Chapter 7

Energy-Secrecy Trade-offs for Wireless Communication

Ruolin Zhang

Additional information is available at the end of the chapter

http://dx.doi.org/10.5772/intechopen.69247

Abstract

This chapter investigates the secrecy-energy trade-offs for communication in wireless networks. It is shown that privacy requirements for applications such as image or video transmissions do not require perfect secrecy, and the level of privacy can be quantified using a Rate-Distortion metric. Using information theoretic analysis, the chapter formulates analytic secrecy trade-offs for various communication channel models. In particular we analyze the advantage of partial secrecy for the Gaussian and Rayleigh fading channel models and the MIMO channel. The impact of secrecy requirements and the inherent secrecy-energy-connectivity trade-offs are also analyzed for networks of wireless nodes.

Keywords: partial secrecy, physical layer security, information theoretic secrecy, one point to one point communication, network level communication

1. Introduction

The secrecy of wireless communication was studied from an information theoretic perspective, and equivocation rate was defined to characterize secrecy capacity. Equivocation rate measures the uncertainty that the eavesdropper decodes about the transmitted message with a certain rate during a transmission. Perfect secrecy can be achieved if the equivocation rate is equal to the transmitted rate. In this chapter, the notion of partial secrecy is introduced, for the scenario that perfect secrecy cannot be achieve. The reason for studying partial secrecy is based on the consideration about another key performance metric of communication systems, energy efficiency. The energy savings can be obtained when a partial secrecy requirement is enforced.

For many practical applications, such as voice and image transmission, a certain percentage of loss will be accepted, since decoded data is useless for the eavesdropper. The quality of the

source data reconstruction for those applications is typically characterized by the rate-distortion function. For example some certain scenarios will keep the eavesdropped message useless for the eavesdropper, such as some images for which all the key objects in the image have been transmitted with perfect secrecy, while the other objects and background in the image that are not important are transmitted without secrecy constrains.

To characterize the partial secrecy, the physical layer and application layer secrecy requirement was analyzed jointly. At the physical layer, the equivocation rate characterizes the uncertainty remaining at the eavesdropper after receiving the transmitted message. At the application layer, the application layer secrecy would be achieve if there is a close to no message which is decoded by the eavesdropper at application layer, and from the information theoretic view, the application layer secrecy is characterized by the rate-distortion function. The application lay metric is the rate-distortion function, and physical layer secrecy metrics is equivocation, which directly translates to the secrecy capacity.

In the remaining, the energy-secrecy trade-offs was studied for one point to one point communication, such as the Gaussian fading channels, MIMO channel and network level communication. In Section 2, the background was mentioned and in Section 3 system model was introduced, and in Sections 3 and 4 the partial secrecy in one point to one point communication and in network level communication has been studied. In Section 5, the further work is depicted.

2. Background

In the chapter, the work is based on the rich literature about information theoretic results for the secrecy capacity for various channel models. The perfect secrecy was in introduced and the wire-tap channel model was also first introduced in Ref. [1]. Later, the classic Gaussian wire-tap channel was introduced in Ref. [2], and the perfect secrecy capacity was first derived. The perfect secrecy capacity was analyzed for fading channels and multiple antennas, for example, in Refs. [3, 4]. An extension of the wire-tap channel model when a common message is transmitted was first proposed in Ref. [5], and it is known as the Broadcast Channel with Confidential Messages (BCC). In Ref. [5] capacity-equivocation region and the perfect secrecy capacity of the discrete memory-less BCC was characterized, while in Refs. [6–8] a more general channel model for the fading BCC was considered. Further results of the secrecy capacity of the BCC was studied [9–11].

Also more recently, multi-users extensions of the wiretap channel and broadcast channel have been investigated in Refs. [1, 12]. The multi-receivers wire-tap channel was considered, and its perfect secrecy capacity was derived for an arbitrary number of users in Refs. [13–15], and for two users in Ref. [16]. The perfect secrecy capacity of the Gaussian scalar multi-receivers wiretap channel, a degraded multi-receivers wiretap channel, was also derived in Refs. [17, 18]. Outage capacity analysis was also proposed for Gaussian MIMO channel in several papers in the literature, such as in Ref. [19].

About secrecy graph for network connectivity, based on a secrecy graph framework [20], earlier work in the literature has proposed network connectivity models, based on this eavesdropper worse than receiver channel condition, showing that network connectivity can be greatly affected by secrecy requirements, such as in Refs. [21, 22].

3. System model

Partial secrecy can be achieved when energy per bit cost need to be reduced, and thus for suitable applications the source may trade-off energy expenditure for secrecy rate. The common definition of secrecy capacity as the maximum rate at which the transmitted message can be transmitted with perfect secrecy was adopted. For this scenario this chapter considers that the initial stream of data can be split into private and non-private information sub-streams, but without imposing the condition that the non-private sub-stream needs to correctly decoded by the eavesdropper as in the previous work in Ref. [23]. R_0 and R_s was denoted as the transmission rate of the non-private sub-stream and the private sub-stream, respectively, with the total transmission rate being defined as $R_t = R_0 + R_s$.

In partial secrecy, the equivocation rate may be smaller than the transmission rate at physical layer. From information theoretic, transmission rate, R, is measured in bits per transmission, if R bits information are transmitted by the transmitter. Assume that a maximum transmission power P can be used by the transmitter, and that transmitter has limited battery energy. Hence a performance metric, the energy per bit, is considered in partial secrecy. Therefore, the new metric of partial secrecy is characterized by energy per bit, E_b. Although the actual transmission rate is related to the system bandwidth, energy per bit is beyond the scope of that discussion. To characterize the energy efficiency of the transmission, the average energy per bit consumption was defined as

$$E_b = \frac{P}{R}\left(Joules/bit\right), \tag{1}$$

where P is the average power transmission constraint, and R is the number of bits per transmission.

In partial secrecy, the minimum Distortion, D_{min}, is the new metric at the application layer. The new metric is measured the transmitted message, which can be guaranteed to achieve at the eavesdropper. Also, the minimum Distortion is related to the transmission rate, and it accurately represent the transmitted message. For illustration purposes, a very simple rate-distortion function was characterized the distortion in the source reconstruction of transmitted message at the eavesdropper is defined as the ratio between the secrecy rate and the total transmission rate. The minimum guaranteed distortion metric, D_{min}, was defined as the percentage of the source rate that achieves secrecy, and thus will not be available at the eavesdropper:

$$D = \frac{R_s}{R_t}. \tag{2}$$

4. Partial secrecy in one point to one point communication

In Gaussian fading channel model, the partial secrecy applied in two cases: the known full channel CSI (Channel Statement Information) and known partial channel CSI, in which only the main channel CSI is known and channel from source to eavesdropper is not known.

