International Journal of Security and Its Applications
Vol. 10, No. 6 (2016) pp.351-362
http://dx.doi.org/10.14257/ijsia.2016.10.6.33

An Analysis Modeling Architecture for Supporting Physical Layer Security of Wireless Networks under Hardware Impairments

Kyusung Shim[1], Nhu Tri Do[2] and Beongku An[3,*]

[1]Information System Graduate School of Smart City Science Management, Hongik University, Republic of Korea
[2]Dept. of Electronics and Computer Engineering in Graduate School, Hongik University, Republic of Korea
[3]Dept. of Computer and Information Communications Engineering, Hongik University, Republic of Korea
[1]kyusung@hongik.ac.kr, [2]dotrinhu@gmail.com, [3,]beongku@hongik.ac.kr*

Abstract

In this paper, we study physical layer security (PLS) of wireless networks in presence of one eavesdropper. Assume that the channel state information (CSI) of the eavesdropper cannot be obtained at the transmitter, such as CSI can be then estimated through the CSI of a torch node. In addition, a practical issue of wireless nodes, i.e., hardware impairment (HI), is considered at the source node of the network. System performances in terms of secrecy outage probability, probability of non-zero secrecy capacity and ergodic secrecy capacity are then investigated over Rayleigh fading channels. In particular, the closed-form expressions of the secrecy outage probability and probability of non-zero secrecy capacity are provided. Analytical results are then validated by Monte-Carlo simulation. Numerical results reveal the effects of the HI and the advantages of the use of the torch node in PLS of wireless communications.

Keywords: *physical layer security, secrecy outage probability, probability of non-zero secrecy capacity, imperfect channel state information, hardware impairment*

1. Introduction

According to the information-theoretic perspective, physical layer security (PLS) secures the wireless communications by exploiting the physical characteristics of the wireless channels [1]. In PLS, the success of security is defined by the difference of the capacity between main channel and eavesdropper channel. More specifically, different from the security techniques that is employed in upper layers, PLS technique utilizes the channel state information (CSI) of all wireless channels in the networks to manage the channel capacity of legitimate transmissions in order to combat the interception of eavesdroppers. The pioneer work in [2] pointed out that there is a secrecy capacity at which the transmission between legitimate nodes is reliable and the eavesdroppers cannot correctly decode the confidential messages. The secrecy capacity will be mathematically described in the next section.

Recently, PLS has been extensively studied in the literature. For example, in [1], the authors investigate security performance in terms of PLS of a classical relay network consisting of one source, one relay and one destination in the presence of one eavesdropper that tries to overhear legitimate transmission from source to destination. Later on, the authors in [3] considered the similar system mode in cognitive radio

[*] Corresponding Author

ISSN: 1738-9976 IJSIA

network, and then extended to the general case of multi-hop relaying networks in [4]. In [5], the authors proposed several relay selection protocols in order to deal with the PLS issue in cooperative networks. The authors in [6] focused on investigating the performance of relay selection protocols subjected to the security constraints in terms of PLS. Considering more general cooperative networks consisting of one base station, multiple users and multiple eavesdropper under underlay-cognitive radio networks, the authors in [7] studied efficient methods for scheduling multiple relays in the case of collaborated and un-collaborated eavesdroppers. However, all the mentioned works above made a common assumption on the available of channel state information (CSI) of the channels between legitimate nodes and eavesdroppers.

In this paper, let us consider a direct wireless transmission, *i.e.*, the transmission of one pair of source-destination, in the presence of one eavesdropper that observes and intercepts the legitimate transmission. The source needs to estimate the channel state information (CSI) of all wireless channels in the system in order to secure the transmission. In case of main channel (the channel between legitimate transmitter and legitimate receiver), the CSI is fed back to the source by the destination. However, in case of eavesdropper channel (the channel between legitimate transmitter and the eavesdropper), since the eavesdropper has to hide its presence so that the eavesdropper does not send its CSI to the source, in other words, the CSI of the eavesdropper channel is not available. Thus, in this paper, we consider the practical scenario in which the eavesdropper does not send its CSI to the transmitters. In order to obtain the CSI of the eavesdropper channel, we deploy one torch node which is located near the eavesdropper and the torch node report its channel condition to the source as done in [8]. Through the torch node's CSI, the source is able to estimate the CSI of the eavesdropper channel by using the model of imperfect CSI channel [9].

On the other hand, we take into account the hardware impairment (HI) issue of wireless communications. Hardware impairment refers to the distortions caused by both transmitters and receivers' hardware. The assumption of ideal hardware makes sense in low-rate systems, but in high-rate systems, it leads to misleading results. In practice, hardware impairments can occur by several reasons, such as high power amplifier nonlinearities, phase noise and I/Q imbalance and so on. For further reading, please refer to [10], and the references therein, where the impact of hardware impairments on wireless communications was investigated in detail. It is noteworthy to point out that in the related works [3]-[8], the hardware impairments effect on the physical layer security was not considered.

