Friendship-based cooperative jamming for secure communication in Poisson networks

Yuanyu Zhang1 • Yulong Shen2 • Xiaohong Jiang2,3

Published online: 10 May 2018
© Springer Science+Business Media, LLC, part of Springer Nature 2018

Abstract
This paper investigates the physical layer security-based secure communication in a finite Poisson network with social friendships among nodes, for which a social friendship-based cooperative jamming scheme is proposed. The jamming scheme consists of a Local Friendship Circle (LFC) and a Long-range Friendship Annulus (LFA), where all legitimate nodes in the LFC serve as jammers, but the legitimate nodes in the LFA are selected as jammers through three location-based policies. To understand both the security and reliability performances of the proposed scheme, we first derive analytical expressions for the transmission outage probability and determine both the upper and lower bounds on the secrecy outage probability, given the basic Laplace transform of the sum interference at any location in the network. With the help of the tools from stochastic geometry, we then provide general expressions for the above Laplace transform under all path loss scenarios as well as closed-form Laplace transform results under two typical path loss cases, such that the overall outage performances of the proposed scheme can be depicted. Finally, we present extensive numerical results to validate our theoretical analysis and also to illustrate the impacts of the friendship-based cooperative jamming on the network performances.

Keywords Poisson networks • Social relationship • Physical layer security • Cooperative jamming

1 Introduction

Due to the rapid proliferation of smart phones, tablets and PDAs, hand-held devices have been an essential integral part of wireless networks. As these devices are usually carried by human beings, wireless networks, such as wireless ad hoc networks [1, 2], device-to-device (D2D) communications [3] and cognitive radio networks [4], exhibit some social behaviors (e.g., friendship) nowadays. Thus, wireless networks with the consideration of social relationships among network nodes are highly appealing for lots of important data communication services, like content distribution, data sharing and data dissemination [5]. The inherent open nature of wireless medium makes the information exchange over wireless channels susceptible to eavesdropping attacks from unauthorized users, posing a significant threat to the security of wireless networks [6]. As a result, ensuring the security of such networks is of great importance to facilitate their applications in supporting future social-based services with strong security guarantee, like mobile online social application, location-based application and autonomous mobile application [7]. This paper focuses on eavesdropping attacks, while solutions to other attacks like packet dropping, jamming, can be found in [8–11].

The traditional solutions to ensure information security are mainly based on cryptography [12, 13], which encrypts the information with secret keys through various kinds of cryptographic protocols. In cryptography, eavesdroppers
are assumed to have limited computing power, so even if they capture the ciphertext, they cannot decrypt it without the secret key. However, as the computing power advances rapidly nowadays, these solutions are facing increasingly high risk of being broken by the relentless attempts of eavesdroppers. In addition, due to the lack of centralized control, secret key management and distribution in decentralized wireless networks are very costly and complex to be implemented. This necessitates the introduction of more powerful schemes to ensure wireless network security. Physical layer (PHY) security [14] has been recognized as a promising strategy to provide a strong form of security for wireless communications. The basic principle of PHY security is to exploit the inherent randomness of noise and wireless channels to ensure the confidentiality of messages against any eavesdropper regardless of its computing power [15]. Compared to the cryptography-based solutions, PHY security can offer some major advantages, like an everlasting security guarantee, no need for key management/distribution, a high scalability for the next-generation networks [16].

Some recent efforts have been devoted to the study of PHY security-based secure communication in wireless networks with social relationships. Wang et al. [17] considered a D2D communication scenario, where the heads of two D2D user (DUE) clusters wish to communicate with the help of an intermediate Decode-and-Forward relay. The communication security is guaranteed by the cooperative jamming scheme [18, 19], where multiple friendly jammers send jamming signals to suppress eavesdroppers, and the social relationship is modeled by a social trust parameter $u \in [0, 1]$. Two sets of jammers (one set per cluster) are selected from DUEs with social trust above some threshold $u_{min}$. With the consideration of power constraint, the authors studied the optimal selection of relay and jammers to maximize the secrecy rate of DUE transmission and also to ensure a required signal-to-interference-plus-noise ratio (SINR) level to cellular users. Tang et al. [20] considered a wireless network consisting of one source-destination pair, a set of cooperative jammers and one eavesdropper. Cooperative jamming is adopted to ensure the security and the concept of social tie is introduced to model the social relationship between jammers and the source/destination. The strength of social tie of the $n$-th jammer is denoted by $a_n \in \{0, 1\}$, where 1 (0) indicates that the jammer is (is not) willing to participate in the cooperative jamming. The authors modeled the decision problem of jammers as a social tie-based cooperative jamming game and then explored the secrecy outage performance of the source-destination pair by computing the Nash equilibrium of the game.

While the above works represent a significant process in the study of PHY security-based secure communication in wireless networks with social relationships, the social relationships they considered are simply modeled by an indicator variable. Although these variables are acceptable for characterizing some location-independent social relationships, like social tie and social trust, they may fail to model some important social properties closely related to geometric properties of networks, e.g., small-world phenomenon [21, 22]. Also, the network scenarios they considered are quite simple, which consists of either only one eavesdropper and several jammers or only two clusters of jammers. To the best of our knowledge, the study of PHY security-based secure communication in more general large scale wireless networks with small-world properties still remains unknown, which is the scope of this paper.

This paper considers a finite Poisson network consisting of one transmitter-receiver pair, multiple legitimate nodes and multiple eavesdroppers distributed according to two independent and homogeneous Poisson Point Processes (PPP), respectively. It is notable that the Poisson network model can nicely capture the random geometric properties of networks and enable the analytical modeling of network interference statistics in general [23], so it has been widely used in the PHY security performance study of large scale wireless networks without the consideration of social relationships [24–32] (please refer to Sect. 6 for related works). In particular, we consider a more realistic location-based friendship model to characterize the small-world properties in the network. The main contributions of this paper are summarized as follows.

- This paper proposes a friendship-based cooperative jamming scheme to ensure the PHY security-based secure communication between the transmitter and receiver. The jamming scheme comprises a Local Friendship Circle (LFC) and a Long-range Friendship Annulus (LFA), where all legitimate nodes in the LFC serve as jammers, and three location-based policies are designed to select legitimate nodes in the LFA as jammers.

- The transmission outage probability (TOP) and secrecy outage probability (SOP) are adopted to model the reliability and security performance of the proposed jamming scheme [33]. For the modeling of these performance metrics, we first derive analytical expressions for the TOP and then determine both the upper and lower bounds on the SOP, provided that the basic Laplace transform of the sum interference from all jammers at any location in the network is available.

- To complete the modeling of TOP and SOP performances of the proposed jamming scheme, we then apply the tools from stochastic geometry to derive general expressions for the above Laplace transform under all path loss scenarios and also provide closed-
form Laplace transform results under two typical path loss scenarios of exponent equal to 2 and 4, respectively [34].

- Finally, we present extensive numerical results to validate the theoretical analysis of TOP and SOP and also to illustrate the impacts of the friendship-based cooperative jamming on the network performance.

The remainder of this paper is organized as follows. Section 2 introduces the preliminaries and friendship-based cooperative jamming scheme. The TOP and SOP are analyzed in Sect. 3 and the Laplace transforms of the sum interference are analyzed in Sect. 4. The numerical results and corresponding discussions are provided in Sect. 5. Section 6 presents the related works of PHY security performance study for Poisson networks without social relationships. Finally, we conclude this paper in Sect. 7.

2 Preliminaries and jamming scheme

2.1 System model

As illustrated in Fig. 1, we consider a finite wireless network with nodes distributed over a bi-dimensional disk $B(o, D) \subset \mathbb{R}^2$ with radius $D$. The network consists of a transmitter located at the origin $o$ and a receiver located at $y_0$ with fixed distance $|y_0| = l$ to $o$. Also present in the network are multiple legitimate nodes and multiple non-colluding eavesdroppers, whose locations are modeled as two independent and homogeneous PPPs $\Phi$ and $\Phi_e$ with intensities $\lambda$ and $\lambda_e$, respectively. Throughout this paper we will use $x$ ($z$) to denote the random location of a legitimate node (eavesdropper) as well as the node (eavesdropper) itself. To suppress the eavesdroppers, a set of legitimate nodes will serve as jammers to send jamming signals. The set of jammer locations is denoted by $\Phi_J$.

The channel suffers from both small-scale Rayleigh fading and large-scale log-distance path loss with exponent $\alpha \geq 2$ [34]. The fading coefficient is constant for a block of transmission and varies randomly and independently from block to block for all channels. We assume that the transmitter and jammers transmit with the same power. Without loss of generality, unit transmit power is assumed.