Assume that the block length is large enough such that coding over one block can achieve a small probability of error. The channel input-output relationship is given by

$$Y = h_1 X + W, Z = h_2 X + V, \tag{3}$$

where X is the channel input, and Y and Z are channel outputs at the legitimate receiver and eavesdropper, respectively. The channel gain coefficients h_1 and h_2 are proper complex random variables. We assume that hi is a stationary and ergodic random process. The noise processes W and V are zero-mean independent and identically distributed (i.i.d.) proper complex Gaussian random variables with variances μ^2 and σ^2, respectively. The input X is subject to the average power constraint P. This chapter assumes different noise power levels and different constant fading gain coefficients for the intended receiver and the eavesdropper. In the previous work [23], the ergodic partial secrecy capacity for this channel model is characterized as:

$$C_{ps}^{GuPS} = \begin{cases} \left(R_0, R_1\right) \\ R_0 \le \frac{1}{2}\log\left(1 + \frac{(1-\beta)P|h_1|^2}{\mu^2 + \beta P|h_1|^2}\right) \\ R_1 \le \frac{1}{2}\log\left(1 + \frac{\beta P|h_1|^2}{\mu^2}\right) - \frac{1}{2}\log\left(1 + \frac{\beta P|h_2|^2}{\sigma^2}\right) \\ R_s \ge R_1 \end{cases}. \tag{4}$$

where $1-\beta$ is the fraction of the total power allocated to the common message, and β is the fraction of the power budget that is allocated to the confidential message, which can be determined optimally [23], such as to maximize the partial secrecy capacity Eq. (4).

As in Ref. [23], given the power budget P, β can be optimized to achieve the secrecy-capacity boundary, under the observation that the secrecy-capacity region is convex:

$$\max_{\beta\in[0,1]}\left\{\gamma_0 R_0(\beta) + \gamma_1 R_1(\beta)\right\}, \tag{5}$$

$$\beta\left(\frac{\gamma_1}{\gamma_0}\right) = \min\left\{\left(\frac{\gamma_1}{\gamma_0}\left(\frac{\sigma^2}{P|h_2|^2} - \frac{\mu^2}{P|h_1|^2}\right) - \frac{\sigma^2}{P|h_2|^2}\right)^+, 1\right\} \tag{6}$$

For $\beta \in [0,1]$, the condition should be satisfied

$$\frac{\sigma^2}{\sigma^2 - \mu^2|h_2|^2/|h_1|^2} \le \frac{\gamma_1}{\gamma_0} \le \left(1 + \frac{\sigma^2}{P|h_2|^2}\right)\frac{P|h_1|^2|h_2|^2}{\sigma^2|h_1|^2 - \mu^2|h_2|^2} \tag{7}$$

The choice of the ratio γ_1/γ_0, characterizes the energy-secrecy trade-off, by influencing both the achievable R_s, as well as the achievable R_t.

For applications more sensitive to transmission delay constraints, the outage partial secrecy capacity was investigate, defined as the maximum transmission and secrecy rate that can be supported for a given outage probability constraint, under the assumption that both the transmitter and the receiver have perfect channel-state information for both the regular transmission, as well as for the eavesdropper channel. Here the assumption is that the transmitter will defer transmission for the states that are associated with outage, and hence incur transmission delay.

$\left(\breve{R}_0, \breve{R}_s\right)$ was used to represent a target rate pair. The non-private sub-stream is transmitted at the rate R_0, while the private sub-stream is transmitted at the rate R_s. If the target rate pair is not achieved, an outage is claimed. The outage probability was defined as

$$P_{out} = \Pr\left\{\left(\breve{R}_0, \breve{R}_s\right) \notin C_s\left(\bar{h}, p\left(\bar{h}\right)\right)\right\}, \tag{8}$$

where $C_s\left(\bar{h}, p\left(\bar{h}\right)\right)$ is the secrecy capacity region for the channel with fading state, $\bar{h} = \left(h_1, h_2\right)$, and $p\left(\bar{h}\right)$ is the transmission power used by the source node. The transmission power is adapted to the CSI. The outage probability is considered under a long-term average power constraint P, so we have

$$E\left[p\left(\bar{h}\right)\right] \le P \tag{9}$$

For this scenario, the Rayleigh-fading broadcast channel with confidential messages was considered. Therefore $|h_1|^2$ and $|h_2|^2$ are exponentially distributed with parameters δ_1 and δ_2, respectively.

From the partial secrecy capacity region Eq. (4) we have the following two conditions:

$$\begin{aligned} R_0 &< \log\left(\frac{1+\frac{p\left(\underline{h}\right)\left|h_1\right|^2}{\mu^2}}{1+\frac{\beta p\left(\underline{h}\right)\left|h_1\right|^2}{\mu^2}}\right), \\ R_s &< \log\left(\frac{1+\frac{\beta p\left(\underline{h}\right)\left|h_1\right|^2}{\mu^2}}{1+\frac{\beta p\left(\underline{h}\right)\left|h_2\right|^2}{\sigma^2}}\right). \end{aligned} \tag{10}$$

Rewriting these conditions to reflect the constraints on the link gain values, such that the required transmission rate (R_0) and secrecy rates (R_s) are achievable, we obtain

$$\frac{\mu^2\left(2^{R_0}-1\right)}{p(\underline{h})\left(1-\beta 2^{R_0}\right)} < |h_1|^2 \quad ,$$

$$|h_2|^2 < \frac{\sigma^2\left[\left(1+\frac{\beta p(\underline{h})|h_1|^2}{\mu^2}\right)2^{-R_s}-1\right]}{\beta p(\underline{h})}. \tag{11}$$

