IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received September 13, 2018, accepted October 2, 2018, date of publication October 8, 2018, date of current version October 31, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2874215

A Zero-Sum Game Approach for Non-Orthogonal Multiple Access Systems: Legitimate Eavesdropper Case

YAMEN ALSABA, (Student Member, IEEE), CHEE YEN LEOW, (Member, IEEE), AND SHARUL KAMAL ABDUL RAHIM, (Senior Member, IEEE)
Wireless Communication Centre, School of Electrical Engineering, Faculty of Engineering, Universiti Teknologi Malaysia, Skudai Johor 81310, Malaysia

Corresponding author: Chee Yen Leow (bruceleow@utm.my)

This work was supported in part by H2020-MSCA-RISE-2015 under Grant 690750, in part by the Ministry of Education Malaysia under Grant 4F818, Grant 07085, Grant 4J210, Grant 4F617, and Grant 4F901, and in part by Universiti Teknologi Malaysia under Grant 17H23, Grant 19H58, Grant 13H08, Grant 4J213, and Grant 04G37.

ABSTRACT In this paper, secure communication in non-orthogonal multiple access (NOMA) downlink system is considered wherein two NOMA users with channel gain difference are paired in each transmission slot. The user with poor channel condition (weak user) is entrusted, while the user with good channel condition (strong user) is a potential eavesdropper. The weak user data can be intercepted by the strong user since the strong user needs to decode the weak user's message for successive interference cancellation operation in NOMA. To impair strong user's eavesdropping capability, weak user's information-bearing signal is merged with an artificial signal (AS). Thus, the eavesdropping process requires extra decoding step at higher power level. The secrecy outage probability of the weak user is derived and provided in closed-form expression. The weak user faces a choice between transmitting the information-bearing signal with the total power and the deploying the AS technique, whereas the strong user can choose whether to eavesdrop the weak user's message or not. To investigate users' power-secrecy tradeoffs, their interactions are modeled as a non-cooperative zero-sum game. The existence of Nash equilibria (NEs) of the proposed game is first analyzed, and pure and mixed-strategy NE profiles are provided. In addition, numerical simulations are conducted to validate the analytical results and to prove that AS-Aided proposed scheme enhances the secrecy performance of NOMA systems while maintaining the NOMA superiority over OMA systems.

INDEX TERMS Game theory, Nash equilibrium, non-orthogonal multiple access, physical layer security, zero-sum game.

I. INTRODUCTION

Non-orthogonal multiple access (NOMA) has been recognized as the potential multiple-access scheme for the future communication systems, for its appealing features of spectral efficiency, low latency and user fairness [1]. Unlike previous multiple access schemes, NOMA differentiates users according to their channel conditions to broadcast the information message at the same time, frequency and code but with different power level. User with better channel condition (strong user) is allocated with lower power level than that of the user with poor channel gain (weak user). In order to deploy downlink NOMA system, two main techniques are involved. First, superposition coding (SC) is used at the base station side to build the information message of the paired NOMA users. Second, successive interference cancellation (SIC) is performed at the strong users' terminals side, where the strong user decodes the information message of the week user [2], subtracts it from the superimposed message before decoding his own message. Meanwhile, the weak user treats the strong user's message as noise since he is allocated with higher power level [3]. The fact that strong user has side-information of the weak user message can be exploited in cooperative NOMA, where strong user relays weak user's messages to increase the reliability of the communication system [4]. On the other hand, from information security perspective, this feature threatens the information secrecy of the system, when the strong user turns into a malicious node.

The open nature of wireless communication necessitates preventive measures to guarantee secure connection. Yet, fully secure communication can only be guaranteed by means of the physical layer (PHY) security [5]. In PHY security approach, the information secrecy is enhanced by exploiting both the physical signal's format in addition to the physical characteristics of the communication system. PHY security relies on signal processing tools like beamforming for turning the physical communication channel's imperfections to a source of secrecy. In [5], secrecy rate is proved to be always positive if the source-destination channel condition is better than that of the source-eavesdropper channel. Furthermore, information secrecy can be achieved by artificial noise (AN) technique even if the source-destination channel is worse than the source-eavesdropper channel [6]. The optimal power ratio between the information-bearing and the AN signals in order to minimize the secrecy outage probability is examined in [7]. In addition, the secrecy outage probability for multiple-input single-output (MISO) wiretap channel in the presence of eavesdroppers is derived and provided in closed-form formula. The secrecy outage probability is derived in [8] for two different cases, with and without the availability of the channel state information (CSI) of the eavesdroppers at the base station. On the other hand, a multi-user large scale AN-aided communication systems with the unavailability of the eavesdropper's CSI is investigated in [9]. The ergodic secrecy sum rate is derived in [9] under both perfect and imperfect CSI training scenarios.

Exploiting PHY security in NOMA systems has gained a lot of attention lately. The authors in [10] derive the secrecy outage probability in downlink NOMA system for several antenna selection schemes. In [11], the secrecy sum rate is maximised in a downlink NOMA system consists of base station, multiple legitimate receivers and an external eavesdropper. References [12] and [13] investigate enhancing information security of large-scale NOMA networks under external eavesdropper scenario. PHY security is enhanced in the aforementioned system model in [12] by introducing the concept of protected zone around the source node. AN technique is exploited in [13] to enhance the secrecy outage probability of multiple-antenna transmission scenario. NOMA internal or legitimate eavesdropper case is investigated in [14], where the cell-edge user (weak user) is considered as a potential eavesdropper who is trying to decode the cell-centre user's message in a beamforming NOMA system. However, in practical scenarios, eavesdroppers are usually users with good channel condition and they are located near to the base station, so that the attack will be more energy efficient and more destructive to the network [15]. Such practical scenario has not been investigated in NOMA system.

Game theory [16] is a mathematical framework used for modeling of all possible strategies among various decision-makers who have partly or completely conflicting goals. Game theory is first adopted in economics to characterize the potential competition among industrial and commercial facilities. Game theory can be classified into two main types, non-cooperative and cooperative games. In the first scheme, no information exchange among the different players, while in the late, players are collaborating to enhance the game outcomes. Non-cooperative games are solved normally by finding its Nash equilibrium (NE), which can be defined as a profile that no player will gain if he diverts alone from NE [17]. Whereas, cooperative games are solved mainly by means of Nash bargaining equilibrium or coalition formation [18]. The competition over communications systems' resources among users motivates a lot of work to introduce the game theory to tackle the power allocation problem in wireless networks [19]–[21]. Recently, game-theoretical approach has been exploited in large scale to enhance the physical layer security of wireless networks [22]. The authors in [23] adopt the game theory discipline to enhance the secrecy rate of cognitive radio networks. A two-player zero-sum game model in multiple-input multiple-output (MIMO) system and malicious relay scenario is adopted in [24] and [25] respectively. However, the use of game theory framework in enhancing the PHY security of NOMA system remains unexplored.

