PHY Security Enhancement of Threshold-Based User Selection in Co-Channel Interference Environment

Tonny Ssettumba* , Ahmed H. Abd El-Malek* , Maha Elsabrouty* , Mohamed Abo-Zahhad*†
*Department of Electronics and Communications Engineering Egypt-Japan University of Science and Technology
New Borg El-Arab City, Alexandria, Egypt
E-mail: {ssettumba.tonny, ahmed.abdelmalek, maha.elsabrouty, mohammed.zahhad}@ejust.edu.eg
†Department of Electrical and Electronics Engineering, Assiut University, Assiut, Egypt

***Abstract*—This paper investigates the secrecy performance of a multiuser threshold-based transmit antenna selection scheme (TAS/tSD) in the presence of co-channel interference (CCI) signals and the existence of a passive eavesdropping node. In particular, an exact closed-form expression for the secrecy outage probability is derived. Then, the asymptotic secrecy outage closed-form expression is obtained at the high signal-to-noise ratio (SNR) values. Based on the obtained asymptotic analysis, an optimization problem for power allocation is formulated and solved to improve the secrecy performance of the system concerning minimizing the asymptotic secrecy outage probability. Numerical and simulation results are obtained to justify the obtained analysis.**

***Keywords*—Co-channel interference (CCI), Eavesdropper, Internet of Things (IoT), Legitimate node, Physical layer (PHY) security, Power allocation, Rayleigh fading, Secrecy outage probability.**

I. Introduction

Physical layer (PHY) security leverages the channel characteristics such as multi-path fading and interference to ensure secure communication in wireless networks in addition to higher layer encryption techniques applied to the protocol stack. Large-scale wireless networks such as Internet-of-Things (IoT) systems are expected to penetrate several areas such as military, government, home, and business applications. Consequently, ensuring security for such devices is of high priority. On the other hand, IoT nodes are usually deployed in a randomly distributed manner. Also, the broadcast nature of the wireless channel makes the IoT nodes liable or vulnerable to malicious jamming or eavesdroppers that tend to overhear the transmitted information [1].

Motivated by the rapidly increasing number of IoT devices in the future, PHY security applies secure-energy efficient schemes for IoT to maximize both energy efficiency and secrecy performance of the legitimate IoT node while impairing the performance of the eavesdropping node. Higher layers of the IoT protocol stack apply traditional encryption techniques to secure communication. The authors in [2] presented notable higher layer encryption techniques.

However, there is a need for low complexity techniques because of the limited hardware, small storage space, and low energy requirements that exist in IoT devices. Thus, PHY security has attracted increased attention because it provides a secure connection between the source and destination by using the wireless channel characteristics. The parameters used in PHY security to measure the system security performance include but not limited to secrecy capacity, secrecy outage probability (SOP), intercept probability (IP), and security reliability trade-off (SRT) among others [3]. A lot of work has been done in the past years more so in the area of multi-antennas to increase data rates and reduce erroneous reception of the signals.

However, the use of PHY security for transmit antenna selection (TAS) scheme has not been fully harnessed to ensure secure and efficient wireless communication systems. Much has been done in the TAS scheme because of its ability to achieve full diversity with an added advantage of low complexity in the realization of the radio frequency links [4].

In [5], [6], the analysis of the secrecy performance for multiple-input-multiple-output (MIMO) wiretap channels with TAS scheme with several receiver techniques and transmit techniques was done and power allocation was addressed for MIMO wiretap channels respectively. Moreover, the authors in [7] proposed a generalized selection combining (GSC) scheme to improve secrecy performance for MIMO wiretap channels. The secrecy performance for TAS/maximal ratio combining (MRC) system with imperfect feedback was addressed in [8].

The authors in [9] proposed a threshold- based channel strategy assuming independent but non-identically distributed channel conditions based on Markov chain theory. Closed-form expressions were obtained, and they were used to analyze the system performance of three communications scenarios (i.e., multi-channel reception, TAS with diversity reception, and cooperative relay selection). Reduction in computational complexity and energy efficiencies were achieved in this work.

In [10], the authors introduced a hybrid scheme combining TAS/threshold-based (TAS/tSD) with tSD selection diversity opportunistic scheduling in a multiuser multi-antenna wiretap network over Nakagami-m channels. Closed-form expressions were derived for the secrecy outage probability cases of no channel side information (CSI) of the eavesdropper (i.e., passive eavesdropper) at the base station (BS). Moreover, closed-form expressions were derived for the ergodic secrecy capacity for the case when the CSI of the eavesdropper is available. The authors in [11], made an investigation on the secure transmission in wireless sensor networks (WSNs) using one multiple-antenna base station (BS), multiple single-

antenna legitimate users, one single-antenna eavesdropper and one multiple-antenna cooperative jammer, two novel hybrid secure transmission schemes were proposed, that is; TAS-SSC-ZFB and TAS-SSC-NAN, for WSNs. In this work exact closed-form expressions for the secrecy outage probability and the effective secrecy throughput of both schemes were derived to characterize the secrecy performance. More specifically the optimal switching threshold and the optimal power allocation factor between the BS and jammer node for both schemes to minimize the secrecy outage probability, while the optimal secrecy rate is decided to maximize the effective secrecy throughput for both schemes were obtained. This work used numerical results to verify the paper's findings.

Based on the literature, it is clear that the secrecy performance of MIMO system especially TAS/tSD scheme has been investigated in different works. However, the impact of co-channel interference (CCI) on the secrecy performance of such scheme has not been addressed yet. Moreover, and to the best of authors knowledge, the power allocation problem for the TAS/tSD scheme to enhance the secrecy performance has not been investigated in previous works. Therefore, the main contributions of this work can be summarized as follows. First, the work study the impact of CCI signals on the secrecy performance of TAS/tSD user selection scheme where the user is selected when its effective signal-to-interference-plus-noise ratio (SINR) exceed a certain threshold. Such selection can be considered as an optimal user selection. Closed-form expression for the exact secrecy outage probability is obtained in the presence of a passive eavesdropper with unknown CSI at the base-station. Then, at the high signal-to-noise ratio (SNR) values, closed-form expression for the asymptotic secrecy outage probability is obtained.

Hence, a power allocation optimization problem is formulated to enhance the system secrecy performance where the obtained optimal power values are used for data transmission between the base station and the selected legitimate user to minimize the secrecy outage probability.

The rest of the paper is organized as follows. Section II discusses the proposed system model. Section III is dedicated to the statistical analysis of the secrecy performance. Moreover, the derivation of the exact secrecy outage probability and the asymptotic secrecy probability are presented in Section III. The proposed power allocation model is introduced in IV. The summary and simulation results of the paper are presented in Section V. Finally, we conclude the paper in Section VI.

Symbol terminologies: We use lower/upper bold case symbols to represent vectors/matrices, respectively. $\binom{\cdot}{\cdot}$ denotes the binomial coefficient and $|.|$ denotes the absolute value. $P_r[x]$ denotes the probability of event x to occur, the probability density function (pdf) and cumulative density function (CDF) of a random variable (RV) Y are represented by $f_Y(y)$ and $F_Y(y)$. $\mathbb{E}[.]$ represents the expectation notation as well as $\Gamma(x) = \int_0^\infty t^{x-1}\exp(-t)\,dt$ and $\Gamma(x,y) = \int_y^\infty t^{x-1}\exp(-t)\,dt$ denoting the Gamma function and incomplete Gamma function, respectively.

