A Random Graph Model Approach for Analyzing Secrecy-Connectivity-Rate Tradeoffs in Wireless Networks

Journal:	*Transactions on Network Science and Engineering*
Manuscript ID	TNSE-2018-09-0278
Manuscript Types:	Regular Paper
Keywords:	information theoretic secrecy, random graph, partial secrecy, privacy, secrecy graph, physical layer security

A Random Graph Model Approach for Analyzing Secrecy-Connectivity-Rate Tradeoffs in Wireless Networks

Ruolin Zhang, and Cristina Comaniciu, *Member, IEEE*

Abstract— This paper presents a new approach for characterizing secrecy-connectivity-rate tradeoffs in wireless networks with eavesdropping nodes, by combining information theoretic metrics with a random connectivity graph model. Full connectivity constraints are determined and the secrecy-connectivity-rate tradeoffs are analyzed using a partial secrecy metric that characterizes the achievable level of privacy. It is shown that both full connectivity and a good level of privacy can be achieved for an appropriate power allocation between the common and private sub-streams for the data transmission, even for scenarios for which perfect secrecy is not achievable.

Index Terms—Information theoretic secrecy, random graph, partial secrecy, privacy, secrecy graph, physical layer security

1 Introduction

SECRECY assurance has been shown to come naturally as an intrinsic property of the physical layer that exploits different channel qualities that are seen by the receiver and eavesdropper, respectively. There is a rich literature on characterizing the information theoretic secrecy capacity of the physical layer that can be achieved at the link level for wireless transmissions. Pioneering work on physical layer secrecy for the wire-tap channel model was introduced by Wyner [5], which showed that if the eavesdropper has a worse channel than the intended receiver, a non-zero perfect secrecy rate can be achieved. Following the research in [5], many different channel models have been studied to characterize secrecy at the link level (see for example [6-23]).

Building on the model proposed by Wyner in [5], a network level characterization has been proposed in [23], showing that the network connectivity can be greatly affected by secrecy requirements (see also [26-27]). The seminal paper in [23] proposed a network secrecy graph model to analyze the impact of secrecy requirements on the network connectivity. However, the secrecy graph model in [23] builds on a wireless model with simplified geometric constraints at the link layer, which does not capture transmission rate requirements for individual links.

In our preliminary work in [3], we have expanded the graph model proposed in [23] to introduce a more accurate link level description for secrecy requirements, that specifically accounts for the secrecy rate, as well as the overall transmission rate requirements for individual links. Connectivity-rate-secrecy tradeoffs were then analyzed [3] based on an extended secrecy-rate network graph model.

In this paper, we propose a novel random graph model approach to characterize the interdependence between network connectivity requirements and the achievable secrecy and transmission rate. The proposed random graph model shows that network connectivity is exhibiting a threshold driven behavior, for which the network is fully connected when the probability of link availability (with secrecy and rate constraints) between any two nodes exceeds a certain value.

The newly proposed model is then analyzed in combination with our previously proposed partial secrecy metric [1] that characterizes the level of privacy that can be achieved for wireless transmissions, for applications that do not necessarily require full secrecy. One example of such application is image transmission. It has been shown in [1] that by securing the most information theoretic significant part of the image, while the other part of the image is transmitted un-securely, we can reduce the secrecy demands, while ensuring that only a part of the image can be eavesdropped, with the goal of maximizing the reconstructed image distortion at the eavesdropper, yielding a certain level of privacy.

Using the partial secrecy metric proposed in [1] in combination with the novel proposed random graph model, we illustrate the rate-distortion operating points that could be achieved in a network when full connectivity is required.

- *R. Zhang is with Voltamp Electrical Contractors, Inc., E-mail: rzhang2@stevens.edu*
- *C. Comaniciu is with the Department of Elecrical and Computer Engineering, Stevens Institute of Technology, E-mail: ccomanic@stevens.edu.*

2 The Rate-Secrecy Graph Model

2.1 Link Level Rate-Secrecy Model

The idea of partial secrecy comes from the image lossy compression algorithms, for which a certain percentage of loss can be tolerated. The accuracy of the image reconstruction for lossy compression can be characterized by the rate-distortion function [1]. Similarly, a certain percentage of loss will be sufficient to render the decoded data useless for the eavesdropper. Consequently, partial secrecy can be achieved if a "sufficient loss" is enforced at the eavesdropper. In other words, the amount of partial secrecy obtained depends on the amount of data revealed and can be characterized by the rate-distortion function.

To partially secure a stream of data, the initial information data stream is split into a common sub-stream and a private sub-stream. The common sub-stream is determined such that it provides minimal information for the eavesdropper, while the private sub-stream contains key privacy information. The splitting can be done using an algorithm reminiscent of lossy compression algorithms, with the most relevant information being assigned to the private stream, and transmitted with perfect secrecy [1].

The partial secrecy-capacity region for transmission between nodes i and j, with eavesdropper e^* could then be determined as in [1]:

$$C_{ps}^{GuPS} = \bigcup_{\beta\in[0,1]}$$

$$\left\{\begin{array}{c} (R_0, R_s) \\ R_0 \le \frac{1}{2}\log\left(1+\frac{(1-\beta)Ph(x_i,x_j)}{\mu^2+\beta Ph(x_i,x_j)}\right) \\ R_1 \le \frac{1}{2}\log\left(1+\frac{\beta Ph(x_i,x_j)}{\mu^2}\right)-\frac{1}{2}\log\left(1+\frac{\beta Ph(x_i,e^*)}{\sigma^2}\right) \\ R_s \ge R_1 \end{array}\right. , \quad (1)$$

where R_0 represents the rate of transmission for the non-private sub-stream (common sub-stream), R_1 represents the rate of transmission for the private sub-stream, and it is guaranteed that the secrecy rate R_s is at least equal to the private sub-stream rate. In (1), μ^2 and σ^2 represent the channel noise levels at the receiver and eavesdropper, respectively, P represents the transmission power, with a power fraction β allocated to the private stream, with β being optimized to achieve the rate capacity region [1], $\beta \in [0,1]$.

The average link gain is inverse proportional to the distance between the receiving and the transmitting nodes:

$$h(x_i x_j) \approx \frac{1}{\left\|x_i - x_j\right\|^{\alpha}}, \quad (2)$$

where α is the amplitude loss exponent.

If we denote by e^* the eavesdropper with the strongest received signal from the transmitter i, i.e.,

$$e^* = \arg\max_{e} Ph(x_i, e), \quad (3)$$

the achieved privacy level can be defined based on (1) by introducing a rate distortion level metric, defined as the percentage of the source rate that is transmitted with perfect secrecy, and consequently will not be available at the eavesdropper:

$$D = \frac{R_s}{R_t}, \quad \text{where } R_t = R_0+R_1. \quad (4)$$

As in [1, 2] the level of privacy is defined as a subjective perception of the user and can be determined visually for an example of image transmission. The level of privacy ranges from low to high, characterized by a higher, and respectively, a lower percentage of the transmission rate being detected by the eavesdropper (common stream). In Table 1 we illustrate some examples of images decoded by the eavesdropper (common image), when the imposed privacy level is low, and medium, respectively. The intended receiver will be able to decode both the common and private sub-streams for a perfect reconstruction of the image, while the eavesdropper will only be able to decode the common image.

The impact of privacy requirements on the network connectivity can be determined based on a geometric constraint requirement that specifies the minimum distance ratios from the transmitter to the receiver and transmitter and eavesdropper respectively, such that a certain distortion requirement can be achieved at the eavesdropper, given the energy constraints.

