# On The Secrecy Performance of Wireless Powered Device to Device Systems

Dinh-Thuan Do
*(Corresponding author: Dinh-Thuan Do)*

Faculty of Electronics Technology, Industrial University of Ho Chi Minh City
12 Nguyen Van Bao Street, Go Vap District, Ho Chi Minh city, Vietnam
(Email: dodinhthuan@iuh.edu.vn)

*(Received May 25, 2017; revised and accepted Oct. 21, 2017)*

## Abstract

This paper investigates a new device-to-device (D2D) paradigm to evaluate system security at physical layer for the D2D link in which the energy harvesting-assisted node can communicate to satisfy quality of service (QoS) and help the conventional system with D2D capability against to eavesdropper. To cope with high security, the D2D deploys the lower layer with using cooperative jamming to eliminate impacts of illegal users. Considering relay node with capability of wireless energy harvesting, this paper attempts to investigate secure performance in case of power splitting fractions is controlled to improve the secrecy capacity. In particular, this work analyzes the secrecy capacities for direct connection, namely D2D links and traditional connections. As an important achievement, simulation results show the performance to deploy our proposed scheme to remain secure requirements in each D2D link in terms of the expected secrecy capacity.

*Keywords: Device-To-Device; Energy Harvesting; Power Splitting; Secrecy Capacity*

## 1 Introduction

Device to device (D2D) equipment has been examined as an inspiring solution to the frequency and channel resource shortage of the base station in cellular networks and inefficiency in its utilization [11–13, 16]. It can be shown that D2D can be combined to traditional cellular network, in which D2D can support more service assurance in a dense users circumstance, in which the two user equipment unit (UE) can be able linked with other UE in the pair of D2D users directly under assigned D2D link of the cellular resource to reduce processing at core equipment. Such D2D link can be self-operated without added controlling signal through the normal base station (BS). In theory, several kinds of gain such as the proximity gain, the recycle gain, the hop gain, and the paring gain are included in D2D communication permits fast admission to the allocated spectrum under required interference levels. Several applications including peer-to-peer file sharing, high resolution services, video on demand, and content-aware applications are goals of design in the distinctive D2D networks. In current research works and literature, D2D links and cellular UEs can be enabled for spectrum sharing mode selection in a wireless network as studied work in [16] and [13]. Resource optimization in time frequency hopping based D2D networks was developed in [12]. To minimize the total transmission power, power allocation schemes are investigated in D2D communications with aims of the quality-of-service (QoS) requirement of users in [11].

To consider security of D2D wireless networks, physical layer security is proposed as an approach which based on the information theoretic assessment to examine the security performance, especially in green communications can be extended to secure requirement [1]. In particular, D2D protocol with security analysis is designed suitable for Public Safety (PS) users with out-of-coverage users considering on sharing encryption keys [8] and J. S Chen *et al.* in [2], in which system model including source node, destination node, and an unwanted eavesdropper was established. As typical example, the authors in [10] proposed a D2D security architecture can be applied in the LTE system and several propositions on D2D security issues. Such solutions can be introduced as authentication and key management, secure routing, access control, and physical-layer security.

Moreover, potential overhearing attacks from third parties can be degraded wireless communication in the natural transmission environment and result in reliable problem of the private information transmitted over relaying networks [15], it denotes as eavesdroppers. Some other physical-layer security (PLS) methods have been implemented in relaying system model to guarantee secure data transmission [17]. The authors of [9] considered the secrecy rate maximization problem in the multiple-input single-output (MISO)-assisted relaying network by improving the transmit covariance matrix with two con-

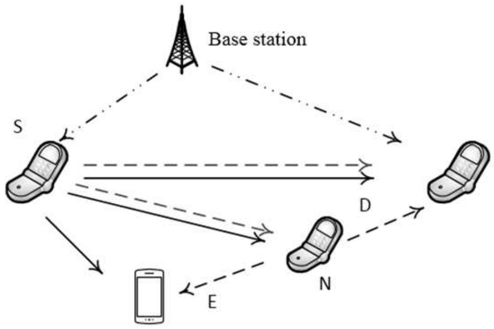

Figure 1: Secure D2D system model

ditions of the transmit power and the interference temperature. In [18], some multi-user scheduling policies are given to develop the PLS for cognitive radio networks against two kinds of the attackers, namely coordinated and uncoordinated ones. Two sub-optimal procedures using a full or partial orthogonal projection were planned to maximize the available relay node of a cognitive users is investigated in [3].

