Forty-Ninth Annual Allerton Conference
Allerton House, UIUC, Illinois, USA
September 28 - 30, 2011

Secrecy Transmission Capacity of Decentralized Wireless Networks

Xiangyun Zhou*, Radha Krishna Ganti†, Jeffrey G. Andrews†, and Are Hjørungnes‡

*Research School of Engineering, Australian National University, ACT 0200, Australia
†Department of Electrical and Computer Engineering, University of Texas at Austin, TX 78712
‡UNIK - University Graduate Center, University of Oslo, Kjeller, NO-2027, Norway
Email: xiangyun.zhou@anu.edu.au, rganti@austin.utexas.edu, jandrews@ece.utexas.edu, arehj@unik.no

***Abstract*—Secure communication over large-scale decentralized wireless networks is an extremely challenging task due to the cost and difficulty in establishing secret keys among all the nodes in a distributed manner. For this reason, the notion of physical layer security has recently drawn significant attention, which may assist with key exchange and provide an additional layer of protection in such networks. In this paper, we investigate how the physical layer security constraints affect the network throughput. We consider a random network in which the legitimate and eavesdropper nodes are located according to independent Poisson point processes. We introduce a new metric "secrecy transmission capacity" to characterize the network throughput in terms of the area spectral efficiency of secure transmissions, subject to constraints on both the quality of service and the level of security. This capacity framework allows us to quantitatively study the throughput cost of physical layer security constraints. We observe 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.**

I. Introduction

Security is a fundamental challenge in wireless networks, and one increasing in importance as more and more computing and sensitive communication is done through wireless devices. Unlike encryption-based security, information-theoretic studies have showed that "perfect" secrecy can be achieved in the physical layer by properly designing an encoder-decoder pair, but only if the legitimate receiver has a stronger channel than the eavesdropper [1, 2]. This has motivated a significant recent effort on physical layer security enhancements, including multi-antenna transmission [3–5] and cooperative communications [6, 7]. These works have mostly focused on systems with a small number of nodes.

Unlike point-to-point communications, the communication between nodes in large-scale networks strongly depends on locations of other nodes and how the nodes interact with each other. When secrecy is added into consideration, the locations and channel information of the eavesdroppers, which are usually unknown, become extra parameters affecting the network performance. Initial works on networks with physical layer security constraints studied the connectivity [8–12], coverage [13], and capacity scaling laws [14–16]. Specifically, various statistical characterizations of the existence of secure connections were given in [8–10, 12]. Using tools from percolation theory, the existence of a secrecy graph was analyzed in [8, 10, 11]. 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 [14–16] 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 [17].

In this work, we aim to characterize the throughput of secure communications in decentralized wireless networks and to understand how the physical layer security requirements affect the network throughput. Our approach uses a metric termed the *transmission capacity* [18], which provides the area spectral efficiency (ASE) of decentralized networks with random topology, identical nodes, and a constraint on outage probability. We extend this capacity framework to study the impact of the security requirements on the network ASE. The network considered have both legitimate nodes and eavesdroppers, whose locations follow homogeneous Poisson 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.

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 quantitatively characterizes the dependence of the network throughput on the key system parameters, *i.e.*, the densities of legitimate nodes and eavesdroppers, as well as the QoS and security constraints. Specifically, we find that the throughput reduction for achieving a moderate

This work was supported by the Australian Research Council's Discovery Projects funding scheme (project no. DP110102548), the DARPA IT-MANET project, and the Research Council of Norway through the project 197565/V30.

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 transmission of confidential messages whilst satisfying both constraints. It turns out that the QoS and security constraints as well as the density of eavesdroppers are crucial in determining whether transmission is allowed, while the density of legitimate nodes is irrelevant.

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. Numerical results are presented in Section IV and concluding remarks in Section V. 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 $\mathrm{P_{so}}$
r	Distance between the legitimate transmitter-receiver pair
τ	Secrecy transmission capacity
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
$\mathbb{P}(.)$	Probability measure
$\mathbb{E}\{.\}$	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.[1] 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 [19]. Note that the eavesdroppers need to have similar mobility and other behaviors as the legitimate nodes since they can be easily identified otherwise [15]. Furthermore, we assume that the eavesdroppers do not collude with each other and, hence, must decode the confidential messages individually.

