Secure Energy Efficiency with Poisson Point Process Distributed Jammers

Kirti Kant Sharma
Bharti School of Telecomm. Technology & Mgmt.
Indian Institute of Technology, Delhi,
New Delhi-110016, India
kirtikant2012@gmail.com

Ranjan Bose
Department of Electrical Engineering
Bharti School of Telecomm. Technology & Mgmt.
Indian Institute of Technology, Delhi,
New Delhi-110016, India
rbose@ee.iitd.ac.in

***Abstract*—In this paper, we analyze a network consisting of a single source, legitimate destination and an eavesdropper in the presence of multiple helping nodes acting as friendly jammer to support secure communication. We propose a practical jamming method for uncoordinated cooperative jamming (UCJ) with less system overhead. Jammers are selected to secure the communication in an energy efficient way. We model the spatial distribution of jammers as a Poisson point process (PPP). Jammers are selected according to the source to destination channel quality within a finite region surrounding the source. The secrecy transmission rate of the network is evaluated from coverage probability and secrecy probability. The secure energy efficiency (SEE) of the system is analyzed by considering a more realistic power consumption model with the transmit power of various nodes as well as their circuit consumption power.**

***Index Terms*—Uncoordinated cooperative jamming, Poisson point process, physical layer security, secure energy efficiency.**

I. Introduction

The future of telecommunication networks is to connect a vast number of heterogeneous devices to the Internet of Things (IoT). The IoT will incorporate various wireless technologies. This inclusion of devices will possibly create the market for new services not only in daily life but also change the machine to machine communication. 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]. The security of communication is a critical issue due to the presence of energy efficient devices with low computational power in IoT, and application areas directly affect human life or productivity in industries. Usually, the security of communication is ensured using cryptographic techniques implemented at higher layers. These cryptographic methods rely on the assumption that the decryption will be difficult and take more time at an intruder. The limited capabilities of IoT devices make the implementations of security difficult. 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. Similar to artificial noise, co-operative jamming methods evolved for the wireless network having one or more helper nodes acting as friendly jammer to secure the communication. 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. 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.

Concerning energy consumption, the security of the network is studied to minimize total transmit power or maximize secrecy performance under power constraints. 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].

In this paper, we propose and analyze a UCJ jammer selection scheme based on channel threshold and selection

This research work is supported by the Visvesvaraya PhD Scheme of Ministry of Electronics & Information Technology, Government of India.

978-1-5386-4980-0/19/$31.00 ©2019 IEEE

region in case of PPP distributed helper nodes. We establish analytical formulation for performance evaluation of the proposed scheme with respect to obtained secrecy rate and energy efficiency. The analytical results to evaluate secrecy performance concerning the coverage probability and the secrecy probability are presented. Our results are verified with the numerical simulations and give insights to many aspects of jammer selection with respect to network parameters from the energy efficiency.

The remaining paper is organized as follows. The system model is explained in Section II. The distance distribution in case of the finite area is presented in Section III. In Section IV, the secrecy performance is analyzed. In Section V, analytical results are verified with simulation results, and discussed the efficacy of the proposed UCJ scheme with the change in selection parameters. Finally, this work is concluded in Section VI.

II. System Model

A. Network Model

Let us consider a distributed wireless network as shown in Fig. 1, with one source S, which wants to communicate securely with one destination D in the presence of an eavesdropper E. There are multiple helper nodes which are distributed randomly across the region uniformly, which act as friendly jammer. Each node in the network consists of only a single antenna. Here, we assume that the source and jammers obtain perfect channel state information (CSI) by the use of training sequence transmitted from the intended receiver. When the source wants to send information symbol to the legitimate destination, each of the selected jammers transmits independent Gaussian noise with constant power P_j. The eavesdropper also monitors the message signal.

