Cooperative Jamming for Secrecy in Decentralized Wireless Networks

Xiangyun Zhou*, Meixia Tao†, and Rodney A. Kennedy*
*Research School of Engineering, The Australian National University, Australia
†Department of Electronic Engineering, Shanghai Jiaotong University, P. R. China
Email: xiangyun.zhou@anu.edu.au, mxtao@sjtu.edu.cn, rodney.kennedy@anu.edu.au

***Abstract*—Cooperative jamming as a physical layer security enhancement has recently drawn considerable attention. While most existing works focus on communication systems with a small number of nodes, we investigate the use of cooperative jamming for providing secrecy in large-scale decentralized networks consisting of randomly distributed legitimate users and eavesdroppers. A modified slotted ALOHA protocol, named CJ-ALOHA, is considered where each legitimate transmitter either sends its message signal or acts as a helping jammer according to a message transmission probability p. We derive the secrecy transmission capacity to characterize the network throughput and show how the throughput is affected by the CJ-ALOHA protocol. Both analytical and numerical insights are provided on the design of the CJ-ALOHA protocol for optimal throughput performance.**

I. Introduction

Guaranteeing security in wireless networks is a fundamental challenge due to the broadcast nature of the communication medium. The commonly used encryption-based approaches rely on high computational complexity to provide secrecy without exploiting the properties of the wireless channels. On the other hand, the notion of physical layer security was developed from information-theoretic studies where "perfect" secrecy can be achieved by properly designing the encoder-decoder pair according to the channel capacities [1, 2]. Many recent works have been devoted to new physical layer security enhancements using advanced wireless technologies.

This paper focuses on one important physical layer security enhancement named cooperative jamming [3]: The secrecy of communication between the legitimate transmitter-receiver pair is improved by having external helper(s) simultaneously send independent signals to confuse the eavesdropper. The authors in [4, 5] studied the case of a single helper who can increase the secrecy capacity or achievable secrecy rate of the legitimate link by sending codewords independent of the transmitted messages. When the wireless channels are affected by small-scale fading, the availability of the channel state information (CSI) must be taken into account in designing the helper's strategy. The authors in [6] designed various strategies of the helping jammer based on different CSI assumptions and showed their impact on the secrecy performance. The case of multiple helping jammers was considered in [7–9], where the jammers transmit noise signals in a cooperative manner to maximize the achievable secrecy rate. Moreover, the helpers may also come from the internal users of the communication system. For example, the users having poor channel conditions in a multiple access scenario can transmit jamming signals instead of their message signals to improve the secrecy rates of the users with better channels [10].

While most of the works on cooperative jamming considered systems with a small number of nodes, very few studies have been carried out for large-scale networks. Unlike point-to-point communications where it is often easy to exchange secret keys which enables encrypted transmissions, security is more expensive and difficult to achieve in large-scale decentralized networks. Hence, the study of physical layer security becomes important in such networks. In this work, we study networks having both legitimate and eavesdropper nodes whose locations follow independent homogeneous Poisson point processes (PPPs) and consider a slotted ALOHA protocol with cooperative jamming (CJ-ALOHA). Specifically, each potential transmitter is allowed to transmit the message signal with probability p. Whenever the message transmission is not allowed, the transmitter acts as a helping jammer instead and emits a noise signal.

The recent work in [11] developed a notion of secrecy transmission capacity to characterize the secrecy throughput of large-scale networks with Poisson distributed nodes. A major assumption in [11] was that eavesdroppers do not have any successive decoding capability and hence treat concurrent message transmissions as noise. From an information-theoretic viewpoint, this assumption is often too optimistic. In this work, we consider a worst-case scenario where eavesdroppers do have successive decoding capability. The CJ-ALOHA protocol is hence introduced to provide secrecy, since the random jamming signals cannot be resolved by the eavesdroppers. The CJ-ALOHA protocol can be easily implemented in decentralized wireless networks, as no inter-node coordination or location knowledge is required. We use the secrecy transmission capacity to characterize the network throughput. A closed-form expression of the secrecy transmission capacity is derived, which allows us to numerically optimize the design parameters of the CJ-ALOHA protocol, *i.e.*, the message transmission probability p and the ratio of the jamming power to the message transmission power. In the case where the power for jamming and message transmission is fixed to the same level, we also derive an analytical result on the optimal transmission

This work was supported by the Australian Research Council's Discovery Projects funding scheme (project no. DP110102548).

978-1-4577-2053-6/12/$31.00 ©2012 IEEE

probability that maximizes the secrecy transmission capacity.

