to the increasing of r, which demonstrates that the secrecy performance of secondary network is improved as r increases. Increasing antenna gain and P_t are beneficial to the improvement of η^U, but could increase the risk of information leakage. In addition, the value of I_w has a great impact on the secrecy performance of secondary sensor node. Therefore, according to the actual network environment, it should be carefully designed to achieve better performance of a secondary network. Furthermore, η^U has a close relationship with λ_E, R_{SP} and the blockage density β.*

3.2. Asymptotic Behavior

To extract additional insights about cognitive mmWave sensor wiretap networks, we derive the asymptotic expression of the ST with $P_t \to \infty$. By using the expression of Equation (17), the asymptotic behavior of ST can be easily calculated, that is, only Q_2 exists in Equation (17), and the lower limit of integration in Q_2 is changed to 0. From the asymptotic behavior of ST, we have found that increasing I_w is not always conducive to the improvement of η^U, and excessive I_w increases the risk of eavesdroppers eavesdropping confidential information. Therefore, the interference temperature constraint of the primary network enables a compromise between reliability and security of the cognitive mmWave sensor wiretap networks.

4. Numerical Results

Here, numerical results of the proposed cognitive mmWave wiretap networks are presented to evaluate its performance. The thermal noise power is assumed to be -90 dBm, and considering an mmWave system with carrier frequency at 28 GHz. As pointed out by [36], the parameters of Nakagami fading of the LOS and NLOS link are $N_L = 3$ and $N_N = 2$, and the path-loss model:

$\beta_L = 61.4$ dB, $\alpha_{\mathrm{L}} = 2$, $\beta_N = 72$ dB , $\alpha_{\mathrm{N}} = 2.92$, $C_L = 10^{-\frac{\beta_L}{10}}$ and $C_N = 10^{-\frac{\beta_N}{10}}$. BPCU is short for bit per channel use.

Figure 2 plots η^U of the secondary sensor node versus P_t with different I_w. The results show that: (1) P_t is not the larger the better. That is, larger P_t would be more conducive to signal transmission, but worse secrecy performance. (2) The ST is close to the floor when P_t is sufficiently high, in this case, the fixed interference power I_w limits P_t of the SU-Tx to affect ST. Interestingly, the ST in the high power region has a very low floor when I_w is either extremely low or very higher. This can be explained as follows. When I_w is lower, the adverse effects of reliability outweigh the benefits of security brought about by I_w. When I_w is higher, the security problems caused by I_w become the main deterioration factor of ST performance. Therefore, it is very important to choose the appropriate I_w to weigh secrecy performance of the system. Furthermore, the ST first increases and then decreases to a floor, indicating that there exists an optimal transmitting power P_t of the SU-Tx for achieving the best performance.

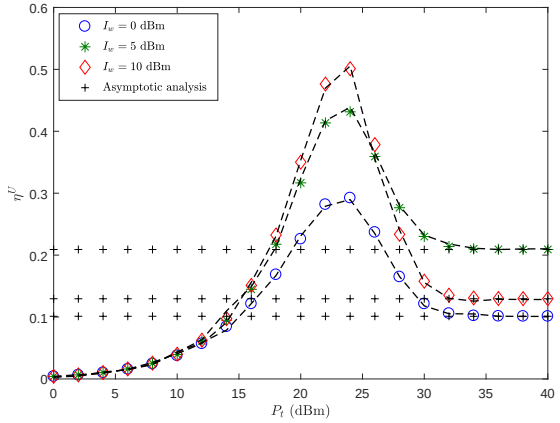

Figure 2. η^U versus P_t with $\lambda_E = 0.001$ *nodes*$/m^2$, $r = 60$ m, $\theta_S = \frac{\pi}{3}$, $R_m = 4.5$ BPCU, $R_m^s = 1$ BPCU, $\beta = \frac{1}{141.4}$, $\delta_0 = 0.1$, $m_S = 0.1$ and $M_S = 200$.

Figure 3 presents η^U of the secondary sensor node versus I_w witha different transmit power P_t. As shown in figure, the ST performance is not always improved with expanding I_w. This is fairly straightforward because there is a tradeoff between reliability and security caused by I_w. In addition, the impacts of P_t on ST performance have similar trends and cause as I_w. Besides, we found that when the transmit power $P_t = 10$ dBm, the ST shows a double peak with I_w, which is mainly due to LOS and NLOS links. Furthermore, with the improving gain of SU-Tx beamforming, the ST would be improved. This can be explained by the high gain antenna improving the receive performance of the secondary sensor node, and increasing the probability of connection; at the same time, it may increase the risk of information leakage.

