cm cm

Secure Energy Efficiency with Poisson Point Process Distributed Jammers

Kirti Kant Sharma and Prof. Ranjan Bose

Bharti School of Telecommunication Technology and Management
Indian Institute of Technology Delhi

IEEE WF-IoT 2019

Table of contents

Introduction

- The Cryptographic Techniques:
  1. Based on sharing of keys
  2. Relies on difficulty in decryption
  3. No guaranteed mathematical measure
  4. Resource dependence of eavesdropper
- The Wireless Network:
  1. The broadcast nature of the wireless medium
  2. Massive growth of wireless devices
  3. Internet of Things (IoT)
  4. Implementation complexity of cryptographic techniques

Introduction

- The Physical Layer Security:
  1. Information-theoretic approach
  2. Utilize the inherent randomness of the communication channel
  3. Mathematically provable and quantifiable
  4. No dependence of eavesdropper resources
  5. No issue of key sharing

Motivation

- The number of connected devices is predicted to rise by about 50 billion by 2020 and accordingly energy consumption by wireless networks will increase [1].
- Physical layer security methods use inherent randomness of the wireless channel to secure the information [2], [3].
- The authors in [4] first proposed the idea of artificial noise to deteriorate the capacity of eavesdropper in case of multi-antenna source and in a cooperative relaying scenario with the help of intended destination.
- Cooperation among communicating nodes to implement physical layer security is widely studied [5].
- In [6], a distributed jammer selection scheme is proposed in which selected jammers radiate independent Gaussian noise to degrade eavesdropper capacity.

Motivation

- Uncoordinated jamming strategies to improve secrecy rate with the help of multiple single antenna helpers in single-input-single-output (SISO) and single-input-multiple-output (SIMO) networks are proposed in [7] and [8], respectively.
- A broad overview of jamming strategies to secure wireless communications is given in [9].
- The secrecy using artificial noise from source and cooperative jamming for single antenna nodes are analyzed in distributed nodes as Ginibre point processes [10].
- Authors proposed a threshold based jammer selection for UCJ having multiple stochastically distributed jammers and eavesdroppers [11].
- In [12], cooperative jamming via local nulling is proposed in case of local channel information at multi-antenna jammers and shown that their scheme performs close to the optimal method in case of global channel information.

Motivation

- In [13], authors analyzed various position based jamming strategies regarding secure throughput and energy efficiency for distributed jamming and eavesdropping nodes.
- The authors in [14], introduced the secrecy capacity per unit cost in terms of the total transmission time and the total energy consumption as a metric to study secure wideband communication in a cost-efficient manner.
- The optimization of SEE for multiple-input-single-output (MISO) and SISO networks is explored in [15] without secrecy rate constraints.
- The authors proposed and compared two schemes using transmit antenna selection with and without artificial noise and shown that artificial noise scheme performs better in terms of energy efficiency when eavesdropper is closer to relay in [16].

Objective

- We propose and analyze a UCJ jammer selection scheme based on channel threshold and selection region in case of PPP distributed helper nodes.
- The aim is to establish analytical formulation for performance evaluation for the proposed scheme with respect to obtained secrecy rate and energy efficiency.