The sum interference caused by the set of jammers at any location $y$ in the network is then given by

$$I(y) = \sum_{x \in \Phi_J} h_{x,y}|x-y|^{-\alpha},$$

(1)

where $h_{x,y}$ is the fading coefficient between $x$ and $y$, and $|x - y|$ is the distance between $x$ and $y$. Due to the Rayleigh fading assumption, $h_{x,y}$ is exponentially distributed. We assume unit mean for $h_{x,y}$, i.e., $\mathbb{E}[h_{x,y}] = 1$. In addition to path-loss and fading, all wireless channels are also impaired by the additive Gaussian white noise with zero mean and variance $N_0$. Note that $N_0$ is normalized by the transmit power. The signal-to-interference-plus-noise ratio (SINR) for the receiver $y_0$ from the transmitter $o$ is then given by

$$\text{SINR}_{y_0} = \frac{h_{o,y_0}l^{-\alpha}}{I(y_0) + N_0},$$

(2)

and the SINR for any eavesdropper $z \in \Phi_e$ is given by

$$\text{SINR}_z = \frac{h_{o,z}|z|^{-\alpha}}{I(z) + N_0}.$$  

(3)

2.2 Friendship model

To depict the inherent friendship among network nodes, we adopted the so-called *octopus* model (as illustrated in Fig. 2) in [22], where each node has not only local friends in a circle (called local friendship circle) around itself but also $N$ long-range friends randomly selected from the region outside the circle. It is notable that $N$ can be drawn from any given discrete probability distribution such as power law distribution, Poisson distribution, geometric distribution, uniform distribution, etc. Thus, one can

![Fig. 1 System model: nodes are distributed over a bi-dimensional disk $B(o, D)$ with radius $D$. The transmitter is located at the origin $o$ and the receiver is located at $y_0$ with $|y_0| = l$. Legitimate nodes and eavesdroppers are distributed according to two independent homogeneous PPPs. The friendship-based cooperative jamming model comprises a LFC with radius $R_1$ and a LFA with inner radius $R_1$ and outer radius $R_2$.](image-url)
generate different types of social networks by varying the distribution of $N$. Based on this model, the authors in [22] analytically derived the average social search delay and found that the results are consistent with the empirical observations obtained from previous well-known small-world experiments. This suggests that [22] can capture some important properties of typical small-world networks, where, roughly speaking, any two individuals in the network can be connected through a few number of acquaintances. For example, the short-range connection (i.e., local friendship) and long-range connection (i.e., long-range friendship) can mimic the strong ties (i.e., close relationship established between individuals that may share common information and resources such as friends, working/living places) and weak ties (i.e., casual relationship established between socially distant individuals that may have few common information and resources) in small-world networks. For a more detailed introduction to the octopus model, please refer to [22].

Notice that the friendship considered in this paper is solely related to node locations, which differs from the friendship conception in the sense of social network. The rationale behind the location-based friendship comes from two aspects. First, in general, the friendship between two entities has a relatively strong dependency on the distance between them [35]. For example, people in a local area (e.g., a community) are more likely to be friends, while people in different cities are less likely to be friends. Second, please notice that the distances between jammers and the receiver are key parameters that determine the jamming strength, because jamming signals usually degrade as propagation distances increase. Thus, this paper highlights the location attribute of the friendship when proposing a social friendship-based cooperative jamming scheme.

2.3 Friendship-based cooperative jamming

Based on the friendship model in Fig. 2, this paper proposes a friendship-based cooperative jamming scheme to ensure the transmission security. In this scheme, the legitimate nodes that are friends of the transmitter serve as jammers. We assume friends are always willing to help each other, and thus friendship is an incentive that is strong enough to encourage legitimate nodes to provide jamming service. However, providing jamming service will consume the energy of jammers. Thus, to compensate such loss and further encourage nodes to participate into the cooperative jamming, some reward mechanisms can be introduced into the cooperative jamming scheme, like the monetary incentive mechanism in [36], which gives the nodes that provide jamming services some monetary reward. Regarding the interference from the jammers, recall that we consider a network scenario with only one transmitter-receiver pair in this paper, so the interference from the jammers only affects the information reception of the receiver. In addition, the key idea of cooperative jamming in this paper is to exploit the interference as cooperative jamming signals that may help protect the transmitter-receiver transmission, so interference will not be a problem in this system.

The proposed jamming scheme is composed of a Local Friendship Circle (LFC) with radius $R_1$ and a Long-range Friendship Annulus (LFA) with inner radius $R_1$ and outer radius $R_2$, where $0 < R_1 \leq R_2 \leq D$ (illustrated in Fig. 3). Both the LFC and LFA are centered at the transmitter (i.e., the origin $o$). Let $\mathcal{A}_1$ denote the LFC and $\mathcal{A}_2$ denote the LFA. In the proposed jamming scheme, all legitimate nodes in $\mathcal{A}_1$ serve as jammers, while each legitimate node $x$ in $\mathcal{A}_2$ is selected as a jammer through a location-based policy $P(|x|) \in [0, 1]$. Notice that different $P(|x|)$ can yield different distributions of long-range jammers (i.e., different $\Phi_J$). In this paper, we design three selection policies $P(|x|)$, which are summarized as follows.

- **Policy E** In this policy, each node $x \in \Phi \cap \mathcal{A}_2$ is selected as a jammer with $Equal$ probability $P(|x|) = p \in [0, 1]$. This policy corresponds to the scenario where long-range jammers are uniformly distributed over $\mathcal{A}_2$.
- **Policy I** In this policy, each node $x \in \Phi \cap \mathcal{A}_2$ is selected as a jammer with probability $P(|x|)$ increasing with its path loss to the transmitter, i.e.,

$$P(|x|) = \frac{|x|^2 - R_1^2}{R_2^2 - R_1^2}.$$  \hspace{1cm} (4)

This policy corresponds to the scenario where most of the long-range jammers are distributed near the outer circle of the LFA.
Policy D

In this policy, each node \( x \in \mathcal{A}_2 \) is selected as a jammer with probability \( P(|x|) \) Decreasing with its path loss to the transmitter, i.e.,

\[
P(|x|) = \frac{R_2^2 - |x|^2}{R_2^2 - R_1^2}.
\]

This policy corresponds to the scenario where most of the long-range jammers are distributed near the inner circle of the LFA.

**Remark 1** The policy \( P(|x|) \) can be interpreted as a thinning operation on \( \Phi \) [37]. According to the property of thinning operation, the number of jammers in \( \mathcal{A}_2 \) still follows a Poisson distribution. Hence, the friendship model in the proposed jamming scheme is a special case of the one in [22], given that \( N \) is drawn from a Poisson distribution.

**Remark 2** Notice that we consider the path loss as a mapping to the distance in the design of long-range jammer selection policies. This is because that the path loss mapping can ensure closed-form main results. In our future work, we will consider other mappings that can better characterize the distances to design the long-range jammer selection policies.

The proposed cooperative jamming scheme can be implemented as follows.

1. The transmitter broadcasts a pilot signal to legitimate nodes, which contains information about the parameters \( R_1 \) and \( R_2 \) as well as the long-range jammer selection policy currently in use. After sending the pilot signal, the transmitter sets a timer to wait for the determination of jammers. We assume the expiration time of the timer is also embedded in the pilot signal and all jammers can be determined before the expiration time.
2. Each legitimate node receives the information for jammer selection (i.e., \( R_1, R_2 \) and long-range jammer selection policy) and extracts the channel state information (especially the distance between the transmitter and itself) from the pilot signal.
3. For each legitimate node, if the distance is less than \( R_1 \), it will become a jammer. If the distance is larger than \( R_1 \) but less than \( R_2 \), go to step 4. If the distance is larger than \( R_2 \), it will stay silent.
4. The node will throw a biased coin with the probability determined by the long-range jammer selection policy. If the result is head, the node will become a jammer, otherwise, it stays silent.
5. After the timer expires, the transmitter starts sending information to the receiver and the jammers generate Gaussian noise to help secure the transmission.

**2.4 Performance metrics**

The impact of friendship-based cooperative jamming scheme on the communication between the transmitter \( o \) and receiver \( y_0 \) is two-edged. On one hand, the interference generated by the jammers can degrade the eavesdropper channels, which may greatly enhance the security of the communication. On the other hand, the transmitter-receiver link is also impaired by the unintended interference, resulting in a probably unreliable communication. In this paper, we will adopt the concepts of transmission outage probability (TOP) and secrecy outage probability (SOP) to measure the reliability and security of the transmitter-receiver communication [33], which can be defined according to the following outage events.

- **Transmission outage** The SINR at the receiver \( y_0 \) is below some threshold \( \beta \), i.e., \( \text{SINR}_{y_0} < \beta \), which results in that the receiver \( y_0 \) fails to decode the message from the transmitter \( o \). The probability that this event happens is referred to as the TOP.
- **Secrecy outage** The SINR at one or more eavesdroppers is above some threshold \( \beta_e \), which results in that the eavesdroppers can intercept the message from the transmitter \( o \). The probability that this event happens is referred to as the SOP.
Formally, the TOP is given by
\[ P_{\text{to}} = P(\text{SINR}_{y_0} < \beta), \]  
where \( P \) represents the probability operator, and the SOP is given by
\[ P_{\text{so}} = P \left( \bigcup_{z \in \Phi_e} \{\text{SINR}_z > \beta_z\} \right), \]  
where \( \bigcup \) denotes the union of events.