Figure 4 plots the effects of η^U of the secondary sensor node versus β with the different P_t and I_w. We can see that η^U decreases with increasing β for a lower P_t. This is because the path loss of mmWave is high; with the increase of β, the ST of the secondary sensor node decreases gradually. Yet, given a high P_t, increasing β does not result in a strict decrease in ST of the mmWave networks under the constraint of the I_w. Actually, there exists an optimal β^*, so that a maximum ST can be obtained. NLOS links dominate the mmWave sensor network when β just reaches the optimum point, using multipath signals to maximize ST of secondary sensor nodes. However, when the environment is full of physical barriers, the probability of information reaching the secondary sensor node decreases and the ST decreases until it saturates. This demonstrates that the blockages can also be used to improve the system performance by reasonably setting parameters according to the actual situation in random cognitive mmWave sensor networks.

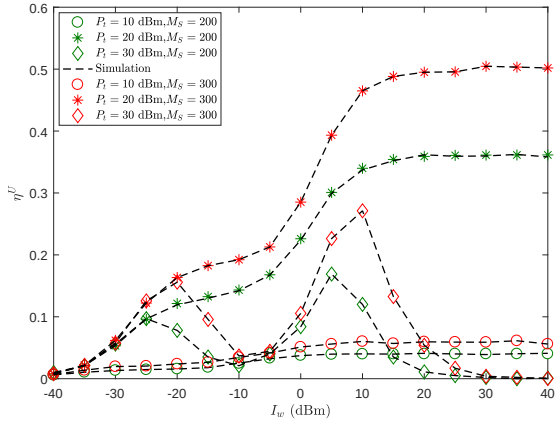

Figure 3. η^U versus I_w with $\lambda_E = 0.001$ $nodes/m^2$, $r = 60$ m, $\theta_S = \frac{\pi}{3}$, $R_m = 4.5$ BPCU, $R_m^s = 1$ BPCU, $\delta_0 = 0.1$, $\beta = \frac{1}{141.4}$.

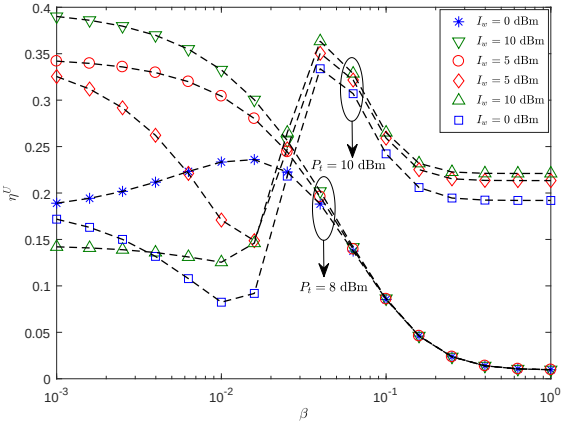

Figure 4. η^U versus β with $\lambda_E = 0.001$ $nodes/m^2$, $r = 60$ m, $\theta_S = \frac{\pi}{3}$, $R_m = 4.5$ BPCU, $R_m^s = 1$ BPCU, $\delta_0 = 0.1$, $m_S = 0.1$ and $M_S = 200$.

Figure 5 presents the effects of η^U of the secondary sensor node versus λ_E with the different I_w and θ_S. It is observed that η^U decreases with the increasing λ_E, since the wiretapping ability of eavesdroppers increases when λ_E is large. We can also see that under the same conditions, the larger the sector guard zone, the better η^U, because the large sector guard zone helps to improve the secrecy performance of the system. Moreover, when λ_E is low, the performance of the system with large I_w is better than that with small I_w. When λ_E is high, the performance of the system with small I_w is better than that of the system with large I_w. The reason for this trend is that the larger I_w will lead to worse secrecy performance when increasing λ_E. It demonstrates that sector guard zone and I_w play an important role in the performance of secondary sensor node. In addition, with the improvement of the directionality of the beamforming of the SU-Tx , η^U would be improved. This can be explained by the fact that the high gain narrow beam antenna reduces the information leakage, improves the receive performance of the SU-Rx, and increases the system reliability. However, we can also see that with the increasing of λ_E, the wiretapping ability of eavesdroppers increases, and the narrow beam would lead to the rapid degradation of system performance. This is because the eavesdroppers may be in the beam, which has a fatal impact on the security of the system considered.

