International Journal of Power Electronics and Drive System (IJPEDS)
Vol. 11, No. 2, June 2020, pp. 879~885
ISSN: 2088-8694, DOI: 10.11591/ijpeds.v11.i2.pp879-885

Jammer against eavesdropper in half-duplex energy harvesting cooperative relaying networks: secrecy outage probability analysis

Phu Tran Tin[1], Duy Hung Ha[2], Minh Tran[3], Tran Thanh Trang[4]
[1] Faculty of Electronics Technology, Industrial University of Ho Chi Minh City, Vietnam
[2] Wireless Communications Research Group, Faculty of Electrical and Electronics Engineering, Ton Duc Thang University, Ho Chi Minh City, Vietnam
[3] Optoelectronics Research Group, Ton Duc Thang University, Vietnam
[4] National Key Laboratory of Digital Control and System Engineering, Vietnam

Article Info

Article history:

Received Jul 24, 2019
Revised Nov 9, 2019
Accepted Dec 5, 2019

Keywords:

Energy harvesting (EH)
Half-Duplex (HD)
Monte carlo simulation
Relaying network
Secrecy outage probability

ABSTRACT

In this paper, we have investigated the Half-Duplex (HD) Energy Harvesting (EH) Cooperative Relaying Networks with one source node, one destination node, one intermediate relay and in the presence of the Jammer Against Eavesdropper. We have analyzed the system performance in terms of the integral form expression of secrecy outage probability. In addition, we have investigated the effect of source rate, time switching factor, energy coefficient, and the ratio Ps/N0 on the system performance. Finally, all the mathematical, analytical expressions are verified by Monte Carlo simulation, and the analytical results match well with the simulation ones to convince the correctness of the analytical expression.

Corresponding Author:

Duy-Hung Ha,
Wireless Communications Research Group
Faculty of Electrical and Electronics Engineering
Ton Duc Thang University, Ho Chi Minh City, Vietnam
Email: haduyhung@tdtu.edu.vn

1. INTRODUCTION

Nowadays, harvesting energy (EH) from green environmental solar, wind, geothermal, and mechanical, the radio frequency (RF) signals can be considered as the prospective energy source in the future. RF signals can be proposed as the role of information transmission or harvesting energy in the communication network [1-8]. In a traditional network, the security problem to protect the wireless communication network is based on cryptographic technologies. Nowadays, the physical layer security (PLS) with the new technology is considered as an extensive research direction to protect the modern communication network. PLS technology is considered as a novel way to protect the confidential communication from a source node to its destination in the wireless cooperative communication network as studied in [9, 10]. In various system network such as cooperative relaying, jamming, multiuser scheduling, multiple-input-multiple-output (MIMO) with using PLS is considered in [11-15].

In this paper, we have proposed and investigated the Jammer Against Eavesdropper In Half-Duplex (HD) Energy Harvesting (EH) Cooperative Relaying Networks with one source node, one destination node, one intermediate relay, and in the presence of the Jammer Against Eavesdropper. We have analyzed the system performance in terms of the integral form expression of secrecy outage probability. In addition, we have investigated the effect of source rate, time switching factor, energy coefficient, and the ratio P_s/N_0 on the system performance. Finally, all the mathematical, analytical expressions are verified by Monte Carlo simulation, and the analytical results match well with the simulation ones to convince the correctness of the analytical expression. The main contribution of this research can be formulated as the following

a. The integral form of expression of secrecy outage probability is derived.
b. The effect of source rate, time switching factor, energy coefficient, and the ratio Ps/N0 on the system performance is demonstrated.
c. The Monte Carlo simulation is conducted to verify the correctness of the analytical expressions.

2. SYSTEM MODEL

We consider a communication scenario with the help of a friendly jammer (J), as illustrated in Figure 1. The EH and IT processing are proposed in Figure 2. In this scheme, T is the block time in which the source fully transmits the information data to the destination. In the first interval time (αT), the R and J harvest energy from the S signal, where α is the time switching factor α ∈ (0, 1) In the two remaining intervals time (1-α)T/2, the S and R node transfer information to the D node [5-7, 16-24].