### 3 Outage performances

In this section, we first introduce the basic Laplace transform of the sum interference \( I(y) \) at any location \( y \) in the network. Based on the Laplace transform, we then determine the exact expression for the TOP of the proposed cooperative jamming scheme, and finally we obtain both the upper and lower bounds on the SOP performance.

We use \( \mathcal{L}_{I(y)}^{A}(s) \) to denote the Laplace transform of the \( I(y) \) in (1), where \( A = \{E, I, D\} \) represents the long-range jammer selection policy. Notice that the derivation of the Laplace transform \( \mathcal{L}_{I(y)}^{A}(s) \) serves as a critical step in modeling the TOP and SOP. We only focus on the analysis of TOP and SOP in this section, and the derivation of \( \mathcal{L}_{I(y)}^{A}(s) \) will be provided in Sect. 4.

#### 3.1 Transmission outage probability

The TOP can be regarded as a measure of the link reliability between the transmitter \( o \) and receiver \( y_0 \). For the Rayleigh fading channel model, the TOP can be directly derived by applying the Laplace transform of the sum interference at the receiver \( y_0 \) [23]. The following theorem is established to summarize the TOP result.

**Theorem 1** Consider a finite Poisson network with nodes distributed over a bi-dimensional disk \( \mathcal{B}(o, D) \) as illustrated in Fig. 1, the upper bound on the TOP of the transmitter-receiver pair under the friendship-based cooperative jamming scheme in Sect. 2.3 is given by
\[ P_{\text{to}}^{\text{UB}} = 1 - \exp \left\{ -2\pi\lambda_e \int_0^D e^{-\beta_e \pi r_e^2} \mathcal{L}^{A}_{I(z)}(\beta_e r_e^2) r_e \, dr_e \right\}, \]  
and the lower bound is given by
\[ P_{\text{to}}^{\text{LB}} = 2\pi\lambda_e \int_0^D e^{-\beta_e \pi r_e^2} e^{-\beta_e \pi z^2} \mathcal{L}^{A}_{I(z^*)}(\beta_e r_e^2) r_e \, dr_e, \]  
where \( \lambda_e \) denotes the density of eavesdroppers, \( \beta_e \) denotes the SINR threshold for successfully decoding of eavesdroppers, \( A = \{E, I, D\} \) denotes the long-range jammer selection policy, \( z^* \) represents the eavesdropper nearest to the transmitter \( o \), \( r_e \) denotes the distance from \( z^* \) to \( o \), and \( \mathcal{L}^{A}_{I(z)}(\cdot) \) and \( \mathcal{L}^{A}_{I(z^*)}(\cdot) \) are the Laplace transforms of the sum interference at \( z \) and \( z^* \), respectively.

**Proof** The proof is given in “Appendix B”.

Although the above upper and lower bounds cannot tell us the exact SOP of the transmitter-receiver transmission, they are helpful for us to understand how the SOP varies with key system parameters. A larger upper bound or lower bound means a securer transmitter-receiver link.

#### 3.2 Secrecy outage probability

The SOP is a commonly-used performance metric to quantify the PHY security. In the performance analysis of large-scale systems, the exact SOP is usually unavailable, mainly due to the reason that the analysis involves computing highly cumbersome integrals in terms of the PPPs of both legitimate nodes and eavesdroppers. We therefore resort to applying the bounding technique used in [27]. We establish the following theorem to summarize the main results.

**Theorem 2** Consider a finite Poisson network with nodes distributed over a bi-dimensional disk \( \mathcal{B}(o, D) \) as illustrated in Fig. 1, the upper bound on the SOP of the transmitter-receiver pair under the friendship-based cooperative jamming scheme in Sect. 2.3 is given by
\[ P_{\text{so}}^{\text{UB}} = 1 - \exp \left\{ -2\pi\lambda_e \int_0^D e^{-\beta_e \pi r_e^2} \mathcal{L}^{A}_{I(z)}(\beta_e r_e^2) r_e \, dr_e \right\}, \]  
and the lower bound is given by
\[ P_{\text{so}}^{\text{LB}} = 2\pi\lambda_e \int_0^D e^{-\beta_e \pi r_e^2} e^{-\beta_e \pi z^2} \mathcal{L}^{A}_{I(z^*)}(\beta_e r_e^2) r_e \, dr_e, \]  
where \( \lambda_e \) denotes the density of eavesdroppers, \( \beta_e \) denotes the SINR threshold for successfully decoding of eavesdroppers, \( A = \{E, I, D\} \) denotes the long-range jammer selection policy, \( z^* \) represents the eavesdropper nearest to the transmitter \( o \), \( r_e \) denotes the distance from \( z^* \) to \( o \), and \( \mathcal{L}^{A}_{I(z)}(\cdot) \) and \( \mathcal{L}^{A}_{I(z^*)}(\cdot) \) are the Laplace transforms of the sum interference at \( z \) and \( z^* \), respectively.

**Proof** The proof is given in “Appendix B”.

Although the above upper and lower bounds cannot tell us the exact SOP of the transmitter-receiver transmission, they are helpful for us to understand how the SOP varies with key system parameters. A larger upper bound or lower bound means a securer transmitter-receiver link.

### 4 Laplace transform of the sum interference

In this section, the Laplace transform of the sum interference \( I(y) \) at any location \( y \in \mathcal{B}(o, D) \) is derived for all three long-range jammer selection policies. We first derive a general expression of the Laplace transform for all path loss exponent scenarios. Based on this expression, we then...
provide closed-from expressions for two typical path loss cases of $\alpha = 2$ and $\alpha = 4$.

### 4.1 General expression of $\mathcal{L}^A_I(s)$

**Theorem 3** Consider a finite Poisson network with nodes distributed over a bi-dimensional disk $B(0, D)$ as illustrated in Fig. 1, the Laplace transform of the sum interference $I(y)$ at any location $y \in B(0, D)$ under the friendship-based cooperative jamming scheme in Sect. 2.3 is given by

$$
\mathcal{L}^A_I(s) = \exp \left\{ -\lambda(s, y) + v(s, y) \right\},
$$

where $A = E, I, D$ denotes the long-range jammer selection policy,

$$
\mu(s, y) = 2 \int_0^{R_d} \int_0^{\pi} \frac{sr \cos \theta dr d\theta}{s + (r^2 + |y|^2 - 2r|y| \cos \theta)^{1/2}},
$$

and

$$
v(s, y) = 2 \int_{R_d}^{R_i} \int_0^{\pi} \frac{srP(r) \cos \theta dr d\theta}{s + (r^2 + |y|^2 - 2r|y| \cos \theta)^{1/2}}.
$$

**Proof** The proof is given in “Appendix C”. □

In general, it is difficult to derive $\mu(s, y)$ and $v(s, y)$ in closed form due to the path-loss exponent $\alpha$. We will show in the following subsection that closed-form expressions for $\mu(s, y)$ and $v(s, y)$ are available for special cases of $\alpha = 2$ and $\alpha = 4$.

### 4.2 Closed-form expression of $\mathcal{L}^A_I(s)$ for $\alpha = 2$ and $\alpha = 4$

Based on the general expression in Theorem 3, we derive the Laplace transform of $I(y)$ for the case of $\alpha = 2$ and $\alpha = 4$ in this subsection. The main results for $\alpha = 2$ are summarized in the following corollary.

**Corollary 1** For the case of $\alpha = 2$, the Laplace transform of the sum interference $I(y)$ under Policy $E$ is given by

$$
\mathcal{L}^{E,2}_I(s) = \exp \left\{ -\lambda \frac{s + R^2_s - |y|^2}{2|y| \sqrt{s}} + \frac{(1 - p) \sqrt{s}}{2|y| \sqrt{s}} - \ln \frac{\sqrt{s}}{|y|} \right\},
$$

where $\text{arcsinh} = \ln(t + \sqrt{t^2 + 1})$ denotes the inverse hyperbolic sine function. The Laplace transform of $I(y)$ under Policy $I$ and Policy $D$ is given by

$$
\mathcal{L}^{I,D,2}_I(s) = \exp \left\{ -\lambda \frac{\Psi_2^D(R_2, s, |y|) - \Psi_2^D(R_1, s, |y|)}{\eta(s, y)} + \frac{(1 - p) \sqrt{s}}{2|y| \sqrt{s}} - \ln \frac{\sqrt{s}}{|y|} \right\},
$$

where $\Psi_2^D(R_2, s, |y|)$ and $\Psi_2^D(R_1, s, |y|)$ are available for special cases of $\alpha = 4$ and $\alpha = 2$ are summarized in the following corollary.