Consider a single 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. 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. A detailed description of the Wyner code can be found in [1, 20, 21].

In an ad hoc network with simultaneous transmissions from infinitely many legitimate transmitters, it is difficult to study the mutual information between an arbitrary 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 [21]:

- **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 $\mathrm{P_{co}}$.
- **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 $\mathrm{P_{so}}$.

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

A. Secrecy Transmission Capacity

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 [18] 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

[1]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.

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 $\mathrm{P_{co}} = \sigma$ and a secrecy outage probability of $\mathrm{P_{so}} = \epsilon$, is defined as

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

where $\bar{R}_s$ is the average rate of confidential messages over all legitimate transmitter-receiver pairs. The rate of confidential messages of a particular transmitter-receiver pair depends on the transmit power and distance. We focus on a simple scenario where the transmit power of all the legitimate nodes is fixed to the same value. In this paper, we also assume that all the transmitter-receiver pairs have equal distance denoted as r. This assumption is often adopted in the transmission capacity literature, *e.g.*, [18, 19]. Consequently, the secrecy transmission capacity can be written as

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

where R_s is a function of r. Note that $R_s = R_t - R_e$ is also a function of the connection outage and secrecy outage constraints: The connection outage constraint σ determines the value of R_t, while the secrecy outage constraint ϵ determines the value of R_e. Whenever R_s is computed to be negative, transmission is not possible and R_s is effectively zero. When transmission is possible 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 $1-\epsilon$.

If one allows the distances between the legitimate transmitter-receiver pairs to be different and follow some distribution $f(r)$, the secrecy transmission capacity can be computed by averaging over $f(r)$. Since in practice the distribution of r depends on specific scenarios, we do not consider the variation in r and focus on characterizing $\tau(r)$ in this paper.

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 [22], 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

$$\mathrm{SIR}_0 = \frac{S_0 r^{-\alpha}}{\sum_{l\in\Phi_l} S_l |X_l|^{-\alpha}}, \tag{3}$$

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

$$\beta_t = 2^{R_t} - 1. \tag{4}$$

Hence, the connection outage probability can be written as

$$\mathrm{P_{co}} = \mathbb{P}\Big(\mathrm{SIR}_0 < \beta_t\Big) = \mathbb{P}\left(\frac{S_0 r^{-\alpha}}{\sum_{l\in\Phi_l} S_l |X_l|^{-\alpha}} < \beta_t\right). \tag{5}$$

The summation term $\sum_{l\in\Phi_l} S_l|X_l|^{-\alpha}$ is a shot noise process [23] in two-dimensional space whose Laplace transform is known in a closed form and was used to compute the connection outage probability in [24] as

$$\mathrm{P_{co}} = 1 - \exp\left[-\lambda_l \pi r^2 \beta_t^{2/\alpha} \Gamma\Big(1-\frac{2}{\alpha}\Big)\Gamma\Big(1+\frac{2}{\alpha}\Big)\right]. \tag{6}$$

With the connection outage constraint given by $\mathrm{P_{co}} = \sigma$, the transmission rate R_t can be found using (4) and (6) as

$$R_t = \log_2\left(1 + \left[\frac{\ln\frac{1}{1-\sigma}}{\lambda_l \pi r^2 \Gamma\Big(1-\frac{2}{\alpha}\Big)\Gamma\Big(1+\frac{2}{\alpha}\Big)}\right]^{\frac{\alpha}{2}}\right). \tag{7}$$

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

$$\mathrm{SIR}_e = \frac{S_e |X_e|^{-\alpha}}{\sum_{l\in\Phi_l} S_{le} |X_{le}|^{-\alpha}}, \tag{8}$$