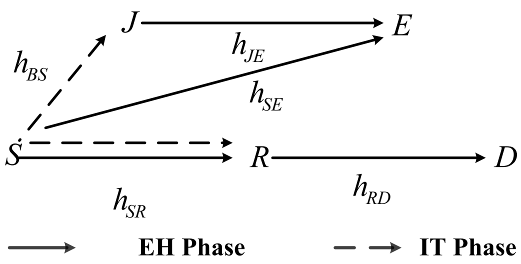

Figure 1. System model

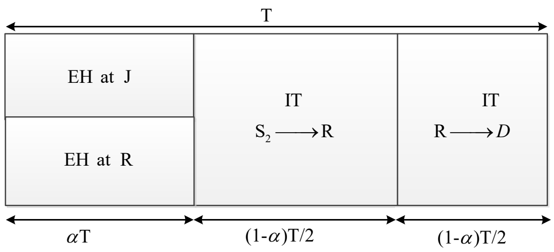

Figure 2. The EH and IT phases.

2.1. Energy harvesting phase

In the first phase, the source will supply the energy for both jammer and relay nodes. Hence, the harvested energy at the jammer and relay can be given as, respectively

$$E_J = \eta P_S \alpha T |h_{SJ}|^2 \quad (1)$$
$$E_R = \eta P_S \alpha T |h_{SR}|^2 \quad (2)$$

The average transmitted power at the jammer and relay nodes can be obtained from (1) and (2), respectively

$$P_J = \frac{E_J}{(1-\alpha)T/2} = \frac{\eta P_S \alpha T |h_{SJ}|^2}{(1-\alpha)T/2} = kP_S |h_{SJ}|^2 \quad (3)$$
$$P_R = kP_S |h_{SR}|^2 \quad (4)$$

Where $k = \frac{2\eta\alpha}{1-\alpha}$

2.2. Information transmission phase

In the second phase, the received signal at the relay can be rewritten as

$$y_r = h_{SR} x_s + n_r \quad (5)$$

Where h_{SR} is the channel gain of S-R link, x_s is the transmitted signal from source and n_r is additive white Gaussian noise (AWGN) with variance N_0 and $E\{|x_s|^2\} = P_S$ which $E\{\bullet\}$ is expectation operator.
In the third phase, the received signal at the destination can be given by

$$y_d = h_{RD} x_r + n_d \quad (6)$$

Where h_{RD} is the channel gain of R-D link, x_r is the transmitted signal from relay and n_d is (AWGN) with variance N_0 and $E\{|x_r|^2\} = P_R$

Here, we consider amplify and forward (AF) mode at the relay. Hence, the amplify factor can be given as

$$\delta = \frac{x_r}{y_r} = \sqrt{\frac{P_R}{P_S|h_{SR}|^2+N_0}} \quad (7)$$

Substituting (7) into (6), we have:

$$y_d = h_{RD}\delta y_r = h_{RD}\delta[h_{SR}x_s + n_r] + n_d = \underbrace{h_{SR}h_{RD}\delta x_s}_{signal} + \underbrace{h_{RD}\delta n_r + n_d}_{noise} \quad (8)$$

From (8), the end to end signal to noise ratio (SNR) of S-R-D link can be calculated as

$$\gamma_{SRD} = \frac{E\{|signal|^2\}}{E\{|noise|^2\}} = \frac{|h_{SR}|^2|h_{RD}|^2\delta^2 P_S}{|h_{RD}|^2\delta^2 N_0+N_0} = \frac{|h_{SR}|^2|h_{RD}|^2 P_S}{|h_{RD}|^2 N_0+\frac{N_0}{\delta^2}} \quad (9)$$

After doing some algebra and using the fact that $N_0 << P_R$, (9) can be rewritten as

$$\gamma_{SRD} = \frac{|h_{SR}|^2|h_{RD}|^2 P_S P_R}{P_R|h_{RD}|^2 N_0+N_0 P_S|h_{SR}|^2} \quad (10)$$

Substituting (3) and (4) into (10), the end to end SNR can be reformulated as

$$\gamma_{SRD} = \frac{k\Phi|h_{SR}|^2|h_{RD}|^2}{k|h_{RD}|^2+1} = \frac{k\Phi XY}{kY+1} \quad (11)$$

