On the Throughput Cost of Physical Layer Security in Decentralized Wireless Networks

Xiangyun Zhou, *Member, IEEE*, Radha Krishna Ganti, *Member, IEEE*,
Jeffrey G. Andrews, *Senior Member, IEEE*, and Are Hjørungnes, *Senior Member, IEEE*

***Abstract*—This paper studies the throughput of large-scale decentralized wireless networks with physical layer security constraints. In particular, we are interested in the question of how much throughput needs to be sacrificed for achieving a certain level of security. We consider random networks where the legitimate nodes and the eavesdroppers are distributed according to independent two-dimensional Poisson point processes. The transmission capacity framework is used to characterize the area spectral efficiency of secure transmissions with constraints on both the quality of service (QoS) and the level of security. This framework illustrates the dependence of the network throughput on key system parameters, such as the densities of legitimate nodes and eavesdroppers, as well as the QoS and security constraints. One important finding is that the throughput cost of achieving a moderate level of security is quite low, while throughput must be significantly sacrificed to realize a highly secure network. We also study the use of a secrecy guard zone, which is shown to give a significant improvement on the throughput of networks with high security requirements.**

***Index Terms*—Physical layer security, decentralized wireless networks, transmission capacity, guard zone.**

I. Introduction

THE problem of securing wireless communications at the physical layer has recently drawn considerable attention. In the pioneering works on physical layer security, Wyner [1] introduced the wiretap channel for single point-to-point communication, which was extended to broadcast channels with both common and confidential messages by Csiszár and Körner [2]. Their results showed that perfect secrecy can be achieved if the intended receiver has a stronger channel than the eavesdropper. Recent studies on physical layer security primarily focused on communications involving a small number of nodes with multi-antenna transmission [3–5], cooperative transmission in relay channels [6, 7] or multiple access channels [8, 9]. However, few studies have been carried out for large-scale wireless networks. Unlike point-to-point communications, where it is reasonably easy to establish secret keys and have encrypted transmissions, security is more expensive and difficult to achieve in large-scale decentralized networks. Therefore, physical layer security may be important for exchanging secret keys and adding another layer of protection in such networks.

The communication between any pair of nodes in large-scale networks strongly depends on the locations of other nodes and how the nodes interact with each other. When secure communication is required in the presence of eavesdroppers, the locations and channel state information of the eavesdroppers, which are usually unknown, become extra parameters affecting the network throughput. Initial works on network security from an information-theoretic viewpoint mainly considered networks where the legitimate nodes and the eavesdroppers are randomly distributed, and studied the connectivity [10–14], coverage [15], and capacity scaling laws [16–18]. Specifically, various statistical characterizations of the existence of secure connections were given in [10–12, 14]. Using tools from percolation theory, the existence of a secrecy graph was analyzed in [10, 12, 13]. These connectivity results are concerned with the possibility of having secure communication, while they do not give insight on the network throughput. The authors in [16–18] derived secrecy capacity scaling laws in static and mobile ad hoc networks, i.e., the order-of-growth of the secrecy capacity as the number of nodes increases. Although the scaling laws may provide insights into the information-theoretic performance of large-scale networks, a finer view of throughput is necessary to better understand the impact of key system parameters and transmission protocols, since most of these design choices affect the throughput but not the scaling behaviors [19].

A. Approach and Contributions

In this work, we aim to characterize the throughput of secure communications in large wireless networks and to understand how the security requirements affect the network throughput. Our approach uses a metric termed the *transmission capacity* [20], which provides the area spectral efficiency (ASE) of decentralized networks with random topology, identical nodes, and a constraint on outage probability. A tutorial on transmission capacity can be found in [21], which showed how analytical results can often be derived in simple forms. We extend this capacity framework to study the impact of physical layer security requirements on the network ASE.

The networks considered have both legitimate nodes and eavesdroppers, whose locations follow homogeneous Poisson

Manuscript received December 21, 2010; revised March 30, 2011; accepted May 9, 2011. The associate editor coordinating the review of this paper and approving it for publication was I.-M. Kim.

X. Zhou and A. Hjørungnes are with UNIK - University Graduate Center, University of Oslo, Kjeller, NO-2027, Norway (e-mail: {xiangyun, arehj}@unik.no).

R. K. Ganti and J. G. Andrews are with the Department of Electrical and Computer Engineering, the University of Texas at Austin, Austin, TX 78712, USA (e-mail: rganti@austin.utexas.edu, jandrews@ece.utexas.edu).

This work was supported by the Research Council of Norway through the FRITEK project 197565/V30 entitled "Theoretical Foundations of Mobile Flexible Networks - THEFONE," and the DARPA IT-MANET Project.

Digital Object Identifier 10.1109/TWC.2011.061511.102257

point processes (PPPs). We define the *secrecy transmission capacity* as the achievable rate of successful transmission of confidential messages per unit area for given constraints on the quality of service (QoS) and the level of security. The QoS constraint is given by the outage probability of the transmission between a legitimate transmitter-receiver pair, while the security constraint is given by the probability of a transmission failing to achieve perfect secrecy. The secrecy transmission capacity shows the dependence of the network ASE on the key system parameters, i.e., the densities of legitimate nodes and eavesdroppers, as well as the QoS and security constraints.

To illustrate the use of the general capacity formulation, we derive an accurate closed-form lower bound on the secrecy transmission capacity for Rayleigh fading channels. This simple capacity bound gives a quantitative characterization of the throughput cost of physical layer security. Specifically, the throughput reduction for achieving a moderate level of security is relatively small, while a significant amount of throughput needs to be sacrificed to realize a highly secure network. We also give a condition for the existence of positive secrecy transmission capacity. It turns out that the QoS and security constraints as well as the density of eavesdroppers are crucial in determining the existence of positive secrecy transmission capacity.

In order to minimize the throughput cost of achieving high network security, it is worthwhile to consider transmission protocols that are robust against eavesdropping and can be implemented in a decentralized manner. Since insecure transmission is mainly due to the presence of an eavesdropper close to the transmitter, we consider the use of a secrecy guard zone for networks in which the legitimate transmitters are able to detect the existence of eavesdroppers in their vicinities [11, 16].[1] Transmission of confidential messages take place only if no eavesdroppers are found inside the guard zone of the corresponding transmitter. We consider two transmission protocols when eavesdropper(s) are found inside the guard zone, i.e., the transmitter either remains silent or produces artificial noise to help the other transmitters. The secrecy transmission capacity is studied for both protocols. Numerical results show that a significant throughput improvement can be achieved from the use of a guard zone for networks with high security requirements.

The rest of the paper is organized as follows: Section II presents the system model and the secrecy transmission capacity formulation. In Section III, we obtain analytical results on the secrecy transmission capacity in Rayleigh fading channels. In Section IV, we investigate the secrecy guard zone with two different transmission protocols. Numerical results are presented in Section V and concluding remarks in Section VI. A summary of the notation used in this paper is given in Table I.

TABLE I
LIST OF NOTATION

Φ_l	Poisson point process (PPP) of legitimate transmitter locations
Φ_e	PPP of eavesdropper locations
λ_l	Density of Φ_l
λ_e	Density of Φ_e
R_t	Rate of the transmitted codewords
R_s	Rate of the confidential messages
R_e	rate loss for securing the messages against eavesdropping
$\mathrm{P_{co}}$	Connection outage probability
$\mathrm{P_{so}}$	Secrecy outage probability
σ	Constraint on $\mathrm{P_{co}}$
ϵ	Constraint on $\mathrm{P_{so}}$
$\tau(r)$	Secrecy transmission capacity with transmission distance r
β_t	Threshold signal to interference ratio (SIR) for connection outage
β_e	Threshold SIR for secrecy outage
S	Rayleigh fading gain of the wireless channel
D	Radius of secrecy guard zones
$\mathbb{P}(.)$	Probability operator
$\mathbb{E}\{.\}$	Expectation operator

II. System Model And Capacity Formulation

We consider an ad hoc network consisting of both legitimate nodes and eavesdroppers over a large two-dimensional space. For each snapshot in time, we have a set of legitimate transmitter locations, denoted by Φ_l.[2] Each transmitter has a unique associated intended receiver. The set of receivers is disjoint with the set of transmitters. In addition, we have a set of eavesdropper locations in each snapshot, denoted by Φ_e. We model Φ_l and Φ_e as independent homogeneous PPPs with densities λ_l and λ_e, respectively. This is a suitable model for decentralized networks with nodes having substantial mobility [21]. Note that the eavesdroppers need to have similar mobility and other behaviors as the legitimate nodes since they can be easily identified otherwise [17]. Furthermore, we assume that the eavesdroppers do not collude with each other and, hence, must decode the confidential messages individually. An example of a network snapshot is shown in Fig. 1.

Consider only one active transmitter that wants to send confidential messages to its intended receiver in the presence of the eavesdroppers. Secure encoding schemes, such as the Wyner code [1], were found in point-to-point systems with the notion of weak secrecy. The notion of strong secrecy and the corresponding encoding scheme were studied in [22]. According to Wyner's encoding scheme, the transmitter chooses two rates, namely, the rate of the transmitted codewords R_t and the rate of the confidential messages R_s. The rate difference $R_e = R_t - R_s$ reflects the cost of securing the messages against eavesdropping. If R_t is less than the mutual information between the channel input and output of the legitimate link, the receiver is able to decode the message with an arbitrarily small error. At the same time, if R_e is larger than the mutual information between the channel input and output of every eavesdropper link (i.e., links from the transmitter to every eavesdropper), perfect secrecy is achieved as the mutual information between the confidential message and every eavesdropper's received signal approaches zero ratewise. The detailed description of the Wyner code can be found in [1, 23, 24].

