Ad Hoc Networks 21 (2014) 123–133

Contents lists available at ScienceDirect

Ad Hoc Networks

journal homepage: www.elsevier.com/locate/adhoc

Secrecy transmission capacity in noisy wireless ad hoc networks

Jinxiao Zhu [a,b,*], Yin Chen [a], Yulong Shen [b], Osamu Takahashi [a], Xiaohong Jiang [a], Norio Shiratori [c,d]

[a] *School of Systems Information Science, Future University Hakodate, Hakodate 041-8655, Japan*
[b] *State Key Laboratory of Integrated Services Networks (ISN), Xidian University, Xi'an 710071, PR China*
[c] *GITS, Waseda University, Tokyo 169-0051, Japan*
[d] *RIEC, Tohoku University, Sendai-shi 980-8579, Japan*

ARTICLE INFO

Article history:
Received 20 December 2013
Received in revised form 22 March 2014
Accepted 18 May 2014
Available online 24 May 2014

Keywords:
Physical layer security
Transmission capacity
Wireless networks
Secrecy outage probability

ABSTRACT

This paper considers the transmission of confidential messages over noisy wireless ad hoc networks, where both background noise and interference from concurrent transmitters affect the received signals. For the random networks where the legitimate nodes and the eavesdroppers are distributed as Poisson point processes, we study the secrecy transmission capacity (STC), as well as the connection outage probability and secrecy outage probability, based on the physical layer security. We first consider the basic fixed transmission distance model, and establish a theoretical model of the STC. We then extend the above results to a more realistic random distance transmission model, namely nearest receiver transmission. Finally, extensive simulation and numerical results are provided to validate the efficiency of our theoretical results and illustrate how the STC is affected by noise, connection and secrecy outage probabilities, transmitter and eavesdropper densities, and other system parameters. Remarkably, our results reveal that a proper amount of noise is helpful to increase the secrecy transmission capacity.

1. Introduction

The inherent openness of wireless medium makes information security one of the most important and difficult problems in wireless networks. Traditionally, information security is ensured by applying cryptography which encrypts a plain message into a ciphertext that is computationally infeasible for any adversary without the key to break (decrypt). However, due to the improvement in computing technology and complication in cryptographic key management, there is an increasing concern that the cryptography no longer suffices, especially in sensitive applications requiring everlasting secrecy. Recently, the physical layer security has been widely demonstrated as a promising approach to providing everlasting secrecy. Unlike the traditional cryptography that ignores the difference between transmitting channels, the recent physical layer security achieves information-theoretic security by properly designing wiretap channel code according to the channel capacities [1,2] such that the original data can be hardly recovered by the eavesdropper regardless of how strong the eavesdropper's computing power is.

Considerable research efforts have been devoted to understand the performance of physical layer security. Wyner initially studied the maximum secret information rate, namely secrecy capacity, for a discrete memoryless wire-tap channel, where only three nodes are involved

* Corresponding author at: State Key Laboratory of Integrated Services Networks (ISN), Xidian University, Xi'an 710071, PR China. Tel.: +81 0138 34 6226.

E-mail addresses: jxzhu1986@gmail.com (J. Zhu), ychen1986@gmail.com (Y. Chen), ylshen@mail.xidian.edu.cn (Y. Shen), Osamu@fun.ac.jp (O. Takahashi), jiang@fun.ac.jp (X. Jiang), norio@shiratori.riec.tohoku.ac.jp (N. Shiratori).

http://dx.doi.org/10.1016/j.adhoc.2014.05.014
1570-8705/© 2014 Elsevier B.V. All rights reserved.

(one transmitter, one legitimate receiver and one eavesdropper), and showed the existence of channel codes to ensure the message is reliably delivered to the legitimate receiver while secured at the eavesdropper [1]. Wyner's work was then extended to other channel models, such as Gaussian wire-tap channel [2], fading wire-tap channel with or without channel correlations [3–6], broadcast channels with confidential messages [7]. Based on these pioneering works on the basic point-to-point wire-tap channels, many recent research efforts have been conducted to understand the performances of physical layer security in large-scale wireless networks, where lots of legitimate nodes and eavesdroppers are involved, in terms of secrecy throughput capacity [8–11], secrecy coverage [12], connectivity [13–16] and percolation phenomenon [10,17,18] under secrecy constraints, etc.

This paper focuses on the study of secrecy transmission capacity (STC) in large-scale wireless networks, which is defined as the achievable rate of successful transmission of confidential messages per unit area of a network, subject to constraints on both connection outage probability and secrecy outage probability. It is notable that the STC indicates the area spectral efficiency (ASE) of wireless networks under the given constraints on the levels of reliability and security, and hence it is of fundamental importance and can serve as a guideline for the design and development of wireless networks. Besides, compared with the aforementioned studies on the *secrecy throughput capacity* of large-scale wireless networks that only provide scaling law results [8–11], exact results can be obtained from STC study, which can lead to a finer optimization on network performance.

Some prior works on STC have been done by Zhou et al. in [19,20], where the authors calculated the secrecy transmission capacity for decentralized wireless networks with a fixed distance transmission scheme under the signal-to-interference ratio (SIR) model that neglects the impact of background noise. It is noticed that the background noise is a ubiquitous natural phenomenon and ignoring it may cause inaccuracy in the performance estimation. Moreover, it is also noticed that the additional noise on one hand is harmful to the reliability of a transmission since it makes the signal received at the intended receiver worse, on the other hand is helpful to the security performance since it makes the signal received at eavesdroppers worse. Hence, a natural question to ask is what is the overall impact of the noise on the STC. Accordingly, a new study is still required to investigate the exact STC in wireless networks under the impact of background noise.

In this work, we focus on the secrecy transmission capacity in noisy wireless ad hoc networks where interference from concurrent transmitters and background noise from natural and sometimes man-made sources affect the received signals. The main contributions of this paper are as follows.

- Based on the tools from stochastic geometry, we start the analysis from a basic fixed transmission distance scenario where each transmitter has an intended receiver at a fixed distance which is the same for all transmitters. We establish a general theoretical model of the STC, as well as the connection outage probability and secrecy outage probability, under the signal-to-interference-noise ratio (SINR) model. Furthermore, for the special scenario when the path-loss exponent $\alpha = 4$ and noise power is the same across space and time slots, we derive a closed-form STC and then propose a condition to achieve a positive STC.
- We then extend the analysis of STC to a more realistic random transmission scenario, nearest receiver transmission in particular, and present the corresponding connection outage probability and STC. It is noticed that the transmission distance has no impact on the secrecy outage probability.
- Finally, we provide extensive simulation and numerical results to validate the efficiency of our theoretical models and also to illustrate our theoretical findings. Remarkably, our results indicate that a proper amount of noise can be helpful to increase the secrecy transmission capacity.

The remainder of this paper is organized as follows. Section 2 presents the system model and performance metrics based on the physical layer security. In Section 3, we obtain analytical results on the secrecy transmission capacity for the fixed transmission distance scenario. Then, Section 4 extends the analysis to the nearest receiver transmission scenario. In Section 5, we validate the theoretical models by simulations and analyze the tradeoff between the system parameters. Finally, concluding remarks are given in Section 6.

2. System model and performance metrics

In this section, we introduce the basic system model of this paper and the performance metrics based on the physical layer security. The notation and symbols used throughout the paper are summarized in Table 1. Random variables are denoted by upper-case Roman letters throughout the paper, e.g., W, H and I.

2.1. System model

We consider an ad hoc wireless network consisting of both legitimate nodes and eavesdroppers over a two-dimensional Euclidean space $\mathbb{R}^2$. For each time snapshot, locations of legitimate nodes are modeled as a homogeneous Poisson point process (PPP) Φ with density λ, denoted by $\Phi = \{X_i\}$, where $X_i \in \mathbb{R}^2$ is the location of the legitimate node i, and locations of eavesdroppers are modeled as a PPP Φ_e with density λ_e, denoted by $\Phi_e = \{X_e\}$, where $X_e \in \mathbb{R}^2$ is the location of the eavesdropper node e. The PPP model for node locations is suitable when the nodes are independently and uniformly distributed over the network area, which is often reasonable for networks with indiscriminate node placement or substantial mobility [21]. The slotted ALOHA is employed at legitimate nodes as the medium access control (MAC) protocol. That is, in each time slot, each legitimate node independently decides to transmit with probability p or act as a potential receiver otherwise. Hence, in each time slot, the set of all transmitters forms a PPP Φ_T with density $\lambda_T = p\lambda$ and the set of all receivers forms a PPP Φ_R with density $\lambda_R = (1-p)\lambda$. Notice that $\Phi = \Phi_T \cup \Phi_R$.