The works in [12, 13] are relevant to ours in the way that cooperative jamming was studied in large-scale networks with Poisson distributed nodes. In [12], the jammers and eavesdroppers are distributed according to independent PPPs, whereas only a single legitimate transmitter-receiver pair is considered. In contrast, we allow message transmissions to take place between all the transmitter-receiver pairs and study the network throughput taking interference into account. The authors in [13] considered the transmissions between all the node pairs and derived secrecy capacity scaling laws, *i.e.*, the order-of-growth of the secrecy capacity as the number of nodes increases. In comparison, we provide a finer view of the network throughput to better understand the impacts of system parameters and transmission protocols, since most such design choices affect the throughput but not the scaling behaviors [14].

II. System Model

We consider an ad hoc network having both legitimate and eavesdropper nodes over a large two-dimensional area. We model the locations of all legitimate transmitters as a homogeneous PPP Φ_l with density λ_l. This is a suitable model for decentralized networks with nodes having substantial mobility [15]. The network employs a slotted ALOHA protocol, that is, each transmitter is allowed to actually transmit the message signal with probability p in each time slot. Hence, the locations of the actual transmitters in any time slot follow a homogeneous PPP Φ_T with density $p\lambda_l$. Each transmitter has an intended receiver at a distance r in a random direction[1]. In addition, the locations of the eavesdroppers are also drawn according to another homogeneous PPP Φ_e with density λ_e. Note that the eavesdroppers need to have similar mobility and other behaviors as the legitimate nodes since they can be easily identified otherwise [16]. Furthermore, we assume that the eavesdroppers do not collude and, hence, must decode the messages individually.

In this work, we modify the slotted ALOHA protocol to include cooperative jamming: In each time slot, the legitimate transmitters at Φ_l are classified into actual transmitters and helping jammers, whose locations are denoted as Φ_T and Φ_J, respectively, with $\Phi_T \bigcup \Phi_J = \Phi_l$. Note that Φ_J is also a homogeneous PPP with density $(1-p)\lambda_l$. The nodes at Φ_J transmit jamming signals in order to improve the secrecy of the message transmissions from nodes at Φ_T. We call this protocol CJ-ALOHA. When the transmit power is allowed to vary, we denote the power for message transmission as $\mathcal{P}_T$ and the power for jamming as $\mathcal{P}_J$, which are the same for all transmitters.

The signal propagation through the wireless medium is affected by the large-scale path loss as well as the small-scale fading. In this work, we consider a path loss exponent of $\alpha > 2$ and Rayleigh fading channels. The instantaneous CSI is known at the receiver side (including the legitimate receivers and the eavesdroppers) but not at the transmitter side. Thermal noise is assumed to be negligible as compared to the aggregate jamming noise at the receiver side. Hence, the detection performance is characterized by the signal-to-interference ratio (SIR).

A. Secrecy Transmission Capacity

The notion of secrecy transmission capacity was developed in [11], which characterizes the area spectral efficiency of secure communication in decentralized wireless networks. The well-known Wyner's encoding scheme was assumed in deriving the secrecy transmission capacity. Specifically, the Wyner code requires the transmitter to choose two rates, namely, the codeword rate R_t and the secrecy data rate R_s, with the rate redundancy $R_e = R_t - R_s$ representing the cost of securing the message against eavesdropping. Detailed descriptions of Wyner's encoding scheme can be found in [1, 17, 18]. For any given R_t and R_s, the following outage events can result from any transmission [11, 18]:

- *Connection Outage*: The capacity of the channel from the transmitter to the intended receiver is below the codeword rate R_t. Hence, the message cannot be correctly decoded by the intended receiver. The probability of this event happening is referred to as the *connection outage probability*, denoted as P_{co}.
- *Secrecy Outage*: The capacity of the channel from the transmitter to one or more eavesdroppers is above R_e. Hence, the message is not perfectly secure against eavesdropping. The probability of this event happening is referred to as the *secrecy outage probability*, denoted as P_{so}.

The connection outage probability can be regarded as the communication quality of service (QoS) while the secrecy outage probability gives a measure of the security level.

Formally, the secrecy transmission capacity is defined as the achievable rate of successful transmission of confidential messages per unit area, with a given connection outage probability $\mathrm{P}_{\mathrm{co}} = \sigma$ and a given secrecy outage probability $\mathrm{P}_{\mathrm{so}} = \epsilon$ [11]:

$$\tau = R_s(1-\sigma)p\lambda_l, \qquad (1)$$

where $(1-\sigma)p\lambda_l$ is the density of successful message transmissions. The secrecy data rate $R_s = [R_t - R_e]^+$, where $[a]^+ = \max\{0, a\}$, is a function of both σ and ϵ. Specifically, σ determines R_t and ϵ determines R_e. Whenever $R_t - R_e$ is negative, message transmission needs to be suspended.

