sensors

MDPI

Article

Secure Multiuser Communications in Wireless Sensor Networks with TAS and Cooperative Jamming

Maoqiang Yang [1,†], Bangning Zhang [1,†], Yuzhen Huang [1,†], Nan Yang [2,†], Daoxing Guo [1,*,†] and Bin Gao [1,†]

1 College of Communications Engineering, PLA University of Science and Technology, No. 2 Biaoying, Qinhuai District, Nanjing 210007, China; yyypub@163.com (M.Y.); zbnpub@163.com (B.Z.); yzh_huang@sina.com (Y.H.); feimaxiao123@gmail.com (B.G.)

2 Research School of Engineering, Australian National University, Canberra, ACT 2601, Australia; nan.yang@anu.edu.au

* Correspondence: nsagfg@163.com; Tel.: +86-136-7511-6908

† These authors contributed equally to this work.

Academic Editors: Ignacio Bravo, Esther Palomar, Alfredo Gardel and José Luis Lázaro
Received: 5 September 2016; Accepted: 8 November 2016; Published: 12 November 2016

Abstract: In this paper, we investigate the secure transmission in wireless sensor networks (WSNs) consisting of one multiple-antenna base station (BS), multiple single-antenna legitimate users, one single-antenna eavesdropper and one multiple-antenna cooperative jammer. In an effort to reduce the scheduling complexity and extend the battery lifetime of the sensor nodes, the switch-and-stay combining (SSC) scheduling scheme is exploited over the sensor nodes. Meanwhile, transmit antenna selection (TAS) is employed at the BS and cooperative jamming (CJ) is adopted at the jammer node, aiming at achieving a satisfactory secrecy performance. Moreover, depending on whether the jammer node has the global channel state information (CSI) of both the legitimate channel and the eavesdropper's channel, it explores a zero-forcing beamforming (ZFB) scheme or a null-space artificial noise (NAN) scheme to confound the eavesdropper while avoiding the interference to the legitimate user. Building on this, we propose two novel hybrid secure transmission schemes, termed TAS-SSC-ZFB and TAS-SSC-NAN, for WSNs. We then derive the exact closed-form expressions for the secrecy outage probability and the effective secrecy throughput of both schemes to characterize the secrecy performance. Using these closed-form expressions, we further determine the optimal switching threshold and obtain the optimal power allocation factor between the BS and jammer node for both schemes to minimize the secrecy outage probability, while the optimal secrecy rate is decided to maximize the effective secrecy throughput for both schemes. Numerical results are provided to verify the theoretical analysis and illustrate the impact of key system parameters on the secrecy performance.

Keywords: wireless sensor networks; physical layer security; multiuser scheduling; transmit antenna selection; cooperative jamming; secrecy outage probability; effective secrecy throughput

1. Introduction

Wireless sensor networks (WSNs) are envisioned as an emerging research field with numerous applications, such as health monitoring, vehicular tracking, military surveillance and environment sensing. Therefore, the research of WSNs has recently attracted a tremendous amount of attention from both industry and academia [1,2]. Generally, in the WSNs, a large number of the sensor nodes are deployed to collect the environmental information, and then report the sensed data to a base station (BS) wirelessly [3,4]. However, the secure transmission of WSNs is a fundamental concern due to the broadcast characteristics of radio propagation, and thus the sensing information is required

to be safeguarded [5,6]. Conventionally, the cryptographic encryption relying on a secrecy key is broadly adopted to protect the confidential message from being wiretapped by the eavesdroppers. Nevertheless, the limitations behind the traditional cryptographic techniques lie in the complex protocols and architectures for the distribution and management of secret keys. It is noteworthy that the sensor nodes are the energy-constrained, cost-constrained, and lightweight computing devices, in which a considerable portion of the available energy is allocated to support the core sensorial and computational capabilities. Hence, there is possibly little left over to provide the security [7–12]. As such, it is of interest to explore efficient and low-complexity protocols to guarantee the secrecy of WSNs.

To address the above concerns, the physical layer security (PLS) technique has emerged as an attractive approach to achieve the perfect secrecy from an information-theoretical perspective [13]. The basic idea of PLS is to take advantage of the imperfection of wireless medium (e.g., fading, interference and noise) to ensure the secure transmission between the legitimate parties. By introducing randomness and structured redundancy into the data signal, the PLS enables legitimate users to decode the confidential messages correctly while keeps the eavesdropper from extracting the messages successfully [4,14,15].

Recently, various advanced techniques such as multi-antenna, cooperative relaying and cooperative jamming have been incorporated to further boost the potential benefits of PLS. In particular, transmit antenna selection (TAS) has been widely investigated on account of the low realization complexity of radio frequency (RF) chain, meanwhile yielding full diversity [16–21]. Recently, Yang et al. [16] proposed and analyzed TAS to enhance PLS in multiple-input multiple-output (MIMO) wiretap channels. Later on, TAS with Alamouti coding and power allocation was addressed in [17]. Considering the outdated channel state information (CSI) due to feedback delay, the authors in [18] investigated the secrecy outage performance of spectrum sharing MIMO networks with generalized TAS and maximal ratio combining (MRC) over the Nakagami-m channel. Based on whether the source node has the global CSIs of both the main link and eavesdropper's link, optimal antenna selection (OAS) and suboptimal antenna selection (SAS) were proposed in [19] with the traditional space-time transmission (STT) as a benchmark in MIMO systems. Meanwhile, [20] examined TAS/MRC and TAS/selection combining (SC) scheme with decode-and-forward (DF) relaying in underlay spectrum sharing with multiple primary users (PU) transceivers and multiple antennas at the secondary users (SUs). In addition, in [21], the secrecy performance of multiple-input single-output (MISO) simultaneous wireless information and the power transfer (SWIPT) system was studied with TAS and imperfect CSI.

In parallel, cooperative jamming has been identified as an effective paradigm to enhance the security due to its ability of reducing the leakage rate to the wiretapper. Loosely speaking, the jamming signals can be transmitted from the source [14,15], the legitimate destination [22,23] and the relay [24–30]. As indicated in these studies, the jamming signals need to be designed carefully since the interference may also be leaked to the desired user. With the assistance of artificial noise, the optimal secure transmission was addressed by considering an on-off transmission scheme and an adaptive transmission scheme in the MISO single-antenna eavesdropper wiretap channel [14] and in the MISO multi-antenna eavesdropper wiretap channel [15], respectively. In [14,15], the artificial noise was transmitted in conjunction with the information signal at the BS, and beamforming matrix was designed to deteriorate the eavesdropper's channel quality by transmitting noise in all directions except towards the intended user. Furthermore, [22] generated the artificial jamming noise at the legitimate receiver, under the assumption that the receiver knows the artificial jamming noise and thus can cancel it by performing self-interference subtraction. In [23], a joint scheme of destination-aid cooperative jamming and precoding at both the source and the relay was proposed for dual-hop amplify-and-forward MIMO untrusted relay systems, where the self-interference is assumed to be perfectly estimated and can be subtracted from the received signal. In addition, considering the jamming signals emitted by the relay, the external helper degraded the eavesdropper's channel without hurting the legitimate channel. With

imperfect CSI, the secure communication aided by a multi-antenna cooperative jammer was addressed in [24]. Taking into account which role the helper should take to enhance the secrecy, [25] investigated a direct transmission scheme (DTS) and a relay transmission scheme (RTS) in terms of ergodic secrecy rate and optimal power allocation. The work in [26] investigated different secrecy rate optimization techniques for a multi-antenna cooperative jammer assisted MIMO secrecy channel. Moreover, in [27], three secure transmission schemes were investigated in multi-antenna relay systems with cooperative jamming in terms of the ergodic achievable secrecy rate. Very recently, the worst-case cooperative jamming for secure communications in the cognitive internet of things (CIoT) was investigated in [28]. In [29], the MRC/ZFB scheme at the relay was designed to enhance the secrecy performance of dual-hop multi-antenna spectrum sharing relaying networks, while the cooperative jamming with the ZFB scheme was addressed in [30] to achieve secure transmission in cooperative relaying networks.

It is critical to note that, in multiuser communication systems, the conventional opportunistic scheduling scheme requires the feedback of channel information for all the diversity branches. Based on the continuously-updated CSIs of all the nodes in the network, full multiuser diversity gains are explored at the central scheduler. However, a significant portion of the battery energy of the low-end terminals and a large share of air-link resources are occupied to feed the CSIs back instead of valuable data traffic [31]. To circumvent this difficulty, the multiuser switched diversity scheduling schemes were proposed in [32] in order to search any acceptable user (i.e., with good channel quality) rather than the best one among all. Recently, PLS with threshold-based multiuser scheduling was studied in multi-antenna wireless networks [33]. Considering the imperfect decoding at the regenerative relay, the secure multiuser scheduling was investigated in dual-hop relay networks over Nakagami-m fading in [34]. In particular, the multi-branch switch-and-stay combining (SSC) scheme was first addressed in [35], which reduces the implementation complexity for multi-channel communication scenarios. In the multi-branch SSC scheme, if the channel quality of the currently connected branch exceeds a predetermined threshold, then this branch is kept. Otherwise, no matter what the channel quality of the switch-to branch is, the scheduler settles on that branch for the next transmission burst [35]. It is noteworthy that, in considering the opportunistic relay selection in cooperative networks, the distributed SSC scheme was explored in [36] for secrecy enhancement. More recently, a secure SSC protocol was proposed in [37] to overcome the high relay switching rate for two-phase underlay cognitive relay networks.