**Corollary 2** For the case of $\alpha = 4$, the Laplace transform $\mathcal{L}^{E,4}_I(s)$ under Policy $E$ is given by

$$
\mathcal{L}^{E,4}_I(s) = \exp \left\{ -\lambda \frac{\pi}{2} \frac{\sqrt{s} + \psi(R_1, s, |y|)}{\eta(s, y)} + \frac{(1 - p) \sqrt{s}}{2|y| \sqrt{s}} - \ln \frac{\sqrt{s}}{|y|} \right\},
$$

where

$$
\eta(s, y) = \sqrt{\frac{g(r, s, |y|)^2 + 4s(r^2 + |y|^2)^2 + g(r, s, |y|)}{\sqrt{2}}},
$$

and

$$
\psi(r, s, |y|) = \frac{\sqrt{s} + |y|^2}{\eta(r, s, |y|)},
$$

and $\text{arctan}$ is the inverse tangent function. The Laplace transform of the sum interference $I(y)$ under Policy $I$ and Policy $D$ is given by

$$
\mathcal{L}^{I,D,4}_I(s) = \exp \left\{ -\lambda \frac{\pi}{2} \frac{\sqrt{s} + \psi(R_2, s, |y|)}{\eta(s, y)} + \frac{(1 - p) \sqrt{s}}{2|y| \sqrt{s}} - \ln \frac{\sqrt{s}}{|y|} \right\},
$$

and

$$
\psi(r, s, |y|) = \frac{\sqrt{s} + |y|^2}{\eta(r, s, |y|)},
$$

and $\text{arctan}$ is the inverse tangent function.
\[ L^{4A}_{I(\gamma)}(s) = \exp \left\{ -\lambda \pi s \left[ \frac{\pi}{2} - \arctan \frac{\sqrt{s + \psi(R_1, s, |y|)}}{\eta(R_1, s, |y|) + R_1^2 - |y|^2} \right] \right\} \]

\[ + \Psi^{4A}_4(R_2, s, |y|) - \Psi^{4A}_4(R_1, s, |y|) \}

where \( A' = I \) and \( D \).

\[ \Psi^{4}_{4}(r, s, |y|) = \frac{2\sqrt{\pi}|y|^2}{R^2 - R'^2} \ln \left[ (\eta(r, s, |y|) + r^2 - |y|^2) \right] \]

\[ + (\sqrt{s + \psi(r, s, |y|)}) \]

\[ - \frac{1}{2(R^2 - R'^2)} \left[ (r^2 + 3|y|^2)\psi(r, s, |y|) \right] \]

\[ - 3\sqrt{s}(r, s, |y|) \]

\[ + \frac{1}{R^2 - R'^2} \frac{4}{|y|^2} \arctan \frac{\sqrt{s + \psi(r, s, |y|)}}{\eta(r, s, |y|) + r^2 - |y|^2}. \]

**Proof** The proof is given in “Appendix F”.

**Corollary 3** For \( P(r) = 0 \), as \( R_1 \to \infty \), the Laplace transform of \( I(y) \) for the case of \( \alpha = 4 \) is

\[ L^{4A}_{I(\gamma)}(s) = \exp \left\{ -\lambda \sqrt{\pi s^2} \right\}, \]

which recovers the well-known Laplace transform of \( I(y) \) for a homogeneous infinite PPP with \( \alpha = 4 \) [23].

**Proof** Letting \( P(r) = 0 \) yields

\[ L^{4A}_{I(\gamma)}(s) = \exp \left\{ -\lambda \pi \sqrt{s} \left[ \frac{\pi}{2} - \arctan \frac{\sqrt{s + \psi(R_1, s, |y|)}}{\eta(R_1, s, |y|) + R^2 - |y|^2} \right] \right\}. \]

As \( R_1 \to \infty \),

\[ \lim \arctan \frac{\sqrt{s + \psi(R_1, s, |y|)}}{\eta(R_1, s, |y|) + R^2 - |y|^2} = \arctan \frac{2\sqrt{s}}{\infty - |y|^2} = 0, \]

which completes the proof.

### 5 Numerical results and discussions

In this section, we first conduct extensive simulations to verify the theoretical analysis of TOP and SOP, and then investigate how the parameters of the friendship-based cooperative jamming scheme affect the TOP and SOP performances of the legitimate transmission.

#### 5.1 Validation for TOP and SOP analysis

To capture the small-world properties of the network, we adopt the octopus friendship model in [22], where each node has both local friends and long-range friends. We only focus on the friends of the transmitter in the simulations. A simulator based on C++ was developed to simulate the PPPs \( \Phi \) and \( \Phi_E \), the friendship-based cooperative jamming model and the transmission process between the transmitter \( o \) and receiver \( y_0 \), which is now available at [38]. The PPP \( \Phi \) (\( \Phi_E \)) is simulated by applying the method in [37], where the first step is to generate two Poisson-distributed number \( M_1 \) and \( M_2 \) with mean \( \lambda D^2 \) and \( \lambda_e D^2 \) respectively, and the second step is to distribute \( M_1 \) legitimate nodes and \( M_2 \) eavesdroppers uniformly over the network \( B(o, D) \). The total number of transmissions is fixed as 100000 and the common transmit power is fixed as 1. The TOP is calculated as the ratio of the number \( n_o \) of transmissions with transmission outage to the total transmission number, i.e.,

\[ \text{TOP} = \frac{n_o}{1,000,000}. \]

Similarly, The SOP is calculated as

\[ \text{SOP} = \frac{n_{so}}{1,000,000}. \]

where \( n_{so} \) is the number of transmissions with secrecy outage.

Extensive simulations have been conducted to verify the theoretical analysis of TOP and SOP. We considered the cases of \( \alpha = 2 \) and \( \alpha = 4 \) and examined how the TOP and SOP vary with the density of legitimate nodes \( \lambda \) under three long-range jammer selection policies E, I and D. For both path loss cases, the network radius was fixed as \( D = 30 \) and the density of eavesdroppers was fixed as \( \lambda_e = 0.001 \). For the friendship-based cooperative jamming scheme, the radius of the LFC was fixed as \( R_1 = 1 \), the outer radius of
the LFA was fixed as $R_2 = 10$ and the selection probability in Policy E was set as $p = 0.1$. The SINR thresholds were fixed as $\beta = 0.5$ for the receiver $y_0$ and $\beta_e = 0.1$ for eavesdroppers. The transmitter-receiver distance was set as $l = 1$. For the case of $\alpha = 2$ and $\alpha = 4$, the normalized noise was fixed as $-20$ and $-50$ dB respectively. The corresponding simulation and theoretical results for TOP and SOP of three different policies are summarized in Fig. 4 for the case of $\alpha = 2$ and in Fig. 5 for the case of $\alpha = 4$. Notice that the theoretical results are calculated based on the Laplace transforms in Corollaries 1 and 2 for the case of $\alpha = 2$ and $\alpha = 4$ respectively.

Figures 4(a) and 5(a) indicate clearly that the simulation results of TOP match nicely with the theoretical ones, so our theoretical results can be applied to model the TOP performance of the concerned Poisson network under Policy E, Policy I and Policy D for the cases of $\alpha = 2$ and $\alpha = 4$. The results in Figs. 4(b–d) and 5(b–d) indicate that the simulation results of SOP are very close to the corresponding theoretical upper bounds, while they are different from the lower bounds, so our theoretical upper bounds can serve as accurate approximations for the exact SOP of the legitimate transmission under Policy E, Policy I and Policy D for the cases of $\alpha = 2$ and $\alpha = 4$. Another observation from Figs. 4 and 5 shows that the behaviors of TOP and SOP for $\alpha = 2$ and $\alpha = 4$ are similar, so we only focus on the case of $\alpha = 4$ in the following Sect. 5.2.

5.2 Performance analysis

We now explore how the TOP and SOP performances vary with the parameters of the friendship-based cooperative jamming scheme as well as other network parameters. Notice that all the theoretical results of the SOP are based on the corresponding upper bounds.

5.2.1 TOP and SOP versus $\lambda$

We first examine the impact of the density of legitimate nodes $\lambda$ on the TOP and SOP performances. It can be observed from Figs. 4 and 5 that the TOP increases as $\lambda$ increases, while the SOP decreases as $\lambda$ increases under all
policies E, I and D for both $\alpha = 2$ and $\alpha = 4$. This is very intuitive since a larger sum interference can be generated in the network as $k$ increases, resulting a worse transmitter-receiver channel and worse eavesdropper channels as well.

