entropy

MDPI

Article

Confidential Cooperative Communication with the Trust Degree of Jammer

Mingxiong Zhao [1,2], Di Liu [1], Hui Gao [3] and Wei Feng [4,*]

1 National Pilot School of Software, Yunnan University, Kunming 650504, China; mx_zhao@ynu.edu.cn (M.Z.); dliu@ynu.edu.cn (D.L.)
2 Key Laboratory in Software Engineering of Yunnan Province, Kunming 650504, China
3 School of Information and Communication Engineering, Beijing University of Posts and Telecommunications, Beijing 100876, China; huigao@bupt.edu.cn
4 School of Communication Engineering, Hangzhou Dianzi University, Hangzhou 310018, China
* Correspondence: fengwei@hdu.edu.cn; Tel.: +86-0571-8532-8949

Received: 16 May 2019; Accepted: 13 June 2019; Published: 15 June 2019

Abstract: In this paper, we consider the trust degree of a jammer, defined as the probability that the jammer cooperates to secure the legitimate transmission, and investigate its influence on confidential cooperative communication. According to the trust degree, we derive the closed-form optimal transmit signal-to-noise ratio (SNR) of the confidential message, $\rho_c^\star$, to maximize the expected secrecy rate, and further obtain the relationship between $\rho_c^\star$ and the trust degree associated with the transmit SNR at the transmit user and channel gains. Simulation results demonstrate that the trust degree has a great effect on the transmit SNR of the confidential message and helps improve the performance of confidential cooperation in terms of the expected secrecy rate.

Keywords: trust degree; confidential communication; cooperative jamming; transmit SNR

1. Introduction

With the rapid growth of communications between socially-connected users, not only physical parameters, e.g., channel qualities and traffic demands, but also the social relationship among users, such as kinship, friendship, and acquaintance, have been taken into account as key design parameters for efficient cooperative communications [1–5]. As the most fundamental concept, the trust degree of the social relationship is interpreted as the degree that reveals how willingly a node helps other nodes' communication in cooperative communications [5]. In other words, the node would like to cooperate with others by consuming their own resources if they have a close relationship, i.e., a high trust degree, which can be evaluated and quantified based on the previous direct or indirect information according to observations of behavior [6].

In the literature, the trust degree has triggered plenty of research interest in various fields, including content caching, mobile social communications, and especially cooperative communications [1–5]. More specifically, the optimal social-aware relay selection strategy was proposed in [1], while a partner selection algorithm was designed based on the social-position relationship in [2]. The trust degree-based beamforming and transmission strategies were investigated for one relay in [3] and two relays with different trusts in [4] for a MISO cooperative communication system. Meanwhile, the traffic demand-driven user cooperation strategies were considered for various antenna configurations based on the trust degree in [5].

Due to the broadcasting nature of wireless mediums, physical (PHY)-layer security has also drawn significant attention in communication networks [7–11]. Specifically, the authors in [8] gave a constructive survey on threats and attacks on mobile networks, while a comprehensive survey

on cooperative relaying and jamming strategies for physical layer security was presented in [9]. Meanwhile, the performance analysis of mmWave-overlaid microwave cellular networks was given in [10] from the security perspective, and secrecy analysis with passive eavesdroppers by using partial cooperation was investigated in [11]. Furthermore, with the rapid development of social awareness networks, the combination of the trust degree and PHY-layer security with application to cooperative communications has attracted plenty of research [12–15]. To be specific, the authors in [12] treated potential eavesdroppers as relays to transmit messages and maximize the expected secrecy rate according to their trustworthiness, instead of regarding them as wiretappers all the time. In [13,14], trust degree-based cooperative secure transmission strategies were proposed, and users with sufficiently high trust degrees would cooperate to transmit data or jamming signals. In [15], jamming-aided cooperative cooperation based on trust degree was investigated to maximize the security rate of the data transmission for P2P communications, where the authors applied a brute-force approach to search over all possible power allocations of the confidential message and jamming signal. However, the trust degree in [13,14] was exploited to choose trustworthy users (jammer [13], jammer and relay [14]) and filter out untrustworthy users (dummy nodes), and the explicit relationship between power allocations and trust degree had not been investigated and given in [15]. Therefore, the characteristics of the jammer' trust degree were not fully utilized to effectively design cooperative secure transmission strategies, and the insight into how the trust degree affects the confidential cooperation was not explicitly investigated and well presented.

Motivated by the aforementioned research and problems, we have observed that the trust degree plays a significant role in cooperative secure communications. Hence, in this paper, we consider the probability that the jammer cooperates in secure legitimate transmission as its trust degree and investigate its influence on the performance of confidential cooperative communications. Different from [15], we not only consider the transmit signal-to-noise ratios (SNRs) of the confidential message and jamming signal, but also investigate the influence of artificial interference at the transmit user (Tu) in the case that the jamming signal from the jammer is not sufficient when the channel gain between the jammer and eavesdropper is weak and obtain their optimal transmit SNRs in closed-form to maximize the expected secrecy rate according to the trust degree. Meanwhile, we further achieve some meaningful results based on the relationship among the trust degree, channel gains, and the transmit SNR at Tu.

Notation: For a complex scalar x , its complex conjugate is denoted by $\bar{x}$. $E[\cdot]$ and $\mathcal{CN}(\cdot)$ denote the statistical expectation and complex Gaussian distributions, respectively.

2. Trust Degree and System Model

2.1. Trust Degree

With the rapid growth of online social networks, more and more people are getting involved in online social interactions. Therefore, the social relationship has emerged as an important issue to investigate how the degree of closeness of the social relationship between users affects their communication strategies [5,16–18]. In the cooperative communication systems, the trust degree can be interpreted as the degree that reveals how much a node is willing to help the communication of the other node [1,3,5]. Similarly, in our system model, the trust degree between $\mathcal{T}$ and $\mathcal{J}$, α, is defined by the probability that $\mathcal{J}$ helps to secure the transmission between $\mathcal{T}$ and $\mathcal{R}$, and thus, α is a value in the range of $0 \leq \alpha \leq 1$.