The main contributions of the paper can be summarized as follows.

- Different from the related works on physical layer security, this paper takes into account the joint practical issues of wireless communications, namely the unavailable of the CSI of the eavesdropper channel, and the hardware impairment (HI) effect at the transmitter.
- After mathematically describing the considered system model, the performance analysis is carried out, and the closed-form expressions of the secrecy outage probability and the probability of non-zero secrecy capacity are obtained.
- Simulation results are then provided to verify the analysis. Through numerical results, we discuss on advantages of the use of the torch node and the impact of HI on the physical layer security performance.

The rest of the paper is arranged as follows. Section 2 introduces the system model and presents the concept of physical layer security and its key analysis metrics. The derivation of the closed-form expression of the secrecy outage probability and the probability of non-zero secrecy capacity is presented in Section 3. Numerical results are shown in Section 4. Finally, the conclusions are given in Section 5.

2. System Model

Let us consider a direct communication from a source S to a destination D as depicted in Figure 1. In addition, the legitimate transmission is observed by one eavesdropper E. A torch node T is deployed to help the source node to evaluate the CSI of the eavesdropper channel, *i.e.,* S-E channel.

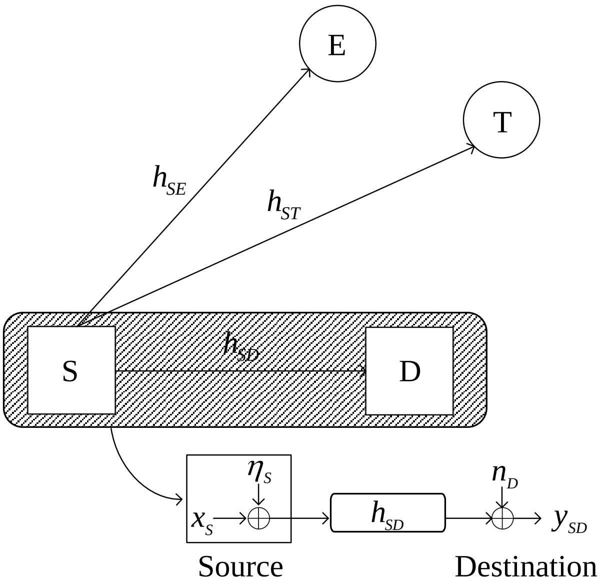

Figure 1. The source-destination transmission is overheard by one eavesdropper. In addition, the hardware impairment effect is taken into account at the source node

Considering hardware impairment at the source, the received signal at D from S can be given by [10]

$$y_{SD} = \sqrt{P} h_{SD} (x_S + \eta_S) + n_D \tag{1}$$

where P denotes the transmit power of the source, h_{SD} denotes the channel coefficient of the S-D channel, x_S denotes the source message where $E[|x_S|^2] = 1$, and $n_D \sim CN(0, N_0)$ represents the complex Gaussian noise with noise variance N_0, herein $CN(.)$ stands for the complex symmetric Gaussian distribution.

The HI effect at the transmitter of the source can be characterized by the distortion noise $\eta_S \sim CN(0, \kappa^2)$. Herein, κ represents the level of HI, which can be interpreted as the error vector magnitudes (EVM). According to 3GPP LTE requirements, the value of EVM should be in the range from 0.08 to 0.175 [11].

The role of the torch node T is to provide its CSI, *i.e.,* information of h_{ST}, to the source S. Then, S uses this information to estimate the CSI of the eavesdropper channel. Thus, the channel coefficient of the eavesdropper channel S-E can be given by [8]

$$h_{SE} = \rho h_{ST} + \varepsilon \sqrt{(1 - \rho^2)} \tag{2}$$

where $\varepsilon \sim CN(0, N_0)$, and ρ denotes the correlation coefficient that indicates the accuracy of channel estimate over all channel state of the S-T channel, herein $0 < \rho \leq 1$.

Due to the broadcast nature of wireless communications, an eavesdropper can overhear the transmitted signal from S to D. Using Eq. (2), the received signal at the eavesdropper can be expressed as

$$\begin{aligned} y_{SE} &= \sqrt{P} h_{SE}(x_S + \eta_S) + n_D \\ &= \sqrt{P}\left(\rho h_{ST} + \varepsilon\sqrt{(1-\rho^2)}\right)(x_S + \eta_S) + n_D \end{aligned} \tag{3}$$