To the best knowledge of the authors, the SSC based secure multiuser transmission with TAS and cooperative jamming for WSNs has not been reported in literature thus far. We are therefore motivated to examine the security level of such networks when cooperative jamming is applied in parallel with user selection. The main contributions of this paper are summarized as follows:

- Two novel hybrid secure transmission schemes, i.e., TAS-SSC-ZFB and TAS-SSC-NAN, are proposed for securing the data transmission in WSNs while achieving low feedback requirements and examination costs.
- Exact closed-form expressions for the secrecy outage probability and effective secrecy throughput are derived for the proposed schemes, which provide an efficient and convenient approach to characterize the secrecy performance of the considered network.
- Using these closed-form expressions, the optimal switching threshold is determined and the optimal power allocation factor between the BS and CJ is obtained for both schemes to minimize the secrecy outage probability. In addition, the optimal secrecy rate is decided for both schemes to maximize the effective secrecy throughput. Our findings demonstrate that the TAS-SSC-ZFB scheme outperforms the TAS-SSC-NAN scheme in terms of both secrecy outage probability and effective secrecy throughput, while the TAS-SSC-NAN scheme is more robust than the TAS-SSC-ZFB scheme.

The remaining parts of the paper are organized as follows. In Section 2, the system model and transmission protocols of TAS-SSC-ZFB and TAS-SSC-NAN are presented, and the secrecy performance

of both schemes are analyzed in Section 3. In Section 4, the numerical simulation and discussions are provided to validate the theoretical analysis. Finally, the conclusions are drawn in Section 5.

2. System Model and Transmission Protocol

2.1. System Model

Let us consider a multiuser downlink wireless sensor network, as illustrated in Figure 1, in which a base station (A) with A_{A} transmit antennas serves N_{B} single-antenna legitimate sensor nodes (B) in the presence of a single-antenna eavesdropper (E), and a friendly pure jammer (J) with A_{J} antennas $(A_{\mathrm{J}} \geq 2)$. In this model, we preserve the practical assumption that the legitimate channel, jammer's channel and the eavesdropper's channel are subject to independent and non-identically distributed (i.n.i.d) flat Rayleigh fading such that they have different average signal-to-noise ratio (SNR), i.e., $\overline{\gamma}_{\mathrm{B}}, \overline{\gamma}_{\mathrm{J}}$ and $\overline{\gamma}_{\mathrm{E}}$, and the involved fading coefficients are quasi-stationary within the channel coherence time. In order to perform secure transmission, the BS encodes the messages with a capacity achieving wiretap codebook and then transmits the resulting codewords to the legitimate user. In addition, each transmission block is considered to be equivalent to the channel coherence time and is composed of two parts, i.e., guard time and data transmission time.

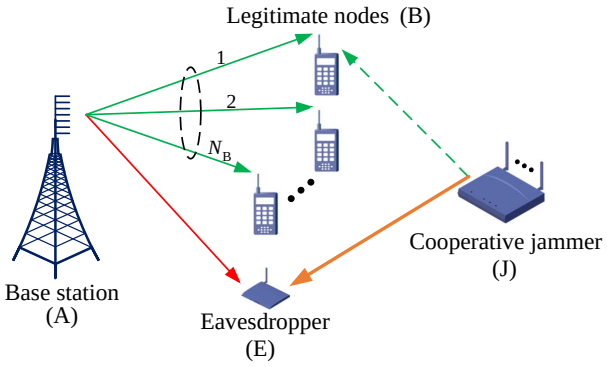

Figure 1. System model.

2.2. Secure Transmission Schemes

We now detail the proposed secure transmission schemes in the considered WSNs. In general, the complete transmission procedure can be separated into two phases.

In the first phase, an acceptable user of N_{B} candidates is selected according to the SSC scheme [35] out of A_{A} transmit antennas within the guard time to carry out the data transmission. To be specific, considering the first transmit antenna (α=1), the previously selected user k ($k \in \{1, 2, ..., N_{\mathrm{B}}\}$) compares its instantaneous SNR $\gamma^{\mathrm{b}}_{\alpha,k}$ with the pre-determined switching threshold γ_{T}. If the received instantaneous SNR exceeds γ_{T}, then it stays without switching over and feeds the SNR and user index back to the BS with $\gamma_{\mathrm{B},\alpha}$=$\gamma^{\mathrm{b}}_{\alpha,k} \geq \gamma_{\mathrm{T}}$. Otherwise, it switches to the next user regardless of its SNR following the similar feedback operation with $\gamma_{\mathrm{B},\alpha}$=$\gamma^{\mathrm{b}}_{\alpha,k+1}$. The same SSC operation repeats for the rest of $A_{\mathrm{A}} - 1$ transmit antennas.

To proceed, the pair of transmit antenna and corresponding selected user that gives the largest instantaneous SNR is picked out, which is right for the data transmission time. As such, only one legitimate user is scheduled for data transmission without continuously examining all the users in the WSNs, which brings about considerable savings of feedback requirements and implementation complexity. Therefore, the selected antenna is given by

$$\alpha^{*} = \underset{1 \leq \alpha \leq A_{\mathrm{A}}}{\operatorname{argmax}} \left(\gamma_{\mathrm{B},\alpha} \right). \tag{1}$$

In the second phase, we consider a cooperative relay node, which serves as the friendly pure jammer. Note that the synchronization requirement between the cooperative jammer and the BS can be implemented by some well-known techniques, for instance, the time-service from the GPS or compass. Alternatively, the BS can broadcast the timing information, which enables the cooperative jammer to keep the same pace with the BS. Depending on whether the relay node has the global CSIs of both J $\rightarrow$ B link and J $\rightarrow$ E link, the ZFB scheme and NAN scheme are, respectively, explored to confound the eavesdropper while avoiding interference with the selected legitimate user.

2.2.1. Zero-Forcing Beamforming

Firstly, similar to [29,30,38,39], we assume that the CSIs of both J $\rightarrow$ B link and J $\rightarrow$ E link are available at the relay. It is pointed out that this scenario is reasonable in the multiuser system where the user may play dual roles as legal receiver for some messages and as eavesdropper for others [40–42].

The purpose of the ZFB scheme is to maximize the interference imposed on the eavesdropper while avoiding the interruption to the selected legitimate user. To this end, according to the principle of ZFB scheme, we obtain

$$\begin{aligned} &\max_{\mathbf{w}} \left|\mathbf{h}_{\mathrm{JE}}^{\dagger}\mathbf{w}\right|, \\ &s.t. \left|\mathbf{h}_{\mathrm{JB}}^{\dagger}\mathbf{w}\right| = 0 \ \& \ \|\mathbf{w}\|_F = 1, \end{aligned} \tag{2}$$

where † denotes the conjugate transpose operator and $\|\cdot\|_F$ represents the Frobenius norm. $\mathbf{w}$ is the weight vector, $\mathbf{h}_{\mathrm{JB}}$ and $\mathbf{h}_{\mathrm{JE}}$, separately, denote the $A_{\mathrm{J}} \times 1$ vector for the CSIs of J $\rightarrow$ B link and J $\rightarrow$ E link, whose entries follow Rayleigh distribution with zero mean, and variance λ_{JB} and λ_{JE}, respectively.

Based on the projection matrix theory [43] (Proposition 1), the optimum beamforming vector $\mathbf{w}$ is given by

$$\mathbf{w} = \frac{\aleph^{\perp}\mathbf{h}_{\mathrm{JE}}}{\left\|\aleph^{\perp}\mathbf{h}_{\mathrm{JE}}\right\|_F}, \tag{3}$$

where $\aleph^{\perp} = \mathbf{I} - \mathbf{h}_{\mathrm{JB}}\left(\mathbf{h}_{\mathrm{JB}}^{\dagger}\mathbf{h}_{\mathrm{JB}}\right)^{-1}\mathbf{h}_{\mathrm{JB}}^{\dagger}$ is the projection idempotent matrix. Hence, the instantaneous SNR of the legitimate channel is given by

$$\gamma_{\mathrm{B}} = \frac{P_{\mathrm{A}}}{\sigma_{\mathrm{B}}^2}|h_{\alpha^*\mathrm{B}}|^2, \tag{4}$$

and the instantaneous received signal-to-interference-and-noise ratio (SINR) of eavesdropper's channel is given by

$$\gamma_{\mathrm{E}}^{(\dagger)} = \frac{\frac{P_{\mathrm{A}}}{\sigma_{\mathrm{E}}^2}|h_{\alpha^*\mathrm{E}}|^2}{\frac{P_{\mathrm{J}}}{\sigma_{\mathrm{E}}^2}\left\|\aleph^{\perp}\mathbf{h}_{\mathrm{JE}}\right\|_F^2 + 1}, \tag{5}$$

where $h_{\alpha^*\mathrm{B}}$ and $h_{\alpha^*\mathrm{E}}$ denote the CSIs of the selected legitimate channel and the selected transmit antenna to the eavesdropper channel, respectively. Its entries follow Rayleigh distribution with zero mean, and variance λ_{AB} and λ_{AE}. σ_{B}^2 and σ_{E}^2 denote the noise variance at the legitimate user and eavesdropper, respectively. P_{A} and P_{J} denote the transmit powers at the BS and the jammer, respectively.

2.2.2. Null-Space Artificial Noise

To relax the assumption in the ZFB scheme, we now consider that the CSI of J $\rightarrow$ E link is unavailable at the relay and the relay only has the knowledge of CSI for J $\rightarrow$ B link. Here, the NAN scheme is exploited to emit artificial noise in the nullspace of the selected legitimate user but

disperse in all directions towards the eavesdropper. We design the $A_{\mathrm{J}} \times A_{\mathrm{J}}$ beamforming matrix as $\mathbf{W} = \left[\mathbf{w}_{\mathrm{JB}}, \mathbf{W}_{\mathrm{JE}}\right]$, where $\mathbf{w}_{\mathrm{JB}}$ is an $A_{\mathrm{J}} \times 1$ vector used for J $\rightarrow$ B link and $\mathbf{W}_{\mathrm{JE}}$ is an $A_{\mathrm{J}} \times \left(A_{\mathrm{J}} - 1\right)$ matrix used to deteriorate the quality of eavesdropper's channel by transmitting AN in all directions except towards the selected legitimate user.