In an ad hoc network with simultaneous transmissions from infinitely many legitimate transmitters, it is difficult to study

[1]The application of secrecy guard zone is not always possible. It is applicable in the scenarios where, for example, the legitimate transmitters are able to physically inspect their surrounding areas [11].

[2]For networks employing a slotted Aloha protocol, Φ_l can be viewed as the locations of the actual transmitters (out of all potential transmitters) in each time slot.

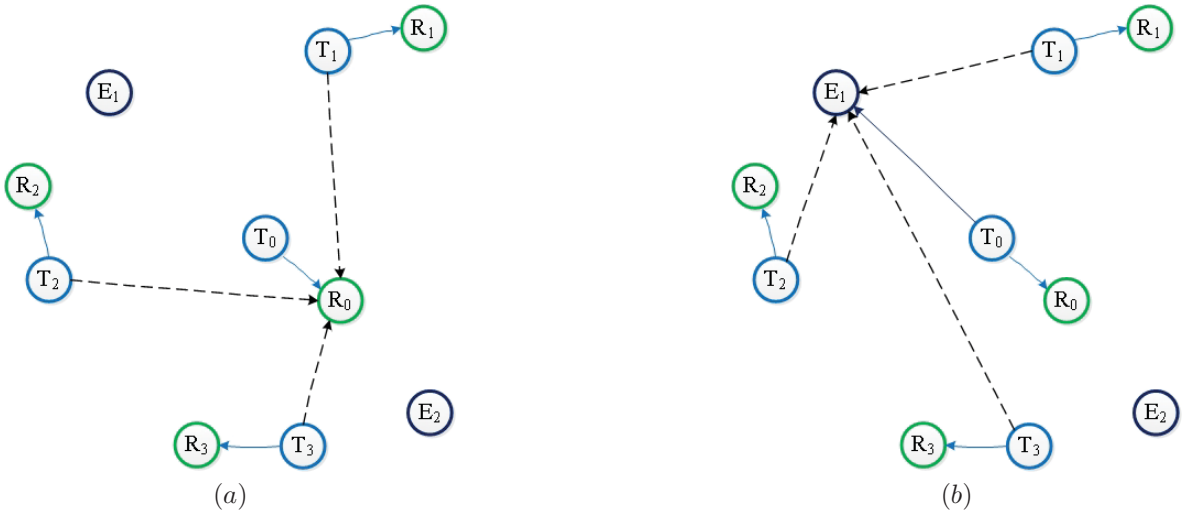


Fig. 1. An example of a part of a network snapshot. Each legitimate transmitter, $\mathrm{T}_i, i = 0, 1, 2, 3$, has an intended receiver $\mathrm{R}_i, i = 0, 1, 2, 3$, located at a distance r. In addition, there are eavesdroppers, $\mathrm{E}_i, i = 1, 2$, presented in the network. Consider the confidential message transmission from T_0. The intended receiver R_0 as well as each eavesdropper $\mathrm{E}_i, i = 1, 2$ all try to individually decode the transmitted message. The signal reception at R_0 and (an arbitrary eavesdropper) E_1 are shown in figures (a) and (b), respectively. In both cases, the concurrent transmissions from T_1, T_2 and T_3 act as interference.

the mutual information between any pair of nodes. To make the design and analysis mathematically tractable, we assume that the transmitted signal (i.e., channel input) has a Gaussian distribution and both the intended receivers and the eavesdroppers treat the interference from concurrent transmissions as noise. In addition, we assume that the network is interference-limited, hence, the receiver noise is negligible. With these assumptions, the mutual information or capacity of either a legitimate link or an eavesdropper link is now determined by the instantaneous signal to interference ratio (SIR). For any given choices of R_t and R_s in Wyner's encoding scheme, the following outage events can result from any transmission [24]:

- **Connection Outage**: The capacity of the channel from the transmitter to the intended receiver is below the transmission 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 the rate 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 QoS while the secrecy outage probability gives a measure of the security level.

The primary goal of this work is to characterize the throughput of secure transmissions in decentralized wireless networks. Although it is extremely difficult to find the network capacity region, the idea of transmission capacity proposed in [20] often gives useful insights on the network ASE and the impacts of the key system parameters. Building on the existing transmission capacity framework, we define the *secrecy transmission capacity* as the achievable rate of successful transmission of confidential messages per unit area, for a given connection outage constraint and a given secrecy outage constraint. Mathematically, the secrecy transmission capacity, with a connection outage probability of $\mathrm{P}_{\mathrm{co}} = \sigma$ and a secrecy outage probability of $\mathrm{P}_{\mathrm{so}} = \epsilon$, is defined as

$$\tau = \bar{R}_s(1-\sigma)\lambda_l, \tag{1}$$

where $\bar{R}_s$ is the average rate of confidential messages. In this work, we focus on a simple scenario where the transmit power and the distances to the intended receivers have fixed values which are the same for all transmitters. Therefore, the confidential message rates also take the same value for all transmitters. Denote the distance between the legitimate transmitter-receiver pairs as r, the secrecy transmission capacity can be written as

$$\tau(r) = R_s(1-\sigma)\lambda_l. \tag{2}$$

The connection outage constraint σ determines the value of R_t, while the secrecy outage constraint ϵ determines the value of R_e. Therefore, the rate of confidential messages R_s in (2), given by $R_t - R_e$, is a function of σ and ϵ. With these choices of rates for the Wyner code, the probability that a message transmission can be successfully decoded by the intended receiver is $1-\sigma$, while the probability that a message transmission is perfectly secure against eavesdropping is $1-\epsilon$, under the assumption of treating interference as noise.

If we allow the distance between the legitimate transmitter-receiver pair varies over time and/or space but follows some known distribution $f(r)$, the secrecy transmission capacity is computed as

$$\tau = \int \tau(r) f(r) \mathrm{d}r. \tag{3}$$

In practice, the distribution of r depends on specific scenarios. Hence, we do not consider the variation in r and focus on $\tau(r)$ in (2).

III. Secrecy Transmission Capacity in Rayleigh Fading Channels

In this section, we derive analytical results on the secrecy transmission capacity for Rayleigh fading channels. We assume that each node has a single antenna for transmission or reception, and the fading channel states are known at the receiver side (including the eavesdroppers) but not at the transmitter side. The derivation of the secrecy transmission capacity involves two main steps: 1) Use the connection outage constraint σ to find the value of R_t. 2) Use the secrecy outage constraint ϵ to find the value of R_e.

Our analysis is based on an arbitrarily chosen transmitter-receiver pair, which are named the typical transmitter and receiver. For confidential message transmission from the typical transmitter, the other transmitters act as interferers to the typical receiver or any eavesdropper. From Slivnyak's Theorem [25], the spatial distribution of the interferers, given the location of the typical transmitter, still follows a homogeneous PPP with density λ_l. By slight abuse of notation (since we have used Φ_l to denote the set of all transmitter locations), we will also refer to Φ_l as the set of interferer locations in the rest of this paper.

For the typical receiver, 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

$$\mathrm{SIR}_0 = \frac{S_0 r^{-\alpha}}{\sum_{l\in\Phi_l} S_l |X_l|^{-\alpha}}, \tag{4}$$

where S_0 and r are the channel fading gain and the distance between the typical transmitter and receiver, respectively, α is the path loss exponent, S_l and $|X_l|$ are the channel fading gain and the distance between the interferer (at position) l in Φ_l and the typical receiver, respectively. We assume $\alpha > 2$ throughout this paper. The fading gains are modeled as independent and identically distributed (i.i.d.) exponential random variables with unit mean.

Define a threshold SIR value for connection outage as

$$\beta_t = 2^{R_t} - 1. \tag{5}$$

Hence, the connection outage probability can be written as

$$\mathrm{P_{co}} = \mathbb{P}\Big(\mathrm{SIR}_0 < \beta_t\Big) = \mathbb{P}\left(\frac{S_0 r^{-\alpha}}{\sum_{l\in\Phi_l} S_l |X_l|^{-\alpha}} < \beta_t\right). \tag{6}$$

The summation term $\sum_{l\in\Phi_l} S_l|X_l|^{-\alpha}$ is a shot noise process [26] in two-dimensional space whose Laplace transform is known in a closed form and was used to compute the connection outage probability in [27] as

$$\mathrm{P_{co}} = 1 - \exp\left[-\lambda_l \pi r^2 \beta_t^{2/\alpha} \Gamma\Big(1-\frac{2}{\alpha}\Big)\Gamma\Big(1+\frac{2}{\alpha}\Big)\right]. \tag{7}$$

With the connection outage constraint given by $\mathrm{P_{co}} = \sigma$, the transmission rate R_t can be found using (5) and (7) as

$$R_t = \log_2\left(1 + \left[\frac{\ln\frac{1}{1-\sigma}}{\lambda_l \pi r^2 \Gamma\Big(1-\frac{2}{\alpha}\Big)\Gamma\Big(1+\frac{2}{\alpha}\Big)}\right]^{\frac{\alpha}{2}}\right). \tag{8}$$

It is clear that a lower connection outage probability (i.e., a higher QoS) requires a lower R_t.

On the other hand, the confidential message transmission is not perfectly secure against the eavesdropper (at position) e in Φ_e if $\log_2(1+\mathrm{SIR}_e) > R_e$, where SIR_e denotes the SIR at e given by

$$\mathrm{SIR}_e = \frac{S_e |X_e|^{-\alpha}}{\sum_{l\in\Phi_l} S_{le} |X_{le}|^{-\alpha}}, \tag{9}$$

where S_e and $|X_e|$ are the channel fading gain and the distance between the typical transmitter and eavesdropper e in Φ_e, respectively, S_{le} and $|X_{le}|$ are the channel fading gain and the distance between node l in Φ_l and eavesdropper e in Φ_e, respectively. The fading gains are modeled as i.i.d. exponential random variables with unit mean.