Where $\Phi = \frac{P_S}{N_0}, X = |h_{SR}|^2, Y = |h_{RD}|^2$

3. OUTAGE PROBABILITY (OP)

The received signal at the eavesdropper can be given by

$$y_E = h_{SE}x_s + h_{JE}x_J + n_E \quad (12)$$

Where h_{SE} is the channel gain of S-E link and n_E is AWGN with variance N_0 and $E\left\{\left|x_J\right|^2\right\} = P_J$

To protect information from being eavesdropped by E, the friendly jammer J performs jamming. Hence, the SNR at the eavesdropper can be expressed as

$$\gamma_E = \frac{|h_{SE}|^2 P_S}{P_J\left|h_{JE}\right|^2+N_0} \quad (13)$$

Substituting (3) and (4) into (13), we have:

$$\gamma_E = \frac{\Phi|h_{SE}|^2}{\kappa\Phi\left|h_{SJ}\right|^2\left|h_{JE}\right|^2+1} = \frac{\Phi Z}{\kappa\Phi V+1} \quad (14)$$

Where $Z = |h_{SE}|^2, V = \left|h_{SJ}\right|^2\left|h_{JE}\right|^2$

Next, the channel capacity of S-R-D and of eavesdropper can be obtained as, respectively

$$R_{SRD} = \frac{(1-\alpha)}{2}log_2(1+\gamma_{SRD}) \quad (15)$$

$$R_E = \frac{(1-\alpha)}{2}log_2(1+\gamma_E) \quad (16)$$

Lemma 1. The cumulative distribution function of V can be computed as

$$F_V(a) = \int_0^\infty F_{|h_{SJ}|^2}\left(\frac{a}{|h_{JE}|^2}\,|\,|h_{JE}|^2 = x\right) f_{|h_{JE}|^2}(x)dx \tag{17}$$

Utilizing the result in [25], the CDF of X and Y can be shown as the below (18)

$$F_V(a) = 1 - 2\sqrt{\lambda_{SJ}\lambda_{JE}a}K_1\left(2\sqrt{\lambda_{SJ}\lambda_{JE}a}\right) \tag{18}$$

where $K_v(\bullet)$is the modified Bessel function of the second kind and vth order and $\lambda_{SJ}, \lambda_{JE}$ are mean of random variables (RVs) $|h_{SJ}|^2, |h_{JE}|^2$, respectively.

From (18), the probability density function (PDF) of V can be calculated as, after applying the following formula $\frac{\partial K_n(z)}{\partial z} = -K_{n-1}(z) - \frac{n}{z}K_n(z)$

$$f_V(a) = \frac{\partial F_V(a)}{\partial a} = 2\sqrt{\lambda_{SJ}\lambda_{JE}}K_0\left(2\sqrt{\lambda_{SJ}\lambda_{JE}a}\right) \tag{19}$$

3.1. Secrecy Outage probability (SOP)

The Secrecy capacity of the system can be defined as

$$R = max(0, R_{SRD} - R_E) = \left[log_2\left(\frac{1+\gamma_{SRD}}{1+\gamma_E}\right)\right]^+ \tag{20}$$

Where $[x]^+ = max(0, x)$
The SOP can be formulated by

$$SOP = Pr(R < R_s) = Pr\left(\frac{1+\gamma_{SRD}}{1+\gamma_E} < \rho\right) = Pr(\gamma_{SRD} < \rho + \rho\gamma_E - 1)$$
$$= \int_0^\infty F_{\gamma_{SRD}}(\rho + \rho\gamma_E - 1|\gamma_E = x)f_{\gamma_E}(x)dx \tag{21}$$

Where $\rho = 2^{R_s}$ and R_s is source rate.

In order to calculate the probability in (21), we have to find $F_{\gamma_{SRD}}(a)$ and $f_{\gamma_E}(b)$
At first, we have:

$$F_{\gamma_{SRD}}(a) = Pr(\gamma_{SRD} < a) \tag{22}$$

Substituting (11) into (22), (22) can be rewritten as

$$F_{\gamma_{SRD}}(a) = Pr\left(\frac{k\Phi XY}{kY+1} < a\right) = Pr\left(X < \frac{a}{\Phi} + \frac{a}{k\Phi Y}\right)$$
$$= \int_0^\infty F_X\left(\frac{a}{\Phi} + \frac{a}{k\Phi Y}|Y = y\right) f_Y(y)dy$$
$$= \int_0^\infty \left(1 - exp\left[-\lambda_{SR}\left(\frac{a}{\Phi} + \frac{a}{k\Phi y}\right)\right]\right) f_Y(y)dy$$
$$= 1 - \lambda_{RD}\, exp\left(-\frac{\lambda_{SR}a}{\Phi}\right)\int_0^\infty exp\left(-\frac{\lambda_{SR}a}{k\Phi y}\right) \times exp(-\lambda_{RD}y)\, dx \tag{23}$$