In the literature, the trust degree has been evaluated and quantified in various ways [6,19–23]. In emergency networks such as disaster relief and public safety networks, the most trustworthy nodes would be those in the immediate region, so the trust degree can be measured based on the proximity between nodes, e.g., physical distance [19]. In general mobile networks, the trust degree can be evaluated by the observations of the previous behaviors of the node [6,20–23]. In [22,23], the trust degree was determined using the Bayesian framework. In the Bayesian framework, the trust degree

is given by the ratio of the observations of the positive behavior among total observations, where the positive behavior is that the node behaves in the predefined way of the network. Similar to [23], in this paper, the positive behavior is defined by jammer, which helps to secure the transmission of Tu, and hence, Tu can estimate the trust degree based on the historical observations of the positive behavior of jammer. The trust degree can also be updated according to new observations. However, when the number of observations is sufficiently large, the trust degree will have ignorable change according to new observation, and it will be more like a constant. Therefore, in our system model, we assume that the trust degree remains unchanged during the transmission [5].

2.2. System Model

Consider a user cooperation network as shown in Figure 1, where there are four single-antenna nodes, including a Tu, a receive user (Ru), a jammer, and an eavesdropper, and we denote them by $\mathcal{T}$, $\mathcal{R}$, $\mathcal{J}$, and $\mathcal{E}$, respectively. The channels from $\mathcal{T}$ to $\mathcal{R}$ and $\mathcal{E}$, and from $\mathcal{J}$ to $\mathcal{E}$ and $\mathcal{R}$ are denoted by h_{tr}, h_{te}, h_{je}, and h_{jr}, where all of them follow a complex Gaussian distribution with zero mean and different covariances, $\sigma^2_{h_{tr}}$, $\sigma^2_{h_{te}}$, $\sigma^2_{h_{je}}$ m and $\sigma^2_{h_{jr}}$, respectively.

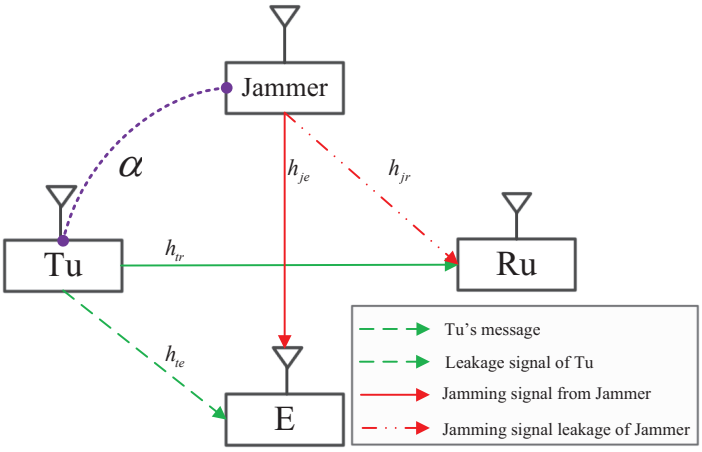

Figure 1. System model. Tu, transmit user; Ru, receive user; E, Eavesdropper.

In this paper, we consider that $\mathcal{J}$ will transmit the jamming signal to confound $\mathcal{E}$ in order to help the legitimate transmission between $\mathcal{T}$ and $\mathcal{R}$ based on trust degree α, which characterize the willingness that $\mathcal{J}$ cooperates with $\mathcal{T}$ for secure communications, i.e., $\mathcal{J}$ helps with high probability when the trust degree is high. In this system, we consider the following two transmission strategies for confidential communications:

(a) *Direct transmission*: $\mathcal{J}$ does not help to confound $\mathcal{E}$ with jamming signal x_j, and thus, $\mathcal{T}$ transmits artificial interference, x_i, together with a confidential message, x_c, to keep its transmission secure, where x_i and x_c are independent. In this strategy, the transmit data at $\mathcal{T}$ and $\mathcal{J}$ are written as $\{x_t = \sqrt{P_c}x_c + \sqrt{P_i}x_i, x_j^d = 0\}$, while $E[x_i\bar{x}_i] = 1$ and $E[x_c\bar{x}_c] = 1$, where $P_c + P_i \leq P_T$ and P_T is the maximum transmit budget at $\mathcal{T}$.

(b) *Cooperative transmission*: $\mathcal{J}$ transmits jamming signal x_j to guarantee additionally the secure transmission between $\mathcal{T}$ and $\mathcal{R}$ and helps to reserve more power for the confidential message at $\mathcal{T}$. However, $\mathcal{T}$ also needs to generate artificial interference for this strategy in case the jamming signal from the jammer is not sufficient when channel gain $|h_{je}|^2$ is small. Thus, the transmit data at $\mathcal{T}$ and $\mathcal{J}$ are given by $\{x_t = \sqrt{P_c}x_c + \sqrt{P_i}x_i,\ x_j^c = \sqrt{P_j}x_j\}$, while $E[x_j^c\bar{x}_j^c] = 1$, where $P_j \leq P_J$ and P_J is the maximum transmit budget at $\mathcal{J}$.