Table 1
Summary of notations.

Symbol	Meaning
Φ	Poisson point process (PPP) of legitimate node locations
Φ_e	PPP of eavesdropper locations
$\Phi_T,\ \Phi_R$	PPP of transmitter and receiver locations, resp.
$\lambda,\ \lambda_e$	Density of Φ and Φ_e, resp.
$\lambda_T,\ \lambda_R$	Density of Φ_T and Φ_R , resp. ($\lambda = \lambda_T + \lambda_R$)
$P_{co},\ P_{so}$	Connection and secrecy outage probabilities, resp.
$\sigma,\ \epsilon$	Constraints on connection and secrecy outage probabilities, resp.
$\beta_t,\ \beta_e$	SINR thresholds for legitimate nodes and eavesdroppers, resp.
$\mathcal{R}_t,\ \mathcal{R}_s$	Codewords rate and secrecy rate, resp.
$\mathcal{R}_e$	Rate loss for securing the message against eavesdropping
$W,\ w$	Random and fixed noise powers, resp.
$\alpha > 2$	Path loss exponent
H_{ij}	Power gain of the channel from node i to node j
X_i	Location of node i
$\|X_i\|$	Distance from node i to the origin
$\|X_{ij}\|$	Distance from node i to node j
$\mathbb{P}(\cdot)$	Probability operator
$\mathbb{E}(\cdot)$	Expectation operator

In this paper, all transmitters are assumed to transmit with the same transmission power ρ. We consider two different scenarios regarding to the transmission distance: (1) fixed transmission distance, i.e., the distances from the transmitters to their intended receivers have a common fixed value; (2) random transmission distance, i.e., the distances from the transmitters to their intended receivers are independent random variables. The signal propagation over the wireless medium is assumed to be affected by the large-scale path loss, the small-scale fading, an additional noise and interference from concurrent transmissions. The large-scale path loss is assumed to be $r^{-\alpha}$ over distance r, where $\alpha > 2$ is the path loss exponent.[1] For the small-scale fading, we assume the channel follows the Rayleigh fading with unit mean and the fading coefficient is independent from path to path. Hence, the signal power received at a receiver j from a transmitter i is given by $\rho H_{ij}|X_{ij}|^{-\alpha}$, where H_{ij} and $|X_{ij}|$ are the channel fading gain and the distance between the nodes i and j, respectively. For the additional noise,[2] we consider the scenario that noise powers (for any time slot) at different receivers are independent of each other, but they all follow a same probability distribution function (PDF), $f_W(w)$. The additional noise is also assumed to be independent of Φ. We will use the random variable W to denote the noise power in general, and use the random variable W_i to denote the noise power at node i. It is assumed that interference from concurrent transmissions is treated as noise at both the intended receivers and eavesdroppers. The detection performance is characterized by the signal-to-interference-noise ratio (SINR), i.e., the ratio of signal power over interference plus noise power.

Remark 1. Although the interference is treated as noise in this paper, the negative impact of interference can be partially alleviated by adopting some advanced techniques like interference alignment [23,24]. It is notable, however, that the analysis under interference alignment will be much more complex, since it not only requires global channel state information of channels from transmitters or interferers to receivers but also involves some complex cooperating transmission strategies.

2.2. Physical layer security and performance metrics

In the considered network, a transmitter wants to send confidential messages to its receiver hoping that the messages are reliably received by the receiver while secured against eavesdroppers. For the secure encoding schemes, we consider the physical layer security that implemented by the well-known Wyner code [1]. Specifically, the Wyner's encoding scheme requires a transmitter to choose two rates, namely, the codeword rate $\mathcal{R}_t$ and secrecy rate $\mathcal{R}_s$. It is noticed that $\mathcal{R}_s \leqslant \mathcal{R}_t$, and the rate difference between the two rates, denoted by $\mathcal{R}_e = \mathcal{R}_t - \mathcal{R}_s$, indicates the rate cost of securing message transmissions against eavesdropping. For any transmitted message, the receiver is able to decode it with an arbitrarily small error probability if $\mathcal{R}_t$ is *less* than the capacity of the channel from the transmitter to this receiver, while an eavesdropper is *not* expected to recover it correctly if $\mathcal{R}_e$ is *larger* than the capacity of the channel from the transmitter to this eavesdropper. In this work, we focus on the scenario that all transmitters choose the same pair of $\mathcal{R}_t$ and $\mathcal{R}_s$ (and thus $\mathcal{R}_e$), which is reasonable since the network is homogeneous. For more details about the Wyner's encoding scheme, please refer to [6,25].

Based on the above physical layer security method, the following three performance metrics are studied in this paper:

- *Connection outage probability (COP)*: We call connection outage happens when the SINR at the intended receiver is below a given threshold β_t. The connection outage probability, denoted by $P_{co}(\beta_t)$, is then defined as the probability that connection outage happens:

$$P_{co}(\beta_t) = \mathbb{P}\{\text{SINR at the target receiver is less than } \beta_t\}. \tag{1}$$

  It is noticed that $\mathcal{R}_t$ is related with β_t by $\beta_t = 2^{\mathcal{R}_t} - 1$.
- *Secrecy outage probability (SOP)*: We call secrecy outage happens when the SINR at one or more eavesdroppers is above a given threshold β_e. The secrecy outage probability, denoted by $P_{so}(\beta_e)$, is then defined as the probability that secrecy outage happens:

$$P_{so}(\beta_e) = 1 - \mathbb{P}\{\text{All eavesdropper SINRs are less than } \beta_e\}. \tag{2}$$

  It is noticed that $\mathcal{R}_e$ is related with β_e by $\beta_e = 2^{\mathcal{R}_e} - 1$.
- *Secrecy transmission capacity (STC)*: It is defined as the achievable rate of successful transmission of confidential messages per unit area, for a given connection outage probability $P_{co}(\beta_t) = \sigma$ and a given secrecy outage probability $P_{so}(\beta_e) = \epsilon$:

[1] Usually, the path loss exponent is in the range of 3–5 [22].

[2] The noise is a summation of unwanted or disturbing energy from natural and sometimes man-made sources, like industrial and aircraft noises.

$$\tau = (1-\sigma)\lambda_{\mathrm{T}}\mathcal{R}_s. \tag{3}$$

It is noticed that the secrecy rate $\mathcal{R}_s = \mathcal{R}_t - \mathcal{R}_e$ is a function of both σ and ϵ.

Notice that the COP gives a measure of the reliability level while the SOP gives a measure of the security level. The STC, which was first defined in [19], is a measure of spatial intensity of successful transmission rate of confidential messages under a reliability constraint and a secrecy constraint. It is noticed that while the analysis of this study mainly follows the framework of [19], the important issue of impact of noise on secrecy transmission capacity is carefully considered in this study.

3. First model: fixed transmission distance

In this section, we present the COP, SOP and STC under the basic fixed transmission distance assumption, i.e., each transmitter is assumed to have a prearranged intended receiver at a fixed distance l away. This assumption has been widely adopted in the literary of transmission capacity [21,26,27]. The extension to random distance will be given in Section 4.

To evaluate the COP, we will condition on a typical transmitter at the origin o of Cartesian coordinate system. It follows by Slivnyak's theorem [28] that the distribution of the point process Φ_{T} is unaffected by conditioning on an addition transmitter node at o. Therefore, the interference (and thus SINR) measured at the intended (typical) receiver of the typical transmitter under this conditional point process is the same as the one measured at any place under a homogeneous PPP with the density λ_{T}. By shifting the entire point process so that the intended (typical) receiver of the typical transmitter lies at the origin, we now analyze the SINR at this typical receiver.