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

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

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

where, x is the transmitted signal and h_{ab} denotes the channel coefficients from the transmitting node a to the receiving node b, distributed as $\mathcal{CN}(0,1)$. Here, $\mathcal{CN}(\mu, \sigma^2)$ denotes complex Gaussian distribution with mean μ and variance σ^2. $1_{\{|h_{jd}|^2 < \epsilon\}}$ is indicator function defined as $1_{\{|h_{jd}|^2 < \epsilon\}} = 1$ if $|h_{jd}|^2 < \epsilon$, and $1_{\{|h_{jd}|^2 < \epsilon\}} = 0$ otherwise. d_{sd} and d_{se} are the S to D and S to E distances, respectively. α is the channel path loss coefficient and ϵ is jammer selection threshold. ϕ_j denotes PPP model for the distribution of jammers and r_j is distance of jth jammer from the source. Here, we assume all the channels are independent and identically distributed quasi static Rayleigh fading. P_s is the source transmission power and P_J is the jammer's transmission power. z_j is AWGN transmitted by the jammer with distribution $\mathcal{CN}(0,1)$. n_k and n_E are the AWGN with distribution $\mathcal{CN}(0,\sigma^2)$.

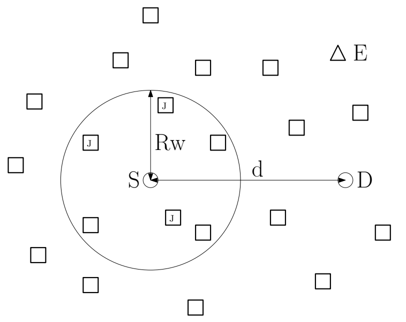


Fig. 1. System model

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

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

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

Let us denote

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

$$I_e = \sum_{j \in \phi_j, r_j \le R_w} |h_{je}|^2 r_{je}^{-\alpha} 1_{\{|h_{jd}|^2 < \epsilon\}}. \quad (6)$$

Successful decoding of information occurs at the legitimate destination when the capacity of the S to D channel is greater than or equal to the transmitted codeword rate $\mathcal{R}_t$. For perfect secrecy, the channel capacity of the S to E channel must be less than or equal to the rate loss for securing the confidential message $\mathcal{R}_e$. Hence, we are using the coverage probability and secrecy probability defined in [10] as performance metrics,

$$P_{cov} = P(SINR_d \ge \eta_T), \quad (7)$$

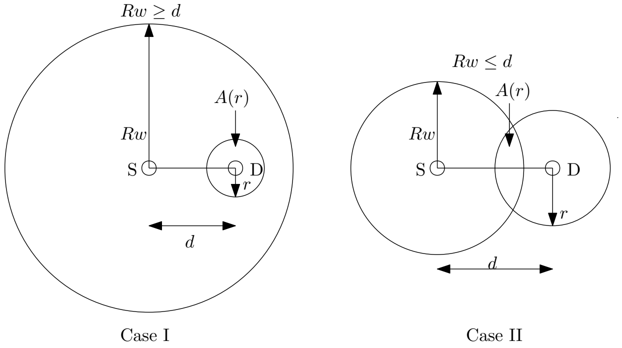
$$P_{sec} = P(SINR_e \le \eta_E), \quad (8)$$

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],

$$\mathcal{R} = (\mathcal{R}_t - \mathcal{R}_e) P_{cov} P_{sec}. \quad (9)$$

B. Power consumption model

Each node consumes power in two ways: the power consumed for the transmission of the signal and the power consumed in circuit components. It is assumed that, if a node is not participating in any of the communication stages, then there will be no power consumption by that node. Let



Case I

Case II

Fig. 2. Geometrical cases for $f_R(r)$

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,

$$P_t = \frac{P_s}{\varepsilon_{as}} + P_c^s + \sum_{j \in \phi_j, r_j \leq R_w} \frac{P_J 1_{\{|h_{jd}|^2 < \epsilon\}}}{\varepsilon_{aj}} + \sum_{j \in \phi_j, r_j \leq R_w} P_c^J. \tag{10}$$