System Model

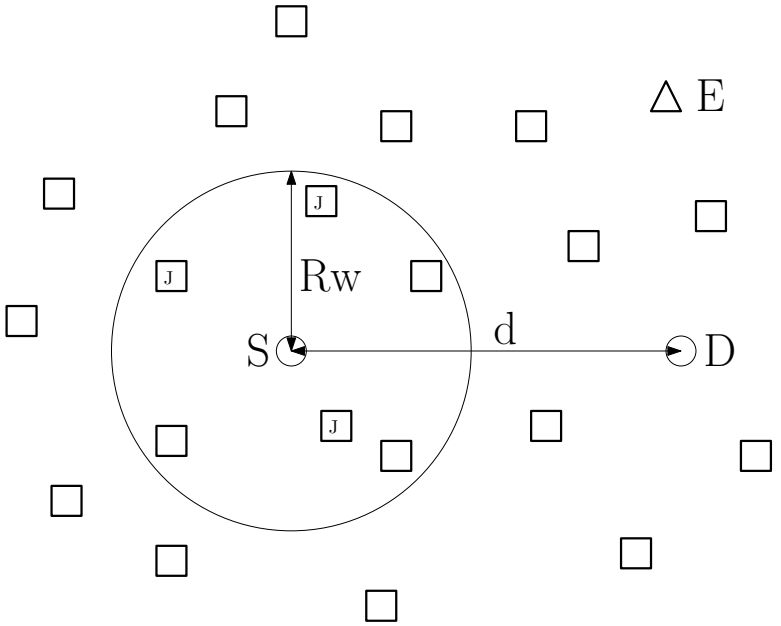

Figure 1: System Model

System Model: Received Signal

- The received signals at the intended destination and the eavesdropper can be written respectively as,

$$y_d = h_{sd} d_{sd}^{-\alpha/2} \sqrt{P_s} x + \sum_{j \in \phi_j, r_j \leq R_w} h_{jd} r_{jd}^{-\alpha/2} 1_{\{|h_{jd}|^2 < \epsilon\}} \sqrt{P_J} z_j + n_d, \quad (1)$$

$$y_e = h_{se} d_{se}^{-\alpha/2} \sqrt{P_s} x + \sum_{j \in \phi_j, r_j \leq R_w} h_{je} r_{je}^{-\alpha/2} 1_{\{|h_{jd}|^2 < \epsilon\}} \sqrt{P_J} z_j + n_e, \quad (2)$$

System Model: Received SINR

- The received signal-to-interference-plus-noise ratio (SINR) at the destination $SINR_d$ and eavesdropper $SINR_E$ are respectively given as,

$$SINR_d = \frac{|h_{sd}|^2 d_{sd}^{-\alpha} P_s}{\sigma^2 + \sum_{j \in \phi_j, r_j \leq R_w} |h_{jd}|^2 r_{jd}^{-\alpha} P_J 1_{\{|h_{jd}|^2 < \epsilon\}}} \tag{3}$$

- The the SINR at eavesdropper is given by

$$SINR_e = \frac{|h_{se}|^2 d_{se}^{-\alpha} P_s}{\sigma^2 + \sum_{j \in \phi_j, r_j \leq R_w} |h_{je}|^2 r_{je}^{-\alpha} P_J 1_{\{|h_{jd}|^2 < \epsilon\}}} \tag{4}$$

- Let us denote

$$I_d = \sum_{j \in \phi_j, r_j \leq R_w} |h_{jd}|^2 r_{jd}^{-\alpha} 1_{\{|h_{jd}|^2 < \epsilon\}} \tag{5}$$

$$I_e = \sum_{j \in \phi_j, r_j \leq R_w} |h_{je}|^2 r_{je}^{-\alpha} 1_{\{|h_{jd}|^2 < \epsilon\}} \tag{6}$$

System Model: Power consumption model

- Power consumption model:
  - Let P_c^s and P_c^J denote the circuit powers of source and jammer respectively. Let ε_{as} and ε_{aj} denotes the amplifier efficiencies of source and jammer, respectively. Thus, the total energy consumed is,

$$P_t = \frac{P_s}{\varepsilon_{as}} + P_c^s + \sum_{j \in \phi_j, r_j \leq R_w} \frac{P_J 1_{\{|h_{jd}|^2 < \epsilon\}}}{\varepsilon_{aj}} + \sum_{j \in \phi_j, r_j \leq R_w} P_c^J \tag{7}$$

  - As the selected number of jammers is not fixed, if there are N number of jamming nodes in set $\{j \in \phi_j, r_j \leq R_w\}$, then we can find the average of total power as

$$P_{tavg|N} = \mathbb{E}[P_t] = \frac{P_s}{\varepsilon_{as}} + P_c^s + \frac{N(1 - e^{-\epsilon})P_J}{\varepsilon_{aj}} + NP_c^J \tag{8}$$

$$P_{tavg} = \mathbb{E}[P_{tavg|N}] = \frac{P_s}{\varepsilon_{as}} + P_c^s + \pi R_w^2 \lambda \{\frac{(1 - e^{-\epsilon})P_J}{\varepsilon_{aj}} + P_c^J\} \tag{9}$$