To do so, we choose $\mathbf{w}_{\mathrm{JB}}$ as the principle eigenvector corresponding to the largest eigenvalue of $\mathbf{h}_{\mathrm{JB}}\mathbf{h}_{\mathrm{JB}}^{\dagger}$, and then choose $\mathbf{W}_{\mathrm{JE}}$ as the remaining $A_{\mathrm{J}} - 1$ eigenvectors of $\mathbf{h}_{\mathrm{JB}}\mathbf{h}_{\mathrm{JB}}^{\dagger}$ such that $\mathbf{W}_{\mathrm{JE}}$ lies in the nullspace of $\mathbf{h}_{\mathrm{JB}}$, i.e., $\mathbf{h}_{\mathrm{JB}}\mathbf{W}_{\mathrm{JE}} = \mathbf{0}$. As such, $\mathbf{W}$ is a unitary matrix. In addition, since the cooperative jammer has no knowledge about $\mathbf{h}_{\mathrm{JE}}$, the jammer distributes the transmit power P_{J} uniformly across the $A_{\mathrm{J}} - 1$ transmit antennas. Building on this, we have the same instantaneous SNR of the legitimate channel as the ZFB scheme, and the corresponding instantaneous SINR of the eavesdropper's channel is given by

$$\gamma_{\mathrm{E}}^{(\ddagger)} = \frac{\frac{P_{\mathrm{A}}}{\sigma_{\mathrm{E}}^2}\left|h_{\alpha^*\mathrm{E}}\right|^2}{\frac{1}{A_{\mathrm{J}}-1}\frac{P_{\mathrm{J}}}{\sigma_{\mathrm{E}}^2}\left\|\mathbf{h}_{\mathrm{JE}}\mathbf{W}_{\mathrm{JE}}\right\|_F^2 + 1}. \tag{6}$$

For both cooperative jamming schemes, we further assume that the total transmit power adopted at the BS and CJ is constrained by P_{S}, i.e., $P_{\mathrm{A}} + P_{\mathrm{J}} = P_{\mathrm{S}}$. We define ϕ, $0 < \phi < 1$, as the power allocation scaling factor which denotes the fraction of the power allocation to the BS, such that $P_{\mathrm{A}} = \phi P_{\mathrm{S}}$ and $P_{\mathrm{J}} = (1-\phi)\, P_{\mathrm{S}}$. For notational convenience, we define the overall average transmit SNR as $\overline{\gamma}_{\mathrm{S}}{=}P_{\mathrm{S}}/\sigma_{\mathrm{B}}^2$, the average transmit SNR of A $\rightarrow$ B link, A $\rightarrow$ E link and J $\rightarrow$ E link as $\overline{\gamma}_{\mathrm{B}} = P_{\mathrm{A}}/\sigma_{\mathrm{B}}^2$, $\overline{\gamma}_{\mathrm{E}} = P_{\mathrm{A}}/\sigma_{\mathrm{E}}^2$ and $\overline{\gamma}_{\mathrm{J}} = P_{\mathrm{J}}/\sigma_{\mathrm{E}}^2$, respectively.

We also denote $\mathcal{M}_{\mathrm{BE}} = \overline{\gamma}_{\mathrm{B}}/\overline{\gamma}_{\mathrm{E}}$ as the ratio between the average SNR of A $\rightarrow$ B link and A $\rightarrow$ E link, i.e., the main-to-eavesdropper (MER) ratio. As such, we have $\overline{\gamma}_{\mathrm{B}}{=}\phi\overline{\gamma}_{\mathrm{S}}$, $\overline{\gamma}_{\mathrm{E}} = \overline{\gamma}_{\mathrm{B}}/\mathcal{M}_{\mathrm{BE}}$ and $\overline{\gamma}_{\mathrm{J}} = (1-\phi)\,\overline{\gamma}_{\mathrm{S}}/\mathcal{M}_{\mathrm{BE}}$.

We highlight that the proposed methods bring about several advantages that are of particular interest to WSNs. First, the exploitation of SSC scheduling among legitimate nodes help to avoid a large amount of CSI feedback, which, in turn, reduces the share of air-link resources. Second, the best antenna at the BS is optimal to the selected legitimate link but is equivalent to a random transmit antenna for the eavesdropper. Thus, the eavesdropper cannot achieve any transmit diversity from the best antenna. Third, the cooperative jamming schemes, i.e., the ZFB scheme and NAN scheme, are designed to increase the interference at the eavesdropper while avoiding interrupting the selected legitimate node, which provides a further safeguard for data transmission in WSNs. Building on these advantages, we clarify that our proposed schemes allow low-cost sensor nodes to fully explore the limited battery energy to support the core sensorial and computational operations, while guaranteeing the secure data transmission from the sensor nodes.

2.3. Achievable Secrecy Rate

Now, the achievable secrecy rate of the SSC based WSNs with TAS and cooperative jamming is provided by

$$\mathcal{C}_{\mathrm{s}} = \left[\mathcal{C}_{\mathrm{B}} - \mathcal{C}_{\mathrm{E}}\right]^{+} = \Big[\log\left(1+\gamma_{\mathrm{B}}\right) - \log\left(1+\gamma_{\mathrm{E}}\right)\Big]^{+}, \tag{7}$$

where $[u]^{+} = \max(u, 0)$, $\mathcal{C}_{\mathrm{B}} = \log\left(1+\gamma_{\mathrm{B}}\right)$ and $\mathcal{C}_{\mathrm{E}} = \log\left(1+\gamma_{\mathrm{E}}\right)$ represent the instantaneous capacity of the legitimate channel and eavesdropper's channel, respectively.

3. Secrecy Performance Analysis

In this section, we analyze the secrecy outage probability and the effective secrecy throughput as the main performance metrics to examine the secrecy performance of the considered network.

3.1. Preliminaries

Before proceeding, we first determine the statistic properties of the end-to-end instantaneous SNRs in the considered network. According to the basic principle of the SSC scheme and following the same steps developed in [35], the cumulative distribution function (CDF) for $\gamma_{\mathrm{B},\alpha}$ is provided by

$$\mathcal{F}_{\gamma_{\mathrm{B},\alpha}}(\gamma) = \begin{cases} \mathcal{F}_{\gamma^{\mathrm{b}}_{\alpha,k}}(\gamma_{\mathrm{T}})\,\mathcal{F}_{\gamma^{\mathrm{b}}_{\alpha,k}}(\gamma), & \gamma < \gamma_{\mathrm{T}}, \\ \mathcal{F}_{\gamma^{\mathrm{b}}_{\alpha,k}}(\gamma) + \mathcal{F}_{\gamma^{\mathrm{b}}_{\alpha,k}}(\gamma_{\mathrm{T}})\left[\mathcal{F}_{\gamma^{\mathrm{b}}_{\alpha,k}}(\gamma) - 1\right], & \gamma \geq \gamma_{\mathrm{T}}. \end{cases} \tag{8}$$

Moreover, according to the antenna selection at the BS, we define γ_{B} as the resulting instantaneous SNR of A $\rightarrow$ B link with $\gamma_{\mathrm{B}} = \max\left\{\gamma_{\mathrm{B},\alpha}\right\}, \alpha \in \{1, 2, ..., A_{\mathrm{A}}\}$. Considering that each legitimate channel is subject to independent and identical distribution (i.i.d.) Rayleigh fading, the CDF of γ_{B} is given by $\mathcal{F}_{\gamma_{\mathrm{B}}}(\gamma) = \left[\mathcal{F}_{\gamma_{\mathrm{B},\alpha}}(\gamma)\right]^{A_{\mathrm{A}}}$. Furthermore, with the assistance of binomial theorem [44] (Equation (1.111)), the CDF of γ_{B} can be re-expressed as

$$\mathcal{F}_{\gamma_{\mathrm{B}}}(\gamma) = \begin{cases} \left[\mathcal{F}_{\gamma^{\mathrm{b}}_{\alpha,k}}(\gamma_{\mathrm{T}})\right]^{A_{\mathrm{A}}}\left[\mathcal{F}_{\gamma^{\mathrm{b}}_{\alpha,k}}(\gamma)\right]^{A_{\mathrm{A}}}, & \gamma < \gamma_{\mathrm{T}}, \\ \sum\limits_{q=0}^{A_{\mathrm{A}}}\binom{A_{\mathrm{A}}}{q}\left[\mathcal{F}_{\gamma^{\mathrm{b}}_{\alpha,k}}(\gamma_{\mathrm{T}})\right]^{q}\sum\limits_{q_1=0}^{q}\binom{q}{q_1}(-1)^{q_1}\left[\mathcal{F}_{\gamma^{\mathrm{b}}_{\alpha,k}}(\gamma)\right]^{A_{\mathrm{A}}-q_1}, & \gamma \geq \gamma_{\mathrm{T}}, \end{cases} \tag{9}$$

where $\mathcal{F}_{\gamma^{\mathrm{b}}_{\alpha,k}}(\gamma) = 1 - \frac{\gamma}{\overline{\gamma}_{\mathrm{B}}}\exp\left(-\frac{\gamma}{\overline{\gamma}_{\mathrm{B}}}\right)$ denotes the CDF for end-to-end instantaneous SNR of each legitimate link.