II. System Model and SINR Statistics

This section consists of two parts. In the first part, the proposed system model is introduced. Whereas, the second part provides the statistical analysis which will be used in next sections.

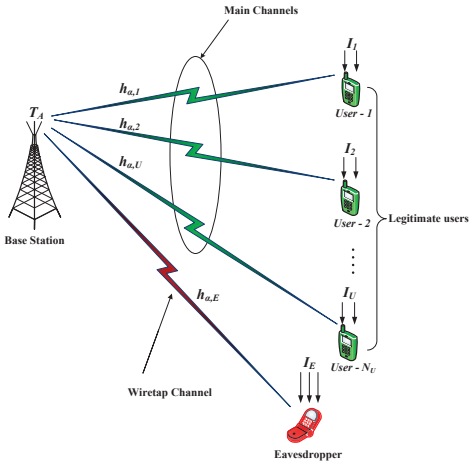

Fig. 1: System model for TAS/tSD user selection with CCI and a single eavesdropper.

A. System Model

The system model considers a multiuser downlink wiretap channel as shown in Figure 1, that comprises of a BS with T_A antennas which communicates with the selected user using the TAS/tSD scheme. For simplicity of the analysis and paper size limitations, a single antenna passive eavesdropping node (Bob) that works alone to avoid being overheard is considered. Also, for a practical scenario, both main and wiretap channels are assumed to suffer from CCI signals. Moreover, N_U users each is equipped with as single antenna are used to completely depict the distributed nature of an IoT system. Each legitimate link is assumed to follow independent and identically distributed (i.i.d.) flat Rayleigh fading distribution. In addition, each legitimate user u is assumed to suffer from a number of I_u identical CCI signals. Similarly, the eavesdropper node suffers from a number of I_E identical CCI signals.

The considered single-hop system operates as the BS applies TAS/tSD scheme to select the legitimate node for communication, i.e., the authorized node whose SINR exceeds a predefined threshold γ_T is selected for transmission. Hence, using the TAS/tSD scheme reduces the complexity of the system since there is no need for scanning all the available links compared to the basic TAS scheme [9]. Therefore, the received signal at the u-th legitimate node from the α-th antenna of the BS is given by

$$y_{\alpha,u} = \sqrt{P_\alpha} h_{\alpha,u} x + \sum_{i_u=1}^{I_u} \sqrt{P_{i_u}} h^I_{i_u,u} x_{i_u} + n_u, \qquad (1)$$

where P_α is the transmitted power from the BS to the selected legitimate user, $h_{\alpha,u}$ is the channel coefficient between the α-th antenna at the BS and the u-th legitimate user with $1 \leq \alpha \leq T_A$, and $1 \leq u \leq N_U$, x is the transmitted symbol to the selected legitimate user with zero mean and unit variance. P_{i_u} denotes the interference power at the u-th legitimate user, $h^I_{i_u,u}$ is the channel coefficient between the i_u-th interferer and the u-th legitimate node with $1 \leq i_u \leq I_u$, x_{i_u} is the transmitted symbol from the CCI sources with zero mean and

unit variance, I_u is the number of co-channel interferer existing with the u-th legitimate node. The term n_u is the additive white Gaussian noise (AWGN) sample at the u-th node with zero mean and unit variance.

Moreover, consider the existence of a passive eavesdropper close to the BS which tries to overhear the legitimate transmission. Similarly, the received signal at the eavesdropper node from the α-th antenna is given by:

$$y_{\alpha,E} = \sqrt{P_\alpha} h_{\alpha,E} x + \sum_{i_E=1}^{I_E} \sqrt{P_{i_E}} h^I_{i_E,E} x_{i_E} + n_E, \quad (2)$$

where $h_{\alpha,E}$ is the channel coefficient between the α-th antenna at BS and the eavesdropper, P_{i_E} is the interference power from the i_E-th interferer at the eavesdropper, $h^I_{i_E,E}$ is the channel coefficient between the i_E-th interferer and the eavesdropper, x_{i_E} is the transmitted symbol from the CCI interferer to the eavesdropper with zero mean and unit variance, I_E is the number of interferers at the eavesdropper, and n_E is the AWGN sample at the eavesdropper with zero mean and unit variance.

According to the capacity achieving codebook for the wiretap channel, in order to achieve a given secrecy, the BS encodes the message block $\mathbf{Z}$ into the codeword $\mathbf{y} = [y(1), ..., y(i), ...y(m)]$ with $\frac{1}{m}\sum_{i=1}^{m} \mathbb{E}\left[|y(i)|^2\right] \leq P_\alpha$ [9]. Thus, the received instantaneous SINRs $(\gamma_{\alpha,u}, \gamma_{\alpha,E})$ at both the u-th legitimate node and the eavesdropper are given by

$$\gamma_{\alpha,x} = \frac{\rho_\alpha |h_{\alpha,x}|^2}{\sum_{i_x=1}^{I_x} \rho_{i_x} \left|h^I_{i_x,x}\right|^2 + 1}, \quad (3)$$

where $x \in \{u, E\}$ denotes the legitimate user and eavesdropper nodes, respectively, $\rho_\alpha = \frac{P_\alpha}{N_0}$, $\rho_{i_x} = \frac{P_{i_x}}{N_0}$, and $P_{i_x} = \zeta P_\alpha$, with $0 \leq \zeta \leq 1$.

By applying the TAS/tSD scheme, the BS estimates if the instantaneous SINR of the selected antenna say $(\alpha = 1)$ exceeds the predefined threshold γ_T, when $\gamma^{\text{tSD}}_{1,u} > \gamma_T$ the tSD process terminates for this antenna. Otherwise, the procedure repeats up to when an antenna having an instantaneous SINR greater than γ_T is found. If the BS fails to find a user with an instantaneous SINR greater than γ_T, the BS selects the best user with the highest SINR following the conventional TAS scheme. For TAS/tSD scheme, the selected antenna-user pair is obtained by $\gamma_{\alpha,u^*} = \max\left(\gamma^{\text{tSD}}_{\alpha,u}\right)$ which defines the end-to-end (e2e) instantaneous SINR of the TAS/tSD scheme , the index of the selected antenna is $\alpha^* = \underset{1\leq\alpha\leq T_A}{\arg\max}(\gamma^{\text{tSD}}_{\alpha,u^*})$ [9].