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

$$\beta_e = 2^{R_e} - 1. \tag{9}$$

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

$$\begin{aligned} \mathrm{P_{so}} &= 1 - \mathbb{E}_{\Phi_l}\Big\{\mathbb{E}_{\Phi_e}\Big\{\mathbb{E}_S\Big\{\prod_{e\in\Phi_e}\Big(1-1_A(e)\Big)\Big\}\Big\}\Big\}, \\ &= 1 - \mathbb{E}_{\Phi_l}\Bigg\{\mathbb{E}_{\Phi_e}\Bigg\{ \\ &\quad \prod_{e\in\Phi_e}\Bigg(1-\mathbb{P}\Big(\frac{S_e|X_e|^{-\alpha}}{\sum_{l\in\Phi_l}S_{le}|X_{le}|^{-\alpha}} > \beta_e\Big|\Phi_e,\Phi_l\Big)\Bigg)\Bigg\}\Bigg\}. \end{aligned} \tag{10}$$

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 (10). Since it is difficult to express $\mathrm{P_{so}}$ in a closed form, we resort to 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

$$\mathrm{P_{so}^{UB}} = 1 - \exp\left[-\frac{\lambda_e}{\lambda_l\beta_e^{2/\alpha}\Gamma\Big(1-\frac{2}{\alpha}\Big)\Gamma\Big(1+\frac{2}{\alpha}\Big)}\right], \tag{11}$$

and bounded from below by

$$\mathrm{P_{so}^{LB}} = \frac{1}{1+\frac{\lambda_l}{\lambda_e}\beta_e^{2/\alpha}\Gamma\Big(1-\frac{2}{\alpha}\Big)\Gamma\Big(1+\frac{2}{\alpha}\Big)}. \tag{12}$$

Proof: Using the generating functional of the PPP Φ_e [22], we can express the secrecy outage probability in (10) as

$$\begin{aligned} \mathrm{P_{so}} &= 1 - \mathbb{E}_{\Phi_l}\Bigg\{ \\ &\quad \exp\left[-\lambda_e\int_{\mathbb{R}^2}\mathbb{P}\Big(\frac{S_e|X_e|^{-\alpha}}{\sum_{l\in\Phi_l}S_{le}|X_{le}|^{-\alpha}} > \beta_e\Big|\Phi_l\Big)\mathrm{d}e\right]\Bigg\}. \end{aligned} \tag{13}$$

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

$$\begin{aligned} \mathrm{P_{so}} &\le 1 - \exp\left[-\lambda_e\int_{\mathbb{R}^2}\mathbb{P}\Big(\frac{S_e|X_e|^{-\alpha}}{\sum_{l\in\Phi_l}S_{le}|X_{le}|^{-\alpha}} > \beta_e\Big)\mathrm{d}e\right] \\ &= 1 - \exp\Bigg[-2\pi\lambda_e \\ &\quad \cdot\int_0^\infty \exp\left[-\lambda_l\pi r_e^2\beta_e^{2/\alpha}\Gamma\Big(1-\frac{2}{\alpha}\Big)\Gamma\Big(1+\frac{2}{\alpha}\Big)\right] r_e\mathrm{d}r_e\Bigg], \end{aligned} \tag{14}$$

where r_e denotes the distance between the typical transmitter and eavesdropper e, (14) is arrived in the same way as (6) followed by changing to polar coordinates. The upper bound in (11) is then obtained by directly evaluating the integral in (14).

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 [25]

$$f(r_{e'}) = 2\lambda_e\pi r_{e'}\exp(-\lambda_e\pi r_{e'}^2). \tag{15}$$

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

$$\begin{aligned} \mathrm{P_{so}} &\ge \int_0^\infty \mathbb{P}\Big(\frac{S_{e'}r_{e'}^{-\alpha}}{\sum_{l\in\Phi_l}S_{le'}|X_{le'}|^{-\alpha}} > \beta_e\Big)f(r_{e'})\mathrm{d}r_{e'} \\ &= \int_0^\infty \exp\left[-\lambda_l\pi r_{e'}^2\beta_e^{2/\alpha}\Gamma\Big(1-\frac{2}{\alpha}\Big)\Gamma\Big(1+\frac{2}{\alpha}\Big)\right] \\ &\qquad \cdot 2\lambda_e\pi r_{e'}\exp(-\lambda_e\pi r_{e'}^2)\mathrm{d}r_{e'}. \end{aligned} \tag{16}$$

