This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2019.2907574, IEEE Internet of Things Journal

Physical Layer Security Enhancement for Internet of Things in the Presence of Co-channel Interference and Multiple Eavesdroppers

Tonny Ssettumba*, Ahmed H. Abd El-Malek*, Maha Elsabrouty*, Mohammed 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 system that utilizes transmit antenna selection scheme at the base station and adopts threshold-based selection diversity opportunistic scheduling over legitimate nodes. The legitimate transmission suffers from the presence of non-colluding and colluding multiple passive eavesdroppers. Both the legitimate and eavesdropping nodes are assumed to suffer from co-channel interference signals from independent channels that follow Rayleigh fading. Closed-form expressions for the probability density functions and cumulative density functions of the end-to-end signal-to-interference-plus-noise ratio for both eavesdropping scenarios in the presence of co-channel interference signals are derived. In addition, closed-form expressions for the network secrecy outage probability for non-colluding/colluding scenarios are derived. At the high signal-to-noise ratio values, closed-form expressions for the asymptotic secrecy outage probabilities are obtained. Following this obtained asymptotic analysis, an optimization problem for power allocation is formulated and solved to improve the secrecy performance of the network by minimizing the asymptotic secrecy outage probability for both colluding and non-colluding cases. The derived analytical expressions are then validated using both simulations and numerical results.**

***Index Terms*—Co-channel interference, Internet of things, physical layer security, power allocation, secrecy outage probability.**

I. Introduction

A. Background and Related Works

INFORMATION security and privacy are critical issues for the wireless communication medium because of its broadcast and distributed nature [1, 2]. With the rapid increase in the number of Internet of things (IoT) devices requiring seamless connectivity at any time anywhere, ensuring security for such devices is of high priority [3, 4].

Higher layers protocol stacks leverage on traditional encryption techniques to secure communication [5]. The major drawback of cryptography is that the management and distribution of the secret keys often require complex architectures and protocols. Consequently, such a method is difficult to apply in resource-constrained IoT devices [1]. On the other hand, physical layer (PHY) security can provide a secure connection between the source and destination by manipulating the wireless channel characteristics, with no increase in the spectral resources as well as reducing signaling overhead [6–9].

In one category of PHY security, uses the wireless medium to develop secret keys over public channels [8]. Another category of PHY security focuses on the design of intelligent transmit codes that do not require a secret key [10–14]. However, it is desirable that PHY techniques employed for IoT applications are energy-efficient and of low-complexity. This can be done through antenna selection and user scheduling [15, 16]. Several works focused on the transmit antenna selection (TAS) scheme because of its ability to achieve full diversity with an added advantage of low cost by reducing the number of required radio frequency (RF) chains [17, 18].

In [19–22], the analysis of the secrecy performance for multiple-input-multiple-output (MIMO) wiretap channels with TAS scheme was investigated, and a power allocation scheme was developed for MIMO wiretap channels. A generalized selection combining (GSC) scheme to improve secrecy performance for MIMO wiretap channel is proposed in [17] . In [23], a secure spatial modulation (SM) system with artificial noise (AN) was introduced. The authors in [24], proposed a threshold-based user scheduling for independent non-identical channels based on Markov chain theory. The work in [25] introduced a hybrid scheme combining TAS with threshold-based switched diversity (tSD) opportunistic scheduling, i.e. TAS/tSD in a multiuser multi-antenna wiretap network over Nakagami-m channels. Closed-form expressions were derived for the secrecy outage probability (SOP) and ergodic secrecy capacity for different cases based on the availability of channel side information (CSI) of the eavesdropper at the base station (BS). The work in [26] investigates the secrecy performance of multiuser networks where a BS communicates with multiple legitimate users with the aid of a trusted regenerative relay in the presence of multiple eavesdroppers. New exact and asymptotic closed-form expressions for the ergodic secrecy rate (ESR) were derived. Imperfect channel knowledge was considered in [27]. The works in [28, 29] considered cellular downlink system, with multiple users distributed according to a Poisson point process with a fixed density, one BS and a single eavesdropper in the presence of co-channel interferers.

B. Motivation and Contributions

The selected scheme for our work is the TAS/tSD scheme because of its reduced complexity compared to the conven-

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2019.2907574, IEEE Internet of Things Journal

tional TAS scheme [25]. From literature, the impact of co-channel interference (CCI) on the secrecy performance of such a scheme has not been addressed yet. Moreover, and to the best of our knowledge, the power allocation optimization problem for the TAS/tSD scheme in the presence of multiple eavesdroppers has not been investigated in previous works. Therefore, the main contributions of this work can be summarized as follows. First, we focus on studying the impact of CCI signals and multiple passive eavesdroppers on the secrecy performance. The eavesdroppers are assumed to be connected to an eavesdropping fusion center (EFC), which may overhear the transmission of all the eavesdroppers or select the best eavesdropper with the highest channel link to the EFC.

We study two eavesdropping cases, namely, non-colluding (Non-Col) case and colluding (Col) case. Although the Col case is more efficient for the eavesdropper to overhear the transmission, the Non-Col scenario may be adopted for four major reasons. First, some of the eavesdropping IoT nodes may not be willing to cooperate, thus the EFC may decide to select the best available node to overhear the transmitted message. Secondly, since we are dealing with passive eavesdroppers, the eavesdroppers and the EFC may fear to be detected and hence, they may decide not to employ colluding. Since colluding increases the probability of overhearing, eavesdropper selection (Non-Col) can be more effective. Thirdly, the eavesdropping IoT nodes are usually small devices with limited energy capability and battery lifetime, *may also be some of the IoT sensor nodes*. In this case, the EFC may decide to follow the Non-Col scenario to increase the lifetime of the eavesdroppers. Finally, the coverage area of an IoT cell is very small with a lot of nodes. In this case, the performance difference between using Col and Non-col scenarios can be considered negligible and acceptable as a compromise to reducing the energy consumption and the probability of being detected.

For both eavesdropping cases, closed-form expressions for the probability density function (PDF) and cumulative density function (CDF) of the end-to-end (e2e) signal-to-interference-plus-noise ratio (SINR) are derived. Moreover, closed-form expressions for the exact SOP are derived in the presence of CCI signals. At high signal-to-noise ratio (SNR) values, closed-form expressions for the asymptotic secrecy outage probability (ASOP) are obtained. Based on these asymptotic results, a power allocation problem is formulated to enhance the network secrecy performance by minimizing the ASOP.

C. Paper Organization and Notations

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 and the derivation of the exact SOP and the ASOP. The proposed power allocation is introduced in Section IV while the results of the paper are presented in Section V. Finally, Section VI. presents the conclusions of the findings

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. $\Pr[x]$ denotes the probability of event x to occur.

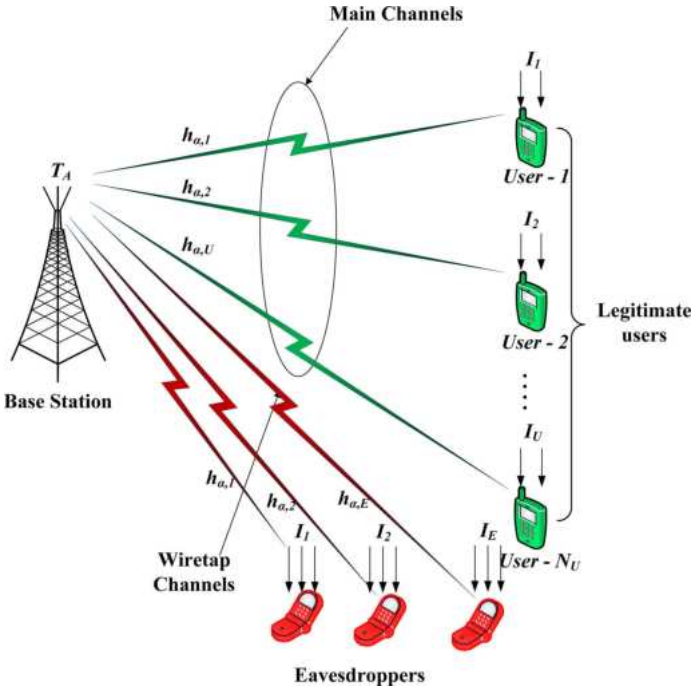

Fig. 1: Simplified system model for TAS/tSD user selection with CCI and multiple eavesdroppers.

The PDF and CDF of a random variable (RV) Y are represented by $f_Y(y)$ and $F_Y(y)$, respectively. $\mathbb{E}[.]$ represents the expectation notation while $\Gamma(x) = \int_0^\infty t^{x-1}\exp(-t)\,dt$ and $\Gamma(x,y) = \int_y^\infty t^{x-1}\exp(-t)\,dt$ denote the Gamma and incomplete Gamma functions, respectively.

II. System Model and SINR Statistics

A. System Model

Let us consider a practical multiuser downlink with many nodes. Due to the fact that the IoT network should have a very high device density (N devices/Km^2), i.e. hundreds of devices connected per square kilometer, more frequency reuse will be required. This eventually causes CCI for cells that use the same frequency. Without loss of generality, we consider the effect of the CCI signals resulting from other cells on one cell and we study the network secrecy performance based on these CCI signals. Figure 1 illustrates the system model. We assume a BS with T_A antennas, which communicates with the selected user from a set of N_U users using the TAS/tSD scheme. This legitimate transmission suffers from the existence of N_E single antenna passive eavesdropping nodes which try to intercept the transmitted message. Also, from a practical point of view, both the main and wiretap channels are assumed to suffer from CCI. Moreover, each legitimate link and wiretap link is assumed to follow independent and identically distributed (i.i.d.) flat Rayleigh fading distribution. We assume that the ratio between the transmitted power and the distance between the BS and all nodes is almost identical. In this case, each legitimate user u suffers from I_U identical CCI. Also, the eavesdroppers suffer from I_e identical CCI.

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 SNR exceeds a predefined

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2019.2907574, IEEE Internet of Things Journal

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 [24]. Hence, the received signal at the u-th user from the α-th antenna of the BS is given by

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

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 $1 \leq u \leq N_U$, and 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 interferers 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.

Similarly, multiple passive eavesdroppers are located near to the BS intercepting the transmitted data. Hence, the received signal at each eavesdropper 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 e-th eavesdropper with $1 \leq e \leq N_E$, 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.