Define a threshold SIR value for secrecy outage as

$$\beta_e = 2^{R_e} - 1. \tag{10}$$

Let $A = \{y \in \Phi_e : \mathrm{SIR}_y > \beta_e\}$, i.e., the set of eavesdroppers that can cause secrecy outage. Hence, we can define the following indicator function: $1_A(e)$, which equals 1 when the eavesdropper e is in the set A. The secrecy outage probability equals the probability that at least one of the eavesdroppers in Φ_e causes a secrecy outage, which can be written as

$$\begin{aligned}\mathrm{P_{so}} &= 1 - \mathbb{E}_{\Phi_l}\Big\{\mathbb{E}_{\Phi_e}\Big\{\mathbb{E}_S\Big\{\prod_{e\in\Phi_e}\Big(1-1_A(e)\Big)\Big\}\Big\}\Big\},\\ &= 1 - \mathbb{E}_{\Phi_l}\Bigg\{\mathbb{E}_{\Phi_e}\Bigg\{\\ &\qquad \prod_{e\in\Phi_e}\left(1-\mathbb{P}\Big(\frac{S_e|X_e|^{-\alpha}}{\sum_{l\in\Phi_l} S_{le}|X_{le}|^{-\alpha}} > \beta_e \Big| \Phi_e, \Phi_l\Big)\right)\Bigg\}\Bigg\}.\end{aligned} \tag{11}$$

where the independence in the fading gains among different eavesdroppers is used to move the expectation over $S = \{S_e, S_{le}\}$ inside the product over Φ_e in (11). Since it is difficult to express $\mathrm{P_{so}}$ in a closed form, we look for analytical bounds on the secrecy outage probability. The results are summarized in the following lemma:

Lemma 1: The secrecy outage probability is bounded from above by

$$\mathrm{P_{so}^{UB}} = 1 - \exp\left[-\frac{\lambda_e}{\lambda_l \beta_e^{2/\alpha}\Gamma\Big(1-\frac{2}{\alpha}\Big)\Gamma\Big(1+\frac{2}{\alpha}\Big)}\right], \tag{12}$$

and bounded from below by

$$\mathrm{P_{so}^{LB}} = \frac{1}{1+\frac{\lambda_l}{\lambda_e}\beta_e^{2/\alpha}\Gamma\Big(1-\frac{2}{\alpha}\Big)\Gamma\Big(1+\frac{2}{\alpha}\Big)}. \tag{13}$$

Proof: Using the generating functional of the PPP Φ_e [25], we can express the secrecy outage probability in (11) as

$$\begin{aligned}\mathrm{P_{so}} &= 1 - \mathbb{E}_{\Phi_l}\Bigg\{\\ &\qquad \exp\left[-\lambda_e \int_{\mathbb{R}^2} \mathbb{P}\Big(\frac{S_e|X_e|^{-\alpha}}{\sum_{l\in\Phi_l} S_{le}|X_{le}|^{-\alpha}} > \beta_e \Big| \Phi_l\Big)\mathrm{d}e\right]\Bigg\}.\end{aligned} \tag{14}$$

Jensen's inequality gives an upper bound on $\mathrm{P_{so}}$

$$\begin{aligned}\mathrm{P_{so}} &\le 1-\exp\left[-\lambda_e\int_{\mathbb{R}^2}\mathbb{P}\Big(\frac{S_e|X_e|^{-\alpha}}{\sum_{l\in\Phi_l}S_{le}|X_{le}|^{-\alpha}}>\beta_e\Big)\mathrm{d}e\right]\\ &= 1-\exp\Bigg[-2\pi\lambda_e \\ &\quad\cdot\int_0^\infty\exp\left[-\lambda_l\pi r_e^2\beta_e^{2/\alpha}\Gamma\Big(1-\frac{2}{\alpha}\Big)\Gamma\Big(1+\frac{2}{\alpha}\Big)\right]r_e\mathrm{d}r_e\Bigg],\end{aligned} \tag{15}$$

where r_e denotes the distance between the typical transmitter and eavesdropper e, (15) is arrived in the same way as (7) followed by changing to polar coordinates. The upper bound in (12) is then obtained by directly evaluating the integration in (15).

The lower bound on $\mathrm{P_{so}}$ is obtained by considering only the eavesdropper nearest to the typical transmitter. Denote the eavesdropper (location) in Φ_e that is nearest to the typical transmitter as e' and denote the distance between e' and the typical transmitter as $r_{e'}$. The probability distribution of $r_{e'}$ is given by [28]

$$f(r_{e'})=2\lambda_e\pi r_{e'}\exp(-\lambda_e\pi r_{e'}^2). \tag{16}$$

The secrecy outage probability is bounded from below by the probability that the nearest eavesdropper causes a secrecy outage, i.e.,

$$\begin{aligned}\mathrm{P_{so}} &\ge \int_0^\infty\mathbb{P}\Big(\frac{S_{e'}r_{e'}^{-\alpha}}{\sum_{l\in\Phi_l}S_{le'}|X_{le'}|^{-\alpha}}>\beta_e\Big)f(r_{e'})\mathrm{d}r_{e'}\\ &= \int_0^\infty\exp\left[-\lambda_l\pi r_{e'}^2\beta_e^{2/\alpha}\Gamma\Big(1-\frac{2}{\alpha}\Big)\Gamma\Big(1+\frac{2}{\alpha}\Big)\right]\\ &\qquad\cdot2\lambda_e\pi r_{e'}\exp(-\lambda_e\pi r_{e'}^2)\mathrm{d}r_{e'}.\end{aligned} \tag{17}$$

The lower bound in (13) is then obtained by directly evaluating the integration in (17). ■

Note that the authors in [29] used the same bounding techniques to derive analytical bounds on the probability of connectivity in a different network scenario and numerically studied the accuracy of the derived bounds. From the numerical illustration in [29, Fig. 5], we know that the upper bound $\mathrm{P_{so}^{UB}}$ in (12) gives an accurate approximation of the exact secrecy outage probability over the entire range of $\mathrm{P_{so}}\in[0,1]$, while the lower bound $\mathrm{P_{so}^{LB}}$ in (13) is usually very different from the exact value of $\mathrm{P_{so}}$. Moreover, both $\mathrm{P_{so}^{UB}}$ and $\mathrm{P_{so}^{LB}}$ are asymptotically tight in the low probability regime. To see this, we consider $\mathrm{P_{so}^{UB}}\approx 0$ and $\mathrm{P_{so}^{LB}}\approx 0$, in which case the bounds in (12) and (13) can be approximated by

$$\mathrm{P_{so}^{UB}}\approx\frac{\lambda_e}{\lambda_l\beta_e^{2/\alpha}\Gamma\Big(1-\frac{2}{\alpha}\Big)\Gamma\Big(1+\frac{2}{\alpha}\Big)}\approx\mathrm{P_{so}^{LB}}. \tag{18}$$

Hence, both $\mathrm{P_{so}^{UB}}$ and $\mathrm{P_{so}^{LB}}$ approach the exact value of $\mathrm{P_{so}}$ in the low probability regime.

Recall that the goal here is to determine the value of R_e from the secrecy outage constraint of $\mathrm{P_{so}}=\epsilon$. Using the upper bound on the secrecy outage probability in (12), the value of R_e that guarantees the required security level can be found as

$$R_e=\log_2\left(1+\Big[\frac{\lambda_l}{\lambda_e}\Gamma\Big(1-\frac{2}{\alpha}\Big)\Gamma\Big(1+\frac{2}{\alpha}\Big)\ln\frac{1}{1-\epsilon}\Big]^{-\frac{\alpha}{2}}\right). \tag{19}$$

It is clear that a lower secrecy outage probability (i.e., a higher security level) requires a higher R_e.

Having R_t in (8) and R_e in (19), a lower bound on the secrecy transmission capacity is obtained as $\tau^{\mathrm{LB}}(r)=(R_t-R_e)(1-\sigma)\lambda_l$. Its expression is presented in the following theorem:

Theorem 1: A lower bound on the secrecy transmission capacity with a connection outage constraint of σ and a secrecy outage constraint of ϵ is given by

$$\begin{aligned}\tau^{\mathrm{LB}}(r) &= (1-\sigma)\lambda_l \\ &\quad\cdot\log_2\left(\frac{1+\Big[\frac{\ln\frac{1}{1-\sigma}}{\lambda_l\pi r^2\Gamma(1-\frac{2}{\alpha})\Gamma(1+\frac{2}{\alpha})}\Big]^{\frac{\alpha}{2}}}{1+\Big[\frac{\lambda_l}{\lambda_e}\Gamma\Big(1-\frac{2}{\alpha}\Big)\Gamma\Big(1+\frac{2}{\alpha}\Big)\ln\frac{1}{1-\epsilon}\Big]^{-\frac{\alpha}{2}}}\right).\end{aligned} \tag{20}$$

From our discussion on the accuracy of $\mathrm{P_{so}^{UB}}$, we know that the lower bound on the secrecy transmission capacity in (20) is generally accurate for any values of σ and ϵ, and is asymptotically tight as $\epsilon\to 0$. Therefore, we will for simplicity refer to $\tau^{\mathrm{LB}}(r)$ in (20) as the secrecy transmission capacity in the rest of this paper. It is clear from (20) that $\tau^{\mathrm{LB}}(r)$ reduces as ϵ decreases. The reduction in $\tau^{\mathrm{LB}}(r)$ as ϵ decreases can be viewed as the throughput cost of improving physical layer security.