Hence, the outage probability can be computed as the probability that the above conditions hold,

$$\widehat{P}_{out} = 1-\int_{f(R_0)}^{\infty}\int_{0}^{f(R_s)}\frac{1}{\delta_1}e^{-\frac{|h_1|^2}{\delta_1}}\frac{1}{\delta_2}e^{-\frac{|h_2|^2}{\delta_2}}d|h_2|^2\,d|h_1|^2 = 1-\exp\left(-\frac{1}{\delta_1}\frac{\mu^2\left(2^{R_0}-1\right)}{p(\underline{h})\left(1-\beta 2^{-R_0}\right)}\right)$$

$$+\frac{\delta_2}{\delta_2+\frac{\sigma^2}{\mu^2}2^{-R_s}\delta_1}\exp\left(-\frac{\sigma^2\left(2^{-R_s}-1\right)}{\beta p(\underline{h})\delta_2}-\frac{\delta_2+\frac{\sigma^2}{\mu^2}2^{-R_s}\delta}{\delta_1\delta_2}\frac{\mu^2\left(2^{R_0}-1\right)}{p(\underline{h})\left(1-\beta 2^{-R_0}\right)}\right), \tag{12}$$

where $f\left(R_0\right)=\left[\mu^2\left(2^{R_0}-1\right)\right]/\left[p(\underline{h})\left(1-\beta 2^{R_0}\right)\right]$ and $f\left(R_s\right)=\sigma^2\left[\left(1+\beta p(\underline{h})|h_1|^2/\mu^2\right)2^{-R_s}-1\right]/\left[\beta p(\underline{h})\right]$.

Similar as the known full channel CSI case, the partial secrecy-capacity region for the guaranteed partial secrecy channel can be determined as:

$$C_{ps}^{GuPS} = \begin{cases} \left(R_0, R_1\right) \\ R_0 \le \frac{1}{2}\log\left(1+\frac{p_0|h_1|^2}{\mu^2+p_1|h_1|^2}\right) \\ R_1 \le \frac{1}{2}\log\left(1+\frac{p_1|h_1|^2}{\mu^2}\right)-\int_0^{|h_1|^2}\frac{1}{2}\log\left(1+\frac{p_1|h_2|^2}{\sigma^2}\right)f\left(|h_2|^2\right)d|h_2|^2 \\ R_s \ge R_1 \end{cases}, \tag{13}$$

where p_0 is the power allocated to the no-private message, and p_1 is the power allocated to the private message. This partial secrecy channel region relies on the assumption of large coherence intervals and ensures that when $h_2 < h_1$. And the transmitter is under the power constraint

$$E\left[P(|h_1|)^2\right] \le P. \tag{14}$$

For this scenario, the Rayleigh fading channel was considered. Therefore, in the Rayleigh fading channel, the partial secrecy capacity region could be changed to

$$C_{ps}^{GuPS} = \begin{cases} \left(R_0, R_1\right) \\ R_0 \le \frac{1}{2}\log\left(1+\frac{p_0\left|h_1\right|^2}{\mu^2+p_1\left|h_1\right|^2}\right) \\ R_1 \le \frac{1}{2}\log\left(1+\frac{p_1\left|h_1\right|^2}{\mu^2}\right)-\frac{1}{2}\log\left(1+\frac{p_1\left|h_1\right|^2}{\sigma^2}\right)\exp\left(-\frac{p_1\left|h_1\right|^2}{\delta_2}\right)+ \\ \exp\left(\frac{1}{\delta_2 p_1/\sigma^2}\right)\left[Ei\left(\frac{\left|h_1\right|^2}{\delta_2}+\frac{1}{\delta_2 p_1/\sigma^2}\right)-Ei\left(\frac{1}{\delta_2 p_1/\sigma^2}\right)\right] \\ R_s \ge R_1 \end{cases} \tag{15}$$

It is easy to check that the objective function is concave in p_1 and hence, by derivation approach for maxing R_s, we get the following optimality condition

$$\frac{\partial\left(\gamma_0 R_0\left(p_1\right)+\gamma_1 R_1\left(p_1\right)\right)}{\partial p_1} = \frac{\left|h_1\right|^2 \Pr\left(\left|h_2\right|^2 \le \left|h_1\right|^2\right)}{\mu^2+\left|h_1\right|^2 p_1} - \int_0^{|h_1|^2}\left(\frac{\left|h_2\right|^2}{\sigma^2+\left|h_2\right|^2 p_1}\right) f\left(\left|h_2\right|^2\right) d\left|h_2\right|^2 = 0 \tag{16}$$

$$p_0 = P - p_1.$$

For any main channel fading state is $\left|h_1\right|^2 \sim e^{x/\delta_1}/\delta_1$, and eavesdropper channel state is $\left|h_2\right|^2 \sim e^{x/\delta_2}/\delta_2$. The optimal transmit power level p_1 is determined from the above equation. If the obtained power level turns out to be negative, then the optimal value of p_1 is equal to 0.

In the Rayleigh fading channel, the condition can be rewrite as

$$\begin{aligned} &\left(\gamma_1-\gamma_0\right)\frac{\left|h_1\right|^2}{\mu^2+\left|h_1\right|^2 p_1} - \gamma_1 \exp\left(-\frac{\left|h_1\right|^2}{\delta_2}\right)\frac{\left|h_1\right|^2}{\sigma^2+\left|h_1\right|^2 p_1} - \gamma_1 \frac{\left(1-\exp\left(-\frac{\left|h_1\right|^2}{\delta_2}\right)\right)}{p_1} \\ &+\gamma_1 \frac{\exp\left(\frac{1}{\delta_2 p_1^2/\sigma^2}\right)}{\delta_2 p_1^2/\sigma^2}\left[Ei\left(\frac{1}{\delta_2 p_1/\sigma^2}\right)-Ei\left(\frac{\left|h_1\right|^2}{\delta_2}+\frac{1}{\delta_2 p_1/\sigma^2}\right)\right]=0 \\ &p_0 = P - p_1. \end{aligned} \tag{17}$$

If there is no positive solution to this equation for a particular, then we set $p_1 = 0$.