On the other hand, according to Equation (5), the probability density function (PDF) of end-to-end instantaneous SNR γ_{E} with ZFB scheme can be expressed as

$$f^{(\dagger)}_{\gamma_{\mathrm{E}}}(x) = \frac{1}{\overline{\gamma}_{\mathrm{E}}}\left(1 + \frac{\overline{\gamma}_{\mathrm{J}}}{\overline{\gamma}_{\mathrm{E}}}x\right)^{-(A_{\mathrm{J}}-1)}\exp\left(-\frac{x}{\overline{\gamma}_{\mathrm{E}}}\right)\left[(A_{\mathrm{J}}-1)\,\overline{\gamma}_{\mathrm{J}}\left(1 + \frac{\overline{\gamma}_{\mathrm{J}}}{\overline{\gamma}_{\mathrm{E}}}x\right)^{-1} + 1\right]. \tag{10}$$

Similarly, based on Equation (6), the PDF of end-to-end instantaneous SNR γ_{E} with NAN scheme is given by

$$f^{(\ddagger)}_{\gamma_{\mathrm{E}}}(x) = \frac{1}{\overline{\gamma}_{\mathrm{E}}}\left(1 + \frac{\overline{\gamma}_{\mathrm{J}}}{\overline{\gamma}_{\mathrm{E}}}\frac{1}{A_{\mathrm{J}}-1}x\right)^{-(A_{\mathrm{J}}-1)}\exp\left(-\frac{x}{\overline{\gamma}_{\mathrm{E}}}\right)\left[\overline{\gamma}_{\mathrm{J}}\left(1 + \frac{\overline{\gamma}_{\mathrm{J}}}{\overline{\gamma}_{\mathrm{E}}}\frac{1}{A_{\mathrm{J}}-1}x\right)^{-1} + 1\right]. \tag{11}$$

Proof. The detailed derivation of Equation (10) can be found in [30] (Appendix D), and following the similar lines we have Equation (11). □

3.2. Secrecy Outage Probability

The definition of secrecy outage probability is the probability that the achievable secrecy rate falls down the predetermined secrecy rate R_{s} [30,38,41]. Mathematically, the secrecy outage probability can be formulated as

$$\mathcal{O}_{\mathrm{out}}(R_{\mathrm{s}}) = \Pr\left(\mathcal{C}_{\mathrm{s}} < R_{\mathrm{s}}\right). \tag{12}$$

Now, an exact closed-form expression for secrecy outage probability of the considered system is derived and expressed in the following theorem.

Theorem 1. *The secrecy outage probability of the SSC based WSNs with TAS and cooperative jamming is derived as*

$$\mathcal{O}_{\text{out}}^{(\kappa)}\left(R_{\text{s}}\right) = \begin{cases} \mathcal{O}_{\text{out}-\text{A}}^{(\kappa)}\left(R_{\text{s}}\right), & \Pi_{\gamma_{\text{T}}} \geq 0, \\ \mathcal{O}_{\text{out}-\text{B}}^{(\kappa)}\left(R_{\text{s}}\right), & \Pi_{\gamma_{\text{T}}} < 0, \end{cases} \tag{13}$$

where $\kappa \in \{\text{I}, \text{II}\}$ *with* I *and* II *stand for the TAS-SSC-ZFB scheme and the TAS-SSC-NAN scheme, respectively.* $\mathcal{O}_{\text{out}}^{(\text{I})}\left(R_{\text{s}}\right)$ *and* $\mathcal{O}_{\text{out}}^{(\text{II})}\left(R_{\text{s}}\right)$ *are provided by Equation (19) and Equation (20), as shown at the top of the next page, respectively.* $z = \frac{2^{R_{\text{s}}} q_2}{\overline{\gamma}_{\text{B}}} + \frac{1}{\overline{\gamma}_{\text{E}}}$, $E_1 = \exp\left(-\frac{2^{R_{\text{s}}}-1}{\overline{\gamma}_{\text{B}}}\right)$, *and* $\Pi_{\gamma_{\text{T}}} = 2^{-R_{\text{s}}}\left(1+\gamma_{\text{T}}\right) - 1$. $\Gamma\left(\alpha, \beta\right)$ *and* $\Psi\left(\mu, \upsilon; \tau\right)$ *denote the upper incomplete Gamma function [44] (Equation (8.350.2)) and confluent hypergeometric function of the second kind [44] (Equation (9.211.4)), respectively.*

Proof of Theorem 1. Based on the definition in Equation (12), we have

$$\mathcal{O}_{\text{out}}\left(R_{\text{s}}\right) = \underbrace{\Pr\left(\mathcal{C}_{\text{s}} < R_{\text{s}} | \gamma_{\text{B}} > \gamma_{\text{E}}\right) \Pr\left(\gamma_{\text{B}} > \gamma_{\text{E}}\right)}_{P_1} + \underbrace{\Pr\left(\gamma_{\text{B}} < \gamma_{\text{E}}\right)}_{P_2}, \tag{14}$$

where P_1 and P_2 are given by, respectively,

$$P_1 = \int_0^{\infty} \int_y^{2^{R_{\text{s}}}(1+y)-1} f_{\gamma_{\text{B}}}\left(x\right) f_{\gamma_{\text{E}}}\left(y\right) dxdy \tag{15}$$

and

$$P_2 = \int_0^{\infty} \int_0^{y} f_{\gamma_{\text{B}}}\left(x\right) f_{\gamma_{\text{E}}}\left(y\right) dxdy. \tag{16}$$

Now, inserting Equations (15) and (16) into Equation (14) for both schemes yields

$$\mathcal{O}_{\text{out}}\left(R_{\text{s}}\right) = \int_0^{\infty} \int_0^{2^{R_{\text{s}}}(1+y)-1} f_{\gamma_{\text{B}}}\left(x\right) f_{\gamma_{\text{E}}}\left(y\right) dxdy = \int_0^{\infty} \mathcal{F}_{\gamma_{\text{B}}}\left(2^{R_{\text{s}}}\left(1+y\right) - 1\right) f_{\gamma_{\text{E}}}\left(y\right) dy, \tag{17}$$

where $f_{\gamma_{\text{B}}}\left(x\right)$ is the PDF of γ_{B}. Owing to the fact that the switching threshold γ_{T} is exploited in the CDF of γ_{B} in Equation (8), we have the relationship between $2^{R_{\text{s}}}\left(1+y\right) - 1$ and γ_{T} in Equation (17), i.e., $2^{R_{\text{s}}}\left(1+y\right) - 1 \geq \gamma_{\text{T}}$ or $2^{R_{\text{s}}}\left(1+y\right) - 1 < \gamma_{\text{T}}$. For the simplicity of notation, we denote a boundary point by $\Pi_{\gamma_{\text{T}}} = 2^{-R_{\text{s}}}\left(1+\gamma_{\text{T}}\right) - 1$. To do so, the derivation of secrecy outage probability is separated into two parts regarding the bound point $\Pi_{\gamma_{\text{T}}}$. Thus, we have,

$$\mathcal{O}_{\text{out}}\left(R_{\text{s}}\right) = \begin{cases} \int_0^{\Pi_{\gamma_{\text{T}}}} \mathcal{F}_{\gamma_{\text{B}}}\left(\lambda_y\right) f_{\gamma_{\text{E}}}\left(y\right) dy + \int_{\Pi_{\gamma_{\text{T}}}}^{\infty} \mathcal{F}_{\gamma_{\text{B}}}\left(\lambda_y\right) f_{\gamma_{\text{E}}}\left(y\right) dy, & \Pi_{\gamma_{\text{T}}} \geq 0, \\ \int_0^{\infty} \mathcal{F}_{\gamma_{\text{B}}}\left(\lambda_y\right) f_{\gamma_{\text{E}}}\left(y\right) dy, & \Pi_{\gamma_{\text{T}}} < 0, \end{cases} \tag{18}$$

where $\lambda_y = 2^{R_{\text{s}}}\left(1+y\right) - 1$.

In the following, by substituting Equations (9) and (10) into Equation (18) and using [44] (Equations (1.111), (3.381.3), and (9.211.4)), the secrecy outage probability $\mathcal{O}_{\text{out}}\left(R_{\text{s}}\right)$ in Equation (18) is derived in Equation (19) for the TAS-SSC-ZFB scheme. Similarly, for the TAS-SSC-NAN scheme, $\mathcal{O}_{\text{out}}\left(R_{\text{s}}\right)$ is presented in Equation (20). □

We remark that our new derived expressions in Equations (19) and (20) are ready to compute because the involved functions are merely the easy-to-calculate exponential functions, power functions, upper incomplete Gamma functions and confluent hypergeometric functions. As such, the optimal performance and optimal parameters of the considered network are achieved with convenience.

We further highlight that the derived theoretical results in Equations (19) and (20) are valid for general WSNs with an arbitrary number of antennas at the BS and cooperative jammer, arbitrary number of legitimate users, arbitrary average SNRs and switching threshold.

$$\begin{aligned}\mathcal{O}_{\text{out}-\text{A}}^{(\text{I})}(R_\text{s}) &= [F_\gamma(\gamma_\text{T})]^{A_\text{A}} \sum_{q=0}^{A_\text{A}} \binom{A_\text{A}}{q} (-1)^q (E_1)^q \frac{\exp\left(\frac{\overline{\gamma}_\text{E} z}{\overline{\gamma}_\text{J}}\right)}{\overline{\gamma}_\text{J}} \left(\frac{\overline{\gamma}_\text{E} z}{\overline{\gamma}_\text{J}}\right)^{A_\text{J}-1} \left\{(A_\text{J}-1)\overline{\gamma}_\text{J}\left[\Gamma\left(1-A_\text{J}, \frac{\overline{\gamma}_\text{E} z}{\overline{\gamma}_\text{J}}\right)\right.\right. \\ &\left.\left. -\Gamma\left(1-A_\text{J}, \frac{\overline{\gamma}_\text{E} z}{\overline{\gamma}_\text{J}} + z\Pi_{\gamma_\text{T}}\right)\right] + \left(\frac{\overline{\gamma}_\text{E} z}{\overline{\gamma}_\text{J}}\right)^{-1}\left[\Gamma\left(2-A_\text{J}, \frac{\overline{\gamma}_\text{E} z}{\overline{\gamma}_\text{J}}\right) - \Gamma\left(2-A_\text{J}, \frac{\overline{\gamma}_\text{E} z}{\overline{\gamma}_\text{J}} + z\Pi_{\gamma_\text{T}}\right)\right]\right\} \\ &+ \sum_{q=0}^{A_\text{A}} \binom{A_\text{A}}{q} [F_\gamma(\gamma_\text{T})]^q \sum_{q_1=0}^{q} \binom{q}{q_1} (-1)^{q_1} \sum_{q_2=0}^{A_\text{A}-q_1} \binom{A_\text{A}-q_1}{q_2} (-1)^{q_2} (E_1)^{q_2} \frac{\exp\left(\frac{\overline{\gamma}_\text{E} z}{\overline{\gamma}_\text{J}}\right)}{\overline{\gamma}_\text{J}} \left(\frac{\overline{\gamma}_\text{E} z}{\overline{\gamma}_\text{J}}\right)^{A_\text{J}-1} \\ &\times \left[(A_\text{J}-1)\overline{\gamma}_\text{J}\Gamma\left(1-A_\text{J}, \frac{\overline{\gamma}_\text{E} z}{\overline{\gamma}_\text{J}} + z\Pi_{\gamma_\text{T}}\right) + \left(\frac{\overline{\gamma}_\text{E} z}{\overline{\gamma}_\text{J}}\right)^{-1}\Gamma\left(2-A_\text{J}, \frac{\overline{\gamma}_\text{E} z}{\overline{\gamma}_\text{J}} + z\Pi_{\gamma_\text{T}}\right)\right],\end{aligned} \tag{19a}$$