The impact of privacy requirements is captured using the distance ratio ξ [3], which is defined as the ratio of the distance between the transmitter and eavesdropper versus the transmitter and receiver distance:

$$\xi = \frac{\left\|x_i - e^*\right\|}{\left\|x_i - x_j\right\|} = \frac{r}{R}, \quad (5)$$

where R = maximum distance transmission achievable between transmitter and receiver for given rate and secrecy constraints, and r = minimum distance requirement between transmitter and eavesdropper.

Based on (2) and (5) the partial secrecy capacity can be rewritten as

$$C_{ps}^{GuPS} =$$

$$\cup_{\beta\in[0,1]} \left\{\begin{array}{c} (R_0, R_S): \\ R_0 \le \frac{1}{2} log\left(1+\frac{(1-\beta(\xi))\frac{P}{R\alpha}}{\mu^2+\beta(\xi)\frac{P}{R\alpha}}\right) \\ R_1 \le \frac{1}{2} log\left(1+\frac{\beta(\xi)\frac{P}{R\alpha}}{\mu^2}\right) - \frac{1}{2} log\left(1+\frac{\beta(\xi)\frac{P}{(\xi R)^\alpha}}{\sigma^2}\right) \\ R_S \ge R_1 \end{array}\right. . \quad (6)$$

In Figure 1, we illustrate how the achievable transmission rates (private and common stream, and total transmitted rate), as well as achievable distortion depend on the distance ratio metric. Numerical results were obtained for $R = 1$, $\alpha = 2$, and $\mu^2 = \sigma^2 = 1$.

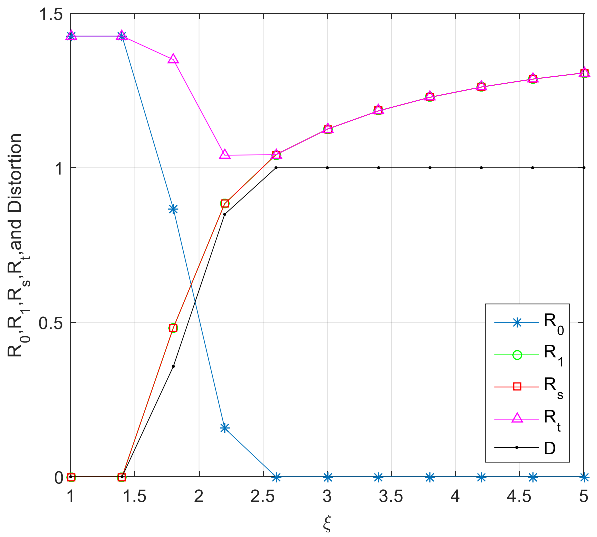


Figure 1. Secrecy-rate-connectivity tradeoffs

From Figure 1, we can see that perfect secrecy ($D = 1$) is obtained for $\xi > 2.5$. We note however that imposing a large value for the distance ratio will negatively impact on the network connectivity. For smaller values for ξ, the network connectivity will improve but at the expense of the achievable secrecy. Imposing only partial secrecy constraints may result in a good tradeoff between connectivity and secrecy.

If $R_t \geq \eta', R_s \geq \eta' D, \text{and } R_t, R_s \in C_{ps}^{GuPs}$, the edge condition could be derived based on ξ, as

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

$$\geq \left(\frac{\mu^2 2^{\eta D_{\min}}}{\sigma^2 \left(1 - R^\alpha / \eta E_b \right) \left(2^{\eta D_{\min}} - 1 \right)} \right)^{1/\alpha} . \qquad (7)$$

with $\eta = 2\eta'$.

2.2 Network Model

We consider N wireless nodes uniformly distributed in a square with dimensions $A \times A$, that are trying to communicate with each other with some level of privacy (i.e., a specified level of partial secrecy is required). We also consider N_e eavesdropper nodes, with $N_e = N$ uniformly distributed in a larger square area, with dimensions $\varepsilon A \times \varepsilon A$, with $\varepsilon > 1$, such that the density of eavesdropper nodes λ_e is equal to $\varepsilon^2 \lambda$, with $\lambda = N/A^2$, and $\lambda_e = N_e / \varepsilon^2 A^2$, where λ is the density of regular nodes.

In [24], the authors have shown that the cumulative distribution function (CDF) that characterizes the distances between any two users that are uniformly distributed in a rectangular area can be well approximated by the CDF obtained considering an alternate model, in which the nodes are distributed according to a Gaussian distribution having the standard deviation $\sigma_1 = A/k$, with $k = 3.5$, as given by

$$F_d \left(y = k \sigma_1 x \right) = 1 - \exp \left(- \frac{k^2}{4} x^2 \right) \qquad (8)$$

For our network model, the CDF for the distance between two wireless nodes can thus be expressed as

$$F_d \left(y \right) = 1 - \exp \left(- \frac{k^2}{4 A^2} y^2 \right) \qquad (9)$$

where y is the distance between any two wireless nodes(9)

Based on (9), the CDF characterizing the distance between an arbitrary wireless node and an arbitrary eavesdropper is determined to be

$$F_{d_e} \left(z \right) = 1 - \exp \left(- \frac{k^2}{4 \varepsilon^2 A^2} z^2 \right) \qquad (10)$$

where z is a random variable representing the distance(10) between a wireless node and an eavesdropper.

The probability of a secure link for a transmission within the radius R, can be defined to be the probability that the distance between a transmitting and a receiving node should be less or equal to R, while the distance between the transmitter and eavesdropper should be at least ξR:

$$P_{link}^{secure} = \Pr \left\{ d_{ij} \leq R \right\} \Pr \left\{ d_{ie} \geq \xi R \right\}, \qquad (11)$$

with R and ξ previously defined in (5).

Based on (10), the probability that the distance between the source and receiver, d_{ij}, is smaller than R, can be determined to be

$$\Pr \left\{ d_{ij} \leq R \right\} = 1 - \exp \left(- \frac{k^2 R^2}{4 A^2} \right) \qquad (12)$$

Similarly, the probability that the distance between the source and eavesdropper, d_{ie}, is smaller than R is given as

$$\Pr \left\{ d_{ie} \geq \xi R \right\} = \exp \left(- \frac{k^2 \xi^2 R^2}{4 \varepsilon^2 A^2} \right) . \qquad (13)$$

In Figure 2 we illustrate the dependence of the link probability on the ratio of densities for wireless nodes vs. eavesdroppers for perfect secrecy. We can see that, for the same density ratio, a higher density of trustful nodes leads to a higher link availability, i.e. the probability of having a secure link between two arbitrary nodes increases.

2.3 A Random Graph Model Approximation for the Secrecy-Connectivity Graph

In this section, we propose to model the secrecy-connectivity graph as a random graph using the Erdős–Rényi (ER) $G(n, p)$ random graph model [26]. In this model, nodes in the graph are connected randomly, and an edge will exist in this graph with probability p independent of all other edges.

In our model, edges will be included in the graph with a link probability given by (11),(12),(13). The assumption of independence implies that the distance distributions for all nodes that are uniformly distributed in the square region, to a fixed node are independent. The correctness of this independence assumption will be verified by determining the nodes' out-degree probability distribution using two different approaches: 1) using a classic spatial point process model which is equivalent with the uniform distribution of the nodes model we use – this approach does not use any independence assumption approximation; 2) using a random graph model that assumes independence of the edges, and edge availability according to the link probability in (11),(12),(13).