III. Secrecy Transmission Capacity with Cooperative Jamming

In this section, we derive analytical results on the secrecy transmission capacity for networks using the CJ-ALOHA protocol. Our analysis conditions on having a typical transmitter-receiver pair at some specific locations. From Slivnyak's Theorem [19], the conditional distributions of all other node locations are the same as the original (unconditional) ones.

[1] A discussion on variable distance transmission can be found in [11].

Consider the message transmission from the typical transmitter, we assume that the typical receiver, located at the origin, treats the interference from all other nodes in Φ_l as noise. Hence, a connection outage occurs if $\log_2(1 + \mathrm{SIR}_0) < R_t$, where SIR_0 denotes the SIR at the typical receiver given by

$$\mathrm{SIR}_0 = \frac{\mathcal{P}_T S_0 r^{-\alpha}}{\mathcal{P}_T \sum_{x \in \Phi_T} S_x \|x\|^{-\alpha} + \mathcal{P}_J \sum_{y \in \Phi_J} S_y \|y\|^{-\alpha}}, \quad (2)$$

where S_0 and r are the channel fading gain and the distance between the typical transmitter and receiver, respectively, S_x (S_y) and $\|x\|$ ($\|y\|$) are the channel fading gain and the distance between the interferer at x (y) and the typical receiver, respectively. The fading gains are independent and identically distributed (i.i.d.) exponential random variables with unit mean.

Define a threshold SIR value for connection outage as

$$\beta_t = 2^{R_t} - 1. \quad (3)$$

Hence, the connection outage probability can be written as

$$\begin{aligned}\mathrm{P}_{\mathrm{co}} &= \mathbb{P}\Big(\mathrm{SIR}_0 < \beta_t\Big)\\ &= \mathbb{P}\left(\frac{\mathcal{P}_T S_0 r^{-\alpha}}{\mathcal{P}_T \sum_{x \in \Phi_T} S_x \|x\|^{-\alpha} + \mathcal{P}_J \sum_{y \in \Phi_J} S_y \|y\|^{-\alpha}} < \beta_t\right),\end{aligned} \quad (4)$$

where $\mathbb{P}(.)$ denotes the probability measure.

Lemma 1: The connection outage probability is given by

$$\mathrm{P}_{\mathrm{co}} = 1 - \exp\left[-\lambda_l \pi r^2 \beta_t^{2/\alpha} \Gamma\Big(1 - \frac{2}{\alpha}\Big)\Gamma\Big(1 + \frac{2}{\alpha}\Big)\nu_1\right]. \quad (5)$$

where $\nu_1 = p + (1-p)(\mathcal{P}_J/\mathcal{P}_T)^{2/\alpha}$.

Proof: The probability in the same form as in (4) often appears in the literature of stochastic geometry. The derivation can be obtained, for example, by following the proof of Lemma 2 in [20]. The key step is using the fact that the interference term in (2) is the sum of two independent shot noise processes in two-dimensional space and their Laplace transforms are known in closed forms [21]. We omit the derivation here for brevity. ■

With the connection outage constraint given by $\mathrm{P}_{\mathrm{co}} = \sigma$, the codeword rate R_t can be found using (3) and (5) as

$$R_t = \log_2\left(1 + \left[\frac{\ln \frac{1}{1-\sigma}}{\lambda_l \pi r^2 \Gamma\big(1 - \frac{2}{\alpha}\big)\Gamma\big(1 + \frac{2}{\alpha}\big)\nu_1}\right]^{\frac{\alpha}{2}}\right). \quad (6)$$

Apart from the intended receiver that is listening to the message transmission, all the eavesdroppers also try to intercept the message at the same time. We consider the worst case scenario where only the jamming signals from Φ_J are not resolvable and hence treated as noise by the eavesdroppers. For the message transmission from the typical transmitter at the origin[2], the message is not perfectly secure against the eavesdropper at z in Φ_e if $\log_2(1 + \mathrm{SIR}_z) > R_e$, where SIR_z denotes the SIR at z given by

$$\mathrm{SIR}_z = \frac{\mathcal{P}_T S_z \|z\|^{-\alpha}}{\mathcal{P}_J \sum_{y \in \Phi_J} S_{yz} \|y - z\|^{-\alpha}}, \quad (7)$$

where S_z and $\|z\|$ are the channel fading gain and the distance between the typical transmitter and eavesdropper at z, respectively, S_{yz} and $\|y - z\|$ are the channel fading gain and the distance between the jammer at y and eavesdropper at z, respectively. Again, the fading gains are i.i.d. exponential random variables with unit mean.