In this work, a secure MISO downlink NOMA communication system is considered. In this system, a multi-antenna base station communicates with two users per transmission slot. NOMA strong user decodes the weak user's message to subtract it by means of SIC process, and hence he can readily eavesdrop the weak user's message, if he is a malicious user. In order to impair the strong user capability of decoding the weak user's information message, the power allocated to the weak user is divided to broadcast artificial signal (AS) in the orthogonal subspace of the weak user's direction with a guarantee that the power allocated to weak user after power dividing is still higher than that of the strong user. For the potential eavesdropper to extract the exact weak user's information-bearing signal from the combined signal, extra decoding process at higher power level is required. The weak user can decode his message as the power allocated to him is still higher than that of the strong user. Since the AS scheme requires the total power split from the weak user perceptive, and the eavesdropping process requires higher SINR and extra decoding processes from the strong user side, both weak and strong users can choose between exploiting the AS scheme or not and to eavesdrop or not respectively. The possible interactions between both users and the energy-security trade-off outcomes are modeled as a non-cooperative two-player zero-sum game, wherein the secrecy capacity is considered as the utility function. The game is first formulated and its NE is proved to exist. Furthermore, pure and mixed-strategy Nash equilibria are proposed to provide an eavesdropping avoidance strategy. In addition, weak user's secrecy outage probability is provided in closed-form formula, and Monte Carlo simulations are performed to validate the obtained results. To the best of the authors' knowledge, the case where NOMA strong user is the potential eavesdropper has not been dealt with before in literature. Considering NOMA strong user as the malicious node is more realistic for two reasons, i) NOMA strong user knows the information message of the weak user in order to decode his message; ii) Eavesdropper is usually node with strong channel condition. Furthermore, this work introduces the game theory and zero-sum model in enhancing the PHY security of NOMA systems for the first time in the literature. The proposed AS-aided secure scheme is proved to enhance the secrecy performance of NOMA system without affecting its functionalities or its superiority over the conventional orthogonal multiple access (OMA) systems. Table I, represents the main notations adopted in this work.

TABLE 1. Table of notation.

Symbol	Definition
s_n, s_m	Information-bearing signals for the n-th and the m-th users respectively.
a_n, a_m	NOMA power coefficient for user n and user m respectively.
$\mathbf{w}_n, \mathbf{w}_m$	Beamforming weight for the n-th and the m-th users respectively.
$\mathbf{V}_m$	Artificial signal transmitting matrix.
$\mathbf{e}_m$	Artificial signal codewords vector.
β	Power splitting ratio between information-bearing signal and artificial signal.
P	Total transmit power.
n_n, n_m	The AWGN generated at the terminal n, m respectively.
$\mathbf{h}_n, \mathbf{h}_m$	Channel gain between the base station and user n, m receptively.
N	The number of the base station antenna.
ρ	Transmit SNR.
C_m	The instantaneous secrecy capacity of the weak user m.
R_m	The target rate of user m.
p	The probability with which the weak user m plays the 'Total transmit' strategy.
q	The probability that the strong user n plays the 'Eavesdrop' strategy.

II. SYSTEM MODEL

Secure communication in downlink single cell NOMA system is considered, where a multi-antenna base station equipped with N antennas communicates with L single antenna users. Without loss of generality, base station-users channels are arranged in ascending order $\|\mathbf{h}_1\mathbf{w}_1\|^2 \leq \ldots\ldots \|\mathbf{h}_m\mathbf{w}_m\|^2 \leq \|\mathbf{h}_n\mathbf{w}_n\|^2 \leq \ldots \|\mathbf{h}_L\mathbf{w}_L\|^2$, where $\mathbf{w}_k$ is the beamforming weight vector for user k. The channel gain represents Rayleigh fading multiplied by the path loss. In each transmission time, two spatially separated users are paired, denoted as m-th and n-th receivers with $(m < n)$, under the potential malicious attempt of the strong user n eavesdropping the m-th user's information message. We assume that perfect CSI of both paired users is available at the transmitter. In order to impair the strong user's capability of decoding the weak user's message, the weak user's information-bearing signal is combined with an AS. Hence, if the strong user wants to intercept the weak user's information-bearing message, he has to extract it from the combined signal.

The principle of masking the beamformed broadcast information with the AS to confuse the strong user will simulate the AN technique [6] and can be outlined as follows: An $N \times N$ matrix $\mathbf{W}_m = [\mathbf{w}_m \quad \mathbf{V}_m]$ that its columns form an orthogonal basis of $\mathbb{C}^N$ is introduced. The first column of the matrix is given by $\mathbf{w}_m = \frac{\mathbf{h}_m^\dagger}{\|\mathbf{h}_m\|}$, while $\mathbf{V}_m$ is a $N \times (N-1)$ matrix with orthogonal columns.

Thus, the superimposed beamformed message for the two corresponding receivers can be expressed as

$$\mathbf{x} = \mathbf{w}_n s_n + \mathbf{w}_m s_m + \mathbf{V}_m \mathbf{e}_m \tag{1}$$

where s_n and s_m, are the information-bearing signals for the n-th and the m-th users respectively, with $\mathbb{E}(\mid s_n \mid^2) = \sigma_{s_n}^2 = a_n P$, $\mathbb{E}(\mid s_m \mid^2) = \sigma_{s_m}^2 = \beta a_m P$. P is the total transmit power, a_n, and a_m are the NOMA power coefficients for user n and m respectively, with $a_n < a_m$ and $a_n + a_m = 1$. β is the power splitting coefficient between information-bearing and the AS with $a_n < \beta a_m$. $\mathbf{e}_m$ is $N-1$ vector, its elements are independent artificial codewords each with variance $\frac{(1-\beta)a_m P}{(N-1)}$, and $\mathbf{w}_n = \frac{\mathbf{h}_n^\dagger}{\|\mathbf{h}_n\|}$ is the beamforming vector of the strong user n.