When nodes are uniformly distributed with a density λ, this model is equivalent to a Poisson point process with rate λ [25]. Considering this spatial point process model, the probability that a receiver will be located within a circle with radius R from an arbitrary transmitting node is [25]

$$P = \frac{\pi R^2}{A^2} \quad . \qquad (14)$$

Similarly, the probability that an eavesdropper will be located within a circle with radius ξR is

$$P_e = \frac{\pi \xi^2 R^2}{\varepsilon^2 A^2} \quad . \qquad (15$$

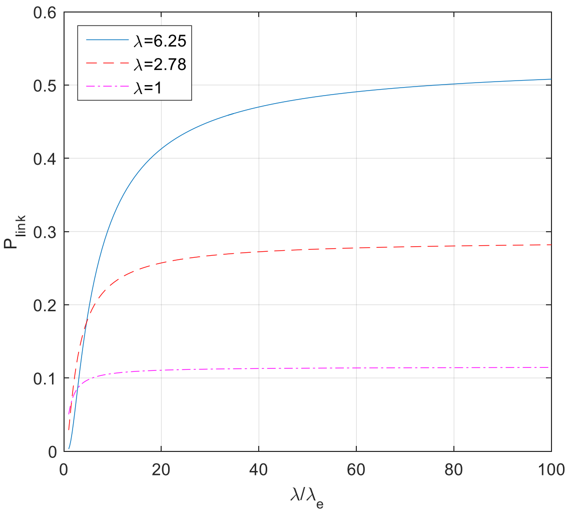


Figure 2. Secure link probability dependence on the ratio of densities of regular vs. eavesdropping nodes

Given (14) and (15) the out-degree probability mass function can be computed as

$$P[N_{out} = n] = \binom{N}{n} P^n (1-P)^{N-n} \binom{N_e}{0} P_e^0 (1-P_e)^{N_e}. \qquad (16)$$

For the random graph model, the out-degree distribution can be determined by computing the probability that n nodes could securely communicate within radius R, given the link probability in (11),(12),(13), and assuming independence for the links.

$$P[N_{out} = n] = \binom{N}{n} \left(P_{link}^{secure}\right)^n \left(1 - P_{link}^{secure}\right)^{N-n} \qquad (17)$$

In Figure 3 the out-degree distribution is plotted for the two models, for $\lambda/\lambda_e = 25$, and $\lambda/\lambda_e = 5$, and for different values for λ. Figure 3 shows a very good match for the out-degree probability for the two calculation methods, with the percentage of error being under 1%.

Based on this result, we conclude that the random graph model (which assumes independence for link availability) approximates well the connectivity behavior of the studied network model, as reflected in the out degree distribution.

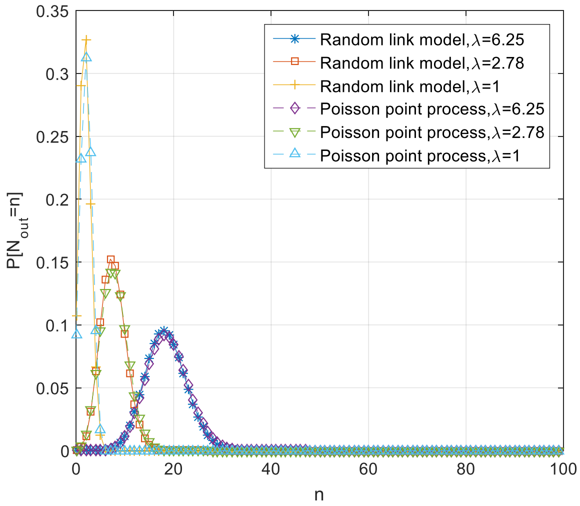


Figure 3a. Out-degree distribution, λ/λ_e=15

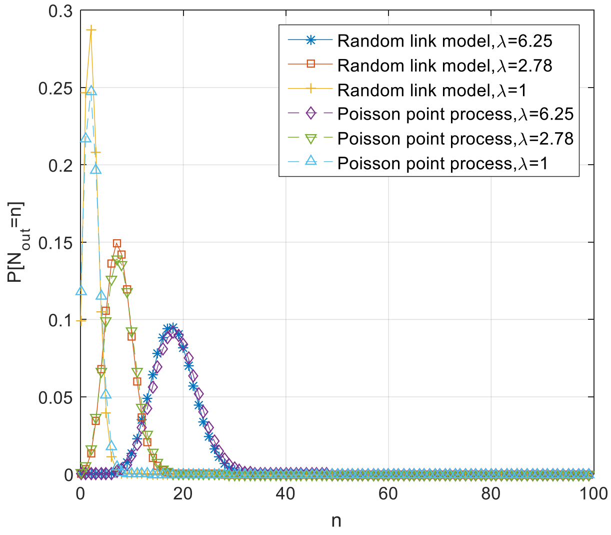


Figure 3b. Out-degree distribution, λ/λ_e=5

3 RATE-SECRECY-CONNECTIVITY TRADEOFFS

In this section, the proposed random graph model is used to analyze rate-secrecy-connectivity tradeoffs.

In Figure 4, the probability of isolation (out degree = 0) for an arbitrary node in the network is illustrated, which is equivalent to the probability that the network is disconnected. We can see that the probability of the network being disconnected decreases significantly as the ratio λ/λ_e increases, but the decrease stops for $\lambda/\lambda_e \geq 20$, which is a point of diminishing returns. Furthermore, it can be seen that the secrecy requirement (quantified by the distortion metric) greatly impacts the connectivity, especially for lower λ/λ_e ratios. Imposing just a partial secrecy constraint with $D = 0.5$, instead of perfect secrecy, reduces up to 7 times the probability of the network being disconnected.

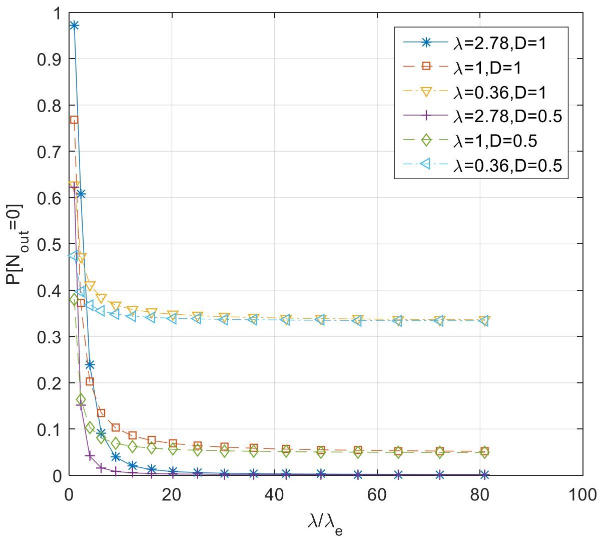


Figure 4. Probability of isolation

The Erdős–Rényi graph model allows to characterize the network connectivity using the result in [26], which states that for the *G(n,p)* model, $\frac{\ln(n)}{n}$ is a sharp threshold for the connectedness of *G(n,p)*.

- If $p < \frac{\ln(n)}{n}$, a graph in *G(n,p)* will almost surely contain isolated nodes, and thus be disconnected.
- If $p > \frac{\ln(n)}{n}$, a graph in *G(n,p)* will almost surely be connected.