In order to achieve a given secrecy, the BS encodes the message block $\mathbf{Z}$ into the codeword $\mathbf{y} = [y(1), ..., y(i), ...y(n)]$ with $\frac{1}{m}\sum_{i=1}^{m} \left[|y(i)|^2\right] \leq P_\alpha$ [25]. 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 $x \in \{u, e\}$, $\rho_\alpha = \frac{P_\alpha}{N_0}$, $\rho_{i_x} = \frac{P_{i_x}}{N_0}$, and $P_{i_x} = \zeta P_\alpha$, with $0 \leq \zeta \leq 1$.

In the TAS/tSD scheme, the BS estimates if the instantaneous SNR of the selected antenna exceeds a predefined threshold γ_T, when $\gamma^{\text{tSD}}_{\alpha,u} > \gamma_T$, the tSD terminates for this antenna. Otherwise, the procedure continues until an antenna with an instantaneous SNR greater than γ_T is found. If the BS fails to find a user with an instantaneous SNR greater than γ_T, the BS selects the best user with the highest SNR 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 e2e instantaneous SNR of the TAS/tSD scheme, the index of the selected antenna is $\alpha^* = \underset{1\leq\alpha\leq T_A}{\arg\max}(\gamma^{\text{tSD}}_{\alpha,u^*})$ [25].

B. Effective Received SINR Statistics for Legitimate Node

The channel coefficient between the α-th antenna and any node $x \in \{u, e\}$ is assumed to follow i.i.d Rayleigh fading distribution. The PDF of the channel gain is given by [30]

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

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 with $\Omega_{\alpha,x}$ is the average channel gain between α and x. Moreover, for simplicity of analysis, the CCI signals are assumed to follow i.i.d Rayleigh fading distribution. Hence, the PDF of CCI signals is given by [30]

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

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), 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 is given as [30]

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

By substituting (4) and (5) in (6) with some mathematical manipulations and [31, (3.381.4)], the PDF of the SINRs at the legitimate node is given by

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

where $\Lambda_u = \frac{\bar{\gamma}_{\alpha,u}}{\bar{\gamma}_{i_u,u}}$ is the average signal-to-interference ratio (SIR) at the legitimate node. The CDF is given by

$$F_{\gamma_{\alpha,u}}(\gamma) = 1 - \left(\frac{\Lambda_u}{\gamma + \Lambda_u}\right)^{I_u} \exp\left(-\frac{\gamma}{\bar{\gamma}_{\alpha,u}}\right). \quad (8)$$

C. Case 1: Effective Received SINR Statistics for The Non-Colluding Eavesdropping Scenario

We consider N_E eavesdroppers operating in a Rayleigh fading environment controlled by an EFC. In this case, the EFC monitors all the eavesdroppers and selects the one with the best channel link. The PDF of SNR of the identically distributed eavesdroppers under Non-Col case is given by [33]

$$f_e^{\text{Non-Col}}(x) = \frac{N_E}{\bar{\gamma}_{\alpha,e}} \sum_{m=0}^{N_E-1} \binom{N_E - 1}{m} (-1)^m \exp\left(-\frac{(m+1)\,x}{\bar{\gamma}_{\alpha,e}}\right). \quad (9)$$

More specifically, we assume that there are multiple CCI interfering signals, independent of the wiretap signal, subject to Rayleigh fading and that the received interfering signals by each node, are identically distributed with instantaneous faded power. Therefore, the SC decision is made based on the required received power by a particular eavesdropper node.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2019.2907574, IEEE Internet of Things Journal

Thus, the SC does not alter the statistics of the interfering signal power irrespective of whether the interfering signals of the nodes are correlated or not. Hence, the PDF of the interfering signal power at the combiner output is same as in (5). Finally, the PDF $f_{\gamma_{\alpha,e}^{\text{Non-Col}}}(\gamma)$ of the average SINR for the Non-Col case is obtained by applying the binomial theorem in [31, (1.111)] with (5) and (9), such as

$$f_{\gamma_{\alpha,e}}^{\text{Non-Col}}(\gamma) = N_E \sum_{m=0}^{N_E-1} \binom{N_E-1}{m} (-1)^m \exp\left(-\frac{(m+1)\gamma}{\bar{\gamma}_e}\right) \times \left[\frac{I_e \Lambda_e^{I_e}}{(\Lambda_e+(m+1)\gamma)^{I_e+1}} + \frac{\Lambda_e^{I_e}}{\bar{\gamma}_e(\Lambda_e+(m+1)\gamma)^{I_e}}\right]. \tag{10}$$

Hence, the corresponding CDF is given by

$$F_{\alpha,e}^{\text{Non-Col}}(\gamma) = 1 - N_E \sum_{m=0}^{N_E-1} \binom{N_E-1}{m} (-1)^m \times \frac{\Lambda_e^{I_e}}{(m+1)(\Lambda_e+(m+1)\gamma)^{I_e}} \exp\left(-\frac{(m+1)\gamma}{\bar{\gamma}_e}\right), \tag{11}$$

where $\Lambda_e = \frac{\bar{\gamma}_{\alpha,e}}{\bar{\gamma}_{ie,e}}$, is the average SIR at the eavesdropper.

D. Case 2: Effective Received SINR Statistics for The Colluding Eavesdropping Scenario

In this case, the eavesdroppers work collectively to intercept the transmitted data by sending all their decoded data to an EFC. In general, the eavesdroppers are not identical but for tractable analysis as well as the limited transmission power and size of the IoT network, we assume the eavesdroppers are identical. Hence, the MRC scheme is used by the EFC where the output is a weighted sum of all the eavesdroppers. Hence, the PDF of the average SNR is given by [33]

$$f_e^{\text{Col}}(x) = \frac{x^{N_E-1}}{\bar{\gamma}_e^{N_E}\Gamma(N_E)} \exp\left(-\frac{x}{\bar{\gamma}_e}\right). \tag{12}$$

To obtain the eavesdropper SINR in this case, we follow similar procedures as in case 1 while using (5) and (12). Thus, after applying binomial theorem as in [31, (1.111)], the PDF of the average SINR for the Col case can be derived as

$$f_{\alpha,e}^{\text{Col}}(\gamma) = \frac{\gamma^{N_E-1}\Lambda_e^{I_e}}{\Gamma(N_E)(I_e-1)!} \exp\left(-\frac{\gamma}{\bar{\gamma}_e}\right) \times \sum_{m=0}^{N_E} \binom{N_E}{m} \frac{\Gamma(I_e+m)}{\bar{\gamma}_e^{N_E-m}(\gamma+\Lambda_e)^{I_e+m}}. \tag{13}$$

Hence, the corresponding CDF is given by

$$F_{\alpha,e}^{\text{Col}}(\gamma) = 1 - \frac{\exp\left(-\frac{\gamma}{\bar{\gamma}_e}\right)}{\Gamma(N_E)(I_e-1)!} \sum_{m=0}^{N_E} \binom{N_E}{m} \Gamma(I_e+m) \times \sum_{s=0}^{N_E-1} \binom{N_E-1}{s} (-1)^{N_E-1-s} \sum_{w=o}^{s-I_e} \frac{(s-I_e)!}{w!} \times \sum_{w_1=0}^{w} \binom{w}{w_1} \Lambda_e^{I_e+w+w_1+N_E-1-s} \bar{\gamma}_e^{I_e+w-N_E-s} \gamma^{w_1}, \tag{14}$$

where $\Lambda_e = \frac{\bar{\gamma}_{\alpha,e}}{\bar{\gamma}_{ie,e}}$, is the average SIR at the eavesdropper.

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 in Section II. We derive the SOP and ASOP to completely study and get more insights into the system secrecy behavior.

A. Preamble

Since the event of selecting a particular antenna for transmission using TAS/tSD scheme is mutually exclusive for a specific antenna α, the CDF of $\gamma_{\alpha^*,u^*}^{\text{tSD}}(\gamma)$ is given by [25]

$$F_{\gamma_{\alpha^*,u^*}^{\text{tSD}}}(\gamma) = \sum_{u=1}^{N_U} \Pr\left[\gamma_{\alpha^*,u^*}^{\text{tSD}}(\gamma) = \gamma_{\alpha,u} \;\&\; \gamma_{\alpha,u} \le \gamma\right]. \tag{15}$$

Moreover, for i.i.d flat fading Rayleigh distribution, the CDF of e2e SINR for the tSD scheme is given by [24, 25]

$$F_{\gamma_{\alpha^*,u^*}^{tSD}}(\gamma) = \begin{cases} F_{\gamma_{\alpha,u}}(\gamma) - F_{\gamma_{\alpha,u}}(\gamma_T) \\ +F_{\gamma_{\alpha,u}}(\gamma_T)\left[F_{\gamma_{\alpha,u}}(\gamma)\right]^{N_U-1}, & \gamma \ge \gamma_T \\ \left[F_{\gamma_{\alpha,u}}(\gamma)\right]^{N_U}, & \gamma < \gamma_T, \end{cases} \tag{16}$$

where $F_{\gamma_{\alpha,u}}(\gamma)$ is given by (8). For $\gamma \ge \gamma_T$, the tSD is used, otherwise the BS employs the conventional SC scheme as stated in (16) when $\gamma < \gamma_T$. Hence, the CDF of the e2e average SNR for the TAS/tSD scheme is obtained by selecting the best antenna from the BS to transmit in [25] such as

$$F_{\gamma_U}(\gamma) = \left(F_{\gamma_{\alpha^*,u^*}}^{\text{tSD}}(\gamma)\right)^{T_A}. \tag{17}$$

By substituting (8) and (16) in (17) with the help of binomial expansion [31, (1.111)], the CDF of γ_U is obtained as

$$F_{\gamma_U}(\gamma) = \begin{cases} \sum_{k=0}^{T_A} \binom{T_A}{k} \left[F_{\gamma_U}(\gamma_T)\right]^k \sum_{k_1=0}^{k} \binom{k}{k1} (-1)^{k+k_1} \\ \times \sum_{k_2=0}^{(N_U-1)k_1+T_A-k} \binom{(N_U-1)k_1+T_A-k}{k_2} (-1)^{k_2} \\ \times \left(\frac{\Lambda_U}{\gamma+\Lambda_U}\right)^{k_2 I_U} \exp\left(-\frac{k_2\gamma}{\bar{\gamma}_U}\right), & \gamma \ge \gamma_T \\ \sum_{t=0}^{T_A N_U} \binom{T_A N_U}{t} (-1)^t \left(\frac{\Lambda_U}{\gamma+\Lambda_U}\right)^{tI_U} \exp\left(-\frac{t\gamma}{\bar{\gamma}_U}\right), & \gamma < \gamma_T. \end{cases} \tag{18}$$

Moreover, the secrecy capacity C_s can be expressed as [8]

$$C_s = [C_U - C_E]^+ = \max(C_U - C_E, 0), \tag{19}$$

where $C_U = \log(1+\gamma_U)$, and $C_E = \log(1+\gamma_E)$ with $\gamma_U = \gamma_{\alpha^*,u^*}$, and $\gamma_E = \gamma_{\alpha^*,e^*}$ for Non-Col and $\sum_{i=1}^{N_E} \gamma_{\alpha^*,e^*}$ for Col, respectively. As stated earlier, we consider passive eavesdroppers such that the eavesdropper CSI is unavailable at the BS. Thus, the BS assumes the rate of the wiretap channel as $C_E^* = C_U - R_s$ for secure transmission, where R_s is the constant secrecy rate set by the BS. The BS constructs wiretap codes using C_U and C_E^* to . If $R_s \le C_s$, perfect secrecy is ensured. Otherwise, secrecy is compromised [25].