In practical network design, the connection outage constraint and the spatial transmission intensity[3] may be under the control of the system designer. The derived closed-form characterization of the secrecy transmission capacity allows the designer to optimize these system parameters to maximize the throughput of secure transmissions with a target security level.

A. Existence of Positive Secrecy Transmission Capacity

A fundamental question to ask is the condition under which positive secrecy transmission capacity exists. From the expression in (20), one can find this condition by solving $\tau^{\mathrm{LB}}(r)>0$.

Corollary 1: The condition for positive secrecy transmission capacity is given by

$$\ln\frac{1}{1-\sigma}\ln\frac{1}{1-\epsilon} \;>\; \pi r^2\lambda_e. \tag{21}$$

In other words, positive secrecy transmission capacity is achieved if the average number of eavesdroppers within a distance r from the transmitter (i.e., having shorter distances than the intended receiver) is less than $\ln\frac{1}{1-\sigma}\ln\frac{1}{1-\epsilon}$.

Remark 1: The condition in (21) clearly gives a trade-off between the QoS and the security level of a network: The QoS needs to be compromised (i.e., allowing a larger value of σ) in order to achieve a higher security level (i.e., a smaller value of ϵ). Therefore, a moderate connection outage probability is usually desirable for highly secure networks. Furthermore, the

[3]In networks employing an Aloha protocol, the spatial transmission intensity equals the density of potential transmitters multiplied by the probability of transmission. In this case, the system designer may control the probability of transmission to vary the spatial transmission intensity.

$$\begin{aligned}\tau^{\mathrm{LB}}(r) &= (1-\sigma)\lambda_l \log_2\left(1+\frac{\left[\frac{\ln\frac{1}{1-\sigma}}{\lambda_l \pi r^2 \Gamma(1-\frac{2}{\alpha})\Gamma(1+\frac{2}{\alpha})}\right]^{\frac{\alpha}{2}} - \left[\frac{\lambda_l}{\lambda_e}\Gamma\left(1-\frac{2}{\alpha}\right)\Gamma\left(1+\frac{2}{\alpha}\right)\ln\frac{1}{1-\epsilon}\right]^{-\frac{\alpha}{2}}}{1+\left[\frac{\lambda_l}{\lambda_e}\Gamma\left(1-\frac{2}{\alpha}\right)\Gamma\left(1+\frac{2}{\alpha}\right)\ln\frac{1}{1-\epsilon}\right]^{-\frac{\alpha}{2}}}\right) \\ &\approx \frac{(1-\sigma)\lambda_l}{\ln 2}\frac{\left[\frac{\ln\frac{1}{1-\sigma}}{\lambda_l \pi r^2 \Gamma(1-\frac{2}{\alpha})\Gamma(1+\frac{2}{\alpha})}\right]^{\frac{\alpha}{2}} - \left[\frac{\lambda_l}{\lambda_e}\Gamma\left(1-\frac{2}{\alpha}\right)\Gamma\left(1+\frac{2}{\alpha}\right)\ln\frac{1}{1-\epsilon}\right]^{-\frac{\alpha}{2}}}{1+\left[\frac{\lambda_l}{\lambda_e}\Gamma\left(1-\frac{2}{\alpha}\right)\Gamma\left(1+\frac{2}{\alpha}\right)\ln\frac{1}{1-\epsilon}\right]^{-\frac{\alpha}{2}}} \\ &= \frac{1-\sigma}{\ln 2}\left[\Gamma\left(1-\frac{2}{\alpha}\right)\Gamma\left(1+\frac{2}{\alpha}\right)\right]^{-\frac{\alpha}{2}}\left[\left(\frac{\ln\frac{1}{1-\sigma}}{\pi r^2}\right)^{\frac{\alpha}{2}} - \left(\frac{\ln\frac{1}{1-\epsilon}}{\lambda_e}\right)^{-\frac{\alpha}{2}}\right]\frac{1}{\lambda_l^{\frac{\alpha}{2}-1}+\left[\Gamma\left(1-\frac{2}{\alpha}\right)\Gamma\left(1+\frac{2}{\alpha}\right)\frac{\ln\frac{1}{1-\epsilon}}{\lambda_e}\right]^{-\frac{\alpha}{2}}\lambda_l^{-1}}. \quad (23)\end{aligned}$$

feasible range of σ can be found from (21) as

$$\sigma \in \left(1-\exp\left[-\frac{\pi r^2 \lambda_e}{\ln\frac{1}{1-\epsilon}}\right], 1\right). \quad (22)$$

Remark 2: The condition in (21) does not depend on the spatial transmission intensity λ_l. That is to say, positive secrecy transmission capacity cannot be achieved simply by bringing in additional legitimate users or deactivating existing legitimate users, if the connection outage and secrecy outage performances of the network do not meet the condition in (21). Once this condition is met and the network is operating with some positive secrecy transmission capacity, there exists an optimal value of λ_l which can be found numerically using (20). To obtain some analytical insights into the optimal λ_l, we consider the low secrecy transmission capacity regime by letting $\ln\frac{1}{1-\sigma}\ln\frac{1}{1-\epsilon} \approx \pi r^2 \lambda_e$ which implies $\tau^{\mathrm{LB}}(r) \approx 0$. We can approximate (20) as (23) shown on the top of this page. Assuming $\tau^{\mathrm{LB}}(r)$ in (23) is positive, the optimal value of λ_l that maximizes $\tau^{\mathrm{LB}}(r)$ is given by

$$\lambda_l^{\mathrm{opt}} = \left(\frac{2}{\alpha-2}\right)^{\frac{2}{\alpha}} \frac{\lambda_e}{\Gamma\left(1-\frac{2}{\alpha}\right)\Gamma\left(1+\frac{2}{\alpha}\right)\ln\frac{1}{1-\epsilon}}. \quad (24)$$

From (24), we see that the optimal spatial transmission intensity increases as the required security level increases (i.e., as ϵ decreases). In addition, the optimal spatial transmission intensity is usually much higher than the density of eavesdroppers for highly secure networks. For example, $\lambda_l^{\mathrm{opt}}/\lambda_e \approx 63$ for $\epsilon = 0.01$ and $\alpha = 4$. Although these observations are made in the regime of arbitrarily low secrecy transmission capacity, as we will see in Section V, they are also valid for more general scenarios.

B. Optimal Connection Outage Probability in Sparse Networks

When the system designer has control over the connection outage constraint, the expression of secrecy transmission capacity in (20) can be used to numerically find the value of σ that maximizes $\tau^{\mathrm{LB}}(r)$. Here, we present a closed-form solution of the optimal connection outage probability in sparse networks, i.e., $\lambda_l \pi r^2 \ll 1$. Note that our analysis is based on the assumption of interference-limited networks, which is valid if the transmit power of the legitimate users is sufficiently high such that the receiver noise is much weaker than the aggregate interference.

From the discussion in Subsection III-A, we know that the value of σ should not be chosen very close to 0. When the network is sparse, i.e., $\lambda_l \pi r^2 \ll 1$, the secrecy transmission capacity in (20) can be approximated as

$$\begin{aligned}\tau^{\mathrm{LB}}(r) &\approx (1-\sigma)\lambda_l \cdot \log_2\left(\frac{\left[\frac{\ln\frac{1}{1-\sigma}}{\lambda_l \pi r^2 \Gamma(1-\frac{2}{\alpha})\Gamma(1+\frac{2}{\alpha})}\right]^{\frac{\alpha}{2}}}{1+\left[\frac{\lambda_l}{\lambda_e}\Gamma\left(1-\frac{2}{\alpha}\right)\Gamma\left(1+\frac{2}{\alpha}\right)\ln\frac{1}{1-\epsilon}\right]^{-\frac{\alpha}{2}}}\right) \quad (25) \\ &= (1-\sigma)\lambda_l \log_2\left(\left[\kappa \ln\frac{1}{1-\sigma}\right]^{\frac{\alpha}{2}}\right), \quad (26)\end{aligned}$$

where we have assumed in (25) that the path loss exponent α is not close to 2 (which happens in most outdoor scenarios) and the connection outage probability is not close to 0, and

$$\kappa = \frac{\left(1+\left[\frac{\lambda_l}{\lambda_e}\Gamma\left(1-\frac{2}{\alpha}\right)\Gamma\left(1+\frac{2}{\alpha}\right)\ln\frac{1}{1-\epsilon}\right]^{-\frac{\alpha}{2}}\right)^{-\frac{2}{\alpha}}}{\lambda_l \pi r^2 \Gamma\left(1-\frac{2}{\alpha}\right)\Gamma\left(1+\frac{2}{\alpha}\right)}. \quad (27)$$

The optimal connection outage probability that maximizes the secrecy transmission capacity in (26) is given by

$$\sigma^{\mathrm{opt}} = 1 - \frac{1}{\exp\left[\frac{1}{\mathrm{W}_0(\kappa)}\right]}, \quad (28)$$

where $\mathrm{W}_0(\cdot)$ is the real-valued principal branch of Lambert's W function. This result is obtained by directly taking the derivative of $\tau^{\mathrm{LB}}(r)$ in (26) w.r.t. σ and solving for the root. Furthermore, one can show that the optimal connection outage probability increases when a higher security level (i.e., a lower ϵ) is required.