The signal received at the n-th user can be expressed as

$$y_n = \mathbf{h}_n \mathbf{w}_n s_n + \mathbf{h}_n \mathbf{w}_m s_m + \mathbf{h}_n \mathbf{V}_m \mathbf{e}_m + n_n \tag{2}$$

where $\mathbf{h}_n$ is the complex channel vector between base station and strong user, and $n_n \sim \mathbb{C}N(0, \sigma^2)$ is the additive white complex Gaussian noise (AWGN) signal. In the proposed scheme, strong user decodes the weak user's information message combined with the AS to be subtracted by means of SIC process, and then proceed to decode his own message. The SINR at the strong user to remove the weak user' message combined with the AS signal (to perform SIC) is

$$\gamma_{nm} = \frac{\beta a_m \|\mathbf{h}_n \frac{\mathbf{h}_m^\dagger}{\|\mathbf{h}_m\|}\|^2 + \frac{(1-\beta)a_m}{N-1}\|\mathbf{h}_n \mathbf{V}_m{}^2\|}{a_n\|\mathbf{h}_n\|^2 + \frac{1}{\rho}} \tag{3}$$

where $\rho = \frac{P}{\sigma^2}$ is the transmit signal to noise ratio (SNR). While the SINR to detect the information-bearing signals to the weak at the strong user n, i.e., internal eavesdropper

$$\gamma_{nm}^{eve} = \frac{\beta a_m \|\mathbf{h}_n \frac{\mathbf{h}_m^\dagger}{\|\mathbf{h}_m\|}\|^2}{a_n\|\mathbf{h}_n\|^2 + \frac{(1-\beta)a_m}{N-1}\|\mathbf{h}_n \mathbf{V}_m\|^2 + \frac{1}{\rho}}. \tag{4}$$

The signal received at the weak user m is given by

$$y_m = \mathbf{h}_m \frac{\mathbf{h}_m^\dagger}{\|\mathbf{h}_m\|} s_m + \mathbf{h}_m \mathbf{w}_n s_n + n_m \tag{5}$$

where $\mathbf{h}_m$ is the complex channel vector between the weak user m and the base station, $n_m \sim \mathbb{C}N(0, \sigma^2)$ is the AWGN, (Note that we assume that $\sigma_n^2 = \sigma_m^2 = \sigma^2$).

The SINR needed by the weak user to decode his own information message

$$\gamma_m = \frac{\beta a_m \|\mathbf{h}_m\|^2}{a_n\|\mathbf{h}_m \frac{\mathbf{h}_n^\dagger}{\|\mathbf{h}_n\|}\|^2 + \frac{1}{\rho}}. \tag{6}$$

The instantaneous secrecy capacity of the weak user m can be expressed as

$$C_m = [\log_2(1 + \gamma_m) - \log_2(1 + \gamma_{nm}^{eve})]^+ \tag{7}$$

where $[x]^+ = \max\{x, 0\}$.

While the secrecy outage probability which is defined as the probability that the secrecy capacity is less than a certain target rate, can be expressed as

$$\begin{aligned}P_{Sout,m} &= \mathbb{P}\{C_m < R_m\}\\ &= \int_0^\infty F_{\gamma_m}(\tau_m x + \tau_m - 1) f_{\gamma_{nm}^{eve}}(x)dx \qquad (8)\end{aligned}$$

where $\tau_m = 2^{R_m}$, and R_m is the target rate at user m, $F_X(.)$ is the cumulative distribution function (CDF) of the random variable X, and $f_X(.)$ its probability density function (PDF). Hence, in order to calculate the secrecy outage probability, the CDF of γ_m, and the PDF of γ_{nm}^{eve} are needed.

The CDF of the SINR at weak user m can be expressed as

$$\begin{aligned}F_{\gamma_m}(x) &= \mathbb{P}\{\gamma_m \le x\}\\ &= \mathbb{P}\left\{\|\mathbf{h}_m\|^2 \le \frac{x}{\beta a_m}(a_n\|\mathbf{h}_m\frac{\mathbf{h}_n^\dagger}{\|\mathbf{h}_n\|}\|^2 + \frac{1}{\rho})\right\}\\ &= \int_0^\infty F_X\left(\frac{x}{\beta a_m}(a_n y + \frac{1}{\rho})\right) f_Y(y)dy \qquad (9)\end{aligned}$$

where $X = \|\mathbf{h}_m\|^2$ obeys Gamma distribution $Gamma(N, 1)$ and $Y = \|\mathbf{h}_m\frac{\mathbf{h}_n^\dagger}{\|\mathbf{h}_n\|}\|^2$ follows the exponential distribution with unit mean. Hence, the CDF of γ_m can be expressed as

$$\begin{aligned}&F_{\gamma_m}(x)\\ &= 1 - \int_0^\infty \sum_{i=0}^{N-1} \frac{x^i}{i!}(\frac{a_n}{\beta a_m}y + \frac{1}{\beta a_m \rho})^i e^{-(\frac{a_n x}{\beta a_m}y + \frac{x}{\beta a_m \rho})} e^{-y}dy\\ &= 1 - \sum_{i=0}^{N-1}\sum_{j=0}^{i} \frac{1}{i!}\binom{i}{j}(\frac{a_n}{\beta a_m})^j(\frac{1}{\beta a_m \rho})^{i-j} x^i e^{-(\frac{x}{\beta a_m \rho})}\\ &\int_0^\infty y^j e^{-(\frac{a_n x}{\beta a_m})y} e^{-y}dy\\ &= 1 - \Phi \frac{x^i}{(1 + \frac{a_n}{\beta a_m}x)^{j+1}} \exp(-\frac{x}{\beta a_m \rho}) \qquad (10)\end{aligned}$$

where $\Phi = \sum_{i=0}^{N-1}\sum_{j=0}^{i} \frac{1}{(i-j)!}(\frac{a_n}{\beta a_m})^j(\frac{1}{\beta a_m \rho})^{i-j}$.

In order to calculate the PDF of γ_{nm}, we will derive its CDF first, then the PDF can be obtained by the deriving the CDF formula. The CDF of γ_{nm} can be expressed as

$$\begin{aligned}F_{\gamma_{nm}^{eve}}(x) &= \mathbb{P}\{\gamma_{nm} \le x\}\\ &= \mathbb{P}\left\{\frac{\beta a_m\|\mathbf{h}_n\frac{\mathbf{h}_m^\dagger}{\|\mathbf{h}_m\|}\|^2}{a_n\|\mathbf{h}_n\|^2 + \frac{(1-\beta)a_m}{N-1}\|\mathbf{h}_n\mathbf{V}_m\|^2 + \frac{1}{\rho}} \le x\right\}\\ &= \mathbb{P}\left\{Z \le \frac{x}{\beta a_m}(I + \frac{1}{\rho})\right\} \qquad (11)\end{aligned}$$