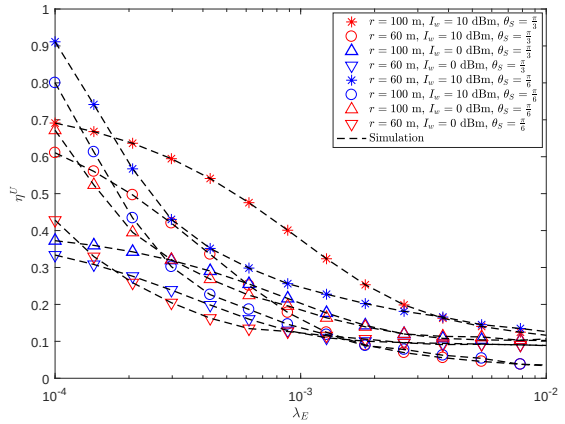

Figure 5. η^U versus λ_E with $P_t = 30$ dBm, $R_m = 4.5$ BPCU, $R_m^s = 1$ BPCU, $\beta = \frac{1}{141.4}$, $\delta_0 = 0.1$, $m_S = 0.1$ and $M_S = 200$.

5. Conclusions

In this paper, we have studied the secrecy performance of the secondary sensor network under the interference temperature constraint of a primary sensor node. Specifically, stochastic geometry-based techniques were adopted for modeling both the locations of sensor nodes and of the eavesdroppers in the networks considered. We considered a special case, where the eavesdroppers and the primary sensor node may be in the secondary network signal beam. Combining the mmWave characteristics, the exact analysis on ST of the secondary sensor node was conducted, and an asymptotic result of ST was further provided. Our results showed that the interference temperature constraint of the primary network can be used to balance the secrecy performance of the secondary network. Moreover, blockages were beneficial to improve the ST of the secondary sensor node under certain conditions. In future works, complex scenarios such as imperfect CSI, base-station (BS) cooperation and nonorthogonal multiple access (NOMA) will be considered. In addition, combining the results presented in this paper with UAV, the secrecy transmission capability may be analyzed.

Author Contributions: Formal analysis, Y.S.; Investigation, Y.S., Z.X. and B.W.; Software, Y.S. and W.Y.; Validation, Z.X. and B.W.; Writing-original draft, Y.S. and W.Y.; Writing-review and editing, Y.C.

Funding: This work was supported by the National Natural Science Foundation of China under Grant No. 61471393 and 61771487.

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

Appendix A

Based on Equation (10), Ψ_1 is calculated in detail. Applying the probability generating function, polar coordinates and [37] (Equation (3.351.1)), we can formulate

$$\begin{aligned}\Psi_1 &= \Pr\left\{\max_{E\in\phi_E^L}\left(\frac{M_S P_t |h_{SE}|^2 L(r_E)}{\sigma_E^2}\right) < \varepsilon_2\right\} = E\left\{\prod_{E\in\phi_E^L}\Pr\left(|h_{SE}|^2 < \frac{\sigma_E^2\varepsilon_2 r_E^{\alpha_L}}{P_t C_L M_S}\right)\right\}\\ &= \exp\left(-\theta_s\lambda_E\int_r^\infty\left(1-\frac{\Upsilon\left(N_L, \frac{\sigma_E^2\varepsilon_2 r_E^{\alpha_L} N_L}{P_t C_L M_S}\right)}{\Gamma(N_L)}\right)e^{-\beta r_E} r_E dr_E\right)\\ &= \exp\left(-\theta_s\lambda_E\left(\frac{\Gamma(2,\beta r)}{\beta^2} - \sum_{n=0}^{\infty}\frac{(-1)^n\left(\frac{\sigma_E^2\varepsilon_2 N_L}{P_t C_L M_S}\right)^{N_L+n}\Gamma(\alpha_L(N_L+n)+2,\beta r)}{n!(N_L+n)\Gamma(N_L)\beta^{\alpha_L(N_L+n)+2}}\right)\right)\end{aligned} \quad . \tag{A1}$$

Following a procedure similar to that used for obtaining Ψ_1, Ψ_2 can be obtained. For the sake of brevity, the calculation procedure of Ψ_2 is omitted.