Consequently, for our network model, the condition to have a network that is fully connected is $p_{link}^{secure} > \frac{\ln(n)}{n}$, and based on this condition, the distance ratio ξ requirement for full connectivity can then be determined to be (based on (11),(12),(13)):

$$\xi < \frac{2\varepsilon A\sqrt{-\frac{\log(N)}{N\left(1-\exp\left(-k^2R^2/4A^2\right)\right)}}}{kR}. \qquad (18)$$

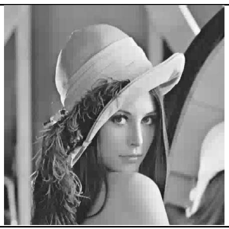
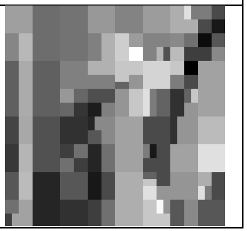
Based on (6), we can determine the achievable distortion and transmission rates under full connectivity constraints, with $D = R_s/R_t$,

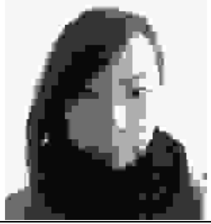
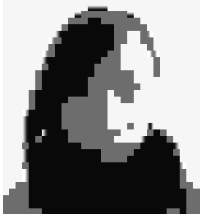
$$\begin{aligned} R_S &\leq \frac{1}{2}log\left(1+\frac{\beta P}{\mu^2R^\alpha}\right)-\frac{1}{2}log\left(1+\frac{\beta P}{\sigma^2\xi^\alpha R^\alpha}\right), \\ R_t &\leq \frac{1}{2}log\left(1+\frac{P}{\mu^2R^\alpha}\right)-\frac{1}{2}log\left(1+\frac{\beta P}{\mu^2R^\alpha}\right) \qquad (19) \\ &+\frac{1}{2}log\left(1+\frac{\beta P}{\mu^2R^\alpha}\right)-\frac{1}{2}log\left(1+\frac{\beta P}{\sigma^2\xi^\alpha R^\alpha}\right). \end{aligned}$$

From (19) we see that both the total transmission rate and the distortion will depend on the power allocation between the common and the private stream (*β, 1-β*), given a power budget *P*. In Figures 5 and 6 we show the dependence of the achievable distortion and transmission rates, respectively, on the ratio λ/λ_e ($\lambda/\lambda_e=\varepsilon^2$), and on the percentage β of the power budget allocated to the private stream, for a fully connected network. Figures 5 and 6 show that the distortion *D* increases with λ/λ_e, while the achievable transmission rate decreases with λ/λ_e. We also note that a higher percentage of power allocation for the private sub-stream will yield a higher distortion (better secrecy) but with a penalty in the achievable transmission rates.

TABLE I

ACHIEVABLE PRIVACY LEVEL FOR FULLY CONNECTED NETWORK, λ=1 (*N*=25, *A*=5). COMMON IMAGE DECODED BY THE EAVESDROPPER.

β (*D*, *R*$_t$)	0.3 (0.43, 0.91) low privacy level	0.5 (0.58, 1.21) medium privacy level
Lena		

Girl		

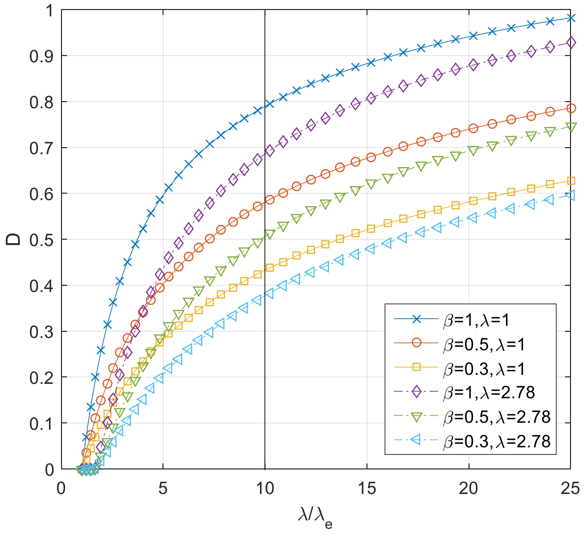


Figure 5. Distortion as a function of relative density of nodes and eavesdroppers, for different power allocations (*βP*, *(1-β)P*)

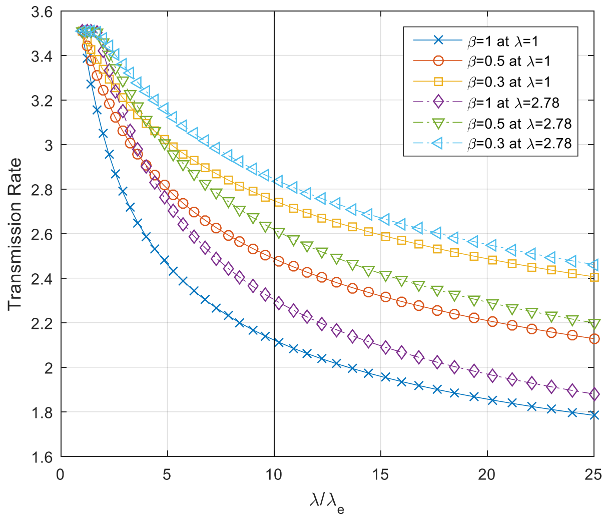


Figure 6. Transmission rate as a function of relative density of nodes and eavesdroppers for different power allocations (*βP*, *(1-β)P*)

In Table I, we illustrate the secrecy-rate tradeoff for two image transmission examples, for a fixed value for the regular to eavesdropper users' density ratio, $\lambda/\lambda_e = 10$. The secrecy is quantified by the distortion metric (D), and its impact on privacy is illustrated visually, by two common images that are decoded by the eavesdropper (images Lena, and Girl are transmitted). We note that a good privacy level (medium) can be achieved with a distortion rate as low as $D = 0.58$. For these examples the network is fully connected (Figures 5 and 6).

We note that a perfect secrecy requirement for this fully connected network can only be achieved for very large values of λ/λ_e (greater than 25), but a good level of privacy (e.g. $D = 0.58$) can be achieved for a range of λ/λ_e ratios, given an appropriate distribution of power, β, between the private and common sub-streams), while maintaining full connectivity for the network (Figure 5). We also note that a medium privacy level ($D = 0.6$) can be achieved for regular nodes to eavesdroppers' density ratios as high as $\lambda/\lambda_e = 5$, if $\beta = 1$, even though obtaining perfect secrecy is not possible in this scenario. From Figure 5 it can be seen that a graceful degradation of secrecy can be achieved when network conditions deteriorate (i.e., as λ/λ_e decreases).

4 Conclusion

In this paper, we proposed a novel approach to characterize secrecy-rate-connectivity tradeoffs for a wireless network with eavesdroppers, based on a random graph model approximation for the secrecy-connectivity graph.

Combining information theoretic metrics with the proposed random graph model, we have shown that perfect secrecy requirements put a high toll on the network performance in terms of both connectivity and achievable transmission rates, and, by relaxing the secrecy constraints, good privacy levels can be achieved for applications that do not require perfect secrecy (e.g. image transmissions), while enforcing full connectivity for the network. We have also shown that the power allocation between the private and common sub-streams for the transmission influences the rate-secrecy operating point, with more power allocated to the private stream resulting in better secrecy, but lower achievable transmission rate. Our analysis shows that it is possible to have a fully connected network and achieve a good level of privacy even when the density of eavesdroppers is high (for our numerical results, as high as 20% of the density of the regular trusted users in the network).