Where $\lambda_{SR}, \lambda_{RD}$ are the mean of RVs$|h_{SR}|^2, |h_{RD}|^2$, respectively.
Apply equation [3.324,1] of the table of integral, we can obtain as followings

$$F_{\gamma_{SRD}}(a) = 1 - 2\, exp\left(-\frac{\lambda_{SR}a}{\Phi}\right)\sqrt{\frac{\lambda_{SR}\lambda_{RD}a}{k\Phi}} \times K_1\left(2\sqrt{\frac{\lambda_{SR}\lambda_{RD}a}{k\Phi}}\right) \tag{24}$$

Next, combine with (14), the CDF of γ_E can be given by

$$F_{\gamma_E}(x) = Pr(\gamma_E < x) = Pr\left(\frac{\Phi Z}{\kappa\Phi V + 1} < x\right) = Pr\left(Z < \frac{x}{\Phi} + kxV\right)$$
$$= \int_0^\infty F_Z\left(\frac{x}{\Phi} + kxV|V = y\right) f_V(y)dy \tag{25}$$

Applying the result from (19), equation (25) can be computed as

$$F_{\gamma_E}(x) = 2\sqrt{\lambda_{SJ}\lambda_{JE}}\int_0^\infty \left\{1 - exp\left[-\lambda_{SE}\left(\frac{x}{\Phi} + kxy\right)\right]\right\} \times K_0\left(2\sqrt{\lambda_{SJ}\lambda_{JE}y}\right)dy$$

$$= 1 - 2\sqrt{\lambda_{SJ}\lambda_{JE}}\, exp\left(-\frac{\lambda_{SE}x}{\Phi}\right)\int_0^\infty exp(-kx\lambda_{SE}y) \times K_0\left(2\sqrt{\lambda_{SJ}\lambda_{JE}y}\right)dy \quad (26)$$

Where λ_{SE} is the mean of RV$|h_{SE}|^2$
Applying Taylor series as follows

$$exp(-kx\lambda_{SE}y) = \sum_{n=0}^\infty \frac{(-kx\lambda_{SE}y)^n}{n!} = \sum_{n=0}^\infty \frac{(-1)^n(kx\lambda_{SE})^n}{n!}y^n \quad (27)$$

Substituting (27) into (26), we have:

$$F_{\gamma_E}(x) = 1 - 2\sqrt{\lambda_{SJ}\lambda_{JE}}\, exp\left(-\frac{\lambda_{SE}x}{\Phi}\right) \times \sum_{n=0}^\infty \frac{(-1)^n(kx\lambda_{SE})^n}{n!}\int_0^\infty y^n \times K_0\left(2\sqrt{\lambda_{SJ}\lambda_{JE}y}\right)dy \quad (28)$$

By changing variable $t = \sqrt{y}$ and then applying equation [6.561,16] of table of integral, equation (28) can be reformulated as

$$F_{\gamma_E}(x) = 1 - \sum_{n=0}^\infty \frac{(-1)^n(kx\lambda_{SE})^n}{n!(\lambda_{SJ}\lambda_{JE})^{n+1/2}} \times exp\left(-\frac{\lambda_{SE}x}{\Phi}\right) \times [\Gamma(n+1)]^2 \quad (29)$$

From (30), the PDF of γ_E can be obtained as

$$f_{\gamma_E}(x) = \frac{\partial F_{\gamma_E}(x)}{\partial x} = \sum_{n=0}^\infty \frac{(-1)^n(kx)^n(\lambda_{SE})^{n+1}}{n!\,(\lambda_{SJ}\lambda_{JE})^{n+1/2}\Phi} \times exp\left(-\frac{\lambda_{SE}x}{\Phi}\right) \times [\Gamma(n+1)]^2$$

$$-\sum_{n=0}^\infty \frac{(-1)^n(k\lambda_{SE})^n x^{n-1}}{(n-1)!(\lambda_{SJ}\lambda_{JE})^{n+1/2}} \times exp\left(-\frac{\lambda_{SE}x}{\Phi}\right) \times [\Gamma(n+1)]^2 \quad (30)$$

