

# Physical Layer Security in Wireless Ad Hoc Networks Under A Hybrid Full-/Half-Duplex Receiver Deployment Strategy

Tong-Xing Zheng, *Member, IEEE*, Hui-Ming Wang, *Senior Member, IEEE*,  
Jinhong Yuan, *Fellow, IEEE*, Zhu Han, *Fellow, IEEE*, and Moon Ho Lee, *Life Senior Member, IEEE*

**Abstract**—This paper studies physical layer security in a wireless ad hoc network with numerous legitimate transmitter-receiver pairs and eavesdroppers. A hybrid full-/half-duplex receiver deployment strategy is proposed to secure legitimate transmissions, by letting a fraction of legitimate receivers work in the full-duplex (FD) mode sending jamming signals to confuse eavesdroppers upon their information receptions, and letting the other receivers work in the half-duplex mode just receiving their desired signals. The objective of this paper is to choose properly the fraction of FD receivers for achieving the optimal network security performance. Both accurate expressions and tractable approximations for the connection outage probability and the secrecy outage probability of an arbitrary legitimate link are derived, based on which the area secure link number, network-wide secrecy throughput and network-wide secrecy energy efficiency are optimized respectively. Various insights into the optimal fraction are further developed and its closed-form expressions are also derived under perfect self-interference cancellation or in a dense network. It is concluded that the fraction of FD receivers triggers a non-trivial trade-off between reliability and secrecy, and the proposed strategy can significantly enhance the network security performance.

**Index Terms**—Physical layer security, ad hoc network, full-duplex receiver, outage, stochastic geometry.

## I. INTRODUCTION

THE rapid development in wireless communications has brought unprecedented attention to information security. Traditionally, security issues are addressed at the upper layers of communication protocols by using encryption. However, the large-scale and dynamic topologies in emerging wireless networks pose a great challenge in implementing secret key management and distribution, particularly in a decentralized wireless ad hoc network without infrastructure support [1]. Fortunately, *physical layer security*, an information-theoretic approach that attains secure transmissions by exploiting the randomness of wireless channels without necessarily relying on secret keys, is becoming increasingly recognized as a promising alternative to complement the cryptography-based security mechanisms [2]-[17].

T.-X. Zheng and H.-M. Wang are with the School of Electronic and Information Engineering, Xi'an Jiaotong University, Xi'an, 710049, Shaanxi, China. Email: txzheng@stu.xjtu.edu.cn, xjbswhm@gmail.com.

J. Yuan is with the School of Electrical Engineering and Telecommunications, University of New South Wales, Sydney, Australia. Email: j.yuan@unsw.edu.au.

Z. Han is with the Electrical and Computer Engineering Department, University of Houston, Houston, TX, USA. Email: zhan2@uh.edu.

M. H. Lee is with the Division of Electronics Engineering, Chonbuk National University, Jeonju 561-756, Korea. Email: moonho@jbnu.ac.kr.

Early studies on physical layer security have mainly focused on point-to-point transmissions, and metrics from user view-point such as secrecy capacity [3], ergodic secrecy rate [4], [5] and secrecy outage probability [6]-[8] have been used to evaluate the secrecy level in different scenarios/applications. From a *network-wide* perspective, physical layer security has also shown its potential [9], [10]. Many efforts have already been devoted to improve network security in terms of the area secure link number (ASLN) [11], [12] and network-wide secrecy throughput (NST) [13], [14]. More recently, energy-efficient green wireless network has attracted considerable interests due to energy scarcity, and some research works have been carried out for enhancing network-wide secrecy energy efficiency (NSEE) [15], [16].

## A. Previous Endeavors and Motivations

To improve the secrecy of information delivery for an ad hoc network, an efficient approach is to degrade the wiretapping ability of eavesdroppers through emitting jamming signals [17]. For example, the authors in [13] propose a cooperative jamming strategy with single-antenna legitimate transmitters, and when eavesdroppers access a transmitter's secrecy guard zone [13], this transmitter will act as a friendly jammer to send jamming signals to confuse eavesdroppers. This work is extended by [14] to a multi-antenna transmitter scenario, and artificial noise [17] with either sectoring or beamforming is exploited to impair eavesdroppers. Although these endeavors are shown to achieve a remarkable secrecy throughput enhancement, friendly jammers or multi-antenna transmitters might not be available in many applications. For instance, constrained by the size and hardware cost, a sensor node is usually equipped with only a single antenna. Furthermore, due to a low-power constraint, a sensor has no extra power to send jamming signals. In such unfavorable situations, information transfer is still vulnerable to eavesdropping.

Fortunately, recent advances in developing in-band full-duplex (FD) radios provide a new opportunity to strengthen information security in the aforementioned situations. Effective self-interference cancellation (SIC) techniques enable a transceiver to transmit and receive at the same time on the same frequency band [18]. Although the transmitter (sensor) is vulnerable to eavesdropping, we can deploy powerful FD receivers such as data collection stations to radiate jamming signals upon their information receptions. By doing so, additional degrees of freedom can be gained for improving

network security. In fact, the idea of using FD receiver jamming to improve physical layer security has already been reported by [19]–[24] for point-to-point transmission scenarios. Specifically, the authors in [19] and [20] consider a single-input multi-output (SIMO) channel with the receiver using single- and multi-antenna jamming, respectively. The authors in [21] consider a multi-input multi-output (MIMO) channel with both transmitter and receiver generating artificial noise. These works are further extended in two-way transmissions [22], cooperative communications [23], [24], and cellular networks [25]. Recently, we have studied the design of the optimal density of the overlaid FD-mode tier to maximize its NST while guaranteeing a minimum network-wide throughput for the underlaid HD-mode tier [26]. Generally, investigating the potential benefits of FD receiver jamming techniques in enhancing information security from a *network* perspective is an interesting, but much more sophisticated issue, since we should take into account numerous interferers and eavesdroppers that are randomly distributed over the network. In addition, using FD receiver jamming in a network is confronted with two fundamental challenges as follows:

- Theoretically, activating too many FD receivers to send jamming signals brings severe self- and mutual-interference to legitimate receivers, thus impairing the reliability of the ongoing information transmission. This will result in few secure links being established and accordingly the poor secrecy throughput.
- Practically, employing FD receivers incurs more system cost and overhead. FD transceivers are more expensive than half-duplex (HD) transceivers. From energy efficiency perspective, more circuit power is consumed to enable the FD operation or to mitigate the self-interference caused by FD radios, which leads to low energy efficiency.

Motivated by these, a proper way to deploy FD receivers is to make a portion of legitimate receivers work in the FD mode simultaneously sending jamming signals and receiving desired signals, and make the rest work in the HD mode just receiving desired signals. This results in a hybrid full-/half-duplex receiver deployment strategy. Then, a question is naturally raised: *What should be the optimal fraction of FD receivers in order to optimize the network security performance?* To the best of our knowledge, this question has not been answered by existing literature. So far, a fundamental analysis on the network security performance, in aspects like *ASLN*, *NST* and *NSEE*, is still lacking for a wireless ad hoc network with hybrid full-/half-duplex receivers. This motivates our work.

### B. Our Work and Contributions

In this paper, we study physical layer security for a wireless ad hoc network under a stochastic geometry framework [27]. Each transmitter in this network is equipped with a single antenna and sends a secret message to an intended single-antenna receiver, in the presence of randomly located multi-antenna eavesdroppers. A hybrid full-/half-duplex receiver deployment strategy is proposed, where a fraction of legitimate receivers work in the FD mode receiving desired signals and radiating

jamming signals simultaneously, and the remaining receivers work in the HD mode just receiving desired signals. The main contributions of this paper are summarized as follows:

- We investigate the fundamental tradeoff between secrecy and reliability via jammers. We analyze the connection outage probability and the secrecy outage probability of a typical legitimate link, and provide both accurate expressions and tractable approximations for them.
- We study three important performance metrics on network security, namely, *ASLN*, *NST* and *NSEE*, respectively. We prove that these metrics are all *quasi-concave* functions of the fraction of FD receivers, and derive the optimal deployment fractions to maximize them.
- We further develop insights into the behavior of the optimal fraction of FD receivers with respect to various network parameters. We also provide closed-form expressions for this optimal fraction in special cases, e.g., under a perfect SIC assumption or in a dense network.

### C. Organization and Notations

The remainder of this paper is organized as follows. In Section II, we describe the system model. In Section III, we analyze the connection outage and secrecy outage probabilities of an arbitrary legitimate link. In Sections IV, V and VI, we optimize the fraction of FD receivers to maximize *ASLN*, *NST* and *NSEE*, respectively. In Section VII, we conclude our work.

*Notations:* bold uppercase (lowercase) letters denote matrices (vectors).  $(\cdot)^H$ ,  $(\cdot)^{-1}$ ,  $\Pr\{\cdot\}$ , and  $\mathbb{E}_A(\cdot)$  denote Hermitian transpose, inversion, probability, and the expectation of  $A$ , respectively.  $\text{CN}(\mu, \nu)$  denotes the circularly symmetric complex Gaussian distribution with mean  $\mu$  and variance  $\nu$ .  $\ln(\cdot)$  denotes the natural logarithm.  $f'(q)$  and  $f''(q)$  denote the first- and second-order derivatives of  $f(q)$  on  $q$ , respectively.  $\mathbf{1}_{\text{FD}}(x)$  is an indicator function with  $\mathbf{1}_{\text{FD}}(x) = 1$  for  $x \in \{\text{FD}\}$  and  $\mathbf{1}_{\text{FD}}(x) = 0$  for  $x \notin \{\text{FD}\}$ .  $L_I(s) = \mathbb{E}_I(e^{-sI})$  is the Laplace transform of  $I$ .  $[x]^+ \triangleq \max(x, 0)$ .

## II. SYSTEM MODEL

We consider a wireless ad hoc network composed of numerous single-antenna legitimate transmitter-receiver pairs, coexisting with randomly located  $N_e$ -antenna eavesdroppers. Each legitimate transmitter sends a secret message to its paired receiver located a distance  $r_o$  away<sup>1</sup>. We assume that a fraction  $q$  of legitimate receivers work in the FD mode such that each of them simultaneously receives the desired signal and radiates a jamming signal to confuse eavesdroppers, and the others work in the HD mode only receiving desired signals. Legitimate receivers and eavesdroppers are distributed according to independent homogeneous Poisson point processes (PPPs) [28]  $\Phi_l$  with density  $\lambda_l$  and  $\Phi_e$  with density  $\lambda_e$ , respectively. Using the property of thinning for a PPP, the distributions of HD and FD receivers follow independent PPPs  $\Phi^{\text{HD}}$  with density  $\lambda^{\text{HD}} = (1 - q)\lambda_l$  and  $\Phi^{\text{FD}}$  with density  $\lambda^{\text{FD}} = q\lambda_l$ ,

<sup>1</sup>The assumption of a common legitimate link distance is quite generic in analyzing a wireless ad hoc network [13], [14], which eases the mathematical analysis. Nevertheless, in principle the obtained results can be generalized to an arbitrary distribution of  $r_o$  [27].

respectively. We denote by  $\tilde{\Phi}^{\text{HD}}$  and  $\tilde{\Phi}^{\text{FD}}$  the location sets of the transmitters corresponding to HD and FD receivers, respectively. According to the displacement theorem [32, page 35],  $\tilde{\Phi}^{\text{HD}}$  and  $\tilde{\Phi}^{\text{FD}}$  are also independent PPPs with densities  $\lambda^{\text{HD}}$  and  $\lambda^{\text{FD}}$ , respectively. We use  $r_{xy}$  to denote the distance between a node located at  $x$  and a node at  $y$ . For convenience, we use  $\tilde{x}$  to denote the location of a transmitter whose paired receiver is located at  $x$ .