System Model: Performance Metrics

- Successful decoding of information occurs at the legitimate destination when the capacity of the S to D channel is greater than or equal to $\mathcal{R}_t$. For perfect secrecy, the channel capacity of the S to E channel must be less than or equal to $\mathcal{R}_e$. Hence, we use two performance metrics: the coverage probability and secrecy probability as defined in [10], respectively

$$P_{cov} = P(SINR_d \geq \eta_T) \tag{10}$$

$$P_{sec} = P(SINR_e \leq \eta_E) \tag{11}$$

  where, $\eta_T = 2^{\mathcal{R}_t} - 1$ and $\eta_E = 2^{\mathcal{R}_e} - 1$.
- Hence, the secrecy transmission rate $\mathcal{R}$ is defined as [10]

$$\mathcal{R} = (\mathcal{R}_t - \mathcal{R}_e) P_{cov} P_{sec} \tag{12}$$

- SEE is calculated as

$$SEE = \frac{\mathcal{R}}{P_{tavg}} \tag{13}$$

Distance Distribution

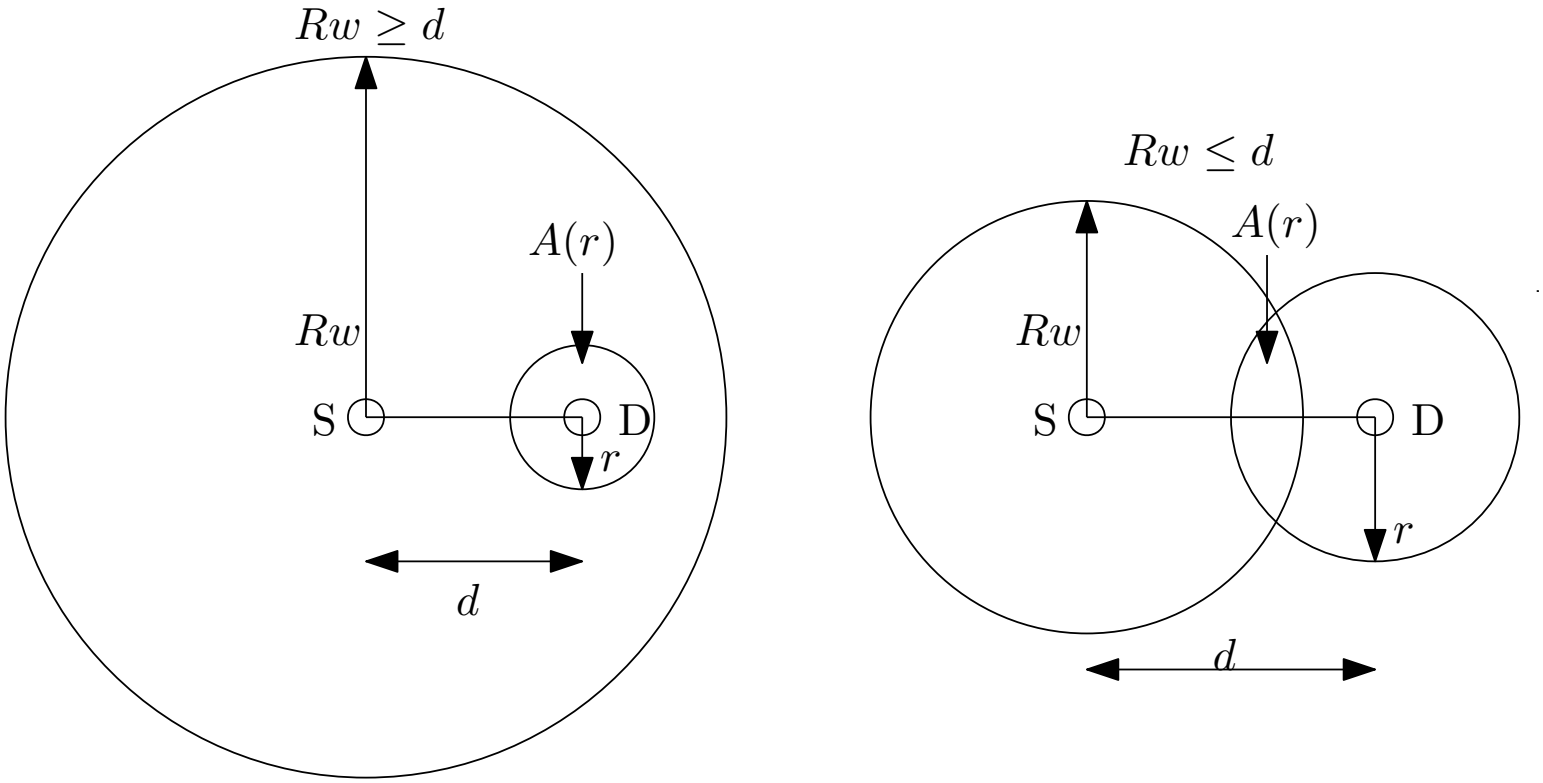

Figure 2: Geometrical cases for $f_R(r)$

Distance Distribution

- If $F_R(r)$ represents distribution function and $A(r)$ is the intersection area between the circular regions centered at source with radius R_w and another region centered at receiver with radius r, the density function $f_R(r)$ can be evaluated as

$$f_R(r) = \frac{d}{dr} F_R(r) = \frac{d}{dr} P\{R \leq r\} = \frac{d}{dr} \frac{A(r)}{\pi R_w^2} \tag{14}$$

- Case I: $R_w \geq d$

$$f_R(r) = \begin{cases} \dfrac{2r}{R_w^2}, & \text{if } 0 \leq r \leq R_w - d \\ g(r) & \text{if } R_w - d \leq r \leq R_w + d \\ 0, & \text{if } R_w + d \leq r \end{cases} \tag{15}$$