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2019.2907574, IEEE Internet of Things Journal

B. Secrecy Outage Probability Analysis

One of the key metrics for measuring the secrecy performance of a communication system is the SOP. A secrecy outage occurs when C_S is less than R_s. This implies that R_s cannot guarantee the secrecy requirement of the system. The SOP for measuring the likelihood that a secrecy outage occurs with a particular fading distribution can be given as $P_{\mathsf{out}}(R_s) = \Pr[C_s < R_s]$ expressed as [24, 25]

$$\begin{aligned} P_{\mathsf{out}}(R_s) =& \Pr(C_s < R_s | \gamma_U > \gamma_E) \Pr(\gamma_U > \gamma_E) \\ &+ \Pr(\gamma_U < \gamma_E), \\ =& \int_0^{\infty} F_{\gamma_U}(2^{R_s}(1+y)-1) f_{\gamma_E}(y) dy, \end{aligned} \quad (20)$$

where $F_{\gamma_U}(x)$ is the CDF of γ_U. Using the fact that the CDF in (18) contains the predefined threshold γ_T, a relationship exists between $2^{R_s}(1+y)-1$ and γ_T in (20) 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

$$P_{\mathsf{out}}(R_s) = \begin{cases} \int_0^{H(\gamma_T)} F_{\gamma_U}(\Theta_y) f_{\gamma_E}(y) dy \\ + \int_{H(\gamma_T)}^{\infty} F_{\gamma_U}(\Theta_y) f_{\gamma_E}(y) dy, & H(\gamma_T) \geq 0 \\ \int_0^{\infty} F_{\gamma_U}(\Theta_y) f_{\gamma_E}(y) dy, & H(\gamma_T) < 0, \end{cases} \quad (21)$$

where $\Theta(y) = 2^{R_s}(y+1)-1$. Using the integral formulas in [31, (3.462.15), (3.462.16), and (3.462.17)] and substituting (18), (13) and (10) into (21) with some mathematical manipulations yields $P_{\mathsf{out}}(R_s)$

$$P_{\mathsf{out}}(R_s) = \begin{cases} \Delta_{1z} + \Delta_{2z}, & H(\gamma_T) \geq 0 \\ \Delta_{3z}, & H(\gamma_T) < 0, \end{cases} \quad (22)$$

where Δ_{1z}, Δ_{2z} and Δ_{3z} with $z \in \{\text{Non-Col}, \text{Col}\}$ are given by (23), (24), and (25) for the Non-Col case; whereas (26), (27) and (28) for the Col case. Besides, $\delta = 2^{R_s}$, $\Lambda_0 = \frac{\delta-1}{\delta}$, $\Lambda' = \frac{\delta-1+\Lambda_U}{\delta}$, $\Theta = \frac{\delta t}{\bar{\gamma}_U} + \frac{m+1}{\bar{\gamma}_E}$, $\Omega = tI_U$, $\alpha = I_e$, $\alpha_1 = I_e+1$, $\beta_1 = \frac{\Lambda_e}{m+1}$, $\lambda = \frac{\Lambda_e^{I_e}}{\bar{\gamma}_E}$, $\mu = I_e \Lambda_e^{I_e}$, $\beta = \frac{m+1}{\bar{\gamma}_E}$, $\theta = t\frac{\delta-1}{\bar{\gamma}_U}$, $\theta_1 = k_2 \frac{\delta-1}{\bar{\gamma}_U}$, $\phi_2 = \Theta_1 = \frac{\delta k_2}{\bar{\gamma}_U} + \frac{m+1}{\bar{\gamma}_E}$. For further reading, the derivations of the SOP can be found in [32].

Insights into the obtained closed-form expressions: Based on the obtained SOP closed-form expressions, it can be noted that the major parameters affecting the SOP are the switched threshold, γ_T, the average SNR of the legitimate node $\bar{\gamma}_U$, the number of legitimate nodes N_U, the number of eavesdropping nodes N_E, the number of transmit antennas at the BS T_A, the average SNR of the eavesdropping nodes $\bar{\gamma}_E$, the number of interferers towards the legitimate nodes and the eavesdropping nodes I_U and I_e, respectively, and the constant secrecy rate R_S set by the BS. From the derived SOP expressions, many insights can be summarized as follows:

- Increasing I_e improves the secrecy performance of the overall system since the wiretap channel quality is compromised as compared to the main channel quality as seen in Figure 3. Similarly, increasing I_U strongly harms the secrecy performance as also shown in Figure 3.
- Increasing T_A improves the secrecy performance since the diversity gain is increased which leads to a better system performance as shown Figure 4.
- Increasing N_E strongly harms the security of the system for both Col and Non-Col scenarios as shown in Figure 7. This can be explained as increasing N_E increases the eavesdroppers probability or chance of overhearing the transmitted data. On the other hand increasing N_U results in improving the system secrecy performance.
- Increasing γ_T is another way of enhancing the system secrecy performance. However, as shown in Figure 8, increasing γ_T beyond a certain value (i.e. $\gamma_T > 15$ dB) does not enhance the secrecy performance of the system and the SOP remains constant beyond this value of γ_T.
- The increase in $\bar{\gamma}_U$ improves the secrecy performance of the system since the main channel quality is enhanced relative to the wiretap channel quality. On the other hand, increasing $\bar{\gamma}_E$ harms the secrecy performance as the wiretap channel quality is improved as seen in Figure 9.

C. Asymptotic Analysis

In order to gain more insight into the secrecy outage behavior, the ASOP is derived to facilitate the analysis. In order to approximate the CDF of the effective SINR in high SINR regime, we carried out a Taylor series expansion on the CDF in (8) as $\bar{\gamma}_U \to \infty$, thus the resulting CDF is given as $F_{\gamma_U}^{\infty}(\gamma) \backsimeq \frac{\gamma}{\bar{\gamma}_U}(I_U \bar{\gamma}_{i,U} + 1)$ and the approximate e2e SINR is given such as

$$F_{\gamma_U}^{\infty}(\gamma) \simeq \begin{cases} \sum_{k=0}^{T_A} \binom{T_A}{k} \left[\frac{\gamma_T}{\bar{\gamma}_U}(I_U \bar{\gamma}_U + 1)\right]^k \sum_{k_1=0}^{k} \binom{k}{k_1} (-1)^{k_1} \\ \times \left[\frac{\gamma}{\bar{\gamma}_U}(I_U \bar{\gamma}_U + 1)\right]^{(N_U-1)k_1 + T_A - k}, & \gamma \geq \gamma_T \\ \left[\frac{\gamma}{\bar{\gamma}_U}(I_U \bar{\gamma}_U + 1)\right]^{N_U T_A}, & \gamma < \gamma_T. \end{cases} \quad (29)$$

Thus, by using equations (10) and (13) and (29) and substituting in (21), the ASOP is derived as

$$P_{\mathsf{out}}^{\infty}(R_s) \approx \begin{cases} \Upsilon_{1z}^{\infty} + \Upsilon_{2z}^{\infty}, & H(\gamma_T) \geq 0 \\ \Upsilon_{3z}^{\infty}, & H(\gamma_T) < 0, \end{cases} \quad (30)$$

where Υ_{1z}^{∞}, Υ_{2z}^{∞} and Υ_{3z}^{∞} are given by (31), (32), and (33) for the Non-Col case; and (34), (35), and (36) for the Col case.

IV. Proposed Power Allocation Model

In this section, a power allocation optimization problem is formulated to improve the secrecy performance of the considered system against multiple eavesdropping attacks in the presence of CCI signals. We substitute for $\bar{\gamma}_U = \frac{P_\alpha \Omega_U}{N_0}$, $\bar{\gamma}_E = \frac{P_\alpha \Omega_E}{N_0}$ into the ASOP expressions in (30), where Ω_U and Ω_E are the channel gains at the legitimate nodes and eavesdroppers respectively. For simplicity, the obtained expressions for the ASOP in the high SNR regions as both $\bar{\gamma}_U \to \infty$ and $\bar{\gamma}_E \to \infty$ are used as target functions in the optimization problem. Because of the high complexity of the expressions for the exact SOP and ASOP in (22) and (30), respectively, we make some mathematical manipulation for the derived ASOP in (30). It can be seen that the first term in the case of $H(\gamma_T) \geq 0$ varnishes to 0 as