Substituting Ψ_1 and Ψ_2 into Equation (10) and after some mathematical manipulations, $F_y(\varepsilon_2)$ can be expressed as

$$F_y(\varepsilon_2) = \exp\left(-\theta_s\lambda_E\left(\left(\frac{(N_N-1)!}{\Gamma(N_N)}\right)\sum_{m=0}^{N_N-1}\frac{\left(\frac{\sigma_E^2\varepsilon_2 N_N}{P_t C_N M_S}\right)^m}{m!}\times\frac{\Gamma\left(\frac{m\alpha_N+2}{\alpha_N},\frac{\sigma_E^2\varepsilon_2 r^{\alpha_N} N_N}{P_t C_N M_S}\right)}{\alpha_N\left(\frac{\sigma_E^2\varepsilon_2 N_N}{P_t C_N M_S}\right)^{\frac{m\alpha_N+2}{\alpha_N}}}\right.\right.$$
$$\left.\left.+\sum_{n=0}^{\infty}\frac{(-1)^n\left(\frac{\sigma_E^2\varepsilon_2 N_N}{P_t C_N M_S}\right)^{N_N+n}}{n!(N_N+n)\Gamma(N_N)}\frac{\Gamma(\alpha_N(N_N+n)+2,\beta r)}{\beta^{\alpha_N(N_N+n)+2}}-\sum_{n=0}^{\infty}\frac{(-1)^n\left(\frac{\sigma_E^2\varepsilon_2 N_L}{P_t C_L M_S}\right)^{N_L+n}}{n!(N_L+n)\Gamma(N_L)}\frac{\Gamma(\alpha_L(N_L+n)+2,\beta r)}{\beta^{\alpha_L(N_L+n)+2}}\right)\right). \quad \text{(A2)}$$

Similarly, $F_v(\varepsilon_1)$ is obtained for Equation (11), which can be expressed as

$$F_v(\varepsilon_1) = \frac{2}{R_U^2}\left(\sum_{i=0}^{\infty}\frac{(-1)^i(A\varepsilon_1 N_L)^{N_L+i}}{i!(N_L+i)\Gamma(N_L)(P_t M_S C_L)^{N_L+i}}\times\frac{\Upsilon(\alpha_L(N_L+i)+2,\beta R_U)}{\beta^{\alpha_L(N_L+i)+2}}\right.$$
$$\left.+\sum_{j=0}^{\infty}\frac{(-1)^j(A\varepsilon_1 N_N)^{N_N+j}}{j!(N_N+j)\Gamma(N_N)(P_t M_S C_N)^{N_N+j}}\left(\frac{(R_U)^{\alpha_N(N_N+j)+2}}{\alpha_N(N_N+j)+2}-\frac{\Upsilon(\alpha_N(N_N+j)+2,\beta R_U)}{\beta^{\alpha_N(N_N+j)+2}}\right)\right). \quad \text{(A3)}$$

Substituting $F_y(\varepsilon_2)$ and $F_v(\varepsilon_1)$ into Equation (9), the proof is completed.

Appendix B

Based on Equation (14), let us now turn our attention on Ψ_3. Using the probability generating function, polar coordinates and [37] (Equation (3.351.1)), we can formulate

$$\Psi_3 = \Pr\left\{\max_{E\in\phi_E^L}\left(\frac{I_w|h_{SE}|^2 L(r_E)}{|h_{SP}|^2 L(r_{SP})\sigma_E^2}\right)<\varepsilon_2\right\}$$
$$=\exp\left(-\theta_s\lambda_E\left(\frac{\Gamma(2,\beta r)}{\beta^2}-\sum_{n=0}^{\infty}\frac{(-1)^n\left(\frac{\sigma_E^2\varepsilon_2 x N_L}{I_w C_L}\right)^{N_L+n}\Gamma(\alpha_L(N_L+n)+2,\beta r)}{n!(N_L+n)\Gamma(N_L)\beta^{\alpha_L(N_L+n)+2}}\right)\right). \quad \text{(A4)}$$

Following a procedure similar to that used for obtaining Ψ_3, Ψ_4 can be obtained. For the sake of brevity, the calculation procedure of Ψ_4 is omitted.