where $Z = \|\mathbf{h}_n\frac{\mathbf{h}_m^\dagger}{\|\mathbf{h}_m\|}\|^2$ follows the exponential distribution with unit mean, and $I = a_n\|\mathbf{h}_n\|^2 + \frac{(1-\beta)a_m}{N-1}\|\mathbf{h}_n\mathbf{V}_m\|^2$, $\|\mathbf{h}_n\|^2$ obeys the Gamma distribution i.e., $\sim Gamma(N, 1)$, then $a_n\|\mathbf{h}_n\|^2 \sim Gamma(N, a_n)$. The elements of $\mathbf{h}_n\mathbf{V}_m$ are random independent Gaussian distributed with zero mean and unit variance then the distribution of $\|\mathbf{h}_n\mathbf{V}_m\|^2$ is $Gamma(N-1, 1)$, and $\frac{(1-\beta)a_m}{N-1}\|\mathbf{h}_n\mathbf{V}_m\|^2 \sim Gamma(N-1, \frac{(1-\beta)a_m}{N-1})$. The sum of two Integer Gamma functions follows the generalized integer Gamma distribution [26], with PDF equals to

$$f_I(z) = \theta_0\left(\theta_1\frac{z^{k-1}}{(k-1)!}e^{-a_n z} + \theta_2\frac{z^{k-1}}{(k-1)!}e^{-\frac{N-1}{(1-\beta)a_m}z}\right) \qquad (12)$$

where $\theta_1 = (-1)^{N-1}\sum_{k=1}^{N} a_{N-k+1,N-1}(\frac{1}{a_n} - \frac{N-1}{(1-\beta)a_m})^{k-(2N-1)}$, $\theta_2 = (-1)^N \sum_{k=1}^{N-1} a_{N-k,N}(\frac{N-1}{(1-\beta)a_m} - \frac{1}{a_n})^{k-(2N-1)}$, $\theta_0 = (\frac{1}{a_n})^N(\frac{N-1}{(1-\beta)a_m})^{N-1}$, and $a_{N-k+1,N-1} = \binom{2N-k-2}{N-2}$, $a_{N-k,N} = \binom{2N-k-2}{N-1}$.

Then the CDF of γ_{nm} is given by

$$\begin{aligned}&F_{\gamma_{nm}^{eve}}(x)\\ &= 1 - e^{-\frac{x}{\beta a_m \rho}}\int_0^\infty e^{-\frac{x}{\beta a_m}z} f_I(z)dz\\ &= 1 - e^{-\frac{x}{\beta a_m \rho}}\theta_0\left[\frac{\theta_1}{(\frac{x}{\beta a_m} + \frac{1}{a_n})^k} + \frac{\theta_2}{(\frac{x}{\beta a_m} + \frac{N-1}{(1-\beta)a_m})^k}\right]. \qquad (13)\end{aligned}$$

By the derivation of $F_{\gamma_{nm}^{eve}}(x)$ we have

$$\begin{aligned}f_{\gamma_{nm}^{eve}}(x) = \frac{\theta_0}{\beta a_m \rho}e^{-\frac{x}{\beta a_m \rho}}\Bigg[&\frac{\theta_1}{(\frac{x}{\beta a_m} + \frac{1}{a_n})^k} + \frac{\theta_2}{(\frac{x}{\beta a_m} + \frac{N-1}{(1-\beta)a_m})^k}\\ &+ \frac{\rho\theta_1 k}{(\frac{x}{\beta a_m} + \frac{1}{a_n})^{k+1}} + \frac{\rho\theta_2 k}{(\frac{x}{\beta a_m} + \frac{N-1}{(1-\beta)a_m})^{k+1}}\Bigg]. \qquad (14)\end{aligned}$$

Theorem 1: Assuming NOMA downlink system, where AS is generated at the base station to impair the strong user capability of decoding the weak user m's information messages, then the secrecy outage probability of the weak user can be expressed as

$$P_{Sout,m} = 1 - \Omega \qquad (15)$$

where

$$\begin{aligned}\Omega = &\frac{\theta_0}{\beta a_m \rho}\exp\left(-\frac{(\tau_m - 1)}{\beta a_m \rho}\right)\Phi\,\Xi(\frac{\beta a_m}{a_n \tau_m})^{j+1}\Gamma(t+1)\\ &\Bigg[\theta_1(\beta a_m)^k\frac{(-1)^{j+k+1}}{\Gamma(k)\Gamma(j+1)}\partial_b^j\partial_{c_1}^{k-1}\\ &\quad\left(\frac{1}{c_1 - b}\left[b^t e^{ba}\Gamma(-t, ba) - c_1^t e^{ac_1}\Gamma(-t, c_1 a)\right]\right)\\ &\quad + \rho\theta_1\, k(\beta a_m)^{k+1}\frac{(-1)^{j+k+2}}{\Gamma(k+1)\Gamma(j+1)}\partial_b^j\partial_{c_1}^{k}\\ &\quad\left(\frac{1}{c_1 - b}\left[b^t e^{ba}\Gamma(-t, ba) - c_1^t e^{ac_1}\Gamma(-t, c_1 a)\right]\right)\\ &\quad + \theta_2(\beta a_m)^k\frac{(-1)^{j+k+1}}{\Gamma(k)\Gamma(j+1)}\partial_b^j\partial_{c_2}^{k-1}\\ &\quad\left(\frac{1}{c_2 - b}\left[b^t e^{ba}\Gamma(-t, ba) - c_2^t e^{ac_2}\Gamma(-t, c_2 a)\right]\right)\\ &\quad + \rho\theta_2\, k(\beta a_m)^{k+1}\frac{(-1)^{j+k+2}}{\Gamma(k+1)\Gamma(j+1)}\partial_b^j\partial_{c_2}^{k}\\ &\quad\left(\frac{1}{c_2 - b}\left[b^t e^{ba}\Gamma(-t, ba) - c_2^t e^{ac_2}\Gamma(-t, c_2 a)\right]\right)\Bigg]\end{aligned}$$

with $a = \frac{\tau_m+1}{\beta a_m \rho}$, $b = \frac{\beta a_m}{\tau_m a_n} + 1 - \frac{1}{\tau_m}$, $c_1 = \frac{\beta a_m}{a_n}$, $c_2 = \frac{\beta(N-1)}{(1-\beta)}$, ∂_x^j *is the partial derivative of the order* j *with respect to* x, $\Xi = \sum_{t=0}^{i} \binom{i}{t} \tau_m^t (\tau_m - 1)^{i-t}$ *and* $\Gamma(.,.)$ *is the upper incomplete gamma function.*

Proof: The secrecy outage probability of user m is given by

$$\begin{aligned} P_{Sout,m} &= \int_0^\infty F_{\gamma_m}(\tau_m x + \tau_m - 1) f_{\gamma_{nm}^{eve}}(x) dx \\ &= 1 - \Phi \underbrace{\int_0^\infty \frac{e^{-\frac{(\tau_m x + \tau_m - 1)}{\beta a_m \rho}} (\tau_m x + \tau_m - 1)^i}{\left(1 + \frac{a_n}{\beta a_m}(\tau_m x + \tau_m - 1)\right)^{j+1}} f_{\gamma_{nm}^{eve}}(x) dx}_{\Omega} . \end{aligned} \tag{16}$$