Wireless channels, including legitimate channels and wiretap channels, are assumed to suffer a large-scale path loss governed by the exponent  $\alpha > 2$  together with a quasi-static Rayleigh fading with fading coefficients independent and identically distributed (i.i.d.) obeying  $\text{CN}(0, 1)$ . Due to uncoordinated concurrent transmissions, the aggregate interference at a receiver dominates the thermal noise. Thereby, we concentrate on an interference-limited scenario by ignoring thermal noise, given that the inclusion of thermal noise results in a more complicated analysis but provides no significant qualitative difference.

Throughout this paper, we denote  $\mathbf{S} \in \{\text{HD}, \text{FD}\}$  by default. For convenience, the legitimate link with an  $\mathbf{S}$  receiver is called an  $\mathbf{S}$ -link. Considering a typical  $\mathbf{S}$  receiver located at the origin  $o$ , its signal-to-interference ratio (SIR) is given by

$$\gamma_o^{\mathbf{S}} = \frac{P_t h_{\tilde{o}o} r_o^{-\alpha}}{I^{\text{HD}} + I^{\text{FD}} + \mathbf{1}_{\text{FD}}(\mathbf{S})\eta P_j}, \quad (1)$$

where  $I^{\text{HD}} \triangleq \sum_{\tilde{x} \in \tilde{\Phi}^{\text{HD}}} P_t h_{\tilde{x}o} r_{\tilde{x}o}^{-\alpha}$ ,  $I^{\text{FD}} \triangleq \sum_{\tilde{x} \in \tilde{\Phi}^{\text{FD}} \setminus \tilde{o}} (P_t h_{\tilde{x}o} r_{\tilde{x}o}^{-\alpha} + P_j h_{x_o} r_{x_o}^{-\alpha})$  and  $\eta P_j$  denote the interferences from HD links, from FD links and from the typical FD receiver itself, respectively;  $P_t$  and  $P_j$  denote the transmit powers of a legitimate transmitter and of an FD receiver, respectively;  $h_{xy}$  denotes the fading channel gain obeying  $\text{Exp}(1)$ ;  $\eta$  is a parameter that reflects the SIC capability, and  $\eta = 0$  refers to a perfect SIC while  $0 < \eta \leq 1$  corresponds to different levels of SIC. Note that  $r_{\tilde{x}o}$  and  $r_{x_o}$  in  $I^{\text{HD}}$  and  $I^{\text{FD}}$  are correlated, and they satisfy  $r_{\tilde{x}o} = \sqrt{r_{x_o}^2 + r_o^2 - 2r_{x_o}r_o \cos \theta_x}$ , where the angle  $\theta_x$  is uniformly distributed in the range  $[0, 2\pi]$ .

For eavesdroppers, we consider a worst-case wiretap scenario where each eavesdropper has multiuser decoding ability and adopts a successive interference cancellation minimum mean square error (MMSE) receiver. The eavesdropper located at  $e$  is able to decode and cancel undesired information signals and uses the MMSE detector

$$\mathbf{w}_e^{\mathbf{S}} = (\mathbf{R}_e^{\mathbf{S}})^{-1} \mathbf{g}_{\tilde{o}e} \quad (2)$$

to aggregate the desired signal, where  $\mathbf{R}_e^{\mathbf{S}} \triangleq \sum_{x \in \Phi^{\text{FD}} \setminus o} P_j \mathbf{g}_{xe} \mathbf{g}_{xe}^H r_{xe}^{-\alpha} + \mathbf{1}_{\text{FD}}(\mathbf{S}) \mathbf{R}_{oe}$  with  $\mathbf{R}_{oe} \triangleq P_j \mathbf{g}_{oe} \mathbf{g}_{oe}^H r_{oe}^{-\alpha}$ , and  $\mathbf{g}_{xe}$  denotes the  $N_e \times 1$  complex fading coefficient vector related to the link from a node at  $x$  to an eavesdropper at  $e$ . The corresponding SIR of the eavesdropper is

$$\gamma_e^{\mathbf{S}} = P_t \mathbf{g}_{\tilde{o}e}^H (\mathbf{R}_e^{\mathbf{S}})^{-1} \mathbf{g}_{\tilde{o}e} r_{\tilde{o}e}^{-\alpha}. \quad (3)$$

#### A. Secrecy Performance Metrics

We assume eavesdroppers do not collude with each other such that each of them individually decodes a secret message.

To guarantee secrecy, each legitimate transmitter adopts the Wyner's wiretap encoding scheme [2] to encode secret information. Thereby, two types of rates, namely, the rate of transmitted codewords  $R_t$  and the rate of embedded information bits  $R_s$ , need to be designed to meet requirements in terms of the connection outage and secrecy outage probabilities.

- *Connection outage probability.* If a legitimate  $\mathbf{S}$ -link can support rate  $R_t$ , the legitimate receiver is able to decode a secret message and perfect connection is assured in this link; otherwise a connection outage occurs. The probability that such a connection outage event takes place is referred to as the connection outage probability, denoted as  $p_{co}^{\mathbf{S}}$ .
- *Secrecy outage probability.* In the Wyner's wiretap encoding scheme, the rate redundancy  $R_e \triangleq R_t - R_s$  is exploited to provide secrecy against eavesdropping. If the value of  $R_e$  lies above the capacity of the most detrimental eavesdropping link, no information is leaked to eavesdroppers and perfect secrecy is promised in the legitimate link [2]; otherwise a secrecy outage occurs. The probability that such a secrecy outage event takes place in an  $\mathbf{S}$ -link is referred to as the secrecy outage probability, denoted as  $p_{so}^{\mathbf{S}}$ .

In this paper, we concern ourselves with the following three important metrics that measure the network-wide security performance from an outage perspective.

1) *ASLN.* A link in which neither connection outage nor secrecy outage occurs is called a secure link [11]. To measure how many secure links can be guaranteed under rates  $R_t$  and  $R_s$ , we use the metric named ASLN, which is defined as the average number of secure links per unit area. Due to the independence of  $p_{co}^{\mathbf{S}}$  and  $p_{so}^{\mathbf{S}}$ , ASLN, denoted as  $N$ , is mathematically given by

$$N \triangleq q\lambda_l(1-p_{co}^{\text{FD}})(1-p_{so}^{\text{FD}}) + (1-q)\lambda_l(1-p_{co}^{\text{HD}})(1-p_{so}^{\text{HD}}). \quad (4)$$

2) *NST.* To assess the efficiency of secure transmissions, we use the metric named NST [13], which is defined as the achievable rate of successful information transmission per unit area under the required connection outage and secrecy outage probabilities. The NST, denoted as  $\Omega$ , under a connection outage probability  $p_{co}^{\mathbf{S}} = \sigma$  and a secrecy outage probability  $p_{so}^{\mathbf{S}} = \epsilon$  is given by

$$\Omega \triangleq q\lambda_l(1-\sigma)R_s^{\text{FD}} + (1-q)\lambda_l(1-\sigma)R_s^{\text{HD}}, \quad (5)$$

where  $R_s^{\mathbf{S}} \triangleq [R_t^{\mathbf{S}} - R_e^{\mathbf{S}}]^+$ , with  $R_t^{\mathbf{S}}$  and  $R_e^{\mathbf{S}}$  the codeword rate and redundant rate that satisfy  $p_{co}^{\mathbf{S}}(R_t^{\mathbf{S}}) = \sigma$  and  $p_{so}^{\mathbf{S}}(R_e^{\mathbf{S}}) = \epsilon$ , respectively. The unit of  $\Omega$  is nats/s/Hz/m<sup>2</sup>.

3) *NSEE.* To evaluate the energy efficiency of secure transmissions, we use the metric named NSEE, denoted as  $\Psi$ , which is defined as the ratio of NST to the power consumed per unit area,

$$\Psi \triangleq \frac{\Omega}{\lambda_l(P_t + P_c) + q\lambda_l P_j}, \quad (6)$$

where  $P_c$  combines the dynamic circuit power consumption of transmit chains and the static power consumption in transmit modes [29]. The unit of  $\Psi$  is nats/Joule/Hz.



We emphasize that, the fraction  $q$  of FD receivers triggers a non-trivial trade-off between reliability and secrecy, and plays a key role in improving the metrics given above. Intuitively, under a larger  $q$ , more FD jammers are activated against eavesdroppers which benefits the secrecy; whereas the increased jamming signals also interfere with legitimate receivers and thus harm the reliability. The overall balance of such conflicting effects needs to be carefully addressed. In Sections IV, V and VI, we are going to respectively determine the optimal fraction  $q$  that

- maximizes ASLN  $N$  given a pair of wiretap code rates  $R_t$  and  $R_s$ ;
- maximizes NST  $\Omega$  given a pair of outage probabilities  $\sigma$  and  $\epsilon$ ;
- maximizes NSEE  $\Psi$  with and without considering a minimum required NST.

Before proceeding, in the following section we first provide some insights into the behavior of the connection outage probability  $p_{co}^S$  and the secrecy outage probability  $p_{so}^S$  with respect to network parameters like  $q$ ,  $\eta$ , etc., which is very important to subsequent network design.

### III. OUTAGE PROBABILITY ANALYSIS

In this section, we derive the connection outage probability and the secrecy outage probability for an arbitrary legitimate link. For ease of notation, we define  $\delta \triangleq 2/\alpha$ ,  $\kappa \triangleq \pi\Gamma(1+\delta)\Gamma(1-\delta)$  and  $\rho \triangleq P_j/P_t$ , which will be used throughout the paper.

#### A. Connection Outage Probability

The connection outage probability of a typical S-link is defined as the probability that the SIR  $\gamma_o^S$  given in (1) falls below an SIR threshold  $\tau_t \triangleq 2^{R_t} - 1$ , i.e.,

$$p_{co}^S \triangleq \Pr\{\gamma_o^S < \tau_t\}. \quad (7)$$

The general expression of  $p_{co}^S$  is provided by the following theorem. The interested readers are referred to [26, Th. 1] for a detailed proof.

*Theorem 1:* The connection outage probability of a typical S-link is given by

$$p_{co}^S = 1 - e^{-\mathbf{1}_{FD}(S)\rho\eta r_o^\alpha \tau_t e^{-\kappa(1-q)\lambda_l r_o^2 \tau_t^\delta} L_{IFD}(r_o^\alpha \tau_t/P_t)}, \quad (8)$$

where  $L_{IFD}(r_o^\alpha \tau_t/P_t) = \exp\left(-q\lambda_l \int_0^\infty \int_0^{2\pi} \left(1 - \frac{1}{1+r_o^\alpha \tau_t v^{-\alpha}} \frac{1}{1+r_o^\alpha \tau_t (v^2+r_o^2-2vr_o \cos \theta)^{-\alpha/2}}\right) v d\theta dv\right)$ .

Theorem 1 provides an exact connection outage probability with three parts  $e^{-\mathbf{1}_{FD}(S)\rho\eta r_o^\alpha \tau_t}$ ,  $e^{-\kappa(1-q)\lambda_l r_o^2 \tau_t^\delta}$  and  $L_{IFD}(r_o^\alpha \tau_t/P_t)$ , reflecting the impacts of the interferences from the typical receiver itself, from HD links and from FD links, respectively. Although with  $p_{co}^S$  given in (8) we no longer need to execute time-consuming Monte Carlo simulations, the double integral in  $L_{IFD}(r_o^\alpha \tau_t/P_t)$  greatly complicates the further analysis, which motivates a more compact form. In the following theorem, we provide the closed-form upper and lower bounds for  $p_{co}^S$ , and refer the interested readers to [26, Th. 2] for a detailed proof.