Let $g_{SD} = |h_{SD}|^2$ and $g_{SE} = |h_{SE}|^2$ denote the channel gains of main channel, i.e., the S-D channel, and eavesdropper channel, i.e., the S-E channel, respectively. From Eq. (1), the signal-to-noise and distortion ratio (SNDR) of main channel can be given by

$$\gamma_{SD} = \frac{P g_{SD}}{P g_{SD} \kappa^2 + N_0} \tag{4}$$

From Eq. (3), and after some arrangements, the SNDR of eavesdropper channel can be given by

$$\gamma_{SE} = \frac{P g_{SE}}{P g_{SE} \kappa^2 + N_0} \tag{5}$$

Based on the SNDR expressions in Eq. (4) and Eq. (5), the capacity of the main channel and eavesdropper channel can be, respectively, expressed as

$$C_M = \log_2\left(1 + \gamma_{SD}\right) \tag{6}$$

$$C_E = \log_2\left(1 + \gamma_{SE}\right) \tag{7}$$

From the physical layer security's point of view, the secrecy capacity can be determined by the difference between the capacity of the main channel and that of the eavesdropper channel [7]. Thus, the secrecy capacity of the considered system can be given by

$$C_S = \max\left(C_M - C_E, 0\right) \tag{8}$$

Additionally, all the wireless channels are characterized with Rayleigh fading model and independent and identically distributed (i.i.d.). Thus, the channel gains, g_{SD} and g_{SE}, are exponentially distributed with parameters, λ_{SD} and λ_{SE}, respectively.

3. Outage Performance Analysis

3.1. Secrecy Outage Probability

The secrecy outage probability can be defined as the probability of the event that the secrecy capacity drops below a predefined target secrecy rate [10]. For predefined target secrecy rate R, the secrecy outage probability, P_{SOP}, of the considered system can be given by

$$\begin{aligned} P_{SOP} &= \Pr\left(C_S < R\right) \\ &= \Pr\left(\log_2\left(1+\frac{Pg_{SD}}{\kappa^2 Pg_{SD}+N_0}\right)-\log_2\left(1+\frac{Pg_{SE}}{\kappa^2 Pg_{SE}+N_0}\right)<R\right) \end{aligned} \tag{9}$$

where the second equal signal is based on the SDNRs expressed in Eq. (4)-(5), and after some algebraic manipulations, P_{SOP} can be re-written as

$$P_{SOP} = \Pr\left(\frac{Pg_{SD}}{\kappa^2 Pg_{SD}+N_0}-\frac{2^R Pg_{SE}}{\kappa^2 Pg_{SE}+N_0}<2^R-1\right) \tag{10}$$

For the sake of notational convenience, let g_{SD} = X and g_{SE} = Y. The cumulative distribution function (CDF) of $W \in \{X, Y\}$ can be given by

$$F_W\left(w\right)=1-\exp\left(-\frac{w}{\lambda_W}\right) \tag{11}$$

where $\lambda_W \in \{\lambda_{SD}, \lambda_{SE}\}$. Next, let $a_0 = 2^R - 1,\ a_1 = P,\ a_2 = 2^R P,\ a_3 = \kappa^2 P,$ and $a_4 = N_0$, P_{SOP} in Eq. (11) can be re-written as

$$P_{SOP} = \Pr\left(\frac{a_1 x}{a_3 x + a_4} < a_0 + \frac{a_2 y}{a_3 y + a_4}\right) \tag{12}$$

Now, Let $\Omega = a_1 x / a_3 x + a_4,\ Z = a_0 + a_2 y / a_3 y + a_4$, Eq. (12) can be re-written as

$$\begin{aligned} P_{SOP} &= \Pr\left(\Omega < Z\right) \\ &= \int_0^\infty F_\Omega\left(z\right) f_Y(y) dy \end{aligned} \tag{13}$$

where the CDF of Ω can be derived as

$$\begin{aligned} F_\Omega\left(z\right) &= \Pr\left(\frac{\alpha_1 x}{\alpha_2 x + \alpha_3} \le z\right) \\ &= \Pr\left(x \le \frac{\alpha_3 z}{\alpha_1 - \alpha_2 z}\right) \end{aligned} \tag{14}$$

Since the value of (α_1 - $\alpha_2 z$) can be positive or negative, CDF of Ω can be given by

$$F_\Omega\left(z\right) = \begin{cases} F_X\left(\dfrac{\alpha_3 z}{\alpha_1 - \alpha_2 z}\right), & 0 \le z < \alpha_1 / \alpha_2 \\ 1, & z \ge \alpha_1 / \alpha_2 \end{cases} \tag{15}$$

Using Eq. (15), Eq. (13) can be re-written as

$$\begin{aligned} P_{SOP} &= \int_0^{z_0} F_X\left(\frac{a_4 z}{a_1 - a_3 z}\right) f_Y(y)\,dy + \int_{z_0}^{\infty} f_Y(y)\,dy \\ &= \underbrace{\int_0^{\infty} \frac{1}{\lambda_Y}\exp\left(-\frac{1}{\lambda_Y}y\right)dy}_{\Phi} - \underbrace{\int_0^{z_0} \frac{1}{\lambda_Y}\exp\left(-\frac{1}{\lambda_X}\frac{a_4 z}{a_1 - a_3 z}\right)\exp\left(-\frac{1}{\lambda_Y}y\right)dy}_{\Psi} \end{aligned} \tag{16}$$