In this paper, D2D link is experienced in energy harvesting (EH) capability and the physical-layer security method is added to protect the confidential signal to against malicious eavesdropping and energy harvesting based protocols are investigated in [4–7]. The authors in [5–7] presented two-way relating network while the work in [4] proved that the relay can be forwarded signal thanks to harvesting wireless power from the source node. In principle, simultaneous wireless information and power transfer (SWIPT) to bring electromagnetic wave to energy bearing for assigned users. To integrate EH to D2D network, D2D scheme in each link will be operated under wireless energy support including energy transfer phase and information processing phase. The main duty is careful calculation of power fraction to satisfy the secrecy capacity of the D2D system.

The rest of this paper is organized as follows. In Section II, we will interpret our system model. In Section III, we formulate our closed-form expression and develop the probability of strictly positive secrecy capacity (SPSC) to examine secure performance problem. The asymptotic analysis is illustrated in Section IV, and Section V concludes the paper [14].

## 2 System Model

In this paper, Figure 1 shows a wireless-powered device to device (D2D) system in underlay cellular network under security consideration. In such model, the representative nodes are considered: A D2D user denoted as source (S), a base station (BS), a D2D user stands for destination (D) and an eavesdropper (E) in the coverage area of D2D links, and D node can be able harvest energy in the D2D link, N denotes as traditional user (non-D2D user). It is assumed that S, E, N and D are furnished with a single antenna. It is noted that D assumed no external power supply, and only relies on harvested energy from S for transmitting signal. The considered system applies power splitting (PS) protocol in the energy-aware receiver at D to process information and energy signal. It is assumed that all links are modeled as independent and identical Rayleigh fading. We denote $h_{ab}$ is channel of link from node $a$ to node $b$ while $P_a$ stands for power at node $a$. In particular, each D2D user is controlled by base station in initial period, and then D2D can be freely communicate each other in next period. It is also assumed that the channel state information is available. In case imperfect channel estimation, the system performance will be reduced but it is beyond of scope of this paper. In conventional principle, the characteristic of the channel state information can be assessed by training sequence and analog feedback. The harvested power can be obtained at D (D2D user) is:

$$P_D = \rho\eta P_S |h_{SD}|^2$$

where with ( $0 < \rho < 1$ ) is power splitting coefficient, $0 < \eta < 1$ is energy conversion efficiency of energy harvesting protocol. The harvested power can be obtained at N (non-D2D user) is:

$$P_N = \rho\eta P_S |h_{SN}|^2$$

The information signal received at D is expressed by

$$y_D = \sqrt{\varphi}(\sqrt{P_S} h_{SD} X_S + n_D) + \sqrt{P_N} h_{ND} X_N + n_c$$

where $X_S$ is the transmitted symbol at S, and $n_c$ is the power splitting (PS) factor, and, denotes as the signal processing noise at D, which is also modeled as AWGN with zero mean and a variance of $N_0$ . It is noted that the power splitting factors satisfy condition $\rho + \varphi = 1$. It worth noting that N node can be made interference to the nearby nodes. It is noted that $E_D = \rho\eta P_S |h_{SD}|^2 T$ is the energy harvested from S and stored in battery to use for next processing, in which T is the symbol duration.

Next, we compute the received signal at E by

$$y_E = \sqrt{P_S} h_{SE} X_S + \sqrt{P_N} h_{NE} X_N + n_E$$

where $n_E$ is the AWGN with zero mean and a variance of $N_0$.