The SINR at the typical receiver located at o is given by

$$\mathrm{SINR}_0 = \frac{\rho H_0 l^{-\alpha}}{W_0 + I_0}, \tag{4}$$

where W_0 and $I_0 = \Sigma_{k\in\Phi_{\mathrm{T}}}\rho H_{k0}|X_k|^{-\alpha}$ denote, respectively, the noise power and interference at the typical receiver, H_0 is the channel power gain between the typical transmitter and receiver, H_{k0} and $|X_k|$ are the channel power gain and the distance between the interferer at X_k and the typical receiver at o, respectively.

Based on the definition in Section 2.2, the COP can be derived by

$$P_{\mathrm{co}}(\beta_t) = \mathbb{P}(\mathrm{SINR}_0 < \beta_t) = 1 - \mathbb{P}(\mathrm{SINR}_0 \geqslant \beta_t). \tag{5}$$

For the exponential H_0 and random noise W, the success probability of transmission in an infinite planar network without eavesdroppers has been derived in [29]. Following the similar method as that of deriving the success probability, the COP can be given by

$$P_{\mathrm{co}}(\beta_t) = 1 - \exp\left[-\theta\left(\frac{\beta_t}{\rho}\right)^{\frac{2}{\alpha}} l^2\right]\mathcal{L}_W\left(\frac{\beta_t}{\rho}l^{\alpha}\right), \tag{6}$$

where $\theta = \pi\lambda_{\mathrm{T}}\Gamma(1-2/\alpha)\Gamma(1+2/\alpha)$, $\Gamma(\cdot)$ is the Gamma function and $\mathcal{L}_W(\cdot)$ is the Laplace transform of the random noise power W_0. It is noticed that the PDF of W_0 is the same as that of the general noise power W, which is given by $f_W(w)$. The derivation of (6) can be found in Appendix A.

We now shift the entire point process back so that the typical transmitter lies at the origin, and consider the SOP. Consider a transmission from the typical transmitter to an eavesdropper e, the received SINR at e is given by

$$\mathrm{SINR}_e = \frac{\rho H_e|X_e|^{-\alpha}}{\Sigma_{k\in\Phi_{\mathrm{T}}}\rho H_{ke}|X_{ke}|^{-\alpha} + W_e}, \tag{7}$$

where W_e is the noise power at the eavesdropper e, H_e and $|X_e|$ are the channel power gain and the distance between the typical transmitter and the eavesdropper e, respectively, H_{ke} and $|X_{ke}|$ are the channel power gain and the distance between the interferers k and e, respectively.

According to the definition in Section 2.2, secrecy outage happens if any one of eavesdroppers is able to recover the transmitted message. Let $E = \{e \in \Phi_e : \mathrm{SINR}_e > \beta_e\}$ be the set of eavesdroppers that can cause secrecy outage. Define an indicator function $1_E(e)$, which equals 1 if $e \in E$ and equals 0 otherwise. Then, $\prod_{e\in\Phi_e}(1 - 1_E(e))$ equals 1 if the transmission from the typical transmitter is secured against any eavesdropper. Hence, the SOP can be obtained by

$$\begin{aligned}P_{\mathrm{so}}(\beta_e) = 1 - \mathbb{E}_{\Phi_l}\left\{\mathbb{E}_{\Phi_e}\left\{\mathbb{E}_H\left\{\prod_{e\in\Phi_e}(1 - 1_E(e))\right\}\right\}\right\}\overset{(a)}{=}1\\ - \mathbb{E}_{\Phi_l}\left\{\mathbb{E}_{\Phi_e}\left\{\prod_{e\in\Phi_e}(1 - \mathbb{P}(\mathrm{SINR}_e \geqslant \beta_e|\Phi_e, \Phi_l))\right\}\right\},\end{aligned} \tag{8}$$

where (a) is due to the assumption that the fading coefficient is independent from path to path. Thus, the bounds of SOP can be derived in the following lemma.

Lemma 1. *For the concerned wireless network with network parameters λ_{T}, λ_e, W_e and α, and transmission power ρ defined above, its secrecy outage probability for a given eavesdroppers' SINR threshold β_e is upper bounded by*

$$P^u_{\mathrm{so}}(\beta_e) = 1 - \exp\left[-2\pi\lambda_e\int_0^\infty e^{-(\frac{\beta_e}{\rho})^{\frac{2}{\alpha}}\theta r^2}\mathcal{L}_W\left(\frac{\beta_e}{\rho}r^{\alpha}\right)r\mathrm{d}r\right], \tag{9}$$

and lower bounded by

$$P^l_{\mathrm{so}}(\beta_e) = 2\pi\lambda_e\int_0^\infty e^{-(\theta\left(\frac{\beta_e}{\rho}\right)^{\frac{2}{\alpha}}+\pi\lambda_e)r^2}\mathcal{L}_W\left(\frac{\beta_e}{\rho}r^{\alpha}\right)r\mathrm{d}r, \tag{10}$$

where $\theta = \pi\lambda_{\mathrm{T}}\Gamma(1-2/\alpha)\Gamma(1+2/\alpha)$ is the same as defined above.

Proof. Based on the secrecy outage formula in (8), we have

$$\begin{aligned}P_{\mathrm{so}}(\beta_e)&\overset{(b)}{=}1 - \mathbb{E}_{\Phi_l}\left\{\exp\left[-\lambda_e\int_{\mathbb{R}^2}\mathbb{P}(\mathrm{SINR}_e \geqslant \beta_e|\Phi_l)\mathrm{d}X_e\right]\right\}\\ &\overset{(c)}{\leqslant}1 - \exp\left[-\lambda_e\int_{\mathbb{R}^2}\mathbb{P}(\mathrm{SINR}_e \geqslant \beta_e)\mathrm{d}X_e\right]\\ &\overset{(d)}{=}1 - \exp\left[-2\pi\lambda_e\int_0^\infty\exp\left[-\theta\left(\frac{\beta_e}{\rho}\right)^{\frac{2}{\alpha}}r^2\right]\mathcal{L}_W\left(\frac{\beta_e}{\rho}r^{\alpha}\right)r\mathrm{d}r\right],\end{aligned} \tag{11}$$

where (b) follows by the probability generating functional of Φ_e, [3] (c) is based on Jensen's inequality, and (d) follows by converting Cartesian to Polar Coordinate and the tail distribution of H_e. It is noticed that the Laplace transforms of W_e and W are the same in this paper.

The lower bound of SOP is obtained by considering the success probability at the eavesdropper nearest to the transmitter. Denote the location of the nearest eavesdropper to the typical transmitter as X_{e_1} and denote their distance as r_e, i.e., $r_e = |X_{e_1}|$. The probability density function of r_e is given by

$$f_{R_e}(r_e) = 2\pi\lambda_e r_e \exp\left(-\pi\lambda_e r_e^2\right), \tag{12}$$

which is the probability that no eavesdropper existing within the disk $\mathcal{B}(o, r_e)$ centered at o with radius r_e. The lower bound of SOP can be given by

$$\begin{aligned} P_{\text{so}}(\beta_e) &\geqslant \mathbb{P}(\text{SINR}(X_{e_1}) \geqslant \beta_e) \\ &= \int_0^\infty \mathbb{P}(\text{SINR}(X_{e_1}) \geqslant \beta_e \| X_{e_1}| = r_e) f(r_e) \mathrm{d}r_e \\ &= \int_0^\infty \exp\left[-\theta\left(\frac{\beta_e}{\rho}\right)^{\frac{2}{\alpha}} r_e^2\right] \mathcal{L}_W\left(\frac{\beta_e}{\rho} r_e^\alpha\right) f(r_e) \mathrm{d}r_e. \end{aligned} \tag{13}$$

The lower bound in (10) follows by simplifying (13). □

From the definitions of COP and SOP, we have the following conclusion regarding to their monotonicity: The connection outage probability $P_{\text{co}}(\beta_t)$ increases with β_t, while the secrecy outage probability $P_{\text{so}}(\beta_e)$ decreases with β_e.

Given the connection outage constraint σ, the codeword rate can be given by

$$\mathcal{R}_t = \log\left(1 + P_{\text{co}}^{-1}(\sigma)\right), \tag{14}$$

where P_{co}^{-1} is the inverse function of P_{co} in (6).

Given the secrecy outage constraint ϵ, the data rate cost against eavesdroppers can be given by

$$\mathcal{R}_e = \log\left(1 + P_{\text{so}}^{-1}(\epsilon)\right), \tag{15}$$

where P_{so}^{-1} is the inverse function of P_{so} in (8).