According to the above strategies, the expected secrecy rate with respect to (w.r.t.) trust degree α, the similar structure of which was given in [15], is obtained by:

$$\begin{aligned}\bar{R}_{se}(\rho_c,\rho_i,\rho_j) = \bar{\alpha}\left[\log_2(1+\rho_c g_{tr}) - \log_2\left(1+\frac{\rho_c g_{te}}{\rho_i g_{te}+1}\right)\right]^+ \\ + \alpha\left[\log_2(1+\rho_c g_{tr}) - \log_2\left(1+\frac{\rho_c g_{te}}{\rho_i g_{te}+\rho_j g_{je}+1}\right)\right]^+,\end{aligned} \tag{1}$$

in which we assume that x_i and x_j are prior-known at $\mathcal{R}$, and $\mathcal{R}$ can completely cancel x_i and x_j from its received signal, which is a common assumption used in [12,24]. Notice that the information of jamming and artificial interference can be shared through an alternative wired connection between the transmitter or jammer and the receiver. In (1), $[x]^+ = \max\{0, x\}$ and $\bar{\alpha} \triangleq 1-\alpha$. The channel gains are defined as $g_{tr} = |h_{tr}|^2, g_{te} = |h_{te}|^2$ and $g_{je} = |h_{je}|^2$. The transmit SNRs are given as $\rho_c = \frac{P_c}{\sigma^2}, \rho_i = \frac{P_i}{\sigma^2}$ and $\rho_j = \frac{P_j}{\sigma^2}$, where σ^2 is the variance of the complex Gaussian distribution, $\mathcal{CN}(0,\sigma^2)$, associated with the additive white Gaussian noise (AWGN) at $\mathcal{R}$ and $\mathcal{E}$. The first term of (1) denotes the secrecy rate at $\mathcal{R}$ obtained by the direct transmission strategy when $\mathcal{J}$ does not help with the possibility $\bar{\alpha}$, while the second term represents the secrecy rate achieved by the cooperative transmission when $\mathcal{J}$ helps to jam with the possibility α.

3. Problem Formulation and Solution

From (1), it is noted that for given $\{\rho_c, \rho_j\}$, (1) is a monotonic increasing function w.r.t. ρ_i, and thus, the optimal transmit SNR of artificial interference that maximizes (1) is achieved when $\rho_i = \rho_T - \rho_c$ i.e., $P_i = P_T - P_c$, where $\rho_T = \frac{P_T}{\sigma^2}$. Meanwhile, it also applies to the case that for given $\{\rho_c, \rho_i\}$, the optimal transmit SNR of the jamming signal is $\rho_j^\star = \rho_J \triangleq \frac{P_J}{\sigma^2}$, which maximizes (1). Therefore, the problem that maximizes (1) can be formulated as:

$$\mathbf{P}: \max_{\rho_c} \bar{R}_{se}(\rho_c) \tag{2a}$$

$$\text{s.t. } 0 \le \rho_c \le \rho_T, \tag{2b}$$

where:

$$\begin{aligned}\bar{R}_{se}(\rho_c) = \bar{\alpha}\left[\log_2(1+\rho_c g_{tr}) - \log_2\left(1+\frac{\rho_c g_{te}}{(\rho_T-\rho_c) g_{te}+1}\right)\right]^+ \\ + \alpha\left[\log_2(1+\rho_c g_{tr}) - \log_2\left(1+\frac{\rho_c g_{te}}{(\rho_T-\rho_c) g_{te}+\rho_J g_{je}+1}\right)\right]^+.\end{aligned} \tag{3}$$

To maximize the expected secrecy rate in **P**, the optimal transmit SNR of confidential message, $\rho_c^\star$, at $\mathcal{T}$ can be achieved resorting to the following theorem.

Theorem 1. *For given channel conditions and transmit SNRs, ρ_T and ρ_J, the optimal transmit SNR of confidential message, $\rho_c^\star$, that maximizes the expected secrecy rate at $\mathcal{R}$ is obtained as:*

$$\rho_c^\star = \begin{cases} \rho_1, & \text{if } g_{te} \ge g_{tr},\ \begin{cases} \left[\frac{\rho_T g_{tr} g_{te} + g_{tr} - g_{te}}{g_{tr} g_{je}}\right]^+ < \rho_J \le \frac{g_{te}-g_{tr}}{g_{tr} g_{je}} \\ \max\left\{\frac{g_{te}-g_{tr}}{g_{tr} g_{je}}, \frac{\rho_T g_{tr} g_{te} + g_{tr} - g_{te}}{g_{tr} g_{je}}\right\} < \rho_J \le \frac{\rho_T g_{tr} g_{te} + g_{te} - g_{tr}}{g_{tr} g_{je}} \end{cases} \\ \rho_c^l, & \text{if } g_{te} \ge g_{tr},\ \frac{g_{te}-g_{tr}}{g_{tr} g_{je}} < \rho_J \le \frac{\rho_T g_{tr} g_{te} + g_{tr} - g_{te}}{g_{tr} g_{je}} \\ \rho_T, & \text{if } g_{te} \ge g_{tr},\ \frac{\rho_T g_{tr} g_{te} + g_{te} - g_{tr}}{g_{tr} g_{je}} < \rho_J \\ \rho_2 \text{ or } \rho_3, & \text{otherwise} \end{cases}, \tag{4}$$

where $\rho_c^l = \frac{\rho_T g_{tr} g_{te} + g_{tr} - g_{te}}{g_{tr} g_{te}}$, $\rho_1 = \frac{\rho_T g_{tr} g_{te} + \rho_J g_{tr} g_{je} + g_{tr} - g_{te}}{2 g_{tr} g_{te}}$,

$$\rho_2 = \begin{cases} \min\left\{\left[\frac{-b+\sqrt{b^2-4ac}}{2a}\right]^+, \rho_c^l\right\}, & \text{if } g_{te} \geq g_{tr} \\ \min\left\{\left[\frac{-b+\sqrt{b^2-4ac}}{2a}\right]^+, \rho_T\right\}, & \text{if } g_{te} < g_{tr} \end{cases}, \text{ and } \rho_3 = \begin{cases} \min\left\{\left[\frac{-b-\sqrt{b^2-4ac}}{2a}\right]^+, \rho_c^l\right\}, & \text{if } g_{te} \geq g_{tr} \\ \min\left\{\left[\frac{-b-\sqrt{b^2-4ac}}{2a}\right]^+, \rho_T\right\}, & \text{if } g_{te} < g_{tr} \end{cases}$$

in which $a = 1$, $b = -\frac{\left[3\rho_T g_{te} + (2-\alpha)\rho_J g_{je} + 3\right] g_{tr} - g_{te}}{2 g_{tr} g_{te}}$, *and* $c = \frac{(\rho_T g_{tr} g_{te} + g_{tr} - g_{te} + \alpha g_{te})(\rho_T g_{te} + \rho_J g_{je} + 1) + \alpha g_{te}(\rho_T g_{te} + 1)}{2 g_{tr} g_{te}^2}$. *It is true that* $\sqrt{b^2 - 4ac} \geq 0$, *and the proof is given as:*