Distance Distribution

- Case II: $R_w \leq d$

$$f_R(r) = \begin{cases} g(r) & \text{if } d - R_w \leq r \leq d + R_w \\ 0, & \text{otherwise.} \end{cases} \tag{16}$$

where, $g(r)$ is given by

$$\begin{aligned} g(r) \quad = \frac{1}{\pi R_w^2} \Bigg\{ & \frac{R_w r}{d\sqrt{1 - \frac{(d^2+R_w^2-r^2)^2}{4d^2R_w^2}}} \\ & - \frac{r^2(\frac{1}{d} - \frac{d^2-R_w^2+r^2}{2dr^2})}{\sqrt{1 - \frac{(d^2-R_w^2+r^2)^2}{4d^2r^2}}} \\ & + 2rCos^{-1}(\frac{d^2 - R_w^2 + r^2}{2dr}) \\ & - \frac{d^2r + R_w^2 r - r^3}{\sqrt{(d + R_w)^2 - r^2)(r^2 - (d - R_w)^2)}} \Bigg\} \end{aligned} \tag{17}$$

Secrecy Performance Analysis

- The distance of any jammer from the receiver is independent of other jammers. $|h_{ab}|^2$ is exponentially distributed, and all channels are independent. Hence, P_{cov} can be evaluated a

$$
\begin{aligned}
P_{cov} &= P\left(\frac{|h_d|^2 d_{sd}^{-\alpha} P_s}{\sigma^2 + P_J I_d} \geq \eta_T\right) \\
&= P\left(|h_d|^2 \geq \frac{\eta_T d_{sd}^{\alpha}(\sigma^2 + P_J I_d)}{P_s}\right) \\
&= \mathbb{E}\left\{exp\left(-\frac{\eta_T d_{sd}^{\alpha}(\sigma^2 + P_J I_d)}{P_s}\right)\right\} \\
&= \left\{exp\left(-\frac{\eta_T d_{sd}^{\alpha}\sigma^2}{P_s}\right)\right\}\mathbb{E}\left\{exp\left(-\frac{\eta_T d_{sd}^{\alpha} P_J I_d}{P_s}\right)\right\} \\
&= \left\{exp\left(-\frac{\eta_T d_{sd}^{\alpha}\sigma^2}{P_s}\right)\right\}\mathbb{L}_{(I_d)}\{s\}, \qquad (18)
\end{aligned}
$$