By applying (14) and some further manipulations, the term Ω can be expressed as

$$\begin{aligned} \Omega = {} & \frac{\theta_0}{\beta a_m \rho} \int_0^\infty \frac{\exp(-\frac{(\tau_m x + \tau_m - 1)}{\beta a_m \rho})(\tau_m x + \tau_m - 1)^i}{\left(1 + \frac{a_n}{\beta a_m}(\tau_m x + \tau_m - 1)\right)^{j+1}} \\ & \exp(-\frac{x}{\beta a_m \rho}) \Bigg[\frac{\theta_1}{(\frac{x}{\beta a_m} + \frac{1}{a_n})^k} + \frac{\theta_2}{(\frac{x}{\beta a_m} + \frac{N-1}{(1-\beta) a_m})^k} \\ & + \frac{\rho \theta_1 k}{(\frac{x}{\beta a_m} + \frac{1}{a_n})^{k+1}} + \frac{\rho \theta_2 k}{(\frac{x}{\beta a_m} + \frac{N-1}{(1-\beta) a_m})^{k+1}} \Bigg] dx \\ = {} & \frac{\theta_0}{\beta a_m \rho} \exp\left(- \frac{(\tau_m - 1)}{\beta a_m \rho} \right) (\frac{\beta a_m}{a_n \tau_m})^{j+1} \\ & \times \sum_{t=0}^{i} \binom{i}{t} \tau_m^t (\tau_m - 1)^{i-t} \\ & \int_0^\infty \frac{e^{-\frac{\tau_m + 1}{\beta a_m \rho} x} x^t}{(\frac{\beta a_m}{\tau_m a_n} + 1 - \frac{1}{\tau_m} + x)^{j+1}} \Bigg[\frac{\theta_1 (\beta a_m)^k}{\left(x + \frac{\beta a_m}{a_n}\right)^k} + \frac{\rho \theta_1 (\beta a_m)^{(k+1)}}{\left(x + \frac{\beta a_m}{a_n}\right)^{(k+1)}} \\ & + \frac{\theta_2 (\beta a_m)^k}{\left(x + \frac{\beta(N-1)}{(1-\beta)}\right)^k} + \frac{\rho \theta_2 (\beta a_m)^{(k+1)}}{\left(x + \frac{\beta(N-1)}{(1-\beta)}\right)^{(k+1)}} \Bigg] dx \\ = {} & \frac{\theta_0}{\beta a_m \rho} \exp\left(- \frac{(\tau_m - 1)}{\beta a_m \rho} \right) \Xi (\frac{\beta a_m}{a_n \tau_m})^{j+1} \int_0^\infty \frac{e^{-ax} x^t}{(b+x)^{j+1}} \\ & \Bigg[\frac{\theta_1 (\beta a_m)^k}{(x + c_1)^k} + \frac{\rho \theta_1 (\beta a_m)^{(k+1)}}{(x + c_1)^{(k+1)}} + \frac{\theta_2 (\beta a_m)^k}{(x + c_2)^k} + \frac{\rho \theta_2 (\beta a_m)^{(k+1)}}{(x + c_2)^{(k+1)}} \Bigg] dx. \end{aligned} \tag{17}$$

We have

$$\begin{aligned} & \int_0^\infty \frac{e^{-ax} x^t}{(x + b)^{j+1} (x + c)^k} \\ & = \frac{(-1)^{j+k+1}}{\Gamma(k)\Gamma(j+1)} \partial_b^j \partial_c^{k-1} \left(\frac{1}{c-b} \int_0^\infty \left[\frac{e^{-ax} x^t}{x + b} - \frac{e^{-ax} x^t}{x + c} \right] \right) dx \\ & = \frac{(-1)^{j+k+1}}{\Gamma(k)\Gamma(j+1)} \partial_b^j \partial_c^{k-1} \\ & \left(\frac{1}{c-b} \left[b^t e^{ba} \Gamma(t+1) \Gamma(-t, ba) - c^t e^{ca} \Gamma(t+1) \Gamma(-t, ca) \right] \right). \end{aligned}$$

By substituting in (17), (15) can be obtained. The proof is completed. ■

III. GAME-THEORETICAL APPROACH

In this section, the proposed wiretap model is formulated as non-cooperative two players zero-sum game. Wherein the utility function is considered as the secrecy capacity between the both users. Non-cooperative zero-sum game is the natural model as the weak user tries to maximize the utility function to secure his information and the strong user attempts to minimize it.

A. NON-COOPERATIVE STRATEGIC GAMES

Strategic non-cooperative games involve competitive decision-makers having either partially or totally conflicting interests in the utility outcome function. More formally, a non-cooperative game in strategic form is defined as follows [18]:

Definition 1: The strategic non-cooperative game is a triplet $\mathcal{G} = (\mathcal{N}_p, (\mathcal{S}_i)_{i \in \mathcal{N}_p}, (u_i)_{i \in \mathcal{N}_p})$ where:

- $\mathcal{N}_p$ is the set of players, i.e., $\mathcal{N}_p = \{1, \ldots, N_p\}$.
- $(\mathcal{S}_i)$ is the available strategies for player i, $\forall i \in \mathcal{N}_P$.
- u_i is the utility function of the i, $\forall i \in \mathcal{N}_P$.

Two-player zero-sum game is one of most common models of non-cooperative games. It involves two players with the same utility function but with completely opposite interests, where the gain of one player equals to the loss of the second player. In other words, in two-player zero-sum game one player is trying to maximize the utility function whereas the other attempts to minimize it. Zero-sum game is the natural game model for secure communication system games, as the legitimate user is trying to improve the secrecy performance of the system under the malicious user attempts to reduce it.

The most common solution for the majority of non-cooperative game models is that of NE [18]. NE is first introduced by John Nash in his seminal work [17], can be defined as the state where no player can enhance its utility outcome by choosing another strategy, if the other players maintain the NE strategies. NE can be defined as follows [27]:

Definition 2: We say that the strategy profile $s^* \in \mathcal{S}$ where $\mathcal{S} = \mathcal{S}_1 \times \ldots \mathcal{S}_i \times \ldots \mathcal{S}_{N_p}$ is a Nash equilibrium of a non-cooperative game $\mathcal{G} = (\mathcal{N}_p, (\mathcal{S}_i)_{i \in \mathcal{N}_p}, (u_i)_{i \in \mathcal{N}_p})$ if

$$u_i(s_i^*, s_{-i}^*) \geq u_i(s_i, s_{-i}^*), \quad \forall i \in \mathcal{N}_p, \ \forall s_i \in \mathcal{S}_i \tag{18}$$

where $\mathcal{S}_{-i}$ denotes the available strategies for all players except the player i.