The above inverse functions P_{co}^{-1} and P_{so}^{-1} exist because of the strict monotonicity of the COP and SOP. For a given distribution of W, P_{co}^{-1} can be numerically calculated based on (6), and bounds of P_{so}^{-1} can be numerically calculated based on the bounds in Lemma 1.

Based on the definition in Section 2.2, the STC can be derived in the following theorem.

Theorem 1. *The secrecy transmission capacity of the concerned wireless network with a connection outage constraint of σ and a secrecy outage constraint of ϵ is given by*

$$\tau = (1 - \sigma)\lambda_T[\mathcal{R}_t - \mathcal{R}_e]^+, \tag{16}$$

where $\mathcal{R}_t$ and $\mathcal{R}_e$ are given in (14) and (15), respectively. In particular, a lower bound of secrecy transmission capacity τ^l is derived when we use P_{so}^u in (9) to calculate $\mathcal{R}_e$, while an upper bound of secrecy transmission capacity τ^u is derived when we use P_{so}^l in (10) to calculate $\mathcal{R}_e$.

Proof. The STC can be directly derived by following the definition in Section 2.2. The potential problem is the existence of the inverse functions of P_{so}^u and P_{so}^l. We now show that P_{so}^u has the unique inverse function; the existence of inverse function of P_{so}^l can be proved in the similar way by showing that it is strictly monotonic. The derivative of P_{so}^u is given by

$$\begin{aligned} \frac{\mathrm{d}P_{\text{so}}^u(\beta_e)}{\mathrm{d}\beta_e} = &-2\pi\lambda_e \exp\left(-2\pi\lambda_e \int_0^\infty e^{-\left(\frac{\beta_e}{\rho}\right)^{\frac{2}{\alpha}}\theta r^2} \mathcal{L}_W\left(\frac{\beta_e}{\rho} r^\alpha\right) r\mathrm{d}r\right) \\ &\times \int_0^\infty \left[\frac{2\theta}{\alpha} \frac{\beta_e^{\frac{2}{\alpha}-1}}{\rho^{\frac{2}{\alpha}}} r^2 \mathcal{L}_W\left(\frac{\beta_e}{\rho} r^\alpha\right) \right. \\ &\left. + \frac{r^\alpha}{\rho} \int_0^\infty w e^{-\frac{\beta_e}{\rho} r^\alpha w} f_W(w)\mathrm{d}w\right] e^{-\left(\frac{\beta_e}{\rho}\right)^{\frac{2}{\alpha}}\theta r^2} r\mathrm{d}r, \end{aligned}$$

where $f_W(w)$ is the probability density function of the random noise W. The Laplace transform of W is given by

$$\mathcal{L}_W\left(\frac{\beta_e}{\rho} r^\alpha\right) = \int_0^\infty e^{-\frac{\beta_e}{\rho} r^\alpha w} f_W(w)\mathrm{d}w. \tag{17}$$

It is obvious that $\frac{\mathrm{d}P_{\text{so}}^u(\beta_e)}{\mathrm{d}\beta_e} < 0$, which proves that P_{so}^u has the unique inverse function. □

Notice that $P_{\text{so}}^u(\beta_e)$ derived in (9) will be shown to be very tight by simulation (see Figs. 3 and 4), and that other results derived based on the same bounding techniques have also been illustrated to be tight in [19,30]. Moreover, the lower bound of STC τ^l derived based on $P_{\text{so}}^u(\beta_e)$ gives a very tight approximation of the exact value of τ.

3.1. $W = w$ and $\alpha = 4$

We now consider the special scenario when the path-loss exponent $\alpha = 4$ and noise power W is a fixed value w across space and time slots, i.e., $W = w$, and derive the closed-form results. This special case allows the closed-form results to be derived, because under this case the complex integration involved in the calculation can be solved based on the identity function (22).

When the noise is a constant w, we can derive the COP and SOP by replacing $\mathcal{L}_W\left(\frac{\beta_t}{\rho} l^\alpha\right)$ by $\exp\left[-\frac{\beta_t}{\rho} w l^\alpha\right]$ into (6) and Lemma 1.

When the noise power is a constant w for each time slot and $\alpha = 4$, the COP is given by

$$P_{\text{co}}(\beta_t) = 1 - \exp\left[-w\frac{\beta_t}{\rho} l^4 - \vartheta l^2 \sqrt{\frac{\beta_t}{\rho}}\right], \tag{18}$$

where $\vartheta = \frac{\pi^2 \lambda_T}{2}$ is the value of θ at $\alpha = 4$. Therefore, for a connection outage constraint $P_{\text{co}}(\beta_t) = \sigma$, we have

$$\beta_t = P_{\text{co}}^{-1}(\sigma) = \rho\left(\frac{-\vartheta + \sqrt{\vartheta^2 + 4w\ln\frac{1}{1-\sigma}}}{2wl^2}\right)^2. \tag{19}$$

Corollary 1. *For the fixed noise w and $\alpha = 4$, the tight upper bound and lower bound of the secrecy outage probability are given by*

$$P_{\text{so}}^u(\beta_e) = 1 - \exp\left[-\frac{\pi^{\frac{3}{2}}\lambda_e}{2}\sqrt{\frac{\rho}{\beta_e w}} \exp\left(\frac{\vartheta^2}{4w}\right) \text{Erfc}\left(\frac{\vartheta}{2\sqrt{w}}\right)\right] \tag{20}$$

[3] For a point process ϕ, the probability generating functional is defined as $G_\phi(f) = \mathbb{E}\left[\prod_{x\in\phi} f(x)\right]$ for $0 < f(x) \leqslant 1$. If ϕ is a PPP with intensity function $\lambda(x)$, then $G_\phi(f) = \exp\left[-\int(1 - f(x))\lambda(x))\mathrm{d}x\right]$.

and

$$P^l_{\mathrm{so}}(\beta_e) = \frac{\pi^{\frac{3}{2}}\lambda_e}{2}\sqrt{\frac{\rho}{\beta_e w}}\exp\left[\frac{\left(\vartheta\sqrt{\frac{\beta_e}{\rho}}+\pi\lambda_e\right)^2}{4w\frac{\beta_e}{\rho}}\right]$$
$$\mathrm{Erfc}\left(\frac{\vartheta\sqrt{\frac{\beta_e}{\rho}}+\pi\lambda_e}{2\sqrt{w\frac{\beta_e}{\rho}}}\right), \tag{21}$$

where $\mathrm{Erfc}(z) = \frac{2}{\sqrt{\pi}}\int_z^\infty e^{-t^2}\mathrm{d}t$ *is the complementary error function.*

Proof. Replacing $\mathcal{L}_W\left(\frac{\beta_e}{\rho}r^\alpha\right)$ by $\exp\left[-\frac{\beta_e}{\rho}wr^\alpha\right]$ and $\alpha = 4$ into (9) and (10), we can derive the above results based on the following identity

$$\int_0^\infty e^{-at^4-bt^2}t\mathrm{d}t = \frac{\sqrt{\pi}}{4\sqrt{a}}\exp\left(\frac{b^2}{4a}\right)\mathrm{Erfc}\left(\frac{b}{2\sqrt{a}}\right). \quad \square \tag{22}$$

For a secrecy outage constraint $P^u_{\mathrm{so}}(\beta_e) = \epsilon$, we have

$$\beta_e = \frac{\rho}{w}\left[\frac{\pi^{\frac{3}{2}}\lambda_e\exp\left(\frac{\vartheta^2}{4w}\right)\mathrm{Erfc}\left(\frac{\vartheta}{2\sqrt{w}}\right)}{2\ln\frac{1}{1-\epsilon}}\right]^2, \tag{23}$$

which is an upper bound of the eavesdropper's decoding threshold under the secrecy constraint of ϵ.

Corollary 2. *For the fixed noise w and $\alpha = 4$, the tight lower bound of secrecy transmission capacity τ^l with a connection outage constraint of σ and a secrecy outage constraint of ϵ is given by*

$$\tau^l = (1-\sigma)\lambda_{\mathrm{T}}[\log(1+\beta_t) - \log(1+\beta_e)]^+, \tag{24}$$

where β_t and β_e are given in (19) and (23).