Define a threshold SIR value for secrecy outage as

$$\beta_e = 2^{R_e} - 1. \quad (8)$$

Let $A = \{x \in \Phi_e : \mathrm{SIR}_x > \beta_e\}$ be the set of eavesdroppers that can cause a secrecy outage. Define an indicator function $1_A(z)$, which equals 1 when the eavesdropper at z is in the set A. The secrecy outage probability equals the probability that at least one of the eavesdroppers in Φ_e belongs to A, which can be written as

$$\begin{aligned}\mathrm{P}_{\mathrm{so}} &= 1 - \mathbb{E}_{\Phi_J}\Big\{\mathbb{E}_{\Phi_e}\Big\{\mathbb{E}_S\Big\{\prod_{z \in \Phi_e}\Big(1 - 1_A(z)\Big)\Big\}\Big\}\Big\},\\ &= 1 - \mathbb{E}_{\Phi_J}\Bigg\{\mathbb{E}_{\Phi_e}\Bigg\{\\ &\prod_{z \in \Phi_e}\Bigg(1 - \mathbb{P}\Big(\frac{\mathcal{P}_T S_z \|z\|^{-\alpha}}{\mathcal{P}_J \sum_{y \in \Phi_J} S_{yz} \|y - z\|^{-\alpha}} > \beta_e \Big| z, \Phi_J\Big)\Bigg)\Bigg\}\Bigg\},\end{aligned} \quad (9)$$

where $\mathbb{E}\{.\}$ denotes the expectation operator. The independence in the fading gains is used to move the expectation over $S = \{S_z, S_{yz}\}$ inside the product over Φ_e in (9). Since a closed-form expression of P_{so} seems intractable, we resort to an analytical upper bound given in the following lemma:

Lemma 2: The secrecy outage probability is bounded from above by

$$\mathrm{P}_{\mathrm{so}}^{\mathrm{UB}} = 1 - \exp\left[-\frac{\lambda_e}{\lambda_l \beta_e^{2/\alpha} \Gamma\big(1 - \frac{2}{\alpha}\big)\Gamma\big(1 + \frac{2}{\alpha}\big)\nu_2}\right], \quad (10)$$

where $\nu_2 = (1-p)(\mathcal{P}_J/\mathcal{P}_T)^{2/\alpha}$.

Proof: The derivation follows the proof of Lemma 1 in [11] and hence is omitted for brevity. ■

From [11] we know that the bounding technique used to derive the upper bound in (10) gives a very accurate approximation of the exact secrecy outage probability in (9). With the secrecy outage constraint given by $\mathrm{P}_{\mathrm{so}} = \epsilon$, the rate redundancy R_e can be found with high accuracy using (8) and (10) as

$$R_e = \log_2\left(1 + \left[\frac{\lambda_l}{\lambda_e}\Gamma\Big(1 - \frac{2}{\alpha}\Big)\Gamma\Big(1 + \frac{2}{\alpha}\Big)\nu_2 \ln \frac{1}{1-\epsilon}\right]^{-\frac{\alpha}{2}}\right). \quad (11)$$

Having R_t in (6) and R_e in (11), we compute the rate of confidential messages as $R_s = [R_t - R_e]^+$. Hence, the secrecy transmission capacity is readily obtained.

[2] Here we shift the coordinates so that the typical transmitter is located at the origin. This does not change the distributions of Φ_l and Φ_e.

Theorem 1: The secrecy transmission capacity with a connection outage constraint of σ and a secrecy outage constraint of ϵ is given by

$$\tau = (1-\sigma)p\lambda_l \cdot \left[\log_2\left(\frac{1+\left[\frac{\ln\frac{1}{1-\sigma}}{\lambda_l\pi r^2\Gamma(1-\frac{2}{\alpha})\Gamma(1+\frac{2}{\alpha})\nu_1}\right]^{\frac{\alpha}{2}}}{1+\left[\frac{\lambda_l}{\lambda_e}\Gamma\left(1-\frac{2}{\alpha}\right)\Gamma\left(1+\frac{2}{\alpha}\right)\nu_2\ln\frac{1}{1-\epsilon}\right]^{-\frac{\alpha}{2}}}\right)\right]^+, \tag{12}$$

where $\nu_1 = p + (1-p)(\mathcal{P}_J/\mathcal{P}_T)^{2/\alpha}$ and $\nu_2 = (1-p)(\mathcal{P}_J/\mathcal{P}_T)^{2/\alpha}$.

Strictly speaking, the expression in (12) is a lower bound on the secrecy transmission capacity. Nevertheless, this lower bound gives an accurate approximation of the exact value due to the fact that the upper bound on the secrecy outage probability in (10) is a very accurate approximation of the exact value [11]. Therefore, we for simplicity refer to τ in (12) as the secrecy transmission capacity.