Applying results from (23) and (30) for (21), finally the SOP can be claimed by

$$SOP = \int_0^\infty \left\{1 - 2\, exp\left(-\frac{\lambda_{SR}[\rho+\rho x-1]}{\Phi}\right)\sqrt{\frac{\lambda_{SR}\lambda_{RD}[\rho+\rho x-1]}{k\Phi}} \times K_1\left(2\sqrt{\frac{\lambda_{SR}\lambda_{RD}[\rho+\rho x-1]}{k\Phi}}\right)\right\} f_{\gamma_E}(x)dx \quad (31)$$

4. NUMERICAL RESULTS AND DISCUSSION

In this section, the effect of source rate, time switching factor, energy coefficient, and the ratio P_s/N_0 on the system performance is investigated. The SOP versus the source rate R_S is plotted in Figure 3 with the main system parameters as ϕ= 5 Db, η=0.8 and α=0.25, 0.5, 0.85. As shown in Figure 3, the SOP significantly increases while the source rate increases from 0 to 6 bps/Hz. Figure 4 presents the influence of ϕ on the system SOP. In Figure 4, we set η=0.8, α=0.5 and R_S= 0.5, 1.0, 1.5 bps/Hz, respectively. From the results, we can see that the system SOP crucially falls down with the rising of ϕ from 0 to 30 dB. In Figure 3 and Figure 4, the simulation results match well with the analytical ones for verifying the correctness of the system performance analysis.

The effect of the energy efficiency coefficient on the system SOP is illustrated in Figure 5, in which we set α=0.5, R_S=0.5 bps/Hz, ϕ=1, 5,10 dB, respectively. Here, we can state that the system SOP has fallen down when η varies from 0 to 1. Furthermore, the system SOP versus time switching factor α is drawn in Figure 6. We set ϕ=5 dB, R_S=0.5 bps/Hz, and η=0.25, 0.5, 1, respectively. The same as the above case, the system SOP decreases massively with the rising of α from 0 to 1. As shown in Figure 5 and Figure 6, the analytical and the simulation results are the same to convince the analytical system performance analysis.

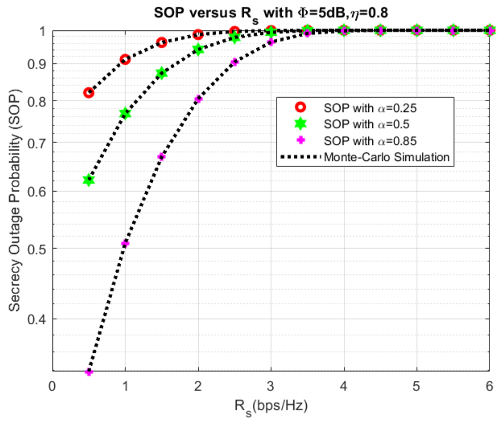

Figure 3. SOP versus R_S.

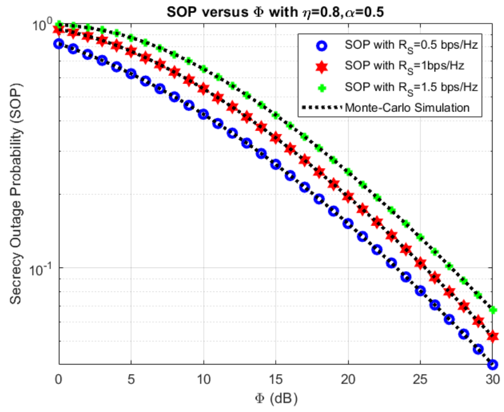

Figure 4. SOP versus ϕ.