Thus, by considering the signal-to-interference-plus-noise ratio (SINR) at D and E node, they are expressed as

$$\begin{aligned} \gamma_D &= \frac{\varphi P_S |h_{SD}|^2}{P_N |h_{ND}|^2 + \varphi N_0 + N_0} \\ &= \frac{\varphi P_S |h_{SD}|^2}{\rho\eta P_S |h_{SN}|^2 |h_{ND}|^2 + \varphi N_0 + N_0} \end{aligned}$$

and

$$\gamma_E = \frac{P_S |h_{SE}|^2}{P_N |h_{NE}|^2 + N_0} = \frac{P_S |h_{SE}|^2}{\rho\eta P_S |h_{SN}|^2 |h_{NE}|^2 + N_0}$$

In high SNR, we have SNR as below

$$\gamma_D \approx \frac{\varphi |h_{SD}|^2}{\rho\eta |h_{SN}|^2 |h_{ND}|^2}$$

## 3 Probability of Strictly Positive Secrecy Capacity (SPSC)

Regarding secure performance, we evaluate this expression as

$$C_s = \max\{R_D - R_E, 0\}$$

in which, the instantaneous achievable rates can be shown as

$$R_D = \log_2(1+\gamma_D)$$

and

$$R_E = \log_2(1+\gamma_E)$$

In such D2D system, SPSC is defined as the probability of the secrecy capacity is greater than zero.

$$P_{SPSC} = \Pr(C_S > 0)$$

It is required high security in D2D, we assume that $\gamma_D > \gamma_E$, then the secrecy rate can be re-expressed as

$$C_S = \log_2\left(\frac{1+\gamma_D}{1+\gamma_E}\right) = \log_2\left(\frac{\frac{\rho\eta|h_{SN}|^2|h_{ND}|^2+\varphi|h_{SD}|^2}{\rho\eta|h_{SN}|^2|h_{ND}|^2}}{\frac{|h_{SE}|^2+\rho\eta|h_{SN}|^2|h_{NE}|^2}{\rho\eta|h_{SN}|^2|h_{NE}|^2}}\right)$$

Therefore, the expression of is expressed by

$$\begin{aligned}\Pr(C_s > 0) &= \Pr\left(\log_2\left(\frac{1+\gamma_D}{1+\gamma_E}\right) > 0\right) \\ &= \Pr\left(\log_2\left(\frac{\frac{\rho\eta|h_{SN}|^2|h_{ND}|^2+\varphi|h_{SD}|^2}{\rho\eta|h_{SN}|^2|h_{ND}|^2}}{\frac{|h_{SE}|^2+\rho\eta|h_{SN}|^2|h_{NE}|^2}{\rho\eta|h_{SN}|^2|h_{NE}|^2}}\right) > 0\right) \\ &= \Pr(X > \frac{Y_1}{Y_2}) = 1 - \Pr(X \leq \frac{Y_1}{Y_2})\end{aligned}$$

We denote $X = \varphi|h_{SD}|^2$, $Y_1 = |h_{ND}|^2|h_{SE}|^2$ and $Y_2 = |h_{NE}|^2$. The CDF of X can be expressed as:

$$f_X(x) = \frac{1}{\varphi\Omega_{SD}}\exp(-\frac{x}{\varphi\Omega_{SD}})$$

and

$$F_X(x) = 1 - \exp(-\frac{x}{\varphi\Omega_{SD}})$$

It can be expressed PDF and CDF of $Y1$ as follow [14]:

$$\begin{aligned}f_{Y_1}(y) &= \int_0^\infty \frac{1}{x} f_{|h_{SE}|^2}(\frac{y}{x}) f_{|h_{ND}|^2}(x)dx \\ &= \frac{1}{\Omega_{SE}}\frac{1}{\Omega_{ND}}\int_0^\infty \frac{1}{x}\exp(-\frac{1}{\Omega_{SE}}\frac{y}{x} - \frac{1}{\Omega_{ND}}x)dx\end{aligned}$$