Corollary 3. *For the fixed noise w and $\alpha = 4$, the condition for a positive secrecy transmission capacity is given by*

$$\frac{\left(-\vartheta+\sqrt{\vartheta^2+4w\ln\frac{1}{1-\sigma}}\right)\ln\frac{1}{1-\epsilon}}{\pi^{\frac{3}{2}}l^2\lambda_e\sqrt{w}\exp\left(\frac{\vartheta^2}{4w}\right)\mathrm{Erfc}\left(\frac{\vartheta}{2\sqrt{w}}\right)} > 1. \tag{25}$$

4. Second model: Random transmission distance

In this section, we consider a more realistic transmission scenario of random transmission distance. In particular, we consider the nearest-receiver transmission (NRT) scheme.

Recall that Φ_{T} is the PPP of intensity λ_{T} of transmitters, and Φ_{R} is the PPP of intensity λ_{R} of potential receivers. We now consider the case that each transmitter adopts NRT, i.e., each transmitter transmits to its nearest receiver. For simplicity, we ignore the failures caused by the fact that multiple transmitters may select the same receiver [31,32].

Denoting the distance from the typical transmitter to its nearest receiver in Φ_{R} by R, the probability density function of R is given by

$$f_R(r) = 2\pi\lambda_{\mathrm{R}}r\exp(-\pi\lambda_{\mathrm{R}}r^2). \tag{26}$$

It is noticed that the transmission distance affects the COP, while it has no impact on the SOP.

Lemma 2. *For the concerned wireless network with network parameters λ_{T}, λ_{R}, W and α, and transmission power ρ defined above, its connection outage probability under NRT for a given β_t is determined by*

$$P_{co,n}(\beta_t) = 1 - 2\pi\lambda_{\mathrm{R}}$$
$$\times\int_0^\infty e^{-\left[\theta\left(\frac{\beta_t}{\rho}\right)^{\frac{2}{\alpha}}+\pi\lambda_{\mathrm{R}}\right]r^2}\mathcal{L}_W\left(\frac{\beta_t}{\rho}r^\alpha\right)r\mathrm{d}r, \tag{27}$$

where $\theta = \pi\lambda_{\mathrm{T}}\Gamma(1-2/\alpha)\Gamma(1+2/\alpha)$ is given in Lemma 1.

Proof. $P_{\mathrm{co,n}}(\beta_t)$ can be derived based on the following formula,

$$P_{\mathrm{co,n}}(\beta_t) = \int_0^\infty P_{\mathrm{co}}(\beta_t)f_R(r)\mathrm{d}r, \tag{28}$$

where $P_{\mathrm{co}}(\beta_t)$ is the COP for a fixed transmission distance derived in Section 3. $\square$

The STC for the nearest receiver transmission can be given as follows.

Theorem 2. *The secrecy transmission capacity under the nearest receiver transmission (NRT) with a connection outage constraint of σ and a secrecy outage constraint of ϵ is given by*

$$\tau_{\mathrm{n}} = (1-\sigma)\lambda_{\mathrm{T}}[\mathcal{R}_t - \mathcal{R}_e]^+, \tag{29}$$

where $\mathcal{R}_t = \log\left(1+P^{-1}_{co,n}(\sigma)\right)$ and $\mathcal{R}_e$ is given in (15). In particular, a lower bound of secrecy transmission capacity τ^l_n is derived when we use P^u_{so} in (9) to calculate $\mathcal{R}_e$, while an upper bound of secrecy transmission capacity τ^u_{n} is derived when we use P^l_{so} in (10) to calculate $\mathcal{R}_e$.

Proof. The STC can be directly derived by following the definition in Section 2.2. The potential problem is the existence of the inverse function $P^{-1}_{\mathrm{co,n}}$. The derivative of $P_{\mathrm{co,n}}$ is given by

$$\frac{\mathrm{d}P_{\mathrm{co,n}}(\beta_t)}{\mathrm{d}\beta_t} = 2\pi\lambda_{\mathrm{R}}\int_0^\infty e^{-\left[\theta\left(\frac{\beta_t}{\rho}\right)^{\frac{2}{\alpha}}+\pi\lambda_{\mathrm{R}}\right]r^2}\left[\frac{2\theta}{\alpha}\frac{\beta_t^{\frac{2}{\alpha}-1}}{\rho^{\frac{2}{\alpha}}}r^2\mathcal{L}_W\left(\frac{\beta_t}{\rho}r^\alpha\right)\right.$$
$$\left.+\frac{r^\alpha}{\rho}\int_0^\infty we^{-\frac{\beta_t}{\rho}r^\alpha w}f_W(w)\mathrm{d}w\right]r\mathrm{d}r, \tag{30}$$

where $f_W(w)$ is the probability density function of the random noise W. It is obvious that $\frac{\mathrm{d}P_{\mathrm{co,n}}(\beta_t)}{\mathrm{d}\beta_t} > 0$, which proves that $P_{\mathrm{co,n}}$ has the unique inverse function $P^{-1}_{\mathrm{co,n}}$. $\square$

4.1. Differences between this study and [19]

In this study, our analysis mainly follows the framework of [19] on secrecy transmission capacity study. The main differences between these two studies are as follows.

- Both noise and interference issues are considered in our analysis, while only the interference issue is considered in [19]. With the consideration of the noise issue, the integrals involved in the calculations of COP and SOP become much more complicated, which prevents us from deriving closed-form results for them and thus the final STC.

- This work includes a new transmission power parameter in the theoretical analysis of STC, which helps us to explore how STC varies with the transmission power.
- In addition to the fixed transmission distance model considered in [19], this work further explores the STC performance under the NRT model.

5. Numeric analysis and discussion

In this section, we first verify the efficiency of the theoretical models of connection outage probability and secrecy outage probability through simulation, and then explore the inherent tradeoffs among different system parameters.

5.1. Model validation

We developed a simulator, which is now available at [33], to simulate the message transmission process under the system model defined in Section 2.1. To model the large-scale network, the network size was set to 100×100 for $\lambda_T \geqslant 10^{-3}$, and 300×300 for $10^{-4} \leqslant \lambda_T < 10^{-3}$ [34]. The performance of the network is considered on an additional transmitter located at the center of the network, called as the typical transmitter. Specifically, we considered the COP and SOP of the typical transmitter. It is noticed that the efficiency of the STC relies on the efficiencies of the COP and SOP.

To validate the COP, we considered networks with $\alpha = 4,\ \rho = 1,\ \beta_t = 0.5$ and several different settings of transmitter density (i.e., $\lambda_T = \{0.1, 0.01, 0.001\}$) in Figs. 1 and 2. In particular, Fig. 1 validates the COP for the fixed transmission distance of $l = 1$, and Fig. 2 validates the COP for the nearest receiver transmission. It can be observed from Figs. 1 and 2 that the simulation results match the theoretical ones very well, which validates the efficiencies of our theoretical models of COP for both of the fixed and random transmission distances. In Figs. 1 and 2, the solid lines show the previous result of COP for interference-limited networks in [19]. It is obvious that the previous result is very loose for network scenarios where noise cannot be neglected.

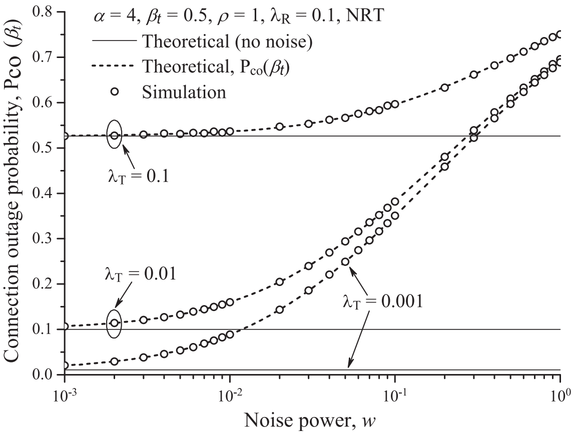


Fig. 2. Connection outage probability P_{co} vs. noise power w for the random transmission distance of NRT.