### 5.2.2 TOP and SOP versus $p$

We then show how the selection probability $p$ affect the TOP and SOP performances of Policy E. For the setting of $R_1 = 1$, $R_2 = 10$, $D = 30$, $\alpha = 4$, $\beta = 0.5$, $l = 1.0$ and $N_0 = -50$ dB, Fig. 6(a) illustrates how the TOP of Policy E varies with $\lambda$ under three different settings of $p = 0.1$, $p = 0.5$ and $p = 1.0$, which correspond to weak, moderate and strong long-range jamming scenarios respectively. Regarding the impact of $p$ on the SOP of Policy E, we show in Fig. 6(b) how the SOP of Policy E varies with $\lambda_e$ under three different settings of $p = 0.1$, $p = 0.5$ and $p = 1.0$ for the scenario of $R_1 = 1$, $R_2 = 10$, $D = 30$, $\alpha = 4$, $\beta_e = 0.1$, $\lambda = 1.0$ and $N_0 = -50$ dB. The TOP and SOP of Policy I and D are also plotted in Fig. 6(a, b) for the purpose of comparison. One can observe from Fig. 6 that as $p$ increases, the TOP increases while the SOP decreases, and we can flexibly control the selection probability $p$ to achieve various desired TOP and SOP performances that may not be achievable by the other two policies. One can also see from Fig. 6 that Policy I outperforms Policy D in terms of the TOP performance, while Policy D can ensure a better SOP performance than Policy I. This is due to the following two reasons. The first one is that Policy D has much more long-range jammers than Policy I, so it will generate more interference in the network, resulting in a better SOP performance but a worse TOP performance. The other reason is that the long-range jammers of Policy D are much closer to the transmitter than those of Policy I. Notice that near (i.e., close to the transmitter) eavesdroppers dominate the behavior of SOP, so Policy D is more effective to suppress near eavesdroppers than Policy I, achieving a better SOP performance. Another observation from Fig. 6(b) shows that as the density of eavesdroppers $\lambda_e$ increases, the SOP of all three policies increase, leading to a degraded security performance.
5.2.3 TOP and SOP versus $R_1$

We now investigate how the TOP and SOP performances are affected by the radius of LFC $R_1$, i.e., the inner radius of LFA. For the scenario of $l = 2.0$, $R_2 = 10$, $D = 30$, $\alpha = 4$, $\beta = 0.5$, $\lambda = 0.1$ and $N_0 = -50$ dB, Fig. 7(a) illustrates how the TOP varies with $R_1$ for Policy I, Policy D and Policy E with $p = 0.5$. We can see from Fig. 7(a) that the TOP first increases as $R_1$ increases, then saturates to a constant value and finally stays almost the same for all policies. The increasing behavior of TOP is because that the total number of jammers increases as $R_1$ increases, although the number of long-range jammers decreases, which results in a larger sum interference in the network. The behavior that TOP of all policies saturates to a same constant is due to the fact that all policies finally reach to the same jamming pattern at the point of $R_1 = R_2$. For the scenario of $R_2 = 10$, $D = 30$, $\alpha = 4$, $\beta = 0.1$, $\lambda = 0.001$, $\lambda = 0.1$ and $N_0 = -50$ dB, Fig. 7(b) shows how the SOP varies with $R_1$ for Policy I, Policy D and Policy E with $p = 0.5$. It can be observed from Fig. 7(b) that the SOP first decreases as $R_1$ increases, then saturates to a constant value and finally stays almost the same for all policies, which is due to the same reason as explained above. A careful observation from Fig. 7(a, b) indicates that the TOP and SOP performances of Policy I are the most sensitive to the variation of $R_1$, while those of the Policy D are the least sensitive. This is because that most of the long-range jammers in Policy I are located far from the LFC (as illustrated in Fig. 8), so increasing $R_1$ will greatly increase the total number of jammers. However, for Policy D, most of the long-range jammers are located near the LFC, so
increasing $R_1$ only results in a slight increase in the total number of jammers.

5.2.4 TOP and SOP versus $R_2$

Regarding the impact of the outer radius of LFA $R_2$ on the TOP performance, we show in Fig. 9(a) how the TOP varies with $R_2$ for Policy I, Policy D and Policy E with $p = 0.5$ under the settings of $l = 2$, $R_1 = 1$, $D = 30$, $\alpha = 4$, $\beta = 0.5$, $\lambda = 0.1$ and $N_0 = -50$ dB. As shown in Fig. 9(a), the TOP of Policy E and Policy D always monotonically increases as $R_2$ increases, but this is not the case for Policy I. The increasing behavior of TOP for all policies are because that the number of long-range jammers increases as $R_2$ increases, generating a larger sum interference in the network. The decreasing behavior of TOP for Policy I is due to that its long-range jammers are getting further away from the receiver as $R_2$ continues to increase, since the majority of these jammers are located in a small annulus region near the outer circle of the LFA, as we can deduce from (4). For the impact of $R_2$ on the SOP performance, we illustrate in Fig. 9(b) SOP versus $R_2$ for Policy I, Policy D and Policy E with $p = 0.5$. As expected, we can observe from Fig. 9(b) that the SOP decreases as $R_2$ increases for all policies.

5.2.5 SOP versus network radius $D$

We now explore how the SOP performance varies with the network radius $D$. For the scenario of $R_1 = 1$, $R_2 = 10$, $\alpha = 4$, $\beta = 0.1$, $\lambda = 0.001$, $\lambda = 0.1$ and $N_0 = -50$ dB, Fig. 10 illustrates how the SOP varies with $D$ for Policy I, Policy D and Policy E with $p = 0.5$. It is interesting to notice from Fig. 10 that the SOP increases as the network radius $D$ increases and finally stays almost unchanged for all policies. This is because that as $D$ increases, the number of near eavesdroppers that can cause a secrecy outage increases, resulting in an increase in the SOP first.
However, as $D$ continues to increase above some threshold (about 40 in Fig. 10), the newly-added eavesdroppers can hardly cause a secrecy outage due to the vanishing received SINR, and thus the SOP stays almost unchanged.

6 Related works

Extensive research efforts have been devoted to the PHY-security based secure communications of Poisson networks without the consideration of social relationships, which can be roughly categorized according to the network scenarios they considered.

In general Poisson networks, the locations of eavesdroppers and legitimate nodes are usually modeled as independent and homogeneous PPPs with different intensities. Some PHY-security properties of the networks were analyzed from the perspective of secrecy graph, like the secure connectivity, the maximum secrecy rate and secrecy outage probability of a single link [24, 25]. Modeling the additional interfering nodes as another independent homogeneous PPP, the authors in [26] explored some other PHY-security properties of the network, like secrecy rate density, secrecy rate outage density and secrecy throughput density. The dependence of the area spectral efficiency of Poisson networks on security and other parameters was studied in [27].

In traditional cellular networks, base stations and mobile users are usually modeled as independent and homogeneous PPPs. Recent efforts, such as [28, 29], have been devoted to study the average secrecy rate achievable for a randomly located mobile user and the related probability of secrecy outage. For the cellular networks with D2D users, the authors in [30] modeled the locations of base stations, cellular users, D2D users and eavesdroppers as four independent and homogeneous PPPs, and studied the connection probabilities and secrecy probabilities of both the cellular and D2D links.

It is notable that some recent works have also been reported on the study of PHY-security secure communications for other promising network scenarios, like cognitive networks [31] and cognitive networks with D2D communications [32].

7 Conclusion

This paper explored the physical layer security-based secure communications in a finite Poisson network with social friendship among nodes, for which a social friendship-based cooperative jamming scheme was proposed. The jamming scheme consists of a Local Friendship Circle (LFC) and a Long-range Friendship Annulus (LFA), where all legitimate nodes in the LFC serve as jammers, but the legitimate nodes in the LFA are selected as jammers through three location-based policies, namely, Policy E, Policy I and Policy D. To understand the security and reliability performances of the proposed jamming scheme, we analyzed its transmission outage probability (TOP) and secrecy outage probability (SOP) based on the Laplace transforms of the sum interference at any location in the network. The results in this paper indicated that, in general, Policy I outperforms Policy D in terms of the reliability performance, while Policy D can ensure a better security performance than Policy I. Also, we can flexibly control the reliability and security performances of Policy E by varying its long-range jammer selection probability. Another interesting observation can also be found that increasing the outer radius of the LFA beyond some threshold can improve both the reliability and security performances of the proposed jamming scheme.

This paper considered a location-based friendship model, which neglected some important social attributes like social similarity and interest. Thus, one possible future work is to integrate more social attributes into the design of cooperative jamming schemes. In addition, social attributes have also been widely considered for efficient information caching and diffusion in mobile networks [39–41], while the security performances therein remain largely unexplored. Thus, another possible research is to design secure socially-aware information caching and diffusion schemes for mobile networks. Notice that this paper considered a relatively simple homogeneous PPP-based system due to its mathematical tractability. To further explore the potentials of social relationships in enhancing the physical layer security performances of various wireless systems, we will consider more complex and practical system models in our future research, like the non-homogeneous PPP model.
Acknowledgements This work was supported in part by the Japan JSPS under Grant 15H02692 and the China NSFC under Grant 61571352, 61373173, and U1536202.

Appendix A: Proof of Theorem 1

From the definition of TOP in (6), we have
\[
p_{so} = P(\text{SINR}_{y_0} < \beta) \\
= P\left( \frac{h_{y_0} I^{-z}}{I(y_0) + N_0} < \beta \right) \\
= \mathbb{E}_{\Phi_I} \left[ P\left( \frac{h_{y_0} I^{-z}}{I(y_0) + N_0} < \beta | \Phi_I \right) \right] \\
= 1 - e^{-\beta N_0} \mathbb{E}_{\Phi_I} \left[ e^{-\beta |I(y_0)|} \right] \\
= 1 - e^{-\beta N_0} L_{(y_0)}^A(R^2),
\]
which completes the proof.