$$\begin{aligned}\mathcal{O}_{\text{out}-\text{B}}^{(\text{I})}(R_\text{s}) &= \sum_{q=0}^{A_\text{A}} \binom{A_\text{A}}{q} [F_\gamma(\gamma_\text{T})]^q \sum_{q_1=0}^{q} \binom{q}{q_1} (-1)^{q_1} \sum_{q_2=0}^{A_\text{A}-q_1} \binom{A_\text{A}-q_1}{q_2} (-1)^{q_2} (E_1)^{q_2} \\ &\times \left[(A_\text{J}-1)\Psi\left(1, 2-A_\text{J}; \frac{\overline{\gamma}_\text{E}}{\overline{\gamma}_\text{J}} z\right) + (\overline{\gamma}_\text{J})^{-1}\Psi\left(1, 3-A_\text{J}; \frac{\overline{\gamma}_\text{E}}{\overline{\gamma}_\text{J}} z\right)\right],\end{aligned} \tag{19b}$$

$$\begin{aligned}\mathcal{O}_{\text{out}-\text{A}}^{(\text{II})}(R_\text{s}) &= [F_\gamma(\gamma_\text{T})]^{A_\text{A}} \sum_{q=0}^{A_\text{A}} \binom{A_\text{A}}{q} (-1)^q (E_1)^q \frac{(A_\text{J}-1)}{\overline{\gamma}_\text{J}} \exp\left(\frac{(A_\text{J}-1)\overline{\gamma}_\text{E} z}{\overline{\gamma}_\text{J}}\right) \left(\frac{(A_\text{J}-1)\overline{\gamma}_\text{E} z}{\overline{\gamma}_\text{J}}\right)^{A_\text{J}-1} \\ &\times \left\{\overline{\gamma}_\text{J}\left[\Gamma\left(1-A_\text{J}, \frac{(A_\text{J}-1)\overline{\gamma}_\text{E} z}{\overline{\gamma}_\text{J}}\right) - \Gamma\left(1-A_\text{J}, \frac{(A_\text{J}-1)\overline{\gamma}_\text{E} z}{\overline{\gamma}_\text{J}} + z\Pi_{\gamma_\text{T}}\right)\right] + \left(\frac{(A_\text{J}-1)\overline{\gamma}_\text{E} z}{\overline{\gamma}_\text{J}}\right)^{-1}\right. \\ &\left.\times\left[\Gamma\left(2-A_\text{J}, \frac{(A_\text{J}-1)\overline{\gamma}_\text{E} z}{\overline{\gamma}_\text{J}}\right) - \Gamma\left(2-A_\text{J}, \frac{(A_\text{J}-1)\overline{\gamma}_\text{E} z}{\overline{\gamma}_\text{J}} + z\Pi_{\gamma_\text{T}}\right)\right]\right\} + \sum_{q=0}^{A_\text{A}} \binom{A_\text{A}}{q} [F_\gamma(\gamma_\text{T})]^q \\ &\times \sum_{q_1=0}^{q} \binom{q}{q_1} (-1)^{q_1} \sum_{q_2=0}^{A_\text{A}-q_1} \binom{A_\text{A}-q_1}{q_2} (-1)^{q_2} (E_1)^{q_2} \frac{(A_\text{J}-1)}{\overline{\gamma}_\text{J}} \exp\left(\frac{(A_\text{J}-1)\overline{\gamma}_\text{E} z}{\overline{\gamma}_\text{J}}\right) \left(\frac{(A_\text{J}-1)\overline{\gamma}_\text{E} z}{\overline{\gamma}_\text{J}}\right)^{A_\text{J}-1} \\ &\times \left[\overline{\gamma}_\text{J}\Gamma\left(1-A_\text{J}, \frac{(A_\text{J}-1)\overline{\gamma}_\text{E} z}{\overline{\gamma}_\text{J}} + z\Pi_{\gamma_\text{T}}\right) + \left(\frac{(A_\text{J}-1)\overline{\gamma}_\text{E} z}{\overline{\gamma}_\text{J}}\right)^{-1}\Gamma\left(2-A_\text{J}, \frac{(A_\text{J}-1)\overline{\gamma}_\text{E} z}{\overline{\gamma}_\text{J}} + z\Pi_{\gamma_\text{T}}\right)\right],\end{aligned} \tag{20a}$$

$$\begin{aligned}\mathcal{O}_{\text{out}-\text{B}}^{(\text{II})}(R_\text{s}) &= \sum_{q=0}^{A_\text{A}} \binom{A_\text{A}}{q} [F_\gamma(\gamma_\text{T})]^q \sum_{q_1=0}^{q} \binom{q}{q_1} (-1)^{q_1} \sum_{q_2=0}^{A_\text{A}-q_1} \binom{A_\text{A}-q_1}{q_2} (-1)^{q_2} (E_1)^{q_2} \\ &\times (A_\text{J}-1)\left[\Psi\left(1, 2-A_\text{J}; \frac{\overline{\gamma}_\text{E} z\,(A_\text{J}-1)}{\overline{\gamma}_\text{J}}\right) + (\overline{\gamma}_\text{J})^{-1}\Psi\left(1, 3-A_\text{J}; \frac{\overline{\gamma}_\text{E} z\,(A_\text{J}-1)}{\overline{\gamma}_\text{J}}\right)\right].\end{aligned} \tag{20b}$$

3.3. Effective Secrecy Throughput

Before proceeding, we first present the definition of the secrecy transmission probability as the probability that the messages are confidentially conveyed from the BS to the legitimate user without leaking to the eavesdropper. Thus, according to [15] (Equation (8)), we have,

$$\mathcal{P}_\text{sec}^{(\kappa)}(R_\text{s}) = 1 - \mathcal{O}_\text{out}^{(\kappa)}(R_\text{s}). \tag{21}$$

From Equation (21), it is found that the effective secrecy throughput can be characterized as the product of the secure transmission probability and secrecy rate R_s, which evaluates the average

rate of the messages that are transmitted from the BS to the legitimate user confidentially in the passive wiretapping scenario [14,15]. We now present the effective secrecy throughput in the following theorem.

Theorem 2. *The effective secrecy throughput of the SSC based WSNs with TAS and cooperative jamming is derived as*

$$\mathcal{S}_{\mathrm{T}}^{(\kappa)}\left(R_{\mathrm{s}}\right)=\begin{cases}\left(1-\mathcal{O}_{\mathrm{out-A}}^{(\kappa)}\left(R_{\mathrm{s}}\right)\right)R_{\mathrm{s}}, & \Pi_{\gamma_{\mathrm{T}}}\geq 0,\\ \left(1-\mathcal{O}_{\mathrm{out-B}}^{(\kappa)}\left(R_{\mathrm{s}}\right)\right)R_{\mathrm{s}}, & \Pi_{\gamma_{\mathrm{T}}}<0,\end{cases} \tag{22}$$

where $\kappa\in\{\mathrm{I},\mathrm{II}\}$ *with* I *and* II *represent the TAS-SSC-ZFB scheme and the TAS-SSC-NAN scheme, respectively.*

Proof of Theorem 2. By substituting Equations (19) and (20) into Equation (22), the exact closed-form expressions for the effective secrecy throughput of the considered WSNs can be obtained. □

4. Simulations and Discussions

In this section, we perform the simulations with MATLAB R2014a 64-bit version (The MathWorks, Inc., Natick, MA, USA) running on a Windows 7 64-bit system (Microsoft, Redmond, Washington D.C., USA). Monte Carlo simulation results of the proposed TAS-SSC-ZFB and TAS-SSC-NAN schemes are presented to validate the conducted analysis and illustrate the joint impact of the key system parameters on the secrecy performance of the considered network.

Figure 2 illustrates the secrecy outage probability versus overall average transmit SNR $\overline{\gamma}_{\mathrm{S}}$ of the considered system with equal power allocation for both schemes. It can be readily observed that the theoretical analyses in Theorem 1 are in exact agreement with the Monte Carlo simulations, which demonstrates the correctness of our derived results. Moreover, we observe that the TAS-SSC-ZFB scheme outperforms the TAS-SSC-NAN scheme, which can be explained by the fact that the TAS-SSC-ZFB scheme benefits from the CSIs of both J $\rightarrow$ B channel and J $\rightarrow$ E channel while the TAS-SSC-NAN scheme merely relies on the knowledge of the J $\rightarrow$ B channel. In addition, as expected, increasing the number of transmit antennas brings about a significant secrecy performance improvement while enhancing the secrecy rate results in larger secrecy outage probability.

Figure 3 examines the secrecy outage probability versus different antenna configurations at the cooperative jammer. Interestingly, we first see that the TAS-SSC-ZFB scheme degrades into the TAS-SSC-NAN scheme when the number of antennas at the jammer is equal to two. Such an observation is explained by the fact that the PDF of γ_{E} for the TAS-SSC-ZFB scheme is equivalent to that for the TAS-SSC-NAN scheme when $A_{\mathrm{J}}=2$. Next, we find that the secrecy performance comes to a floor for both schemes when the number of antennas grows large. Notably, the secrecy outage floors can be further improved by increasing the number of antennas at the BS or decreasing the predetermined secrecy rate. Finally, we find that the secrecy performance is independent of the number of legitimate users in the networks. This is demonstrated by the observation that $\mathcal{O}_{\mathrm{out}}\left(R_{\mathrm{s}}\right)$ stays the same when $N_{\mathrm{B}}=2$ increases to $N_{\mathrm{B}}=4$ with $A_{\mathrm{A}}=2, R_{\mathrm{s}}=1$ setup for both schemes.