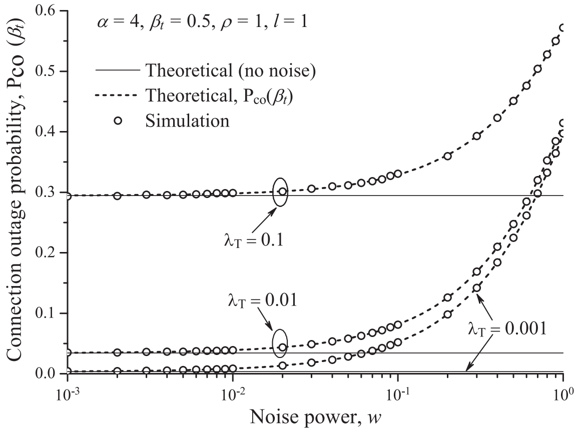


Fig. 1. Connection outage probability vs. noise power w for the fixed transmission distance of $l = 1$.

To validate the SOP, we considered networks with $\alpha = 4,\ \rho = 1,\ \beta_e = 0.1$ and eavesdropper density $\lambda_e = 0.001$ in Figs. 3 and 4. In particular, Fig. 3 validates the SOP for a transmitter density of $\lambda_T = 0.01$ and different settings of noise power, and Fig. 4 validates the SOP for a noise power of $w = 0.001$ and different settings of transmitter density. The results in Figs. 3 and 4 indicate that the upper and lower bounds of SOP derived in this paper are tight, and that the upper bound is very close to the simulated SOP. In Figs. 3 and 4, the solid lines show the previous upper bound of SOP for interference-limited networks in [19]. It is obvious that the previous upper bound is very loose for network scenarios where noise cannot be neglected.

5.2. Outage performances vs. noise and interference

We now explore the impacts of noise and interference on the COP. We can see from Figs. 1 and 2 that the connection outage probability P_{co} increases with the noise power

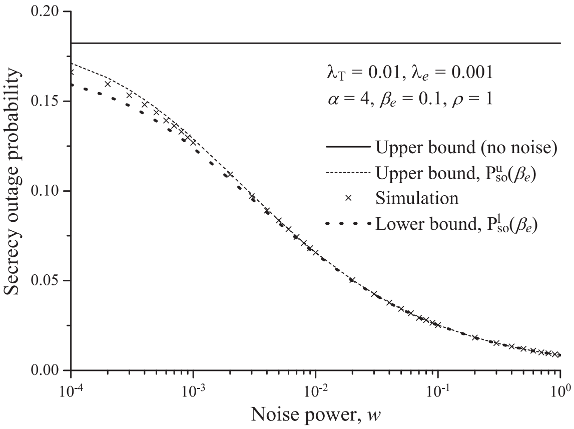


Fig. 3. Secrecy outage probability vs. noise power w.

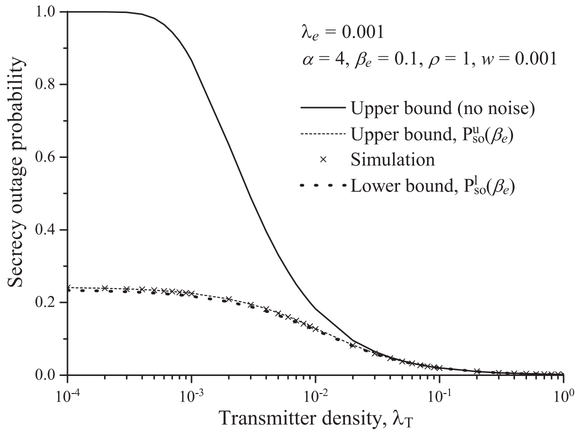


Fig. 4. Secrecy outage probability vs. transmitter density λ_T.

w, which indicates that noise deteriorates the reliability performance in the sense that the legitimate receiver cannot recover messages successfully. For a given w, we can also observe from Figs. 1 and 2 that P_{co} becomes greater for a larger transmitter density λ_T. This indicates that interference also deteriorates the reliability performance.

To illustrate the impacts of noise and interference on the SOP, we summarize in Fig. 3 how the secrecy outage probability P_{so} varies with w, and summarize in Fig. 4 how P_{so} varies with λ_T. We can see from Figs. 3 and 4 that P_{so} decreases with either w or λ_T, which indicates that both noise and interference help the security performance in the sense that eavesdroppers cannot recover messages successfully.

5.3. Secrecy transmission capacity vs. noise and interference

To further explore the impacts of noise and interference on the STC, we show in Fig. 5 how the (lower bound of) secrecy transmission capacity τ^l varies with w, and summarize in Fig. 6 how τ^l varies with λ_T. It can be observed from Fig. 5 that τ^l first increases with w and then decreases with w. It is noticed that the overall impact of noise on τ^l composes both impacts of noise on P_{co} and P_{so}. The above phenomenon is due to that the helpful impact of noise on P_{so} dominates the overall impact of noise on τ^l at first, and the harmful impact of noise on P_{co} dominates the overall impact of noise on τ^l after the optimum w. Therefore, it is suggested to add some artificial noise to achieve a larger STC for some occasions [35]. The artificial noise can be generated in many different ways, two of them are: (1) generate noise in the null space of the receiver's channel by one of the transmitter's antennas if it has multiple antennas, such that the noise can degrade the eavesdropper's channel without affecting the channel of the intended receiver [35]; (2) produce noise by potential receiver nodes. From Fig. 6, we also find that τ^l first increases with λ_T and then decreases with λ_T. The reason for such a phenomenon is similar as the one for the impact of noise.

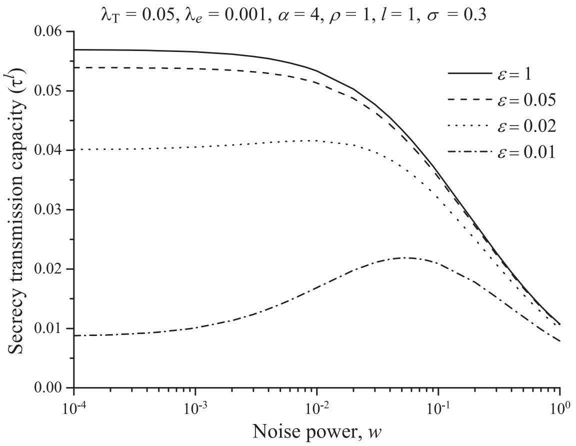


Fig. 5. Secrecy transmission capacity (τ^l) vs. noise power w.

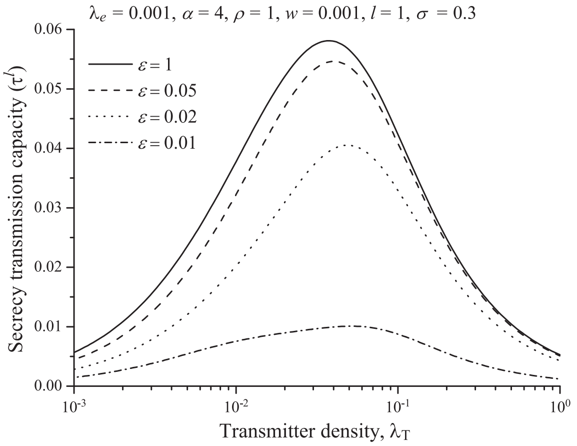


Fig. 6. Secrecy transmission capacity (τ^l) vs. transmitter density λ_T.

Notice that, although the lower bound of secrecy transmission capacity τ^l is adopted in Figs. 5 and 6, we can get the same conclusions about the impacts of noise and interference on the exact secrecy transmission capacity, since τ^l is very close to τ. We show in Fig. 7 how the gap between the upper and lower bounds of secrecy transmission capacity, $\tau^u - \tau^l$, changes with w under the same settings of the

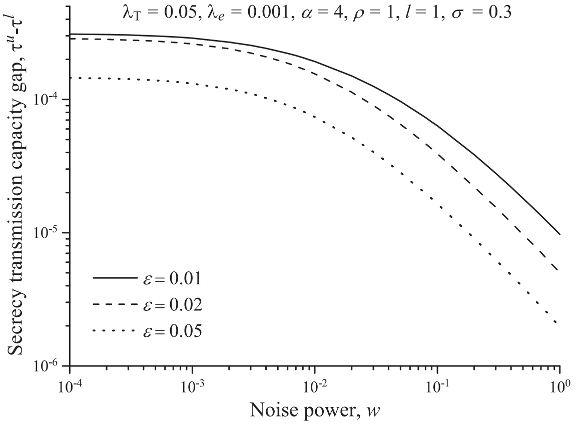


Fig. 7. Gap between the upper and lower bounds of secrecy transmission capacity ($\tau^u - \tau^l$) vs. noise power w.