B. GAME FORMULATION

In the proposed secure NOMA model, the weak user can choose between transmitting with total power or splitting this power to deploy the AS scheme to enhance the secrecy performance. The strong user chooses whether to eavesdrop with higher power and extra decoding process or not to eavesdrop in order to maintain his power to perform his functionalities. To express both players energy-security trade-offs we will formulate the proposed secure NOMA zero-sum game $\mathcal{G} = (\mathcal{N}_p, (\mathcal{S}_i)_{i \in \mathcal{N}_p}, (u_i)_{i \in \mathcal{N}_p})$ as follows:

TABLE 2. Utility function matrix of the secure NOMA zero-sum game.

User n / User m	Eavesdrop ($\mathcal{E}$)	Not eavesdrop ($\mathcal{N}$)
Total Power ($\mathcal{T}$)	$C_{\mathcal{TE}}$	$C_{\mathcal{TN}}$
Artificial signal ($\mathcal{A}$)	$C_{\mathcal{AE}}$	$C_{\mathcal{AN}}$

- $\mathcal{N}_p = 1, 2$ is the set of weak and strong players.
- $(\mathcal{S} = \mathcal{S}_m \times \mathcal{S}_n)$ denotes the compact strategic action space for both players, where $\mathcal{S}_m$, $\mathcal{S}_n$ are the available strategies for the weak and strong players respectively. User m asks the base station to transmit with 'Total power' allocated without considering the potential threat of the strong user, this strategy will be denoted by $\mathcal{T}$, or to deploy the 'AS' scheme and protect his information-bearing signal by dividing the total power between information-bearing and artificial signals with ratio β, we denote this strategy as $\mathcal{A}$. Hence, the available strategies set for the weak player can be expressed as $\mathcal{S}_m = \{\mathcal{T}, \mathcal{A}\}$. Strong user can choose between two strategies, either to push more power and 'Eavesdrop' the weak user message at higher SINR ratios denoted by $\mathcal{E}$. Or the 'Not eavesdrop' strategy to maintain the available power for his own functionalities denoted by $\mathcal{N}$. Therefore, the strategic space of the strong user is expressed as $\mathcal{S}_m = \{\mathcal{E}, \mathcal{N}\}$.
- The utility function of the proposed game is the instantaneous secrecy rate defined by the difference between the weak user n rate and the rate of decoding his message by the strong user n, i.e., $C = [\log_2(1+\gamma_m) - \log_2(1+\gamma_{nm})]^+$.

Based on the game formulation, we can build the utility matrix for the proposed secure NOMA zero-sum game as following table,

In the utility matrix, for the (Eavesdrop, Total power) combination, the weak user is not protecting his information-bearing signal and the strong user is trying to intercept it. In this case the strong user will manage to decode the weak user message and intercept it easily therefore the secrecy capacity is zero, i.e.,

$$C_{\mathcal{TE}} = 0. \tag{19}$$

In the (Not eavesdrop, Total power) combination, the weak user uses all available power for transmitting his information-bearing signal. As the strong user plays 'Not eavesdrop', the eavesdropping rate is zero, i.e., $\log_2(1+\gamma_{nm}) = 0$, and the utility function for this combination can be written as

$$C_{\mathcal{TN}} = \log_2(1 + \frac{a_m\|\mathbf{h}_m\|^2}{a_n\|\mathbf{h}_m\frac{\mathbf{h}_n^\dagger}{\|\mathbf{h}_n\|}\|^2 + \frac{1}{\rho}}). \tag{20}$$

For the combination (Eavesdrop, Artificial signal), the weak users asks the base station to implement the AS scheme and the strong user tries to intercept the weak user by extracting it from the AS mixture. Hence, the utility function can be expressed as

$$C_{\mathcal{AE}} = \Bigg[\log_2(1 + \frac{\beta a_m\|\mathbf{h}_m\|^2}{a_n\|\mathbf{h}_m\frac{\mathbf{h}_n^\dagger}{\|\mathbf{h}_n\|}\|^2 + \frac{1}{\rho}}) - \log_2(1 + \frac{\beta a_m\|\mathbf{h}_n\frac{\mathbf{h}_m^\dagger}{\|\mathbf{h}_m\|}\|^2}{a_n\|\mathbf{h}_n\|^2 + \frac{(1-\beta)a_m}{N-1}\|\mathbf{h}_n\mathbf{V}_m\|^2 + \frac{1}{\rho}})\Bigg]^+. \tag{21}$$

For the (Not eavesdrop, Artificial signal) case, the weak user is protecting his information message using the AS technique while the strong user is not trying to intercept it, and hence the utility function corresponding to this case can be given by

$$C_{\mathcal{AN}} = \log_2(1 + \frac{\beta a_m\|\mathbf{h}_m\|^2}{a_n\|\mathbf{h}_m\frac{\mathbf{h}_n^\dagger}{\|\mathbf{h}_n\|}\|^2 + \frac{1}{\rho}}). \tag{22}$$

C. EXISTENCE OF NASH EQUILIBRIA

In this subsection, we prove that an NE exists for the proposed NOMA secrecy non-cooperative zero-sum gain. To this end, we apply the following Nash equilibria existence theorem [16].

Theorem 2: A strategic game $\mathcal{G} = (\mathcal{N}_p, (\mathcal{S}_i)_{i\in\mathcal{N}_p}, (u_i)_{i\in\mathcal{N}_p})$ has at least one NE if the action set $(\mathcal{S}_i)\forall i \in \mathcal{N}_p$ is non empty, compact and convex subset of a Euclidean space.