Figure 4 depicts the secrecy outage probability versus different switching threshold γ_{T} for the given equal power allocation. Firstly, we find that there exists an optimal switching threshold γ_{T}^{*} for both schemes, which accounts for the SSC scheduling being employed in the networks and being independent of the way that the cooperative jammer operates. Regarding the antenna configuration of the cooperative jammer, it can be observed that increasing the number of antennas has a positive impact on the secrecy performance and the minimum $\mathcal{O}_{\mathrm{out}}\left(R_{\mathrm{s}}\right)$ shifts to the left. In addition, we see that the secrecy outage probability degrades when $\overline{\gamma}_{\mathrm{E}}$ increases and the optimal γ_{T}^{*} shifts to right. For instance, γ_{T}^{*} increases from 10.9 dB for $\mathcal{M}_{\mathrm{BE}}$=10 to 11.7 dB for $\mathcal{M}_{\mathrm{BE}}$=5 concerning the TAS-SSC-ZFB scheme when $A_{\mathrm{J}}=3$, and increases from 11.6 dB for $\mathcal{M}_{\mathrm{BE}}$=10 to 12.45 dB for $\mathcal{M}_{\mathrm{BE}}$=5 concerning the

TAS-SSC-NAN scheme when $A_{\mathrm{J}} = 3$. This reveals that a larger switching threshold setup is required to obtain the minimum $\mathcal{O}_{\mathrm{out}}(R_{\mathrm{s}})$ for larger $\overline{\gamma}_{\mathrm{E}}$.

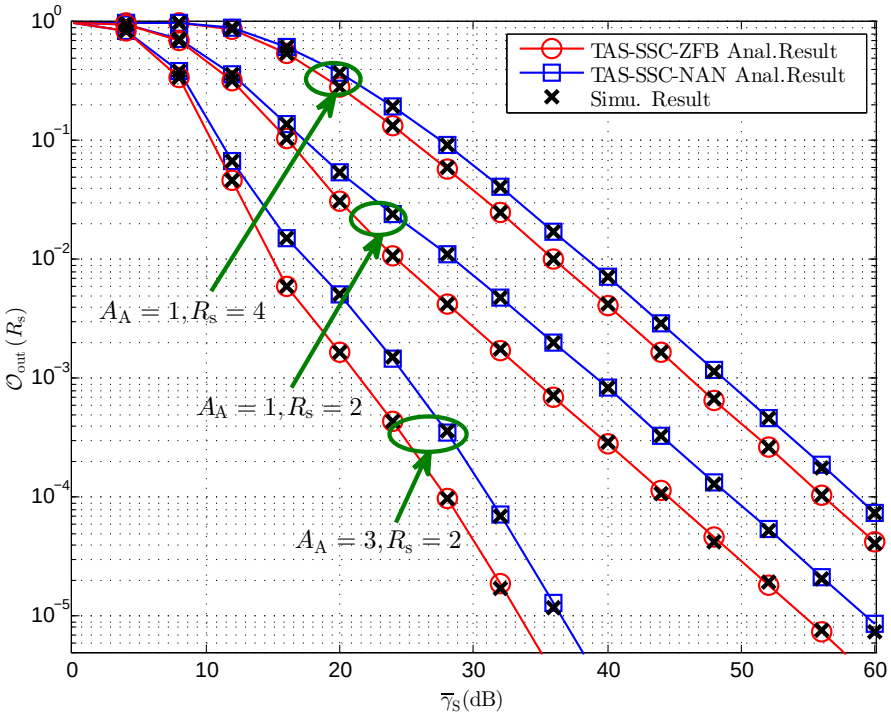

Figure 2. Secrecy outage probability versus different $\overline{\gamma}_{\mathrm{S}}$ for $A_{\mathrm{J}} = 3$, $N_{\mathrm{B}} = 2, \gamma_{\mathrm{T}} = 10$ dB, $\mathcal{M}_{\mathrm{BE}} = 5$, and $\phi = 0.5$.

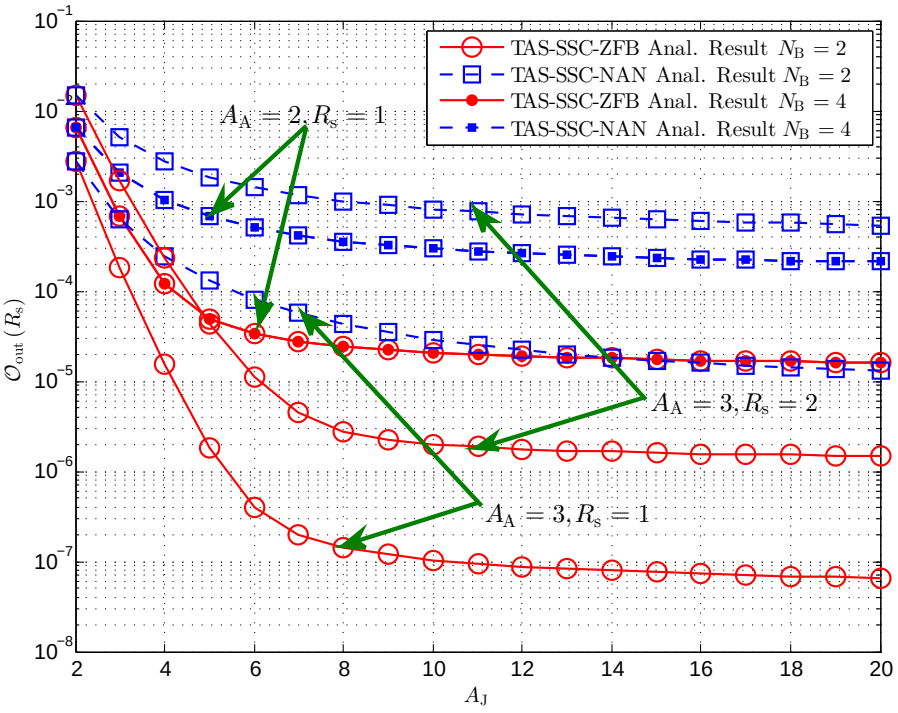

Figure 3. Secrecy outage probability versus different A_{J} for $\gamma_{\mathrm{T}} = 10$ dB, $\mathcal{M}_{\mathrm{BE}} = 5$, $\overline{\gamma}_{\mathrm{S}} = 20$ dBW, and $\phi = 0.5$.

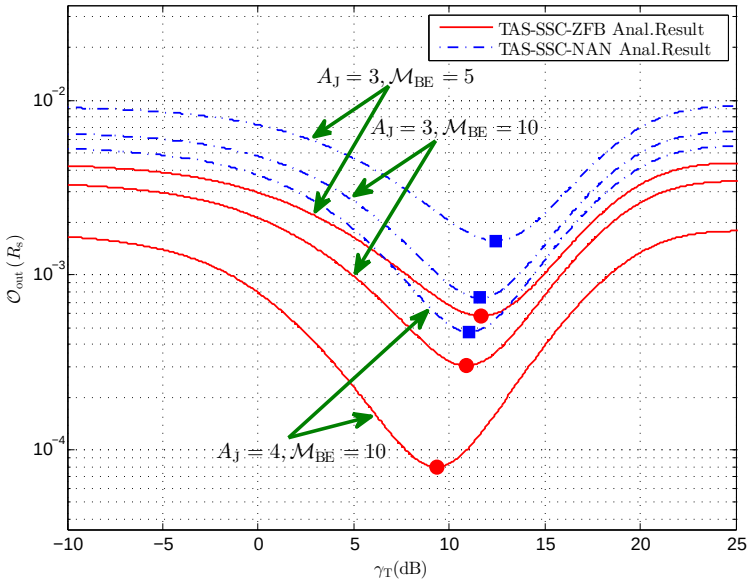

Figure 4. Secrecy outage probability versus different γ_T for $A_A = 2$, $N_B = 2$, $R_s = 1$, $\overline{\gamma}_S = 20$ dB, and $\phi = 0.5$.

Figure 5 shows the secrecy outage probability versus different power allocation between the BS and the cooperative jammer. Considering a given switching threshold, we can see that an optimal power allocation factor ϕ^* is found for both schemes. Specifically, the optimal factor ϕ^* shifts to the right when the number of antennas at the cooperative jammer increases (e.g., $A_J = 2, \mathcal{M}_{BE} = 5$ and $A_J = 3, \mathcal{M}_{BE} = 5$). This reveals that less power is allocated at the cooperative jammer since this antenna configuration improves the capabilities of jamming. Once again, we can see that the TAS-SSC-ZFB scheme and the TAS-SSC-NAN scheme yield the same secrecy performance when the cooperative jammer is equipped with only two antennas. Furthermore, the optimal ϕ^* shifts to the left for both schemes when $\overline{\gamma}_E$ increases. This indicates that more power is necessary to be allocated for the jamming signal to achieve the minimum $\mathcal{O}_{out}(R_s)$ in view of higher $\overline{\gamma}_E$.