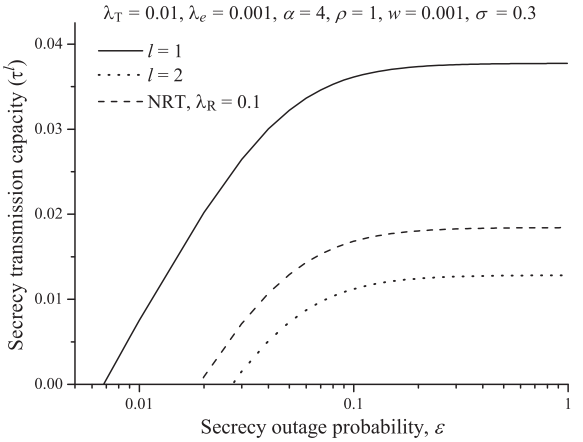


Fig. 8. Secrecy transmission capacity (τ^l) vs. secrecy outage constraint ϵ.

system parameters as that in Fig. 5. A careful observation of Fig. 7 shows that these gaps are very small and decrease quickly with w. For example, the largest gap value in Fig. 7 (i.e., when $\epsilon = 0.01$ and $w = 10^{-4}$) is within 3.6% of τ^l.

5.4. Impacts of secrecy on secrecy transmission capacity

To understand the impact of secrecy on STC, we show in Fig. 8 how τ^l varies with the secrecy outage constraint $P_{so}(\beta_e) = \epsilon$ for the scenarios of $\lambda_T = 0.01$, $\lambda_e = 0.001$, $\alpha = 4, \rho = 1$ and different transmission schemes (i.e., fixed distance of $l = 1, 2$ or NRT of $\lambda_R = 0.1$). Fig. 8 shows that τ^l increases with ϵ sharply when ϵ is small while increases with ϵ slowly when ϵ is large. For example, there is an over 85% increment in τ^l by relaxing the secrecy constraint from $\epsilon = 0.02$ to $\epsilon = 0.1$ for NRT with $\lambda_R = 0.1$, but only less than 15% increment from $\epsilon = 0.1$ to $\epsilon = 1$. This indicates that the performance of STC can be improved a lot by allowing small probability of secrecy outage. A careful observation of Fig. 8 shows that τ^l almost increases exponentially with ϵ when ϵ is small, e.g., $\epsilon < 0.1$. However, a positive τ^l cannot be achieved if an over-restrictive security constraint is required, e.g., $\epsilon < 0.01$ for the NRT scheme in Fig. 8. This is because it is very hard to achieve a positive secrecy rate under which a very small probability of secrecy outages against all eavesdroppers can be ensured. Furthermore, it is noticed that the impact of secrecy on STC is the same for fixed or random distance transmissions.

6. Conclusion

6.1. Summary of the paper

This paper studied the secrecy transmission capacity in noisy wireless ad hoc networks, where both background noise and interference from concurrent transmitters affect the received signals, which cover the previous result of secrecy transmission capacity in interference-limited networks as a special case [19]. Based on the tools from stochastic geometry, we first focused on a basic scenario where the transmission distances are assumed to be the same for all the transmitters, and derived the exact connection outage probability, and bounds of secrecy outage probability and secrecy transmission capacity. We then extended our analysis to a more realistic transmission scenario where each transmitter transmits to its nearest receiver. The simulation has also been conducted to verify the efficiency of our theoretical results. It is notable that the upper bound of secrecy outage probability or lower bound of secrecy transmission capacity has been shown very tight. Remarkably, we found that there exists an optimum noise level, at which the optimum secrecy transmission capacity can be achieved.

6.2. Future work

In this paper, we analyzed the STC based on a basic network setting, where each node has one antenna, passive eavesdroppers are independent each other, all nodes follow a homogeneous Poisson distribution, etc. Therefore, one future direction is to consider nodes with multiple antennas, where different antennas cooperate to transmit signals and produce artificial noise [35]. In real networks, eavesdroppers may cooperate with each other to exchange and combine the information received by themselves [36], or they may generate modified packets to interfere message transmissions [9]. Hence, this work can be extended to consider these network scenarios. This work can be further improved by considering other inhomogeneous distributions of nodes, e.g., for networks where nodes are scheduled to transmit or nodes are either clustered or more regularly distributed [34]. Another promising future research direction is to explore the interference alignment to alleviate the negative impact of interference on signals received at intended receivers [24].

Appendix A. Derivation of Eq. (6)

The success probability of the transmission from the typical transmitter to the typical receiver can be derived as

$$\begin{aligned}\mathbb{P}(\mathrm{SINR}_0 \geqslant \beta_t) \\ &= \mathbb{P}\left(H_0 \geqslant (W_0 + I_0)\frac{\beta_t}{\rho} l^\alpha\right) \overset{(a)}{=} \mathbb{E}\left(e^{-(W_0+I_0)\frac{\beta_t}{\rho}l^\alpha}\right) \\ &= \mathbb{E}_{W_0}\left(e^{-W_0\frac{\beta_t}{\rho}l^\alpha}\right)\mathbb{E}_{I_0}\left(e^{-I_0\frac{\beta_t}{\rho}l^\alpha}\right) \overset{(b)}{=} \\ &\quad \times \exp\left[-\theta\left(\frac{\beta_t}{\rho}\right)^{\frac{2}{\alpha}} l^2\right]\mathcal{L}_{W_0}\left(\frac{\beta_t}{\rho} l^\alpha\right) \\ &= \exp\left[-\theta\left(\frac{\beta_t}{\rho}\right)^{\frac{2}{\alpha}} l^2\right]\mathcal{L}_{W}\left(\frac{\beta_t}{\rho} l^\alpha\right),\end{aligned}$$

where (a) follows that H_0 is an exponential random variable and (b) is due to the Laplace transform of interference evaluated at $s = \frac{\beta_t}{\rho} l^\alpha$ (which can be found in many previous works, such as [29,34]). It is noticed that the Laplace transforms of W_0 and W are the same in this paper. Thus, the connection outage probability in (6) follows since $P_{co} = 1 - \mathbb{P}(\mathrm{SINR}_0 \geqslant \beta_t)$.

References

[1] A.D. Wyner, The wire-tap channel, Bell Syst. Tech. J. 54 (8) (1975) 1355–1387.

[2] S.K. Leung-Yan-Cheong, M.E. Hellman, The Gaussian wire-tap channel, IEEE Trans. Inf. Theory 24 (4) (1978) 451–456.

[3] M. Bloch, J. Barros, M.R.D. Rodrigues, S.W. McLaughlin, Wireless information-theoretic security, IEEE Trans. Inf. Theory 54 (6) (2008) 2515–2534.

[4] H. Jeon, N. Kim, J. Choi, H. Lee, J. Ha, Bounds on secrecy capacity over correlated ergodic fading channels at high SNR, IEEE Trans. Inf. Theory 57 (4) (2011) 1975–1983.

[5] J. Zhu, X. Jiang, O. Takahashi, N. Shiratori, Effects of channel correlation on outage secrecy capacity, J. Inform. Process. 21 (4) (2013) 640–649.

[6] J. Zhu, Y. Shen, X. Jiang, O. Takahashi, N. Shiratori, Secrecy capacity and outage performance of correlated fading wire-tap channel, IEICE Trans. Commun. E97-B (2) (2014) 396–407.

[7] I. Csiszár, J. Korner, Broadcast channels with confidential messages, IEEE Trans. Inf. Theory 24 (3) (1978) 339–348.

[8] O. Koyluoglu, C.E. Koksal, H.E. Gamal, On secrecy capacity scaling in wireless networks, IEEE Trans. Inf. Theory 58 (5) (2012) 3000–3015.

[9] Y. Liang, H.V. Poor, L. Ying, Secrecy throughput of MANETs under passive and active attacks, IEEE Trans. Inf. Theory 57 (10) (2011) 6692–6702.

[10] P.C. Pinto, M.Z. Win, Continuum percolation in the intrinsically secure communications graph, in: Int. Symp. Inf. Theory and its Applications (ISITA), 2010, pp. 349–354.