A. Condition for Positive Secrecy Transmission Capacity

Clearly, the secrecy transmission capacity is zero when the expression inside $[\cdot]^+$ in (12) is non-positive. In this case, message transmission is not allowed since the connection and/or secrecy outage constraint(s) cannot be satisfied otherwise. Therefore, it is important to determine the condition under which a positive secrecy transmission capacity is achieved.

Corollary 1: For a connection outage constraint of σ and a secrecy outage constraint of ϵ, the secrecy transmission capacity given in (12) is positive when

$$\ln\frac{1}{1-\sigma}\ln\frac{1}{1-\epsilon} > \pi r^2\lambda_e\left[1+\frac{p}{1-p}\left(\frac{\mathcal{P}_T}{\mathcal{P}_J}\right)^{\frac{2}{\alpha}}\right]. \tag{13}$$

Remark: This condition depends on the densities of the actual transmitters and helping jammers only through their ratio $p/(1-p)$. If the condition in (13) does not hold, changing the number of legitimate users in the network does not help in obtaining a positive secrecy transmission capacity if the users do not reduce their message transmission probability p.

B. Optimizing the CJ-ALOHA Protocol

The effect of cooperative jamming on the secrecy transmission capacity can be described using two parameters, namely, the message transmission probability p and the normalized jamming power $\mathcal{P}_J/\mathcal{P}_T$ (*i.e.*, normalized by the power of message transmission). With the closed-form expression of the secrecy transmission capacity derived in (12), one can easily carry out numerical search to obtain the optimal values of p and $\mathcal{P}_J/\mathcal{P}_T$. Note that the individual values of $\mathcal{P}_J$ and $\mathcal{P}_T$ should satisfy any given power constraints.

In what follows, we consider the important special case where the nodes only transmit with fixed power, *i.e.*, $\mathcal{P}_J = \mathcal{P}_T$, and present an analytical result on the optimal message transmission probability.

Corollary 2: In the case of fixed power transmission, the optimal message transmission probability for networks in the high security regime (i.e., with ϵ very close to 0) is given by

$$p^* = 1 - \frac{1}{\mathrm{W}_0\Big(\exp(1)\kappa\Big)}, \tag{14}$$

where $\mathrm{W}_0(\cdot)$ is the real-valued principal branch of the Lambert W function and

$$\kappa = \frac{\lambda_l}{\lambda_e}\Gamma\Big(1-\frac{2}{\alpha}\Big)\Gamma\Big(1+\frac{2}{\alpha}\Big)\ln\frac{1}{1-\epsilon} \cdot\left(1+\left[\frac{\ln\frac{1}{1-\sigma}}{\lambda_l\pi r^2\Gamma\Big(1-\frac{2}{\alpha}\Big)\Gamma\Big(1+\frac{2}{\alpha}\Big)}\right]^{\frac{\alpha}{2}}\right)^{\frac{2}{\alpha}}. \tag{15}$$

Proof: See Appendix. ■

Remark: Using the fact that the Lambert W function $\mathrm{W}_0(z)$ is increasing in $z \in (0,\infty)$, we obtain the following results: 1) p^* reduces as the density of eavesdroppers λ_e increases. 2) p^* increases as the density of legitimate transmitters λ_l increases. 3) p^* reduces as the connection outage constraint gets tighter (*i.e.*, as σ decreases). The first result is intuitive since a higher jamming noise level is needed to fight against an increasing number of eavesdroppers. The last two results are less intuitive. Here we only give a rough explanation for the last result: With fixed power transmission, the connection outage probability $\mathrm{P_{co}}$ in (5) and the codeword rate R_t in (6) are independent of p. Hence, a decrease in σ results in a reduction in R_t regardless how p changes. In order to maximize the secrecy transmission capacity, it is desirable to reduce R_e in (11). Since R_e does not depend on σ, we need to decrease p in order to make R_e smaller, which explains why p^* decreases as σ decreases.

IV. Numerical Results and Discussion

In this section, we present numerical results to illustrate how the CJ-ALOHA protocol affects the secrecy transmission capacity.

Fig. 1 shows the secrecy transmission capacity τ over a wide range of the message transmission probability p. The normalized jamming power $\mathcal{P}_J/\mathcal{P}_T$ is fixed to a constant value for each curve. We see that a poor throughput performance often occurs when p is either too small or too large. A small p can result in inefficient spatial reuse, which directly affects the area spectral efficiency. On the other hand, a large p may cause an insufficient amount of jamming noise against eavesdropping, in which case the data rate needs to be reduced to meet the target secrecy constraint. The benefit of optimizing the message transmission probability is usually significant. For example, in the case of fixed power transmission ($\mathcal{P}_J = \mathcal{P}_T$), the maximum secrecy transmission capacity is 0.0057 achieved at $p = 0.42$, whereas the secrecy transmission capacity reduces to 0.004 (*i.e.*, a 30% reduction) if we reduce p to 0.21 (*i.e.*, p is halved). Comparing across the three curves with different normalized jamming power,