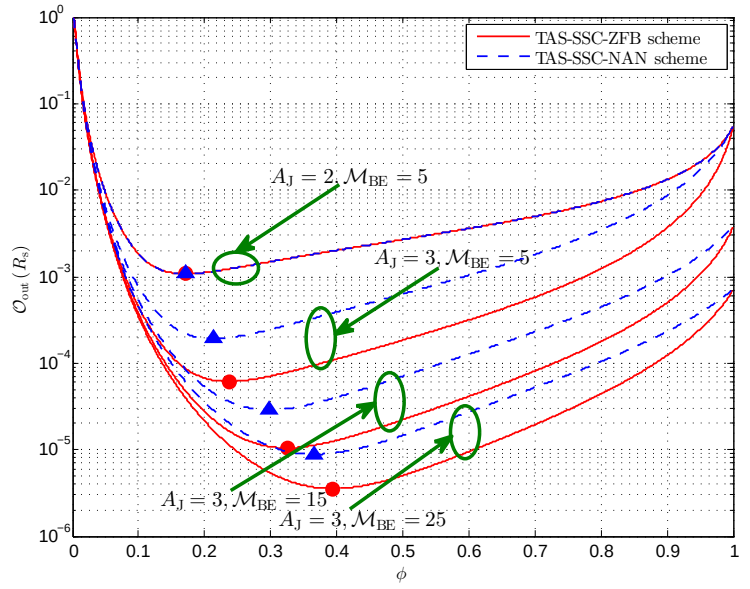

Figure 5. Secrecy outage probability versus different ϕ for $\gamma_T = 10$ dB, $A_A = 3, N_B = 2, R_s = 1$, and $\overline{\gamma}_S = 20$ dB.

Figure 6 plots the effective secrecy throughput versus different secrecy rates for a given switching threshold and power allocation factor. In this figure, it is found that $\mathcal{S}_{\mathrm{T}}$ first increases and then decreases as R_{s} increases, which demonstrates that there exists an optimal R_{s}^{*} point to achieve the largest effective secrecy throughput. To begin with, we concentrate on the impact of the number of transmit antenna elements A_{A} and the total transmit power $\overline{\gamma}_{\mathrm{S}}$. We readily observe that a larger effective secrecy throughput is obtained while either A_{A} or $\overline{\gamma}_{\mathrm{S}}$ increases. Moreover, it can be seen that the TAS-SSC-ZFB scheme slightly outperforms the TAS-SSC-NAN scheme in the medium to high regime of R_{s}. Furthermore, the optimal R_{s}^{*} shifts to the right while considering that either A_{A} or $\overline{\gamma}_{\mathrm{S}}$ improves. For instance, considering the cases $A_{\mathrm{A}}=2, \overline{\gamma}_{\mathrm{S}}=20$ dBW and $A_{\mathrm{A}}=2, \overline{\gamma}_{\mathrm{S}}=25$ dBW, we see that increasing $\overline{\gamma}_{\mathrm{S}}$ from 20 dBW to 25 dBW leads to enhancement of R_{s}^{*} from 4.1 to 5.3 for the TAS-SSC-NAN scheme as well as from 4.3 to 5.6 for the TAS-SSC-ZFB scheme. Likewise, considering the cases $A_{\mathrm{A}}=2, \overline{\gamma}_{\mathrm{S}}=25$ dBW and $A_{\mathrm{A}}=4, \overline{\gamma}_{\mathrm{S}}=25$ dBW, we find that increasing A_{A} from 2 to 4 increases R_{s}^{*} from 5.3 to 5.8 for the TAS-SSC-NAN scheme as well as from 5.6 to 6.2 for the TAS-SSC-ZFB scheme. These observations indicate that the BS supports a larger secrecy rate for higher A_{A} and $\overline{\gamma}_{\mathrm{S}}$.

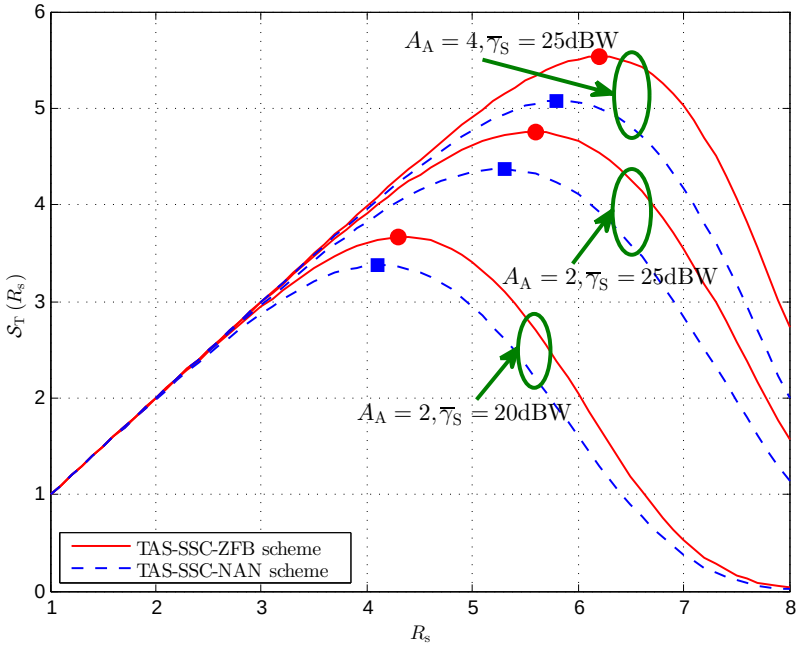

Figure 6. Effective secrecy throughput versus different R_{s} for $A_{\mathrm{J}}=3$, $\gamma_{\mathrm{T}}=10$ dB, $N_{\mathrm{B}}=2$, $\overline{\gamma}_{\mathrm{B}}/\overline{\gamma}_{\mathrm{E}}=10$, and $\phi=0.5$.

We now focus on the impact of the number of antenna elements at the jammer A_{J} or the average SNR of legitimate channel $\overline{\gamma}_{\mathrm{E}}$. As can be obviously revealed from Figure 7, decreasing A_{J} or increasing $\overline{\gamma}_{\mathrm{E}}$ results in a reduction in the effective secrecy throughput. Moreover, we find that R_{s}^{*} shifts to the left when A_{J} decreases or $\overline{\gamma}_{\mathrm{E}}$ increases. Considering the cases $A_{\mathrm{J}}=2, \mathcal{M}_{\mathrm{BE}}=10$ and $A_{\mathrm{J}}=3, \mathcal{M}_{\mathrm{BE}}=10$, it can be seen that reducing A_{J} from 3 to 2 decreases R_{s}^{*} from 4.4 to 4.3 for the TAS-SSC-NAN scheme and from 4.7 to 4.3 for the TAS-SSC-ZFB scheme. Similarly, comparing the cases of $A_{\mathrm{J}}=3, \mathcal{M}_{\mathrm{BE}}=10$ and the case of $A_{\mathrm{J}}=3, \mathcal{M}_{\mathrm{BE}}=25$, it can be found that increasing $\overline{\gamma}_{\mathrm{E}}$ from $\overline{\gamma}_{\mathrm{B}}/25$ to $\overline{\gamma}_{\mathrm{B}}/10$ decreases R_{s}^{*} from 4.6 to 4.4 for the TAS-SSC-NAN scheme and from 4.8 to 4.7 for the TAS-SSC-ZFB scheme. These observations indicate that the BS supports a lower secrecy rate for higher $\overline{\gamma}_{\mathrm{E}}$ and smaller A_{J}.

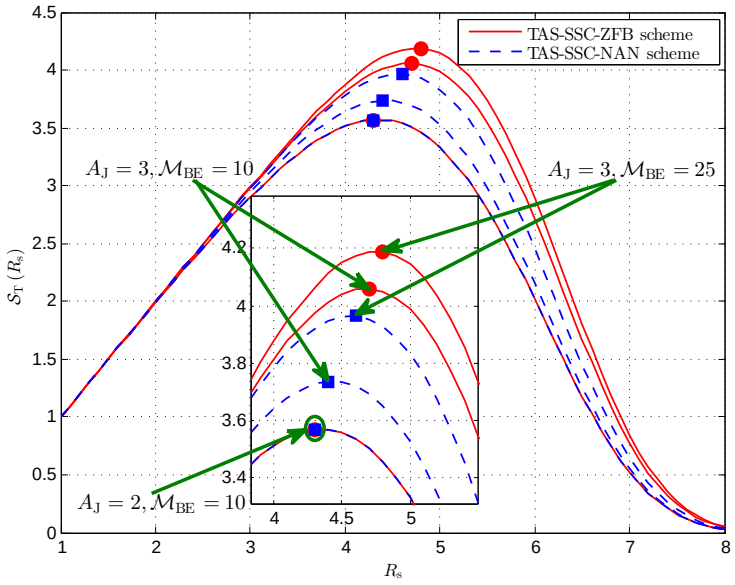

Figure 7. Effective secrecy throughput versus different R_s for $A_A = 3$, $\gamma_T = 10$ dB, $N_B = 2$, $\overline{\gamma}_S = 20$ dBW, and $\phi = 0.5$.

5. Conclusions

In this paper, we designed the secure transmission in the SSC based WSNs with TAS and cooperative jamming. Specifically, the TAS scheme was adopted at the BS, and the ZFB scheme as well as the NAN scheme were, respectively, explored at the cooperative jammer to further improve the security of the considered network. In doing so, we derived the novel exact closed-form expressions for the secrecy outage probability and the effective secrecy throughput to evaluate the secrecy performance achieved by both schemes. Additionally, numerical results were presented to validate the analysis of the proposed schemes and provide insights into the impact of key system parameters on the secrecy performance. Finally, it was revealed that the TAS-SSC-ZFB scheme outperforms the TAS-SSC-NAN scheme in terms of the secrecy outage probability and the effective secrecy throughput, while the TAS-SSC-NAN scheme is more robust than the TAS-SSC-ZFB scheme.

Acknowledgments: This work was supported by the National Science Foundation of China (No. 61501507), and the Jiangsu Provincial Natural Science Foundation of China (No. BK20150719). The work of Nan Yang is supported by the Australian Research Council Discovery Project (DP150103905). The authors would like to extend their gratitude to the anonymous reviewers for their valuable and constructive comments, which have largely improved and clarified this paper.

Author Contributions: Maoqiang Yang, Bangning Zhang and Yuzhen Huang conceived of the main proposal of TAS-SSC-ZFB and TAS-SSC-NAN schemes, conducted system modeling, and derived analysis and numerical simulation of the proposed schemes. Maoqiang Yang and Daoxing Guo wrote the manuscript. Nan Yang, Yuzhen Huang, and Bin Gao provided considerable comments and technique review of the proposed scheme and contributed to the revision of the paper. Bangning Zhang and Daoxing Guo read and approved the final manuscript.