Making the use of the following formula, $\int_0^{\infty} \beta \exp(-\beta x)\,dx = 1$ [12], we have

$$\begin{aligned} \Phi &= \int_0^{\infty} \frac{1}{\lambda_Y}\exp\left(-\frac{1}{\lambda_Y}y\right)dy \\ &= 1 \end{aligned} \tag{17}$$

On the other hand, Ψ in Eq. (16) can be expressed as

$$\begin{aligned} \Psi &= \int_0^{z_0} \frac{1}{\lambda_Y}\exp\left(-\frac{1}{\lambda_Y}\frac{a_4 z}{a_1 - a_3 z}\right)\exp\left(-\frac{1}{\lambda_Y}y\right)dy \\ &= \int_0^{z_0} \frac{1}{\lambda_Y}\exp\left(-\frac{1}{\lambda_X}\frac{a_4\left(a_0 + \dfrac{a_2 y}{a_3 y + a_4}\right)}{a_1 - a_3\left(a_0 + \dfrac{a_2 y}{a_3 y + a_4}\right)}\right)\exp\left(-\frac{1}{\lambda_Y}y\right)dy \end{aligned} \tag{18}$$

After some algebraic manipulations, Eq. (18) can be re-expressed as

$$\Psi = \int_0^{z_0} \frac{1}{\lambda_Y}\exp\left(-\frac{1}{\lambda_X}\frac{\left(a_0 a_3 a_4 + a_0 a_4\right)y + a_0 a_4^2}{\left(a_1 a_3 - a_0 a_3^2 + a_2 a_3\right)y + \left(a_1 a_4 - a_0 a_3 a_4\right)}\right)\exp\left(-\frac{1}{\lambda_Y}y\right)dy \quad (1$$

9)

Let $b_1 = a_0 a_3 a_4 + a_0 a_4$, $b_2 = a_0 a_4^2$, $b_3 = a_1 a_3 - a_0 a_3^2 + a_2 a_3$ and $b_4 = a_1 a_4 - a_0 a_3 a_4$. Eq. (19) can be re-written as

$$\begin{aligned} \Psi &= \int_0^{z_0} \frac{1}{\lambda_Y}\exp\left(-\frac{1}{\lambda_X}\frac{b_1 y + b_2}{b_3 y + b_4} - \frac{1}{\lambda_Y}y\right)dy \\ &= \int_0^{z_0} \frac{1}{\lambda_Y}\exp\left(-\frac{\lambda_X b_3 y^2 + \left(\lambda_X b_4 + \lambda_Y b_1\right)y + \lambda_Y b_2}{\lambda_X \lambda_Y b_3 y + \lambda_X \lambda_Y b_4}\right)dy \end{aligned} \tag{20}$$

Let $c_1 = \lambda_X b_3$, $c_2 = \lambda_X b_4 + \lambda_Y b_1$, $c_3 = \lambda_Y b_2$, $c_4 = \lambda_X \lambda_Y b_3$, and $c_5 = \lambda_X \lambda_Y b_4$. Eq. (20) can be further expressed as

$$\begin{aligned}\Psi &= \int_0^{z_0} \frac{1}{\lambda_Y}\exp\left(-\frac{c_1y^2+c_2y+c_3}{c_4y+c_5}\right)dy \\ &= \left[-\frac{1}{\lambda_Y}\left(-\frac{c_4^2y^2+2c_4c_5y+c_5^2}{c_1c_4y^2+2c_1c_5y+\left(c_2c_5-c_3c_4\right)}\right)\exp\left(-\frac{c_1y^2+c_2y+c_3}{c_4y+c_5}\right)\right]_0^{z_0}\end{aligned} \tag{21}$$

Since random variable Y is non-negative, the range of z_0 from Eq. (15), the range of y can be re-written as

$$0 < y < \frac{a_1a_4 - a_0a_3a_4}{a_2a_3 - a_1a_3 + a_0a_3^2} \tag{22}$$

Let $y_0 = a_1a_4 - a_0a_3a_4 / a_2a_3 - a_1a_3 + a_0a_3a_3$. Combining Eq. (17) and Eq. (21), the closed-form expression of the secrecy outage probability of the system can be given by

$$\begin{aligned}P_{SOP} &= 1 - \frac{1}{\lambda_Y}\left(-\frac{c_5^2}{c_2c_5-c_3c_4}\right)\exp\left(-\frac{c_3}{c_5}\right) \\ &\quad + \frac{1}{\lambda_Y}\left(-\frac{c_4^2y_0^2+2c_4c_5y_0+c_5^2}{c_1c_4y_0^2+2c_1c_5y_0+\left(c_2c_5-c_3c_4\right)}\right)\exp\left(-\frac{c_1y_0^2+c_2y_0+c_3}{c_4y_0+c_5}\right)\end{aligned} \tag{23}$$