Proof: By definition, the strategy set for each player $(\mathcal{S}_m)$ and $(\mathcal{S}_n)$ is not empty and convex. Each user's strategy is limited between 'Total power' and 'AS' for user m, and 'Eavesdrop' or 'Not eavesdrop' for user n. Hence, the strategy sets are bounded and thus compact. Therefore, the proposed secrecy NOMA zero-sum gain has at least one NE. The proof is completed. ■

D. PURE-STRATEGY NASH EQUILIBRIA

In this subsection, we analyses the pure-strategy Nash equilibria that the players can reach when moving without considering the other player's strategy. Pure-strategy is a deterministic strategy selection from the strategies space (with probability equals to one) by a given player. The pure-strategy NE and its corresponding strategies for the proposed secure NOMA two-player sum-game are provided by the following theorem:

Theorem 3: For the proposed NOMA zero-sum game model and for an arbitrary transmit powers, arbitrary channel status conditions and arbitrary eavesdropping power and information to AS power ratio, the pure-strategy NE profile is given by

$$C(s_m^*, s_n^*) = C_{\mathcal{AE}}. \tag{23}$$

Proof: The definition of the utility function and its possible values presented in the utility matrix in Table 2 imply the following instantaneous secrecy capacity outcomes order

$$C_{\mathcal{TN}} \geq C_{\mathcal{AN}} \geq \underbrace{C_{\mathcal{AE}}}_{NE} \geq C_{\mathcal{TE}}. \tag{24}$$

$C_{\mathcal{AE}}$ represents the NE profile, since neither the strong nor weak user can enhance his utility function by changing his strategy individually, i.e., the instantaneous secrecy capacity utility will increase if the strong user moves to 'Not eavesdrop' strategy instead of 'Eavesdrop' as the utility function will change to $C_{\mathcal{AN}}$ that has higher utility function value. Similarly, the utility function value will decrease if the weak user changes his strategy from 'AS' to 'Total power' as the utility function profile will be $C_{\mathcal{TE}}$ that has worse utility function values. The proof is completed. ■

Hence, the NE strategies are 'AS' and 'Eavesdrop' for users m and n respectively.

E. MIXED-STRATEGY EQUILIBRIA

In order to tackle the probabilistic nature of the zero-sum game model, the concept of mixed-strategy is proposed. Mixed-strategy considers the number of the available strategies and the probabilities corresponding to choosing each strategy for a given player. The proposed non-cooperative zero-sum game model is finite (as the sets of strategies $\mathcal{S}_n$ and $\mathcal{S}_m$ are finite), then it has a saddle-point in the mixed-strategy mode [17].

Let us define $\mathbf{p} = (p, 1-p)$, where $0 \leq p \leq 1$ is the probability with which the weak user m plays the 'Total transmit' strategy. Hence, $1-p$ is the probability with which it plays the 'AS' strategy. Similarly, we define $\mathbf{q} = (q, 1-q)$, where $0 \leq q \leq 1$ is the probability that the strong user plays the 'Eavesdrop' strategy and so $1-q$ is the probability to play 'Not eavesdrop' strategy.

The weak user reaches his optimal action by solving the following problem

$$\max_{p} \min_{q} \mathbf{p}^T \mathbf{C}\mathbf{q} \tag{25}$$

where $\mathbf{C}$ is the instantaneous secrecy capacity matrix represented in Table 2, and $(.)^T$ is the transpose function.

The strong user obtains his optimal move by solving

$$\min_{q} \max_{p} \mathbf{p}^T \mathbf{C}\mathbf{q}. \tag{26}$$

Solving the above equations yields the optimal probability value of each strategy for a given user

$$p^* = \frac{C_{\mathcal{AN}} - C_{\mathcal{AE}}}{C_{\mathcal{TE}} + C_{\mathcal{AN}} - (C_{\mathcal{TN}} + C_{\mathcal{AE}})} \tag{27}$$

$$1-p^* = \frac{C_{\mathcal{TE}} - C_{\mathcal{TN}}}{C_{\mathcal{TE}} + C_{\mathcal{AN}} - (C_{\mathcal{TN}} + C_{\mathcal{AE}})} \tag{28}$$

$$q^* = \frac{C_{\mathcal{AN}} - C_{\mathcal{TN}}}{C_{\mathcal{TE}} + C_{\mathcal{AN}} - (C_{\mathcal{TN}} + C_{\mathcal{AE}})} \tag{29}$$

$$1-q^* = \frac{C_{\mathcal{TE}} - C_{\mathcal{AE}}}{C_{\mathcal{TE}} + C_{\mathcal{AN}} - (C_{\mathcal{TN}} + C_{\mathcal{AE}})} \tag{30}$$

and hence the unique corresponding mixed-strategy NE value u^* of the proposed game is given by

$$u^*(p^*, q^*) = \frac{C_{\mathcal{TE}}C_{\mathcal{AN}} - C_{\mathcal{TN}}C_{\mathcal{AE}}}{C_{\mathcal{TE}} + C_{\mathcal{AN}} - (C_{\mathcal{TN}} + C_{\mathcal{AE}})}. \tag{31}$$

IV. NUMERICAL RESULTS

In this section, numerical simulations are provided to validate the analytical results and to demonstrate the impact of system parameters on the secrecy performance. The representative results in the considered network are drawn according to the following NOMA power allocation coefficient $a_n = 0.2$ $a_m = 0.8$ for weak and strong user respectively. The users' locations in the network are assumed to follow the uniform distribution. Channel model is Rayleigh fading with the path loss model $128.1 + 37.6 * \log(r)$ dB, where $r[Km]$ is the distance between the base station and the user terminal. Total transmit power is 43 dBm, receivers' noise density -169 dBm.

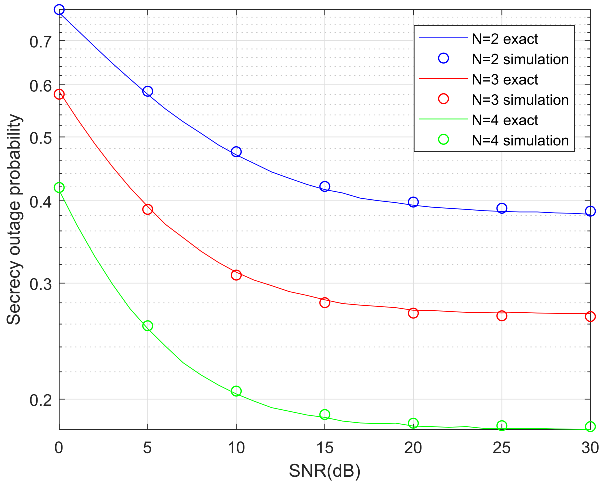

FIGURE 1. Secrecy outage probability versus SNR for $N = 2, 3, 4$ at $\beta = 0.8$.

The curves shown in Figure 1 represent the analytic outage secrecy probability of the weak user (solid line) and the Monte Carlo simulations (circle dots) as a function of transmit SNR for different numbers of antenna. The match between the analytical and the simulated results validates our derived closed-form expressions of the secrecy outage probability.

Figure 2 plots the secrecy outage probability versus antenna number for different values of information to artificial signals power ratio β. One can notice that increasing the number of transmit antenna N improves the secrecy behaviour of the proposed system. This is due to the fact that the higher the number of antennas the better the quality of the information signal received by the weak receiver, as the random variable $\mathbf{h}_m$ follow the Gamma distribution with N parameter, i.e., $\Gamma(N, 1)$. Moreover, increasing the antenna number creates more confusion to the strong user when trying to intercept the weak user message, in addition to impairing its eavesdropping SINR (γ_{nm}^{eve}).