.

References

[1] C. Comaniciu, H. V. Poor and R. Zhang, "An information theoretic framework for energy efficient secrecy," in Proc. 38thConf. International Conference on Acoustics, Speech, and Signal Processing (ICASSP), Vancouver, BC, May 2013.

[2] R. Zhang, C. Cristina and V. Poor, "Outage capacity and partial secrecy for energy efficient physical layer security in Gaussian fading channels," *Wireless Personal Multimedia Communications (WPMC), 2013 16th International Symposium on*, Atlantic City, 2013.

[3] R. Zhang, C. Comaniciu, H.V. Poor, "On rate, secrecy, and network connectivity tradeoffs for wireless networks," IEEE Comm. Letter, vo. 20, issue 8, August 2016, pp. 1559-1562.

[4] C. E. Shannon, "Communication theory of secrecy systems," Bell Syst. Tech. J., vol. 29, pp. 656-715, 1949.

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

[6] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," IEEE Trans. Inf. Theory, vol. 24, no. 3, pp. 339-348, 1978.

[7] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," IEEE Trans. Inf. Theory, vol. 24, no. 4, pp. 451-456, July 1978.

[8] A. Hero, "Secure space-time communication," IEEE Trans. Inf. Theory, vol. 49, no. 12, pp. 3235-3249, Dec. 1975.

[9] R. Negi and S. Goel, "Secret communication using artificial noise," in Proc. IEEE Vehicular Technology Conference, vol. 3, Dallas, TX, Sep. 2005, pp. 1906-1910.

[10] E. Ekrem and S. Ulukus, "Secrecy capacity region of the Gaussian multi-receiver wiretap channel," in Proc. IEEE Int. Symp. on Inf. Theory, Seoul, Korea, June 2009, pp. 2612-2616.

[11] T. Liu and S. Shamai, "A note on the secrecy capacity of the multiple-antenna wiretap channel," IEEE Trans. Inf. Theory, vol. 55, no. 6, pp. 2547-2553, June 2009.

[12] L. Weingarten, T. Liang, Y. Steinberg, and P. Viswanath, "The capacity region of the degraded multiple-input multiple-output compound broadcast channel," IEEE Trans. Inf. Theory, vol. 55, no. 11, pp. 5011-5023, Nov. 2009.

[13] L. Zhang, R. Zhang, Y. Liang, Y. Lin and S. Cui, "On the relationship between the multi-antenna secrecy communications and cognitive radio communication," in Proc. Allerton. Conf. on Communications, Control, and Computing., Monticello, IL, Sep. 2009.

[14] S. Goel and R. Negi, "Secret communication in presence of colluding eavesdropper," in Proc. Military Commun. Conf., Oct. 2005, pp. 1501-1506.

[15] P. C. Pinto, J. O. Barros and M. Z. Win, "Wireless physical-layer security: The case of colluding eavesdroppers," in Proc. IEEE Int. Symp. on Inf. Theory, Seoul, South Korea, July 2009, pp. 2442-2446.

[16] E. Ekrem and S. Ulukus, "Secrecy capacity of SIMO and slow fading channels," in Proc. IEEE Int. Symp. on Inf. Theory, Toronto, ON, July 2008, pp. 2217-2221.

[17] P. Parada and R. Blahut, "Secrecy in cooperative relay broadcast channels," in Proc. IEEE Int. Symp. on Inf. Theory, Adelaide, Australia, Sep. 2005, pp. 2152-2155.

[18] P. Gopala, L. Lai, and H. EI Gamal, "On the Secrecy capacity of Fading Channels," IEEE Trans. Inf. Theory, vol. 54, no.10, Oct. 2008.

[19] Z. Li, R. Yates, and W. Trappe, "Secrecy capacity of independent parallel channels," Proc. Annu. Allerton Conf. Communication, Control and Computing, pp. 841-848, Sep. 2006.

[20] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," IEEE Trans. Inf. Theory, vol. 54, no. 6, pp. 2515-2534, 2008.

[21] J. Barros and M. Bloch, "Strong secrecy for wireless channels,," in Proc. International Conf. on Inf. Theory Security, Calgary, Canada, Aug, 2008.

[22] U. Maurer, "Secret key agreement by public discussion from common information," IEEE Trans. Inf. Theory, vol. 39, no. 3, pp. 733-742, May 1993.

[23] M. Haenggi, "The secrecy graph and some of its properties," in *Prof. of IEEE International Symposium on Information Theory, ISIT'08*, Toronto, Canada, 2008.

[24] L. E. Miller. Distribution of link distances in a wireless network. Journal of Research of the National Institute of Standards and Technology, 106(2):401–412, March-April 2001.

[25] A. Baddeley, Spatial point processes and their applications, appears in, *Stochastic Geometry: Lectures* given at the C.I.M.E. Summer School held in Martina Franca, Italy, September 13-18, 2004, 306 GUNNAR CARLSSON Lecture Notes in Mathematics 1892, Springer-Verlag, W. Weil, editor, Berlin, 2007. ISBN 3-540-38174-0, pp. 1–75. MR2327290 (2008c:60045)

[26] P. Erdős, A. Rényi, "On the Evolution of Random Graphs," Publications of the Mathematical Institute of the Hungarian Academy of Science, 1960, vol 5, pp. 17-61.

[27] S. Goel, V. Aggarwal, A. Yener, A.R. Calderbank, "Modeling Location Uncertainty for Eavesdroppers: A Secrecy Graph Approach", in *Proc. IEEE International Symposium on Information Theory Proceedings (ISIT)*, pp. 2627-2631, 2010.

[28] S. Goel, V. Aggarwal, A. Yener, A.R. Calderbank, "The Effect of Eavesdroppers on Network Connectivity: A Secrecy Graph Approach," *IEEE Transactions on Information Forensics and Security*, 6(3), pp.712-724, 2011.

Ruolin Zhang received the B.E. degree in electrical engineering from the Hebei University of Techonology, Tianjin , China, in 2010, and the Master of Engineering in Electrical Engineering degree from the Stevens Institute of Technology (SIT), New Jersey, United States, in 2012. In December 2016 she graduated from Stevens Institute of Technology with a Ph.D. degree in Electrical and Computer Engineering. She is currently with Voltamp Electrical Contractors. Her research interests are in optimization of wireless networks performance, and information theoretic analysis for quantifying energy-secrecy tradeoffs.

Cristina Comaniciu received the M.S. degree in electronics from the Polytechnic University of Bucharest in 1993, and the Ph.D. degree in electrical and computer engineering from Rutgers University in 2002.

From 2002 to 2003 she was a postdoctoral fellow with the Department of Electrical Engineering, Princeton University. Since August 2003, she is with Stevens Institute of Technology, Department of Electrical and Computer Engineering, where she is now an Associate Professor and serves as Associate Department Chair for Graduate Studies. In Fall 2011 she was a visiting faculty fellow with the Department of Electrical Engineering, Princeton University. She served as an associate editor for the IEEE COMMUNICATION LETTERS (2007-2011).

Professor Comaniciu is a recipient of the 2007 IEEE Marconi Best Paper Prize Award in Wireless Communications and of the 2012 Rutgers School of Engineering Distinguished Young Alumnus Medal of Excellence. She is a coauthor of the book Wireless Networks: Multiuser Detection in Cross-Layer Design (Springer, NY). Her research interests are focused on applications of game theory, evolutionary games and machine learning for resource management and optimization of complex distributed networks.