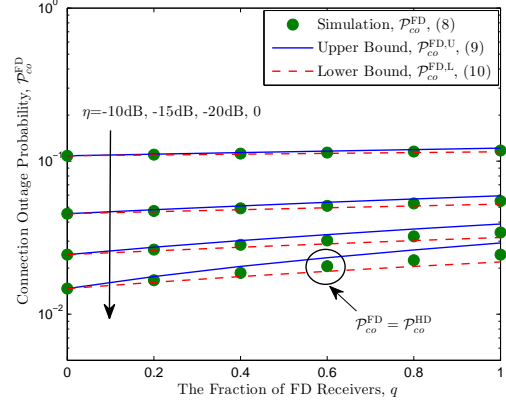


Fig. 1: Connection outage probability vs.  $q$  for different values of  $\eta$ , with  $\alpha = 4$ ,  $\rho = 1$ ,  $r_o = 1$ ,  $\lambda_l = 3 \times 10^{-3}$  and  $\tau_t = 1$ .

*Theorem 2:* Connection outage probability  $p_{co}^S$  is upper and lower bounded respectively by

$$p_{co}^{S,U} = 1 - e^{-\mathbf{1}_{FD}(S)\rho\eta r_o^\alpha \tau_t e^{-\kappa r_o^2 \tau_t^\delta \lambda_l (1+\rho^\delta q)}}, \quad (9)$$

$$p_{co}^{S,L} = 1 - e^{-\mathbf{1}_{FD}(S)\rho\eta r_o^\alpha \tau_t e^{-\kappa r_o^2 \tau_t^\delta \lambda_l \left(1 + \frac{(1+\delta)\rho^\delta - (1-\delta)}{2} q\right)}}. \quad (10)$$

Theorem 2 shows that both bounds for the connection outage probability increase exponentially in  $\eta$ ,  $q$  and  $\lambda_l$ , because of the increase of self- and mutual-interference. The relationships between the connection outage probability  $p_{co}^S$  and parameters  $q$  and  $\eta$  are validated in Fig. 1, where the results labeled by  $\eta = 0$  also refer to an HD counterpart. We observe that, although  $p_{co}^S$  increases as  $q$  increases, the effect is not very remarkable when  $\eta$  is large. This is because, in the large  $\eta$  region the self-interference perceived at an FD receiver dominates the interference (including both undesired and jamming signals) from the other network nodes.

#### B. Secrecy Outage Probability

The secrecy outage probability of a typical S-link is defined as the complement of the probability that any eavesdropper's SIR  $\gamma_e^S$  falls below an SIR threshold  $\tau_e \triangleq 2^{R_e} - 1$ , i.e.,

$$p_{so}^S \triangleq 1 - \mathbb{E}_{\Phi^{FD}} \mathbb{E}_{\Phi_e} \left[ \prod_{e \in \Phi_e} \Pr\{\gamma_e^S < \tau_e | \Phi_e, \Phi^{FD}\} \right]. \quad (11)$$

To calculate exact  $p_{so}^S$  is very difficult. Instead, we give an upper bound for  $p_{so}^S$  in the following theorem. Please refer to [26, Th. 3] for a detailed proof.

*Theorem 3:* Secrecy outage probability  $p_{so}^S$  of a typical S-link is upper bounded by

$$p_{so}^{S,U} = 1 - \exp\left(-\lambda_e \sum_{n=0}^{N_e-1} \sum_{i=0}^{\min(n,1)} \frac{(\kappa \lambda^{FD} \rho^\delta \tau_e^\delta)^{n-i}}{(n-i)!} \Xi_{n,i}^S\right), \quad (12)$$

where  $\Xi_{n,i}^S = \int_0^\infty \int_0^{2\pi} \Lambda_{i,\theta,v}^S v^{2(n-i)} e^{-\kappa \lambda^{FD} \rho^\delta \tau_e^\delta v^2} d\theta dv$  with  $\Lambda_{i,\theta,v}^S = \frac{(\mathbf{1}_{FD}(S)\rho\tau_e(v/\sqrt{v^2+r_o^2-2vr_o \cos \theta})^\alpha)^i}{1+\mathbf{1}_{FD}(S)\rho\tau_e(v/\sqrt{v^2+r_o^2-2vr_o \cos \theta})^\alpha}$ .

In the following sections, we use upper bound  $p_{so}^{S,U}$  to replace exact  $p_{so}^S$ , not simply for a tractable analysis but also

for the following two reasons: on one hand,  $p_{so}^{\text{S,U}}$  provides a pessimistic evaluation of secrecy performance, which actually benefits a robust design; on the other hand, as [13] shows,  $p_{so}^{\text{S,U}}$  will converge to  $p_{so}^{\text{S}}$  at the low secrecy outage probability regime, and a low secrecy outage probability is expected in order to guarantee a high level of secrecy.

Clearly, since  $\mathbf{1}_{\text{FD}}(\text{HD}) = 0$ , we have  $\Lambda_{0,\theta,v}^{\text{HD}} = 1$  and  $\Lambda_{i,\theta,v}^{\text{HD}} = 0$  for  $i > 0$ . Substituting these results into (12) yields a closed-form expression for  $p_{so}^{\text{HD}}$  given below,

$$p_{so}^{\text{HD}} = 1 - \exp \left( -\pi\lambda_e \sum_{n=0}^{N_e-1} \frac{(\kappa\lambda^{\text{FD}}\rho^\delta\tau_e^\delta)^n}{n!} \int_0^\infty v^{2n} \times e^{-\kappa\lambda^{\text{FD}}\rho^\delta\tau_e^\delta v^2} dv^2 \right) = 1 - e^{-\frac{\pi\lambda_e N_e}{\kappa q \lambda_l \rho^\delta \tau_e^\delta}}, \quad (13)$$

where the last equality follows from formula [33, (3.381.4)]. As to  $p_{so}^{\text{FD}}$ , the double integral in (12) makes it difficult to analyze. Given that a single-antenna transmitter in a large-scale ad hoc network usually has low transmit power and very limited coverage, we should set the legitimate link distance  $r_o$  sufficiently small (compared with the distance between two nodes that are not in pair) to guarantee both reliability and secrecy. In the following, we resort to an asymptotic analysis by letting  $r_o \rightarrow 0$  in (12) in order to develop useful and tractable insights into the behavior of  $p_{so}^{\text{FD}}$ . The following corollary gives a quite simple approximation for  $p_{so}^{\text{FD}}$ .

*Corollary 1:* In the small  $r_o$  regime, i.e.,  $r_o \rightarrow 0$ ,  $p_{so}^{\text{FD}}$  in (12) is approximated by

$$\hat{p}_{so}^{\text{FD}} = 1 - \exp \left( -\frac{\pi\lambda_e N_e}{\kappa q \lambda_l \rho^\delta \tau_e^\delta} \left( 1 - \frac{\rho\tau_e/N_e}{1 + \rho\tau_e} \right) \right). \quad (14)$$

*Proof 1:* Recalling Theorem 3, plugging  $r_o \rightarrow 0$  into  $\Lambda_{i,\theta,v}^{\text{FD}}$  yields  $\Lambda_{i,\theta,v}^{\text{FD}} = \frac{(\rho\tau_e)^i}{1 + \rho\tau_e}$ , and thus  $\Xi_{n,i}^{\text{FD}} = \frac{2\pi(\rho\tau_e)^i (n-i)!}{(1 + \rho\tau_e)} (\kappa\lambda^{\text{FD}}\rho^\delta\tau_e^\delta)^{i-n-1}$ . Substituting  $\Xi_{n,i}^{\text{FD}}$  into (12) completes the proof.

We stress that, although Corollary 1 is established under the assumption  $r_o \rightarrow 0$ , it actually applies to more general scenarios. Fig. 2 shows that  $\hat{p}_{so}^{\text{FD}}$  in (14) approximates to  $p_{so}^{\text{FD}}$  in (12) in quite a wide range of  $r_o$  and  $\lambda_e$  particularly when  $\lambda_f$  is small, which demonstrates high accuracy for the approximation. Hereafter, unless specified otherwise, we often use this approximation to deal with the secrecy outage probability.

Eqn. (13) and (14) clearly show that secrecy outage probabilities increase exponentially with  $\lambda_e$  and  $N_e$ . This is ameliorated by increasing  $q$  or  $\rho$ . In addition, secrecy outage probabilities increase as  $\alpha$  increases. This is because, in a large path-loss exponent environment, jamming signals have undergone a strong attenuation before they arrive at eavesdroppers.

#### IV. AREA SECURE LINK NUMBER

In this section, we maximize ASLN  $N$  under a given pair of wiretap code rates  $R_t$  and  $R_s$  by determining the optimal fraction  $q$  of FD receivers.

To facilitate a robust design, we use the upper bounded connection outage probability  $p_{co}^{\text{S,U}}$  given in (9), which actually pessimistically assess the connection performance. We also

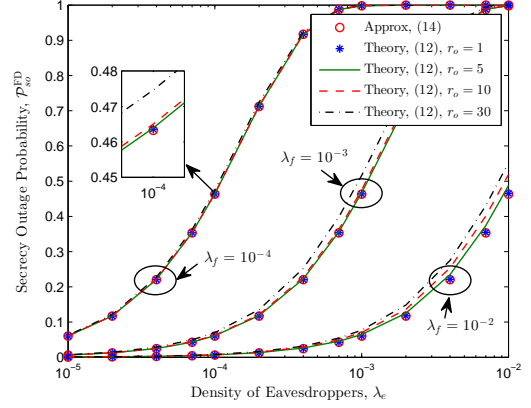


Fig. 2: Secrecy outage probability vs.  $\lambda_e$  for different values of  $r_o$  and  $\lambda_f$ , with  $\alpha = 4$ ,  $\rho = 10$  and  $\tau_e = 1$ .

suppose eavesdroppers use a large number of antennas in order to do better wiretapping, which also gives a pessimistic evaluation of the secrecy performance. Resorting to an asymptotic analysis of  $p_{so}^{\text{FD}}$  by letting  $N_e \gg 1$  in (14),  $p_{so}^{\text{FD}}$  shares the same expression as  $p_{so}^{\text{HD}}$  in (13), i.e.,

$$p_{so}^{\text{S}} = 1 - e^{-\frac{\pi\lambda_e N_e}{\kappa q \lambda_l \rho^\delta \tau_e^\delta}}. \quad (15)$$

Substituting (9) and (15) into (4) yields

$$N = \lambda_l \left( qe^{-\rho\eta r_o^\alpha \tau_t} + 1 - q \right) e^{-\kappa r_o^2 \tau_t^\delta \lambda_l (1 + \rho^\delta q) - \frac{\pi\lambda_e N_e}{\kappa q \lambda_l \rho^\delta \tau_e^\delta}}. \quad (16)$$

Introducing an auxiliary function  $F(q) = (qA + (1 - q))e^{-Bq - C/q}$  with  $A \triangleq e^{-\rho\eta r_o^\alpha \tau_t} < 1$ ,  $B \triangleq \kappa r_o^2 \tau_t^\delta \rho^\delta \lambda_l$  and  $C \triangleq \frac{\pi\lambda_e N_e}{\kappa \lambda_l \rho^\delta \tau_e^\delta}$ , we have  $N = \lambda_l e^{-\kappa r_o^2 \tau_t^\delta \lambda_l} F(q)$  such that parameter  $q$  only exists in  $F(q)$ . Hence, maximizing  $N$  is equivalent to maximizing  $F(q)$ , which can be formulated as

$$\max_q F(q) = (qA + (1 - q))e^{-Bq - C/q}, \quad \text{s.t. } 0 < q \leq 1. \quad (17)$$

In the following theorem, we prove the quasi-concavity [34, Sec. 3.4.2] of  $F(q)$  in  $q$ , and give the optimal solution of problem (17).

*Theorem 4:* The optimal fraction of FD receivers that maximizes ASLN  $N$  is given by

$$q_{sl}^* = \begin{cases} 1, & \pi\lambda_e N_e > \kappa\lambda_l \rho^\delta \tau_e^\delta (1/A + B - 1), \\ q_{sl}^o, & \text{otherwise,} \end{cases} \quad (18)$$

where  $q_{sl}^o$  is the unique root  $q$  of the following equation

$$(A + q^{-1} - 1)(1 + Cq^{-1} - Bq) - q^{-1} = 0. \quad (19)$$

The left-hand side (LHS) of (19) is initially positive and then negative when  $C \leq 1/A + B - 1$ ; and thus,  $q_{sl}^o$  can be efficiently calculated using the bisection method with (19).