B. Effective Received SINR Statistics

The channel coefficient between the α-th antenna and any node $x \in \{u, E\}$ is assumed to follow an i.i.d Rayleigh fading distribution. Hence, the pdf of the channel gain $\gamma_{h_{\alpha,x}}$ is

$$f_{\gamma_{h_{\alpha,x}}}(t) = \frac{1}{\bar{\gamma}_{\alpha,x}} \exp\left(-\frac{t}{\bar{\gamma}_{\alpha,x}}\right), \quad (4)$$

where $\bar{\gamma}_{\alpha,x} = \frac{P_\alpha}{N_0}\mathbb{E}\left[|h_{\alpha,x}|^2\right]) = \frac{P_\alpha}{N_0}\Omega_{\alpha,x}$ is the average SNR of the channel link. Where, $\mathbb{E}[.]$ is the expectation operator, and $\Omega_{\alpha,x}$ is the average channel gain between α and x. Moreover, for simplicity of analysis without loss in generality, the CCI signals are assumed to follow i.i.d Rayleigh fading distribution, and hence, the pdf of CCI signals is given by [12]

$$f_{\text{CCI}}(\gamma) = \frac{\gamma^{I_x-1}}{\bar{\gamma}^{I_x}_{i_x,x}\,(I_x-1)!} \exp\left(-\frac{\gamma}{\bar{\gamma}_{i_x,x}}\right), \quad (5)$$

where $\bar{\gamma}_{i_x,x} = \frac{\zeta P_\alpha}{N_0}\mathbb{E}\left[|h^I_{i_x,x}|^2\right]) = \frac{\zeta P_\alpha}{N_0}\Omega_{i_x,x}$ is the average interference plus noise ratio (INR) of the interference signal, and $\Omega_{i_x,x}$ is the average channel gain between i_x-th interferer and node $x \in \{u, E\}$. Thus, the pdf $f_{\gamma_{\alpha,x}}(\gamma)$ of the effective SINR at both the legitimate node and the eavesdropper can be expressed as [12]

$$f_{\gamma_{\alpha,x}}(\gamma) = \int_0^\infty (g+1) f_{\gamma_{h_{\alpha,x}}}((g+1)\gamma) f_{\text{CCI}}(g) dg. \quad (6)$$

By substituting (4) and (5) in (6) with some mathematical manipulations and the help of [13, (3.3381.4)] yields the pdf of the instantaneous SINRs at the legitimate node and eavesdropping node given by

$$f_{\gamma_{\alpha,x}}(\gamma) = \exp\left(-\frac{\gamma}{\bar{\gamma}_{\alpha,x}}\right)\left[\frac{I_x \Lambda_x^{I_x}}{(\gamma+\Lambda_x)^{I_x+1}} + \frac{1}{\bar{\gamma}_{\alpha,x}}\left(\frac{\Lambda_x}{\gamma+\Lambda_x}\right)^{I_x}\right], \quad (7)$$

where $\Lambda_x = \bar{\gamma}_{\alpha,x}/\bar{\gamma}_{i_x,x}$ with $x \in \{u, E\}$. Then, the corresponding CDFs for both legitimate user and eavesdropper can be expressed such as

$$F_{\gamma_{\alpha,x}}(\gamma) = 1 - \left(\frac{\Lambda_x}{\gamma+\Lambda_x}\right)^{I_x} \exp\left(-\frac{\gamma}{\bar{\gamma}_{\alpha,x}}\right), \quad (8)$$

III. Secrecy Performance Statistics and Analysis

In this section, we carry out a thorough analysis on the effective e2e SINR of the TAS/tSD diversity scheme defined prior as $\gamma^{tSD}_{\alpha^*,u^*}$. We derive the secrecy outage probability and asymptotic secrecy outage probability to completely study and get more insight on the system behavior in a more general case and in high SNR regime, respectively.

A. Preamble

Since the event of selecting a particular antenna for transmission according to the TAS scheme is mutually exlcusive for a specific antenna α, the CDF of the e2e instantaneous SINR $\gamma^{\text{tSD}}_{\alpha^*,u^*}(\gamma)$ is given such as [9]

$$F_{\gamma^{\text{tSD}}_{\alpha^*,u^*}}(\gamma) = \sum_{u=1}^{N_U} \Pr\left[\gamma^{\text{tSD}}_{\alpha^*,u^*}(\gamma) = \gamma_{\alpha,u}\ \&\ \gamma_{\alpha,u} \leq \gamma\right]. \quad (9)$$

Moreover from the assumption we made initially that each legitimate link follows i.i.d flat fading Rayleigh distribution, using related procedures , the end-to end instantaneous SINR can be expressed as [7], [9]

$$F_{\gamma^{tSD}_{\alpha^*,u^*}}(\gamma) = \begin{cases} F_{\gamma_{\alpha,u}}(\gamma) - F_{\gamma_{\alpha,u}}(\gamma_T) \\ +F_{\gamma_{\alpha,u}}(\gamma_T)\left[F_{\gamma_{\alpha,u}}(\gamma)\right]^{N_U-1}, & \gamma \geq \gamma_T \\ \left[F_{\gamma_{\alpha,u}}(\gamma)\right]^{N_U}, & \gamma < \gamma_T \end{cases} \quad (10)$$

where $F_{\gamma_{\alpha,u}}(\gamma)$ is given by (8). For $\gamma \geq \gamma_T$ (predefined threshold) the TAS/tSD is used, otherwise the BS has to scan through all the available legitimate nodes to select the best user and the CDF for tradition TAS is used as stated in (10)

by the second term of $\gamma < \gamma_T$. Hence, the CDF of the e2e instantaneous SINR for the TAS/tSD scheme is obtained by selecting the best antenna from the BS to transmit as in [9]

$$F_{\gamma_U}(\gamma) = \left(F^{\text{tSD}}_{\gamma_{\alpha^*,u^*}}(\gamma)\right)^{T_A}. \tag{11}$$

By substituting (8) and (10) in (11) with the help of binomial expansion [13, (1.111)], yields the CDF of γ_U such as

$$F_{\gamma_U}(\gamma) = \begin{cases} \sum\limits_{k=0}^{T_A} \binom{T_A}{k} \left[F_{\gamma_U}(\gamma_T)\right]^k \sum\limits_{k_1=0}^{k} \binom{k}{k1}(-1)^{k+k_1} \\ \times \sum\limits_{k_2=0}^{(N_U-1)k_1+T_A-k} \binom{(N_U-1)k_1+T_A-k}{k_2}(-1)^{k_2} \\ \times \left(\frac{\Lambda_U}{\gamma+\Lambda_U}\right)^{k_2 I_U} \exp\left(-\frac{k_2\gamma}{\bar{\gamma}_U}\right), & \gamma \geq \gamma_T \\ \sum\limits_{t=0}^{T_A N_U} \binom{T_A N_U}{t}(-1)^t \left(\frac{\Lambda_U}{\gamma+\Lambda_U}\right)^{tI_U} \exp\left(-\frac{t\gamma}{\bar{\gamma}_U}\right), & \gamma < \gamma_T \end{cases} \tag{12}$$

Moreover, the instantaneous secrecy capacity C_S of the considered system model can be expressed as [9]

$$C_S = [C_U - C_E]^+ = \max(C_U - C_E, 0) \tag{13}$$

where $C_U = \log(1+\gamma_U)$, and $C_E = \log(1+\gamma_E)$ with $\gamma_U = \gamma_{\alpha^*,u^*}$, and $\gamma_E = \gamma_{\alpha^*,E}$, respectively. As stated earlier, this work considers a passive eavesdropping scenario such that the eavesdropper channel side information (ECSI) is unavailable at the BS, thus the BS assumes the instantaneous rate of the eavesdropping channel as $C_S = C_U - R_s$ for secure transmission, where R_s is a constant secrecy rate set by BS.