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

References

1. Deng, Y.; Wang, L.; Elkashlan, M.; Nallanathan, A.; Mallik, R.K. Physical layer security in three-tier wireless sensor networks: A stochastic geometry approach. *IEEE Trans. Inf. Forensics Secur.* **2016**, *11*, 1128–1138.
2. Gope, P.; Hwang, T. A realistic lightweight anonymous authentication protocol for securing real-time application data access in wireless sensor networks. *IEEE Trans. Ind. Electron.* **2016**, *63*, 7124–7132.
3. Sun, L.; Ren, P.; Du, Q.; Wang, Y. Fountain-coding aided strategy for secure cooperative transmission in industrial wireless sensor networks. *IEEE Trans. Ind. Inform.* **2016**, *12*, 291–300.

4. Liau, Q.Y.; Leow, C.Y.; Ding, Z. Physical layer security using two-path successive relaying. *Sensors* **2016**, *16*, 846.
5. Mehmood, A.; Song, H.; Lloret, J. In Multi-agent based framework for secure and reliable communication among open clouds, Network Protocols and Algorithms. *Macrothink Inst.* **2014**, *6*, 60–76.
6. Butun, I.; Erol-Kantarci, M.; Kantarci, B.; Song, H. Cloud-centric multi-level authentication as a service for secure public safety device networks. *IEEE Commun. Mag.* **2016**, *54*, 47–53.
7. Trappe, W. The challenges facing physical layer security. *IEEE Commun. Mag.* **2015**, *53*, 16–20.
8. Xu, Q.; Ren, P.; Song, H.; Du, Q. Security enhancement for IoT communications exposed to eavesdroppers with uncertain locations. *IEEE Access* **2016**, *4*, 2840–2853.
9. Curiac, D.I. Wireless sensor network security enhancement using directional antennas: State of the art and research challenges. *Sensors* **2016**, *16*, 488.
10. Song, H.; Rawat, D.B.; Jeschke, S.; Brecher, C. *Cyber-Physical Systems: Foundations, Principles and Applications*, 1st ed.; Elsevier/Academic Press: Boston, MA, USA, 2016.
11. Sheng, G.; Wang, Y.; Lv, Z.; Song, H. Multiple-antenna systems and multiuser communications: Fundamentals and an overview of software-based modeling techniques. *Comput. Electr. Eng.* **2016**, doi:10.1016/j.compeleceng.2016.08.015.
12. Xu, D.; Ren, P.; Sun, L.; Song, H. Precoder-and-receiver design scheme for multi-user coordinated multi-point in LTE-A and fifth generation systems. *IET Commun.* **2016**, *10*, 292–299.
13. 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.
14. 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.
15. Yang, N.; Elkashlan, M.; Duong, T.Q.; Yuan, J.; Malaney, R. Optimal transmission with artificial noise in MISOME wiretap channels. *IEEE Trans. Veh. Technol.* **2016**, *65*, 2170–2181.
16. Yang, N.; Yeoh, P.L.; Elkashlan, M.; Schober, R.; Collings, I.B. Transmit antenna selection for security enhancement in MIMO wiretap channels. *IEEE Trans. Commun.* **2013**, *61*, 144–154.
17. Yan, S.; Yang, N.; Malaney, R.; Yuan, J. Transmit antenna selection with Alamouti coding and power allocation in MIMO wiretap channels. *IEEE Trans. Wirel. Commun.* **2014**, *13*, 1656–1667.
18. Huang, Y.; Al-Qahtani, F.; Duong, T.; Wang, J.; Xiao, C. Secure transmission in spectrum sharing MIMO channels with generalized antenna selection over Nakagami-*m* channels. *IEEE Access* **2016**, *4*, 4058–4065.
19. Zhu, J.; Zou, Y.; Wang, G.; Yao, Y.D.; Karagiannidis, G.K. On secrecy performance of antenna-selection-aided MIMO systems against eavesdropping. *IEEE Trans. Veh. Technol.* **2016**, *65*, 214–225.
20. Yeoh, P.L.; Elkashlan, M.; Kim, K.J.; Duong, T.Q.; Karagiannidis, G.K. Transmit antenna selection in cognitive MIMO relaying with multiple primary transceivers. *IEEE Trans. Veh. Technol.* **2016**, *65*, 483–489.
21. Pan, G.; Lei, H.; Deng, Y.; Fan, L.; Yang, J.; Chen, Y.; Ding, Z. On secrecy performance of MISO SWIPT systems with TAS and imperfect CSI. *IEEE Trans. Commun.* **2016**, *64*, 3831–3843.
22. Park, K.H.; Wang, T.; Alouini, M.S. On the jamming power allocation for secure amplify-and-forward relaying via cooperative jamming. *IEEE J. Sel. Areas Commun.* **2013**, *31*, 1741–1750.
23. Xiong, J.; Cheng, L.; Ma, D.; Wei, J. Destination aided cooperative jamming for dual-hop amplify-and-forward MIMO untrusted relay systems. *IEEE Trans. Veh. Technol.* **2016**, *65*, 7274–7284.
24. Chen, X.; Chen, J.; Zhang, H.; Zhang, Y.; Yuen, C. On secrecy performance of a multi-antenna jammer aided secure communications with imperfect CSI. *IEEE Trans. Veh. Technol.* **2016**, *65*, 8014–8024.
25. Hao, D.; Hui-Ming, W.; Wei, G.; Wenjie, W. Secrecy transmission with a helper: To relay or to jam. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 293–307.
26. Zheng, C.; Cumanan, K.; Ding, Z.; Johnston, M.; Le Goff, S.Y. Secrecy rate optimizations for a MIMO secrecy channel with a cooperative jammer. *IEEE Trans. Veh. Technol.* **2015**, *64*, 1833–1847.
27. Zhao, R.; Huang, Y.; Wang, W.; Lau, V.K.N. Ergodic achievable secrecy rate of multiple-antenna relay systems with cooperative jamming. *IEEE Trans. Wirel. Commun.* **2016**, *15*, 2537–2551.
28. Li, Z.; Jing, T.; Ma, L.; Huo, Y.; Qian, J. Worst-case cooperative jamming for secure communications in CIOT networks. *Sensors* **2016**, *16*, 339.
29. Zhang, T.; Huang, Y.; Cai, Y.; Yang, W. Secure transmission in spectrum sharing relaying networks with multiple antennas. *IEEE Commun. Lett.* **2016**, *20*, 824–827.

30. Huang, Y.; Wang, J.; Zhong, C.; Duong, T.Q.; Karagiannidis, G.K. Secure transmission in cooperative relaying networks with multiple antennas. *IEEE Trans. Wirel. Commun.* **2016**, *15*, 6843–6856.
31. Shaqfeh, M.; Alnuweiri, H.; Alouini, M.S. Multiuser switched diversity scheduling schemes. *IEEE Trans. Commun.* **2012**, *60*, 2499–2510.
32. Holter, B.; Alouini, M.S.; Oien, G.E.; Hong-Chuan, Y. Multiuser switched diversity transmission. In Proceedings of the IEEE Vehicular Technology Conference, Los Angeles, CA, USA, 26–29 September 2004; pp. 2038–2043.
33. Yang, M.; Guo, D.; Huang, Y.; Duong, T.Q.; Zhang, B. Physical layer security with threshold-based multiuser scheduling in multi-antenna wireless networks. *IEEE Trans. Commun.* **2016**, doi:10.1109/TCOMM.2016.2606396.
34. Yang, M.; Guo, D.; Huang, Y.; Duong, T.Q.; Zhang, B. Secure multiuser scheduling in downlink dual-hop regenerative relay networks over Nakagami-*m* fading channels. *IEEE Trans. Wirel. Commun.* **2016**, doi:10.1109/TWC.2016.2610965.
35. Hong-Chuan, Y.; Alouini, M.S. Performance analysis of multibranch switched diversity systems. *IEEE Trans. Commun.* **2003**, *51*, 782–794.
36. Al-Qahtani, F.S.; Zhong, C.; Alnuweiri, H.M. Opportunistic relay selection for secrecy enhancement in cooperative networks. *IEEE Trans. Commun.* **2015**, *63*, 1756–1770.
37. Fan, L.; Zhang, S.; Duong, T.Q.; Karagiannidis, G.K. Secure switch-and-stay combining (SSSC) for cognitive relay networks. *IEEE Trans. Commun.* **2016**, *64*, 70–82.
38. Bloch, M.; Barros, J.; Rodrigues, M.R.D.; McLaughlin, S.W. Wireless information-theoretic security. *IEEE Trans. Inf. Theory* **2008**, *54*, 2515–2534.
39. Zou, Y.; Wang, X.; Shen, W. Optimal relay selection for physical-layer security in cooperative wireless networks. *IEEE J. Sel. Areas Commun.* **2013**, *31*, 2099–2111.
40. Wang, L.; Kim, K.J.; Duong, T.Q.; Elkashlan, M.; Poor, H.V. Security enhancement of cooperative single carrier systems. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 90–103.
41. Hoang, T.M.; Duong, T.Q.; Suraweera, H.A.; Tellambura, C.; Poor, H.V. Cooperative beamforming and user selection for improving the security of relay-aided systems. *IEEE Trans. Commun.* **2016**, *63*, 5039–5051.
42. Yang, M.; Zhang, B.; Huang, Y.; Guo, D.; Yi, X. Ergodic secrecy capacity for downlink multiuser networks using switch-and-examine combining with post-selection scheduling scheme. *IET Electron. Lett.* **2016**, *52*, 720–722.
43. Ding, Z.; Leung, K.K.; Goeckel, D.L.; Towsley, D. On the application of cooperative transmission to secrecy communications. *IEEE J. Sel. Areas Commun.* **2012**, *30*, 359–368.
44. Gradshteyn, I.S.; Ryzhik, I.M. *Table of Integrals, Series, and Products*, 7th ed.; Elsevier/Academic Press: Amsterdam, The Netherlands, 2007.