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

$$P_{tavg|N} = \mathbb{E}[P_t] = \frac{P_s}{\varepsilon_{as}} + P_c^s + \frac{N(1-e^{-\epsilon})P_J}{\varepsilon_{aj}} + NP_c^J, \tag{11}$$

$$P_{tavg} = \mathbb{E}[P_{tavg|N}] = \frac{P_s}{\varepsilon_{as}} + P_c^s + \pi R_w^2 \lambda \{\frac{(1-e^{-\epsilon})P_J}{\varepsilon_{aj}} + P_c^J\}, \tag{12}$$

where, λ is node density and R_w is the radius of region in which jammers are selected. SEE is calculated using (9) and (12) as

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

III. Distance Distribution

As jammers are distributed randomly according to the PPP, their distance from the receiving node is a random variable. Let r is the distance between the receiving node which may be the D or E, and a jammer which is present in a circular region of radius R_w centered at the source. Let d is the distance between S and receiving node (D or E). 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 with another region centered at receiver with radius r, the density function $f_R(r)$ can be evaluated as,

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

$f_R(r)$ is given by
Case I: $R_w \geq d$

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

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

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

IV. 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

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

where, $s = \frac{\eta_T d_{sd}^{\alpha} P_J}{P_s}$ and $\mathbb{L}_X(s) = \mathbb{E}\{exp(-sX)\}$ is the Laplace Transformation of X. 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

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

where, r_{dl} and r_{du} are chosen according to the choice of $f_R(r)$. 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 is evaluated as,

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

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

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

where, $s = \frac{\eta_E d_e^{\alpha} P_J}{P_s}$, and, r_{el} and r_{eu} are chosen according to the choice of $f_R(r)$. The integrals in (20) and (22) can be efficiently evaluated by numerical methods.

V. Results and Discussions

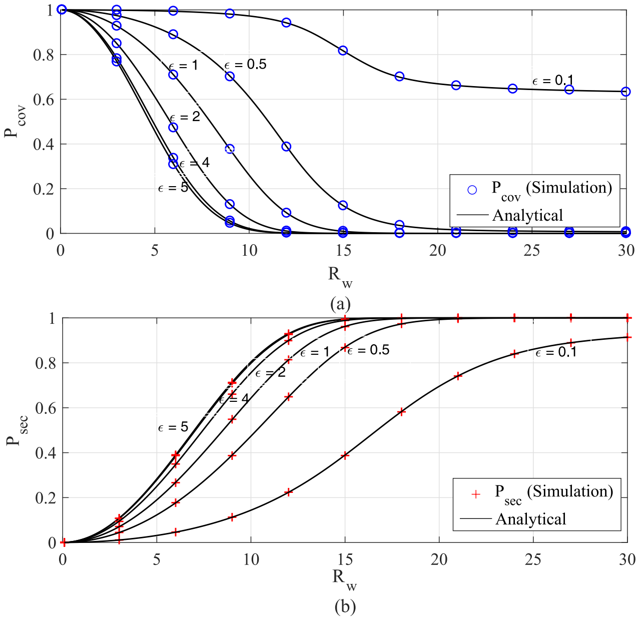
In this section, we verify the analytical results obtained in the previous section with numerical simulations. The average results are obtained over 10^5 independent realizations of channel and point process. Various parameters used for simulation are listed in Table I.

TABLE I
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
$P_c^s = P_c^J$	0.005 W
$\varepsilon_{as} = \varepsilon_{aj}$	0.8
α	3
d_{sd}	15 m
d_{se}	20 m
No	-70 dB

In Fig. 3(a) and (b), P_{cov} and P_{sec} are plotted with respect to (w.r.t.) R_w for various values of selection threshold ϵ. It can be observed that the analysis is well supported by simulation results. P_{cov} decreases slowly for smaller values of ϵ because the number of jammers selected is less. For large values of ϵ, P_{cov} decreases at a faster rate as more number of jammers are selected for the small value of R_w and more jamming noise is received by any receiving node. Similarly, P_{sec} increases for various values of ϵ. It can be observed for a large value of ϵ, plots become steeper and tend to saturate as most of the jammers will be selected for higher values of ϵ.