The BS utilizes C_U and C_E to construct wiretap codes. If $R_s \leq C_S$, the codewords insure a perfect secrecy. Otherwise, the secrecy is compromised [9]. Therefore, the secrecy outage probability (SOP) which is discussed and derived in the next section is the best performance metric to consider in this case.

B. Secrecy Outage Probability Analysis

One of the key performance metrics for measuring the secrecy performance of a communication system is the secrecy outage probability. A secrecy outage occurs provided that the current secrecy rate R_S is less than a predefined threshold C_S . This implies that R_S cannot guarantee the security requirement of the system. The secrecy outage probability for measuring the likelihood that a secrecy outage occurs with a particular fading distribution can be given as $P_{\mathsf{out}}(R_s) = \Pr[R_s < C_S]$ expressed mathematically as [9]

$$\begin{aligned} P_{\mathsf{out}}(R_s) &= \Pr(C_s < R_s | \gamma_U > \gamma_E) \Pr(\gamma_U > \gamma_E) \\ &\quad + \Pr(\gamma_U < \gamma_E), \\ &= \int_0^{\infty} \int_0^{2^{R_s}(1+y)-1} f_{\gamma_U}(x) f_{\gamma_E}(y) dx dy \\ &= \int_0^{\infty} F_{\gamma_U}(2^{R_s}(1+y)-1) f_{\gamma_E}(y) dy \end{aligned} \tag{14}$$

where, $f_{\gamma_U}(x)$ is the pdf of γ_U. Using the fact that the CDF in (12) contains the predefined threshold γ_T, a relationship exists between $2^{R_s}(1+y)-1$ and γ_T in (14) for $2^{R_s}(1+y)-1 \geq \gamma_T$ or $2^{R_s}(1+y)-1 < \gamma_T$. Thus, the piecewise $P_{\mathsf{out}}(R_s)$ w.r.t. a bound point $H(\gamma_T) = 2^{-R_s}(\gamma_T+1)-1$ is given by

$$P_{\mathsf{out}}(R_s) = \begin{cases} \int_0^{H(\gamma_T)} F_{\gamma_U}(\Theta_y) f_{\gamma_E}(y) dy \\ + \int_{H(\gamma_T)}^{\infty} F_{\gamma_U}(\Theta_y) f_{\gamma_E}(y) dy, & H(\gamma_T) \geq 0 \\ \int_0^{\infty} F_{\gamma_U}(\Theta_y) f_{\gamma_E}(y) dy, & H(\gamma_T) < 0 \end{cases}, \tag{15}$$

where $\Theta(y) = 2^{R_s}(y+1)-1$. Using the integral formulas in [13, (3.462.15), (3.462.16), and (3.462.17)] in (15) with some mathematical manipulations yields $P_{\mathsf{out}}(R_s)$ which is given by

$$P_{\mathsf{out}}(R_s) = \begin{cases} \Delta_1 + \Delta_2, & H(\gamma_T) \geq 0 \\ \Delta_3, & H(\gamma_T) < 0 \end{cases}, \tag{16}$$

where, Δ_1, Δ_2 and Δ_3 are given by (17), (18) and (19) respectively.

C. Asymptotic Analysis

In order to gain more insights, the asymptotic secrecy outage probability is derived to facilitate the analysis. Using Taylor's series expansion on (8) as $\bar{\gamma}_U \to \infty$ yields $F_{\gamma_{\alpha,x}}(\gamma) \backsimeq \frac{\gamma}{\bar{\gamma}_U}(I_U \bar{\gamma}_{i_U} + 1)$, substituting this in (10) yields the asymptotic CDF of the e2e SINR given by

$$F^{\infty}_{\gamma_U}(\gamma) \simeq \begin{cases} \sum\limits_{k=0}^{T_A} \binom{T_A}{k} \left[\frac{\gamma_T}{\bar{\gamma}_U}(I_u \bar{\gamma}_{i_U} + 1)\right]^k \sum\limits_{k_1=0}^{k} \binom{k}{k_1}(-1)^k_1 \\ \times \left[\frac{\gamma}{\bar{\gamma}_U}(I_U \bar{\gamma}_{i_U} + 1)\right]^{(N_U-1)k_1+T_A-k}, & \gamma \geq \gamma_T \\ \left[\frac{\gamma}{\bar{\gamma}_U}(I_U \bar{\gamma}_{i_U} + 1)\right]^{N_U T_A}, & \gamma < \gamma_T \end{cases}, \tag{20}$$

Hence, by substituting (20) in (15), and following the mathematical manipulations as shown in Appendix B, the asymptotic secrecy outage probability $P^{\infty}_{\mathsf{out}}(R_s)$ is given by (21).

IV. Proposed Power Allocation Model

In this section, a power allocation optimization problem is formulated and solved to improve the secrecy performance of the considered system against a single eavesdropping attack in the presence of CCI signals. To do so, we use the obtained expression for the asymptotic secrecy outage probability in the high SNR regions as both $\bar{\gamma}_U \to \infty$ and $\bar{\gamma}_E \to \infty$ to formulate the optimization problem.

For the derived asymptotic outage probability in (21) and with some mathematical manipulation, it can be shown that the first term in the case of $H(\gamma_T) \geq 0$ varnishes to 0 as $\bar{\gamma}_E \to \infty$, and the term $H(\gamma_T)$ is very small compared to $\gamma_{\alpha^*,E}$ which can be neglected. Moreover, the incomplete gamma function $\Gamma(s,x)$ is expressed in its series representation with gamma function $\Gamma(.)$, and hence, the asymptotic secrecy outage probability in (21) can be simplified to (22) after representing $\bar{\gamma}_U = \frac{P_\alpha \Omega_{\alpha^*,u^*}}{N_0}$, $\bar{\gamma}_E = \frac{P_\alpha \Omega_{\alpha^*,E}}{N_0}$, $\bar{\gamma}_{I_U} = \frac{\zeta P_\alpha \Omega_{I_U,U}}{N_0}$, $\bar{\gamma}_{I_E} = \frac{\zeta P_\alpha \Omega_{I_E,E}}{N_0}$. where,

$$\Delta_1 = \sum_{t=0}^{T_A N_U} \binom{T_A N_U}{t} (-1)^t \exp(\theta) \left[(\beta_1+\beta_2) \sum_{t_1=1}^{tI_U} A_{t_1} \Theta_1^{t_1-1} \exp\left(\Theta_1 \Lambda'\right) \left[\Gamma\left(-t_1+1, \Lambda' \Theta_1\right) - \Gamma\left(-t_1+1, \Theta_1\left(\Lambda' + H(\gamma_T)\right)\right)\right] \right.$$
$$+\beta_1 \sum_{t_2=1}^{I_E+1} B_{t_2} \Theta_1^{t_2-1} \exp(\Theta_1 \Lambda_E) \left[\Gamma(-t_2+1, \Lambda_E \Theta_1) - \Gamma(-t_2+1, \Theta_1(\Lambda_E + H(\gamma_T)))\right] + \beta_2 \sum_{t_3=1}^{I_E} B_{t_3} \Theta_1^{t_3-1} \exp(\Theta_1 \Lambda_E)$$
$$\left. \times \left[\Gamma(-t_3+1, \Lambda_E \Theta_1) - \Gamma(-t_3+1, \Theta_1(\Lambda_E + H(\gamma_T)))\right]\right] \tag{17}$$