3.2. Probability of Non-Zero Secrecy Capacity

The probability of non-zero secrecy capacity, $P_{NZ\text{-}SC}$, can be defined as the probability that the main channel capacity is larger than an eavesdropper's channel capacity [13]. Such probability characterizes the likelihood of obtaining the secure transmission in PLS. Thus, the probability of non-zero secrecy capacity of the considered system can be formulated as

$$\begin{aligned}P_{NZ-SC} &= \Pr\left(C_S > 0\right) \\ &= 1 - \Pr\left(C_S < 0\right)\end{aligned} \tag{24}$$

It is easy to observe that the case of $\Pr(C_S < 0)$ in Eq. (24) is the special case of the P_{SOP} when $R = 0$. Thus, after some algebraic manipulations, $\Pr(C_S < 0)$ can be given by

$$\Pr\left(C_S < 0\right) = 1 - \frac{\lambda_X}{\lambda_X+\lambda_Y}\left(1-\exp\left(-\frac{\lambda_X+\lambda_Y}{\kappa^2\lambda_X\lambda_Y}\right)\right) \tag{25}$$

Plugging Eq. (25) into Eq. (24) yields the closed-form expression of the probability of non-zero secrecy capacity which can be expressed as

$$\begin{aligned}P_{NZ-SC} &= 1 - \left(1 - \frac{\lambda_X}{\lambda_X+\lambda_Y}\left(1-\exp\left(-\frac{\lambda_X+\lambda_Y}{\kappa^2\lambda_X\lambda_Y}\right)\right)\right) \\ &= \frac{\lambda_X}{\lambda_X+\lambda_Y}\left(1-\exp\left(-\frac{\lambda_X+\lambda_Y}{\kappa^2\lambda_X\lambda_Y}\right)\right)\end{aligned} \tag{26}$$

Next, the computer simulation will be carried out to verify the developed analysis.

4. Numerical Results

In this section, the developed analysis will be validated by a computer simulation. The simulation results are obtained by carrying out the Monte-Carlo simulations. As we can observe through the following numerical results, the simulation results collaborate with the analytical results, which confirms the correctness of our analysis. Without loss of generality, in the simulation, we set $\lambda_{SD} = 0.5$, $R = 0.5$ bits/s/Hz, $P = 10$ dB, $N_0 = 1$, and the simulation was run with 10^6 times. Unless otherwise stated, we set $\kappa = 0.185$ for the case of the system with HI and $\kappa = 0$ for the case of that without HI, i.e., ideal hardware.

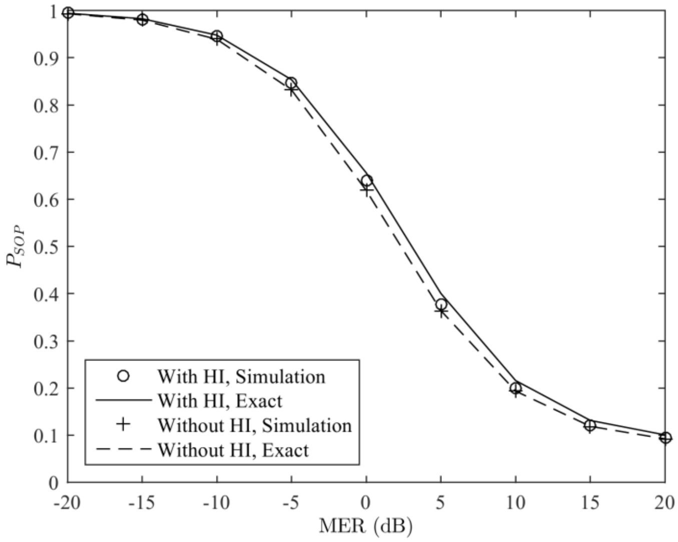

Figure 2. Secrecy Outage Probability P_{SOP} versus MER in the Case of the System with and without HI.