The lower bound in (12) is then obtained by directly evaluating the integral in (16). ■

Note that the authors in [26] 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 [26, Fig. 5], we know that the upper bound $\mathrm{P_{so}^{UB}}$ in (11) 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 (12) 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 (11) and (12) can be approximated by

$$\mathrm{P_{so}^{UB}} \approx \frac{\lambda_e}{\lambda_l\beta_e^{2/\alpha}\Gamma\Big(1-\frac{2}{\alpha}\Big)\Gamma\Big(1+\frac{2}{\alpha}\Big)} \approx \mathrm{P_{so}^{LB}}. \tag{17}$$

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 (11), the value of R_e that guarantees the required security level can be found as

$$R_e = \log_2\left(1+\Big[\frac{\lambda_l}{\lambda_e}\Gamma\Big(1-\frac{2}{\alpha}\Big)\Gamma\Big(1+\frac{2}{\alpha}\Big)\ln\frac{1}{1-\epsilon}\Big]^{-\frac{\alpha}{2}}\right). \tag{18}$$

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

Having R_t in (7) and R_e in (18), we compute the rate of confidential messages as $R_s = [R_t - R_e]^+$, where $[z]^+ = \max\{0, z\}$. Hence, a lower bound on the secrecy transmission capacity is obtained as $\tau^{\mathrm{LB}}(r) = R_s(1-\sigma)\lambda_l$, which 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

$$\tau^{\mathrm{LB}}(r) = (1-\sigma)\lambda_l \cdot \left[\log_2\left(\frac{1+\left[\frac{\ln\frac{1}{1-\sigma}}{\lambda_l \pi r^2 \Gamma(1-\frac{2}{\alpha})\Gamma(1+\frac{2}{\alpha})}\right]^{\frac{\alpha}{2}}}{1+\left[\frac{\lambda_l}{\lambda_e}\Gamma\left(1-\frac{2}{\alpha}\right)\Gamma\left(1+\frac{2}{\alpha}\right)\ln\frac{1}{1-\epsilon}\right]^{-\frac{\alpha}{2}}}\right)\right]^+. \quad (19)$$

From our discussion on the accuracy of $\mathrm{P}_{\mathrm{so}}^{\mathrm{UB}}$, we know that the lower bound on the secrecy transmission capacity in (19) 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 (19) as the secrecy transmission capacity in the rest of this paper. It is clear from (19) 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[2] 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. Condition for Transmission

A fundamental question to ask is the condition under which transmission is allowed whilst still satisfying the QoS and security constraints. From the expression in (19), one can find a sufficient condition for transmission by solving $\tau^{\mathrm{LB}}(r) > 0$:

Corollary 1: For a connection outage constraint of σ and a secrecy outage constraint of ϵ, secure transmission is possible when

$$\ln\frac{1}{1-\sigma}\ln\frac{1}{1-\epsilon} \quad > \quad \pi r^2 \lambda_e. \quad (20)$$

In other words, transmission is possible 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 (20) 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 feasible range of σ can be found from (20) as

$$\sigma \in \left(1-\exp\left[-\frac{\pi r^2 \lambda_e}{\ln\frac{1}{1-\epsilon}}\right], 1\right). \quad (21)$$

[2]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.

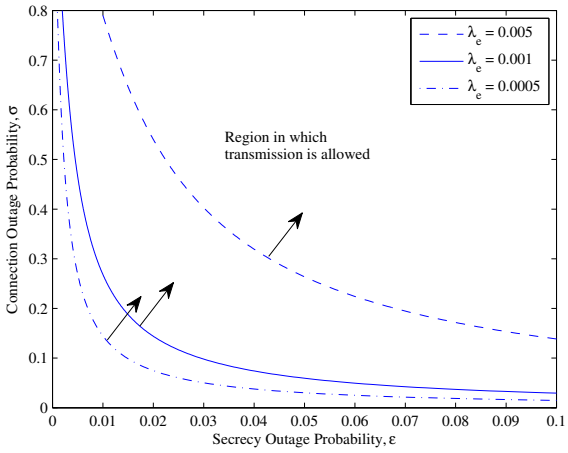

Fig. 1. The region in which transmission is allowed. Results are shown for networks with different densities of eavesdroppers, *i.e.*, $\lambda_e = 0.005, 0.001, 0.0005$. The curves are plotted based on the relationship between the connection outage probability σ and the secrecy outage probability ϵ given in (20). The transmission distance is $r = 1$.