Secrecy Performance Analysis

- If there are N number of helper nodes present in the circular region of radius R_w, the Laplace transform of interference $\mathbb{L}_{(I_d|N)}$, using $f_R(r)$ from (14), (15) and (16), $\mathbb{L}_{(I_d)}$ is given by

$$\mathbb{L}_{(I_d)|N}\{s\} = \left\{ \int_{r_{dl}}^{r_{du}} \{\frac{1 - e^{-\epsilon(1+sr^{-\alpha})}}{1 + sr^{-\alpha}} + e^{-\epsilon}\} f_R(r)\, \mathrm{d}r \right\}^N \tag{19}$$

- As the number of nodes present is a Poisson random variable, if the node density is λ, the unconditional Laplace transform of interference at the destination can be evaluated as

$$\begin{aligned}
\mathbb{L}_{(I_d)}\{s\} &= \mathbb{E}\{\mathbb{L}_{(I_d)|N}\{s\}\} \\
&= \sum_{N=0}^{\infty} \mathbb{L}_{(I_d)|N}\{s\} \frac{e^{-\pi R_w^2 \lambda} (\pi R_w^2 \lambda)^N}{N!} \\
&= exp\left\{ \pi R_w^2 \lambda \left(\int_{r_{dl}}^{r_{du}} \{\frac{1 - e^{-\epsilon(1+sr^{-\alpha})}}{1 + sr^{-\alpha}} + e^{-\epsilon}\} f_R(r)\, \mathrm{d}r - 1 \right) \right\}
\end{aligned} \tag{20}$$

Secrecy Performance Analysis

- Similarly, P_{sec} can be simplified as

$$P_{sec} = 1 - \{exp(-\frac{\eta_E d_e^{\alpha} \sigma^2}{P_s})\}\mathbb{L}_{(I_e)}\{s\} \tag{21}$$

and $\mathbb{L}_{(I_e)}$ is given by

$$\mathbb{L}_{(I_e)}\{s\} = exp\left\{\pi R_w^2 \lambda \left(\int_{r_{el}}^{r_{eu}} \{\frac{1 - e^{-\epsilon}}{1 + sr^{-\alpha}} + e^{-\epsilon}\} f_R(r)\, \mathrm{d}r - 1 \right) \right\} \tag{22}$$

Results and Discussions

- Various parameters used for simulation are listed in Table I.

Table 1: Simulation parameters

Parameter	Value
λ	0.1 m^{-2}
R_t	1 bps
R_e	0.5 bps
P_s	0.100 W
P_J	0.010 W
$Pcs = Pcj$	0.005 W
$\varepsilon_{as} = \varepsilon_{aj}$	0.8
α	3
d_{sd}	15 m
d_{se}	20 m
No	-70 dB