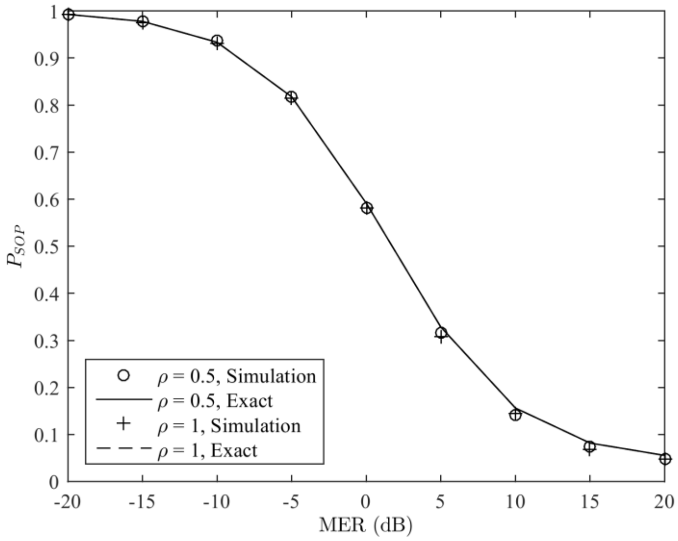

Figure 3. Secrecy Outage Probability P_{SOP} versus MER at Different Values of ρ

Firstly, Figure 2 plots the secrecy outage probability P_{SOP} as a function of the main-to-eavesdropper ratio (MER) for the cases of ideal hardware and that of hardware impairment. From Figure 2, we can observe that P_{SOP} decreases as the MER increases. On the other hand, for a given value of MER, P_{SOP} in the case of HI is higher than that of the case of ideal hardware, *i.e.*, non-HI. Thus, HI effects make the system is more vulnerable in terms of physical layer security.

Figure 3 plots that secrecy outage probability P_{SOP} as a function of the MER at different values of the correlation coefficient ρ. It can be seen from Figure 3 that the secrecy outage probability does not change when we vary the value of correlation coefficient. It means that the imperfect estimation of the eavesdropper channel via the torch node does not impact on the secrecy outage probability. This result highlights the advantage of the use of the torch node in PLS.

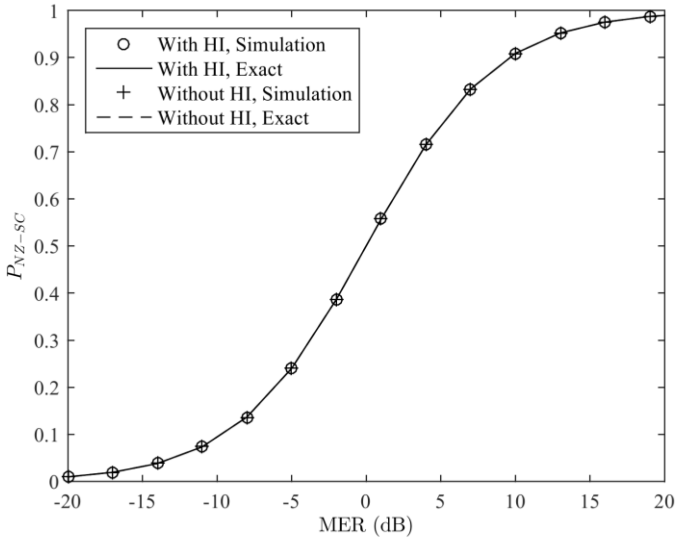

Figure 4. Probability of Non-Zero Secrecy Capacity $P_{NZ\text{-}SC}$ versus MER at Different Values of Level of HI κ

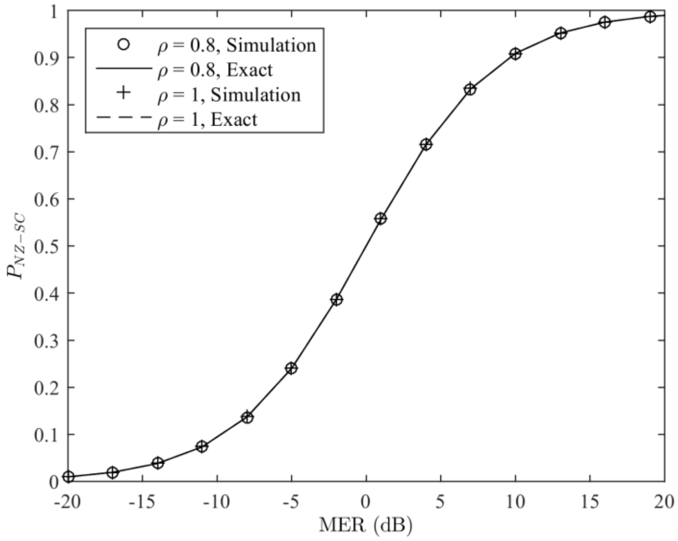

Figure 5. Probability of Non-Zero Secrecy Capacity $P_{NZ\text{-}SC}$ versus MER at Different Values of ρ

In Figure 4, the probability of non-zero secrecy capacity $P_{NZ\text{-}SC}$ is plotted as a function of MER for the case of HI and that of ideal hardware, *i.e.*, without HI. From Figure 4, we can see that the probability of non-zero secrecy capacity increases as the MER increases. There is a degradation of secrecy capacity since the value of exp($-\lambda_X-\lambda_Y/\kappa^2\lambda_X\lambda_Y$) in Eq. (26) increases when κ increases. However, this degradation is too small to clearly be present in Figure 4.

Figure 5 plots the probability of non-zero secrecy capacity as a function of MER at different values of the correlation coefficient ρ. As shown in Figure 5, $P_{NZ\text{-}SC}$ does not change when the value of ρ is varied. This is in line with the result presented in Figure 3 since $P_{NZ\text{-}SC}$ is a special case of P_{SOP} when R = 0.