Appendix B: Proof of Theorem 2

From the definition of SOP in (7), we have
\[
p_{so} = P\left( \bigcup_{z \in \Phi_E} \text{SINR}_z > \beta_e \right) \\
= 1 - P\left( \bigcap_{z \in \Phi_E} \text{SINR}_z < \beta_e \right) \\
= 1 - \mathbb{E}_{\Phi_E} \left[ P\left( \bigcap_{z \in \Phi_E} \frac{h_{y_0} |z|^{-z}}{I(z) + N_0} < \beta_z | \Phi_E, \Phi_I \right) \right] \\
= 1 - \mathbb{E}_{\Phi_E} \left[ \prod_{z \in \Phi_E} \left( 1 - P\left( \frac{h_{y_0} |z|^{-z}}{I(z) + N_0} > \beta_z | \Phi_E, \Phi_I \right) \right) \right] \\
(\beta) 1 - \mathbb{E}_{\Phi_E} \left[ \exp\left( -\lambda_e \int_{B(o,D)} P\left( \frac{h_{y_0} |z|^{-z}}{I(z) + N_0} > \beta_z | \Phi_E, \Phi_I \right) dz \right) \right],
\]
where (a) follows since $h_{y_0}$, $z \in \Phi_E$ are i.i.d. random variables, and (b) follows after applying the probability generating functional of $\Phi_E$. Applying the Jensen’s Inequality yields the upper bound on $p_{so}$
\[
p_{so} \leq 1 - \exp\left\{ -\lambda_e \int_{B(o,D)} \mathbb{E}_{\Phi_E} \left[ P\left( \frac{h_{y_0} |z|^{-z}}{I(z) + N_0} > \beta_z | \Phi_I \right) \right] dz \right\} \\
= 1 - \exp\left\{ -2\pi \lambda_e \int_0^D e^{-\beta N_0 r^2} L_{\beta_e}^A(\beta_e r^2) r dr \right\}.
\]

The lower bound is obtained by considering only the eavesdropper $z^*$ nearest to the transmitter. Let $R_{z^*}$ denote the random distance between $z^*$ and $o$. The probability distribution function of $R_{z^*}$ can be given by
\[
f_{R_{z^*}}(r_{z^*}) = \begin{cases} 
2\pi \lambda_e e^{-\lambda_e t^2} e^{-\beta N_0 r_{z^*}^2}, & 0 \leq r_{z^*} \leq D \\
0, & \text{otherwise}
\end{cases}
\]

Please refer to “Appendix G” for the proof. The SOP can then be bounded from below by the probability that $z^*$ causes a secrecy outage, i.e.,
\[
p_{so} \geq P(\text{SINR}_{z^*} > \beta_e) \\
= \int_0^D \mathbb{E}_{\Phi_E} \left[ P\left( \frac{h_{o,z^*} r_{z^*}^2}{I(z^*) + N_0} > \beta_e \right) f_{R_{z^*}}(r_{z^*}) dr_{z^*} \right] \\
= 2\pi \lambda_e \int_0^D e^{-\lambda_e t^2} e^{-\beta N_0 r_{z^*}^2} L_{\beta_e}^A(\beta_e r_{z^*}^2) r_{z^*} dr_{z^*}.
\]

Appendix C: Proof of Theorem 3

According to the definition, the Laplace transform of $I(y)$ is given by
\[
L_{I(y)}^A(s) = \mathbb{E}_{\Phi_I} \left[ e^{-s I(y)} \right] \\
= \mathbb{E}_{\Phi_I} \left[ \exp\left( -s \sum_{x \in \Phi_E} h_{x,y} |x - y|^{-z} \right) \right] \\
= \mathbb{E}_{\Phi_I} \left[ \prod_{x \in \Phi_E} \exp\left( -s h_{x,y} |x - y|^{-z} \right) \right] \\
= \mathbb{E}_{\Phi_I} \left[ \prod_{x \in \Phi_E} \frac{1}{1 + s |x - y|^{-z}} \right],
\]
From the cooperative jamming scheme in Sect. 2.3, we can see that $\Phi_I$ is indeed an inhomogeneous PPP obtained by applying two independent thinning operations on $\Phi$. We now define the intensity measure of $\Phi_I$ by $A(\cdot)$, which gives the expected number of nodes in a given set. By applying the probability generating functional of $\Phi_I$, we have
\[
L_{I(y)}^A(s) = \exp\left\{ - \int_{B(o,D)} \left( 1 - \frac{1}{1 + s |x - y|^{-z}} \right) A(dx) \right\} \\
= \exp\left\{ - \int_{B(o,D)} \left( \frac{1}{1 + \frac{1}{1 + s |x - y|^{-z}}} \right) A(dx) \right\},
\]
where $A(dx)$ is given by
\[(33)\]
\[
A(dx) = \begin{cases} 
\lambda dx, & x \in A_1 \\
\lambda P(|x|)dx, & x \in A_2.
\end{cases}
\] \tag{34}

following from the thinning property of PPP. The term \( A \) in (33) can be rewritten as
\[
T = \lambda \int_{A_1} \left( \frac{\lambda}{1 - \lambda A_1} \right) dx + \lambda \int_{A_2} P(|x|)dx.
\] \tag{35}

Changing Cartesian coordinates to polar coordinates, we can rewrite the \( \mu(s, y) \) and \( v(s, y) \) as (12) and (13), respectively.

**Appendix D: Integral identities**

**Identity 1** For \( a, b \in \mathbb{R} \) and \( a > |b| \), we have from [42] and [43]
\[
\int_0^\pi \frac{d\theta}{(a + b \cos\theta)^{m+1}} = \frac{\pi P_m\left(\frac{a}{\sqrt{a^2 - b^2}}\right)}{(a^2 - b^2)^{m+1}},
\] \tag{36}

where \( P_n(\cdot) \) is the \( n \)-th Legendre polynomial and \( P_0(\cdot) = 1 \).

**Identity 2** Let \( a, b, c \in \mathbb{R} \) and \( c > 0 \). Defining \( Q = c^2 + bt + a \) and \( A = 4ac - b^2 \), we have from [42] and [43]
\[
\int \frac{dt}{\sqrt{Q}} = \frac{1}{\sqrt{c}} \ln\left(2\sqrt{cQ} + 2ct + b\right) \quad [c > 0]
\]
\[
= \frac{1}{\sqrt{c}} \arcsin\left(\frac{2ct + b}{\sqrt{A}}\right) \quad [c > 0, A > 0],
\] \tag{37}

**Identity 3** For \( m, n \in \mathbb{Z} \) and \( Q = c^2 + bt + a \), we have from [42]
\[
\int \frac{dQ}{\sqrt{Q^{2n+1}}} = \frac{1}{(m - 2)n!} \int \frac{d\theta}{\sqrt{\theta^{2n-1}}}
\]
\[
= \frac{(2m - 2n - 1)b}{2(m - 2)n!} \int \frac{d\theta}{\sqrt{\theta^{2n-1}}}
\]
\[
- \frac{(m - 1)a}{2(m - 2)n!} \int \frac{d\theta}{\sqrt{\theta^{2n-1}}}
\] \tag{38}

where \( a, b, c \in \mathbb{R} \) and \( c > 0 \).

**Appendix E: Proof of Corollary 1**

For \( \alpha = 2 \), we can rewrite the \( \mu(s, y) \) in (12) as
\[
\mu_2(s, y) = 2 \int_0^{R_1} \int_0^\pi \frac{srd\theta dr}{s^2 + r^2 + |y|^2 - 2sr|y|\cos\theta}.
\] \tag{39}

Applying Identity 1 in “Appendix D”, we have
\[
\mu_2(s, y) = \pi s \int_0^{R_1} \frac{2rdr}{\sqrt{r^4 + 2(s - |y|^2)r^2 + (s + |y|^2)^2}}
\]
\[
\equiv \pi s \int_0^{R_1} \frac{dt}{\sqrt{(t^2 + 2(s - |y|^2)t + (s + |y|^2)^2)}},
\] \tag{40}

where (c) follows from substituting \( r^2 \) with \( t \). We then apply Identity 2 in “Appendix D” and substitute \( t \) with \( r^2 \) to obtain
\[
\mu_2(s, y) = \pi s \left( \arcsinh \frac{s + R_1^2 - |y|^2}{2|y|\sqrt{s}} - \ln \frac{\sqrt{s}}{|y|} \right).
\] \tag{41}

Similarly, applying Identity 1, we can rewrite \( v(s, y) \) in (13) as
\[
v_2(s, y) = \pi s \int_{R_1}^{R_2} \frac{2rP(r)dr}{\sqrt{r^4 + 2(s - |y|^2)r^2 + (s + |y|^2)^2}}.
\] \tag{42}