Upon substituting Ψ_3 and Ψ_4 into Equation (14), as well as after some mathematical manipulations, the expressions for $F_z(\varepsilon_2)$ and $F_u(\varepsilon_1)$ are expressed as

$$F_z(\varepsilon_2) = \exp\left(-\theta_s\lambda_E\left(\left(\frac{(N_N-1)!}{\Gamma(N_N)}\right)\sum_{m=0}^{N_N-1}\frac{\left(\frac{\sigma_E^2\varepsilon_2 x N_N}{I_w C_N}\right)^m}{m!}\times\frac{\Gamma\left(\frac{m\alpha_N+2}{\alpha_N},\frac{\sigma_E^2\varepsilon_2 x r^{\alpha_N} N_N}{I_w C_N}\right)}{\alpha_N\left(\frac{\sigma_E^2\varepsilon_2 x N_N}{I_w C_N}\right)^{\frac{m\alpha_N+2}{\alpha_N}}}\right.\right.$$
$$\left.\left.+\sum_{n=0}^{\infty}\frac{(-1)^n\left(\frac{\sigma_E^2\varepsilon_2 x N_N}{I_w C_N}\right)^{N_N+n}}{n!(N_N+n)\Gamma(N_N)}\frac{\Gamma(\alpha_N(N_N+n)+2,\beta r)}{\beta^{\alpha_N(N_N+n)+2}}-\sum_{n=0}^{\infty}\frac{(-1)^n\left(\frac{\sigma_E^2\varepsilon_2 x N_L}{I_w C_L}\right)^{N_L+n}}{n!(N_L+n)\Gamma(N_L)}\frac{\Gamma(\alpha_L(N_L+n)+2,\beta r)}{\beta^{\alpha_L(N_L+n)+2}}\right)\right). \quad \text{(A5)}$$

$$F_u(\varepsilon_1) = \frac{2}{R_U^2}\left(\sum_{i=0}^{\infty}\frac{(-1)^i(Ax\varepsilon_1 N_L)^{N_L+i}}{i!(N_L+i)\Gamma(N_L)(I_w C_L)^{N_L+i}}\times\frac{\Upsilon(\alpha_L(N_L+i)+2,\beta R_U)}{\beta^{\alpha_L(N_L+i)+2}}\right.$$
$$\left.+\sum_{j=0}^{\infty}\frac{(-1)^j(Ax\varepsilon_1 N_N)^{N_N+j}}{j!(N_N+j)\Gamma(N_N)(I_w C_N)^{N_N+i}}\left(\frac{(R_U)^{\alpha_N(N_N+j)+2}}{\alpha_N(N_N+j)+2}-\frac{\Upsilon(\alpha_N(N_N+j)+2,\beta R_U)}{\beta^{\alpha_N(N_N+j)+2}}\right)\right). \quad \text{(A6)}$$

Upon substituting $F_z(\varepsilon_2)$ and $F_u(\varepsilon_1)$ into Equation (13), Q_2 is given by Equation (16).