$$\Delta_2 = \sum_{k=0}^{T_A} \binom{T_A}{k} \left[F_{\gamma_U}(\gamma_T)\right]^k \sum_{k_1=0}^{k} \binom{k}{k_1} (-1)^{k+k_1} \sum_{k_2=0}^{(N_U-1)k_1+T_A-k} \binom{(N_U-1)k_1+T_A-k}{k_2} (-1)^k \exp(\phi) \left[\frac{\Lambda_U}{\delta}\right]^{k_2 I_U}$$
$$\times \left[(\mu_1+\mu_2) \sum_{q=1}^{kI_U} A_q \Theta_2^{q-1} \exp\left(\Theta_2 \Lambda'\right) \Gamma\left(-q+1, \Theta_2\left(\Lambda' + H(\gamma_T)\right)\right) + \mu_1 \sum_{q_1=1}^{I_E+1} B_{q_1} \Theta_2^{q_1-1} \exp(\Theta_2 \Lambda_E) \right.$$
$$\left. \times \Gamma(-q_1+1, \Theta_2(\Lambda_E + H(\gamma_T))) + \mu_2 \sum_{q_2=1}^{I_E} B_{q_2} \Theta_2^{q_2-1} \exp(\Theta_2 \Lambda_E) \Gamma(-q_2+1, \Theta_2(\Lambda_E + H(\gamma_T)))\right] \tag{18}$$

$$\Delta_3 = \sum_{k=0}^{T_A} \binom{T_A}{k} \left[F_{\gamma_U}(\gamma_T)\right]^k \sum_{k_1=0}^{k} \binom{k}{k_1} (-1)^{k+k_1} \sum_{k_2=0}^{(N_U-1)k_1+T_A-k} \binom{(N_U-1)k_1+T_A-k}{k_2} (-1)^k \exp(\phi) \left[\frac{\Lambda_U}{\delta}\right]^{k_2 I_U}$$
$$\times \left[(\mu_1+\mu_2) \sum_{q=1}^{kI_U} A_q \Theta_2^{q-1} \exp\left(\Theta_2 \Lambda'\right) \Gamma\left(-q+1, \Theta_2 \Lambda'\right) + \mu_1 \sum_{q_1=1}^{I_E+1} B_{q_1} \Theta_2^{q_1-1} \exp(\Theta_2 \Lambda_E) \Gamma(-q_1+1, \Theta_2 \Lambda_E) \right.$$
$$\left. + \mu_2 \sum_{q_2=1}^{I_E} B_{q_2} \Theta_2^{q_2-1} \exp(\Theta_2 \Lambda_E) \Gamma(-q_2+1, \Theta_2 \Lambda_E)\right] \tag{19}$$

where, $\delta = 2^{R_s}$, $\Lambda^0 = \frac{\delta-1}{\delta}$, $\theta = t\frac{1-\delta}{\bar{\gamma}_U}$, $\Lambda' = \frac{\delta-1+\Lambda_U}{\delta}$, $\Theta_1 = \frac{\delta t}{\bar{\gamma}_U} + \frac{1}{\bar{\gamma}_E}$, $\phi = k_2\frac{1-\delta}{\bar{\gamma}_U}$, $\Theta_2 = \frac{\delta k_2}{\bar{\gamma}_U} + \frac{1}{\bar{\gamma}_E}$, $\mu_1 = I_E \Lambda_E^{I_E}$, $\mu_2 = \frac{\Lambda_E^{I_E}}{\bar{\gamma}_E}$, $\beta_1 = \mu_1 \left[\frac{\Lambda_U}{\delta}\right]^{tI_U}$, $\beta_2 = \mu_2 \left[\frac{\Lambda_U}{\delta}\right]^{tI_U}$ Moreover, $A_{(.)}$ and $B_{(.)}$ are the partial fraction coefficients (Please see Appendix A).

$$P_{\mathsf{out}}^{\infty}(R_s) \simeq \begin{cases} \left[\left(\frac{\delta}{\bar{\gamma}_U}\right)(I_u\bar{\gamma}_{i,U}+1)\right]^{T_A N_U} \left\{ I_E \Lambda_E^{I_E} \exp\left(\frac{\Lambda_E}{\bar{\gamma}_E}\right) \left[\sum_{r_1=0}^{T_A N_U} \binom{T_A N_U}{r_1} \left(\Lambda^0 - \Lambda_E\right)^{T_A N_U - r_1} \bar{\gamma}_E^{r_1 - I_E} \Gamma\left(r_1 - I_E, \frac{\Lambda_E}{\bar{\gamma}_E}\right) - \Gamma\left(r_1 - I_E \right.\right.\right. \\ \left.\left.\left., \frac{\Lambda_E + H(\gamma_T)}{\bar{\gamma}_E}\right) + \frac{\Lambda_E^{I_E}}{\bar{\gamma}_E} \sum_{r_2=0}^{T_A N_U} \binom{T_A N_U}{r_2} \left(\Lambda^0 - \Lambda_E\right)^{T_A N_U - r_2} \bar{\gamma}_E^{r_2 - I_E + 1} \Gamma\left(r_2 - I_E + 1, \frac{\Lambda_E}{\bar{\gamma}_E}\right) - \Gamma\left(r_2 - I_E + 1, \frac{\Lambda_E + H(\gamma_T)}{\bar{\gamma}_E}\right) \right] \right\} \\ + \sum_{k=0}^{T_A} \binom{T_A}{k} \left[(\gamma_T/\bar{\gamma}_U)(I_u\bar{\gamma}_{i,U}+1)\right]^k (-1)^k \sum_{k_1=0}^{k} \binom{k}{k_1} (-1)^{k_1} \left[(\delta/\bar{\gamma}_U)(I_u\bar{\gamma}_{i,U}+1)\right]^{(N_U-1)K_1+T_A-k} (-1)^k \left\{ I_E \Lambda_E^{I_E} \right. \\ \times \exp\left(\frac{\Lambda_E}{\bar{\gamma}_E}\right) \left[\sum_{p_1=0}^{(N_U-1)k_1+T_A-k} \binom{(N_U-1)k_1+T_A-k}{p_1} \left(\Lambda^0 - \Lambda_E\right)^{(N_U-1)k_1+T_A-k} \bar{\gamma}_E^{p_1 - I_E} \Gamma\left(p_1 - I_E, \frac{\Lambda_E + H(\gamma_T)}{\bar{\gamma}_E}\right) \right. \\ \left. \left. + \frac{\Lambda_E^{I_E}}{\bar{\gamma}_E} \sum_{p_2=0}^{(N_U-1)k_1+T_A-k} \binom{(N_U-1)k_1+T_A-k}{p_2} \left(\Lambda^0 - \Lambda_E\right)^{(N_U-1)k_1+T_A-k} \bar{\gamma}_E^{p_2 - I_E + 1} \Gamma\left(p_2 - I_E + 1, \frac{\Lambda_E + H(\gamma_T)}{\bar{\gamma}_E}\right) \right] \right\}, H(\gamma_T) \geq 0 \\ \sum_{k=0}^{T_A} \binom{T_A}{k} \left[(\gamma_T/\bar{\gamma}_U)(I_u\bar{\gamma}_{i,U}+1)\right]^k (-1)^k \sum_{k_1=0}^{k} \binom{k}{k_1} (-1)^{k_1} \left[(\delta/\bar{\gamma}_U)(I_u\bar{\gamma}_{i,U}+1)\right]^{(N_U-1)K_1+T_A-k} (-1)^k \left\{ I_E \Lambda_E^{I_E} \right. \\ \times \exp\left(\frac{\Lambda_E}{\bar{\gamma}_E}\right) \left[\sum_{v_1=0}^{(N_U-1)k_1+T_A-k} \binom{(N_U-1)k_1+T_A-k}{v_1} \left(\Lambda^0 - \Lambda_E\right)^{(N_U-1)k_1+T_A-k-v_1} \bar{\gamma}_E^{v_1 - I_E} \Gamma\left(v_1 - I_E, \frac{\Lambda_E}{\bar{\gamma}_E}\right) \right. \\ \left. \left. + \frac{\Lambda_E^{I_E}}{\bar{\gamma}_E} \sum_{v_2=0}^{(N_U-1)k_1+T_A-k} \binom{(N_U-1)k_1+T_A-k}{v_2} \left(\Lambda^0 - \Lambda_E\right)^{(N_U-1)k_1+T_A-k-v_2} \bar{\gamma}_E^{v_2 - I_E + 1} \Gamma\left(v_2 - I_E + 1, \frac{\Lambda_E}{\bar{\gamma}_E}\right) \right] \right\}, H(\gamma_T) < 0 \end{cases} \tag{21}$$