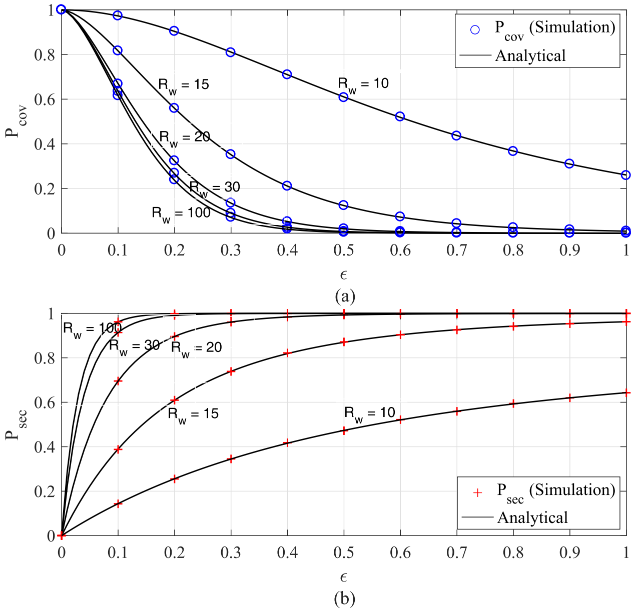
In Fig. 4(a) and (b), P_{cov} and P_{sec} are plotted w.r.t. ϵ for various values of selection region defined by R_w. It can be seen that for a smaller value of R_w, P_{cov} decreases and P_{sec} increases slowly as the available number of jammers are selected within a smaller region. On the other hand, when a large number of jammers are available in a wider area, curves for P_{cov} decreases rapidly and increases in case of P_{sec}. It is also observed that after reaching enough value of R_w, curves tend to saturate. It happens due to the selection of jammers at a far distance do not affect a receiving node significantly.



(a)

(b)

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

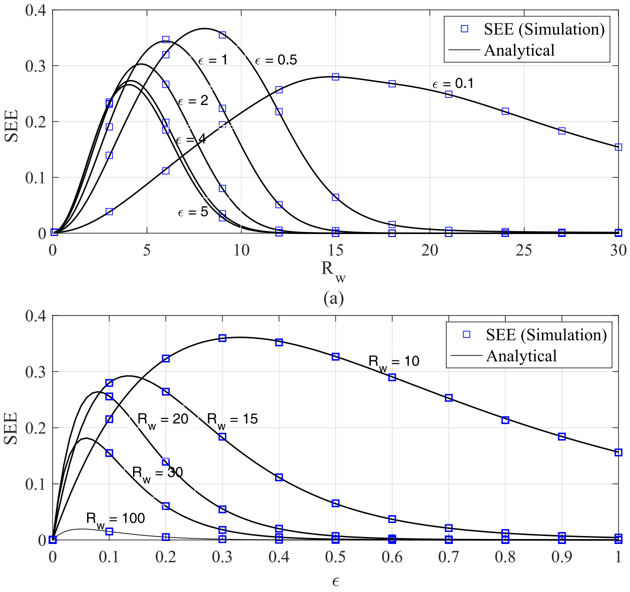


(a)

(b)

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

In Fig. 5(a), SEE is plotted as the function of R_w for various values of ϵ. It can be observed that for any given value of ϵ, SEE first increases up to certain value and then decreases with increase in R_w. As SEE is the ratio of secure throughput and power consumed, it increases until power consumption by selected jammers is small. When R_w is sufficiently large,



(b)

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

power consumption by selected jammers starts dominating and SEE starts decreasing. A similar trend is followed by the curves of SEE as the function of ϵ for any given value of R_w. It is obvious from the SEE curves that there exist some optimal value of R_w and ϵ for which SEE is maximum.

VI. Conclusion

In this paper, we 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. Our analysis is well matched with simulation results. The SEE maximization and the effect of multiple stochastically distributed evesdroppers on security and energy efficiency performance can be analyzed further.

References

[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.