On Rate, Secrecy, and Network Connectivity Tradeoffs for Wireless Networks

Ruolin Zhang, *Student Member, IEEE,* Cristina Comaniciu, *Member, IEEE,* and H. Vincent Poor, *Fellow, IEEE*

***Abstract*—A new approach to the characterization of network connectivity under transmission rate and secrecy constraints is proposed, based on a rate-secrecy graph model. The proposed model is based on an information theoretic framework and rate-distortion requirements are used to characterize the level of secrecy for individual links in the network. Rate-secrecy-connectivity tradeoffs are illustrated and it is shown that by relaxing the secrecy constraint an acceptable secrecy level can be achieved while significantly improving network connectivity and transmission rate efficiency for the wireless nodes.**

***Index Terms*—Information theoretic secrecy, partial secrecy, privacy, secrecy graph, physical layer security.**

I. Introduction

SECRECY assurance comes as a natural property of the physical layer, and can be exploited at the expense of a lower transmission rate and higher energy expenditure per bit. There is a rich literature on characterizing the information theoretic secrecy capacity of the physical layer that can be achieved at the link level for wireless transmissions, starting with the wire-tap channel model introduced by Wyner [4], for which it is shown that if the eavesdropper has a worse channel than the intended receiver, a non-zero perfect secrecy rate can be achieved. Based on this eavesdropper-worse-than-receiver channel condition, earlier work in the literature has proposed network connectivity models based on a secrecy graph framework [3] showing that network connectivity can be greatly affected by secrecy requirements (see also [5] and [6]).

In this work, we expand the graph model proposed in [3] to introduce a more accurate description of secrecy requirements, that specifically accounts for the secrecy rate, as well as for the overall transmission rate requirements for individual links. The proposed rate-secrecy graph provides a general framework that can capture the tradeoffs between transmission rate (which also reflects energy expenditure per bit for a given transmission power budget), secrecy rate, and connectivity. A better understanding of these tradeoffs will allow for a graceful degradation of performance in wireless networks when resources are scarce.

II. Layer Characterization for Rate-secrecy Tradeoffs

We consider the problem of transmitting information from a source to a destination node via a Gaussian channel with multiplicative fading gain coefficients. We adopt the partial secrecy capacity proposed in [1] and [2] for which the transmission requires some security protection against eavesdropper nodes with additional transmission rate constraints. We note that, for a fixed power budget, the transmission rate constraints directly map into energy per bit constraints.

In [1] partial secrecy is achieved by splitting the initial data stream into private and non-private sub-streams, and transmitting the former under perfect secrecy constraints and the latter with no secrecy, using superposition encoding [1],[7]. This sub-stream splitting can be implemented using an inverse lossy compression approach. i.e., the most significant information will be allocated to the private sub-stream. The partial secrecy-capacity region for transmission between two nodes x_i and x_j, with an eavesdropper e* is given similarly to (6) in [1]

$$C_{ps}^{GuPS} = \tag{1}$$

$$\mathrm{U}_{\beta\in[0,1]}\begin{cases}(R_0,R_s):\\ R_0\leq\frac{1}{2}\log(1+\frac{(1-\beta)Ph(x_i,x_j)}{\mu^2+\beta Ph(x_i,x_j)})\\ R_1\leq\frac{1}{2}\log(1+\frac{\beta Ph(x_i,x_j)}{\mu^2})-\frac{1}{2}\log(1+\frac{\beta Ph(x_i,e^*)}{\sigma^2}),\\ R_s\geq R_1\end{cases}$$

where R_0 represents the rate of transmission for the non-private sub-stream, R_1 represents the rate of transmission for the private sub-stream, and it is guaranteed that the secrecy rate R_s is at least equal to the private sub-stream rate. In (1), μ^2 and σ^2 represent the channel noise levels at the receiver and eavesdropper, respectively, P represents the transmission power, with a power fraction β allocated to the private stream, β being optimized to achieve the rate capacity region [1]. The average link gain in (1) can be determined based on the distance between the receiving and the transmitting nodes:

$$h(x_i,x_j)\approx\frac{1}{\parallel x_i-x_j\parallel^{\alpha}}, \tag{2}$$

where α is the amplitude loss exponent.

The eavesdropper e^* in (1) is considered to be the eavesdropper with the strongest received signal from the transmitter x_i, i.e.,

$$e^*=\arg\max_{e} Ph(x_i,e). \tag{3}$$

The achieved privacy level is defined based on (1) by introducing a rate distortion level metric, defined as the percentage

R. Zhang is with the Department of Electrical and Computer Engineering, Stevens Institute of Technology, Hoboken, NJ, 07030 USA e-mail: rzhang2@stevens.edu.

C. Comaniciu is with the Department of Electrical and Computer Engineering, Stevens Institute of Technology, Hoboken, NJ, 07030 USA e-mail: ccomanic@stevens.edu.

H. Vincent Poor is with the Department of Electrical Engineering, Princeton University, Princeton, NJ, 08540 USA e-mail: poor@princeton.edu.

Manuscript received February 13, 2016; revised April 21, 2016.

of the source rate that achieves secrecy, and as such, it will not be available at the eavesdropper:

$$D = \frac{R_s}{R_t}, \text{ where } R_t = R_0 + R_1. \tag{4}$$

It has been shown in [1] and [2] that the level of privacy is a subjective perception of the user and can be determined visually for an example of image transmission (see Fig.1). The level of privacy proposed in [1] and [2] ranges from low to high, characterized by a higher and respectively a lower percentage of the transmission rate being detected by the eavesdropper (common stream). In Fig. 1 we show the common sub-stream image that the eavesdropper would be able to decode from the transmission of the Lena image for an imposed distortion level of $D = 0.6$, medium privacy level. We note that the intended receiver will decode both common and private sub-streams for a perfect reconstruction of the image.

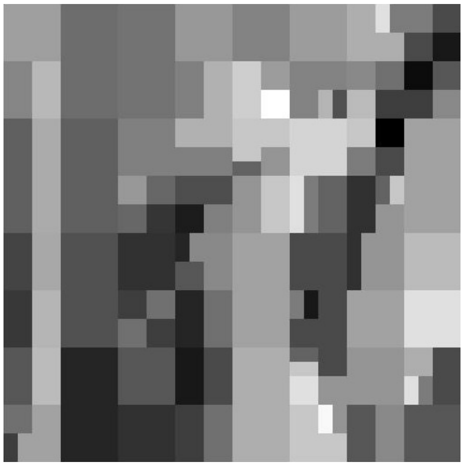


Fig. 1. Common sub-stream decoded by an eavesdropper from image Lena

Energy requirements can be characterized using the energy consumption per bit metric, determined for a power budget P:

$$E_b = \frac{P}{R_t}(Joules/tx). \tag{5}$$

To better understand the impact of privacy requirements on the network connectivity, we derive a geometric constraint requirement that specifies the minimum distance ratios from the transmitter to the receiver and eavesdropper respectively, such that a certain distortion requirement can be achieved at the eavesdropper, given the energy constraints.

We define the distance ratio, as the ratio of the distance between the transmitter and eavesdropper to that between the transmitter and receiver as

$$\xi = \frac{\parallel x_i - e^* \parallel}{\parallel x_i - x_j \parallel} = \frac{r}{R}, \tag{6}$$

where $R =$ maximum distance transmission achievable between the transmitter and receiver for given rate and secrecy constraints, and $r =$ minimum distance requirement between the transmitter and eavesdropper.