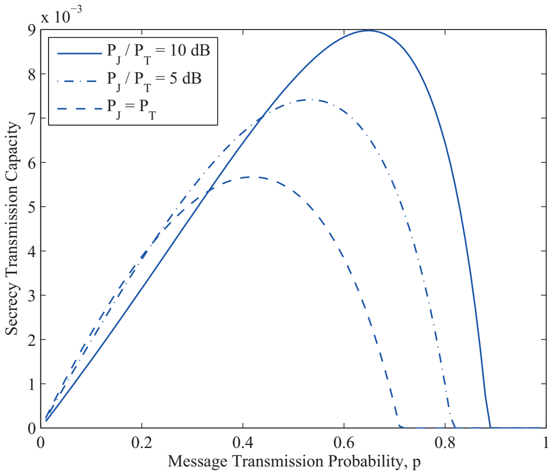

Fig. 1. The secrecy transmission capacity τ in (12) versus the message transmission probability p. Results are shown for networks with different normalized jamming power, *i.e.*, $\mathcal{P}_J/\mathcal{P}_T = 10$ dB, 5 dB and 0 dB (*i.e.*, $\mathcal{P}_J = \mathcal{P}_T$). The other system parameters are $r = 1$, $\alpha = 4$, $\sigma = 0.3$, $\epsilon = 0.03$, $\lambda_l = 0.01$, and $\lambda_e = 0.001$.

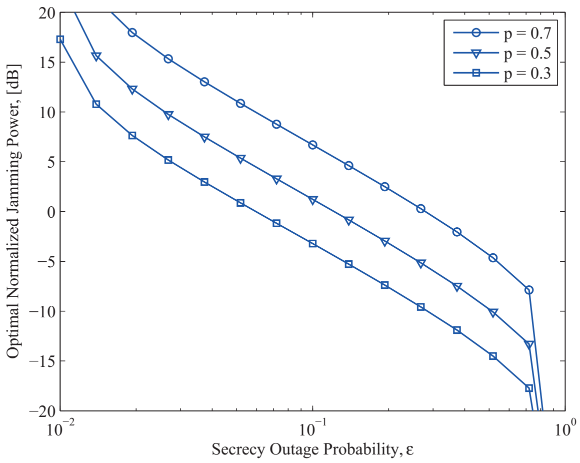

Fig. 2. The optimal normalized jamming power $\mathcal{P}_J/\mathcal{P}_T$ versus the secrecy outage probability ϵ. Results are shown for networks with different message transmission probability, *i.e.*, $p = 0.7$, 0.5, and 0.3. The other system parameters are $r = 1$, $\alpha = 4$, $\sigma = 0.3$, $\lambda_l = 0.01$, and $\lambda_e = 0.001$.

we see that choosing appropriate power levels can also give a significant throughput improvement.

Fig. 2 shows the optimal ratio of the jamming power to the message transmission power for networks with different security requirements. The message transmission probability p is fixed to a constant value for each curve. As the security requirement increases (from right to left in the figure), it is desirable to increase the normalized jamming power to reduce the SIRs at the eavesdroppers, which in turn minimizes the data rate reduction needed to meet a higher secrecy constraint. For networks with high security requirements, *e.g.*, $\epsilon = 0.01$, the optimal normalized jamming power is shown to reach 20 dB or higher. Such a large difference between the jamming power and the message transmission power may not be practical due to the transmitter's limited dynamic range as well as issues with fast switching between high and low power levels. Comparing across the three curves with different message transmission probabilities, we see that a lower normalized jamming power is needed if p is smaller, since there are more jammers available in the network.