Besides, we have

$$\begin{aligned}F_{Y_1}(y) &= \int_0^\infty \int_0^{\frac{y}{x}} f_{|h_{SE}|^2}(z) f_{|h_{ND}|^2}(x)dxdz \\ &= \int_0^\infty F_{|h_{SE}|^2}(\tfrac{y}{x}) f_{|h_{ND}|^2}(x)dx \\ &= \int_0^\infty (1 - \exp(-\tfrac{y}{x}\tfrac{1}{\Omega_{SE}})).\tfrac{1}{\Omega_{ND}}\exp(-\tfrac{1}{\Omega_{ND}}x)dx \\ &= \int_0^\infty \tfrac{1}{\Omega_{ND}}\exp(-\tfrac{1}{\Omega_{ND}}x)dx \\ &\quad - \int_0^\infty \tfrac{1}{\Omega_{ND}}\exp(-\tfrac{y}{x}\tfrac{1}{\Omega_{SE}})\exp(-\tfrac{1}{\Omega_{ND}}x)dx \\ &= 1 - \tfrac{1}{\Omega_{ND}}\int_0^\infty \exp(-(-\tfrac{y}{x}\tfrac{1}{\Omega_{SE}} - \tfrac{1}{\Omega_{ND}}x))dx \\ &= 1 - 2\sqrt{\tfrac{y}{\Omega_{SE}\Omega_{ND}}}K_1(2\sqrt{\tfrac{y}{\Omega_{SE}\Omega_{ND}}})\end{aligned}$$

in which $K_1(.)$ is Bessel function with second kind of first order.

In next step, the PDF of $Y = \frac{y_1}{y_2}$ is formulated as [14]:

$$\begin{aligned}f_Y(y) &= \int_0^\infty x f_{Y_1}(yx) f_{y_2}(x)dx \\ &= \tfrac{2}{\Omega_{SE}\Omega_{ND}\Omega_{NE}}\int_0^\infty x\exp(-\tfrac{x}{\Omega_{NE}})K_0(2\sqrt{\tfrac{yx}{\Omega_{SE}\Omega_{ND}}})dx \\ &= \sqrt{\tfrac{\Omega_{NE}}{\Omega_{SE}\Omega_{ND}}}y^{-\frac{1}{2}}\exp(\tfrac{y\Omega_{NE}}{2\Omega_{SE}\Omega_{ND}})W_{-\frac{3}{2},0}(\tfrac{y\Omega_{NE}}{\Omega_{SE}\Omega_{ND}})\end{aligned}$$

in which $W_{\lambda,\mu}(.)$ is Whittaker function.

Finally, it can be obtained SPSC formula as

$$\begin{aligned}\Pr(C_s > 0) &= 1 - \int_0^\infty\int_0^y f_X(x)f_Y(y)dxdy \\ &= 1 - \int_0^\infty (1 - \exp(-\frac{1}{\varphi\Omega_{SD}}y))f_Y(y)dy \\ &= \int_0^\infty \exp(-\frac{1}{\varphi\Omega_{SD}}y)f_Y(y)dy \\ &= \int_0^\infty \left[\exp(-\frac{1}{\varphi\Omega_{SD}}y)\sqrt{\frac{\Omega_{NE}}{\Omega_{SE}\Omega_{ND}}}y^{-\frac{1}{2}}A\right]dy\end{aligned}$$

where $A = \exp(\frac{y\Omega_{NE}}{2\Omega_{SE}\Omega_{ND}})W_{-\frac{3}{2},0}(\frac{y\Omega_{NE}}{\Omega_{SE}\Omega_{ND}})$

## 4 Simulation

In this section, empirical parameters will be adopted to examine the secrecy performance of D2D system. The D2D system distributes between D2D users and non-D2D user. In this section, numerical results are presented. Unless otherwise explicitly specified, the parameters are set as transmit SNR equals to 20 (dB), channel gains equal to 1, $\eta = 0.9$ , and $\alpha = h_{SD}/h_{SE}$.

In Figure 2, we plot the secrecy capacity versus $\alpha$. In this observation, we can figure out that the secrecy capacity increases when more power is allocated for the energy