From the partial secrecy capacity region formula, the two conditions is abstained as following:

$$R_0 < \log\left(\frac{1+P|h_1|^2/\mu^2}{1+\beta P|h_1|^2/\mu^2}\right), R_s < \log\left(\frac{1+\beta P|h_1|^2/\mu^2}{1+\beta P|h_2|^2/\sigma^2}\right). \tag{18}$$

Rewriting these conditions to reflect the constraints on the link gains values such as given transmission rate (R_0) and secrecy rates (R_s) are achievable, we obtain:

$$\frac{\mu^2\left(2^{R_0}-1\right)}{P\left(1-\beta 2^{R_0}\right)} < |h_1|^2 \;, |h_2|^2 < \sigma^2\left[\left(1+\frac{\beta P|h_1|^2}{\mu^2}\right)2^{-R_s}-1\right]/\beta P \tag{19}$$

Hence, the outage probability could be computed as the probability that the above conditions Eq. (19) do not hold.

$$\begin{aligned} P_{out} &= 1-\int_{\frac{\mu^2\left(2^{R_0}-1\right)}{P\left(1-\beta 2^{R_0}\right)}}^{\infty}\int_0^{\frac{\sigma^2\left[\left(1+\frac{\beta P|h_1|^2}{\mu^2}\right)2^{-R_s}-1\right]}{\beta P}}\frac{1}{\delta_1}\exp\left(\frac{|h_1|^2}{\delta_1}\right)\frac{1}{\delta_2}\exp\left(\frac{|h_2|^2}{\delta_2}\right)d|h_1|^2\,d|h_2|^2 \\ &= 1-\exp\left(-\frac{1}{\delta_1}\frac{\mu^2\left(2^{R_0}-1\right)}{P\left(1-\beta 2^{R_0}\right)}\right)+\frac{\delta_2}{\delta_2+\frac{\sigma^2}{\mu^2}2^{-R_1}\delta_1}\exp\left(-\frac{\sigma^2\left(2^{-R_s}-1\right)}{\beta P\delta_2}-\frac{\delta_2+\frac{\sigma^2}{\mu^2}2^{-R_1}\delta_1}{\delta_1\delta_2}\frac{\mu^2\left(2^{R_0}-1\right)}{P\left(1-\beta 2^{R_0}\right)}\right). \end{aligned} \tag{20}$$

In order to determine the partial capacity region for the MIMO fading channels, this chapter start from the results derived in Ref. [24] for perfect secrecy he MIMO Gaussian broadcast channel with non-private and confidential message. It expands the analysis in Ref. [24] to account for the fading model presented in partial secrecy, and consider that the private sub-stream will be transmitted as a private message (with rate R_s) and the no-private sub-stream will have no secrecy constraints and only the constraint that it will be correctly received by the intended receiver. The non-private stream will be transmitted with rate R_0.

The partial secrecy capacity formula can be then be determined as:

$$C_{ps} = \bigcup_{\beta\in[0,1]}\left\{\begin{array}{c} R_0 \le \frac{1}{2}\log\left|\mathrm{I}_M+\frac{(1-\beta)\frac{P}{N}}{\mu^2+\beta\frac{P}{N}}\mathrm{H}_1\mathrm{H}_1^{H}\right| \\ R_1 \le \frac{1}{2}\log\left|\mathrm{I}_M+\frac{\beta P}{\mu^2 N}\mathrm{H}_1\mathrm{H}_1^{H}\right|-\frac{1}{2}\log\left|\mathrm{I}_M+\frac{\beta P}{\sigma^2 N}\mathrm{H}_2\mathrm{H}_2^{H}\right|, \\ R_s > R_1 \\ R_t = R_0+R_1 \end{array}\right. \tag{21}$$

where (·)H denotes the Hermitian transpose. In a full-rank system, Eq. (21) can be simplified by using singular value decomposition as

$$C_{ps} = \bigcup_{\beta_i \in [0,1]} \begin{cases} R_0 \le \frac{1}{2}\sum_{i=1}^{M} \log\left| \mathrm{I}_M + \frac{(1-\beta_i)\frac{P}{N}}{\mu^2 + \beta_i \frac{P}{N}} \lambda_i\left(\mathrm{H}_1 \mathrm{H}_1{}^H\right) \right| \\ R_1 \le \frac{1}{2}\sum_{i=1}^{M} \log\left| \mathrm{I}_M + \frac{\beta_i P}{\mu^2 N} \lambda_i\left(\mathrm{H}_1 \mathrm{H}_1{}^H\right) \right| - \frac{1}{2}\sum_{i=1}^{M} \log\left| \mathrm{I}_M + \frac{\beta_i P}{\sigma^2 N} \lambda_i\left(\mathrm{H}_2 \mathrm{H}_2{}^H\right) \right| \\ R_t = R_0 + R_1 \\ R_s = R_1 \end{cases}, \quad (22)$$

where $\lambda_i(\mathrm{H}_1\mathrm{H}_1{}^{\mathrm{H}})$ or $\lambda_i(\mathrm{H}_2\mathrm{H}_2{}^{\mathrm{H}})$ are the eigenvalues of $\mathrm{H}_1\mathrm{H}_1{}^{\mathrm{H}}$ and $\mathrm{H}_2\mathrm{H}_2{}^{\mathrm{H}}$. At the *i*th antennas, the power allocation is $(1-\beta_i)P$ for the non-private sub-stream, and the power allocation is $\beta_i P$ for the private sub-stream.

As in Eq. (22), given that the power budget P, β_i can be optimized to achieve the secrecy-capacity boundary, and under the observation that the secrecy-capacity region is convex, we have the optimization condition:

$$\max_{\beta \in (0,1)} \left\{ \gamma_0 R_0(\beta_i) + \gamma_1 R_s(\beta_i) \right\}. \quad (23)$$

By taking the derivative and setting it to 0 we get the optimal power allocation between the non-private and private sub-streams:

$$\beta_i = \frac{\gamma_1}{\gamma_0}\left(\frac{\sigma^2 N}{P\lambda_i\left(\mathrm{H}_2\mathrm{H}_2{}^H\right)} - \frac{\mu^2 N}{P\lambda_i\left(\mathrm{H}_1\mathrm{H}_1{}^H\right)} \right) - \frac{\sigma^2 N}{P\lambda_i\left(\mathrm{H}_2\mathrm{H}_2{}^H\right)}. \quad (24)$$

When there are stringent delay constraints, the transmitter cannot defer transmission and consequently, for some states of the channel, and outage may occur. Outage the event is defined as which the secrecy rate Rs is not contained in the partial secrecy capacity,

$$R_s \notin C_{ps}\left(\mathrm{H}_1, \mathrm{H}_2, P\right). \quad (25)$$

In case of an outage, the private sub-stream is not secured against eavesdropping. The probability of this event happening is referred to as the secrecy outage probability.