IV. Secrecy Guard Zone

In this section, we consider simple protocols for improving the secrecy transmission capacity. We assume that the legitimate transmitters are able to detect the existence of eavesdroppers within a finite range. We model this range as a disk with radius D centered at each transmitter and call it the secrecy guard zone. Transmission of confidential messages only happens when there is no eavesdropper inside the secrecy guard zone. As we are concerned with decentralized networks, it is assumed that each transmitter individually

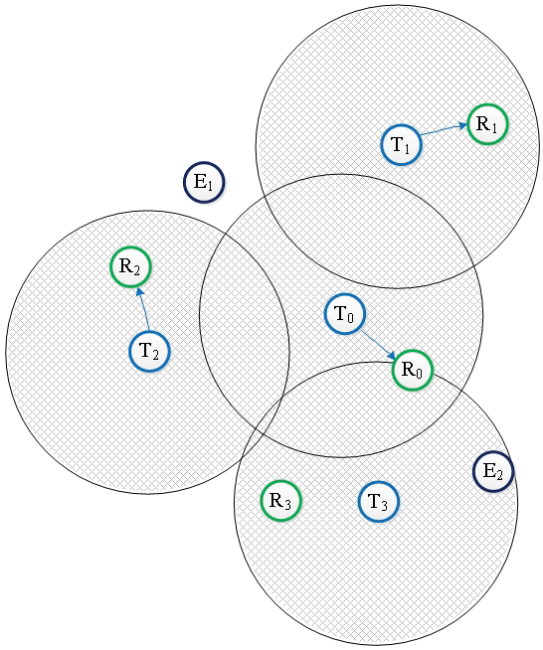


Fig. 2. An example of a part of a network snapshot with a secrecy guard zone around each transmitter. Transmitters T_0, T_1, and T_2 do not find any eavesdropper inside their individual guard zone, and hence, transmit confidential messages to their intended receivers. However, transmitter T_3 detects an eavesdropper, E_2, insides its guard zone. If the non-cooperative protocol is used, T_3 remains silent. If the cooperative protocol is used, T_3 transmits artificial noise.

decides whether or not to transmit based on the existence of eavesdroppers inside its own guard zone.

The general idea of guard zone is not new and has been applied in wireless ad hoc networks without or with security considerations: In [30], the authors used a guard zone around each receiver such that the receiver is active when there is no interferers inside the guard zone. The authors in [11] and [16] studied the secure connectivity and secrecy capacity scaling law of ad hoc networks in the presence of eavesdroppers, respectively, and applied a secrecy guard zone around each legitimate node. In this work, we apply a secrecy guard zone around each legitimate transmitter and consider the following two transmission protocols:

1) **Non-Cooperative Transmitters**: The transmitter remains silent when eavesdropper(s) are found inside its secrecy guard zone.
2) **Cooperative Transmitters**: The transmitter produces artificial noise when eavesdropper(s) are found inside its secrecy guard zone.

The idea of using artificial noise for secrecy was first proposed for multi-antenna transmissions in [31], which is also related to the idea of cooperative jamming studied in [6, 9, 18, 32, 33]. An example of a network snapshot with secrecy guard zones is shown in Fig. 2. In the following, we study the secrecy transmission capacity with each transmission protocol.

A. Secrecy Guard Zone with Non-Cooperative Transmitters

The set of actual transmitter locations, denoted as $\Phi_{l'}$, has density of

$$\lambda_l' = \lambda_l \exp[-\pi\lambda_e D^2], \tag{29}$$

where the exponential term in (29) is the probability of no eavesdropper located inside the secrecy guard zone of an arbitrary transmitter. With the secrecy guard zone, the distribution of the actual transmitters does not still follow a homogeneous PPP. The non-homogeneous nature resulted from the introduction of guard zone was discussed in [30]. In particular, the authors in [30] applied standard Poisson tests to show that the distribution of the actual transmitters can still be well-approximated by a homogeneous PPP outside $\mathcal{B}(b, D)$ from the viewpoint of a receiver at location b, where the notation $\mathcal{B}(b, D)$ stands for a disk of radius D centered at b. Based on this result, we apply the following two approximations: From the viewpoint of eavesdropper e, the actual transmitter $\Phi_{l'}$ follows a homogeneous PPP with density λ_l' outside $\mathcal{B}(e, D)$. From the viewpoint of any legitimate receiver, the actual transmitter $\Phi_{l'}$ follows a homogeneous PPP with density λ_l'.[4]

For the typical receiver, the connection outage[5] probability is given by

$$\mathrm{P_{co}} = 1-\exp\left[-\lambda_l'\pi r^2\beta_t^{2/\alpha}\Gamma\Big(1-\frac{2}{\alpha}\Big)\Gamma\Big(1+\frac{2}{\alpha}\Big)\right]. \tag{30}$$

With the connection outage constraint $\mathrm{P_{co}} = \sigma$ and $\beta_t = 2^{R_t} - 1$, the transmission rate R_t is found as

$$R_t = \log_2\left(1+\left[\frac{\ln\frac{1}{1-\sigma}}{\lambda_l'\pi r^2\Gamma\Big(1-\frac{2}{\alpha}\Big)\Gamma\Big(1+\frac{2}{\alpha}\Big)}\right]^{\frac{\alpha}{2}}\right). \tag{31}$$

From the viewpoint of the typical transmitter located at the origin o, the eavesdroppers Φ_e follows a homogeneous PPP with density λ_e outside $\mathcal{B}(o, D)$. Similar to the proof of Lemma 1, an upper bound on the secrecy outage probability is obtained by using the generating functional of Φ_e and applying Jensen's inequality as

$$\begin{aligned}\mathrm{P_{so}^{UB}} &= 1-\exp\Bigg[-\lambda_e \\ &\qquad \cdot\int_{\mathbb{R}^2\setminus\mathcal{B}(o,D)}\mathbb{P}\Big(\frac{S_e|X_e|^{-\alpha}}{\sum_{l\in\Phi_{l'}}S_{le}|X_{le}|^{-\alpha}}>\beta_e\Big)\mathrm{d}e\Bigg] \\ &= 1-\exp\left[-\lambda_e\int_{\mathbb{R}^2\setminus\mathcal{B}(o,D)}\mathbb{E}_Z\Big\{\exp[-\beta_e|X_e|^\alpha Z]\Big\}\mathrm{d}e\right] \\ &= 1-\exp\left[-2\pi\lambda_e\int_D^\infty\mathcal{L}_Z(\beta_e r_e^\alpha)r_e\mathrm{d}r_e\right],\end{aligned} \tag{32}$$

where $Z = \sum_{l\in\Phi_{l'}}S_{le}|X_{le}|^{-\alpha}$ is the sum of interference power at eavesdropper e and $\mathcal{L}_Z(\cdot)$ denotes the Laplace transform of Z. Note that we have assumed that $\Phi_{l'}$ is a homogeneous PPP outside $\mathcal{B}(e, D)$ from the viewpoint of

[4]Note that the second approximation usually underestimates the interference power at the typical receiver, since the potential interferers near the typical (active) transmitter is more likely to be active than the ones far away from the typical transmitter. However, this underestimation is marginal as long as λ_l' is reasonably close to λ_l, such as the scenarios to be considered in Fig. 5.

[5]The connection outage event is defined as the *transmitted* message being undecodable at the intended receiver. Hence, it does not include the event of no transmission due to the existence of eavesdropper(s) inside the guard zone. A similar note applies to the secrecy outage event. The effect of transmission probability on the secrecy transmission capacity is incorporated in λ_l'.

eavesdropper e. Hence, $\mathcal{L}_Z(\cdot)$ is given by [26]

$$\begin{aligned}\mathcal{L}_Z(x) \;=\; \exp\Bigg[\pi\lambda_l'\Bigg(& D^2\mathbb{E}_S\Big\{1-\exp[-xSD^{-\alpha}]\Big\}\\ &-x^{2/\alpha}\mathbb{E}_S\Big\{S^{2/\alpha}\Big\}\Gamma\Big(1-\frac{2}{\alpha}\Big)\\ &+x^{2/\alpha}\mathbb{E}_S\Big\{S^{2/\alpha}\Gamma\Big(1-\frac{2}{\alpha},xSD^{-\alpha}\Big)\Big\}\Bigg)\Bigg],\end{aligned} \tag{33}$$

where S is an exponentially distributed random variable with unit mean and $\Gamma(\cdot,\cdot)$ is the upper incomplete Gamma function. Using integral identities from [34] to evaluate the expectations in (33), we have

$$\begin{aligned}\mathcal{L}_Z(x) = \exp\Bigg[\pi\lambda_l'\Bigg(&\frac{xD^{2-\alpha}}{1+xD^{-\alpha}}-x^{2/\alpha}\Gamma\Big(1+\frac{2}{\alpha}\Big)\Gamma\Big(1-\frac{2}{\alpha}\Big)\\ &+\frac{xD^{2-\alpha}}{(1-\frac{2}{\alpha})(1+xD^{-\alpha})^2}\,{}_2\mathrm{F}_1\Big(1,2;2+\frac{2}{\alpha};\frac{1}{1+xD^{-\alpha}}\Big)\Bigg)\Bigg],\end{aligned} \tag{34}$$

where ${}_2\mathrm{F}_1(\cdot)$ is the Gauss hypergeometric function.

Substituting (34) into (32), $\mathrm{P}_{\mathrm{so}}^{\mathrm{UB}}$ is expressed in an integral form, hence, R_e can be solved numerically with the secrecy outage constraint $\mathrm{P}_{\mathrm{so}}^{\mathrm{UB}}=\epsilon$ and $\beta_e=2^{R_e}-1$. A lower bound on the secrecy transmission capacity is found as

$$\tau^{\mathrm{LB}}(r)=(R_t-R_e)(1-\sigma)\lambda_l'. \tag{35}$$

B. Secrecy Guard Zone with Cooperative Transmitters

In this scenario, the legitimate transmitters cooperative with each other. When eavesdropper(s) are found inside the secrecy guard zone, the transmitter produces artificial noise to help masking the confidential message transmissions from others. The artificial noise is assumed to be statistically identical to the confidential messages and hence, it cannot be distinguished from message transmissions by the eavesdroppers. It is noted that this cooperative protocol is entirely distributive as it does not require any coordination between the legitimate transmitters.