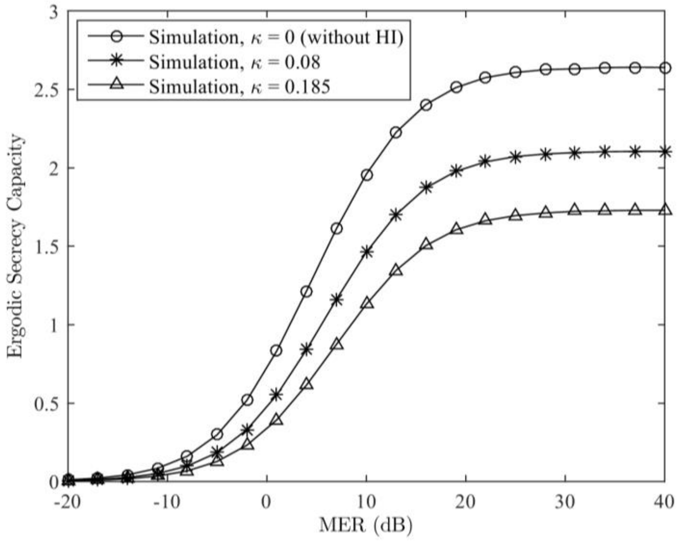

Figure 6. Ergodic Secrecy Capacity versus MER at Different Values of κ

The ergodic capacity of the system will be discussed by using the simulation results. In Figure 6, the ergodic secrecy capacity is plotted as a function of MER at different values of the level of HI κ. From Figure 6, we can observe that the ergodic secrecy capacity increases as MER increases. For a given value of MER, the higher κ, the lower the ergodic capacity is.

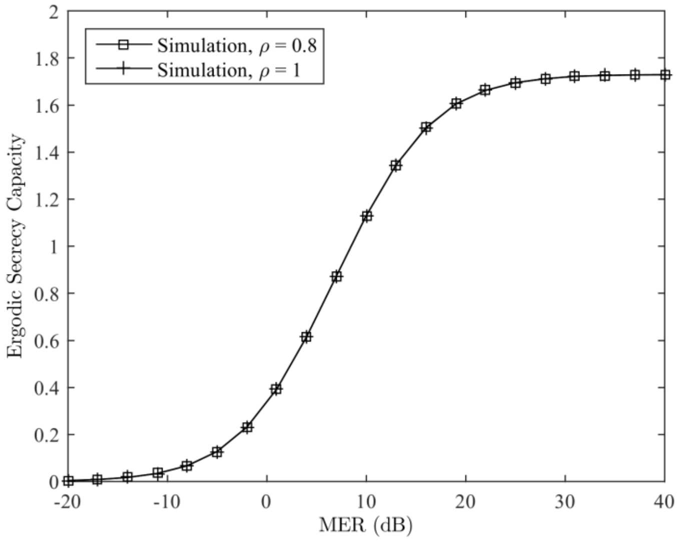

Figure 7. Ergodic Secrecy Capacity versus MER at Different Values of Correlation Coefficient ρ

Figure 7 plots the ergodic secrecy capacity as a function of MER at different values of the correlation coefficient ρ. As we can observe from Figure 7, the ergodic capacity increases as MER increases. In line with the previous results in Figure 3 and 4, the ergodic secrecy capacity does not change when we vary the value of correlation coefficient ρ.

As we can observe from the above results, the HI effect degrades the wireless communication performance and make it be more vulnerable. In contrast to HI, the correlation coefficient ρ between S-T and S-E channels does not affect the performance of secrecy outage probability.

5. Conclusions

In this paper, we study the physical layer security of wireless networks under the effects of hardware impairments. More specifically, we assume that the channel state information of the eavesdropper channel is not available at the source. Thus, one torch node is deployed close to the eavesdropper in order to estimate the eavesdropper channel's CSI. In addition, the practical issue on hardware impairment is taken into account at the source. The HI effect is characterized by the distortion noise and the level of HI κ. The security performance of the system has been investigated in terms of secrecy outage probability, probability of non-zero secrecy capacity, and ergodic secrecy capacity. More specifically, the closed-form expressions of secrecy outage probability and probability of non-zero secrecy capacity have been derived and validated by Monte-Carlo simulation. The numerical results show that the torch node can provide the good information of the eavesdropper channel since the correlate coefficient does not impact on the outage probability. On the other hand, the hardware impairment effects make the wireless transmission more vulnerable to the eavesdropper.

Acknowledgments

This research was supported by the MSIP (Ministry of Science, ICT and Future Planning), Korea, under the ICT/SW Creative Research program (IITP-2015-R2212150026) supervised by the IITP(Institute for Information & communication Technology Promotion).