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2019.2907574, IEEE Internet of Things Journal

$$\Delta_{\text{1Non-Col}} = \sum_{t=0}^{T_A N_U} \binom{T_A N_U}{t} (-1)^t N_E \sum_{m=0}^{N_E-1} \binom{N_E-1}{m} (-1)^m \exp\left(-t\frac{2^{R_s}-1}{\bar{\gamma}_U}\right) \left(\frac{\Lambda_U}{2^{R_s}}\right)^{tI_U} \Bigg[\Bigg\{ \sum_{w=0}^{tI_U} A_w \Theta^{w-1} \times \left[\Gamma\left(-w+1, \Lambda^{'}\Theta\right) - \Gamma\left(-w+1, \Theta\left(H(\gamma_T)+\Lambda^{'}\right)\right)\right] + \sum_{w_2=1}^{tI_U} A_{w_2} \Theta^{w_2-1} \left[\Gamma\left(-w_2+1, \Lambda^{'}\Theta\right) - \Gamma\left(-w_2+1, \Theta\left(H(\gamma_T)+\Lambda^{'}\right)\right)\right] \Bigg\} \times \exp\left(\Theta\Lambda^{'}\right) + \Bigg\{ \sum_{w_1=0}^{I_e+1} A_{w_1} \Theta^{w_1-1} \left[\Gamma\left(-w_1+1, \beta_1\Theta\right) - \Gamma\left(-w_1+1, \Theta\left(H(\gamma_T)+\beta_1\right)\right)\right] + \sum_{w_2=1}^{I_e} A_{w_3} \Theta^{w_3-1} \left[\Gamma\left(-w_3+1, \beta_1\Theta\right) - \Gamma\left(-w_3+1, \Theta\left(H(\gamma_T)+\beta_1\right)\right)\right] \Bigg\} \exp\left(\Theta\beta_1\right) \Bigg]. \tag{23}$$

$$\Delta_{\text{2Non-Col}} = \sum_{k=0}^{T_A} \binom{T_A}{k} \left[F_{\gamma_U}(\gamma_T)\right]^k \sum_{k_1=0}^{k} \binom{k}{k_1} (-1)^{k+k_1} \sum_{k_2=0}^{(N_U-1)k_1+T_A-k} \binom{(N_U-1)k_1+T_A-k}{k_2} (-1)^{k_2} N_E \sum_{m=0}^{N_E-1} \binom{N_E-1}{m} (-1)^m \times \exp\left(-k_2\frac{2^{R_s}-1}{\bar{\gamma}_U}\right) \left(\frac{\Lambda_U}{2^{R_s}}\right)^{k_2 I_U} \Bigg[\Bigg\{ \sum_{w=0}^{k_2 I_U} B_w \Theta_1^{w-1} \Gamma\left(-w+1, \left(\Lambda^{'}+H(\gamma_T)\right)\Theta_1\right) + \sum_{w_2=1}^{k_2 I_U} B_{w_2} \Theta_1^{w_2-1} \Gamma\left(-w_2+1, \left(\Lambda^{'}+H(\gamma_T)\right)\Theta_1\right) \Bigg\} \times \exp\left(\Theta_1\Lambda^{'}\right) + \Bigg\{ \sum_{w_1=0}^{I_e+1} B_{w_1} \Theta^{w_1-1} \Gamma\left(-w_1+1, \left(\beta_1+H(\gamma_T)\right)\Theta_1\right) + \sum_{w_2=1}^{I_e} B_{w_3} \Theta_1^{w_3-1} \Gamma\left(-w_3+1, \left(\beta_1+H(\gamma_T)\right)\Theta_1\right) \Bigg\} \exp\left(\Theta_1\beta_1\right) \Bigg]. \tag{24}$$

$$\Delta_{\text{3Non-Col}} = \sum_{k=0}^{T_A} \binom{T_A}{k} \left[F_{\gamma_U}(\gamma_T)\right]^k \sum_{k_1=0}^{k} \binom{k}{k_1} (-1)^{k+k_1} \sum_{k_2=0}^{(N_U-1)k_1+T_A-k} \binom{(N_U-1)k_1+T_A-k}{k_2} (-1)^{k_2} N_E \sum_{m=0}^{N_E-1} \binom{N_E-1}{m} (-1)^m \times \exp\left(-k_2\frac{2^{R_s}-1}{\bar{\gamma}_U}\right) \left(\frac{\Lambda_U}{2^{R_s}}\right)^{k_2 I_U} \Bigg[\Bigg\{ \sum_{w=0}^{k_2 I_U} B_w \Theta_1^{w-1} \Gamma\left(-w+1, \Lambda^{'}\Theta_1\right) + \sum_{w_2=1}^{k_2 I_U} B_{w_2} \Theta_1^{w_2-1} \Gamma\left(-w_2+1, \Lambda^{'}\Theta_1\right) \Bigg\} \exp\left(\Theta_1\Lambda^{'}\right) + \Bigg\{ \sum_{w_1=0}^{I_e+1} B_{w_1} \Theta^{w_1-1} \Gamma\left(-w_1+1, \beta_1\Theta_1\right) + \sum_{w_2=1}^{I_e} B_{w_3} \Theta_1^{w_3-1} \Gamma\left(-w_3+1, \beta_1\Theta_1\right) \Bigg\} \exp\left(\Theta_1\beta_1\right) \Bigg]. \tag{25}$$

$$\Delta_{\text{1Col}} = \sum_{t=0}^{T_A N_U} \binom{T_A N_U}{t} (-1)^t \frac{\Lambda_E^{I_e}}{\Gamma(N_E)(I_e-1)!} \sum_{m=0}^{N_E} \binom{N_E}{m} \frac{I_e+m}{\bar{\gamma}_E^{N_E-m}} \left(\frac{\Lambda_U}{2^{R_s}}\right)^{tI_U} \exp\left(-t\frac{2^{R_s}-1}{\bar{\gamma}_U}\right) \sum_{n=0}^{N_E-1} \binom{N_E-1}{n} \times (-\Lambda_E)^{N_E-1-n} \exp\left(\left\{\frac{t2^{R_s}}{\bar{\gamma}_U}+\frac{1}{\bar{\gamma}_E}\right\}\Lambda^{'}\right) \sum_{n_1=0}^{n-I_e-m} \binom{n-I_e+m}{n_1} \left(\Lambda_E-\Lambda^{'}\right)^{n-I_e-m-n_1} \frac{1}{\left\{\frac{t2^{R_s}}{\bar{\gamma}_U}+\frac{1}{\bar{\gamma}_E}\right\}^{n_1-tI_U+1}} \times \left[\Gamma\left(n_1-tI_U+1, \Lambda^{'}\left\{\frac{t2^{R_s}}{\bar{\gamma}_U}+\frac{1}{\bar{\gamma}_E}\right\}\right) - \Gamma\left(n_1-tI_U+1, \left(\Lambda^{'}+H(\gamma_T)\right)\left\{\frac{t2^{R_s}}{\bar{\gamma}_U}+\frac{1}{\bar{\gamma}_E}\right\}\right)\right]. \tag{26}$$

$$\Delta_{\text{2Col}} = \sum_{k=0}^{T_A} \binom{T_A}{k} \left[F_{\gamma_U}(\gamma_T)\right]^k \sum_{k_1=0}^{k} \binom{k}{k_1} (-1)^{k+k_1} \sum_{k_2}^{(N_U-1)k_1+T_A-k} \binom{(N_U-1)k_1+T_A-k}{k_2} (-1)^{k_2} \left[\frac{\Lambda_E^{I_e}}{\Gamma(N_E)(I_e-1)!}\right] \times \sum_{m=0}^{N_E} \binom{N_E}{m} \left[\frac{\Gamma(m+I_e)}{\bar{\gamma}_E^{N_E-m}}\right] \left(\frac{\Lambda_U}{2^{R_s}}\right)^{kI_U} \exp\left(-k_2\frac{2^{R_s}-1}{\bar{\gamma}_U}\right) \exp\left(\left\{\frac{k_2 2^{R_s}}{\bar{\gamma}_U}+\frac{1}{\bar{\gamma}_E}\right\}\Lambda^{'}\right) \sum_{g=0}^{N_E-1} \binom{N_E-1}{g} (-\Lambda_E)^{N_E-1-g} \times \sum_{g_1=0}^{g-I_e-m} \binom{g-I_e-m}{g_1} \left(\Lambda_E-\Lambda^{'}\right)^{g-I_e-m-g_1} \left[\frac{\bar{\gamma}_U\bar{\gamma}_E}{(\bar{\gamma}_U+2^{R_s}k_2\bar{\gamma}_E)}\right]^{g_1-k_2 I_U+1} \Gamma\left(g_1-k_2 I_U+1, \left\{\frac{k_2 2^{R_s}}{\bar{\gamma}_U}+\frac{1}{\bar{\gamma}_E}\right\}\left(\Lambda^{'}+H(\gamma_T)\right)\right). \tag{27}$$

$$\Delta_{\text{3Col}} = \sum_{k=0}^{T_A} \binom{T_A}{k} \left[F_{\gamma_U}(\gamma_T)\right]^k \sum_{k_1=0}^{k} \binom{k}{k_1} (-1)^{k+k_1} \sum_{k_2}^{(N_U-1)k_1+T_A-k} \binom{(N_U-1)k_1+T_A-k}{k_2} (-1)^{k_2} \left[\frac{\Lambda_E^{I_e}}{\Gamma(N_E)(I_e-1)!}\right] \times \sum_{m=0}^{N_E} \binom{N_E}{m} \left[\frac{\Gamma(m+I_e)}{\bar{\gamma}_E^{N_E-m}}\right] \left(\frac{\Lambda_U}{2^{R_s}}\right)^{kI_U} \exp\left(-k_2\frac{2^{R_s}-1}{\bar{\gamma}_U}\right) \exp\left(\left\{\frac{k_2 2^{R_s}}{\bar{\gamma}_U}+\frac{1}{\bar{\gamma}_E}\right\}\Lambda^{'}\right) \sum_{g=0}^{N_E-1} \binom{N_E-1}{g} (-\Lambda_E)^{N_E-1-g} \times \sum_{g_1=0}^{g-I_e-m} \binom{g-I_e-m}{g_1} \left(\Lambda_E-\Lambda^{'}\right)^{g-I_e-m-g_1} \left[\frac{\bar{\gamma}_U\bar{\gamma}_E}{(\bar{\gamma}_U+2^{R_s}k_2\bar{\gamma}_E)}\right]^{g_1-k_2 I_U+1} \Gamma\left(g_1-k_2 I_U+1, \left\{\frac{k_2 2^{R_s}}{\bar{\gamma}_U}+\frac{1}{\bar{\gamma}_E}\right\}\Lambda^{'}\right). \tag{28}$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2019.2907574, IEEE Internet of Things Journal

$$\Upsilon^{\infty}_{\text{1Non-Col}} = N_E \sum_{m=0}^{N_E-1} \binom{N_E-1}{m} (-1)^m \left[2^{R_s} \frac{I_U \bar{\gamma}_{iU}+1}{\bar{\gamma}_U}\right]^{N_U T_A} \exp\left(\frac{\Lambda_E}{\bar{\gamma}_E}\right) \sum_{i=0}^{N_U T_A} \left(\Lambda_0 - \frac{\Lambda_E}{m+1}\right)^{N_U T_A - i} \left[\frac{\bar{\gamma}_E}{m+1}\right]^{i-I_e} \left[\frac{\Lambda_E^{I_e}}{(m+1)^{I_e+1}}\right] \times \left\{ I_e \left[\Gamma\left(i-I_e, \frac{\Lambda_E}{\bar{\gamma}_E}\right) - \Gamma\left(i-I_e, \frac{\Lambda_E}{\gamma_E} + H(\gamma_T)\frac{m+1}{\bar{\gamma}_E}\right)\right] + \left[\Gamma\left(i-I_e+1, \frac{\Lambda_E}{\bar{\gamma}_E}\right) - \Gamma\left(i-I_e+1, \frac{\Lambda_E}{\gamma_E} + H(\gamma_T)\frac{m+1}{\bar{\gamma}_E}\right)\right]\right\}. \tag{31}$$