For any legitimate receiver or eavesdropper, the set of interferers is still Φ_l with density λ_l. On the other hand, the set of actual transmitters is $\Phi_{l'}$ with density λ_l' given by

$$\lambda_l'=\lambda_l\exp[-\pi\lambda_e D^2]. \tag{36}$$

Since the interferers remain the same as if no secrecy guard zone is applied, the connection outage probability P_{co} and the transmission rate R_t are still given by (7) and (8), respectively.

From the viewpoint of the typical transmitter located at the origin o, the eavesdroppers Φ_e follows a homogeneous PPP with density λ_e outside $\mathcal{B}(o,D)$. Again, an upper bound on the secrecy outage probability is found using the generating functional of Φ_e and applying Jensen's inequality as

$$\begin{aligned}&\mathrm{P}_{\mathrm{so}}^{\mathrm{UB}}\\ &=1-\exp\Bigg[-\lambda_e\int_{\mathbb{R}^2\setminus\mathcal{B}(o,D)}\mathbb{P}\Big(\frac{S_e|X_e|^{-\alpha}}{\sum_{l\in\Phi_l}S_{le}|X_{le}|^{-\alpha}}>\beta_e\Big)\mathrm{d}e\Bigg]\\ &=1-\exp\Bigg[-\frac{\lambda_e\exp\Big[-\lambda_l\pi\beta_e^{2/\alpha}\Gamma\Big(1-\frac{2}{\alpha}\Big)\Gamma\Big(1+\frac{2}{\alpha}\Big)D^2\Big]}{\lambda_l\beta_e^{2/\alpha}\Gamma\Big(1-\frac{2}{\alpha}\Big)\Gamma\Big(1+\frac{2}{\alpha}\Big)}\Bigg].\end{aligned} \tag{37}$$

With the secrecy outage constraint of $\mathrm{P}_{\mathrm{so}}^{\mathrm{UB}}=\epsilon$, we find R_e as

$$R_e=\log_2\left(1+\left[\frac{\mathrm{W}_0\Big(\lambda_e\pi D^2\Big[\ln\frac{1}{1-\epsilon}\Big]^{-1}\Big)}{\lambda_l\pi D^2\Gamma\Big(1-\frac{2}{\alpha}\Big)\Gamma\Big(1+\frac{2}{\alpha}\Big)}\right]^{\frac{\alpha}{2}}\right). \tag{38}$$

Theorem 2: A lower bound on the secrecy transmission capacity for networks having cooperative transmitters with secrecy guard zones is given by

$$\begin{aligned}\tau^{\mathrm{LB}}(r) \;&=\; (R_t-R_e)(1-\sigma)\lambda_l'\\ &=\; (1-\sigma)\lambda_l\exp[-\pi\lambda_e D^2]\\ &\quad\cdot\log_2\left(\frac{1+\left[\frac{\ln\frac{1}{1-\sigma}}{\lambda_l\pi r^2\Gamma(1-\frac{2}{\alpha})\Gamma(1+\frac{2}{\alpha})}\right]^{\frac{\alpha}{2}}}{1+\left[\frac{\mathrm{W}_0\left(\lambda_e\pi D^2[\ln\frac{1}{1-\epsilon}]^{-1}\right)}{\lambda_l\pi D^2\Gamma(1-\frac{2}{\alpha})\Gamma(1+\frac{2}{\alpha})}\right]^{\frac{\alpha}{2}}}\right).\end{aligned} \tag{39}$$

From the closed-form expression of $\tau^{\mathrm{LB}}(r)$ in (39), we can derive the condition for positive secrecy transmission capacity by solving $\tau^{\mathrm{LB}}(r)>0$.

Corollary 2: The condition for positive secrecy transmission capacity is given by

$$\Big[\frac{1}{1-\sigma}\Big]^{\left(\frac{D}{r}\right)^2}\ln\frac{1}{1-\sigma}\ln\frac{1}{1-\epsilon}>\pi r^2\lambda_e. \tag{40}$$

When the system designer has control over the connection outage constraint and the guard zone size, positive secrecy transmission capacity can be achieved by carefully choosing the values of σ and/or D to meet the condition in (40). Similar to the networks without guard zones, the density of the legitimate transmitters has no say for the existence of positive secrecy transmission capacity for fixed connection outage probability and guard zone size. Comparing (21) with (40), we see that the improvement from having the secrecy guard zone is given by the factor of $[\frac{1}{1-\sigma}]^{(D/r)^2}$. For a fixed r, the minimum required value of D increases as σ or ϵ decreases (below certain threshold value). Hence, one may also expect that the optimal value of D, which maximizes the secrecy transmission capacity in (39), increases as σ or ϵ decreases.

To further improve the network throughput, the secrecy guard zone could in the future be used in combination with other types of guard zone, such as carrier sense multiple access (CSMA) at the transmitters [35] and the interference guard zone at the receivers [30].

V. Numerical Results and Discussion

In this section, we present numerical results on the secrecy transmission capacity. We first show the interplay of different

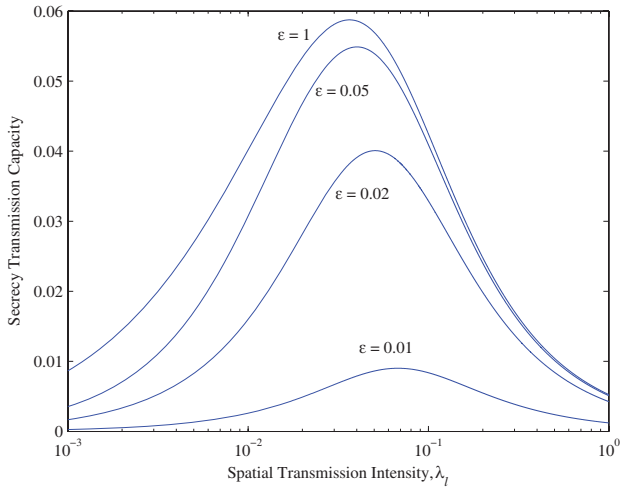


Fig. 3. The secrecy transmission capacity $\tau^{\mathrm{LB}}(r)$ in (20) versus the density of legitimate transmitters λ_l. Results are shown for networks with different secrecy outage constraints, i.e., $\epsilon = 0.01, 0.02, 0.05$, as well as no secrecy constraint, i.e., $\epsilon = 1$. The other system parameters are $r = 1$, $\alpha = 4$, $\sigma = 0.3$, and $\lambda_e = 0.001$.

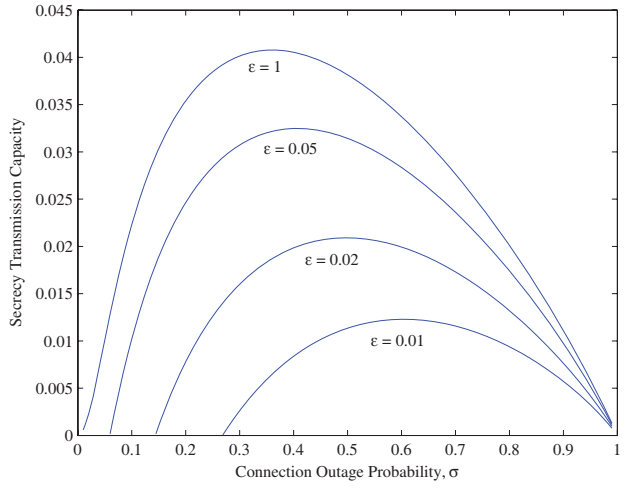


Fig. 4. The secrecy transmission capacity $\tau^{\mathrm{LB}}(r)$ in (20) versus the connection outage probability σ. Results are shown for networks with different secrecy outage constraints, i.e., $\epsilon = 0.01, 0.02, 0.05$, as well as no secrecy constraint, i.e., $\epsilon = 1$. The other system parameters are $r = 1$, $\alpha = 4$, $\lambda_l = 0.01$, and $\lambda_e = 0.001$.

system parameters and their effects on the secrecy transmission capacity for networks without secrecy guard zones. Fig. 3 shows the secrecy transmission capacity $\tau^{\mathrm{LB}}(r)$ in (20) versus the spatial transmission intensity λ_l with different security requirements. Comparing between the four curves, we see that the gap in $\tau^{\mathrm{LB}}(r)$ between $\epsilon = 1$ and $\epsilon = 0.05$ is relatively small over a wide range of λ_l. This suggests that the throughput cost of achieving a moderate security requirement is relatively low. On the other hand, $\tau^{\mathrm{LB}}(r)$ drops dramatically as ϵ decreases towards 0. For example, there is a 84% reduction in $\tau^{\mathrm{LB}}(r)$ for improving the security level from $\epsilon = 0.02$ to $\epsilon = 0.01$ at $\lambda_l = 0.01$. This reflects a significant increase in the throughput cost of achieving highly secure networks.

For each curve in Fig. 3, we see that the optimal value of λ_l is generally much larger than λ_e. This suggests that it is desirable to have a significantly larger number of legitimate nodes than the number of eavesdroppers in the network, which creates a high level of interference to mask the confidential message transmissions against eavesdropping. Furthermore, the optimal value of λ_l increases as ϵ decreases. For example, the optimal λ_l is 0.04 for $\epsilon = 0.05$, while it increases to 0.051 for $\epsilon = 0.02$ and to 0.068 for $\epsilon = 0.01$. Note that the optimal value of λ_l computed from (24) is 0.063 for $\epsilon = 0.01$, which is very close to the numerical result.