References

1. Wu, Y.; Khisti, A.; Xiao, C.; Caire, G.; Wong, K.-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]
2. Hosseini, H.; Anpalagan, A.; Raahemifar, K.; Erkucuk, S. Wavelet-Based Cognitive SCMA System for mmWave 5G Communication Networks. *IET Commun.* **2017**, *11*, 831–836. [CrossRef]
3. Hosseini, H.; Anpalagan, A.; Raahemifar, K.; Erkucuk, S.; Habib, S. Joint Wavelet-Based Spectrum Sensing and FBMC Modulation for Cognitive mmWave Small Cell Networks. *IET Commun.* **2016**, *10*, 1803–1809. [CrossRef]
4. Park, J.; Andrews, J.G.; Heath, R.W. Inter-Operator Base Station Coordination in Spectrum-Shared Millimeter Wave Cellular Networks. *IEEE Trans. Cogn. Commun. Netw.* **2018**, *4*, 513–528. [CrossRef]
5. Xu, X.; Yang, W.; Cai, Y.; Jin, S. On the Secure Spectral-Energy Efficiency Tradeoff in Random Cognitive Radio Networks. *IEEE J. Sel. Areas Commun.* **2016**, *34*, 2706–2722. [CrossRef]
6. Fragkiadakis, A.G.; Tragos, E.Z.; Askoxylakis, I.G. A Survey on Security Threats and Detection Techniques in Cognitive Radio Networks. *IEEE Commun. Surv. Tutor.* **2013**, *15*, 428–445. [CrossRef]
7. Bloch, M.; Barros, J.; Rodrigues, M.R.D.; McLaughlin, S.W. Wireless Information-Theoretic Security. *IEEE Trans. Inf. Theory* **2008**, *54*, 2515–2534. [CrossRef]
8. Shi, H.; Yang, W.; Chen, D.; Luo, Y.; Cai, Y. Secure Transmission for Simultaneous Wireless Information and Power Transfer in AF Untrusted Relay Networks. *Sensors* **2018**, *19*, 76–97. [CrossRef]
9. Tang, X.; Cai, Y.; Yang, W.; Yang, W.; Chen, D.; Hu, J. Secure Transmission of Cooperative Zero-Forcing Jamming for Two-User SWIPT Sensor Networks. *Sensors* **2018**, *18*, 331. [CrossRef]
10. Xiang, Z.; Yang, W.; Pan, G.; Cai, Y.; Sun, X. Secure Transmission in Non-Orthogonal Multiple Access Networks with an Untrusted Relay. *IEEE Wirel. Commun. Lett.* **2019**, *8*, 905–908. [CrossRef]
11. Xiang, Z.; Yang, W.; Pan, G.; Cai, Y.; Song, Y. Physical Layer Security in Cognitive Radio Inspired NOMA Network. *IEEE J. Sel. Top. Signal Process.* **2019**, *13*, 700–714. [CrossRef]
12. Tang, X.; Cai, Y.; Huang, Y.; Duong, T.Q.; Yang, W.; Yang, W. Secrecy Outage Analysis of Buffer-Aided Cooperative MIMO Relaying Systems. *IEEE Trans. Veh. Technol.* **2017**, *67*, 2035–2048. [CrossRef]
13. Li, B.; Qi, X.; Huang, K.; Fei, Z.; Zhou, F.; Hu, R.Q. Security-Reliability Tradeoff Analysis for Cooperative NOMA in Cognitive Radio Networks. *IEEE Trans. Commun.* **2019**, *67*, 83–96. [CrossRef]
14. Atallah, M.; Kaddoum, G. Secrecy Analysis in Wireless Network with Passive Eavesdroppers by Using Partial Cooperation. *IEEE Trans. Veh. Technol.* **2019**, *68*, 7225–7230. [CrossRef]
15. Jameel, F.; Wyne, S.; Kaddoum, G.; Duong, T.Q. A Comprehensive Survey on Cooperative Relaying and Jamming Strategies for Physical Layer Security. *IEEE Commun. Surv. Tutor.* **2019**. [CrossRef]
16. Xu, X.; He, B.; Yang, W.; Zhou, X.; Cai, Y. Secure Transmission Design for Cognitive Radio Networks With Poisson Distributed Eavesdroppers. *IEEE Trans. Inf. Forensics Secur.* **2016**, *11*, 373–387. [CrossRef]
17. Cai, Y.; Xu, X.; Yang, W. Secure Transmission in the Random Cognitive Radio Networks with Secrecy Guard Zone and Artificial Noise. *IET Commun.* **2017**, *10*, 1904–1913. [CrossRef]
18. Zou, Y.; Li, X.; Liang, Y.-C. Secrecy Outage and Diversity Analysis of Cognitive Radio Systems. *IEEE J. Sel. Areas Commun.* **2017**, *32*, 2222–2236. [CrossRef]
19. Atallah, M.; Kaddoum, G. Design and Performance Analysis of Secure Multicasting Cooperative Protocol for Wireless Sensor Network Applications. *IEEE Wirel. Commun. Lett.* **2019**. [CrossRef]
20. Valliappan, N.; Lozano, A.; Heath, R.W. Antenna Subset Modulation for Secure Millimeter-Wave Wireless Communication. *IEEE Trans. Commun.* **2013**, *61*, 3231–3245. [CrossRef]
21. Yang, N.; Wang, L.; Geraci, G.; Elkashlan, M.; Yuan, J.; Renzo, M.D. Safeguarding 5G Wireless Communication Networks Using Physical Layer Security. *IEEE Commun. Mag.* **2015**, *53*, 20–27. [CrossRef]
22. Yang, W.; Tao, L.; Sun, X.; Ma, R.; Cai, Y.; Zhang, T. Secure on-off transmission in mmWave systems with randomly distributed eavesdroppers. *IEEE Access.* **2019**, *7*, 32681–32692. [CrossRef]
23. Vuppala, S.; Biswas, S.; Ratnarajah, T. An Analysis on Secure Communication in Millimeter/Micro-Wave Hybrid Networks. *IEEE Trans. Commun.* **2015**, *64*, 3507–3519. [CrossRef]
24. Wang, L.; Elkashlan, M.; Duong, T.Q.; Heath, R.W. Secure Communication in Cellular Networks: The Benefits of Millimeter Wave Mobile Broadband. In Proceedings of the 2014 IEEE 15th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC), Toronto, ON, Canada, 22–25 June 2014; pp. 115–119.