*Proof 2:* Please refer to Appendix A.

Theorem 4 indicates that as eavesdropper density  $\lambda_e$  or eavesdropper antenna number  $N_e$  is sufficiently large such that  $\pi\lambda_e N_e > \kappa\lambda_l \rho^\delta \tau_e^\delta (1/A + B - 1)$ , all legitimate receivers should work in the FD mode; otherwise a portion of HD receivers are permitted, just as depicted in Fig. 3.

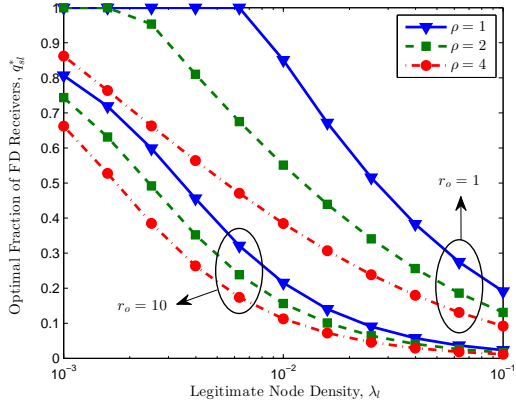


Fig. 3: The optimal fraction of FD receivers that maximizes ASLN  $N$  vs.  $\lambda_l$  for different values of  $r_o$  and  $\rho$ , with  $\alpha = 4$ ,  $\lambda_e = 10^{-3}$ ,  $N_e = 6$ ,  $\eta = -10\text{dB}$ ,  $\tau_t = 2$  and  $\tau_e = 1$ .

Although it is difficult to provide an explicit expression for the optimal  $q_{sl}^o$  given in (18), we are still able to develop some insights into the behavior of  $q_{sl}^o$  in the following corollary.

*Corollary 2:* The optimal  $q_{sl}^o$  given in (18) monotonically increases with  $\lambda_e$  and  $N_e$ , and monotonically decreases with  $\lambda_l$ ,  $r_o$ ,  $\eta$ ,  $\rho$ ,  $\tau_t$  and  $\tau_e$ . In the perfect SIC case, i.e.,  $\eta = 0$ , a closed-form expression on  $q_{sl}^o$  can be further given by

$$q_{sl}^{o,\eta=0} = \sqrt{\frac{C}{B}} = \frac{1}{\kappa \lambda_l \rho^\delta r_o} \sqrt{\frac{\pi \lambda_e N_e}{\tau_t^\delta \tau_e^\delta}}, \quad (20)$$

where  $q_{sl}^{o,\eta=0}$  decreases linearly in  $\lambda_l$  and  $r_o$ , and increases linearly in  $\sqrt{\lambda_e}$  and  $\sqrt{N_e}$ .

*Proof 3:* Please refer to Appendix B.

Corollary 2 provides some useful insights into the optimal fraction of FD receivers, which will benefit network design. For example, more FD receivers are needed to cope with more eavesdroppers or more eavesdropping antennas; whereas adding legitimate nodes or increasing jamming power allows a smaller fraction of FD receivers. In addition, we should better activate fewer FD receivers when legitimate link distance  $r_o$  increases, since the desired signal suffers a greater attenuation and the negative effect of self-interference increases more significantly. Some of the properties in Corollary 2 are verified in Fig. 3, and the others are relatively intuitive.

Having obtained the optimal fraction  $q_{sl}^*$  given in (18), the maximum ASLN  $N^*$  can be calculated by plugging  $q_{sl}^*$  into (16). Fig. 4 depicts ASLN as a function of  $N_e$  and clearly demonstrates the superiority of our optimization scheme over those fixed- $q$  schemes. For example, the maximum ASLN obtained at  $q = q_{sl}^*$  is nearly twice as large as that obtained at  $q = 0.5$  for a small  $N_e$ , and is more than twice as large as that obtained at  $q = 0.1$  for a large  $N_e$ . We observe that, as  $\rho$  increases, the ASLN obtained at  $q = 0.5$  becomes smaller in the small  $N_e$  region whereas becomes larger in the large  $N_e$  region. The underlying reason is, when  $N_e$  is small, the negative impact of jamming signals on legitimate links is larger than that on wiretap links such that fewer FD jammers should be activated; conversely, as  $N_e$  increases, the negative effect of jamming signals on wiretap links increases obviously. In

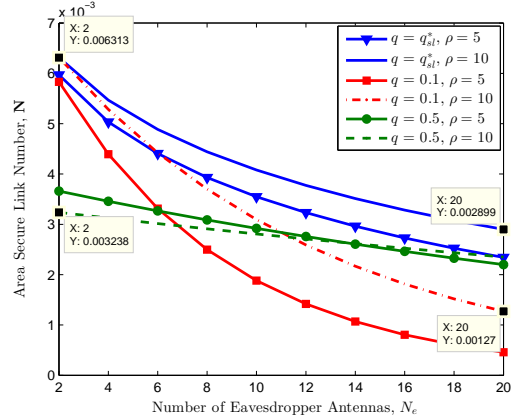


Fig. 4: ASLN vs.  $N_e$  for different values of  $q$  and  $\rho$ , with  $\alpha = 3$ ,  $\lambda_l = 10^{-2}$ ,  $\lambda_e = 10^{-3}$ ,  $\eta = -7\text{dB}$ ,  $\tau_t = 2$  and  $\tau_e = 1$ .

sharp contrast to this, the maximum  $N^*$  always increases in  $\rho$  regardless of  $N_e$ . This is because the optimal fraction  $q_{sl}^*$  adaptively decreases as  $\rho$  increases so as to mitigate the negative effect of jamming signals.

## V. NETWORK-WIDE SECRECY THROUGHPUT

In this section, we maximize NST  $\Omega$  under a pair of outage probabilities  $\sigma$  and  $\epsilon$  by determining the optimal fraction  $q$  of FD receivers, which can be formulated as

$$\max_q \Omega, \quad \text{s.t. } 0 < q \leq 1. \quad (21)$$

To proceed, we first derive the SIR thresholds  $\tau_t^S$  and  $\tau_e^S$  that satisfy  $p_{co}^S(\tau_t^S) = \sigma$  and  $p_{so}^S(\tau_e^S) = \epsilon$ , respectively. We can easily calculate  $\tau_t^{\text{HD}}$  from (9); whereas it is in general difficult to derive analytical expressions for  $\tau_t^{\text{FD}}$ . However, as reported in [30], self-interference can be efficiently mitigated by exploiting the propagation domain, analog circuit domain and digital circuit domain; particularly in analog and digital signal processing it is now feasible to have up to 110 dB SIC capability [31]. Such positive news motivates us to consider a perfect SIC case by ignoring self-interference in order to facilitate the design. Letting  $\eta = 0$  in (9) and (15) yields uniform expressions for  $\tau_t^S$  and  $\tau_e^S$ , respectively, given by

$$\tau_t^o = \left( \frac{\sigma_o}{\kappa (\lambda^{\text{HD}} + [1 + \rho^\delta] \lambda^{\text{FD}}) r_o^2} \right)^{\alpha/2}, \quad (22)$$

$$\tau_e^o = \left( \frac{\pi \lambda_e N_e}{\kappa \rho^\delta \lambda^{\text{FD}} \epsilon_o} \right)^{\alpha/2}, \quad (23)$$

where  $\sigma_o \triangleq \ln \frac{1}{1-\sigma}$  and  $\epsilon_o \triangleq \ln \frac{1}{1-\epsilon}$ . Substituting  $\tau_t^S = \tau_t^o$  and  $\tau_e^S = \tau_e^o$  into (5) yields

$$\Omega = \lambda_l (1 - \sigma) \left[ \ln \frac{1 + \tau_t^o}{1 + \tau_e^o} \right]^+. \quad (24)$$

Clearly, to achieve a positive  $\Omega$ , we should ensure  $\tau_t^o > \tau_e^o$ , which is equivalent to

$$q > q_m \triangleq (\Delta - 1)^{-1} \rho^{-\delta}, \quad (25)$$

where  $\Delta \triangleq \frac{\sigma_o \epsilon_o}{\pi \lambda_e N_e r_o^2}$ . This indicates, to meet outage probability constraints, a minimum fraction  $q_m$  must be guaranteed. Given that  $q_m < 1$ , the choice of  $\sigma$  and  $\epsilon$  should satisfy

$$\Delta > 1 + \rho^{-\delta}, \quad (26)$$

i.e., too small a  $\sigma$  and/or too small an  $\epsilon$  might not be promised. In the following, we only consider the non-trivial case of a positive  $\Omega$ , i.e.,  $q > q_m$ ; and thus, maximizing  $\Omega$  in (24) is equivalent to maximizing  $\ln \frac{1+\tau_o}{1+\tau_e}$ . Recalling (22), we introduce the following auxiliary function

$$w(q) = \ln \frac{w_1(q)}{w_2(q)}, \quad (27)$$

where  $w_1(q) = 1 + \beta_1(1 + \rho^\delta q)^{-\frac{\alpha}{2}}$  with  $\beta_1 \triangleq \left(\frac{\sigma_o}{\kappa \lambda_l r_o^2}\right)^{\frac{\alpha}{2}}$ ,  $w_2(q) = 1 + \beta_2(\rho^\delta q)^{-\frac{\alpha}{2}}$  with  $\beta_2 \triangleq \left(\frac{\pi \lambda_e N_e}{\kappa \lambda_l \epsilon_o}\right)^{\frac{\alpha}{2}}$ , and  $w_1(q) > w_2(q) > 1$  for  $q \in (q_m, 1]$ . Hence, problem (24) changes to

$$\max_q w(q), \quad \text{s.t. } 0 < q_m < q \leq 1. \quad (28)$$

Fortunately, we also successfully prove the quasi-concavity of  $w(q)$  in  $q$  and provide the optimal solution of problem (28) in the following theorem.

**Theorem 5:** The optimal fraction of FD receivers that maximizes the NST  $\Omega$  in (24) is

$$q_{st}^* = \begin{cases} \emptyset, & \pi \lambda_e N_e \epsilon_o^{-1} \in [X, \infty), \\ 1, & \pi \lambda_e N_e \epsilon_o^{-1} \in [Y, X), \\ q_{st}^o, & \pi \lambda_e N_e \epsilon_o^{-1} \in (0, Y), \end{cases} \quad (29)$$

where  $q_{st}^* = \emptyset$  corresponds to an empty feasible region of  $q$ ,  $X \triangleq \sigma_o / (r_o^2 (1 + \rho^{-\delta}))$ ,  $Y \triangleq \left( \kappa^{-\alpha/2} \lambda_l^{-\alpha/2} \rho^{-(1+\delta)} + (1 + \rho^{-\delta}) X^{-\alpha/2} \right)^{-\delta} < X^2$ , and  $q_{st}^o$  is the unique root  $q$  that satisfies

$$1 - \frac{1 + \rho^\delta q + \beta_1^{-1} (1 + \rho^\delta q)^{1+\alpha/2}}{\rho^\delta q + \beta_2^{-1} (\rho^\delta q)^{1+\alpha/2}} = 0. \quad (30)$$

The LHS of (30) is a monotonically increasing function of  $q$  in the range  $q \in (q_m, 1]$ , and is first negative and then positive when  $\pi \lambda_e N_e \epsilon_o^{-1} \in (0, Y)$ ; and thus, the value of  $q_{st}^o$  can be efficiently calculated using the bisection method with (30).

*Proof 4:* Please refer to Appendix C.