$$\Upsilon^{\infty}_{\text{2Non-Col}} = \sum_{k=0}^{T_A} \binom{T_A}{k} \left[\gamma_T \frac{I_U \bar{\gamma}_{iU}+1}{\bar{\gamma}_U}\right]^k \sum_{k_1}^{k} \binom{k_1}{k} (-1)^{k_1} \left[2^{R_s} \frac{I_U \bar{\gamma}_{iU}+1}{\bar{\gamma}_U}\right]^{(N_U-1)k_1+T_A-k} N_E \sum_{m=0}^{N_E-1} \binom{N_E-1}{m} (-1)^m \times \exp\left(-\frac{\Lambda_E}{\bar{\gamma}_E}\right) \sum_{\tau}^{(N_U-1)k_1+T_A-k} \binom{(N_U-1)k_1+T_A-k}{\tau} \left(\Lambda_0 - \frac{\Lambda_E}{m+1}\right)^{(N_U-1)k_1+T_A-k-\tau} \left[\frac{\Lambda_E^{I_e} \bar{\gamma}_E^{\tau-I_e}}{(m+1)^{1+\tau}}\right] \times \left\{ I_e \Gamma\left(\tau - I_e, \frac{\Lambda_E^{I_e}}{\bar{\gamma}_E} + H(\gamma_T)\frac{m+1}{\bar{\gamma}_E}\right) + \Gamma\left(\tau - I_e + 1, \frac{\Lambda_E^{I_e}}{\bar{\gamma}_E} + H(\gamma_T)\frac{m+1}{\bar{\gamma}_E}\right)\right\}. \tag{32}$$

$$\Upsilon^{\infty}_{\text{3Non-Col}} = \sum_{k=0}^{T_A} \binom{T_A}{k} \left[\gamma_T \frac{I_U \bar{\gamma}_{iU}+1}{\bar{\gamma}_U}\right]^k \sum_{k_1}^{k} \binom{k_1}{k} (-1)^{k_1} \left[2^{R_s} \frac{I_U \bar{\gamma}_{iU}+1}{\bar{\gamma}_U}\right]^{(N_U-1)k_1+T_A-k} N_E \sum_{m=0}^{N_E-1} \binom{N_E-1}{m} (-1)^m \times \exp\left(-\frac{\Lambda_E}{\bar{\gamma}_E}\right) \sum_{\tau}^{(N_U-1)k_1+T_A-k} \binom{(N_U-1)k_1+T_A-k}{\tau} \left(\Lambda_0 - \frac{\Lambda_E}{m+1}\right)^{(N_U-1)k_1+T_A-k-\tau} \left[\frac{\Lambda_E^{I_e} \bar{\gamma}_E^{\tau-I_e}}{(m+1)^{1+\tau}}\right] \times \left\{ I_e \Gamma\left(\tau - I_e, \frac{\Lambda_E}{\bar{\gamma}_E}\right) + \Gamma\left(\tau - I_e + 1, \frac{\Lambda_E}{\bar{\gamma}_E}\right)\right\}. \tag{33}$$

$$\Upsilon^{\infty}_{\text{1Col}} = \left[\frac{2^{R_s}(I_U \bar{\gamma}_{iU}+1)}{\bar{\gamma}_U}\right]^{N_U T_A} \sum_{m=0}^{N_E} \binom{N_E}{m} \frac{\Lambda_E^{I_e}}{\Gamma(N_E)(I_e-1)! \bar{\gamma}_E^{N_E-m}} \exp\left(\frac{\Lambda_E}{\gamma_E}\right) \sum_{\mu_1=0}^{N_U T_A} \binom{N_U T_A}{\mu_1} (\Lambda_0 - \Lambda_E)^{N_U T_A - \mu_1} \times \sum_{\mu_2=0}^{N_E-1} \binom{N_E-1}{\mu_2} \frac{-\Lambda_E^{N_E-1-\mu_2}}{\bar{\gamma}_E^{-(\mu_1+\mu_2-I_e-m+1)}} \left\{\Gamma\left(\mu_1+\mu_2-I_e-m+1, \frac{\Lambda_E}{\bar{\gamma}_E}\right) - \Gamma\left(\mu_1+\mu_2-I_e-m+1, \frac{\Lambda_E+H(\gamma_T)}{\bar{\gamma}_E}\right)\right\}. \tag{34}$$

$$\Upsilon^{\infty}_{\text{2Col}} = \sum_{k=0}^{T_A} \binom{T_A}{k} \left[\frac{\gamma_T(I_U \gamma_{iU}+1)}{\gamma_U}\right]^k (-1)^k \sum_{k_1=0}^{k} \binom{k}{k_1} (-1)^{k_1} \left[\frac{2^{R_s}(I_U \gamma_{iU}+1)}{\gamma_U}\right]^{(N_U-1)k_1+T_A-k} \sum_{m=0}^{N_E} \binom{N_E}{m} \times \frac{\Lambda_E^{I_e}}{\Gamma(N_E)(I_e-1)! \bar{\gamma}_E^{N_E-m}} \exp\left(\frac{\Lambda_E}{\bar{\gamma}_E}\right) \sum_{r_1=0}^{(N_U-1)k_1+T_A-k} \binom{(N_U-1)k_1+T_A-k}{r_1} (\Lambda_0 - \Lambda_E)^{(N_U-1)k_1+T_A-k-r_1} \times \sum_{r_2=0}^{N_E-1} \binom{N_E-1}{r_2} (-\Lambda_E)^{N_E-1-r_2} \bar{\gamma}_E^{r_1+r_2-I_e-m+1} \Gamma\left(r_1+r_2-I_e-m+1, \frac{\Lambda_E+H(\gamma_T)}{\bar{\gamma}_E}\right). \tag{35}$$

$$\Upsilon^{\infty}_{\text{3Col}} = \sum_{k=0}^{T_A} \binom{T_A}{k} \left[\frac{\gamma_T(I_U \gamma_{iU}+1)}{\gamma_U}\right]^k (-1)^k \sum_{k_1=0}^{k} \binom{k}{k_1} (-1)^{k_1} \left[\frac{2^{R_s}(I_U \gamma_{iU}+1)}{\gamma_U}\right]^{(N_U-1)k_1+T_A-k} \sum_{m=0}^{N_E} \binom{N_E}{m} \times \frac{\Lambda_E^{I_e}}{\Gamma(N_E)(I_e-1)! \bar{\gamma}_E^{N_E-m}} \exp\left(\frac{\Lambda_E}{\bar{\gamma}_E}\right) \sum_{r_1=0}^{(N_U-1)k_1+T_A-k} \binom{(N_U-1)k_1+T_A-k}{r_1} (\Lambda_0 - \Lambda_E)^{(N_U-1)k_1+T_A-k-r_1} \times \sum_{r_2=0}^{N_E-1} \binom{N_E-1}{r_2} (-\Lambda_E)^{N_E-1-r_2} \bar{\gamma}_E^{r_1+r_2-I_e-m+1} \Gamma\left(r_1+r_2-I_e-m+1, \frac{\Lambda_E}{\bar{\gamma}_E}\right). \tag{36}$$

$\bar{\gamma}_E \to \infty$, and the term $H(\gamma_T)$ is very small compared to $\bar{\gamma}_E$ which can be neglected. Also, the incomplete gamma function $\Gamma(s,x)$ is expressed in its series representation, and hence, the ASOP in (30) can be simplified to (37) and (38) for both Non-Col and Col cases, respectively, where $\varepsilon = \binom{T_A}{k}\binom{k}{k_1}\binom{N_E-1}{m}\binom{v}{\tau}(-1)^{k+k_1+m} \gamma_T^k \delta^v \left[\frac{N_0}{\Omega_U}(I_U \bar{\gamma}_{iU}+1)\right]^{k+v} \times N_E \left(\Lambda_0 - \frac{\Lambda_E}{m+1}\right)^{v-\tau}$, $\varepsilon_1 = \binom{\tau-\alpha}{\Omega_1} \Lambda_E^{\tau-\alpha-\Omega_1} \left(\frac{\Omega_E}{N_0}\right)^{1+\Omega_1} \times \Gamma(\Omega_1+1)$, $\varepsilon_2 = \binom{\tau-\alpha_1}{\Omega_2} \Lambda_E^{\tau-\alpha_1-\Omega_2} \left(\frac{\Omega_E}{N_0}\right)^{\Omega_2} \Gamma(\Omega_2+1)$, $\epsilon_1 = \binom{\tau-\alpha}{\mu} \Lambda_E^{\tau-\alpha-\mu} \left(\frac{\Omega_E}{N_0}\right)^{1+\mu} \Gamma(\mu+1)$, and $\epsilon_2 = \binom{\tau-\alpha_1}{\mu_1} \times \Lambda_E^{\tau-\alpha_1-\mu_1} \left(\frac{\Omega_E}{N_0}\right)^{\mu_1} \Gamma(\mu_1+1)$.

Hence, the optimization problem is formulated such as

$$\min_{P_\alpha} \quad P^{\infty}_{\mathsf{out}}(R_s) \quad \text{Subject to}: \quad 0 < P_\alpha < P_{\max}. \tag{43}$$

By differentiating (37) and (38) w.r.t. P_α, the results are given in (39) and (40) for Non-Col and Col cases, respectively, where Ξ is given by (41) and ϖ is given by (42). Equations (39) and (40) are polynomials in P_α that is solved using any mathematical software package to find the optimal power P^*_α.