25. Wang, C.; Wang, H.-M. Physical Layer Security in Millimeter Wave Cellular Networks. *IEEE Trans. Wirel. Commun.* **2016**, *15*, 5569–5585. [CrossRef]
26. Zhu, Y.; Wang, L.; Wong, K.-K.; Heath, R.W. Secure Communications in Millimeter Wave Ad Hoc Networks. *IEEE Trans. Wirel. Commun.* **2017**, *16*, 3205–3217. [CrossRef]
27. Sun, X.; Yang, W.; Cai, Y.; Xiang, Z.; Tang, X. Secure Transmissions in Millimeter Wave SWIPT UAV-Based Relay Networks. *IEEE Wirel. Commun. Lett.* **2019**, *8*, 785–788. [CrossRef]
28. Zhu, Y.; Zheng, G.; Fitch, M. Secrecy Rate Analysis of UAV-Enabled mmWave Networks Using Matérn Hardcore Point Processes. *IEEE J. Sel. Areas Commun.* **2018**, *36*, 1397–1409. [CrossRef]
29. Rangan, S.; Rappaport, T.S.; Erkip, E. Millimeter-Wave Cellular Wireless Networks: Potentials and Challenges. *arXiv* **2014**, arXiv:1401.2560.
30. Vuppala, S.; Tolossa, Y.J.; Member, S.S.; Kaddoum, G.; Abreu, G.; Member, S.S. On the Physical Layer Security Analysis of Hybrid Millimeter Wave Networks. *IEEE Trans. Commun.* **2018**, *66*, 1139–1152. [CrossRef]
31. Tao, L.; Yang, W.; Yang, W.; Cai, Y. Capacity Threshold-based On-off Transmission in mmWave Systems with Randomly Distributed Eavesdroppers. In Proceedings of the 10th International Conference on Wireless Communications and Signal Processing (WCSP 2018), Hangzhou, China, 18–20 October 2018; pp. 1–6.
32. Song, Y.; Yang, W.; Xiang, Z.; Wang, B.; Cai, Y. Secure Transmission in mmWave NOMA Networks With Cognitive Power Allocation. *IEEE Access.* **2019**, *7*, 76104–76119. [CrossRef]
33. Turgut, E.; Gursoy, M.C. Coverage in Heterogeneous Downlink Millimeter Wave Cellular Networks. *IEEE Trans. Commun.* **2017**, 65, 4463–4477. [CrossRef]
34. He, B.; Member, S.; Zhou, X.; Abhayapala, T.D.; Member, S. Achieving Secrecy Without Knowing the Number of Eavesdropper Antennas. *IEEE Trans. Wirel. Commun.* **2015**, *14*, 7030–7043. [CrossRef]
35. Kolawole, O.Y.; Vuppala, S.; Sellathurai, M.; Ratnarajah, T. On the Performance of Cognitive Satellite-Terrestrial Networks. *IEEE Trans. Cogn. Commun. Netw.* **2017**, *3*, 668–683. [CrossRef]
36. MacCartney, G.R.; Rappaport, T.S.; Sun, S.; Deng, S. Indoor Office Wideband Millimeter-wave Propagation Measurements and Channel Models at 28 and 73 GHz for Ultra-Dense 5G Wireless Networks. *IEEE Access.* **2015**, *3*, 2388–2424. [CrossRef]
37. Gradshteyn, I.S.; Ryzhik, I.M. *Table of Integrals, Series, and Products*, 7th ed.; Academic Press: New York, NY, USA, 2007.