Formula (22) shows the partial secrecy capacity, as a function of the eigenvalues of matrix $\mathrm{H_k}\mathrm{H_k}{}^{\mathrm{H}}$, which are random variables. The joint probability density function (pdf.) of these eigenvalues, after being ordered according to their amplitude, has been shown in Ref. [19] to be

$$p_{order}(\lambda_{k1},\ldots,\lambda_{kM}) = K_{M,N}^{-1}\left(\prod_i \lambda_{ki}^{N-M}\right)\cdot\left(\prod_{i>j}(\lambda_{ki}-\lambda_{kj})^2\right)\exp(-\sum_i \lambda_{ki}) \quad (26)$$

where $K_{M,N}$ is a normalizing factor.

Using the pdf in Eq. (26), the secrecy outage probability could be derived as follows

$$\begin{aligned} P_S &= \Pr\left(\sum_{i=1}^{M}\left(\log_2\left(1+\frac{\beta P}{\mu^2 N}\lambda_i\left(\mathrm{H}_1\mathrm{H}_1{}^H\right)\right)-\log_2\left(1+\frac{\beta P}{\sigma^2 N}\lambda_i\left(\mathrm{H}_2\mathrm{H}_2{}^H\right)\right)\right)<R_s\right) \\ &= \Pr\left(\log_2\left(1+\frac{P}{\mu^2 N}\frac{1}{M}\sum_{i=0}^{M}\lambda_i\left(\mathrm{H}_1\mathrm{H}_1{}^H\right)\right)-\log_2\left(1+\frac{P}{\sigma^2 N}\frac{1}{M}\sum_{i=0}^{M}\lambda_i\left(\mathrm{H}_2\mathrm{H}_2{}^H\right)\right)<R_s\right) \\ &= \Pr\left(tr\left(\mathrm{H}_2\mathrm{H}_2{}^H\right)>\frac{1-2^{R_s}+M\frac{\beta_i P}{\mu^2 N}\mathrm{E}\left(\lambda_i\left(\mathrm{H}_1\mathrm{H}_1{}^H\right)\right)}{2^{R_s}\frac{\beta_i P}{MN\sigma^2}}\right) \\ &= 1-P\left[\frac{1-2^{R_s}+M\frac{\beta_i P}{\mu^2 N}\mathrm{E}\left(\lambda_i\left(\mathrm{H}_1\mathrm{H}_1{}^H\right)\right)}{2^{R_s}\frac{\beta_i P}{MN\sigma^2}}, MN\right] \end{aligned} \quad (27)$$

where tr(A) denotes the trace of A, and $\mathrm{E}\left(\lambda_1\left(\mathrm{H}_1\mathrm{H}_1{}^H\right)\right)=tr\left(H_1H_1^H\right)/M$ is the expectation of $\lambda_i\left(\mathrm{H}_1\mathrm{H}_1{}^H\right)$. P[*x*,*a*] is the normalized incomplete gamma function defined as

$$P[x,a]=\frac{1}{\Gamma(a)}\int_0^x u^{a-1}e^{-u}du,\ x\geq 0\ . \quad (28)$$

5. Partial secrecy in network level communication

In the wireless network, the partial secrecy-capacity region for transmission between nodes *i* and *j*, with eavesdropper e^* is given similarly as Eq. (4)

$$C_{ps}^{GuPS}=\bigcup_{\beta\in[0,1]}\begin{cases}(R_0,R_S):\\ R_0\leq\frac{1}{2}\log\left(1+\frac{(1-\beta)Ph(x_i,x_j)}{\mu^2+\beta Ph(x_i,x_j)}\right)\\ R_1\leq\frac{1}{2}\log\left(1+\frac{\beta Ph(x_i,x_j)}{\mu^2}\right)-\frac{1}{2}\log\left(1+\frac{\beta Ph(x_i,e*)}{\sigma^2}\right)\\ R_S\geq R_1\end{cases} \quad (29)$$

Similar as Eq. (4), μ^2 and σ^2 represent the channel noise levels at the receiver and eavesdropper, respectively. Also, P represents the transmission power, with a power fraction β which is power allocation fraction to the private stream.

The average link gain in Eq. (29) can be determined based on the distance between the receiving and the transmitting nodes:

$$h(x_i x_j) \approx \frac{1}{\|x_i - x_j\|^{\alpha}}, \tag{30}$$

where α is the amplitude loss exponent.

Then e^* is denoted the eavesdropper with the nearest to the transmitter i,

$$e^* = \arg\max_{e} Ph(x_i, e) \tag{31}$$

.

To better analyze the privacy requirements on the network connectivity, we define the distance ratio ξ, as the ratio of the distance between the transmitter and eavesdropper versus the transmitter and receiver, as

$$\xi = \frac{\|x_i - e^*\|}{\|x_i - x_j\|} = \frac{r}{R}, \tag{32}$$

R is the maximum distance for transmission achievable between transmitter and receiver at given rate and secrecy constraints. r is the minimum distance requirement between transmitter and eavesdropper.

Using Eqs. (29) and (30) in conjunction with Eq. (32), we rewrite the partial secrecy capacity as follows

$$C_{ps}^{GuPS} = \bigcup_{\beta\in[0,1]} \begin{cases} (R_0, R_s): \\ R_0 \le \frac{1}{2}\log\left(1 + \frac{(1-\beta(\xi))\frac{P}{R^{\alpha}}}{\mu^2 + \beta(\xi)\frac{P}{R^{\alpha}}}\right) \\ R_1 \le \frac{1}{2}\log\left(1 + \frac{\beta(\xi)\frac{P}{R^{\alpha}}}{\mu^2}\right) - \frac{1}{2}\log\left(1 + \frac{\beta(\xi)\frac{P}{(\xi R)^{\alpha}}}{\sigma^2}\right) \\ R_S \ge R_1 \end{cases}. \tag{33}$$

The legitimate nodes and potential eavesdroppers are randomly located in the space according to a Poisson Point Process. To capture Eq. (29), the distance between the transmitter to closest eavesdropper node is further than the distance from transmitter to the receiver, which is equivalent to a geometrical condition: $r \geq R$.

The distance was derived to meet the constraints about the transmission rate, energy and secrecy requirement, according to Eqs. (29) and (32). A family of graphs is characterize by the secrecy and rate requirement.