Results and Discussions

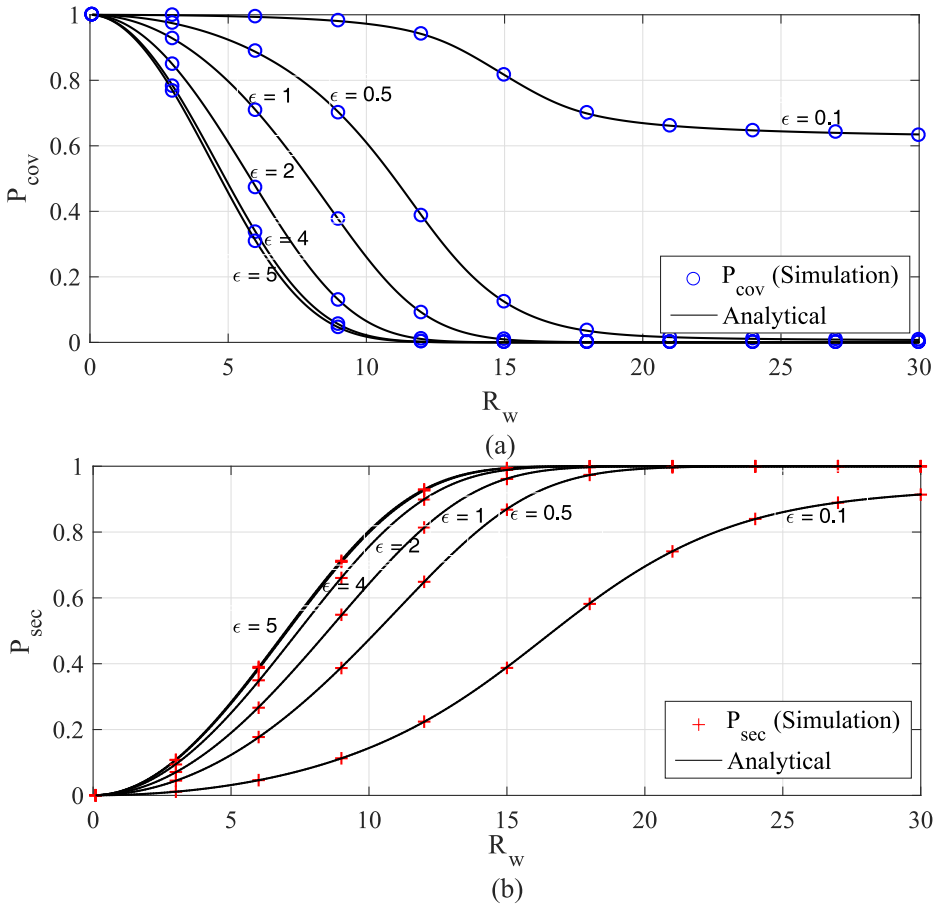

Figure 3: The coverage probability P_{cov} and secure communication probability P_{sec} as a function of R_w.