Theorem 5 shows that when  $N_e$  or  $\lambda_e$  is sufficiently small such that  $\pi \lambda_e N_e \epsilon_o^{-1} < X$ , there exists a unique fraction  $q$  that maximizes NST  $\Omega$ ; otherwise no positive  $\Omega$  can be achieved.

In the following corollary, we provide some insights into the optimal  $q_{st}^o$  given in (29).

**Corollary 3:** The optimal  $q_{st}^o$  given in (29) monotonically increases with  $\lambda_e$ ,  $N_e$  and  $r_o$ , and monotonically decreases with  $\sigma$ ,  $\epsilon$ ,  $\rho$  and  $\lambda_l$ .

*Proof 5:* Please refer to Appendix D.

Corollary 3 indicates that under a moderate constraint on the connection outage probability (a large  $\sigma$ ) or on the secrecy outage probability (a large  $\epsilon$ ), we should reduce the portion of FD receivers. This is because, on one hand, reducing FD receivers decreases interference such that greatly benefits

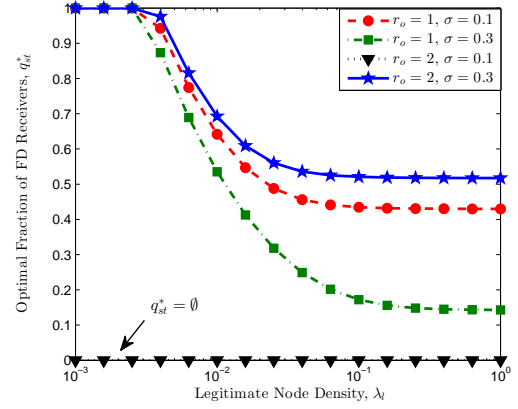


Fig. 5: The optimal fraction of FD receivers that maximizes NST  $\Omega$  vs.  $\lambda_l$  for different values of  $r_o$  and  $\sigma$ , with  $\alpha = 4$ ,  $\lambda_e = 10^{-4}$ ,  $N_e = 4$ ,  $\rho = 2$  and  $\epsilon = 0.05$ .

legitimate transmissions especially when a large  $\sigma$  is tolerable; on the other hand, if a large  $\epsilon$  is tolerable, we need fewer FD jammers against eavesdropping. It is worth mentioning that the optimal fraction  $q_{st}^o$  increases as  $r_o$  increases, which is just the opposite of what we have observed in Corollary 2. The reason behind is that here we have ignored self-interference and meanwhile eavesdroppers who are close to a legitimate transmitter is less impaired by the paired FD receiver as  $r_o$  increases, hence more FD receivers are needed.

The aforementioned theoretic results are validated in Fig. 5, where we see that the optimal fraction  $q_{st}^o$  deeply depends on parameters  $r_o$  and  $\sigma$ . When  $r_o$  is large and meanwhile  $\sigma$  is small (e.g.,  $r_o = 2$ ,  $\sigma = 0.1$ ) such that condition (26) is violated, there exists no positive NST no matter how the network design allocates FD and HD receivers. That means in such a legitimate transmission distance, the connection outage probability requirement is too rigorous to satisfy. In order to achieve a certain level of NST, network design should have to relax the connection outage probability constraint or shorten the legitimate distance.

Let us recall (47) in Appendix D, it is not difficult to deduce that  $q_{st}^o$  is inversely proportional to  $\rho^\delta$ , since  $\rho^\delta q_{st}^o$  keeps constant in  $\phi(\rho^\delta q_{st}^o) = 0$  when the other parameters are fixed. As a consequence,  $q_{st}^o \rightarrow 0$  as  $\rho \rightarrow \infty$ . If we consider a dense network by letting  $\lambda_l \rightarrow \infty$  in (48), we can further obtain a simple expression for  $q_{st}^o$  given below

$$q_{st}^o, \lambda_l \rightarrow \infty = \left( \Delta^{1/(1+\delta)} - 1 \right)^{-1} \rho^{-\delta}, \quad (31)$$

which is independent of  $\lambda_l$ , just as shown in Fig. 5. This is different from what we can see in Fig. 3 where the optimal  $q_{st}^*$  goes to zero as  $\lambda_l$  goes to infinity. This is because a positive secrecy rate mainly depends on the relative interference strength between legitimate nodes and eavesdroppers as  $\lambda_l$  goes to infinity, and a certain portion of FD receivers must be activated to ensure the superiority of the main channel over the wiretap channel in terms of channel quality.

Substituting  $q_{st}^*$  given in (29) into (24), we obtain the maximum NST  $\Omega^*$ . Fig. 6 compares this NST  $\Omega^*$  and those obtained at fixed  $q$ 's. Obviously, activating a proper fraction

$$^2 Y < ((1 + \rho^{-\delta}) X^{-\alpha/2})^{-\delta} = (1 + \rho^{-\delta})^{-\delta} X < X.$$



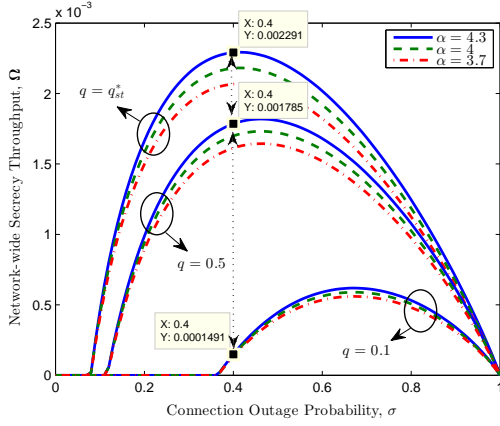


Fig. 6: NST vs.  $\sigma$  for different values of  $\alpha$ , with  $\lambda_l = 10^{-3}$ ,  $\lambda_e = 10^{-4}$ ,  $N_e = 4$ ,  $r_o = 1$ ,  $\epsilon = 0.01$  and  $\rho = 1$ .

of FD receivers significantly improves NST. For example, the optimal fraction  $q_{st}^*$  increases NST by about 28% than the equal proportion case (i.e.,  $q = 0.5$ ), and by up to 1400% than the small- $q$  case (e.g.,  $q = 0.1$ ). We can observe that, too small a  $\sigma$  might not be satisfied while too large a  $\sigma$  results in a small successful transmission probability and accordingly small NST. Therefore, a moderate constraint on the connection outage probability is desirable for improving NST. Fig. 6 also illustrates the influence of the path loss exponent  $\alpha$  on NST. A general trend is that NST increases as  $\alpha$  becomes larger. The reason behind is that the distance between a legitimate transmitter-receiver pair is small such that the signal attenuation in a legitimate link is less significant than it is in the eavesdropper link. This implies short-range secure communications might prefer a large path-loss exponent, especially in a sparse-eavesdropper environment.

## VI. NETWORK-WIDE SECRECY ENERGY EFFICIENCY

In this section, we determine the optimal fraction  $q$  of FD receivers that maximizes the NSEE  $\Psi$  with and without considering a required minimum NST. As presented in previous sections, we consider the scenario where self-interference is efficiently canceled.

### A. Without NST Constraint

In this subsection, we ignore the requirement of a minimum NST. Substituting (24) into (6), the optimization problem of interest can be formulated as

$$\max_q \Psi = \frac{\lambda_l(1-\sigma)w(q)}{\lambda_l(P_t + P_c) + q\lambda_l P_j}, \quad \text{s.t. } 0 < q_m < q \leq 1, \quad (32)$$

where  $w(q)$  and  $q_m$  have been defined in (27) and (28), respectively. Introducing  $\rho_c \triangleq \frac{P_j}{P_t + P_c}$  and the following auxiliary function

$$J(q) = \frac{w(q)}{1 + \rho_c q}, \quad (33)$$

the object function  $\Psi$  of problem (32) can be rewritten in the form of  $\Psi = \frac{1-\sigma}{P_t + P_c} J(q)$ . Clearly, maximizing  $\Psi$  is equivalent

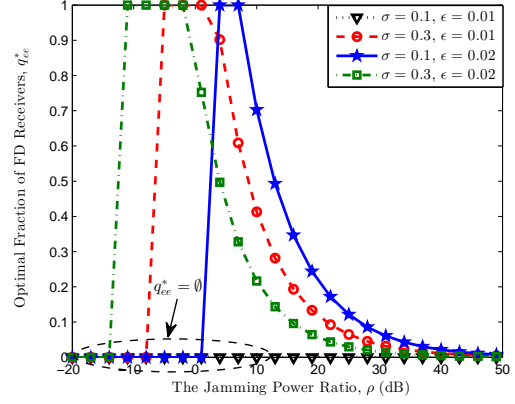


Fig. 7: The optimal fraction of FD receivers that maximizes NSEE  $\Psi$  vs.  $\rho$  for different values of  $\sigma$  and  $\epsilon$ , with  $\alpha = 4$ ,  $\lambda_l = 10^{-3}$ ,  $\lambda_e = 10^{-4}$ ,  $N_e = 4$  and  $r_o = 1$ .

to maximizing  $J(q)$ . In the following theorem, we prove the quasi-concavity of  $J(q)$  in  $q$ , again, and provide the optimal solution to problem (32).

**Theorem 6:** The optimal fraction of FD receivers that maximizes the NSEE  $\Psi$  in (32) is

$$q_{ee}^* = \begin{cases} \emptyset, & \pi\lambda_e N_e \epsilon_o^{-1} \geq X, \\ 1, & \pi\lambda_e N_e \epsilon_o^{-1} < X \text{ \& } \frac{W}{w(1)} > \frac{\delta\rho_c}{1+\rho_c}, \\ q_{ee}^o, & \text{otherwise,} \end{cases} \quad (34)$$

where  $W \triangleq 1 - w_2^{-1}(1) - \frac{1-w_1^{-1}(1)}{1+\rho_c}$  and  $X$  has been defined in Theorem 5. In (34),  $q_{ee}^o$  is the unique root  $q$  of the following equation

$$Q(q) = 0, \quad (35)$$

where  $Q(q) = w'(q)(1 + \rho_c q) - \rho_c w(q)$  is initially positive and then negative as  $q$  increases; and thus the value of  $q_{ee}^o$  can be efficiently computed using the bisection method with (35).

*Proof 6:* Please refer to Appendix E.

In the following corollary, we develop some insights into the behavior of  $q_{ee}^o$  given in (34).

**Corollary 4:** The optimal  $q_{ee}^o$  given in (34) monotonically increases with  $\lambda_e$ ,  $N_e$  and  $r_o$ , and monotonically decreases with  $\sigma$ ,  $\epsilon$  and  $\rho$ .

*Proof 7:* Please refer to Appendix F.

The properties of  $q_{ee}^o$  follow Corollary 3. Fig. 7 depicts the optimal fraction  $q_{ee}^*$  and verifies Corollary 4 well. We see that, too small  $\sigma$  and  $\epsilon$  might not be simultaneously satisfied (e.g.,  $\sigma = 0.1$ ,  $\epsilon = 0.01$ ). As can be observed, the optimal  $q_{ee}^*$  keeps large in the small  $\rho$  region, and dramatically decreases as  $\rho$  increases. This is because the increase of jamming power provides a relief to the need of FD jammers. In addition, as  $\sigma$  or  $\epsilon$  decreases, the feasible region of  $\rho$  that produces a positive  $\Psi$  reduces. This suggests that to meet more rigorous connection outage and secrecy outage constraints, we should consume more power in sending jamming signals.