Proof. Define $f(\alpha) = b^2 - 4ac$. With some mathematic manipulations, we can obtain:

$$f(\alpha) = \frac{(2-\alpha)^2 \rho_J^2 g_{tr}^2 g_{je}^2 + (4-6\alpha)\rho_J g_{tr} g_{je}(\rho_T g_{tr} g_{te} + g_{tr} + g_{te}) + (\rho_T g_{tr} g_{te} + g_{tr} + g_{te})^2}{4 g_{tr}^2 g_{te}^2}. \quad (5)$$

Based on the property of the derivative, it is straightforward to know that $f(\alpha)$ is a decreasing function w.r.t. α for $\alpha \in [0, 1]$, and $\min_\alpha f(\alpha) = f(\alpha)_{\alpha=1} \geq 0$. □

Proof. The proof of Theorem 1 is presented in Appendix A. □

Notice that the one yielding the larger expected secrecy rate is regarded as $\rho_c^\star$ between ρ_2 and ρ_3; meanwhile, the optimal transmit SNR of artificial interference is given by $\rho_i^\star = \rho_T - \rho_c^\star$. To get a better insight into the relationship between the optimal transmit SNR of the confidential message, $\rho_c^\star$, and trust degree α, we have the following corollary.

Corollary 1. *When the transmit SNR of the jamming signal goes to infinity, i.e.,* $\rho_J \to +\infty$, *the optimal transmit SNR of the confidential message,* $\rho_c^\star$, *can be obtained as:*

$$\rho_c^\star = \begin{cases} 0, & \text{if } g_{te} \geq g_{tr},\ 0 \leq \alpha < \alpha_1 \\ \rho_\alpha, & \text{if } \begin{cases} g_{te} \geq g_{tr},\ \alpha_1 \leq \alpha < \alpha_2 \\ g_{te} < g_{tr},\ 0 \leq \alpha < \alpha_3 \end{cases} \\ \rho_c^l, & \text{if } \ g_{te} \geq g_{tr},\ \alpha_2 \leq \alpha < \alpha_3 \\ \rho_T, & \text{if } \begin{cases} g_{te} \geq g_{tr}, \\ g_{te} < g_{tr}, \end{cases} \alpha_3 \leq \alpha \leq 1 \end{cases}, \quad (6)$$

where $\rho_\alpha = \frac{\rho_T g_{tr} g_{te} + g_{tr} - g_{te} + \alpha g_{te}}{(2-\alpha) g_{tr} g_{te}}$, $\alpha_1 = \left[\frac{g_{te} - g_{tr} - \rho_T g_{tr} g_{te}}{g_{te}}\right]^+$, $\alpha_2 = \left[\frac{\rho_T g_{tr} g_{te} + g_{tr} - g_{te}}{\rho_T g_{tr} g_{te} + g_{tr}}\right]^+$, *and* $\alpha_3 = \left[\frac{\rho_T g_{tr} g_{te} + g_{te} - g_{tr}}{\rho_T g_{tr} g_{te} + g_{te}}\right]^+$.

Proof. The proof is given in Appendix C. □

Remark 1. *From Corollary 1, we observe that the optimal transmit SNR of the confidential message,* $\rho_c^\star$, *is mainly determined by the relationship among the trust degree, channel qualities, and the transmit SNR at* $\mathcal{T}$. *If the eavesdropping channel quality is better than that of the legitimate channel such that* $g_{te} \geq g_{tr}$, *it is not secure to transmit any confidential message when* α *is small. With growing* α *within a moderate range, the transmit SNR of the confidential message basically depends on* α. *More specifically,* $\mathcal{T}$ *will reduce the power for artificial interference and allocate more power for the confidential message to exploit the cooperation of* $\mathcal{J}$ *fully. Furthermore, when* $\mathcal{J}$ *helps to jam with high probability, equivalently* α *is high,* $\mathcal{T}$ *relies on* $\mathcal{J}$ *to guarantee secure transmission and assigns all the power for confidential message. Notice that when the legitimate channel quality is good such that* $g_{te} < g_{tr}$, *it is still secure to send the confidential message with an appropriate transmit SNR even if* α *is small.*

4. Simulation Results

In this section, we evaluate the performance of the trust degree-based confidential cooperative communication and use the average gains of channel elements as $\{\sigma^2_{h_{tr}}, \sigma^2_{h_{te}}, \sigma^2_{h_{je}}\} = \{-20, -20, -20\}$ dB, and the expected secrecy rates are averaged over 10^4 channel realizations.

In Figure 2, we plot the expected secrecy rates at $\mathcal{R}$ versus the trust degree of $\mathcal{J}$, when the transmit SNRs at $\mathcal{T}$ and $\mathcal{J}$ are given by $\rho_T = \rho_J = 30$ dB. To compare with the proposed confidential cooperation scheme, we also plot the expected secrecy rate of the *no cooperation case* (NCC) ($\alpha = 0$). For the proposed confidential cooperation, the optimal transmit SNR of the confidential message at $\mathcal{T}$ for cooperation is obtained as $\rho_c^\star$ in Theorem 1. In Figure 2, it is certified that the expected secrecy rate can be significantly improved by the jammer's cooperation and increased with growing the trust degree of $\mathcal{J}$, yielding a higher expected secrecy rate than NCC.