Using (2) and (6) in conjunction with (1), we rewrite the partial secrecy capacity as follows:

$$C_{ps}^{GuPS} = \tag{7}$$

$$\mathrm{U}_{\beta\in[0,1]} \begin{cases} (R_0, R_s) : \\ R_0 \leq \frac{1}{2}\log(1 + \frac{(1-\beta(\xi))\frac{P}{R^\alpha}}{\mu^2+\beta(\xi)\frac{P}{R^\alpha}}) \\ R_1 \leq \frac{1}{2}\log(1 + \frac{\beta(\xi)\frac{P}{R^\alpha}}{\mu^2}) - \frac{1}{2}\log(1 + \frac{\beta(\xi)\frac{P}{(\xi R)^\alpha}}{\sigma^2}). \\ R_s \geq R_1 \end{cases}$$

Fig. 2 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, $R = 1$.

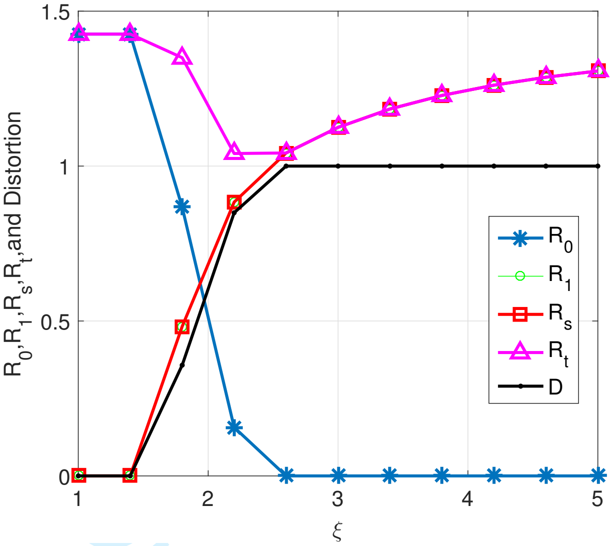


Fig. 2. Secrecy-energy connectivity tradeoffs

From Fig. 2 we note that the highest transmission rate (yielding the most energy efficient transmission) is obtained for the case in which the eavesdropper is much further away than the intended receiver (large ξ). This case also corresponds to perfect secrecy, but will enforce stricter constraints on the link availability at the network level and thus it will negatively impact connectivity. As the eavesdropper is allowed to be closer to the transmitter, the network connectivity will improve, but at the expense of lower transmission rate, and consequently lower energy efficiency, as well as decreased distortion at the eavesdropper.

From the above results, it becomes apparent that the network connectivity can be increased either by increasing the allowable distance ratio (secrecy constraint) or by increasing the reliable transmission distance (energy constraint). We can infer that relaxing the perfect secrecy constraints may result in increased connectivity for the network.

In what follows, we will further quantify the connectivity metrics using a random graph network model, with the focus on analyzing the tradeoffs with the other key performance metrics: energy/transmission rate and secrecy constraints.

III. The Rate-Secrecy Graph

Consider a wireless network in which legitimate nodes and potential eavesdroppers are randomly scattered in space, according to a Poisson point process. In [3], the secrecy constraint is captured at the network level by invalidating links that do not meet the condition that the closest eavesdropping node is further away from transmitter than the receiver is. The secrecy condition in [3] is equivalent to a geometric condition: $r \geq R$. However, this condition does not capture the rate transmission requirements for individual links.

From the results in Section II, we refine this geometric constraint to be tightly linked with transmission and secrecy rate requirements. Based on (1) and (6), we can derive distance ratio constraints to meet the transmission rate, energy, and secrecy requirements. We can then define a family of rate-secrecy graphs, parametrized by the secrecy and rate constraints, such that links that do not meet these constraints are eliminated from the network communication graph.

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

$$E = \{\overrightarrow{x_i x_j} : R_t \geq \eta', R_s \geq \eta' D, R_t, R_s \in C_{ps}\}, \quad (8)$$

where C_{ps} is the partial secrecy capacity of the link between the transmitter x_i and the receiver x_j; η' is a threshold representing the minimum required transmission rate for each communication link, and $\eta' D$ is a threshold representing the required minimum secrecy rate for the individual links.

The edge existence condition in (8) can be expressed as a geometric relationship between the requirements for the distance to the receiver relative to the distance to the eavesdropper as a function of distortion and energy per bit consumption constraints based on (1) and (6), with $\eta = \eta'/2$:

$$E = \left\{ \overrightarrow{x_i x_j} : \begin{array}{l} R \leq \frac{r}{[(2^{\eta}-1)\frac{\mu^2}{\eta E_b} r^{\alpha} + \frac{\mu^2}{\sigma^2} 2^{\eta} \beta(\xi)]^{1/\alpha}} \\ R \leq \frac{r}{[(2^{\eta D}-1)\frac{\mu^2}{\beta(\xi)\eta E_b} r^{\alpha} + \frac{\mu^2}{\sigma^2} 2^{\eta D}]^{1/\alpha}}, \end{array} \right\}. \quad (9)$$

As in [3], we define the Poisson rate-secrecy graph as a rate-secrecy graph for which $\mathit{\Pi}$ and $\mathit{\Pi}_E$ are mutually independent, homogeneous Poisson point processes with densities λ and λ_E, respectively, and consider a unit arrival rate for the friendly nodes Poisson point process, $\lambda = 1$.

We now redefine the rate-secrecy graphs as being parametrized by the transmission range and the distance ratio requirements that incorporate energy and secrecy constraints. We denote the rate-secrecy graph by $\overrightarrow{G}_{1,\lambda_E,R,\xi}$, where the radius R is the maximum transmission distance achievable between transmitter and receiver, r is the minimum distance requirement between transmitter and eavesdropper and ξ is the distance ratio r/R.

We rewrite the edge condition in (9) based on definition (6):

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

$$\geq \left(\frac{\mu^2 2^{\eta D_{min}}}{\sigma^2(1 - \frac{R^{\alpha}}{\eta E_b})(2^{\eta D_{min}-1})} \right)^{1/\alpha}. \quad (10)$$

We can see from (10) that a rate-secrecy capacity feasibility condition can be obtained by requiring ξ to be positive, and it is given by

$$R < \left(\frac{\beta \eta E_b}{(2^{\eta D_{min}} - 1)\mu^2} \right)^{1/\alpha} \leq \left(\frac{\eta E_b}{(2^{\eta D_{min}} - 1)\mu^2} \right)^{1/\alpha}. \quad (11)$$

The bounds in (10) and (11) hold for $\beta \in [0, 1]$.

Equation (11) gives a bound on the maximum transmission range that can be achieved, given transmission rate, energy per bit consumption, and eavesdroppers distortion constraints. We can see that, 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.

We can see from (10) and (11) that secrecy can be achieved when we impose range and distance ratio constraints.

IV. Impact On Network Connectivity

We study the connectivity of the network by determining the out-degree distributions of the nodes, the probability of out-isolation, and the average out-degree for an arbitrary node in the network.

We consider two cases: (a) the range limited case for which R is limited to a maximum value; (b) the $R \longrightarrow \propto$ case, which corresponds to the unlimited transmission power case.