Fig. 8 depicts NSEE versus  $\rho$  for different values of  $q$ . We see that as  $\rho$  increases, NSEE first increases and then decreases. The underlying reason is that too small jamming power makes NST small whereas too large jamming power



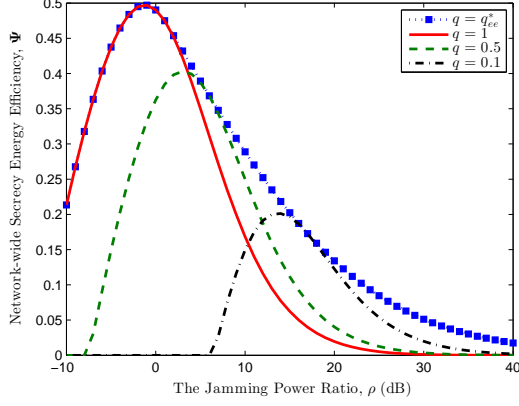


Fig. 8: NSEE  $\Psi$  vs.  $\rho$  for different values of  $q$ , with  $\alpha = 4$ ,  $\lambda_l = 10^{-3}$ ,  $\lambda_e = 10^{-4}$ ,  $N_e = 4$ ,  $\sigma = 0.3$ ,  $\epsilon = 0.02$  and  $r_o = 1$ .

leads to large power consumption; both aspects result in small NSEE. We also find that adaptively adjusting the fraction of FD receivers to jamming power significantly improves NSEE compared with fixed- $q$  cases, although the latter can approach the optimal performance in some specific regions, e.g.,  $q = 1$  in the small  $\rho$  region.

In the following corollary, we reveal how the legitimate node density  $\lambda_l$  influences the optimal allocation between FD and HD receivers and the corresponding NSEE.

*Corollary 5:* In a sparse network, i.e.,  $\lambda_l \rightarrow 0$ , both the optimal fraction  $q_{ee}^*$  and the maximum NSEE  $\Psi^*$  keep constant, which are independent of  $\lambda_l$ .

*Proof 8:* Please refer to Appendix G.

### B. With NST Constraint

For more practical design, we should also take NST into consideration when maximizing NSEE. In this subsection, we impose a constraint on problem (32) that NST  $\Omega$  lies above threshold  $\Omega^\circ$ , i.e.,  $\Omega > \Omega^\circ$ . Since we have already obtained the maximum  $\Omega^*$  in Sec. VI-A, for convenience, we only consider the case  $\Omega^* > \Omega^\circ$  here. If  $\Omega^* \leq \Omega^\circ$ , we just set  $\Psi$  to zero.

*Corollary 6:* The optimal fraction of FD receivers that maximizes the NSEE  $\Psi$  in (32) subject to the constraint  $\Omega > \Omega^\circ$  is given as follows

$$q_{ee}^* = \begin{cases} \emptyset, & \pi\lambda_e N_e \epsilon_o^{-1} \geq X, \\ 1, & \pi\lambda_e N_e \epsilon_o^{-1} < X \text{ \& } \frac{W}{w(1)} > \frac{\delta\rho_c}{1+\rho_c}, \\ \max\left(q_{st}^{(1)}, q_{ee}^\circ\right), & Y \leq \pi\lambda_e N_e \epsilon_o^{-1} < X \text{ \& } \frac{W}{w(1)} \leq \frac{\delta\rho_c}{1+\rho_c}, \\ q_{ee}^+, & \text{otherwise,} \end{cases} \quad (36)$$

where  $q_{ee}^\circ$  has been given in (34) and  $q_{ee}^+$  is determined as

$$q_{ee}^+ = \begin{cases} q_{ee}^\circ, & q_{st}^{(1)} \leq q_{ee}^\circ < q_{st}^{(2)}, \\ q_{st}^{(1)}, & q_{ee}^\circ < q_{st}^{(1)}, \\ q_{st}^{(2)}, & q_{ee}^\circ \geq q_{st}^{(2)}. \end{cases} \quad (37)$$

Let us denote  $\Omega(q)$  as a function of  $q$ . If there exists only one root  $q \in (q_m, 1]$  that satisfies  $\Omega(q) = \Omega^\circ$ , we denote this root

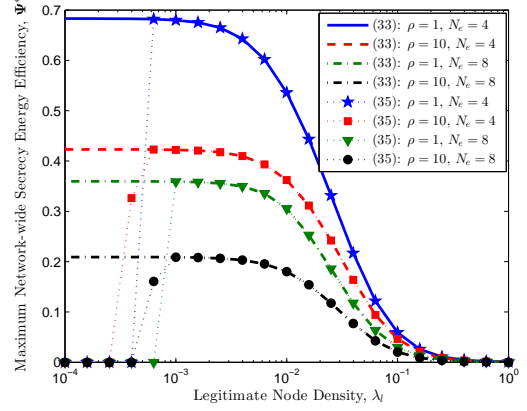


Fig. 9: The maximum NSEE  $\Psi^*$  vs.  $\lambda_l$  for different values of  $\rho$  and  $N_e$ , with  $\alpha = 4$ ,  $\lambda_e = 10^{-4}$ ,  $r_o = 1$ ,  $\sigma = 0.3$ ,  $\epsilon = 0.03$  and  $\Omega^\circ = 0.001$ . The results labeled (34) and (36) are obtained without and with the constraint  $\Omega > \Omega^\circ$ , respectively.

TABLE I: Relationships between Optimal  $q^*$  and Key Parameters

| Objectives | $q^*$ increases with  | $q^*$ decreases with                         |
|------------|-----------------------|--|
| ASLN       | $\lambda_e, N_e$      | $\lambda_l, r_o, \eta, \rho, \tau_t, \tau_e$ |
| NST        | $\lambda_e, N_e, r_o$ | $\lambda_l, \rho, \sigma, \epsilon$          |
| NSEE       | $\lambda_e, N_e, r_o$ | $\rho, \sigma, \epsilon$                     |

as  $q_{st}^{(1)}$ ; if there are two such roots, we denote them as  $q_{st}^{(1)}$  and  $q_{st}^{(2)}$  such that  $q_{st}^{(1)} < q_{st}^{(2)}$ .

*Proof 9:* Please refer to Appendix H.

Fig. 9 shows the maximum NSEE  $\Psi^*$  with  $q_{ee}^*$  in (34) and  $\Psi^*$  with  $q_{ee}^*$  in (36). As indicated in Corollary 4,  $\Psi^*$  keeps constant in the small  $\lambda_l$  region, whereas  $\Psi^*$  becomes zero since the constraint  $\Omega > \Omega^\circ$  is not satisfied. When  $\lambda_l$  falls in the medium range, the curve of  $\Psi^*$  and its counterpart  $\Psi^*$  merge and vary smoothly. As  $\lambda_l$  increases further, both  $\Psi^*$  and  $\Psi^*$  quickly drop to zero. Therefore, a moderate network density is desirable. Fig. 9 also indicates that although increasing jamming power helps to suppress eavesdroppers, it is at a cost of energy efficiency.

To better guide network designers on how to well design the network, Table I summarizes the relationships between the optimal fraction  $q$  of FD receivers and key parameters in different objectives.

## VII. CONCLUSION AND FUTURE WORK

In this paper, we study physical layer security in a wireless ad hoc network with a hybrid full/half-duplex receiver deployment strategy. We provide a comprehensive performance analysis and network design under a stochastic geometry framework. We first analyze connection outage and secrecy outage probabilities for a typical legitimate link, and show that enabling more FD receivers increases the connection outage probability but decreases the secrecy outage probability. Based on the analytical results of the dual probabilities, we prove that ASLN, NST and NSEE are all *quasi-concave* on the fraction of FD receivers, and maximize each of them by providing the optimal fraction. We further develop various useful properties on this optimal fraction. Numerical results are demonstrated to validate our theoretical findings.

This paper opens up several interesting research directions. For example, the proposed framework can be extended to investigate the cooperative or multi-antenna FD receivers, where additional degrees of freedom might be gained not only in alleviating the self-interference but also in designing the jamming signals. The benefit of FD receiver jamming techniques can be further exploited by jointly optimizing the allocation between FD and HD receivers and the jamming transmit power of each FD receiver, given that the latter also strikes a non-trivial tradeoff between reliability and secrecy. Another possible direction for future research is to consider the randomness of self-interference and propose an adaptive and intelligent criterion to select work mode for receivers, e.g., letting those receivers with instantaneous self-interference power lying below a certain value work in the FD mode and the rest work in the HD mode.

## APPENDIX

### A. Proof of Theorem 4

We start by taking the first-order derivative of  $F(q)$  on  $q$

$$F'(q) = K(q)e^{-Bq-C/q}, \quad (38)$$

where

$$K(q) = (A + 1/q - 1)(1 + C/q - Bq) - 1/q. \quad (39)$$

To determine the sign of  $F'(q)$ , we first investigate the behavior of  $K(q)$  at the boundaries  $q \rightarrow 0^+$  and  $q = 1$ , respectively. Substituting  $q \rightarrow 0^+$  into (39) yields  $\lim_{q \rightarrow 0^+} K(q) = \lim_{q \rightarrow 0^+} (C/q^2) > 0$ . Substituting  $q = 1$  into (39) yields  $K(1) = A(1 + C - B) - 1$ , the sign of which relies on specific values of  $A$ ,  $B$  and  $C$ . Consider the following two cases.

1)  $K(1) > 0$ : We have  $A(1 + C - B) > 1 \Rightarrow C - B > 1/A - 1 > 0$ , which yields  $C/q - Bq \geq C - B > 0$ . Substituting this inequality along with  $1/q > 1$  into (38), we obtain  $K(q) > A(1 + C - B) - 1 > 0$ , i.e.,  $F'(q) > 0$ . This means  $F(q)$  monotonically increases in  $q$  within the entire range  $q \in (0, 1]$ , and the optimal  $q$  that maximizes  $F(q)$  or  $N$  is  $q^* = 1$ .

2)  $K(1) < 0$ : There at least exists one point  $q \in (0, 1]$  that satisfies  $K(q) = 0$  since  $K(q)$  is a continuous function of  $q$  and  $\lim_{q \rightarrow 0^+} K(q) > 0$ . Denote an arbitrary zero-crossing point  $q$  of  $K(q)$  as  $q_o$ , i.e.,  $K(q_o) = 0$ . To determine the monotonicity of  $F(q)$  in  $q$ , we first take the second-order derivative of  $F(q)$  at  $q = q_o$  from (38)

$$F''(q_o) = K'(q_o)e^{-Bq_o-C/q_o}, \quad (40)$$

where

$$K'(q_o) = (B + Cq_o^{-2})A + 2Cq_o^{-3} - Cq_o^{-2} - B. \quad (41)$$

Clearly, the sign of  $F''(q_o)$  follows that of  $K'(q_o)$ . We resort to the equation  $K(q_o) = 0$  in (39), which yields  $A = 1 - \frac{1}{q_o} \left(1 - \frac{1}{1+C/q_o-Bq_o}\right)$ . Given that  $0 < A < 1$ , we readily obtain  $C/q > Bq$ , substituting which combined with  $0 < q_o \leq 1$  into (41) yields  $K'(q_o) < 0$ , i.e.,  $F''(q_o) < 0$ . Invoking the definition of single-variable quasi-concave function [34, Sec. 3.4.2], we conclude that  $F(q)$  is a quasi-concave function of  $q$ , and there exists a unique  $q$  that maximizes  $F(q)$ . In other

words,  $F(q)$  initially increases and then decreases in  $q$ , and the peak value of  $F(q)$  is achieved at the unique root  $q$  of the equation  $K(q) = 0$ . By now, we have completed the proof.

### B. Proof of Corollary 2

Recall (39), and the optimal  $q_{sl}^o$  satisfies  $K(q_{sl}^o) = 0$ . We first take the first-order derivative of  $q_{sl}^o$  on  $A$  using the derivative rule for implicit functions with  $K(q_{sl}^o) = 0$ , i.e.,

$$\frac{dq_{sl}^o}{dA} = -\frac{\partial K(q_{sl}^o)/\partial A}{\partial K(q_{sl}^o)/\partial q_{sl}^o}. \quad (42)$$

From (39), we have  $\partial K(q_{sl}^o)/\partial A = 1 + C/q_{sl}^o - Bq_{sl}^o > 0$ . From (41), we know that  $\partial K(q_{sl}^o)/\partial q_{sl}^o < 0$ . Thus, we obtain  $dq_{sl}^o/dA > 0$ . In a similar way, we can prove  $dq_{sl}^o/dB < 0$  and  $dq_{sl}^o/dC > 0$ . Observing the expressions of  $A$ ,  $B$  and  $C$  directly yields the relationships between the optimal  $q_{sl}^o$  and the relevant parameters. For the perfect SIC case, substituting  $\eta = 0$ , or, equivalently,  $A = 1$ , into (19) directly yields the result given in (20).