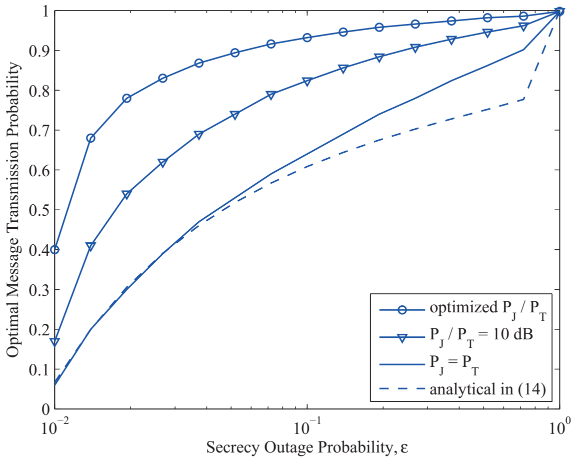

Fig. 3. The optimal message transmission probability p versus the secrecy outage probability ϵ. Results are shown for networks with different normalized jamming power, *i.e.*, the numerically optimized $\mathcal{P}_J/\mathcal{P}_T$, $\mathcal{P}_J/\mathcal{P}_T = 10$ dB, and $\mathcal{P}_J/\mathcal{P}_T = 0$ dB (*i.e.*, $\mathcal{P}_J = \mathcal{P}_T$). For the case of numerically optimized $\mathcal{P}_J/\mathcal{P}_T$, we limit the dynamic range of the transmit power to be 20 dB. We also plot the analytical expression of the optimal p given in (14) for the case of $\mathcal{P}_J = \mathcal{P}_T$. The other system parameters are $r = 1$, $\alpha = 4$, $\sigma = 0.3$, $\lambda_l = 0.01$, and $\lambda_e = 0.001$.

Fig. 3 shows the optimal message transmission probability for networks with different security requirements. When the normalized jamming power is also optimized[3], we see that the network can enjoy a moderately high probability of message transmission, even if the security requirement is as high as $\epsilon = 0.01$. In practice, however, the transmitting nodes may not have such a degree of freedom in fast varying their transmit power. Hence, we also plot the optimal message transmission probability for the case of fixed power transmission ($\mathcal{P}_J = \mathcal{P}_T$). Specifically, the solid line shows the optimal p obtained by a numerical search, while the dashed line shows the analytical result obtained in (14). We see that the analytical result is accurate for networks with relatively high security requirements, *e.g.*, $\epsilon < 0.05$. Compared with the case of optimized power levels, the optimal value of p in fixed power transmission is significantly lower, due to the need for a larger number of jammers to produce a satisfactory amount of jamming noise.

[3] In this figure, we limit the dynamic range of the transmit power to be 20 dB. Hence, the optimal $\mathcal{P}_J/\mathcal{P}_T$ is numerically found within the range from -20 dB to 20 dB.

V. Conclusion

In this paper, cooperative jamming as a physical layer security technique was studied in the context of large-scale decentralized wireless networks. Its impact on the network throughput was characterized using the secrecy transmission capacity. Our numerical results showed that significant throughput improvements can be obtained by properly designing the parameters of the CJ-ALOHA protocol.

References

[1] A. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[2] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[3] X. He and A. Yener, "Cooperative jamming: The tale of friendly interference for secrecy," in *Securing Wireless Communications at the Physical Layer*, R. Liu and W. Trappe, Eds. New York: Springer, 2009, pp. 65–88.

[4] L. Lai and H. El Gamal, "The relay-eavesdropper channel: cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4005–4019, Sep. 2008.

[5] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "Interference assisted secrect communication," *IEEE Trans. Inf. Theory*, vol. 57, no. 5, pp. 3153–3167, May 2011.

[6] J. P. Vilela, M. Bloch, J. Barros, and S. W. McLaughlin, "Wireless secrecy regions with friendly jamming," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 2, pp. 256–266, Jun. 2011.

[7] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.

[8] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperative relays," *IEEE Trans. Signal Processing*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[9] G. Zheng, L.-C. Choo, and K.-K. Wong, "Optimal cooperative jamming to enhance physical layer security using relays," *IEEE. Trans. Signal Processing*, vol. 59, no. 3, pp. 1317–1322, Mar. 2011.

[10] E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735–2751, Jun. 2008.

[11] X. Zhou, R. K. Ganti, J. G. Andrews, and A. Hjørungnes, "On the throughput cost of physical layer security in decentralized wireless networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 8, pp. 2764–2775, Aug. 2011.

[12] J. P. Vilela, P. C. Pinto, and J. Barros, "Position based jamming for enhanced wireless secrecy," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 616–627, Sep. 2011.

[13] S. Vasudevan, D. Goeckel, and D. Towsley, "Security-capacity tradeoff in large wireless networks using keyless secrecy," in *Proc. ACM Int. Symp. Mobile Ad Hoc Networking and Computing (MobiHoc)*, Chicago, IL, Sep. 2010, pp. 21–30.

[14] M. Haenggi, J. G. Andrews, F. Baccelli, O. Dousse, and M. Franceschetti, "Stochastic geometry and random graphs for the analysis and design of wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 7, pp. 1029–1046, Sep. 2009.

[15] S. Weber, J. G. Andrews, and N. Jindal, "An overview of the transmission capacity of wireless networks," *IEEE Trans. Commun.*, vol. 58, no. 12, Dec. 2010.

[16] Y. Liang, H. V. Poor, and L. Ying, "Secrecy throughput of MANETs with malicious nodes," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Seoul, Korea, Jun. 2009, pp. 1189–1193.