$$P_{\mathsf{out}}^{\infty}=\begin{cases}\sum\limits_{k=0}^{T_A}\sum\limits_{k_1=0}^{k}\varphi_1\left[\sum\limits_{v_1=0}^{(N_U-1)k_1+T_A-k}\sum\limits_{u_1=0}^{v_1-I_E-1}\varphi_2 P_{\alpha}^{u_1-(N_U-1)k_1-T_A+1}+\sum\limits_{v_2=0}^{(N_U-1)k_1+T_A-k}\sum\limits_{u_2=0}^{v_2-I_E-1}\varphi_3 P_{\alpha}^{u_2-(N_U-1)k_1-T_A}\right], H(\gamma_T)\geq 0\\ \sum\limits_{k=0}^{T_A}\sum\limits_{k_1=0}^{k}\varphi_1\left[\sum\limits_{p_1=0}^{(N_U-1)k_1+T_A-k}\sum\limits_{w_1=0}^{p_1-I_E-1}\varphi_4 P_{\alpha}^{w_1-(N_U-1)k_1-T_A+1}+\sum\limits_{p_2=0}^{(N_U-1)k_1+T_A-k}\sum\limits_{w_2=0}^{p_2-I_E-1}\varphi_5 P_{\alpha}^{w_2-(N_U-1)k_1-T_A}\right], H(\gamma_T)<0\end{cases} \tag{22}$$

where,

$$\varphi_1=\binom{T_A}{k}(\gamma_T)^k(-1)^k\binom{k}{k_1}(-1)^{k_1}\delta^{(N_U-1)k_1+T_A-k}\left[\frac{N_0\left(\gamma_{i,U}I_U+1\right)}{\Omega_{\alpha,U}}\right]^{(N_U-1)k_1+T_A}$$

$$\varphi_2=I_E\Lambda_E^{I_E}\binom{(N_U-1)k_1+T_A-k}{v_1}\left(\Lambda^0-\Lambda_E\right)^{(N_U-1)k_1+T_A-k-v_1}\binom{v_1-I_E-1}{u_1}\Lambda_E^{v_1-I_E-u_1-1}\left(\frac{\Omega_{\alpha,E}}{N_0}\right)^{u_1+1}\Gamma(u_1+1)$$

$$\varphi_3=\Lambda_E^{I_E}\binom{(N_U-1)k_1+T_A-k}{v_2}\left(\Lambda^0-\Lambda_E\right)^{(N_U-1)k_1+T_A-k-v_2}\binom{v_2-I_E}{u_2}\Lambda_E^{v_2-I_E-u_2}\left(\frac{\Omega_{\alpha,E}}{N_0}\right)^{u_2+1}\Gamma(u_2+1)$$

$$\varphi_4=I_E\Lambda_E^{I_E}\binom{(N_U-1)k_1+T_A-k}{p_1}\left(\Lambda^0-\Lambda_E\right)^{(N_U-1)k_1+T_A-k-p_1}\binom{p_1-I_E-1}{w_1}\Lambda_E^{p_1-I_E-w_1-1}\left(\frac{\Omega_{\alpha,E}}{N_0}\right)^{w_1+1}\Gamma(w_1+1)$$

$$\varphi_5=\Lambda_E^{I_E}\binom{(N_U-1)k_1+T_A-k}{p_2}\left(\Lambda^0-\Lambda_E\right)^{(N_U-1)k_1+T_A-k-p_2}\binom{p_2-I_E}{w_2}\Lambda_E^{p_2-I_E-w_2}\left(\frac{\Omega_{\alpha,E}}{N_0}\right)^{w_2+1}\Gamma(w_2+1)$$

P_{α} is the system transmission power, $P_{\mathsf{out}}^{\infty}(R_s)$ is the asymptotic secrecy outage probability that surpass the minumum secrecy outage probability when P_{α} the system transmission power is used for only transmission. The optimisation problem was then formulated such as

$$\underset{P_{\alpha}}{\text{Minimize}} \quad P_{\mathsf{out}}^{\infty}(R_s) \quad \text{Subject to}: \quad 0<P_{\alpha}<P_{\max} \tag{23}$$

By differentiating (22) w.r.t. P_{α} and equating to zero such as shown in (24), the optimal power can be obtained. Moreover, (24) is a polynomial in P_{α} that can be solved by any software package to obtain the optimal power.

V. Simulation Results

In this section, some numerical results are presented to validate the derived analytical expressions for the secrecy outage probability and the proposed power allocation model.

The system secrecy outage probability against $\bar{\gamma}_U$ for different number of CCI interferers at the eavesdropper I_E is presented in Figure 2. It is shown that increasing I_E enhances the system secrecy performance as expected since the eavesdropper will be harmed deeply by the increasing the interferers. Moreover, the figure illustrates that the exact analytical analysis match both simulation results and asymptotic analysis at medium to high $\bar{\gamma}_U$ values.

The impact of the number of BS antennas T_A on the system secrecy performance against SNR is investigated in Figure 3. The results show that increasing T_A improves the secrecy performance due to the fact that increasing T_A increases the diversity order of the TAS/tSD scheme even in the presence of co-channel interference. Moreover, it is shown that the asymptotic results comply with the exact results in the high SNR values. However, For $T_A=4$, the figure shows a floor in the secrecy performance at the high SNR values. This can be explained as the system performance is dominated by the CCI signals which limits the system secrecy performance.