In Figure 3, we plot the expected secrecy rates at $\mathcal{R}$ versus the transmit SNR of the jamming signal at $\mathcal{J}$, when the transmit SNR at $\mathcal{T}$ is given by $\rho_T = 30$ dB. In this figure, we first observe that when the transmit SNR of the jamming signal increases from 5 dB to 60 dB, i.e., ρ_J goes to infinity, as shown in Corollary 1, the expected secrecy rate at $\mathcal{R}$ can be increased through the cooperation of $\mathcal{J}$, and $\mathcal{T}$ will assign more power for the confidential message with growing α to achieve a higher expected secrecy rate. However, the expected secrecy rate does not increase all the time and will become saturated with the growth of ρ_J, as shown in (A5), which has no relationship with ρ_J when ρ_J goes to infinity.

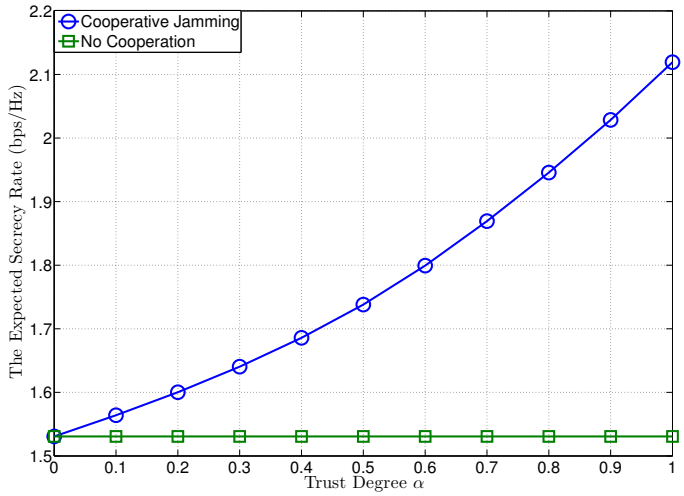

Figure 2. The expected secrecy rate versus trust degree α, where $\rho_T = \rho_J = 30$ dB.

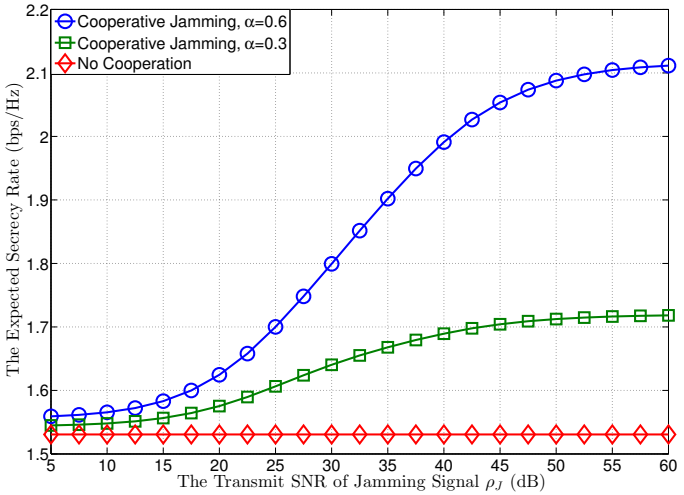

Figure 3. The expected secrecy rate versus the transmit SNR of jamming signal ρ_J, where $\rho_T = 30$ dB.

5. Conclusions

In this paper, we investigated the confidential cooperative communication according to the jammer's trust degree and exploited its characteristics to design efficient cooperative strategies. To maximize the expected secrecy rate, we derived the closed-form optimal transmit SNR of the confidential message based on the trust degree and observed that the expected secrecy rate will become saturated along with the increasing ρ_J. Simulation results showed that $\mathcal{T}$ will achieve a better performance with more power assignment for the confidential message instead of artificial interference with the growing trust degree of $\mathcal{J}$, which has a great influence on the performance of confidential cooperation in terms of the expected secrecy rate.

Author Contributions: Conceptualization, M.Z.; investigation, M.Z.; methodology, D.L.; supervision, W.F.; writing, original draft, M.Z.; writing, review and editing, H.G; all authors have read and approved the final manuscript.

Funding: This work of Mingxiong Zhao is supported in part by the National Natural Science Foundation of China under Grant 61801418, in part by Yunnan Applied Basic Research Projects under Grant 2019FD-12, in part by the Open Foundation of Key Laboratory in Software Engineering of Yunnan Province under Grant 2017SE203. This work of Hui Gao is supported by the National Natural Science Foundation of China under Grant 61401041 and 61671072.

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

Appendix A. Proof of Theorem 1

If $g_{te} \geq g_{tr}$, from (3), we first deal with the operation of $[x]^+$ in (3) and consider two conditions (i) $\rho_c \leq \rho_c^l \triangleq \frac{\rho_T g_{tr} g_{te} + g_{tr} - g_{te}}{g_{tr} g_{te}}$ and (ii) $\rho_c \leq \rho_c^u \triangleq \frac{\rho_T g_{tr} g_{te} + \rho_J g_{tr} g_{je} + g_{tr} - g_{te}}{g_{tr} g_{te}}$ to make the first and the second term in (3) non-negative. Notice that $\rho_c \geq 0$ and $\rho_J \geq 0$. According to (i) and (ii), we investigate (3) and solve **P** as follows:

(1) If $\rho_c^u \leq \rho_c \leq \rho_T$, we obtain $\rho_J \leq \frac{g_{te} - g_{tr}}{g_{tr} g_{je}}$, and $\bar{R}_{se}(\rho_c) = 0$.