For Policy E, \( P(r) = p \). Then,
\[
v_2(s, y) = \pi s \pi s \frac{p \text{sincsinh}}{p \text{sincsinh}} = \left. \begin{array}{c}
\frac{s + r^2 - |y|^2}{2|y|\sqrt{s}} \frac{R_1^2}{|y|} = \left. \frac{R_1^2}{R_1 - R_1^2} \right\} v = \frac{1}{\frac{R_1^2}{R_1 - R_1^2}} \right\}
\] \tag{43}

Substituting (43) and (41) into (35), and then substituting (35) into (33) yields (14). \( P(r) \) can be written as
\[
P(r) = u + vr^2, \quad u = -\frac{R_1^2}{R_1 - R_1^2}, \quad v = -\frac{1}{R_1 - R_1^2} \text{ for Policy I,}
\]
\[
\text{and } u = \frac{R_1^2}{R_1 - R_1^2}, \quad v = \frac{1}{R_1 - R_1^2} \text{ for Policy D. Hence,}
\]
\[
v_2(s, y) = \pi s \int_{R_1}^{R_2} \frac{2r(r + vr^2)dr}{\sqrt{r^4 + 2(s - |y|^2)r^2 + (s + |y|^2)^2}}
\]
\[
= \pi s \left[ u \int_{R_1}^{R_2} \frac{rdr}{\sqrt{r^2 + 2(s - |y|^2)t + (s + |y|^2)^2}}
\]
\[
+ v \int_{R_1}^{R_2} \frac{rdr}{\sqrt{r^2 + 2(s - |y|^2)t + (s + |y|^2)^2}} \right]
\]
\[
= \pi s \left[ \left( u + v \frac{s + t - |y|^2}{2|y|\sqrt{s}} \right) \arcsinh \frac{s + t - |y|^2}{2|y|\sqrt{s}} + \pi s \right]_{t = R_1^2}.
\] \tag{44}

where (d) follows from applying Identity 2 and 3. Substituting \( t \) with \( r^2 \), we have
\[ v_2(s, y) = \pi s \left[ (u - vs + v|y|^2) \text{arcsinh} \frac{s + r^2 - |y|^2}{2|y|\sqrt{s}} + \sqrt{s + 2(s - |y|^2)r^2 + (s + |y|^2)^2} \right]_{r=R_1}^{R_2} \]

Finally, we substitute (41) and (45) with into (35), and then substitute (35) into (33) to obtain (15).

**Appendix F: Proof of Corollary 2**

For \( \alpha = 4 \), we can rewrite \( \mu(s, y) \) in (12) as

\[ \mu_4(s, y) = \pi \int_0^{R_1} \int_0^{\pi} \frac{srd\theta dr}{(s + (r^2 + |y|^2 - 2r|y|\cos \theta)^2)} \]

\[ = 2 \int_0^{R_1} \sqrt{s} d\theta \int_0^{\pi} \frac{2dr}{(s + (r^2 + |y|^2 - 2r|y|\cos \theta - i \sqrt{s})^2)} \]

\[ = \frac{\pi \sqrt{s}}{2i} \ln \left[ \frac{C_1 + r^2 - (i \sqrt{s} + |y|^2)}{C_2 + r^2 + (i \sqrt{s} - |y|^2)} \right]_{r=0}^{R_1} \]

where (e) follows from applying Identity 1, (f) follows from applying Identity 2,

\[ C_1 = (r^2 - |y|^2)^2 - s - 2i\sqrt{s}(r^2 + |y|^2), \]  

and \( C_2 = C_1^* \) is the complex conjugate of \( C_1 \). Now, we rewrite \( C_1 \) as

\[ C_1 = (\eta - i\psi)^2 = \eta^2 - \psi^2 - 2i\eta\psi, \]

for some real-valued functions \( \eta(r, s, |y|) \) and \( \psi(r, s, |y|) \). We can then establish the following equation system

\[ \begin{cases} 
\eta^2 - \psi^2 &= (r^2 - |y|^2)^2 - s \\
\eta\psi &= \sqrt{s}(r^2 + |y|^2) 
\end{cases} \]

(19) and (20) then follow from solving the above equation system. For simplicity of notation, we also use \( \eta \) and \( \psi \) to represent \( \eta(r, s, |y|) \) and \( \psi(r, s, |y|) \), respectively. Given \( C_1 \) as in (48),

\[ \mu_4(s, y) = \pi \int_0^{R_1} \frac{\eta + r^2 - |y|^2 - i(\sqrt{s} + \psi)}{2i} \]

\[ = \pi \int_0^{R_1} \frac{1 - i - \sqrt{s} + \psi}{\eta + r^2 - |y|^2} \]

\[ = - \pi \sqrt{s} \arctan \frac{\sqrt{s} + \psi}{\eta + r^2 - |y|^2} \]

(51)

where (g) follows from

\[ \lim_{r \to 0} \arctan \frac{\sqrt{s} + \psi}{\eta + r^2 - |y|^2} = \arctan \infty = \frac{\pi}{2} \]

(52)

Similarly, applying Identity 1, we can rewrite \( \nu(s, y) \) in (13) as

\[ \nu_4(s, y) = \pi \int_0^{R_1} \frac{2rP(r)dr}{\sqrt{C_1}} - \frac{2rP(r)dr}{\sqrt{C_2}} \]

(53)

For Policy E, \( P(r) = p \in [0, 1] \). Then,

\[ v_4(s, y) = -p \pi \sqrt{s} \arctan \frac{\sqrt{s} + \psi}{\eta + r^2 - |y|^2} \]

(54)

Substituting (54) and (51) into (35) and then substituting (35) into (33) yields (18). \( P(r) \) can be written as

\[ P(r) = u + vr^4, \]

where \( u = -\frac{R_1^2}{R_2^2 - R_1^2}, v = \frac{1}{R_2^2 - R_1^2} \) for Policy I, and \( u = \frac{R_1^2}{R_2^2 - R_1^2}, v = -\frac{1}{R_2^2 - R_1^2} \) for Policy D. Hence,

\[ \nu_4(s, y) = \pi \int_0^{R_1} \frac{2r(u + vr^4)dr}{\sqrt{C_1}} - \frac{2r(u + vr^4)dr}{\sqrt{C_2}} \]

\[ = \frac{\pi \sqrt{s}}{2i} \int_0^{R_1} \frac{(u + vr^2)dr}{\sqrt{\sqrt{r^2 - 2(i\sqrt{s} + |y|^2)r + (|y|^2 - i\sqrt{s})^2}}} \]

(55)

where (h) follows from substituting \( r^2 \) with \( t \). Next, we have
\[
\int \frac{(u + vr^2)dt}{\sqrt{t^2 - 2(i\sqrt{s} + |y|^2)t + (|y|^2 - i\sqrt{s})^2}} = u \int \frac{dt}{\sqrt{t^2 - 2(i\sqrt{s} + |y|^2)t + (|y|^2 - i\sqrt{s})^2}} + v \int \frac{r^2dt}{\sqrt{t^2 - 2(i\sqrt{s} + |y|^2)t + (|y|^2 - i\sqrt{s})^2}}
\]

(56)

where \(i\) follows from applying Identity 3 in “Appendix D” and substituting \(t\) with \(r^2\). Similarly, we have

\[
\int \frac{(u + vr^2)dt}{\sqrt{t^2 - 2(i\sqrt{s} - |y|^2)t + (|y|^2 + i\sqrt{s})^2}} = \frac{v}{2} \int (r^2 + 3|y|^2 - 3i\sqrt{s})(\eta + iv\psi) + (u + vr^2 - vs - 4i\sqrt{s}|y|^2) \ln \left[ \sqrt{C_2 + r^2 - (i\sqrt{s} + |y|^2)} \right].
\]

(57)

Thus, substituting (56) and (57) into (55) and then conducting some algebraic manipulations yields

\[
v_4(s, y) = 2\pi y^2 |y|^2 \ln \left[ \left( \eta(r, s, |y|) + r^2 - |y|^2 + (\sqrt{s} + \psi(r, s, |y|)) \right) \right. \\
- \pi \sqrt{s} \left. \left\{ \frac{v}{2} \left( r^2 + 3|y|^2 \right) \psi(r, s, |y|) - 3\sqrt{s} \eta(r, s, |y|) \right\} \right]^{\frac{C_1 + r^2 - (i\sqrt{s} + |y|^2)}{C_2 + r^2 - (i\sqrt{s} + |y|^2)}},
\]

(58)

Finally, we substitute (51) and (58) into (35), and then substitute (35) into (33) to obtain (21).