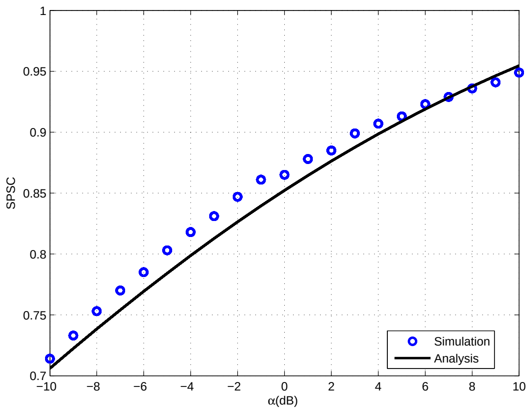

Figure 2: Secure performance D2D versus $\alpha$

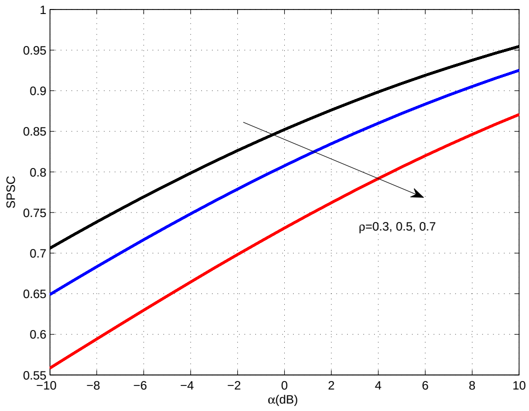

Figure 3: SPSC versus $\alpha$ as considering impact of power splitting fractions

harvesting -assisted node. In Figure 2, we present analytical and simulation results for SPSC vs. $\alpha$. It can be seen that analytical results are obtained to meet with line for Monte Carlo simulation. One can see that simulation results are approximate same with analytical results, which validates the accuracy of the analytical expression derived.

Figure 3 examines impact of power splitting fraction on SPSC performance. It can be shown that SPSC with a higher $\rho$ is outperformed by that with a lower $\rho$. The main reason is that a higher $\rho$ leads to a lower portion of the received power is separated ratio for information decoding and more power is harvested. As a result, a low received SINR is resulted at D, which leads to a lower capacity at D.

Similarly, Figure 4 shows SPSC performance versus power splitting coefficients. When increasing $\rho$ leads to reducing power for information processing and result in lower SPSC performance. As a result, the careful calculation of $\rho$ need be required for high secure D2D networks.

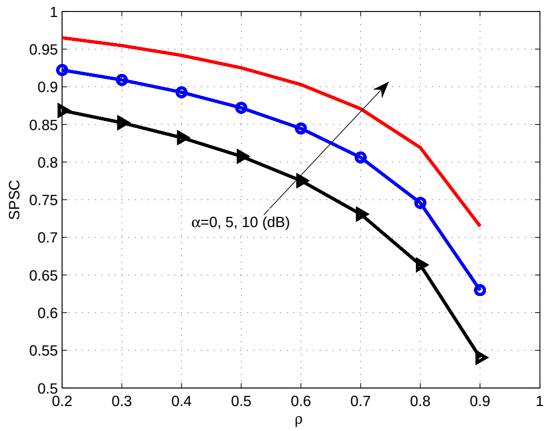

Figure 4: SPSC versus power splitting fractions

# 5 Conclusion

This paper has considered the secrecy performance in D2D networks with wireless-powered node system. By considering energy harvesting-assisted node can simultaneously receive information and energy from the source through power splitting protocol, the probability of strictly secrecy capacity has been studied. Exact expression of probability of strictly positive secrecy capacity have been derived. Numerical results show that under the condition that the energy harvesting together to become the exact probability of strictly positive secrecy capacity.

# References

[1] S. Bi, C. K. Ho, and R. Zahang, "Wireless powered communication: Opportunities and challenges," *IEEE Communications Magazine*, vol. 53, no. 4, pp. 117-125, 2015.

[2] J. S. Chen, C. Y. Yang and M. S. Hwang, "The capacity analysis in the secure cooperative communication system," *International Journal of Network Security*, vol. 19, no. 6, pp. 863-869, 2017.

[3] T. Chen, H. Q. Yuan, T. Z. Zhao, *et al.*, "Joint beamforming and powerallocation for secure communication in cognitive radio networks," *IET Communications*, vol. 10, no. 10, pp. 1156-1162, 2016.

[4] D. T. Do, "Optimal throughput under time power switching based relaying protocol in energy harvesting cooperative network," *Wireless Personal Communications*, vol. 87, no. 2, pp. 551-564, 2016.