V. Simulation and Numerical Results

In this section, numerical results are presented to validate the derived analytical expressions for the SOP, ASOP, and the proposed power allocation model. In

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2019.2907574, IEEE Internet of Things Journal

$$P^{\infty}_{\mathsf{out,Non-Col}}(R_s) = \begin{cases} \sum\limits_{k=0}^{T_A}\sum\limits_{k_1=0}^{k}\sum\limits_{m=0}^{N_E-1}\sum\limits_{\tau=0}^{v}\varepsilon \left\{ \frac{I_e}{(m+1)^{1+\tau}} \sum\limits_{\Omega_1=0}^{\tau-\alpha} \varepsilon_1 P_\alpha^{1+\Omega_1-k-v} + \frac{1}{(m+1)^{1+\tau}} \sum\limits_{\Omega_2=0}^{\tau-\alpha_1} \varepsilon_2 P_\alpha^{1+\Omega_2-k-v} \right\}, & H(\gamma_T) \geq 0 \\ \sum\limits_{k=0}^{T_A}\sum\limits_{k_1=0}^{k}\sum\limits_{m=0}^{N_E-1}\sum\limits_{\tau=0}^{v}\varepsilon \left\{ \frac{I_e}{(m+1)^{1+\tau}} \sum\limits_{\mu=0}^{\tau-\alpha} \epsilon_1 P_\alpha^{1+\mu-k-v} + \frac{1}{(m+1)^{1+\tau}} \sum\limits_{\mu_1=0}^{\tau-\alpha_1} \epsilon_2 P_\alpha^{1+\mu_1-k-v} \right\}, & H(\gamma_T) < 0. \end{cases} \tag{37}$$

$$P^{\infty}_{\mathsf{out,Col}}(R_s) = \begin{cases} \sum\limits_{k=0}^{T_A}\sum\limits_{k_1=0}^{k}\sum\limits_{m=0}^{N_E}\sum\limits_{r_1=0}^{(N_U-1)k_1+T_A-k}\sum\limits_{r_2=0}^{N_E-1}\sum\limits_{\pi_1=0}^{r_1+r_2-I_e-m} \Xi P_\alpha^{1+m+\pi_1-M-((N_U-1)k_1+T_A)}, & H(\gamma_T) \geq 0 \\ \sum\limits_{k=0}^{T_A}\sum\limits_{k_1=0}^{k}\sum\limits_{m=0}^{N_E}\sum\limits_{r_1=0}^{(N_U-1)k_1+T_A-k}\sum\limits_{r_2=0}^{N_E-1}\sum\limits_{w=0}^{r_1+r_2-I_e-m} \varpi P_\alpha^{1+m+w-M-((N_U-1)k_1+T_A)}, & H(\gamma_T) < 0. \end{cases} \tag{38}$$

$$\frac{dP^{\infty}_{\mathsf{out,Non-Col}}(R_s)}{dP_\alpha} = \begin{cases} \sum\limits_{k=0}^{T_A}\sum\limits_{k_1=0}^{k}\sum\limits_{m=0}^{N_E-1}\sum\limits_{\tau=0}^{v}\varepsilon \left\{ \sum\limits_{\Omega_1=0}^{\tau-\alpha} \frac{I_e\varepsilon_1(1+\Omega_1-k-v)}{(m+1)^{1+\tau}} P_\alpha^{\Omega_1-k-v} + \sum\limits_{\Omega_2=0}^{\tau-\alpha_1} \frac{\varepsilon_2(1+\Omega_2-k-v)}{(m+1)^{1+\tau}} P_\alpha^{\Omega_2-k-v} \right\}, & H(\gamma_T) \geq 0 \\ \sum\limits_{k=0}^{T_A}\sum\limits_{k_1=0}^{k}\sum\limits_{m=0}^{N_E-1}\sum\limits_{\tau=0}^{v}\epsilon \left\{ \sum\limits_{\mu=0}^{\tau-\alpha} \frac{I_e\epsilon_1(1+\mu-k-v)}{(m+1)^{1+\tau}} P_\alpha^{\mu-k-v} + \sum\limits_{\mu_1=0}^{\tau-\alpha_1} \frac{\epsilon_2(1+\mu_1-k-v)}{(m+1)^{1+\tau}} P_\alpha^{\mu_1-k-v} \right\}, & H(\gamma_T) < 0. \end{cases} \tag{39}$$

$$\frac{dP^{\infty}_{\mathsf{out,Col}}(R_s)}{dP_\alpha} = \begin{cases} \sum\limits_{k=0}^{T_A}\sum\limits_{k_1=0}^{k}\sum\limits_{m=0}^{N_E}\sum\limits_{r_1=0}^{(N_U-1)k_1+T_A-k}\sum\limits_{r_2=0}^{N_E-1}\sum\limits_{\pi_1=0}^{r_1+r_2-I_e-m} \frac{P_\alpha^{m+\pi_1-M-((N_U-1)k_1+T_A)}}{[\Xi(1+m+\pi_1-M-(N_U-1)k_1-T_A)]^{-1}}, & H(\gamma_T) \geq 0 \\ \sum\limits_{k=0}^{T_A}\sum\limits_{k_1=0}^{k}\sum\limits_{m=0}^{N_E}\sum\limits_{r_1=0}^{(N_U-1)k_1+T_A-k}\sum\limits_{r_2=0}^{N_E-1}\sum\limits_{w=0}^{r_1+r_2-I_e-m} \frac{P_\alpha^{m+w-M-((N_U-1)k_1+T_A)}}{[\varpi(1+m+w-M-(N_U-1)k_1-T_A)]^{-1}}, & H(\gamma_T) < 0. \end{cases} \tag{40}$$

$$\Xi = \binom{T_A}{k}\binom{k}{k_1}\binom{N_E}{m}\binom{(N_U-1)k_1+T_A-k}{r_1}\binom{N_E-1}{r_2}\binom{r_1+r_2-I_e-m}{\pi_1}(-1)^{k+k_1+M-r_2-1}\left[\frac{N_0}{\Omega_U}(I_U\bar{\gamma}_{iU}+1)\right]^{(N_U-1)k_1+T_A} \times (\gamma_T)^k \delta^{(N_U-1)k_1+T_A-k}\Lambda_E^{I_e+N_E-1}\frac{\Gamma(m+I_e)}{\Gamma(N_E)(I_e-1)!}(\Lambda_0-\Lambda_E)^{(N_U-1)k_1+T_A-k-r_1}\left(\frac{\Omega_E}{N_0}\right)^{r_1+r_2-I_e+\pi_1+2-M}\Gamma(\pi_1+1). \tag{41}$$

$$\varpi = \binom{T_A}{k}\binom{k}{k_1}\binom{N_E}{m}\binom{(N_U-1)k_1+T_A-k}{r_1}\binom{N_E-1}{r_2}\binom{r_1+r_2-I_e-m}{w}(-1)^{k+k_1+M-r_2-1}\left[\frac{N_0}{\Omega_U}(I_U\bar{\gamma}_{iU}+1)\right]^{(N_U-1)k_1+T_A} \times (\gamma_T)^k \delta^{(N_U-1)k_1+T_A-k}\Lambda_E^{N_E-m-w-1}\frac{\Gamma(m+I_e)}{\Gamma(N_E)(I_e-1)!}(\Lambda_0-\Lambda_E)^{(N_U-1)k_1+T_A-k-r_1}\left(\frac{\Omega_E}{N_0}\right)^{1+m+w-M}\Gamma(w+1). \tag{42}$$

all simulation results, unless they are stated elsewhere, the following parameters are adjusted as follows, $P_\alpha = 1, \text{SNR} = 10$ dB, $\bar{\gamma}_{i_u,u} = 2$ dB, $\bar{\gamma}_{i_e,e} = 1$ dB, $P_{i_e} = P_{i_u} = 0.15P_\alpha$, and $\bar{\gamma}_E = 0$ dB. The other simulation parameters are listed in TABLE I.

TABLE I: Simulation Parameters per Figure

Par. / Fig.	T_A	N_U	N_E	$\bar{\gamma}_T$(dB)	R_s	I_U	I_e
Figure 3	2	2	1	5	4	3	3,5,8
Figure 4	1	2	2	10	4	1,0,3	3,0,1
Figure 5	1,2	2	4	10	1,4	2	5
Figure 6	1	2	2	8	3	1	3
Figure 7	1	2	4	10,20	1,4	2	5
Figure 8	1	2	4,6	10	1,4	2	5
Figure 9	1	2	2	0-35	4	2	5
Figure 10	1	2	2	10	1,4	2	5
Figure 11	3	3	2	10	4	2	2

The SOP against $\bar{\gamma}_U$ for different values of I_e is presented in Figure 2. It is shown that increasing I_e enhances the system secrecy performance as expected since the eavesdropper suffers from high values of interference. Moreover, the exact and simulation results match at medium to high $\bar{\gamma}_U$ values.

The impact of CCI signals is investigated in Figure 3 for the Col case. It is clear that when $I_e > I_U$ the SOP reduces, which improves the secrecy performance of the system. This is because, increasing I_e reduces the SINR of the eavesdropper compared to that of the legitimate node. Similarly, increasing I_U compared to I_e degrades the system secrecy performance.

The impact of the number of BS antennas T_A against $\bar{\gamma}_U$ is investigated in Figure 4. The results show that increasing T_A and consequently increasing the diversity order of the TAS/tSD improves the secrecy performance. It is also worthy noting that the Col eavesdropper case has a poorer secrecy performance than the Non-Col case. For the Col case, the EFC output is a weighted sum of all the eavesdropper SNR values whereas for the Non-Col case the EFC output is from a single eavesdropping node with the best channel link quality.

Figure 5 compares the secrecy performance of the TAS/tSD scheme and TAS/SC scheme, in the presence of CCI against $\bar{\gamma}_U$. Noting that, the TAS/SC scheme uses TAS at the BS and selects the best legitimate node with the highest SNR by adopting SC mode. It is evident that the TAS/SC scheme has a better secrecy performance as compared to the TAS/tSD

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2019.2907574, IEEE Internet of Things Journal

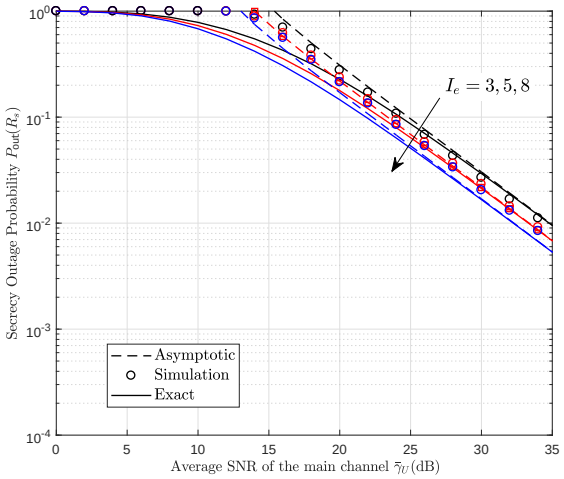

Fig. 2: Secrecy outage probability against $\bar{\gamma}_U$ for different number of I_e, with $P_\alpha = 1, I_U = 3, T_A = 2, N_E = 1, N_U = 2, \gamma_T = 5$ dB, SNR $= 10$ dB, $\bar{\gamma}_{i_u,u} = 2$ dB, $\bar{\gamma}_{i_e,e} = 1$ dB, $\bar{\gamma}_E = 0$ dB, $R_s = 4$, and $\zeta = 0.15$.