[11] S. Vasudevan, D. Goeckel, D.F. Towsley, Security-capacity trade-off in large wireless networks using keyless secrecy, in: ACM Int. Symp. Mobile Ad Hoc Networking and Computing (MobiHoc), Chicago, IL, 2010, pp. 21–30.

[12] A. Sarkar, M. Haenggi, Secrecy coverage, in: Asilomar Conf. Signals, Systems and Computers (ASILOMAR), 2010, pp. 42–46.

[13] M. Haenggi, The secrecy graph and some of its properties, in: IEEE Int. Symp. Information Theory (ISIT), 2008, pp. 539–543.

[14] P.C. Pinto, J. Barros, M.Z. Win, Secure communication in stochastic wireless networks-Part I: Connectivity, IEEE Trans. Inf. Forensics Secur. 7 (1) (2012) 125–138.

[15] S. Goel, V. Aggarwal, A. Yener, A.R. Calderbank, Modeling location uncertainty for eavesdroppers: a secrecy graph approach, in: IEEE Int. Symp. Information Theory (ISIT), 2010, pp. 2627–2631.

[16] X. Zhou, R.K. Ganti, J.G. Andrews, Secure wireless network connectivity with multi-antenna transmission, IEEE Trans. Wireless Commun. 10 (2) (2011) 425–430.

[17] A. Sarkar, M. Haenggi, Percolation in the secrecy graph: bounds on the critical probability and impact of power constraints, in: IEEE Inf. Theory Workshop (ITW), 2011, pp. 673–677.

[18] A. Sarkara, M. Haenggib, Percolation in the secrecy graph, Discrete Appl. Math. 161 (2013) 2120–2132.

[19] X. Zhou, R.K. Ganti, J.G. Andrews, A. Hjorungnes, On the throughput cost of physical layer security in decentralized wireless networks, IEEE Trans. Wireless Commun. 10 (8) (2011) 2764–2775.

[20] X. Zhou, M. Tao, R.A. Kennedy, Cooperative jamming for secrecy in decentralized wireless networks, in: IEEE International Conf. Commun. (ICC), 2012, pp. 2339–2344.

[21] S. Weber, J.G. Andrews, N. Jindal, An overview of the transmission capacity of wireless networks, IEEE Trans. Commun. 58 (12) (2010) 3593–3604.

[22] T.S. Rappaport, Wireless Communications: Principles and Practice, vol. 2, Prentice Hall PTR, New Jersey, 1996.

[23] S. Weber, J.G. Andrews, et al., Transmission capacity of wireless networks, Found. Trends Networking 5 (2-3) (2012) 109–281.

[24] O.O. Koyluoglu, H. El Gamal, L. Lai, H.V. Poor, Interference alignment for secrecy, IEEE Trans. Inf. Theory 57 (6) (2011) 3323–3332.

[25] X. Zhou, M. McKay, B. Maham, A. Hjorungnes, Rethinking the secrecy outage formulation: a secure transmission design perspective, IEEE Commun. Lett. 15 (3) (2011) 302–304.

[26] S.P. Weber, X. Yang, J.G. Andrews, G. De Veciana, Transmission capacity of wireless ad hoc networks with outage constraints, IEEE Trans. Inf. Theory 51 (12) (2005) 4091–4102.

[27] R.K. Ganti, J.G. Andrews, M. Haenggi, High-SIR transmission capacity of wireless networks with general fading and node distribution, IEEE Trans. Inform. Theory 57 (5) (2011) 3100–3116.

[28] D. Stoyan, W.S. Kendall, J. Mecke, Stochastic Geometry and its Applications, second ed., John Wiley & Sons, 1996.

[29] F. Baccelli, B. Blaszczyszyn, P. Muhlethaler, An Aloha protocol for multihop mobile wireless networks, IEEE Trans. Inf. Theory 52 (2) (2006) 421–436.

[30] R.K. Ganti, M. Haenggi, Single-hop connectivity in interference-limited hybrid wireless networks, in: IEEE Int. Symp. Information Theory (ISIT), 2007, pp. 366–370.

[31] S. Weber, J.G. Andrews, N. Jindal, The effect of fading, channel inversion, and threshold scheduling on ad hoc networks, IEEE Trans. Inf. Theory 53 (11) (2007) 4127–4149.

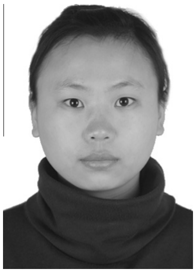
[32] F. Baccelli, B. Blaszczyszyn, Stochastic Geometry and Wireless Networks: Volume 1: THEORY, Now Publishers Inc., 2010.

[33] J. Zhu, A Java simulator for secrecy transmission in noisy wireless ad hoc networks, 2013 <https://www.researchgate.net/publication/259388923_A_java_simulator_for_secrecy_transmission_in_noisy_wireless_ad_hoc_networks>.

[34] M. Haenggi, R.K. Ganti, Interference in Large Wireless Networks, Now Publishers Inc., 2009.

[35] S. Goel, R. Negi, Guaranteeing secrecy using artificial noise, IEEE Trans. Wireless Commun. 7 (6) (2008) 2180–2189.

[36] P.C. Pinto, J. Barros, M.Z. Win, Wireless physical-layer security: the case of colluding eavesdroppers, in: IEEE Int. Symp. Information Theory (ISIT), 2009, pp. 2442–2446.



Jinxiao Zhu received the B.S. and M.E. degrees both in Software Engineering from Xidian University in 2008 and 2011, respectively. She is currently working towards a Ph.D. degree at the School of Systems Information Science at Future University Hakodate. Her research interests are in the areas of physical layer security of wireless communications, and performance modeling and evaluation of wireless networks.

Yin Chen received his B.S. and M.S. degrees both in Computer Science from Xidian University, China in 2008 and 2011, respectively. He is in the School of Systems Information Science at Future University Hakodate, Japan, where he is studying towards a Ph.D. degree. His scientific interests include stochastic geometry and queuing theory, with applications to performance analysis and optimization in Ad hoc networks and Mobile ad hoc networks.

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

Osamu Takahashi received his degree from Hokkaido University in 1975. He worked for NTT research laboratory and NTTDoCoMo research laboratory. He is currently a professor at the Department of System Information Science at Future University Hakodate. His research interest includes ad hoc networks, network security, and mobile computing. He is a fellow of IPSJ (Information Processing Society of Japan) and a member of IEEE and IEICE.

Xiaohong Jiang received his B.S., M.S. and Ph.D. degrees all from Xidian University, China. He is currently a full professor of Future University Hakodate, Japan. Dr.Jiang was an Associate professor of Tohoku University, Japan, from February 2005 to March 2010, an assistant professor in Japan Advanced Institute of Science and Technology (JAIST), from October 2001 to January 2005. Dr. Jiang was a JSPS research fellow at JAIST from October 1999 to October 2001. He was a research associate in the University of Edinburgh from March1999 to October 1999. Dr. Jiang's research interests include computer communications networks, mainly wireless networks, optical networks, etc. He has published over 200 technical papers at premium international journals and conferences, which include over 20 papers published in IEEE journals like IEEE/ACM Transactions on Networking, IEEE Journal of Selected Areas on Communications, etc. Dr. Jiang was the winner of the Best Paper Award and Outstanding Paper Award of IEEE WCNC 2012, IEEE WCNC 2008, IEEE ICC 2005-Optical Networking Symposium, and IEEE/IEICE HPSR 2002. He is a Senior Member of IEEE and a member of IEICE.

Norio Shiratori is currently an Emeritus and Research Professor at the RIEC (Research Institute of Electrical Communication), Tohoku University, Japan. He is also a board member of Future University of Hakodate and a Visiting Professor of Chuo University, Japan. He is a fellow of the IEEE (Institute of Electrical and Electronic Engineers), the IPSJ (Information Processing Society of Japan) and the IEICE (The Institute of Electronics, Information and Communication Engineers). He was the president of the IPSJ from 2009 to 2011. He has published more than 15 books and over 400 refereed papers in computer science and related fields. He was the recipient of the "IPSJ Memorial Prize Winning Paper Award" in 1985, the "Telecommunication Advancement Foundation Incorporation Award" in 1991, the "Best Paper Award of ICOIN-9" in 1994, the "IPSJ Best Paper Award" in 1997, and many others including the most recent "Outstanding Paper Award of UIC-07" in 2007.