References

[1] L. Dong, Z. Han, A. Petropulu and H. Poor, “Improving wireless physical layer security via cooperating relays”, IEEE Transactions on Signal Processing, vol. 58, no. 3, **(2010)**, pp. 1875-1888.

[2] A. D. Wyner, “The wire-tap channel”, Bell Syst. Tech. J., vol. 54, no. 8, **(1975)**, pp. 1355–1367.

[3] N. T. Do and B. An, “Secure transmission using decode-and-forward protocol for underlay cognitive radio networks”, Proceedings of the 7th International Conference on Ubiquitous and Future Networks, Sapporo, Japan, **(2015)** July 7-10.

[4] K. Shim, N. T. Do, B. An and S. Nam, “Outage performance of physical layer security for multi-hop underlay cognitive radio networks with imperfect channel state information”, Proceedings of the 15th International Conference on Electronics, Information, and Communication, Danang, Vietnam, **(2016)** January 27-30.

[5] Y. Zou, X. Wang and W. Shen, “Optimal Relay Selection for Physical-Layer Security in Cooperative Wireless Networks”, IEEE Journal in Selected Areas in Communications, vol. 31, no. 10, **(2013)**, pp. 2099-2111.

[6] V. N. Q. Bao, Linh-Trung N. and Debbah M., “Relay Selection Schemes for Dual-Hop Networks under Security Constraints with Multiple Eavesdroppers”, IEEE Transactions in Wireless Communications, vol. 12, no. 12, **(2013)**, pp. 6076-6085.

[7] 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, **(2014)**, pp. 2222-2236.

[8] Y. Choi and D. Kim, “Performance analysis with and without torch node in secure communications”, Proceedings of the 8th International Conference on Advanced technologies for Communications, Ho Chi Minh city, Vietnam, **(2015)** October 14-16.

[9] T. L. Thanh, V. N. Q. Bao and B. An, "On the performance of outage probability in underlay cognitive radio with imperfect CSI", 5th International 2013 Conference on Advanced Technologies for Communications, Ho Chi Minh city, Vietnam, **(2013)** October 16-18.

[10] E. Bjornson, M. Matthaiou and M. Debbah, "A New Look at Dual-Hop Relaying: Performance Limits with Hardware Impairments", IEEE Transactions on Communications, vol. 61, no. 11, **(2013)** pp. 4512-4525.

[11] M. Matthaiou, A. Papadogiannis, E. Bjornson and M. Debbah, "Two-Way Relaying Under the Presence of Relay Transceiver Hardware Impairments", IEEE Communications Letters, vol. 17, no. 6, **(2013)**, pp. 1136-1139.

[12] I. S. Gradshteyn, I. M. Ryzhik, A. Jeffrey and D. Zwillinger, "Table of integrals, series and products (7th editions)", Elsevier, **(2007)**.

[13] V. N. Q. Bao, N. Linh-Trung and M. Debbah, "Relay Selection Schemes for Dual-Hop Networks under Security Constraints with Multiple Eavesdroppers", IEEE Transactions on Wireless Communications, vol. 12, no. 12, **(2013)**, pp. 6076-6085.

Authors

Kyusung Shim, was born in Seoul, Republic of Korea. He received B. S. in computer and Information communications engineering from Hongik University, in 2012. Since 2015, he has been working as a M.S student in Information System Graduate School of Smart City Science Management, Hongik University, Republic of Korea. His major research interests are wireless communications, cognitive radio and physical layer security.

Nhu Tri Do was born in Danang, Vietnam. He received B.S. in electronics and communications engineering from the Posts and Telecommunications Institute of Technology, Vietnam, in 2012 and M.S. in electronics and computer engineering from Hongik University, Republic of Korea, in 2015. Since 2015, he has been working as a PhD student in the department of electronics and computer engineering at Hongik University, Republic of Korea. His major research interests are wireless communications, cognitive radio, and cooperative networks.

Beongku An received M.S. degree in Electrical Engineering from New York University (Polytechnic), NY, USA, in 1996 and Ph.D. degree from New Jersey Institute of Technology (NJIT), NJ, USA, in 2002, respectively. He received B.S. degree in electronic engineering from Kyungpook National University, Korea, in 1988. From 2003, he joined the Faculty of the Department of Computer and Information Communication Engineering, Hongik University in Korea, where he is currently a professor. From 1990 to 1994, he was a senior researcher in RIST, Pohang, Korea. He was a lecturer and RA in NJIT from 1997 to 2002. In 2012, he worked as a president in IEIE computer society in Korea, and from 2011 to 2016 as a general chair in International Conference, ICGHIT, respectively. His current research interests include wireless networks and wireless communications such as ad-hoc networks, sensor networks, wireless internet, ubiquitous networks, and cellular networks, cognitive radio networks, mobile clouding, IoT, visible light communications (VLC). Professor An was listed in Marquis Who's Who in Science and Engineering and Marquis Who in the World, respectively.