Remark 2: The condition for transmission does not depend on the spatial transmission intensity λ_l. That is to say, one cannot enable transmission simply by bringing in additional legitimate users or deactivating existing legitimate users, if the required connection outage and secrecy outage performances of the network do not meet the condition in (20).

IV. Numerical Results and Discussion

In this section, we present numerical results to show the interplay of different system parameters and their effects on the secrecy transmission capacity.

The feasible regions of the connection outage probability σ and the secrecy outage probability ϵ in which transmission at a positive rate is allowed are illustrated in Fig. 1. In general, it is impossible to have arbitrarily low outage probabilities while still operating at some positive secrecy transmission capacity. The boundary lines shown in the figure illustrate the trade-off between the QoS and security performance as discussed in Remark 1 in Section III-A. For example, a connection outage probability of at least $\sigma = 0.27$ is required to enable transmission in a network with a security requirement of $\epsilon = 0.01$ and an eavesdropper density of $\lambda_e = 0.001$.

Fig. 2 shows the secrecy transmission capacity $\tau^{\mathrm{LB}}(r)$ in (19) 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.

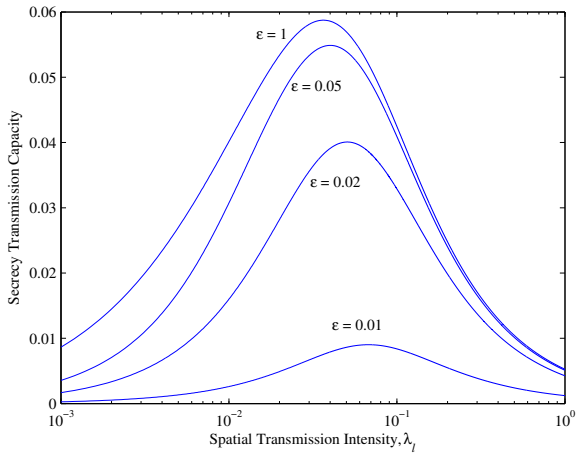

Fig. 2. The secrecy transmission capacity $\tau^{\mathrm{LB}}(r)$ in (19) versus the density of legitimate transmitters λ_l. Results are shown for networks with different secrecy outage constraints, *i.e.*, $\epsilon = 0.01, 0.02, 0.05$, as well as no secrecy constraint, *i.e.*, $\epsilon = 1$. The other system parameters are $r = 1$, $\alpha = 4$, $\sigma = 0.3$, and $\lambda_e = 0.001$.

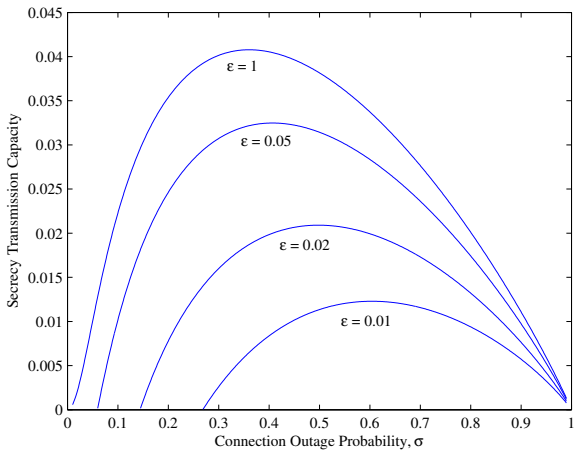

Fig. 3. The secrecy transmission capacity $\tau^{\mathrm{LB}}(r)$ in (19) versus the connection outage probability σ. Results are shown for networks with different secrecy outage constraints, *i.e.*, $\epsilon = 0.01, 0.02, 0.05$, as well as no secrecy constraint, *i.e.*, $\epsilon = 1$. The other system parameters are $r = 1$, $\alpha = 4$, $\lambda_l = 0.01$, and $\lambda_e = 0.001$.