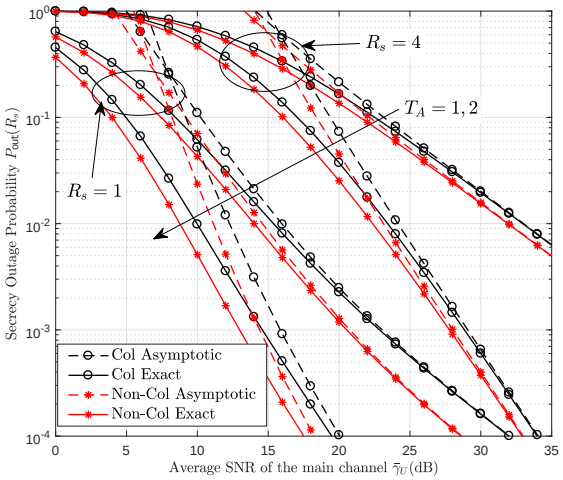

Fig. 4: Secrecy outage probability against $\bar{\gamma}_U$ for different number of T_A, with $P_\alpha = 1, I_U = 2, I_e = 5, N_U = 2, N_E = 4, \gamma_T = 10$ dB, SNR $= 10$ dB, $\bar{\gamma}_{i_u,u} = 2$ dB, $\bar{\gamma}_{i_e,e} = 1$ dB, $\bar{\gamma}_E = 0$ dB, and $P_{i_e} = P_{i_u} = 0.15P_\alpha$.

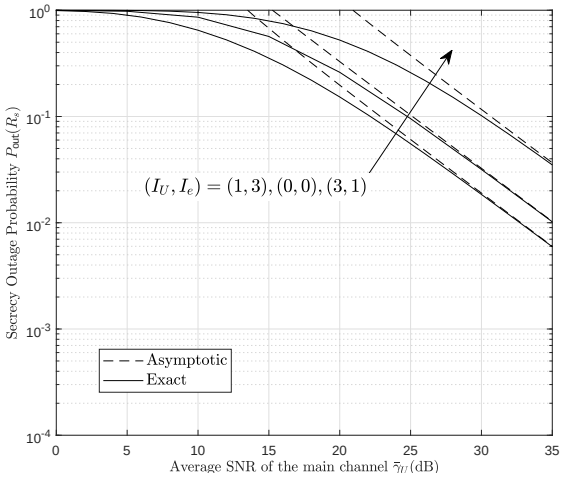

Fig. 3: Secrecy outage probability against $\bar{\gamma}_U$ in the presence of different number of I_U and I_e, with $P_\alpha = 1, T_A = 1, N_E = 2, N_U = 2, R_S = 4, \gamma_T = 10$ dB, SNR $= 10$ dB, $\bar{\gamma}_{i_u,u} = 2$ dB, $\bar{\gamma}_{i_e,e} = 1$ dB, $\bar{\gamma}_E = 0$ dB, and $P_{i_e} = P_{i_u} = 0.15P_\alpha$.

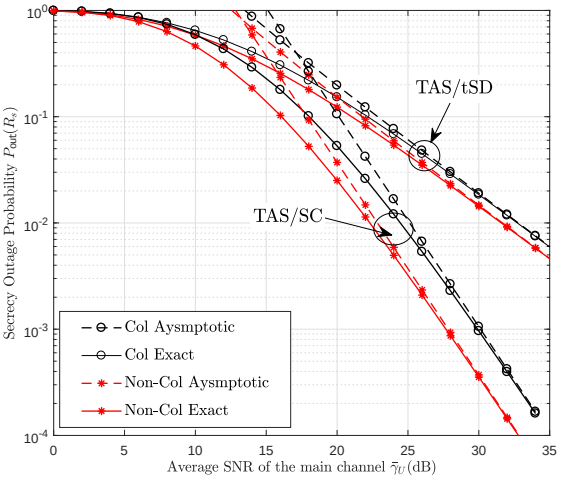

Fig. 5: Comparing the secrecy performance of TAS/SC and TAS/tSD schemes, with $P_\alpha = 1, I_U = 1, I_e = 3, T_A = 1, N_E = 2, N_U = 2, \gamma_T = 10$ dB, SNR $= 10$ dB, $\bar{\gamma}_{i_u,u} = 2$ dB, $\bar{\gamma}_{i_e,e} = 1$ dB, $\bar{\gamma}_E = 0$ dB, and $P_{i_e} = P_{i_u} = 0.15P_\alpha$.

scheme. This can be explained as the TAS/SC scheme selects the best user with the highest SNR whereas for the TAS/tSD scheme, a user whose SNR is greater or equal to a predefined threshold γ_T is selected even though its channel quality is not the best. The performance trade-off between TAS/tSD scheme and TAS/SC scheme is the reduction in hardware complexity, since there is no need for a dedicated system to monitor each branch SNR as compared to using TAS/SC [25, 33].

The SOP against $\bar{\gamma}_U$ is presented in Figure 6. The figure indicates that the SOP decreases as γ_T increases for both the Non-Col and Col cases. This indicates that increasing γ_T can be an effective way of enhancing the secrecy performance.

Figure 7 shows the impact of N_E on the secrecy performance. As the collusion intensity increases, so does the SOP, implying that the eavesdropper collusion significantly increase the possibility of secrecy outage. For example, for $N_E = 6$ the SOP is greater than the Non-Col case.

Figure 8 represents the SOP versus γ_T for different values of I_U and I_e. The SOP decreases as γ_T increases for both the Non-Col and Col cases. Moreover, even in the absence of CCI, increase in the γ_T improves the secrecy performance of the system. However, after a certain γ_T value, a floor in the secrecy performance appears as we approach high γ_T values. This means that the network performance after this instance, converts to the conventional TAS/SC scheme instead of the TAS/tSD scheme by selecting the best available legitimate node. Another important observation from this figure, is that the system with CCI at the legitimate node and eavesdropping nodes undergoes the floor faster than the system without CCI.

Figure 9 depicts the SOP versus eavesdropper average SNR $\bar{\gamma}_E$. The SOP approaches 1 if the eavesdropper average SNR increases beyond $\bar{\gamma}_U$ for both cases. Furthermore, this figure shows an improvement in the secrecy performance when the constant rate R_s is reduced.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2019.2907574, IEEE Internet of Things Journal

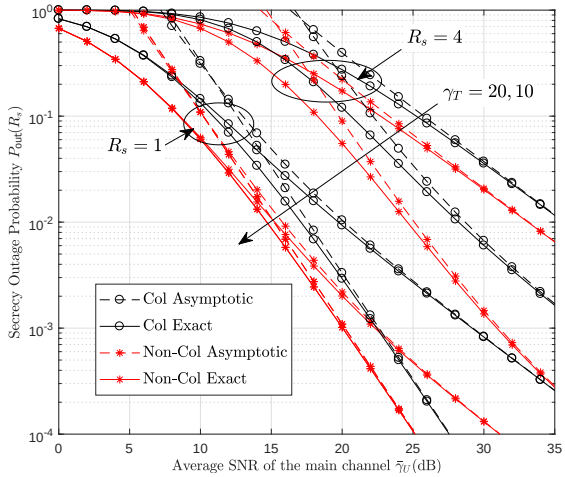

Fig. 6: Secrecy outage probability against $\bar{\gamma}_U$ for different values of γ_T, with $P_\alpha = 1, I_U = 2, I_e = 5, T_A = 1, N_E = 4, N_U = 2, \text{SNR} = 10$ dB, $\bar{\gamma}_{i_u,u} = 2$ dB, $\bar{\gamma}_{i_e,e} = 1$ dB, $\bar{\gamma}_E = 0$ dB, and $P_{i_e} = P_{i_u} = 0.15P_\alpha$.

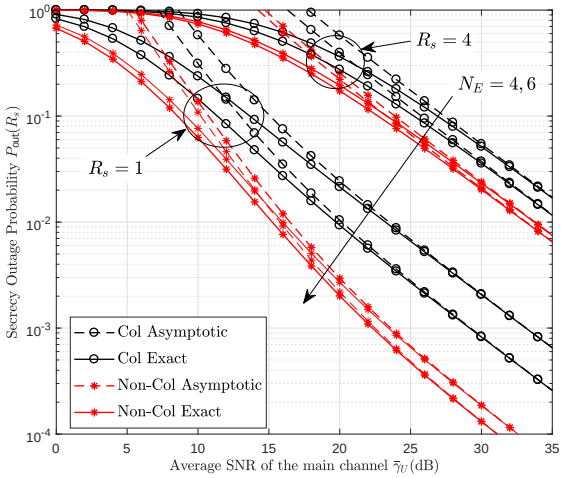

Fig. 7: Secrecy outage probability against $\bar{\gamma}_U$ for different number of eavesdroppers N_E, with $P_\alpha = 1, I_U = 2, I_e = 5, T_A = 1, N_U = 2, \gamma_T = 10$ dB, $\text{SNR} = 10$ dB, $\bar{\gamma}_{i_u,u} = 2$ dB, $\bar{\gamma}_{i_e,e} = 1$ dB, $\bar{\gamma}_E = 0$ dB and $P_{i_e} = P_{i_u} = 0.15P_\alpha$.

The secrecy performance versus $\bar{\gamma}_U$ for TAS/tSD and TAS/SC schemes with optimal power allocation solution P_α^* and maximum power model (i.e., $P_\alpha = 1$) is investigated in Figure 10. The results show that the proposed power allocation model has worse secrecy performance compared to the maximum power model at low to medium $\bar{\gamma}_U$ values for both TAS schemes. However, as $\bar{\gamma}_U$ increases, the optimal power allocation model for both Non-Col and Col cases outperforms the maximum power model. This is because the proposed power allocation optimization problem was formulated based on the asymptotic analysis for high SNR values.

VI. Conclusions

The effect of CCI on the secrecy performance of TAS/tSD scheme has been investigated for IoT networks in the presence of multiple eavesdroppers. Identical CCI signals have been assumed to harm both the legitimate nodes and the

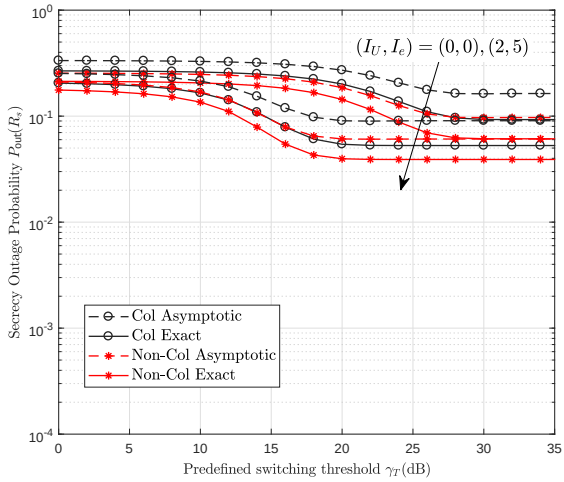

Fig. 8: Secrecy outage probability against γ_T for for interference and no interference, with $P_\alpha = 1, T_A = 1, N_E = 2, N_U = 2, \bar{\gamma}_U = 30$ dB, $\text{SNR} = 10$ dB, $\bar{\gamma}_{i_u,u} = 2$ dB, $\bar{\gamma}_{i_e,e} = 1$ dB, $\bar{\gamma}_E = 0$ dB and $P_{i_e} = P_{i_u} = 0.15P_\alpha$.