A. Rate-Secrecy Graph: The Unlimited Power Scenario

For the case of unlimited transmission power, no range transmission limit is imposed. To calculate the out-degree of a vertex we follow a derivation similar to that in [3], where we replace the condition $R < r$ with $R \leq \xi r$. We determine the out-degree probability to be

$$P[N_{out} = n] = \frac{\lambda_E \xi^2}{1 + \lambda_E \xi^2} \left(\frac{1}{1 + \lambda_E \xi^2} \right)^n. \quad (12)$$

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

$$P_{out-isolation} = P[N_{out} = 0] = \frac{\lambda_E \xi^2}{1 + \lambda_E \xi^2}. \quad (13)$$

B. Rate-Secrecy Graph: The Limited Power Scenario

When a transmission power constraint is imposed, a maximum transmission range R can be determined as in (11).

As in [3], we distinguish two cases:

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

$$P_0 = \exp(-\lambda_E \pi r^2) = \exp(-\lambda_E \pi \xi^2 R^2). \quad (14)$$

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

2) There is an eavesdropper at radius ρ. Then the number of friendly nodes is given by a Poisson distribution restricted to a radius $R' = \rho/\xi$, having a 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 [3], but for an enhanced equivalent arrival rate for the eavesdropper, $\lambda_E^* = \lambda_E \xi^2$:

$$P[N_{out} = n] = \frac{\lambda_E^*(1 - \frac{\Gamma(n,a)}{\Gamma(n)}) + \exp(-a)\frac{a^n}{n!}}{(\lambda_E^* + 1)^{n+1}}. \qquad (15)$$

with $a = \pi R^2(\lambda_E^* + 1)$, $R =$ transmission range, and $\Gamma(\cdot,\cdot) =$ the upper incomplete gamma function.

The probability of out-isolation is then given as

$$P[N_{out} = 0] = \frac{\exp(-\pi R^2(\lambda_E^* + 1)) + \lambda_E^*}{1 + \lambda_E^*}. \qquad (16)$$

The mean out and in degrees can be determined to be

$$E[N_{out}] = E[N_{in}] = \frac{1}{\lambda_E^*}(1 - \exp(-\lambda_E^* \pi R^2)). \qquad (17)$$

For numerical results, we assume $\lambda = 1m^{-2}$ and $\lambda_E = 0.08m^{-2}$.

Fig. 3 analyzes the dependence of the out-degree probability on the level of privacy required for the unlimited range scenario. ξ is selected for perfect secrecy ($D = 1$) and for a value of distortion that gives a good level of privacy ($D = 0.6$- Fig.1). We note the significant impact on network connectivity that the secrecy constraint imposes. Note also that $\xi = 1$ (which corresponds to the secrecy constraint imposed in [3]) yields zero secrecy ($D = 0$) when transmission rate and energy constraints are also imposed.

In Fig. 4 we illustrate the dependence of the probability of out-isolation and the mean out degree on ξ for the case of limited transmission range. We can see that as the secrecy requirements increase (with the increase of ξ), the probability of out-isolation significantly increases. In particular, we note that to obtain perfect secrecy, under transmission rate requirements, a ξ minimum value of 2.5 is required (see Fig.2), which leads to a 3.4 fold increase in the out-isolation probability compared to the case studied in [3] and a 58% decrease in the average mean degree for a vertex. We also note that by relaxing the secrecy constraints and imposing a distortion at the eavesdropper of $D = 0.6$ (obtained for $\xi = 2$), there is a 73% reduction for the out-isolation probability and a 72% increase in the mean out-degree for an arbitrary vertex, compared to the case of perfect secrecy.

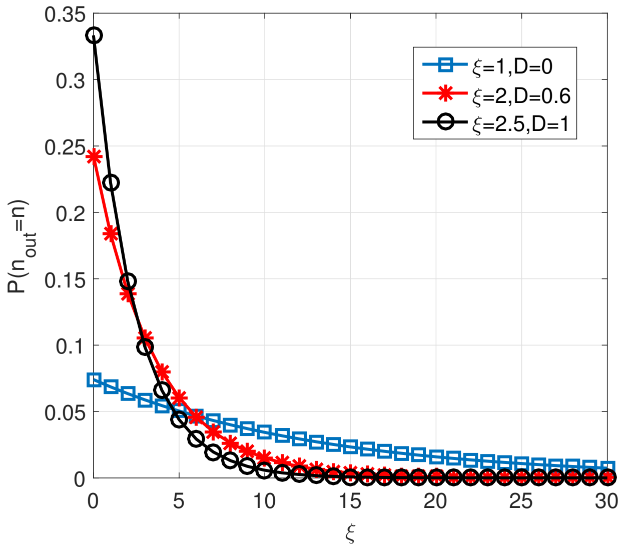


Fig. 3. Out-degree probability - unlimited range scenario

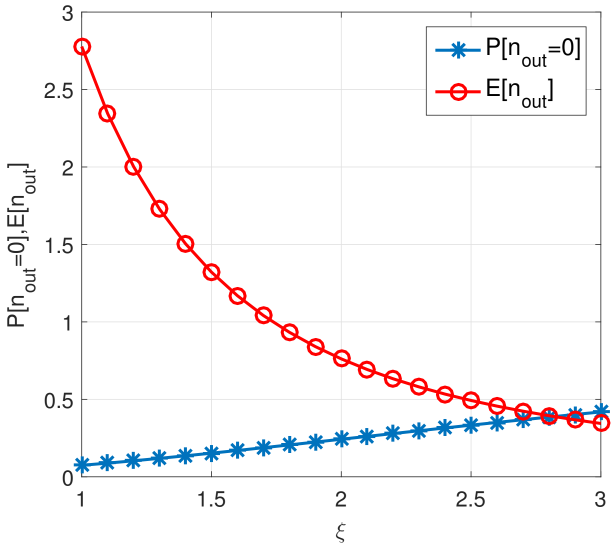


Fig. 4. Out-isolation probability and mean degree - limited range scenario

References

[1] C. Comaniciu and H. V. Poor, "On Energy-Secrecy Trade-offs for Gaussian Wiretap Channels," *IEEE Trans. Inf. Forensics and Security*, 8(2), pp. 314-323, 2013.

[2] C. Comaniciu, H. V. Poor, and R. Zhang "An Information Theoretic Framework for Energy Efficient Secrecy," in *Proc. IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pp. 2906-2910, 2013, Vancouver, Canada.

[3] M. Haenggi, "The Secrecy Graph and Some of Its Properties," in *Proc. IEEE International Symposium on Information Theory, ISIT08*, Toronto, Canada, 2008.

[4] A. D. Wyner, "The Wiretap Channel," *Bell Syst. Tech. J.*, 54(8), pp. 1355-13870, Oct. 1975.

[5] S. Goel, V. Aggarwal, A. Yener, and A. R. Calderbank "Modeling Location Uncertainty for Eavesdropper: A Secrecy Graph Approach," in *Proc. IEEE International Symposium on Information Theory (ISIT)*, pp. 2527-2631, 2010.

[6] S. Goel, V. Aggarwal, A. Yener, and A. R. Calderbank "The Effect of Eavesdroppers on Network Connectivity: A Secrecy Graph Approach," *IEEE Trans. Inf. Forensics and Security*, 6(3), pp. 712(3)-724, 2011.

[7] Y. Liang, H. V. Poor, and S. Shamai "Secure Communications over Fading Channels," in *IEEE Trans. Inf. Theory*, 54(6), pp. 2470-24920, 2008.