Let $\Pi = \{x_i\} \subset \Re^d$ denote the set of legitimate nodes, and $\Pi_E = \{e_i\} \subset \Re^d$ denote the set of eavesdroppers. We define the rate secrecy family of graphs $G = \{\Pi, \mathrm{E}\}_{(E_b, R_S)}$, characterized by energy per bit and secrecy rate requirements, as the graph with vertex set and edge set

$$E = \left\{ \vec{x_i x_j} : R_0 \geq \eta', R_s \geq \eta' D, R_0, R_s \in C_{ps} \right\} \tag{34}$$

where C_{ps} is the partial secrecy capacity of the link between the transmitter x_i and the receiver x_j, such as in Eqs. (29) and (30). η' is a threshold of the minimum required transmission rate for the communication link, and $\eta' D$ is a threshold is the required minimum secrecy rate for the communication links.

The condition of the edge in Eq. (34) can be rewrote as a geometrical relationship between the requirements for the distance from transmitter to receiver, and to the eavesdropper, as a function of distortion and energy per bit based on Eqs. (29) and (33), with $\eta = \eta'/2$:

$$E = \left\{ \overrightarrow{x_i x_j} : \begin{array}{c} R \leq \dfrac{r}{\left[\left(2^{\eta} - 1\right) \dfrac{\mu^2}{\eta E_b} r^{\alpha} + \dfrac{\mu^2}{\sigma^2} 2^{\eta} \beta(\xi) \right]^{1/\alpha}} \\ R \leq \dfrac{r}{\left[\left(2^{\eta D} - 1\right) \dfrac{\mu^2}{\beta(\xi) \eta E_b} r^{\alpha} + \dfrac{\mu^2}{\sigma^2} 2^{\eta D} \right]^{1/\alpha}} \end{array} \right\}. \tag{35}$$

Figure 1 shows the dependence of the achievable secrecy rate, the overall transmission rate, the non-private stream rate and the distortion at the eavesdropper, as functions of the distance ratio metric. Numerical results were obtained for $\alpha = 2$ and $\mu^2 = \sigma^2 = 1$. Unless otherwise specified, $R = 1$.

Figure 1 shows us that the highest transmission rate, yielding the most energy efficient transmission, is obtained for the case in which the eavesdropper is more further than the legitimate receiver, larger ξ. This case also related to perfect secrecy, but it will enforce more stricter constraints for the link availability at the network level. Hence it will negatively impact

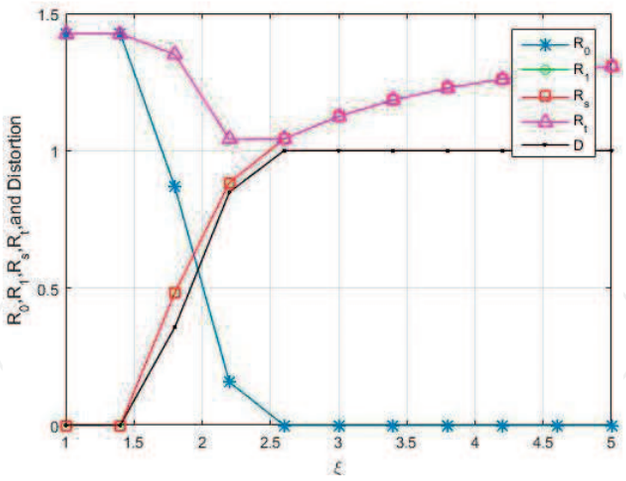

Figure 1. Secrecy-energy-connectivity trade-offs.

connectivity. If the eavesdropper is closer to the transmitter, the network connectivity is improved, while the higher energy expense is also much higher.

As in Ref. [20], the Poisson rate-secrecy graph is defined. In the Poisson rate-secrecy graph, Π, Π_E are mutually independent, homogeneous Poisson point processes with densities λ and λ_E, respectively, and consider $\lambda = 1$. But the rate-secrecy graphs are redefined by the transmission range and the distance ratio requirements by incorporate energy and secrecy constraints.

The edge condition in Eq. (35) is rewrite based on definition Eq. (34):

$$\xi \geq \left(\frac{\mu^2 2^{\eta D_{\min}} \beta(\xi) \eta E_b}{\sigma^2 \left(\beta(\xi) \eta E_b - R^\alpha \left(2^{\eta D_{\min}} - 1 \right) \right)} \right)^{1/\alpha} \geq \left(\frac{\mu^2 2^{\eta D_{\min}}}{\sigma^2 \left(1 - \frac{R^\alpha}{\eta E_b} \left(2^{\eta D_{\min}} - 1 \right) \right)} \right)^{1/\alpha}. \tag{36}$$

Eq. (37) shows that a rate-secrecy capacity feasibility condition can be obtained by requiring to be positive, and it is given by

$$R < \left(\frac{\beta \eta E_b}{\left(2^{\eta D_{\min}} - 1 \right) \mu^2} \right)^{1/\alpha} \leq \left(\frac{\eta E_b}{\left(2^{\eta D_{\min}} - 1 \right) \mu^2} \right)^{1/\alpha}. \tag{37}$$

The bounds in Eqs. (36) and (37) hold for $\beta \in [0,1]$.

Eq. (37) gives a bound on the maximum transmission range that can be achieved, given transmission rate, energy per bit consumption, and eavesdropper's distortion constraints. For a given transmission rate and distortion requirements, the range of transmission can be made infinitely large by allowing infinitely large transmission power, with the energy per bit consumption going to infinity.

From Eqs. (36) and (37), it shows that secrecy can be achieved when we impose a range and a distance ratio constraint. The connectivity of the network is analyzed by determining the out-degree distributions of the nodes, and the probability of out-isolation, and the average out-degree for an arbitrary node in the network are studied.

There are two cases, which are worth to study: (a) the range limited case – for which distance from transmitter and receiver, R, is limited to a maximum value; (b) the unlimited case - $R \to \infty$, which corresponds to the unlimited transmission power case.