(2) If $\rho_c^l \leq \rho_c < \rho_c^u \leq \rho_T$,

$$\bar{R}_{se}(\rho_c) = \alpha \left[\log_2(1 + \rho_c g_{tr}) - \log_2 \left(1 + \frac{\rho_c g_{te}}{(\rho_T - \rho_c) g_{te} + \rho_J g_{je} + 1} \right) \right], \tag{A1}$$

which is a concave function w.r.t. ρ_c. Resorting to $\frac{\mathrm{d}\bar{R}_{se}(\rho_c)}{\mathrm{d}\rho_c} = 0$, we can get $\rho_c^o = \frac{\rho_T g_{tr} g_{te} + \rho_J g_{tr} g_{je} + g_{tr} - g_{te}}{2 g_{tr} g_{te}}$. Based on whether ρ_c^o lies in $[\rho_c^l,\ \rho_c^u)$, different situations are given as follows:

- If $\left[\frac{\rho_T g_{tr} g_{te} + g_{tr} - g_{te}}{g_{tr} g_{je}} \right]^+ \leq \rho_J \leq \frac{g_{te} - g_{tr}}{g_{tr} g_{je}}$, $\rho_c^o \in [\rho_c^l,\ \rho_c^u)$, the optimal transmit SNR of the confidential message that maximizes (A1) is obtained by $\rho_c^\star = \frac{\rho_T g_{tr} g_{te} + \rho_J g_{tr} g_{je} + g_{tr} - g_{te}}{2 g_{tr} g_{te}}$;
- If $\rho_J \leq \min \left\{ \left[\frac{\rho_T g_{tr} g_{te} + g_{tr} - g_{te}}{g_{tr} g_{je}} \right]^+, \frac{g_{te} - g_{tr}}{g_{tr} g_{je}} \right\}$, $\rho_c^o \in [0,\ \rho_c^l]$, the optimal transmit SNR of the confidential message is obtained by $\rho_c^\star = \rho_c^l$ due to the concavity of (A1).

(3) If $0 \leq \rho_c \leq \rho_c^l \leq \rho_c^u \leq \rho_T$ or $0 \leq \rho_c \leq \rho_c^l \leq \rho_T \leq \rho_c^u$, where the boundary point ρ_c^l can be included in this interval without affecting the optimal transmit SNR of confidential message $\rho_c^\star$, the formulation of $\bar{R}_{se}(\rho_c)$ is the same, given by:

$$\bar{R}_{se}(\rho_c) = \log_2(1 + \rho_c g_{tr}) - \bar{\alpha} \log_2 \left(1 + \frac{\rho_c g_{te}}{(\rho_T - \rho_c) g_{te} + 1} \right) - \alpha \log_2 \left(1 + \frac{\rho_c g_{te}}{(\rho_T - \rho_c) g_{te} + \rho_J g_{je} + 1} \right), \tag{A2}$$

which is concave w.r.t. ρ_c, and the proof is given in Appendix B. With the help of factorization, the optimal transmit SNR of the confidential message that maximizes (A2) is obtained by using $\frac{\mathrm{d}\bar{R}_{se}(\rho_c)}{\mathrm{d}\rho_c} = 0$ to get ρ_c^o, which is part of ρ_2 and ρ_3 in Theorem 1. Notice that it is necessary to check the feasibility of ρ_c^o whether it lies in $[0,\ \rho_c^l]$. If not, the boundary point is chosen as $\rho_c^\star$ due to the concavity of (A2), and thus, the result in the second part of (2) in this Appendix can be classified in this part.

(4) If $\rho_c^l \le \rho_c \le \rho_T < \rho_c^u$, we obtain $\rho_J > \frac{g_{te}-g_{tr}}{g_{tr}g_{je}}$, and the formulation of $\bar{R}_{se}(\rho_c)$ is given by (A1). Resorting to $\frac{\mathrm{d}\bar{R}_{se}(\rho_c)}{\mathrm{d}\rho_c} = 0$, we can get $\rho_c^o = \frac{\rho_T g_{tr}g_{te}+\rho_J g_{tr}g_{je}+g_{tr}-g_{te}}{2g_{tr}g_{te}}$. Based on the feasibility check, we can get the following results:

- If $\frac{\rho_T g_{tr}g_{te}+g_{te}-g_{tr}}{g_{tr}g_{je}} < \rho_J$, $\rho_c^o > \rho_T$, the optimal transmit SNR of the confidential message is obtained by $\rho_c^\star = \rho_T$ due to the concavity of (A1);
- If $\max\left\{\frac{g_{te}-g_{tr}}{g_{tr}g_{je}}, \frac{\rho_T g_{tr}g_{te}+g_{tr}-g_{te}}{g_{tr}g_{je}}\right\} < \rho_J \le \frac{\rho_T g_{tr}g_{te}+g_{te}-g_{tr}}{g_{tr}g_{je}}$, $\rho_c^o \in (\rho_c^l,\ \rho_T]$, the optimal transmit SNR of the confidential message is obtained by $\rho_c^\star = \frac{\rho_T g_{tr}g_{te}+\rho_J g_{tr}g_{je}+g_{tr}-g_{te}}{2g_{tr}g_{te}}$;
- If $\frac{g_{te}-g_{tr}}{g_{tr}g_{je}} < \rho_J \le \frac{\rho_T g_{tr}g_{te}+g_{tr}-g_{te}}{g_{tr}g_{je}}$, $\rho_c^o \in [0,\ \rho_c^l]$, the optimal transmit SNR of the confidential message is $\rho_c^\star = \rho_c^l$, and this result can be categorized into (3) in this Appendix.

If $g_{te} < g_{tr}$, the formulation of $\bar{R}_{se}(\rho_c)$ is given in (A2) with $0 \le \rho_c \le \rho_T < \rho_c^l$, and the optimal transmit SNR of the confidential message is similar to that in (3).