Fig. 4 shows the secrecy transmission capacity $\tau^{\mathrm{LB}}(r)$ in (20) versus the connection outage probability σ with different security requirements. The feasible range of σ for positive secrecy transmission capacity never reaches 0, which agrees with the result in (22). We see that a moderate connection outage probability is desirable for achieving high secrecy transmission capacity. Furthermore, the optimal value of σ increases as ϵ reduces. This is because that a larger R_e is needed for a stronger security requirement, in which case larger R_t and (hence) σ are desirable for maximizing the secrecy transmission capacity. For example, the optimal σ is 0.4 for $\epsilon = 0.05$ while it increases to 0.5 for $\epsilon = 0.02$ and to 0.6 for $\epsilon = 0.01$. Note that the optimal value of σ can be accurately computed from the closed-form expression in (28) for sparse networks.

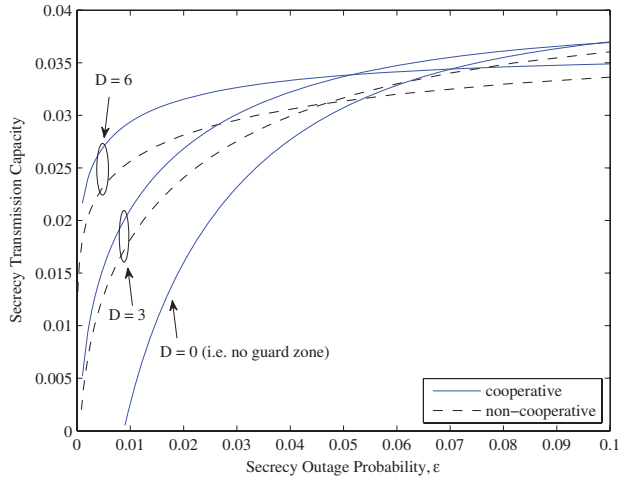


Fig. 5. The secrecy transmission capacity $\tau^{\mathrm{LB}}(r)$ with guard zone in (35) and (39) versus the secrecy outage probability ϵ. Results are shown for networks with different guard zone radii, i.e., $D = 0, 3, 6$. The other system parameters are $r = 1$, $\alpha = 4$, $\sigma = 0.3$, $\lambda_l = 0.01$, and $\lambda_e = 0.001$.

Now, we present the results on the use of a guard zone for improving the secrecy transmission capacity. Fig. 5 shows $\tau^{\mathrm{LB}}(r)$ in (35) and (39) versus the secrecy outage probability ϵ for both the non-cooperative and cooperative protocols.[6] This figure clearly shows the remarkable benefit of guard zone for networks with high security requirements. For example, the secrecy transmission capacity at $\epsilon = 0.01$ increases from 0.003 at $D = 0$ (i.e., no guard zone) to 0.018 with non-cooperative protocol and 0.021 with cooperative protocol at $D = 3$. On the other hand, the benefit of guard zone reduces as the security requirement reduces. We also see that the cooperative protocol outperforms the non-cooperative protocol and the difference

[6]Although we have chosen $r = 1$ in Fig. 5, the benefit of using a secrecy guard zone demonstrated in Fig. 5 is also observed for other values of r which can be either less than or greater than D (plots omitted for brevity).

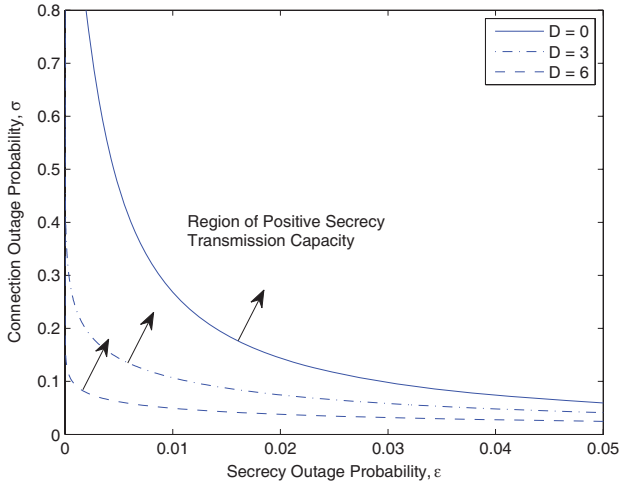


Fig. 6. The region of positive secrecy transmission capacity with and without secrecy guard zone. The case of cooperative transmitters is shown with different guard zone radii, i.e., $D = 0, 3, 6$. The curves are plotted based on the relationship between the connection outage probability σ and the secrecy outage probability ϵ given in (40). The other system parameters are $r = 1$ and $\lambda_e = 0.001$.

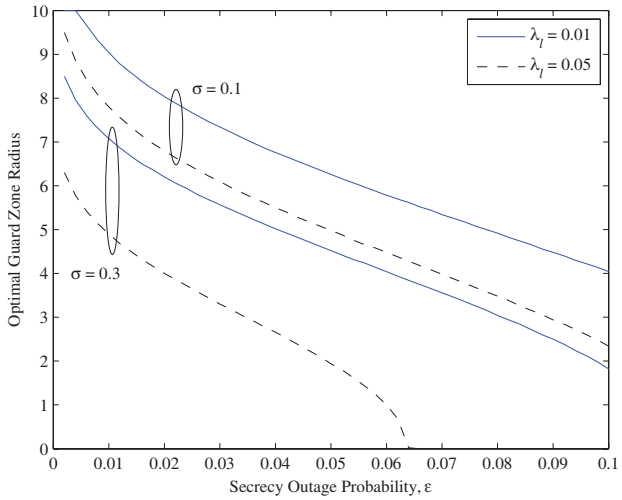


Fig. 7. The optimal secrecy guard zone radius versus the secrecy outage probability ϵ for the case of cooperative transmitters. Results are shown for networks with different connection outage constraints, i.e., $\sigma = 0.1, 0.3$, and different densities of legitimate transmitters, i.e., $\lambda_l = 0.01, 0.05$. The other system parameters are $r = 1$, $\alpha = 4$, and $\lambda_e = 0.001$.

in secrecy transmission capacity is significant for networks with high security requirement. For example, the increase in $\tau^{\mathrm{LB}}(r)$ from the non-cooperative case to the cooperative case at $\epsilon = 0.01$ is 17% when $D = 3$ and 14% when $D = 6$.

The feasible regions of the connection outage probability σ and the secrecy outage probability ϵ for positive secrecy transmission capacity are illustrated in Fig. 6. The case of cooperative transmitters is considered when the guard zone is used. In general, it is impossible to have arbitrarily low outage probabilities while still operating at some positive secrecy transmission capacity. Nevertheless, the use of a guard zone greatly enlarges the feasible ranges of both outage probabilities.

Fig. 7 shows the optimal guard zone radius for cooperative transmitters. We see that the optimal value of D reduces as the acceptable secrecy outage probability ϵ increases and it reaches zero at moderate to high values of ϵ. We can also see the dependence of the optimal D on σ and λ_l. The general trend is that the optimal D reduces as σ or λ_l increases. The dependence of the optimal D on σ agrees with our earlier observation from (40). The dependence on λ_l can be understood as follows: As the interference level (i.e., λ_l) increases, the signal power received at the eavesdroppers is allowed to be higher for maintaining the same SIR. This in turn allows us to reduce the guard zone radius, which increases the spatial intensity of message transmissions. In practice, a legitimate transmitter may only be able to detect the existence of eavesdroppers in its vicinity, hence, the guard zone is usually small. Nevertheless, we have seen from Fig. 5 that a significant improvement in the secrecy transmission capacity can be achieved even with a small guard zone. Furthermore, by allowing a moderate connection outage probability, it is possible for the network to operate with the optimal guard zone radius which is within the maximum detection range of the transmitters.

VI. Conclusions

In this work, we defined a performance metric named the secrecy transmission capacity, which was used to study the impact of physical layer security requirements on the throughput of large-scale decentralized wireless networks. Using tools and existing results from stochastic geometry, the secrecy transmission capacity can usually be characterized in simple analytical forms, as shown in this paper for Rayleigh fading channels. One important finding is that the throughput cost of achieving a moderate security level is relatively low, while it becomes very expensive to realize a highly secure network. In addition, we showed that the application of secrecy guard zone with artificial noise is a simple technique that can be used to dramatically reduce the throughput cost of achieving highly secure networks.

This model of secrecy transmission capacity can be extended to analyze and design networks with other transmission techniques, medium access control protocols, and eavesdropping strategies in future work. Similar to other transmission capacity formulations, the main limitation of this model is that it only considers single-hop transmissions, while the communication between an arbitrary source-destination pair usually requires multiple hops. End-to-end throughput analysis of wireless networks with physical layer security requirements is still an open problem. Another limitation of the current model is the homogeneous Poisson distribution of nodes. The impact of eavesdropper distribution on secrecy throughput is an interesting problem to investigate.

References

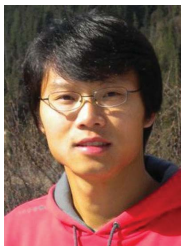
[1] A. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[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] Z. Li, W. Trappe, and R. Yates, "Secret communication via multi-antenna transmission," in *Proc. 41st Annual Conf. on Inform. Sciences and Syst.*, Mar. 2007, pp. 905–910.

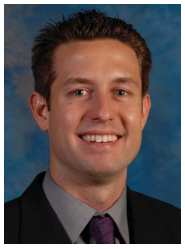
[4] S. Shafiee and S. Ulukus, "Achievable rates in Gaussian MISO channels with secrecy constraints," in *Proc. IEEE Int. Symp. Inform. Theory*, June 2007, pp. 2466–2470.