[5] D. T. Do, "Energy-aware two-way relaying networks under imperfect hardware: Optimal throughput design and analysis," *Telecommunication Systems*, vol. 62, no. 2, pp. 449-459, 2015.

[6] D. T. Do, H. S. Nguyen, "A tractable approach to analyze the energy-aware two-way relaying networks in presence of co-channel interference," *EURASIP Journal on Wireless Communica-*

*tions and Networking*, 2016. (`https://doi.org/10.1186/s13638-016-0777-z`)

[7] D. T. Do, ”Power switching protocol for two-way relaying network under hardware impairments,” *Radioengineering*, vol. 24 , no. 3, pp. 765-771, 2015.

[8] L. Goratti, *et al.* ”Connectivity and security in a D2D communication protocol for public safety applications,” in *Proceeding of 2014 11th International Symposium on Wireless Communications Systems (ISWCS'14)*, 2014. DOI: 10.1109/ISWCS.2014.6933414.

[9] Y. Pei, Y.-C. Liang, L. Zhang, *et al.*, ”Secure communication over MISO cognitive radio channels,” *IEEE Transactions on Wireless Communications*, vol. 9, no. 4, pp. 1494-1502, Apr. 2010.

[10] M. Wang, and Z. Yan, ”Security in D2D communications: A review,” *2015 IEEE Trustcom/BigDataSE/ISPA*, vol. 1, 2015.

[11] X. Xiao, X. Tao, and J. Lu, ”A Qos-aware power optimization scheme in OFDMA systems with integrated device-to-device (D2D) communications,” in *Proceeding IEEE Vehicle Technology Conference*, pp. 1–5, Sep. 2011.

[12] Q. Ye, M. Al-Shalash, C. Caramanis, and J. G. Andrews, ”Resource optimization in device-to-device cellular systems using time-frequency hopping,” *IEEE Translation Wireless Communications*, vol. 13, no. 10, pp. 5467–5480, Oct. 2014.

[13] C. H. Yu, K. Doppler, C. B. Ribeiro, and O. Tirkkonnen, ”Resource sharing optimization for device-to-device communication underlaying cellular networks,” *IEEE Translation Wireless Communications*, vol. 10, no. 8, pp. 2752–2763, Aug. 2011.

[14] J. Zhang, G. Pan, and H-M Wang, ”On physical-layer security in underlay cognitive radio networks with full-duplex wireless-powered secondary system,” *IEEE Access*, vol. 4, pp. 3887–3893, 2016.

[15] Y. Zou, J. Zhu, X. Wang, *et al.*, ”A survey on wireless security: Technical challenges, recent advances and future trends,” *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1727-1765, Sep. 2016.

[16] M. Zulhasnine, C. Huang, and A. Srinivasan, ”Efficient resource allocation for device-to-device communication underlaying LTE network,” in *Proceeding IEEE 6th International Conference Wirless Mobile Computing*, Oct. 2010, pp. 368–375.

[17] Y. Zou, J. Zhu, L. Yang, *et al.*, ”Securing physical-layer communications for cognitive radio networks,” *IEEE Communications Magazine*, vol. 53, no. 9, pp. 48-54, Sep. 2015.

[18] Y. Zou, X. Li, and Y. C. Liang, ”Secrecy outage and diversity analysis of cognitive radio systems,” *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 11, pp. 2222-2236, Nov. 2014.

# Biography

**Dinh-Thuan Do** received the B. S. degree, M. Eng. degree, and Ph.D. degree from Vietnam National University (VNUHCMC) in 2003, 2007, and 2013 respectively, all in Communications Engineering. He was a visiting Ph. D. student with Communications Engineering Institute, National Tsing Hua University, Taiwan from 2009 to 2010. Prior to joining Ton Duc Thang University, he was senior engineer at the VinaPhone Mobile Network from 2003 to 2009. He was the recipient of the 2015 Golden Globe Award by Ministry of Science and Technology. He is currently Assistant Professor at the Wireless Communications & Signal Processing Lab (WICOM LAB). His publication includes 21+ SCI/SCIE journals. His research interest includes signal processing in wireless communications network, mmWave, device-to-device networks, cooperative communications, full-duplex transmission and energy harvesting.