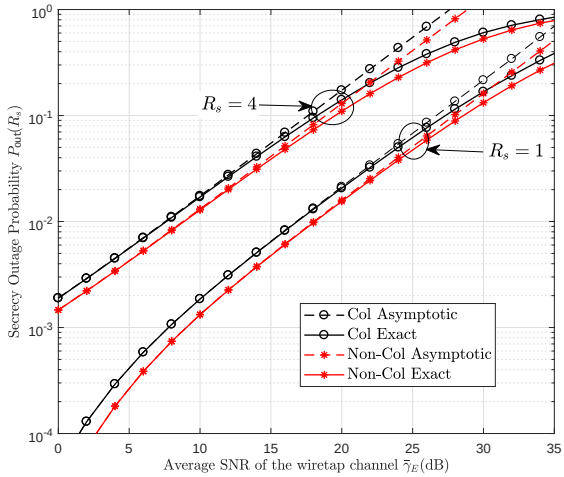

Fig. 9: Secrecy outage probability against $\bar{\gamma}_E$ for different values of a constant secrecy rate R_s, with $P_\alpha = 1, I_U = 2, I_e = 5, T_A = 1, N_E = 2, N_U = 2, \gamma_T = 10$ dB, $\text{SNR} = 10$ dB, $\bar{\gamma}_{i_u,u} = 2$ dB, $\bar{\gamma}_{i_e,e} = 1$ dB, $\bar{\gamma}_E = 0$ dB and $P_{i_e} = P_{i_u} = 0.15P_\alpha$.

eavesdroppers. Two eavesdropping scenarios are considered; namely, the non-colluding and the colluding scenario. We have derived new closed-form expressions for the PDF and CDF of the SINR for both cases in the presence of CCI signals. Moreover, closed-form expressions for the exact SOP and ASOP have been derived for both cases. In addition, a new power allocation model has been proposed to enhance the secrecy performance by minimizing the ASOP. The numerical results indicate that increasing the number of eavesdroppers adversely affects the secrecy performance of the network. Further, increasing the switching threshold γ_T effectively improves the overall system secrecy performance since it enhances the quality of the selected main channel link compared to that of the wiretap channel link. The results have also shown that the performance of the proposed power allocation model surpasses that of the traditional one.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2019.2907574, IEEE Internet of Things Journal

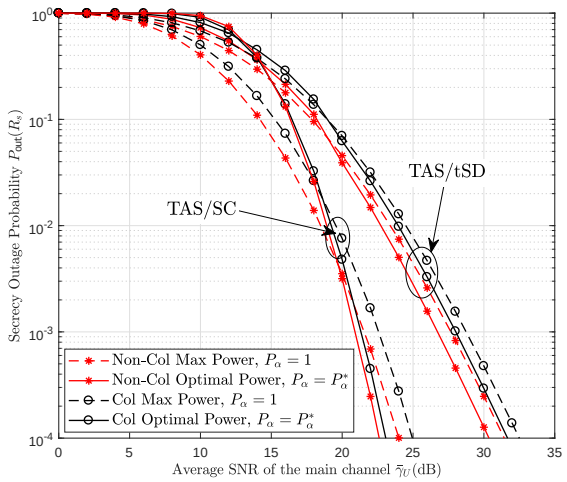

Fig. 10: Secrecy outage probability against $\bar{\gamma}_U$ of TAS/tSD and TAS/SC schemes for Col and Non-Col cases with different power values, with $I_U = 2, I_e = 2, T_A = 3, N_E = 2, N_U = 3, R_S = 4, \gamma_T = 10$ dB, SNR $= 10$ dB, $\bar{\gamma}_{i_u,u} = 2$ dB, $\bar{\gamma}_{i_e,e} = 1$ dB, $\bar{\gamma}_E = 0$ dB and $P_{i_e} = P_{i_u} = 0.15P_\alpha$.

REFERENCES

[1] Y. Wu, A. Khisti, C. Xiao, G. Caire, K. Wong, and X. Gao, "A survey of physical layer security techniques for 5G wireless networks and challenges ahead," *IEEE J. Sel. Areas Commun.,* vol. 36, no. 4, pp. 679–695, Apr. 2018.

[2] F. Shi, W. Tan, J. Xia, D. Xie, L. Fan, and X. Liu, "Hybrid cache placement for physical-layer security in cooperative networks," in *IEEE Access*, vol. 6, pp. 8098–8108, Jan. 2018.

[3] Y. Huo, Y. Tian, L. Ma, X. Cheng, and T. Jing, "Jamming strategies for physical layer security," *IEEE Wireless Commun. Mag.,* vol. 25, no. 1, pp. 148–153, Feb. 2018.

[4] L. Fan, X. Lei, N. Yang, T. Q. Duong, and G. K. Karagiannidis, "Secrecy cooperative networks with outdated relay selection over correlated fading channels," *IEEE Trans. Veh. Technol.,* vol. 66, no. 8, pp. 7599–7603, Aug. 2017.

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

[6] C. Hu, J. Luo, Y. Pu, J. Yu, R. Zhao, H. Huang, and T. Xiang, "An efficient privacy-preserving data aggregation scheme for IoT," in Proc. *Int. Conf. Wireless Algorithms, Syst. Appl.,* Tianjin, China, 20-22 June 2018, pp. 164–176.

[7] A. Menezes, P. Oorschot, and S. Vanstone, Handbook of Applied Cryptography, Boca Raton, FL, USA: CRC Press, 2001.

[8] J. Talbot and D. Welsh, Complexity and Cryptography: *An Introduction, Cambridge, U.K.:Cambridge Univ. Press,* Springer, Feb. 2006.

[9] Y. Zhang, Y. Shen, H. Wang, J. Yong, and X. Jiang, "On secure wireless communications for IoT under eavesdropper collusion," *IEEE Trans. Autom. Sci. Eng.,* vol. 13, no. 3, pp. 1281–1293, Jul. 2016.

[10] N. Yang, S. Yan, J. Yuan, R. Malaney, R. Subramanian, and I. Land, "Artificial noise: Transmission optimization in multi-input single-output wiretap channels," *IEEE Trans. Commun.,* vol. 63, no. 5, pp. 1771–1783, May 2015.

[11] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," in Proc. *IEEE,* vol. 104, no. 9, pp. 1–39, Sep. 2016.

[12] A. D. Wyner, "The wire-tap channel," in *Bell Syst. Tech. J.,* vol. 54, pp. 1355–1387, Oct. 1975.

[13] X. S. Zhou, L. Song, Y. Zhang, Physical Layer Security in Wireless Communications, Boca Raton, FL, USA:CRC Press, 2013.

[14] M. Bloch, and J. Barros, Physical-Layer Security: From Information Theory to Security Engineering, 1st ed. Cambridge, UK:Cambridge University Press, 2011.

[15] H. M. Wang, T. X. Zheng, Physical Layer Security in Random Cellular Networks, Singapore:Springer, 2016.

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

[17] C. E. Shannon, "Communications theory of secrecy systems," *Bell Syst. Tech. J.,* vol. 28, pp. 656–715, 1949.

[18] Y. Shiu, S. Y. Chang, H. Wu, S. C. Huang, and H. Chen, "Physical layer security in wireless networks: A tutorial," *IEEE Wireless Commun.*, vol. 18, no. 2, pp. 66–74, Apr. 2011.

[19] 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. Conf. Commun. Workshops (ICC'13)*, Budapest, Hungary, 9-13 Jun. 2013, pp. 381–385.

[20] 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, Jan. 2013.

[21] 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, Mar. 2014.

[22] 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, Aug. 2015.

[23] F. Shu, Z. Wang, R. Chen, Y. Wu, and J. Wang, "Two high-performance schemes of transmit antenna selection for secure spatial modulation," *IEEE Trans. Veh. Technol.,* vol. 67, no. 9, pp. 8969–8973, Sept. 2018.

[24] 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, Feb. 2016.

[25] 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, Dec. 2016.

[26] M. Yang, D. Guo, Y. Huang, T. Q. Duong and B. Zhang, "Secure multiuser scheduling in downlink dual-hop regenerative relay networks over Nakagami-m fading channels," *IEEE Trans. Wireless Commun.,* vol. 15, no. 12, pp. 8009–8024, Dec. 2016.

[27] M. Yang, B. Zhang, Y. Huang, N. Yang, D. Guo, B. Gao, "Secure multiuser communication in wireless sensor networks with TAS and cooperative jamming," *J. Sensors*, vol. 16, no. 11, pp. 1908, Nov. 2016.

[28] B. Li, J. Zhou, Y. Zou, and F. Wang, "Closed-form secrecy outage analysis of cellular downlink systems in the presence of co-channel interference," *IEEE Trans. Wireless Commun.,* vol. 17, no. 7, pp. 4721–4734, Jul. 2018.

[29] V. N. Vo, T. G. Nguyen, C. So-In, and D. Ha, "Secrecy performance analysis of energy harvesting wireless sensor networks with a friendly jammer," *IEEE Access,* vol. 5, pp. 25196–25206, Oct. 2017.

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

[31] A. Jeffrey and D. Zwillinger, *Table of integrals, series, and products, 7th ed.* New York: Academic Press, 2007.

[32] T. Ssettumba, A. H. A. El-Malek, M. Elsabrouty, and M. Abo-Zahhad, "Physical layer security enhancement for internet of things in the presence of co-channel interference and multiple eavesdroppers," Preprint *Researchgate website*, Dec. 2018, [Online]. Available: https://www.researchgate.net/publication/329335779_Physical_Layer_Security_Enhancement_for_Internet_of_Things_in_the_Presence_of_Co-channel_Interference_and_Multiple_Eavesdroppers, DOI: 10.13140/RG.2.2.10840.96008/1.

[33] A. Goldsmith, Wireless Communications, *Cambridge, U.K.:Cambridge Univ. Press,* 2005.