[17] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. W. McLaughlin, and J.-M. Merolla, "Applications of LDPC codes to the wiretap channel," *IEEE. Trans. Inf. Theory*, vol. 53, no. 8, pp. 2933–2945, Aug. 2007.

[18] X. Tang, R. Liu, P. Spasojević, and H. V. Poor, "On the throughput of secure hybrid-ARQ protocols for Gaussian block-fading channels," *IEEE. Trans. Inf. Theory*, vol. 55, no. 4, pp. 1575–1590, Apr. 2009.

[19] D. Stoyan, W. Kendall, and J. Mecke, *Stochastic Geometry and Its Applications*, 2nd ed. John Wiley and Sons, 1996.

[20] X. Zhou, R. K. Ganti, and J. G. Andrews, "Secure wireless network connectivity with multi-antenna transmission," *IEEE Trans. Wireless Commun.*, vol. 10, no. 2, pp. 425–430, Feb. 2011.

[21] J. Venkataraman, M. Haenggi, and O. Collins, "Shot noise models for outage and throughput analyses in wireless ad hoc networks," in *Proc. IEEE Military Commun. Conf. (MILCOM)*, Washington, DC, Oct. 2006, pp. 1–7.

[22] R. M. Corless and D. J. Jeffrey, "On the Wright ω function," available at http://www.orcca.on.ca/TechReports/TechReports/2000/TR-00-12.pdf.

Appendix

Proof of Corollary 2

With $\mathcal{P}_J = \mathcal{P}_T$, the secrecy transmission capacity reduces to

$$\tau = (1-\sigma)p\lambda_l \cdot \left[\log_2\left(\frac{1+\left[\frac{\ln\frac{1}{1-\sigma}}{\lambda_l\pi r^2\Gamma(1-\frac{2}{\alpha})\Gamma(1+\frac{2}{\alpha})}\right]^{\frac{\alpha}{2}}}{1+\left[\frac{\lambda_l}{\lambda_e}(1-p)\Gamma\Big(1-\frac{2}{\alpha}\Big)\Gamma\Big(1+\frac{2}{\alpha}\Big)\ln\frac{1}{1-\epsilon}\right]^{-\frac{\alpha}{2}}}\right)\right]^{+}.$$

Now we assume that the condition for positive secrecy transmission capacity in (13) holds and focus on the high security regime where ϵ is very small. As $\epsilon \to 0$, τ can be approximated as

$$\begin{aligned}\tau &\approx (1-\sigma)p\lambda_l \cdot \log_2\left(\frac{1+\left[\frac{\ln\frac{1}{1-\sigma}}{\lambda_l\pi r^2\Gamma(1-\frac{2}{\alpha})\Gamma(1+\frac{2}{\alpha})}\right]^{\frac{\alpha}{2}}}{\left[\frac{\lambda_l}{\lambda_e}(1-p)\Gamma\Big(1-\frac{2}{\alpha}\Big)\Gamma\Big(1+\frac{2}{\alpha}\Big)\ln\frac{1}{1-\epsilon}\right]^{-\frac{\alpha}{2}}}\right), \\ &= (1-\sigma)\lambda_l\frac{\alpha}{2\ln 2}p\ln\Big((1-p)\kappa\Big),\end{aligned}$$

where κ is given in (15). Hence, the optimal message transmission probability is

$$\arg\max_{p} f(p), \qquad \text{where } f(p) = p\ln\Big((1-p)\kappa\Big).$$

The first and second derivatives of $f(p)$ w.r.t. p are computed as

$$\begin{aligned}\frac{\mathrm{d}f(p)}{\mathrm{d}p} &= 1+\ln\kappa-\ln\frac{1}{1-p}-\frac{1}{1-p}, \\ \frac{\mathrm{d}^2f(p)}{\mathrm{d}p^2} &= -\frac{1}{1-p}-\frac{1}{(1-p)^2}.\end{aligned}$$

Since the second derivative is negative for $p \in (0,1)$, $f(p)$ is concave in p. The optimal p is obtained by letting the first derivative equal to zero, *i.e.*,

$$\ln z + z = 1+\ln\kappa, \qquad \text{where } z = \frac{1}{1-p^*}.$$

The value of z that satisfies the above equality is given by the Wright ω function as [22]

$$z = \omega(1+\ln\kappa),$$

which can also be expressed in terms of the Lambert W function as [22]

$$z = \mathrm{W}_0\Big(\exp(1+\ln\kappa)\Big).$$

Note that the principal branch of the Lambert W function is used due to the fact that $\kappa > 1$ when the condition for positive secrecy transmission capacity in (13) holds. Using the definition that $z = \frac{1}{1-p^*}$, the value of p^* is readily obtained.