Figure 4 studies the impact of CCI signals and the constant secrecy rate R_s on the system secrecy performance against $\bar{\gamma}_U$. It is clear that the secrecy outage probability reduces in presence of a high number of interferers at the eavesdropper I_E compared to the number of interferers at the selected legitimate node I_U (i.e., $I_E > I_U$), which improves the secrecy performance of the system. This can be explained as I_E reduces the SINR of the eavesdropper compared to that of the legitimate node, consequently, the main channel is more secure compared to the wiretap channel which enhances the secrecy performance. On the other hand, increasing I_U compared to I_E degrades the system secrecy performance. Moreover, increasing the predefined secrecy rate R_s degrades the secrecy performance of the system since the difference between main channel capacity C_U and the wiretap channel capacity C_E must be greater than R_s in order to guarantee secure transmission which increases the possibility of secrecy outage.

The system secrecy outage probability versus $\bar{\gamma}_U$ for different values of predefined threshold (γ_T) with optimal power allocation solutions P_{α}^{*} and maximum power model (i.e., $P_{\alpha}=1$) is investigated in Figure 5. The results show that the proposed power allocation model has a close performance to the maximum power at low to medium $\bar{\gamma}_U$ values. However, as $\bar{\gamma}_U$ keeps increasing, the optimal power allocation model outperforms the maximum power model for different values (γ_T). This can be explained in a way that the proposed power allocation model optimization problem was formulated based on the asymptotic analysis for high SNR values. Hence, the proposed power allocation model is expected to perform in a more accurate way at high SNR values. However, the performance of the proposed power allocation model are still acceptable compared to the maximum power model at low SNR values. These findings clarify the importance of the proposed power allocation model as it improves the secrecy performances of the system which enhances the work contribution.

$$\frac{dP_{\text{out}}^{\infty}}{dP_{\alpha}}=\begin{cases}\sum\limits_{k=0}^{T_A}\sum\limits_{k_1=0}^{k}\varphi_1\left[\sum\limits_{v_1=0}^{(N_U-1)k_1+T_A-k}\sum\limits_{u_1=0}^{v_1-I_E-1}\widehat{\varphi}_2 P_{\alpha}^{u_1-(N_U-1)k_1-T_A}+\sum\limits_{v_2=0}^{(N_U-1)k_1+T_A-k}\sum\limits_{u_2=0}^{v_2-I_E-1}\widehat{\varphi}_3 P_{\alpha}^{u_2-(N_U-1)k_1-T_A-1}\right], H(\gamma_T)\geq 0\\ \sum\limits_{k=0}^{T_A}\sum\limits_{k_1=0}^{k}\varphi_1\left[\sum\limits_{p_1=0}^{(N_U-1)k_1+T_A-k}\sum\limits_{w_1=0}^{p_1-I_E-1}\widehat{\varphi}_4 P_{\alpha}^{w_1-(N_U-1)k_1-T_A}+\sum\limits_{p_2=0}^{(N_U-1)k_1+T_A-k}\sum\limits_{w_2=0}^{p_2-I_E-1}\widehat{\varphi}_5 P_{\alpha}^{w_2-(N_U-1)k_1-T_A-1}\right], H(\gamma_T)<0\end{cases} \tag{24}$$

where $\widehat{\varphi}_2 = (u_1-(N_U-1)k_1-T_A+1)\,\varphi_2$, $\widehat{\varphi}_3 = (u_2-(N_U-1)k_1-T_A)\,\varphi_3$, $\widehat{\varphi}_4 = (v_1-(N_U-1)k_1-T_A+1)\,\varphi_4$, and $\widehat{\varphi}_5 = (v_2-(N_U-1)k_1-T_A)\,\varphi_5$.

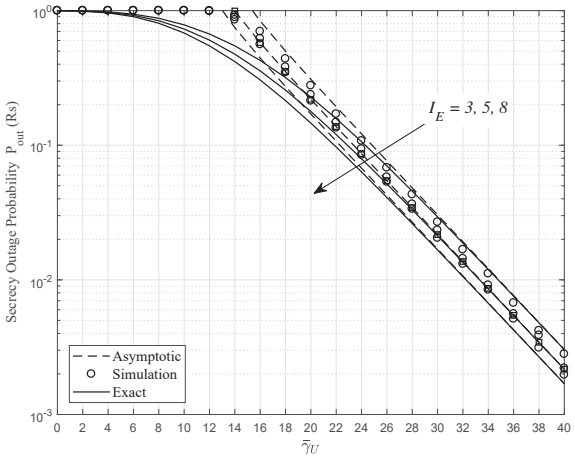

Fig. 2: Secrecy outage probability against $\bar{\gamma}_U$ for different number of I_E with $P_\alpha = 1, I_U = 3, \gamma_T = 5$ dB, SNR $= 10$ dB, $\bar{\gamma}_{i_U,U} = 2$ dB, $\bar{\gamma}_{i_E,E} = 1$ dB, $\bar{\gamma}_E = 0$ dB, $R_s = 4$, and $\zeta = 0.15$.

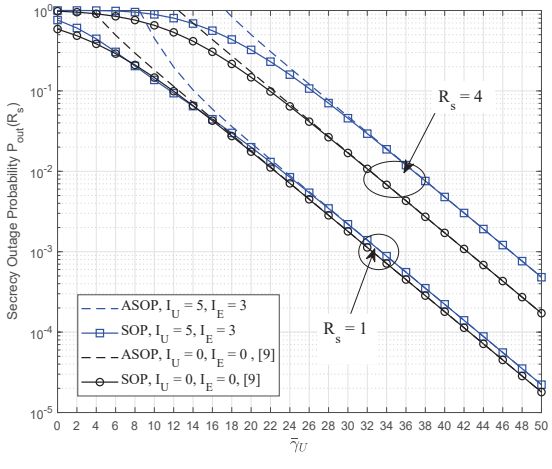

Fig. 4: Secrecy outage probability against $\bar{\gamma}_U$ in the presence of different interferers at the eavesdropper and legitimate nodes with $T_A = 1, N_U = 3, P_\alpha = 1, \gamma_T = 10$ dB, SNR $= 10$ dB, $\bar{\gamma}_{i_U,U} = 2$ dB, $\bar{\gamma}_{i_E,E} = 1$ dB, $\bar{\gamma}_E = 0$ dB, and $\zeta = 0.15$.

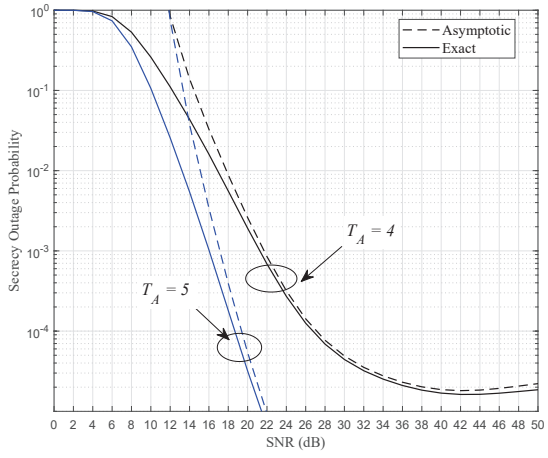

Fig. 3: Secrecy outage probability against SINR for different number of Transmit Antennas with $P_\alpha = 1, I_U = 3, I_E = 5, \gamma_T = 5$ dB, $\bar{\gamma}_{i_U,U} = -5$ dB, $\bar{\gamma}_{i_E,E} = -2$ dB, $\bar{\gamma}_E = 10$ dB, $R_s = 4$, and $\zeta = 0.15$.