### C. Proof of Theorem 5

Taking the first-order derivative of  $w(q)$  in (27) on  $q$ , i.e.,

$$w'(q) = \frac{w'_1(q)}{w_1(q)} - \frac{w'_2(q)}{w_2(q)}, \quad (43)$$

where  $w'_1(q) = -\frac{\rho^\delta[w_1(q)-1]}{\delta(1+\rho^\delta q)}$  and  $w'_2(q) = -\frac{w_2(q)-1}{\delta q}$ . Directly determining either the sign of  $w'(q)$  or the concavity of  $w(q)$  from the second-order derivative  $w''(q)$  is difficult. Instead, we prove the quasi-concavity of  $w(q)$  on  $q$  by reforming  $w'(q)$  as  $w'(q) = \frac{w_1(q)}{w_1(q)}\phi(q)$  with  $\phi(q)$  given by

$$\phi(q) = 1 - \frac{w_1(q)w'_2(q)}{w'_1(q)w_2(q)} = 1 - \frac{(1 + \rho^\delta q)w_1(q)(w_2(q) - 1)}{\rho^\delta q(w_1(q) - 1)w_2(q)}. \quad (44)$$

Apparently, the first term  $w'_1(q)/w_1(q)$  is negative. Next, we determine the sign of  $\phi(q)$ . Taking the first-order derivative of  $\phi(q)$  on  $q$ , and after some algebraic manipulations, we obtain

$$\phi'(q) = \frac{[1 + \delta w_2(q)]w_1(q) + \rho^\delta q[w_1(q) - w_2(q)]}{\delta \rho^\delta q^2[w_1(q) - 1]w_2^2(q)/[w_2(q) - 1]}. \quad (45)$$

Since  $w_1(q) > w_2(q) > 1$ ,  $\phi'(q) > 0$  always holds, i.e.,  $\phi(q)$  monotonically increases with  $q$ . When  $q = q_m$ , we have  $w_1(q_m) = w_2(q_m)$  and  $\frac{w_2(q_m)}{w_1(q_m)} = \frac{1+\rho^\delta q_m}{\rho^\delta q_m}$ , thus  $\phi(q_m) = -\frac{1}{\rho^\delta q_m} < 0$ . When  $q = 1$ ,  $\phi(1) = 1 - \frac{\beta_2(1+\rho^\delta)(\beta_1+(1+\rho^\delta)^{\alpha/2})}{\beta_1\rho^\delta(\beta_2+\rho)}$ , the sign of which depends on  $\beta_1$  and  $\beta_2$ . Specifically, if  $1 + \beta_1^{-1}(1 + \rho^\delta)^{1+\alpha/2} > \beta_2^{-1}\rho^{1+\delta}$ , we have  $\phi(1) < 0$ ; otherwise,  $\phi(1) \geq 0$ . In the following, we derive the optimal  $q$  that maximizes  $w(q)$  by distinguishing two cases.

1) If  $\phi(1) < 0$ ,  $\phi(q) < 0$  holds in the entire range  $q \in (q_m, 1]$ . Accordingly, we have  $w'(q) > 0$ , i.e.,  $w(q)$  monotonically increases with  $q$ . Therefore, the optimal  $q$  that maximizes  $w(q)$  is  $q^* = 1$ .

2) If  $\phi(1) \geq 0$ ,  $\phi(q)$  is initially negative and then positive in the range  $q \in (q_m, 1]$ ; the zero-crossing point  $q$  that satisfies

$\phi(q) = 0$  is denoted by  $q_o$ . We can also conclude that  $w'(q)$  is initially positive and then negative after  $q$  exceeds  $q_o$ . In other words,  $w(q)$  first increases and then decreases with  $q$ , and  $q_o$  is the solution that yields the peak value of  $w(q)$ .

By now, we have proved the quasi-concavity of  $w(q)$  on  $q$ . Combined with  $q_m < 1 \Rightarrow \Delta > 1 + \rho^{-\delta}$  and the given results, we complete the proof.

#### D. Proof of Corollary 3

Recall (44), and the optimal  $q_{st}^o$  satisfies  $\phi(q_{st}^o) = 0$ . Taking the first-order derivative of  $q_{st}^o$  on  $\beta_1$  using the derivative rule for implicit functions with  $\phi(q_{st}^o) = 0$  yields

$$\frac{dq_{st}^o}{d\beta_1} = -\frac{\partial\phi(q_{st}^o)/\partial\beta_1}{\partial\phi(q_{st}^o)/\partial q_{st}^o}, \quad (46)$$

where  $\frac{\partial\phi(q_{st}^o)}{\partial\beta_1} = \frac{\beta_1^{-2}(1+\rho^\delta q)^{1+\alpha/2}}{\rho^\delta q + \beta_2^{-1}(\rho^\delta q)^{1+\alpha/2}} > 0$  and  $\frac{\partial\phi(q_{st}^o)}{\partial q_{st}^o} > 0$  (see (45)); and thus,  $\frac{dq_{st}^o}{d\beta_1} < 0$ . Similarly, we can prove  $\frac{dq_{st}^o}{d\beta_2} > 0$ . From the expressions of  $\beta_1$  and  $\beta_2$  given in (27), we can infer that  $q_{st}^o$  increases in  $\lambda_e$ ,  $N_e$  and  $r_o$ , while decreases in  $\sigma$  and  $\epsilon$ . As to  $\frac{dq_{st}^o}{d\rho}$ , we first express  $\phi(\rho^\delta q)$  as

$$\phi(\rho^\delta q) = 1 - \frac{1 + \rho^\delta q + \beta_1^{-1}(1 + \rho^\delta q)^{1+\alpha/2}}{\rho^\delta q + \beta_2^{-1}(\rho^\delta q)^{1+\alpha/2}}. \quad (47)$$

Taking the first-order derivative of  $\phi(\rho^\delta q)$  on  $\rho^\delta q$  and invoking the equation  $\phi(\rho^\delta q_{st}^o) = 0$ , we can prove  $\frac{\partial\phi(q_{st}^o)}{\partial\rho} > 0$ . Thereby, we have  $\frac{dq_{st}^o}{d\rho} = -\frac{\partial\phi(q_{st}^o)/\partial\rho}{\partial\phi(q_{st}^o)/\partial q_{st}^o} < 0$ . As to  $\frac{dq_{st}^o}{d\lambda_l}$ , we let

$$\phi(\lambda_l) = 1 - \frac{1 + \rho^\delta q + b_1 \lambda_l^{\alpha/2} (1 + \rho^\delta q)^{1+\alpha/2}}{\rho^\delta q + b_2 \lambda_l^{\alpha/2} (\rho^\delta q)^{1+\alpha/2}}, \quad (48)$$

where  $b_1 \triangleq \left(\frac{\kappa r_o^2}{\sigma_o}\right)^{\frac{\alpha}{2}}$  and  $b_2 \triangleq \left(\frac{\kappa \epsilon_o}{\pi \lambda_e N_e}\right)^{\frac{\alpha}{2}}$ . Taking the first-order derivative of  $\phi(\lambda_l)$  on  $\lambda_l$  and invoking  $\beta_1(1 + \rho^\delta q)^{-\alpha/2} > \beta_2(\rho^\delta q)^{-\alpha/2}$  in (27), we can prove  $\frac{\partial\phi(q_{st}^o)}{\partial\lambda_l} > 0$  and  $\frac{dq_{st}^o}{d\lambda_l} = -\frac{\partial\phi(q_{st}^o)/\partial\lambda_l}{\partial\phi(q_{st}^o)/\partial q_{st}^o} < 0$ . By now, the proof is complete.

#### E. Proof of Theorem 6

We start by giving the first-order derivative of  $J(q)$  on  $q$ ,

$$J'(q) = Q(q)(1 + \rho_c q)^{-2}, \quad (49)$$

where  $Q(q)$  is given in (35). To proceed, we first give the following lemma which is very important to subsequent proof.

**Lemma 1:** If  $w'(q) > 0$  for  $q \in (q_m, 1]$ ,  $Q'(q) < 0$  holds.

**Proof 10:** Since  $Q'(q) = w''(q)(1 + Bq)$ , to prove  $Q'(q) > 0$  we need only to prove  $w''(q) > 0$ . Taking the derivative of  $w'(q)$  in (43) on  $q$  yields  $w''(q)$  which is given in (50) at the top of the next page, where the last equality holds for  $w_1'(q) = ((1 + \delta)[w_1(q) - 1]\rho^{2\delta}) / (\delta^2(1 + \rho^\delta q)^2)$  and  $w_2'(q) = ((1 + \delta)[w_2(q) - 1]) / (\delta^2 q^2)$ . Invoking (43), we can readily obtain the following relationship

$$w'(q) > 0 \Rightarrow \frac{w_2(q) - 1}{w_1(q) - w_2(q)} > \frac{\rho^\delta q}{w_1(q)}. \quad (51)$$

Plugging the above inequality into (50) yields

$$w''(q) < -\frac{w_1(q) - w_2(q)}{\delta^2 w_1(q) w_2^2(q) \rho^{-\delta} q (1 + \rho^\delta q)^2} \times \\ (1 + \rho^\delta q [1 - w_2(q)/w_1(q)] + \delta(1 + \rho^\delta q) w_2(q)) < 0, \quad (52)$$

which completes the proof.

Next, we are going to determine the sign of  $Q(q)$  or  $J'(q)$  in (49). We first determine the sign of  $Q(q)$  at the boundaries  $q_m$  and 1. Combined with  $w_1(q_m) = w_2(q_m)$ , we have

$$Q(q_m) = \frac{w_1(q_m) - 1}{\delta w_1(q_m)} \left( \frac{1}{q_m} - \frac{\rho^\delta}{1 + \rho^\delta q_m} \right) > 0. \quad (53)$$

Substituting  $q = 1$  into  $Q(q)$  yields

$$Q(1) = w'(1)(1 + \rho_c) - \rho_c w(1) = \\ \frac{\alpha}{2}(1 + \rho_c) \left( 1 - w_2^{-1}(1) - \frac{1 - w_1^{-1}(1)}{1 + \rho^{-\delta}} \right) - \rho_c w(1), \quad (54)$$

The sign of  $Q(1)$  depends on the values of involved parameters. Let us distinguish two cases.

1) If  $Q(1) > 0$ , we have  $w'(1) > 0$ . Since  $w(q)$  is quasi-concave in  $q$  (Theorem 5),  $w'(q) > 0$  holds in the whole range of  $q \in (q_m, 1]$ , which further yields  $Q'(q) < 0$  according to Lemma 1. In other words,  $Q(q)$  monotonically decreases in  $q$ , and thus,  $Q(q) > Q(1) > 0$ , or,  $J'(q) > 0$ . This means  $J(q)$  monotonically increases in  $q$ , and the optimal  $q$  that maximizes  $J(q)$  is  $q = 1$ .