[5] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas: the MIMOME channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.
[6] 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.
[7] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Secure wireless communications via cooperation," in *Proc. 46th Annual Allerton Conf. Commun., Control, and Computing*, Sep. 2008, pp. 1132–1138.
[8] Y. Liang and H. V. Poor, "Multiple-access channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 54, no. 3, pp. 976–1002, Mar. 2008.
[9] 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, June 2008.
[10] M. Haenggi, "The secrecy graph and some of its properties," in *Proc. IEEE Int. Symp. Inf. Theory*, July 2008, pp. 539–543.
[11] P. C. Pinto, J. Barros, and M. Z. Win, "Secure communication in stochastic wireless networks," submitted. Available at http://arxiv.org/abs/1001.3697.
[12] S. Goel, V. Aggarwal, A. Yener, and A. R. Calderbank, "Modeling location uncertainty for eavesdroppers: a secrecy graph approach," in *Proc. IEEE Int. Symp. Inf. Theory*, June 2010.
[13] P. C. Pinto and M. Z. Win, "Continuum percolation in the intrinsically secure communications graph," in *Proc. IEEE Int. Symp. Inf. Theory and its Applications*, Oct. 2010.
[14] 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.
[15] A. Sarkar and M. Haenggi, "Secrecy coverage," in *Proc. Asilomar Conf. Signals, Systems, and Computers*, Nov. 2010.
[16] O. O. Koyluoglu, C. E. Koksal, and H. El Gamal, "On secrecy capacity scaling in wireless networks," submitted. Available at http://arxiv.org/abs/0908.0898.
[17] Y. Liang, H. V. Poor, and L. Ying, "Secrecy throughput of MANETs with malicious nodes," in *Proc. IEEE Int. Symp. Inf. Theory*, June 2009, pp. 1189–1193.
[18] S. Vasudevan, D. Goeckel, and D. Towsley, "Security-capacity trade-off in large wireless networks using keyless secrecy," in *Proc. ACM Int. Symp. Mobile Ad Hoc Networking and Computing*, Sep. 2010, pp. 21–30.
[19] 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.
[20] S. Weber, X. Yang, J. G. Andrews, and G. de Veciana, "Transmission capacity of wireless ad hoc networks with outage constraints," *IEEE Trans. Inf. Theory*, vol. 51, no. 12, pp. 4091–4102, Dec. 2005.
[21] 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.
[22] A. Subramanian, A. Thangaraj, M. Bloch, and S. W. McLaughlin, "Strong secrecy on the binary erasure wiretap channel using large-girth LDPC codes," to appear in *IEEE Trans. Inf. Forensics and Security*. Available at http://arxiv.org/abs/1009.3130.
[23] 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.
[24] 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.
[25] D. Stoyan, W. Kendall, and J. Mecke, *Stochastic Geometry and Its Applications*, 2nd edition. John Wiley and Sons, 1996.
[26] 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.*, Oct. 2006, pp. 1–7.
[27] F. Baccelli, B. Błaszczyszyn, and P. Mühlethaler, "An Aloha protocol for multihop mobile wireless networks," *IEEE Trans. Inf. Theory*, vol. 52, no. 2, pp. 421–436, Feb. 2006.
[28] M. Haenggi, "On distances in uniformly random networks," *IEEE Trans. Inf. Theory*, vol. 51, no. 10, pp. 3584–3586, Oct. 2005.
[29] R. K. Ganti and M. Haenggi, "Single-hop connectivity in interference-limited hybrid wireless networks," in *Proc. IEEE Int. Symp. Inf. Theory*, June 2007, pp. 366–370.
[30] A. Hasan and J. G. Andrews, "The guard zone in wireless ad hoc networks," *IEEE Trans. Wireless Commun.*, vol. 6, no. 3, pp. 897–906, Mar. 2007.
[31] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, June 2008.
[32] E. Ekrem and S. Ulukus, "Secrecy in cooperative relay broadcast channels," submitted to *IEEE Trans. Inf. Theory*. Available at http://arxiv.org/abs/0811.1317.
[33] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "Interference assisted secrect communication," to appear in *IEEE Trans. Inf. Theory*. Available at http://arxiv.org/pdf/0908.2397.
[34] I. S. Gradshteyn and I. M. Ryzhik, *Tables of Integrals, Series, and Products*, 7th edition. Academic Press, 2007.
[35] L. Kleinrock and F. A. Tobagi, "Packet switching in radio channels–part I: carrier sense multiple access modes and their throughput-delay characteristics," *IEEE Trans. Commun.*, vol. 23, no. 12, pp. 1400–1416, Dec. 1975.



Xiangyun Zhou (S'08, M'11) received the B.E. (hons.) degree in electronics and telecommunications engineering and the Ph.D. degree in telecommunications engineering from the Australian National University, Australia, in 2007 and 2010, respectively. He is currently a postdoctoral research fellow at UNIK - University Graduate Center, University of Oslo, Norway. His research interests are in the fields of wireless communications and signal processing, including MIMO systems, ad hoc networks, relay and cooperative communications, and physical layer security. He is a recipient of the Best Paper Award at the 2011 IEEE International Conference on Communications.

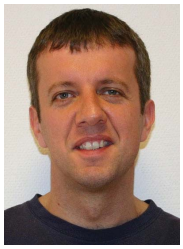
Radha Krishna Ganti (M'10) is a Postdoctoral researcher in the Wireless Networking and Communications Group at UT Austin. He received his B.Tech. and M.Tech. in EE from Indian Institute of Technology, Madras, and Masters in Applied Math and Ph.D. in EE from University of Notre Dame in 2009. His doctoral work focused on the spatial analysis of interference networks using tools from stochastic geometry. He is co-author of the monograph *Interference in Large Wireless Networks*.



Jeffrey Andrews (S'98, M'02, SM'06) received the B.S. in Engineering with High Distinction from Harvey Mudd College in 1995, and the M.S. and Ph.D. in Electrical Engineering from Stanford University in 1999 and 2002, respectively. He is an Associate Professor in the Department of Electrical and Computer Engineering at the University of Texas at Austin, and the Director of the Wireless Networking and Communications Group (WNCG), a research center comprising 17 faculty and 13 industrial affiliates. He developed Code Division Multiple Access systems at Qualcomm from 1995-97, and has consulted for entities including the WiMAX Forum, Microsoft, Apple, Clearwire, Palm, Sprint, ADC, and NASA.

Dr. Andrews is co-author of two books, *Fundamentals of WiMAX* (Prentice-Hall, 2007) and *Fundamentals of LTE* (Prentice-Hall, 2010), and holds the Earl and Margaret Brasfield Endowed Fellowship in Engineering at UT Austin, where he received the ECE department's first annual High Gain award for excellence in research. He is a Senior Member of the IEEE, served as an associate editor for the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS from 2004-08, was the Chair of the 2010 IEEE Communication Theory Workshop, and is the Technical Program co-Chair of ICC 2012 (Comm. Theory Symposium) and Globecom 2014. He has also been a guest editor for two recent IEEE JSAC special issues on stochastic geometry and femtocell networks.

Dr. Andrews received the National Science Foundation CAREER award in 2007 and is the Principal Investigator of a 9 university team of 12 faculty in DARPA's Information Theory for Mobile Ad Hoc Networks program. He has been co-author of five best paper award recipients, two at Globecom (2006 and 2009) Asilomar (2008), the 2010 IEEE Communications Society Best Tutorial Paper Award, and the 2011 Communications Society Heinrich Hertz Prize. His research interests are in communication theory, information theory, and stochastic geometry applied to wireless ad hoc and heterogeneous cellular networks.



Are Hjørungnes works as a Professor at the Faculty of Mathematics and Natural Sciences at the University of Oslo, Norway with office located at UNIK - University Graduate Center. He obtained his Sivilingeniør (M.Sc.) degree (with honors) in 1995 from the Department of Telecommunications at the Norwegian Institute of Technology in Trondheim, Norway, and his Doktor ingeniør (Ph.D.) degree in 2000 from the Signal Processing Group at the Norwegian University of Science and Technology. His current main research areas are signal processing, communications, and wireless networks. He authored the book *Complex-Valued Matrix Derivatives: With Applications in Signal Processing and Communications* (Cambridge University Press, 2011).

From August 2000 to December 2000, he worked as a researcher at Tampere University of Technology, in Finland, within the Tampere International Center for Signal Processing. From March 2001 to July 2002, he worked as a postdoctoral fellow at the Federal University of Rio de Janeiro in Brazil, within the Signal Processing Laboratory. From September 2002 to August 2003, he worked as a postdoctoral fellow at the Helsinki University of Technology in Finland, within the Signal Processing Laboratory. From September 2003 to August 2004, he was working as a postdoctoral fellow at the University of Oslo in Norway, at the Department of Informatics, within the Digital Signal Processing and Image Analysis Group.

He has held visiting appointments at the Image and Signal Processing Laboratory at the University of California, Santa Barbara, the Signal Processing Laboratory of the Federal University of Rio de Janeiro, the Mobile Communications Department at Eurecom Institute in France, the University of Manitoba in Canada, the Alcatel-Lucent Chair at SUPÉLEC in France, the Department of Electrical and Computer Engineering at the University of Houston in USA, the Electrical and Computer Engineering Department at University of California, San Diego, USA, and the Department of Electrical Engineering, University of Hawai'i at Mānoa, USA.

Since March 2007, he has been serving as an Editor for IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS. In 2010 and 2011, he was a Guest Editor for IEEE JOURNAL OF SELECTED TOPICS IN SIGNAL PROCESSING and IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, in the special issues on "Model Order Selection in Signal Processing Systems" and "Cooperative Networking - Challenges and Applications," He co-authored the papers winning the best paper awards at IEEE International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM 2007), 7th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt 2009), and 5th International Conference on Internet Monitoring and Protection (ICIMP 2010).