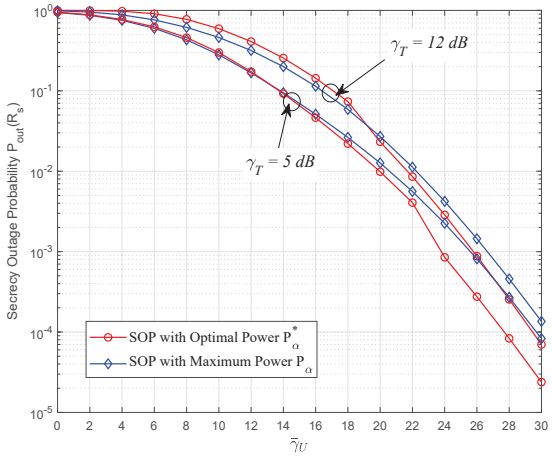

Fig. 5: Secrecy outage probability against $\bar{\gamma}_U$ for different constant secrecy rate γ_T, set by the BS with $T_A = 3, N_U = 3, P_\alpha = 1$, SNR $= 10$ dB, $\bar{\gamma}_{i_U,U} = 2$ dB, $\bar{\gamma}_{i_E,E} = 1$ dB, $\bar{\gamma}_E = 0$ dB, $R_s = 4, I_E = I_K = 2$, and $\zeta = 0.15$.

VI. Conclusion

In this paper, the effect of co-channel interference on the secrecy performance of TAS/tSD scheme was investigated for large-scale wireless networks in the presence of a single passive eavesdropper. The identical CCI signals were assumed to harm both the legitimate nodes and the eavesdropper. Closed-form expressions for the exact and asymptotic secrecy outage probabilities were derived. Moreover, a novel power allocation model was proposed to enhance the secrecy performance by minimizing the asymptotic secrecy outage probability. The optimization problem was formulated, and the solution for optimal transmission power was obtained. The results show that the increase in the number of interferers at the eavesdropper compared to the legitimate nodes improves the secrecy performance. On the other hand, increase in the number of interferers at the authorized node harms the secrecy performance of the system. Moreover, the performance of the proposed power allocation model outperforms that of the maximum power model in literature which emphasizes the importance of the work contributions.

Acknowledgment

This work has been supported by Egypt Japan University of Science and Technology (E-JUST), and the Egyptian Ministry of Higher Education (MoHE).

Appendix A

Consider the solution of the integral below for Secrecy outage derivation that gives the solution given as

$$\int_0^\infty \frac{\exp(-x)}{(x+m)^{T_A N_U}(x+n)^{I_E}}dx = \sum_q^{T_A N_U} A_q \int_0^\infty \frac{\exp(-x)}{(x+m)^q}dx + \sum_k^{I_E} B_k \int_0^\infty \frac{\exp(-x)}{(x+n)^k}dx. \quad (25)$$

With the help of [13, (3.462.15), (3.462.16), and (3.462.17)], the bove integrals can be compared such as

$$\int_0^\infty \frac{1}{(x+n)^k}\exp(-x)\,dx = \exp(m)\Gamma(-k+1,m) \quad (26)$$

to obtain $\Gamma(x,r)$ which is the incomplete gamma function

Appendix B

Consider the following integral that yields the incomplete gamma function comparable to [13, (8.352)] with application of the binomial expansion in [13, (1.111)].

$$\int_0^\infty \frac{(x+n)^A}{(x+m)^k}\exp(-x)\,dx = \exp(m)\sum_{f=0}^{A}\beta^{A-f} \times \int_m^\infty y^{f-k}\exp(-y)dy = \exp(m)\sum_{f=0}^{A}\beta^{A-f}\Gamma(f-k+1,m) \quad (27)$$

where m, $\beta = n-m$, k, n, and A are constants. $y = x+m$ is the change of variables and $\Gamma(x,r)$ is the incomplete gamma function given in [13, (8.352)].

References

[1] A. Soni, R. Upadhyay, and A. Jain, "Internet of things and wireless physical layer security: A survey," in *Proc. Springer Comput. Commun., Netw. and Internet Security Conf.*. Singapore, 2017, pp. 115–123.

[2] H.-M. Wang and T.-X. Zheng,"Physical layer security in random cellular networks," *Springer, 2016*.

[3] A. Mukherjee, "Physical-layer security in the Internet of things: Sensing and communication confidentiality under resource constraints," in *Proc. of the IEEE*, vol. 103, no. 10, pp. 1747–1761, September 2015.

[4] F. A. Khan, K. Tourki, M.-S. Alouini, and K. A. Qaraqe, "Outage and SER performance of spectrum sharing system with TAS/MRC," in *Proc. IEEE Int'l Conf. Commun. Workshops (ICC 2013)*. Budapest, Hungary, 9-13 June 2013, pp. 381–385.

[5] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and I. B. Collings, "Transmit antenna selection for security enhancement in MIMO wiretap channels," *IEEE Trans. Commun.*, vol. 61, no. 1, pp. 144–154, January 2013.

[6] S. Yan, N. Yang, R. Malaney, and J. Yuan, "Transmit antenna selection with Alamouti coding and power allocation in MIMO wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 13, no. 3, pp. 1656–1667, March 2014.

[7] P. S. Bithas, A. A. Rontogiannis, and G. K. Karagiannidis, "An improved threshold-based channel selection scheme for wireless communication systems," *IEEE Trans. Wireless Commun.*, vol. 15, no. 2, pp. 1531–1546, February 2016.

[8] J. Xiong, Y. Tang, D. Ma, P. Xiao, and K.-K. Wong, "Secrecy performance analysis for TAS-MRC system with imperfect feedback," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 8, pp. 1617–1629, August 2015.

[9] M. Yang, D. Guo, Y. Huang, T. Q. Duong, and B. Zhang, "Physical layer security with threshold-based multiuser scheduling in multi-antenna wireless networks," *IEEE Trans. Commun.*, vol. 64, no. 12, pp. 5189–5202, December 2016.

[10] Y. Huang, F. S. Al-Qahtani, T. Q. Duong, and J. Wang, "Secure transmission in MIMO wiretap channels using general-order transmit antenna selection with outdated CSI," *IEEE Trans. Commun.*, vol. 63, no. 8, pp. 2959–2971, August 2015.

[11] Yang, Maoqiang and Zhang, Bangning and Huang, Yuzhen and Yang, Nan and Guo, Daoxing and Gao, Bin, "Secure multiuser Communication in wireless sensor networks with TAS and cooperative jamming" *J.Sensors*, vol. 16, no. 11, pp. 1908, Nov. 2016.

[12] S. S. Ikki and S. Aissa, "Performance analysis of dual-hop relaying systems in the presence of co-channel interference," in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM 2010),* Miami, Florida, USA, 6–10 December 2010, pp. 1–5.

[13] A. Jeffrey and D. Zwillinger, *Table of integrals, series, and products*. Academic Press, 2007.