Appendix B. Proof of the Concavity of (A2)

The following proof is to show the concavity of (A2). We first obtain the derivative of (A2) w.r.t. ρ_c as:

$$\frac{\mathrm{d}\bar{R}_{se}(\rho_c)}{\mathrm{d}\rho_c} = \frac{1}{\ln 2}\left(\frac{g_{tr}}{1+\rho_c g_{tr}} - \frac{\bar{\alpha}g_{te}}{\rho_T g_{te}-\rho_c g_{te}+1} - \frac{\alpha g_{te}}{\rho_T g_{te}-\rho_c g_{te}+\rho_J g_{je}+1}\right). \tag{A3}$$

To know whether (A2) is concave or not w.r.t ρ_c, we further obtain its second derivative as:

$$\frac{\mathrm{d}^2\bar{R}_{se}(\rho_c)}{\mathrm{d}\rho_c^2} = \frac{-1}{\ln 2}\left[\frac{g_{tr}^2}{(1+\rho_c g_{tr})^2} + \frac{\bar{\alpha}g_{te}^2}{(\rho_T g_{te}-\rho_c g_{te}+1)^2} + \frac{\alpha g_{te}^2}{(\rho_T g_{te}-\rho_c g_{te}+\rho_J g_{je}+1)^2}\right]. \tag{A4}$$

Based on the expression of $\frac{\mathrm{d}^2\bar{R}_{se}(\rho_c)}{\mathrm{d}\rho_c^2}$ above, the second derivative is negative, and thus, (A2) is concave w.r.t. ρ_c [25].

Appendix C. Proof of Corollary 1

When $\rho_J \to +\infty$, we only need to consider Case (3), Case (4), and the case when $g_{te} < g_{tr}$ in Appendix A. If $g_{te} \ge g_{tr}$, (3) is recast as follows:

(1) If $0 \le \rho_c \le \rho_c^l \le \rho_T \ll \rho_c^u$,

$$\bar{R}_{se}(\rho_c) = \log_2(1+\rho_c g_{tr}) - \bar{\alpha}\log_2\left(1+\frac{\rho_c g_{te}}{(\rho_T-\rho_c)g_{te}+1}\right), \tag{A5}$$

which is concave w.r.t. ρ_c. Resorting to $\frac{\mathrm{d}\bar{R}_{se}(\rho_c)}{\mathrm{d}\rho_c} = 0$, we have $\rho_c^o = \frac{\rho_T g_{tr}g_{te}+g_{tr}-g_{te}+\alpha g_{te}}{(2-\alpha)g_{tr}g_{te}}$. Based on whether ρ_c^o lies in $[0,\ \rho_c^l]$, different situations are given as:

- If $0 \le \alpha < \left[\frac{g_{te}-g_{tr}-\rho_T g_{tr}g_{te}}{g_{te}}\right]^+$, $\rho_c^o < 0$, the optimal transmit SNR of the confidential message is $\rho_c^\star = 0$ due to the concavity of (A5);
- If $\left[\frac{g_{te}-g_{tr}-\rho_T g_{tr}g_{te}}{g_{te}}\right]^+ \le \alpha < \left[\frac{\rho_T g_{tr}g_{te}+g_{tr}-g_{te}}{\rho_T g_{tr}g_{te}+g_{tr}}\right]^+$, $\rho_c^o \in [0,\ \rho_c^l)$, the optimal transmit SNR of the confidential message that maximizes (A5) is $\rho_c^\star = \frac{\rho_T g_{tr}g_{te}+g_{tr}-g_{te}+\alpha g_{te}}{(2-\alpha)g_{tr}g_{te}}$;
- If $\left[\frac{\rho_T g_{tr}g_{te}+g_{tr}-g_{te}}{\rho_T g_{tr}g_{te}+g_{tr}}\right]^+ \le \alpha < \left[\frac{\rho_T g_{tr}g_{te}+g_{te}-g_{tr}}{\rho_T g_{tr}g_{te}+g_{te}}\right]^+$, $\rho_c^o \in [\rho_c^l,\ \rho_T]$, the optimal transmit SNR of the confidential message is $\rho_c^\star = \rho_c^l$ due to the concavity of (A5).

(2) If $\rho_c^l \le \rho_c \le \rho_T \ll \rho_c^u$, where the boundary point ρ_c^l can be included in this interval without affecting the optimal transmit SNR of confidential message $\rho_c^\star$, $\bar{R}_{se}(\rho_c) = \alpha\log_2(1+\rho_c g_{tr})$, and the optimal transmit SNR of the confidential message is $\rho_c^\star = \rho_T$.

If $g_{te} < g_{tr}$, the formulation of $\bar{R}_{se}(\rho_c)$ is the same as (A5) with $0 \leq \rho_c \leq \rho_T$. Due to its concavity w.r.t. ρ_c, we can get $\rho_c^o = \frac{\rho_T g_{tr} g_{te} + g_{tr} - g_{te} + \alpha g_{te}}{(2-\alpha) g_{tr} g_{te}}$ resorting to $\frac{\mathrm{d}\bar{R}_{se}(\rho_c)}{\mathrm{d}\rho_c} = 0$. Based on whether ρ_c^o lies in $[0,\ \rho_T]$, the following different situations are given as:

- If $0 \leq \alpha < \left[\frac{\rho_T g_{tr} g_{te} + g_{te} - g_{tr}}{\rho_T g_{tr} g_{te} + g_{te}}\right]^+$, $\rho_c^o \in [0,\ \rho_T]$, the optimal transmit SNR of the confidential message is $\rho_c^\star = \frac{\rho_T g_{tr} g_{te} + g_{tr} - g_{te} + \alpha g_{te}}{(2-\alpha) g_{tr} g_{te}}$;
- If $\left[\frac{\rho_T g_{tr} g_{te} + g_{te} - g_{tr}}{\rho_T g_{tr} g_{te} + g_{te}}\right]^+ \leq \alpha \leq 1$, $\rho_c^o > \rho_T$, the optimal transmit SNR of the confidential message is $\rho_c^\star = \rho_T$ due to the concavity of (A5).