For the range limited case, unlimited transmission power and no range transmission limit is imposed. To calculate the out-degree of a vertex, we follow a derivation similar to that in Eq. (35), where it replaces the condition $R < r$. The out-degree probability can be wrote as:

$$P\left[N_{out} = n\right] = \frac{\lambda_E \xi^2}{1+\lambda_E \xi^2}\left(\frac{1}{1+\lambda_E \xi^2}\right)^n. \tag{38}$$

The probability that the origin node cannot communicate with another node in $\vec{G}_{1,\lambda_E,\infty,\xi}$ (out-isolation) is then determined to be

$$P_{out-isolation} = P\left[N_{out} = 0\right] = \frac{\lambda_E \xi^2}{1+\lambda_E \xi^2}. \tag{39}$$

When a transmission power constraint is imposed, a maximum transmission range R can be determined as in Eq. (37).

As in Ref. [20], this thesis distinguishes two cases:

1. There is no eavesdropper inside a circle with radius $r = \xi R$. This case occurs with probability

$$P_0 = \exp\left(-\lambda_E \pi r^2\right) = \exp\left(-\lambda_E \pi \xi^2 R^2\right). \tag{40}$$

For this case, the number of good nodes inside the radius R is given by a Poisson distribution, with the mean, πR^2.

2. There is an eavesdropper at the distance, ρ. Then the number of good nodes is given by a Poisson distribution restricted to a radius $R' = \rho/\xi$, with the mean of $\pi R'^2 = \pi\rho^2/\xi^2$.

Averaging cases (1) and (2) and making the change of variable $r = \rho^2/\xi^2$, we obtain an out-degree probability expression similar to that in Ref. [20], but for an enhanced equivalent arrival rate for the eavesdropper, $\lambda_E^* = \lambda_E \xi^2$:

$$P\left[N_{out} = n\right] = \frac{\lambda_E^*\left(1 - \frac{\Gamma(n,a)}{\Gamma(n)}\right) + \exp(-a)\frac{a^n}{n!}}{(\lambda_E^* + 1)^{n+1}}, \tag{41}$$

in which a is $\pi R^2(\lambda^*_E + 1)$, and R is transmission range radius. Also, $\Gamma(.,.)$ is the upper incomplete gamma function.

Hence, the probability of out-isolation is derived as

$$P[N_{out} = 0] = \frac{\exp(-\pi R^2(\lambda^*_E + 1)) + \lambda^*_E}{1 + \lambda^*_E}. \tag{42}$$

The mean out-degree or in-degree can be determined to be

$$E[N^{out}] = E[N^{in}] = \frac{1}{\lambda^*_E}(1 - \exp(-\lambda^*_E \pi R^2)). \tag{43}$$

To achieve numerical results, we assume $\lambda = 1\ \mathrm{m}^{-2}$ and $\lambda_E = 0.08\ \mathrm{m}^{-2}$. **Figure 2** analyzes the out-degree probability on different secrecy level, D. The secrecy level is selected for perfect secrecy ($D = 1$) and for a value of distortion that gives a good level of privacy ($D = 0.6$). In **Figure 2**, the significant impact on network connectivity works when the secrecy constraint imposes. Note also that $\xi = 1$, which is the secrecy constraint imposed in Eq. (33), yields non-secrecy ($D = 0$), when transmission rate and energy constraints are also imposed.

In **Figure 3**, it shows the probability of out-isolation and the mean out degree distribution at the case of limited transmission range. When the secrecy level increases, the probability of out-isolation significantly increases. At the perfect secrecy situation, under transmission rate requirements, a minimum value of ξ, 2.5, is required (see **Figure 1**). And at the perfect secrecy, it leads to a 3.4 times increasing in the out-isolation probability and a 58% decreasing in the average mean

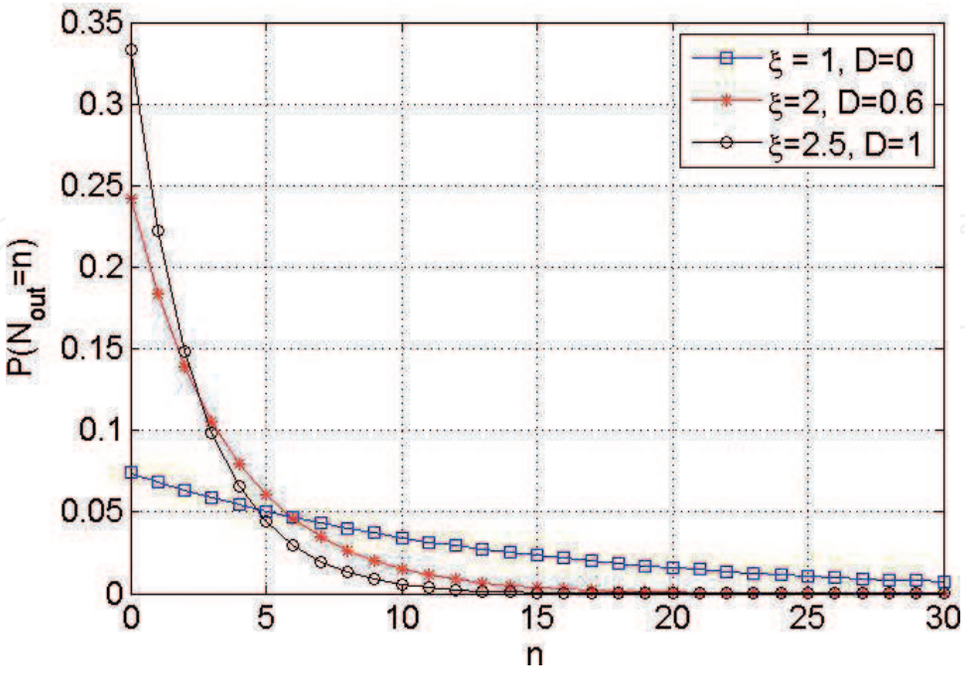

Figure 2. Out-degree probability—unlimited range scenario.