2) If  $Q(1) \leq 0$ , combined with  $Q(q_m) > 0$  in (53), there at least exists one point  $q \in (q_m, 1]$  that satisfies  $Q(q) = 0$  due to the continuity of  $Q(q)$  in  $q$ . Denote a zero-crossing point  $q$  of  $Q(q)$  as  $q_o$  such that  $Q(q_o) = 0$ , or,  $J'(q_o) = 0$ . To determine the quasi-concavity of  $J(q)$  in  $q$ , we first take the second-order derivative of  $J(q)$  at  $q = q_o$ , which is

$$J''(q_o) = Q'(q_o)(1 + \rho_c q_o)^{-2}. \quad (55)$$

Recalling  $Q(q_o) = 0$  yields  $w'(q_o) = \frac{Bw(q_o)}{1 + \rho_c q_o} > 0$ . From Lemma 1, we obtain  $Q'(q_o) < 0$ , i.e.,  $J''(q_o) < 0$ . This means  $J(q)$  is quasi-concave on  $q$ , and the optimal  $q$  that maximizes  $J(q)$  is the unique root of equation  $Q(q) = 0$ , i.e.,  $q = q_o$ . By now, the proof is complete.

#### F. Proof of Corollary 4

Recall (35), and the optimal  $q_{ee}^o$  satisfies  $Q(q_{ee}^o) = 0$ . Similar to the proof of Corollary 3, we take the first-order derivative of  $q_{ee}^o$  on  $w_1(q_{ee}^o)$  and on  $w_2(q_{ee}^o)$ , respectively, using the derivative rule for implicit functions with  $Q(q_{ee}^o) = 0$ , and then prove  $\frac{dq_{ee}^o}{dw_1(q_{ee}^o)} < 0$  and  $\frac{dq_{ee}^o}{dw_2(q_{ee}^o)} > 0$ . Through observing the monotonicity of  $w_1(q)$  and  $w_2(q)$  with respect to the parameters involved in Corollary 4, we can complete the proof.

#### G. Proof of Corollary 5

The expressions of  $w_1(q)$  and  $w_2(q)$  in (27) tell that as  $\lambda_l \rightarrow 0$ , we have  $\frac{w_1(q)-1}{w_1(q)} \rightarrow 1$ ,  $\frac{w_2(q)-1}{w_2(q)} \rightarrow 1$  and  $w(q) \rightarrow \frac{\alpha}{2} \ln \Delta$ . Substituting these results into (35), we find  $Q(q)$  independent of  $\lambda_l$  and so is the root  $q$  of  $Q(q) = 0$ . Plugging the obtained solution  $q$  into (32), we can easily conclude that the resulting  $\Psi$  is also independent of  $\lambda_l$ . The proof is complete.

$$\begin{aligned}
w''(q) &= \frac{w_1''(q)w_1(q) - (w_1'(q))^2}{w_1^2(q)} - \frac{w_2''(q)w_2(q) - (w_2'(q))^2}{w_2^2(q)} \\
&= \frac{(w_1(q) - w_2(q))}{\delta^2 w_1^2(q) w_2^2(q) q^2 (1 + \rho^\delta q)^2} \left\{ \rho^\delta q \left( \rho^\delta q [w_1(q) + w_2(q) - w_1(q)w_2(q)] - \frac{2w_1^2(q)[w_2(q) - 1]}{w_1(q) - w_2(q)} \right) - \frac{w_1^2(q)[w_2(q) - 1]}{[w_1(q) - w_2(q)]} \right. \\
&\quad \left. + \delta \rho^\delta q w_1(q) w_2(q) \left( \rho^\delta q - \frac{2w_1(q)[w_2(q) - 1]}{w_1(q) - w_2(q)} \right) - \frac{\delta w_1^2(q) w_2(q)[w_2(q) - 1]}{w_1(q) - w_2(q)} \right\}, \quad (50)
\end{aligned}$$

## H. Proof of Corollary 6

Let us recall (34). Obviously,  $q_{ee}^* = \emptyset$  if  $q_{ee}^* = \emptyset$ ;  $q_{ee}^* = 1$  if  $q_{ee}^* = 1$  and  $\Omega(1) > \Omega^\circ$  simultaneously hold. When  $q_{ee}^* = q_{ee}^\circ$ , let us distinguish two cases. In the first case, there is only one root  $q \in (q_m, 1]$ , denoted as  $q_{st}^{(1)}$ , that satisfies  $\Omega(q) = \Omega^\circ$ . If  $q_{st}^{(1)} < q_{ee}^\circ$ , we have  $\Omega(q_{ee}^\circ) > \Omega^\circ$  and  $q_{ee}^* = q_{ee}^\circ$ ; otherwise,  $q_{ee}^* = q_{st}^{(1)}$ . In the second case, there are two roots  $q_{st}^{(1)}$  and  $q_{st}^{(2)}$  such that  $q_{st}^{(1)} < q_{st}^{(2)}$ . In a similar way, we can obtain  $q_{ee}^* = q_{ee}^+$  with  $q_{ee}^+$  given in (36). By now, the proof is complete.

## REFERENCES

- [1] H. V. Poor, "Information and inference in the wireless physical layer," *IEEE Wireless Commun.*, vol. 19, no. 1, pp. 40–47, Feb. 2012.
- [2] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.
- [3] R. Liu, T. Liu, H. V. Poor, and S. Shamai, "Multiple-input multiple-output Gaussian broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 56, no. 9, pp. 4215–4227, Sep. 2010.
- [4] X. Zhou and M. R. McKay, "Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation," *IEEE Trans. Veh. Technol.*, vol. 59, no. 8, pp. 3831–3842, Oct. 2010.
- [5] H.-M. Wang, T.-X. Zheng, and X.-G. Xia, "Secure MISO wiretap channels with multi-antenna passive eavesdropper: Artificial noise vs. artificial fast fading," *IEEE Trans. Wireless Commun.*, vol. 14, no. 1, pp. 94–106, Jan. 2015.
- [6] T.-X. Zheng, H.-M. Wang, F. Liu, and M. H. Lee, "Outage constrained secrecy throughput maximization for DF relay networks," *IEEE Trans. Communications*, vol. 63, no. 5, pp. 1741–1755, May 2015.
- [7] T.-X. Zheng, H.-M. Wang, J. Yuan, D. Towsley, and M. H. Lee, "Multi-antenna transmission with artificial noise against randomly distributed eavesdroppers," *IEEE Trans. Commun.*, vol. 63, no. 11, pp. 4347–4362, Nov. 2015.
- [8] T.-X. Zheng and H.-M. Wang, "Optimal power allocation for artificial noise under imperfect CSI against spatially random eavesdroppers," *IEEE Trans. Veh. Technol.*, vol. 65, no. 10, pp. 8812–8817, Oct. 2016.
- [9] H.-M. Wang, T.-X. Zheng, J. Yuan, D. Towsley, and M. H. Lee, "Physical layer security in heterogeneous cellular networks," *IEEE Trans. Commun.*, vol. 64, no. 3, pp. 1204–1219, Mar. 2016.
- [10] H.-M. Wang and T.-X. Zheng, *Physical Layer Security in Random Cellular Networks*. Singapore: Springer, 2016.
- [11] C. Ma, J. Liu, X. Tian, H. Yu, Y. Cui, and X. Wang, "Interference exploitation in D2D-enabled cellular networks: a secrecy perspective," *IEEE Trans. Commun.*, vol. 63, no. 1, pp. 229–242, Jan. 2015.
- [12] C. Wang and H.-M. Wang, "Physical layer security in millimeter wave cellular networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 8, pp. 5569–5585, Aug. 2016.
- [13] X. Zhou, R. Ganti, J. Andrews, and A. Hjørungnes, "On the throughput cost of physical tier security in DWNs," *IEEE Trans. Wireless Commun.*, vol. 10, no. 8, pp. 2764–2775, Aug. 2011.
- [14] X. Zhang, X. Zhou, and M. R. McKay, "Enhancing secrecy with multi-antenna transmission in wireless ad hoc networks," *IEEE Trans. Inf. Forensics and Security*, vol. 8, no. 11, pp. 1802–1814, Nov. 2013.
- [15] D. W. K. Ng, E. S. Lo, and R. Schober, "Energy-efficient resource allocation for secure OFDMA systems," *IEEE Trans. Veh. Technol.*, vol. 61, no. 6, pp. 2572–2585, July 2012.
- [16] X. Chen and L. Lei, "Energy-efficient optimization for physical layer security in multi-antenna downlink networks with QoS guarantee," *IEEE Commun. Lett.*, vol. 17, no. 4, pp. 637–640, Apr. 2013.
- [17] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.
- [18] L. Song, R. Wichman, Y. Li, and Z. Han, *Full-Duplex Communications and Networks*, Cambridge, UK: Cambridge Univ. Press, in progress, 2016.
- [19] W. Li, M. Ghogho, B. Chen, and C. Xiong, "Secure communication via sending artificial noise by the receiver: Outage secrecy capacity/region analysis," *IEEE Commun. Lett.*, vol. 16, no. 10, pp. 1628–1631, Oct. 2012.
- [20] G. Zheng, I. Krikidis, J. Li, A. Petropulu, and B. Ottersten, "Improving physical tier secrecy using full-duplex jamming receivers," *IEEE Trans. Signal Process.*, vol. 61, no. 20, pp. 4962–4974, Oct. 2013.
- [21] Y. Zhou, Z. Xiang, Y. Zhu, and Z. Xue, "Application of full-duplex wireless technique into secure MIMO communication: achievable secrecy rate based optimization," *IEEE Signal Process. Lett.*, vol. 21, no. 7, pp. 804–808, Jul. 2014.
- [22] Ö. Cepheli, S. Tedik, and G. K. Kurt, "A high data rate wireless communication system with improved secrecy: full duplex beamforming," *IEEE Commun. Lett.*, vol. 18, no. 6, pp. 1075–1078, Jun. 2014.
- [23] G. Chen, Y. Gong, P. Xiao, and J. A. Chambers, "Physical layer network security in the full-duplex relay system," *IEEE Trans. Inf. Forensics and Security*, vol. 10, no. 3, pp. 574–583, Mar. 2015.
- [24] S. Parsaefard, and . Le-Ngoc, "Improving wireless secrecy rate via full-duplex relay-assisted protocols," *IEEE Trans. Inf. Forensics and Security*, vol. 10, no. 10, pp. 2095–2107, Oct. 2015.
- [25] F. Zhu, F. Gao, T. Zhang, K. Sun, and M. Yao, "Physical-layer security for full duplex communications with self-interference mitigation," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 329–340, Jan. 2016.
- [26] T.-X. Zheng, H.-M. Wang, Q. Yang, and M. H. Lee, "Safeguarding decentralized wireless networks using full-duplex jamming receivers," *IEEE Trans. Wireless Commun.*, vol. 16, no. 1, pp. 278–292, Jan. 2017.
- [27] M. Haenggi, J. 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.
- [28] T.-X. Zheng, H.-M. Wang, and Q. Yin, "On transmission secrecy outage of a multi-antenna system with randomly located eavesdroppers," *IEEE Commun. Lett.*, vol. 18, no. 8, pp. 1299–1302, Aug. 2014.
- [29] D. Ha, K. Lee, and J. Kang, "Energy efficiency analysis with circuit power consumption in massive MIMO systems," in *Proc. 2013 Int. Symp. Personal, Indoor Mobile Radio Commun.*, pp. 938–942, London, UK, Sep. 2013.
- [30] J. Lee, and T. Q. S. Quek, "Hybrid full/half-duplex system analysis in heterogeneous wireless networks," *IEEE Trans. Wireless Commun.*, vol. 14, no. 5, pp. 2883–1895, May 2015.
- [31] D. Bharadia, E. McMillin, and S. Katti, "Full duplex radios," in *Proc. ACM SIGCOMM 2013*, Hong Kong, China, Aug. 2013.
- [32] M. Haenggi, *Stochastic Geometry for Wireless Networks*. Cambridge University Press, 2012.
- [33] I. S. Gradshteyn, I. M. Ryzhik, A. Jeffrey, D. Zwillinger, and S. Technica, *Table of Integrals, Series, and Products*, 7th ed. New York: Academic Press, 2007.
- [34] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, UK: Cambridge Univ. Press, 2004.