**Appendix G: Probability density function of \(R_c\)**

The CCDF \(F_{R_c}(r_c)\) of the random distance \(R_c\) equals the probability that no eavesdroppers are in \(B(o, r_c)\) for \(0 \leq r_c \leq D\). Hence, the CDF of \(R_c\) is given by

\[
F_{R_c}(r_c) = 1 - \Phi_E(B(o, r_c)) = 0
\]

\[
= 1 - \sum_{n=0}^{\infty} \Phi_E(B(o, r_c)) = 0 \Phi_E(B(o, D)) = n
\]

\[
= 1 - \sum_{n=0}^{\infty} \left( 1 - \frac{r_c^n}{n!} \right) \exp(-\lambda_r \pi D^2)
\]

\[
= 1 - \exp(-\lambda_r \pi D^2) \sum_{n=0}^{\infty} \left( 1 - \frac{r_c^n}{n!} \right) \exp(-\lambda_r \pi D^2)
\]

\[
= 1 - \exp(-\lambda_r \pi D^2) \exp \left[ 1 - \frac{r_c^n}{n!} \right] \exp(-\lambda_r \pi D^2)
\]

\[
f_{R_c}(r_c) = \left\{ \begin{array}{ll}
2\lambda_r \pi r_c \exp(-\lambda_r \pi r_c^2), & 0 \leq r_c \leq D \\
0, & \text{otherwise}
\end{array} \right.
\]

(60)

**References**

1. Kayastha, N., Niyato, D., Ping Wang, & Hossain, E. (2011). Applications, architectures, and protocol design issues for mobile social networks: A survey. *Proceedings of the IEEE*, 99(12), 2130–2158.

2. Qin, Y., Jia, R., Zhang, J., Wu, W., & Wang, X. (2016). Impact of social relation and group size in multcast ad hoc networks. *IEEE/ACM Transactions on Networking*, 14(3), 609–621.

3. Zhang, Y., Pan, E., Song, L., Saad, W., Dawy, Z., & Han, Z. (2015). Social network aware device-to-device communication in wireless networks. *IEEE Transactions on Wireless Communications*, 14(1), 177–190.

4. Chen, X., & Huang, J. (2015). Imitation-based social spectrum sharing. *IEEE Transactions on Mobile Computing*, 14(6), 1189–1202.

5. Xia, F., Liu, L., Li, J., Ma, J., & Vasilakos, A. V. (2015). Socially aware networking: A survey. *IEEE Systems Journal*, 9(3), 904–921.

6. Shiue, Y.-S., Chang, S. Y., Wu, H.-C., Huang, S. C. H., & Chen, H.-H. (2011). Physical layer security in wireless networks: A tutorial. *IEEE Wireless Communications*, 18(2), 66–74.

7. Liang, X., Zhang, K., Shen, X., & Lin, X. (2014). Security and privacy in mobile social networks: Challenges and solutions. *IEEE Wireless Communications*, 21(1), 33–41.

8. Hayajneh, T., Almasahqeh, G., & Ullah, S. (2015). A green approach for selfish misbehavior detection in 802.11-based wireless networks. *Mobile Networks and Applications*, 20(5), 623–635.

9. Hayajneh, T., Almasahqeh, G., Ullah, S., & Vasilakos, A. V. (2014). A survey of wireless technologies coexistence in WBAN: Analysis and open research issues. *Wireless Networks*, 20(8), 2165–2199.

10. Hayajneh, T., Krishnamurthi, P., Tipper, D., & Kim, T. (2009). Detecting malicious packet dropping in the presence of collisions and channel errors in wireless ad hoc networks. In *IEEE International Conference on Communications, 2009. ICC’09* (pp. 1–6). IEEE.
11. Panyim, K., Hayajneh, T., Krishnamurthy, P., & Tipper, D. (2009). On limited-range strategic/random jamming attacks in wireless ad hoc networks. In IEEE 34th Conference on Local Computer Networks, 2009. LCN '09 (pp. 922–929). IEEE.
12. Stallings, W. (2010). Cryptography and network security: Principles and practice (5th ed.). Upper Saddle River: Prentice Hall.
13. Mohd, B. J., Hayajneh, T., & Vasilakos, A. V. (2015). A survey on lightweight block ciphers for low-resource devices. Journal of Network and Computer Applications, 58, 73–93.
14. Bloch, M., & Barros, J. (2011). Physical-layer security: From information theory to security engineering. Cambridge: Cambridge University Press.
15. Mukherjee, A., Fakoorian, S. A. A., Huang, J., & Swindlehurst, A. L. (2014). Principles of physical layer security in multiuser wireless networks: A survey. IEEE Communications Surveys & Tutorials, 16(3), 1550–1573.
16. Yang, N., Wang, L., Geraci, G., Elkashlan, M., Yuan, J., & Di Renzo, M. (2015). Safeguarding 5G wireless communication networks using physical layer security. IEEE Communications Magazine, 53(4), 20–27.
17. Wang, L., Cao, C., & Huaqing, W. (2015). Secure inter-cluster communications with cooperative jamming against social outcasts. Computer Communications, 63, 1–10.
18. Zhang, Y., Shen, Y., Wang, H., Zhang, Y., & Jiang, X. (2018). On secure wireless communications for service oriented computing. IEEE Transactions on Services Computing, 11(2), 318–328.
19. Zhang, Y., Shen, Y., Wang, H., Yong, J., & Jiang, X. (2016). On secure wireless communications for IoT under eavesdropper collusion. IEEE Transactions on Automation Science and Engineering, 13(3), 1281–1293.
20. Tang, L., Chen, H., & Li, Q. (2015). Social tie based cooperative jamming for physical layer security. IEEE Communications Letters, 19(10), 1790–1793.
21. Kleinberg, J. (2000). The small-world phenomenon: An algorithmic perspective. In Proceedings of the Thirty-second Annual ACM Symposium on Theory of Computing, STOC ’00 (pp. 163–170).
22. Inalchekin, H., Chiang, M., & Poor, H. V. (2014). Delay of social search on small-world graphs. The Journal of Mathematical Sociology, 38(1), 1–46.
23. Haenggi, M., & Ganti, R. K. (2009). Interference in large wireless networks. Foundations and Trends in Networking, 3(2), 127–248.
24. Pinto, P. C., Barros, J., & Win, M. Z. (2012). Secure communication in stochastic wireless networks—Part I: Connectivity. IEEE Transactions on Information Forensics and Security, 7(1), 125–138.
25. Pinto, P. C., Barros, J., & Win, M. Z. (2012). Secure communication in stochastic wireless networks—Part II: Maximum rate and collusion. Information Forensics and Security, 7(1), 139–147.
26. Rabbachin, A., Conti, A., & Win, M. Z. (2015). Wireless network intrinsic secrecy. IEEE/ACM Transactions on Networking, 23(1), 56–69.
27. Zhou, X., Ganti, R. K., Andrews, J. G., & Hjorungnes, A. (2011). On the throughput cost of physical layer security in decentralized wireless networks. IEEE Transactions on Wireless Communications, 10(8), 2764–2775.
28. Wang, H., Zhou, X., & Reed, M. C. (2013). Physical layer security in cellular networks: A stochastic geometry approach. IEEE Transactions on Wireless Communications, 12(6), 2776–2787.
29. Geraci, G., Dhillon, H. S., Andrews, J. G., Yuan, J., & Collings, I. B. (2014). Physical layer security in downlink multi-antenna cellular networks. IEEE Transactions on Communications, 62(6), 2006–2021.
Yuanyu Zhang received his B.S. degree in Software Engineering and M.S. degree in Computer Science from Xidian University, Xi’an, China, in 2011 and 2014, respectively, and received his Ph.D. degree at the School of Systems Information Science, Future University Hakodate, Hokkaido, Japan in 2017. He is currently working as an assistant professor at the Graduate School of Science and Technology, Nara Institute of Science and Technology, Japan. His research interests include physical layer security of wireless communications, performance modeling and evaluation of wireless networks and blockchain.

Yulong Shen received the B.S. and M.S. degrees in Computer Science and Ph.D degree in Cryptography from Xidian University, Xian, China, in 2002, 2005, and 2008, respectively. He is currently a professor at the School of Computer Science and Technology, Xidian University, China. He is also an associate director of the Shaanxi Key Laboratory of Network and System Security and a member of the State Key Laboratory of Integrated Services networks Xidian University, China. He has also served on the technical program committees of several international conferences, including ICEBE, INCoS, CIS and SOWN. His research interests include Wireless network security and cloud computing security.

Xiaohong Jiang received his B.S., M.S. and Ph.D degrees in 1989, 1992, and 1999 respectively, all from Xidian University, China. He is currently a full professor of Future University Hakodate, Japan. Before joining Future University, Dr. Jiang was an Associate professor, Tohoku University, from February 2005 to March 2010. Dr. Jiang’s research interests include computer communications networks, mainly wireless networks and optical networks, network security, routers/switches design, etc. He has published over 260 technical papers at premium international journals and conferences, which include over 50 papers published in top IEEE journals and top IEEE conferences, like IEEE/ACM Transactions on Networking, IEEE Journal of Selected Areas on Communications, IEEE Transactions on Parallel and Distributed Systems, IEEE INFOCOM. Dr. Jiang was the winner of the Best Paper Award of IEEE HPCC 2014, IEEE WCNC 2012, IEEE WCNC 2008, IEEE ICC 2005-Optical Networking Symposium, and IEEE/IEICE HPSR 2002. He is a Senior Member of IEEE, a Member of ACM and IEICE.