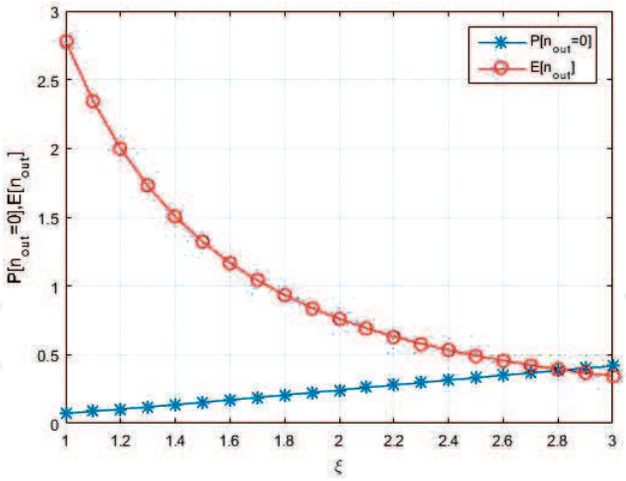

Figure 3. Out-isolation probability and mean out degree—limited range scenario.

degree, compared to the perfect secrecy studied in Ref. [20]. We also note that by relaxing the secrecy requirements, the out-isolation probability will reduce and the mean out-degree will improve. For example, choosing a distortion at the eavesdropper of $D = 0.6$ (obtained for $\xi = 2$), there is a 73% decreasing for the out-isolation probability and a 72% increasing in the mean out-degree, compared to the case of perfect secrecy (obtained for $\xi = 2.5$).

6. Further works

The partial secrecy could also applies in the multi-nodes communication, such as relay-eavesdropper channel. In the no relay case, the source and receiver cannot have secure communication when the eavesdropper's channel is the same or better than the receiver's channel holds. In the relay case, although the source and receiver cannot have secure communication, while they can achieve the partial secrecy. Assuming the nodes of eavesdropper is the randomly distributed in the area, the probability of achieving at least a secrecy level of medium secrecy level could be characterized based on the properties of the random distribution.

Also, for the network level, the partial secrecy could be studied in different distribution of nodes. For example, the case that users are uniformly distributed in area could be considered.

Author details

Ruolin Zhang

Address all correspondence to: rzhang2@stevens.edu

Stevens Institute of Technology, Hoboken, USA

References

[1] Wyner AD. The wire-tap channel. The Bell System Technical Journal. Oct. 1975;**54** (8):1355–1387

[2] Leung-Yan-Cheong SK and Hellman ME. The Gaussian wire-tap channel. IEEE Transactions on Information Theory. Jul. 1978;**24**(4):451–456

[3] Parada P and Blahut R. Secrecy capacity of SIMO and slow fading channels. In: Proceedings of the IEEE International Symposium on Information Theory (ISIT), pp. 2152–2155, Adelaide, Australia, September 2005

[4] Barros J and Rodrigues MRD. Secrecy capacity of wireless channels. In: Proc. IEEE International Symposium on Information Theory, Seattle, WA, USA, July 2006, pp. 356–360

[5] Csiszár I and Körner J. Broadcast channels with confidential messages. IEEE Transactions on Information Theory. May 1978;**24**(3):339–348

[6] Liang Y, Poor HV, and Shamai S. Secure communications over fading channels. IEEE Transactions on Information Theory. Jun. 2008;**54**(6):2470–2492

[7] Shamai S and Steiner A. A broadcast approach for a single-user slowly fading MIMO channel. IEEE Transactions on Information Theory. Oct. 2003;**49**(10):2617–2635

[8] Liang Y, Lai L, Poor HV, and Shamai S. The broadcast approach over fading Gaussian wiretap channels. In: Proc. IEEE Inform. Theory Workshop, Taormina, Italy; Oct. 2009. pp. 1–5

[9] Li L and Goldsmith AJ. Capacity and optimal resource allocation for fading broadcast channels-Part I: Ergodic capacity. IEEE Transactions on Information Theory. Mar. 2001;**47** (3):1083–1102

[10] Li L and Goldsmith AJ. Capacity and optimal resource allocation for fading broadcast channels-Part II: Outage capacity. IEEE Transactions on Information Theory. Mar. 2001;**47** (3):1103–1127

[11] Jain A, Gunduz D, Kulkarni SR, Poor HV, and Verdú S. Energy-distortion tradeoffs in Gaussian joint source-channel coding problems. IEEE Transactions on Information Theory. May 2012;**58**(5):3153–3168

[12] Leung-Yan-Cheong SK and Hellman ME. The Gaussian wiretap channel. IEEE Transactions on Information Theory. Jul. 1978;**IT-24**(4):451–456

[13] Csiszár I and Körner J. Broadcast channels with confidential messages. IEEE Transactions on Information Theory. May 1978;**IT-24**(3):339–348

[14] Ekrem E and Ulunkus S. Secrecy capacity of a class of broadcast channels with an eavesdropper. EURASIP Journal on Wireless Communications and Networking 2009. 2009: 824235, Aug. 2009

[15] Ekrem E and Ulukus S. "On secure broadcasting," presented at the. 42th Asilomar Conf. Signals, Syst. Comput., Pacific Grove, CA, USA, Oct. 2008

[16] Oggier F and Hassibi B. The secrecy capacity of the MIMO wiretap channel. IEEE Transactions on Information Theory. Aug. 2011;**57**(8):4961–4972

[17] Ekrem E and Ulukus S. The secrecy capacity region of the Gaussian MIMO multi-receiver wiretap channel. Submitted to IEEE Trans. Inf. Theory, Mar. 2009

[18] Ekrem E and Ulukus S. The effect of eavesdroppers on network connectivity: A secrecy graph approach. IEEE Transactions on Information Forensics and Security, 6(3):712–724, 2006

[19] Shen H and Ghrayeb A. Analysis of the outage probability for MIMO systems with receiver antenna selection. IEEE Transactions on Vehicular Technology. Jul. 2006;**55**: 1435–1440

[20] Haenggi M. The secrecy capacity region of the Gaussian MIMO multi-receiver wiretap channel. In: IEEE Trans. Inf. Theory; vol. 57, no. 4, pp. 2083–2114, Apr. 2011

[21] Goel S, Aggarwal V, Yener A, Calderbank AR. Modeling location uncertainty for eavesdroppers: A secrecy graph approach. In: Proc. IEEE International Symposium on Information Theory Proceedings (ISIT); 2010. pp. 2627–2631

[22] Goel S, Aggarwal V, Yener A, Calderbank AR. The effect of eavesdroppers on network connectivity: A secrecy graph approach. IEEE Transactions on Information Forensics and Security. 2006;**6**(3):712–724

[23] Comaniciu C, Poor HV. On energy-secrecy trade-offs for Gaussian wiretap channels. IEEE Transactions on Information Forensics and Security. 2013;**8**(2):314–323

[24] Ly HD, Liu T and Liang Y. Multiple-input multiple-output Gaussian broadcast channels with common and confidential message. IEEE Transactions on Information Theory. Nov 2010;**56**(11)