Results and Discussions

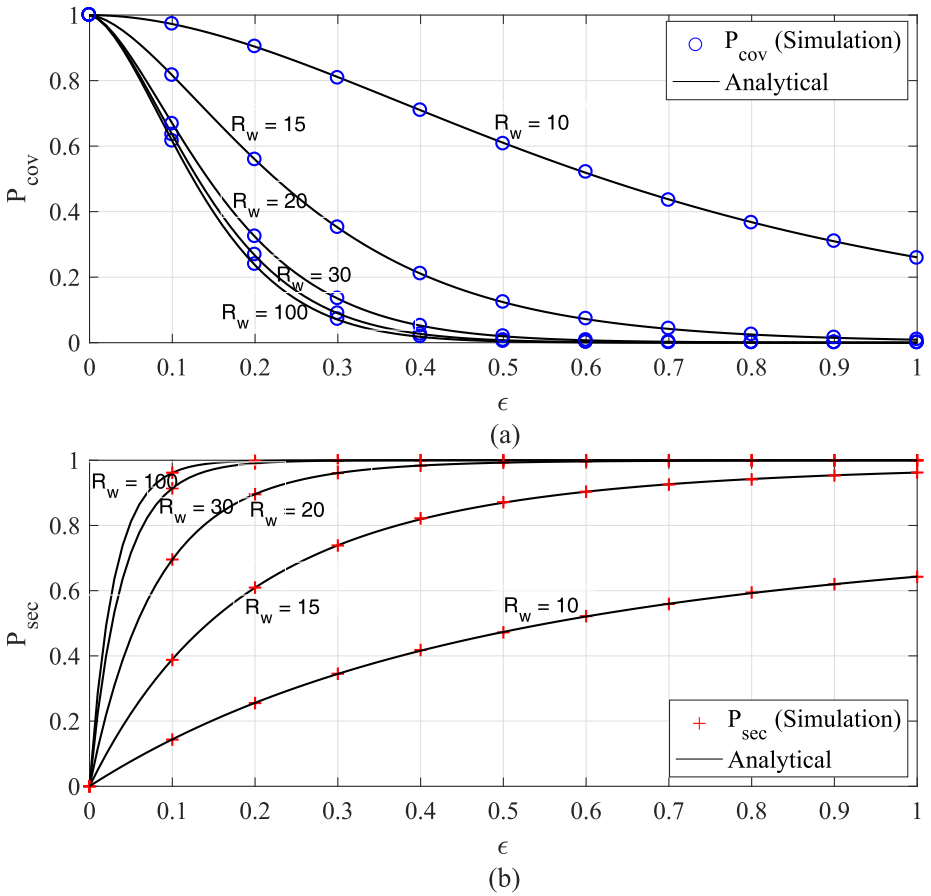

Figure 4: The coverage probability P_{cov} and secure communication probability P_{sec} as a function of ϵ.

Simulation Result

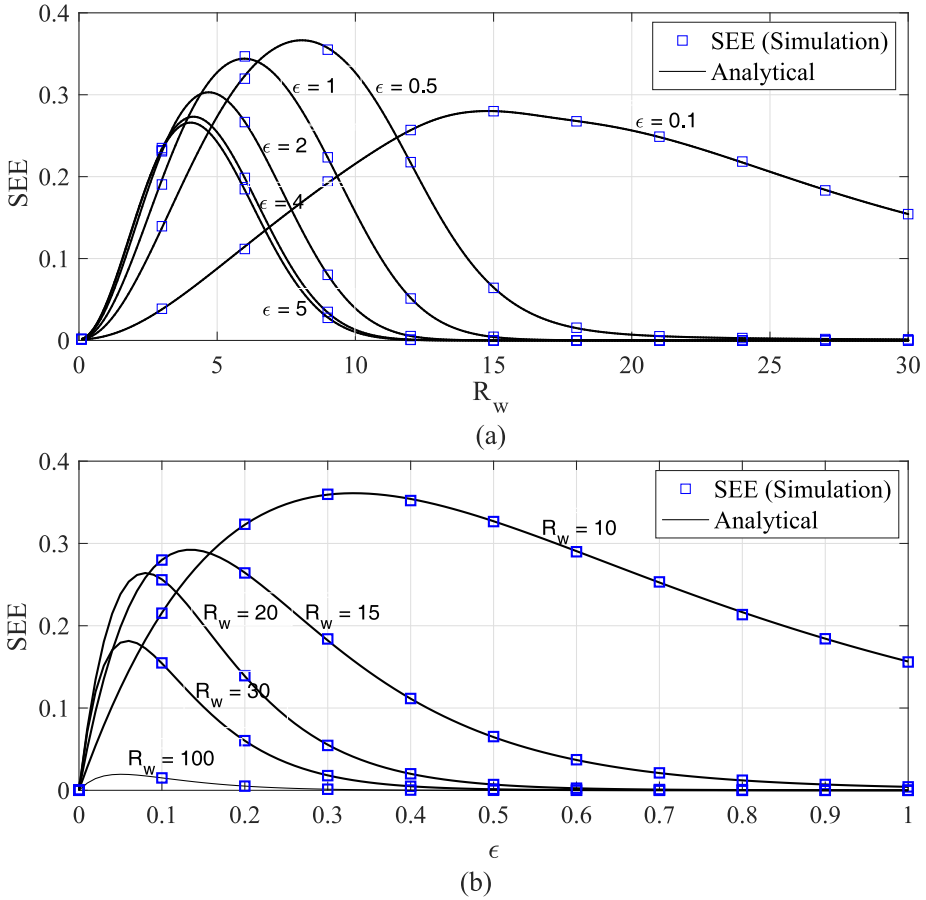

Figure 5: The SEE as a function of (a) R_w and (b) ϵ.