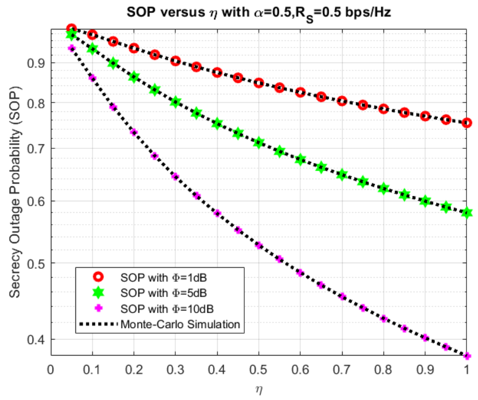

Figure 5. SOP versus η.

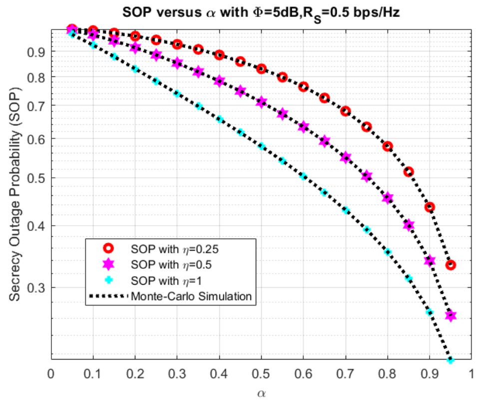

Figure 6. SOP versus α.

5. CONCLUSION

In this paper, we have investigated the HD EH Cooperative Relaying Networks in the presence of the Jammer Against Eavesdropper. We have analyzed the system performance in terms of the integral form expression of secrecy outage probability. In addition, we have investigated the effect of source rate, time switching factor, energy coefficient, and the ratio P_s/N_0 on the system performance. Finally, all the mathematical, analytical expressions are verified by Monte Carlo simulation, and the analytical results match well with the simulation ones to convince the correctness of the analytical expression.

ACKNOWLEDGMENTS

This research was supported by National Key Laboratory of Digital Control and System Engineering (DCSELAB), HCMUT, VNU-HCM, Vietnam.

REFERENCES

[1] Bi, S., Ho, C. K., & Zhang, "R. wireless powered communication: Opportunities and challenges," *IEEE Communications Magazine*, vol. 53, no. 4, pp. 117-125, 2015.
[2] Niyato, D., Kim, D. I., Maso, M., & Han, Z., "Wireless powered communication networks: research directions and technological approaches," *IEEE Wireless Communications*, vol. 24, no. 6, pp. 2-11, 2017.
[3] Yu, H., Lee, H., & Jeon, H, "What is 5G? Emerging 5G mobile services and network requirements. sustainability," *Sustainability*, vol. 9, no. 10, pp. 1838, 2017.
[4] Zhou, Xun, Rui Zhang, and Chin Keong Ho, "Wireless information and power transfer: architecture design and rate-energy tradeoff," *2012 IEEE Global Communications Conference (GLOBECOM)*, pp. 3982-3987, 2012.

[5] Tan N. Nguyen, T.H.Q.Minh, Phuong T. Tran, Miroslav Voznak, T.T.Duy, Thanh-Long Nguyen and Phu Tran Tin, "Performance enhancement for energy harvesting based Two-Way relay protocols in wireless Ad-hoc networks with partial and full relay selection methods," *Ad hoc networks*, vol. 84, pp. 178-187, Mar.2019.

[6] Tan N. Nguyen, T.H.Q. Minh, Phuong T. Tran and Miroslav Voznak, "Energy harvesting over rician fading channel: A performance analysis for Half-Duplex bidirectional sensor networks under hardware impairments," *Sensors*, vol. 18, no. 6, pp. 1781, 2018.

[7] Tan N. Nguyen, T.H.Q. Minh, Phuong T. Tran and Miroslav Voznak, "Adaptive energy harvesting relaying protocol for Two-Way half duplex system network over rician fading channels," *Wireless Communications and Mobile Computing*, vol. 2018, pp. 1-10, 2018.

[8] Bhatnagar, M. R., "On the capacity of Decode-and-Forward relaying over rician fading channels," *IEEE Communications Letters*, vol. 17, no. 6, pp. 1100-1103, 2013.

[9] Shannon, C. E., "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656-715, 1949.

[10] Li, Bin, Yulong Zou, Jianjiang Zhou, Fei Wang, Weifeng Cao, and Yu-Dong Yao, "Secrecy outage probability analysis of friendly jammer selection aided multiuser scheduling for wireless networks," *IEEE Transactions on Communications*, vol. 67, no. 5, pp. 3482-3495, 2019.