For each curve in Fig. 2, 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 $\epsilon = 0.01$.

Fig. 3 shows the secrecy transmission capacity $\tau^{\mathrm{LB}}(r)$ in (19) versus the connection outage probability σ with different security requirements. Again, the feasible range of σ for positive secrecy transmission capacity never reaches 0, which agrees with the result in (21). 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 $\epsilon = 0.01$.

The numerical results in Figs. 2 and 3 quantitatively showed the throughput cost of physical layer security constraints, from which we see the need for transmission protocols that significantly reduce the throughput cost of achieving high security. Since insecure transmission is mainly due to the presence of eavesdroppers close to the transmitter, the idea of guard zone becomes appropriate for avoiding high-risk transmissions and was studied in the journal version of this paper [27]. This protocol requires the transmitters to detect the presence of eavesdroppers within their guard zones. Message transmission only happens if no eavesdropper is found.

V. Conclusions

In this paper, we introduced a new notion of secrecy transmission capacity that was used to characterize the impact of physical layer security requirements on the throughput of large-scale decentralized wireless networks. We obtained simple and tractable results for Rayleigh fading channels, and gave a sufficient condition on the system parameters for having positive secrecy transmission capacity. An important observation 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. This model of secrecy transmission capacity can be extended in future to analyze and design networks with other transmission techniques, medium access control protocols, and eavesdropping strategies.

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. Inform. 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. (CISS)*, Baltimore, MD, 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 (ISIT)*, Nice, France, Jun. 2007, pp. 2466–2470.

[5] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas: The MIMOME channel," *IEEE Trans. Inform. 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. Inform. 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*, Monticello, IL, Sep. 2008, pp. 1132–1138.

[8] M. Haenggi, "The secrecy graph and some of its properties," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Toronto, Canada, Jul. 2008, pp. 539–543.
[9] P. C. Pinto, J. Barros, and M. Z. Win, "Secure communication in stochastic wireless networks," submitted. Available at http://arxiv.org/abs/1001.3697.
[10] 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 (ISIT)*, Austin, TX, Jun. 2010.
[11] 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 (ISITA)*, Taichung, Taiwan, Oct. 2010.
[12] 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.
[13] A. Sarkar and M. Haenggi, "Secrecy coverage," in *Proc. Asilomar Conf. Signals, Systems, and Computers (ACSSC)*, Pacific Grove, CA, Nov. 2010.
[14] 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.
[15] Y. Liang, H. V. Poor, and L. Ying, "Secrecy throughput of MANETs with malicious nodes," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Seoul, Korea, Jun. 2009, pp. 1189–1193.
[16] 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 (MobiHoc)*, Chicago, IL, Sep. 2010, pp. 21–30.
[17] 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.
[18] 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.
[19] 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.
[20] 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.
[21] 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.
[22] D. Stoyan, W. Kendall, and J. Mecke, *Stochastic Geometry and Its Applications*, 2nd ed. John Wiley and Sons, 1996.
[23] J. Venkataraman, M. Haenggi, and O. Collins, "Shot noise models for outage and throughput analyses in wireless ad hoc networks," in *Proc. IEEE Military Commun. Conf. (MILCOM)*, Washington, DC, Oct. 2006, pp. 1–7.
[24] F. Baccelli, B. Błaszczyszyn, and P. Mühlethaler, "An Aloha protocol for multihop mobile wireless networks," *IEEE Trans. Inform. Theory*, vol. 52, no. 2, pp. 421–436, Feb. 2006.
[25] M. Haenggi, "On distances in uniformly random networks," *IEEE Trans. Inf. Theory*, vol. 51, no. 10, pp. 3584–3586, Oct. 2005.
[26] R. K. Ganti and M. Haenggi, "Single-hop connectivity in interference-limited hybrid wireless networks," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Nice, France, Jun. 2007, pp. 366–370.
[27] X. Zhou, R. K. Ganti, J. G. Andrews, and A. Hjørungnes, "On the throughput cost of physical layer security in decentralized wireless networks," *IEEE Trans. Wireless Commun.*