References

1. Zhang, M.; Chen, X.; Zhang, J. Social-aware relay selection for cooperative networking: An optimal stopping approach. In Proceedings of the 2014 IEEE International Conference on Communications (ICC), Sydney, Australia, 10–14 June 2014; pp. 2257–2262.
2. Mao, H.; Feng, W.; Zhao, Y.; Ge, N. Joint social-position relationship based cooperation among mobile terminals. *IEEE Commun. Lett.* **2014**, *18*, 2165–2168. [CrossRef]
3. Ryu, J.Y.; Lee, J.; Quek, T.Q. Trust degree based beamforming for MISO cooperative communication system. *IEEE Commun. Lett.* **2015**, *19*, 1957–1960. [CrossRef]
4. Ryu, J.Y.; Lee, J.H. Trust Degree-Based MISO Cooperative Communications with Two Relay Nodes. *Wirel. Commun. Mob. Comput.* **2019**. [CrossRef]
5. Zhao, M.; Ryu, J.Y.; Lee, J.; Quek, T.Q.; Feng, S. Exploiting trust degree for multiple-antenna user cooperation. *IEEE Trans. Wirel. Commun.* **2017**, *16*, 4908–4923. [CrossRef]
6. Sun, Y.L.; Han, Z.; Yu, W.; Liu, K.R. A Trust Evaluation Framework in Distributed Networks: Vulnerability Analysis and Defense Against Attacks. In Proceedings of the 25th IEEE International Conference on Computer Communications (INFOCOM 2006), Barcelona, Spain, 23–29 April 2006; pp. 1–13.
7. Zhao, M.; Wang, X.; Feng, S. Joint Power Splitting and Secure Beamforming Design in the Multiple Non-Regenerative Wireless-Powered Relay Networks. *IEEE Commun. Lett.* **2015**, *19*, 1540–1543. [CrossRef]
8. Mavoungou, S.; Kaddoum, G.; Taha, M.; Matar, G. Survey on threats and attacks on mobile networks. *IEEE Access* **2016**, *4*, 4543–4572. [CrossRef]
9. 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.* **2018**. [CrossRef]
10. Vuppala, S.; Tolossa, Y.J.; Kaddoum, G.; Abreu, G. On the physical layer security analysis of hybrid millimeter wave networks. *IEEE Trans. Commun.* **2017**, *66*, 1139–1152. [CrossRef]
11. Atallah, M.; Kaddoum, G. Secrecy Analysis in Wireless Network with Passive Eavesdroppers by Using Partial Cooperation. *IEEE Trans. Veh. Technol.* **2019**. [CrossRef]
12. Ryu, J.Y.; Lee, J.; Quek, T.Q. Confidential Cooperative Communication with Trust Degree of Potential Eavesdroppers. *IEEE Trans. Wirel. Commun.* **2016**, *15*, 3823–3836. [CrossRef]
13. Tang, L.; Chen, H.; Li, Q. Social tie based cooperative jamming for physical layer security. *IEEE Commun. Lett.* **2015**, *19*, 1790–1793. [CrossRef]
14. Wang, H.M.; Xu, Y.; Huang, K.W.; Han, Z.; Tsiftsis, T.A. Cooperative secure transmission by exploiting social ties in random networks. *IEEE Trans. Commun.* **2018**, *66*, 3610–3622. [CrossRef]
15. Wang, L.; Wu, H.; Stüber, G.L. Cooperative jamming-aided secrecy enhancement in P2P communications with social interaction constraints. *IEEE Trans. Veh. Technol.* **2017**, *66*, 1144–1158. [CrossRef]
16. Gong, X.; Chen, X.; Zhang, J. Social group utility maximization game with applications in mobile social networks. In Proceedings of the 2013 51st Annual Allerton Conference on Communication, Control, and Computing (Allerton), Monticello, IL, USA, 2–4 October 2013; pp. 1496–1500.
17. Gong, X.; Chen, X.; Zhang, J. Social group utility maximization in mobile networks: From altruistic to malicious behavior. In Proceedings of the 2014 48th Annual Conference on Information Sciences and Systems (CISS), Princeton, NJ, USA, 19–21 March 2014; pp. 1–6.
18. Chen, X.; Proulx, B.; Gong, X.; Zhang, J. Exploiting social ties for cooperative D2D communications: A mobile social networking case. *IEEE Trans. Wirel. Commun.* **2015**, *23*, 1471–1484. [CrossRef]

19. Coon, J.P. Modelling trust in random wireless networks. In Proceedings of the 2014 11th International Symposium on Wireless Communications Systems (ISWCS), Barcelona, Spain, 26–29 August 2014; pp. 976–981.
20. Li, J.; Li, R.; Kato, J. Future trust management framework for mobile ad hoc networks. *IEEE Commun. Mag.* **2008**, *46*, 108–114.
21. Theodorakopoulos, G.; Baras, J.S. On trust models and trust evaluation metrics for ad hoc networks. *IEEE J. Sel. Areas Commun.* **2006**, *24*, 318–328. [CrossRef]
22. Zouridaki, C.; Mark, B.L.; Hejmo, M.; Thomans, R.K. A quantitative trust establishment framework for reliable data packet delivery in MANETs. In Proceedings of the Milcom 2010 Military Communications Conference, San Jose, CA, USA, 31 October–3 November 2005; pp. 1–10.
23. Changiz, R.; Halabian, H.; Yu, F.R.; Lambadaris, I.; Tang, H.; Mason, P.C. Trust establishment in cooperative wireless networks. In Proceedings of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks, Lexandria, VA, USA, 7 November 2005; pp. 1074–1079.
24. Jorgensen, M.L.; Yanakiev, B.R.; Kirkelund, G.E.; Popovski, P.; Yomo, H.; Larsen, T. Shout to secure: Physical-layer wireless security with known interference. In Proceedings of the IEEE GLOBECOM 2007—IEEE Global Telecommunications Conference, Washington, DC, USA, 26–30 November 2007; pp. 33–38.
25. Boyd, S.; Vandenberghe, L. *Convex Optimization*; Cambridge University Press: Cambridge, UK, 2004.