[11] Alemdar, Ali, and Mohamed Ibnkahla., "A Survey of wireless sensor networks: Technologies, challenges, and future trends," *Adaptation and Cross Layer Design in Wireless Networks*, pp. 243-262, 2018.

[12] Zhang, Yajun, *et al*, "Joint transmit antenna selection and jamming for security enhancement in MIMO Wiretap channels," *2015 IEEE/CIC International Conference on Communications in China (ICCC)*, pp. 1-6, 2015.

[13] Cumanan, Kanapathippillai, Zhiguo Ding, Bayan Sharif, Gui Yun Tian, and Kin K. Leung, "Secrecy rate optimizations for a MIMO Secrecy channel with a Multiple-Antenna eavesdropper," *IEEE Transactions on Vehicular Technology*, vol. 63, no. 4, pp. 1678-1690, 2014.

[14] Mukherjee, Pritam, and Sennur Ulukus, "Secrecy in MIMO networks with no eavesdropper CSIT." *IEEE Transactions on Communications*, vol. 65, no. 10, pp. 4382-4391, 2017.

[15] Chu, Zheng, Kanapathippillai Cumanan, Zhiguo Ding, Martin Johnston, and Stephane Y. Le Goff, "Secrecy rate optimizations for a MIMO secrecy channel with a cooperative jammer," *IEEE Transactions on Vehicular Technology,* vol. 64, no. 5, pp. 1833-1847, 2015.

[16] Ju, Hyungsik, *et al*, "Catching Resource-devouring worms in Next-generation wireless relay systems: Two-way relay and Full-duplex relay," *IEEE Communications Magazine*, vol. 47, no. 9, pp. 58-65, 2009.

[17] Riihonen, Taneli, Stefan Werner, Risto Wichman, and Jyri Hamalainen, "Outage probabilities in Infrastructure-Based Single-Frequency relay links," *IEEE Wireless Communications and Networking Conference*, pp.1-6, 2009.

[18] Ng, Derrick Wing Kwan, *et. al*, "Dynamic resource allocation in MIMO-OFDMA systems with Full-Duplex and hybrid relaying," *IEEE Transactions on Communications*, vol. 60, no. 5, 1291-1304, 2012.

[19] Krikidis, Ioannis, *et al*, "Full-Duplex Relay selection for Amplify-and-Forward cooperative networks," *IEEE Transactions on Wireless Communications*, vol. 11, no. 12, pp. 4381-4393, 2012.

[20] S. Luo, R. Zhang, and T. J. Lim, "Optimal save-then-transmit protocol for energy harvesting wireless transmitters," *IEEE Transactions on Wireless Communications*, vol. 12, no. 3, pp. 1196-1207, 2013.

[21] Suraweera, H., G. Karagiannidis, and P. Smith, "Performance analysis of the Dual-hop asymmetric fading channel," *IEEE Transactions on Wireless Communications*, vol. 8, no. 6, pp. 2783-788, 2009.

[22] Tin, Phu Tran, Tran Hoang Quang Minh, Tan N. Nguyen, and Miroslav Voznak, "System performance analysis of Half-Duplex relay network over rician fading channel," *TELKOMNIKA*, vol. 16, no. 1, pp. 189-199, 2018.

[23] Rashid, Tarique, Sunil Kumar, Akshay Verma, Prateek Raj Gautam, and Arvind Kumar, "Pm-EEMRP: postural movement-based energy efficient Multi-Hop routing protocol for intra wireless body sensor network (Intra-WBSN)," *TELKOMNIKA (Telecommunication, Computing, Electronics and Control)*, vol. 16, no. 1, pp. 166-173, 2018.

[24] A. F. Morabito, "Power Synthesis of Mask-Constrained Shaped Beams Through Maximally-Sparse Planar Arrays," *TELKOMNIKA (Telecommunication, Computing, Electronics and Control)*, vol. 14, no. 4, pp. 1217-1219, 2016.

[25] C. Zhong, S. Jin, K.-K. Wong, and M. R. Mckay, "Ergodic Mutual Information Analysis for Multi-Keyhole MIMO Channels," *IEEE Transactions on Wireless Communications*, vol. 10, no. 6, pp. 1754–1763, 2011.