Conclusion

- We have studied the energy efficiency for a secure wireless network with the help of stochastically distributed friendly jammers.
- Here, we proposed a practical jammer selection method for UCJ. Jammers are selected in a finite area around the source to limit the power consumption.
- Our analysis shows that some optimal value of selection parameters exists at which SEE achieves maximum value.
- The SEE maximization and the effect of multiple stochastically distributed eavesdroppers on security and energy efficiency performance can be analyzed further.

References I

[1] G. Auer, V. Giannini, C. Desset, I. Godor, P. Skillermark, M. Olsson, M. A. Imran, D. Sabella, M. J. Gonzalez, O. Blume, and A. Fehske, "How much energy is needed to run a wireless network?," *IEEE Wireless Communications*, vol. 18, pp. 40–49, October 2011.

[2] C. E. Shannon, "Communication theory of secrecy systems," *The Bell System Technical Journal*, vol. 28, pp. 656–715, Oct 1949.

[3] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, pp. 1355–1387, Oct 1975.

[4] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Transactions on Wireless Communications*, vol. 7, pp. 2180–2189, June 2008.

[5] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Communications Surveys Tutorials*, vol. 16, pp. 1550–1573, Third 2014.

[6] C. Wang and H. Wang, "Opportunistic jamming for enhancing security: Stochastic geometry modeling and analysis," *IEEE Transactions on Vehicular Technology*, vol. 65, pp. 10213–10217, Dec 2016.

[7] X. Hu, P. Mu, B. Wang, and Z. Li, "On the secrecy rate maximization with uncoordinated cooperative jamming by single-antenna helpers," *IEEE Transactions on Vehicular Technology*, vol. 66, pp. 4457–4462, May 2017.

[8] P. Mu, X. Hu, B. Wang, and Z. Li, "Secrecy rate maximization with uncoordinated cooperative jamming by single-antenna helpers under secrecy outage probability constraint," *IEEE Communications Letters*, vol. 19, pp. 2174–2177, Dec 2015.

[9] Y. Huo, Y. Tian, L. Ma, X. Cheng, and T. Jing, "Jamming strategies for physical layer security," *IEEE Wireless Communications*, vol. 25, pp. 148–153, February 2018.

[10] H. Kong, P. Wang, D. Niyato, and Y. Cheng, "Physical layer security in wireless networks with ginibre point processes," *IEEE Transactions on Wireless Communications*, vol. 17, pp. 5132–5147, Aug 2018.

[11] C. Wang, H. Wang, X. Xia, and C. Liu, "Uncoordinated jammer selection for securing simome wiretap channels: A stochastic geometry approach," *IEEE Transactions on Wireless Communications*, vol. 14, pp. 2596–2612, May 2015.

[12] S. Luo, J. Li, and A. P. Petropulu, "Uncoordinated cooperative jamming for secret communications," *IEEE Transactions on Information Forensics and Security*, vol. 8, pp. 1081–1090, July 2013.

[13] J. P. Vilela, P. C. Pinto, and J. Barros, "Position-based jamming for enhanced wireless secrecy," *IEEE Transactions on Information Forensics and Security*, vol. 6, pp. 616–627, Sept 2011.

[14] M. El-Halabi, T. Liu, and C. N. Georghiades, "Secrecy capacity per unit cost," *IEEE Journal on Selected Areas in Communications*, vol. 31, pp. 1909–1920, Sep. 2013.

[15] A. Kalantari, S. Maleki, S. Chatzinotas, and B. Ottersten, "Secrecy energy efficiency optimization for miso and siso communication networks," in *2015 IEEE 16th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, pp. 21–25, June 2015.

[16] J. Farhat, G. Brante, and R. D. Souza, "On the secure energy efficiency of tas/mrc with relaying and jamming strategies," *IEEE Signal Processing Letters*, vol. 24, pp. 1228–1232, Aug 2017.

[17] E. Salbaroli and A. Zanella, "Interference analysis in a poisson field of nodes of finite area," *IEEE Transactions on Vehicular Technology*, vol. 58, pp. 1776–1783, May 2009.

Thank You!