In Figure 3, the secrecy outage probability is drawn with respect to information-bearing signal to AS power coefficient β, for different number of antenna. $\beta = 1$ means that all power is allocated to the information-bearing signal and

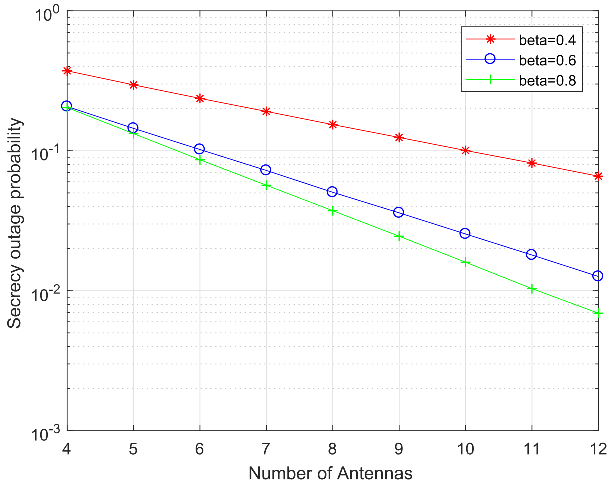

FIGURE 2. Secrecy outage probability versus number of antennas for $\beta = 0.4, 0.6, 0.8$ at $\rho = 43dBm$.

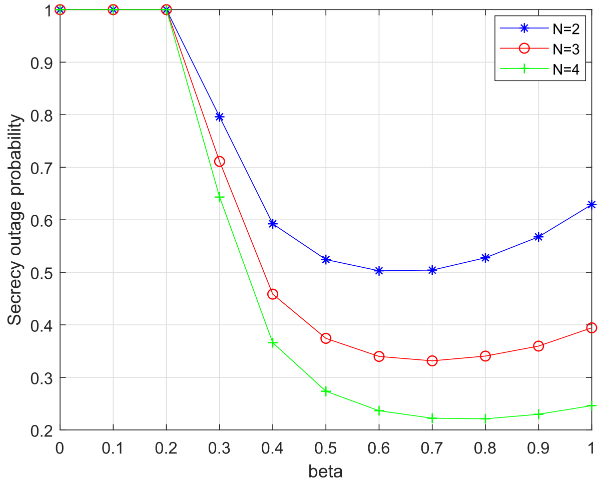

FIGURE 3. Secrecy outage probability versus β for $N = 2, 3, 4$ at $\rho = 43dBm$.

no artificial signal is injected (conventional NOMA system). While $\beta = 0$ implies that all power is assigned to the artificial signal and no information exchange. The figure demonstrates that the secrecy outage probability reaches its lowest value at $\beta \neq 1$ which proves that physical layer security is enhanced when AS is injected. Of course, not all values of β is available as its value has to satisfy $\beta * a_m > a_n$ so NOMA system can be implemented.

Figure 4 plots the capacity region for conventional NOMA, conventional OMA, the AS-Aided NOMA and the AS-Aided OMA systems. The comparisons yield that the boundary of achievable rate pairs of the proposed AS-Aided NOMA is still outside the AS-Aided OMA capacity region. Therefore, the proposed secure NOMA system guards the superiority of NOMA system over the OMA system in terms of system-level throughput. Moreover, the capacity region of the proposed AS-Aided NOMA scheme is even larger than that of the conventional OMA system ($\beta = 1$) in general.

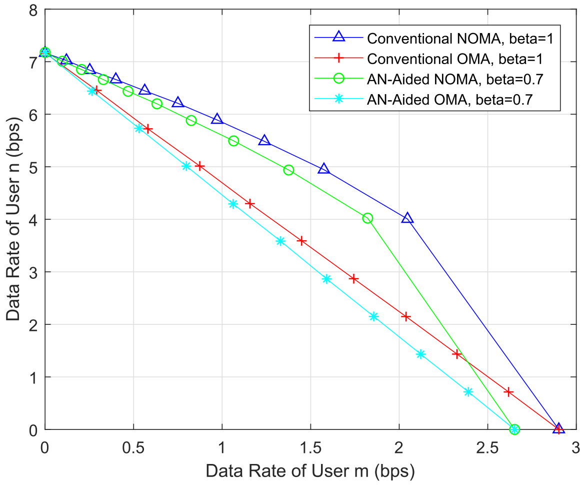

FIGURE 4. Capacity Regions of NOMA and OMA systems for $\beta = 0.7, 1$.

Hence, the proposed AS-Aided scheme enhances the security aspect of the NOMA system without compromising its performance.

The curves drawn in Figure 5 represent the zero-sum game utility functions with the pure and mixed NE values as a function of the transmit SNR. At low SNR regime the strong user can eavesdrop the weak user's information message and the pure-strategy NE is not optimal. Hence, it is better that both users randomize over the possible strategies to reach the mixed-strategy NE which obviously better than the pure NE $(C_{\mathcal{AE}})$ at this region. At the point that SNR is high enough and the eavesdropping power is not sufficient to extract the weak user's information-bearing signal from the AS combination, the pure-strategy NE $C_{\mathcal{AE}}$ provides better utility outcomes and users have to switch to their pure deterministic strategies. i.e., weak user chooses the 'AS' strategy and the strong user plays the 'Eavesdrop' strategy.

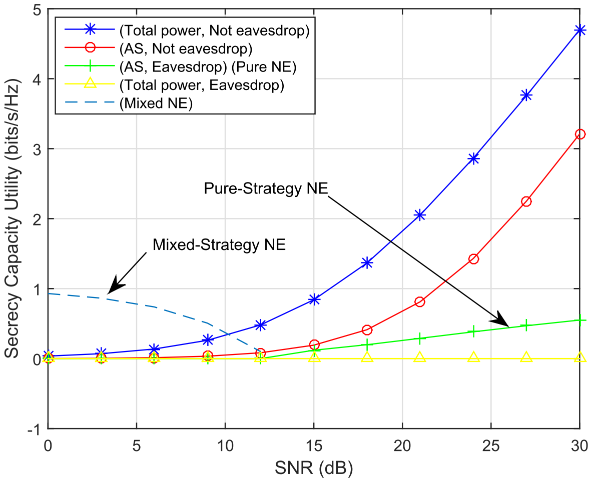

FIGURE 5. Non-cooperative NOMA zero-sum game utility functions.

Figures 6 plots the optimal mixed-strategy probabilities as a function of transmit SNR. In the region where the strong

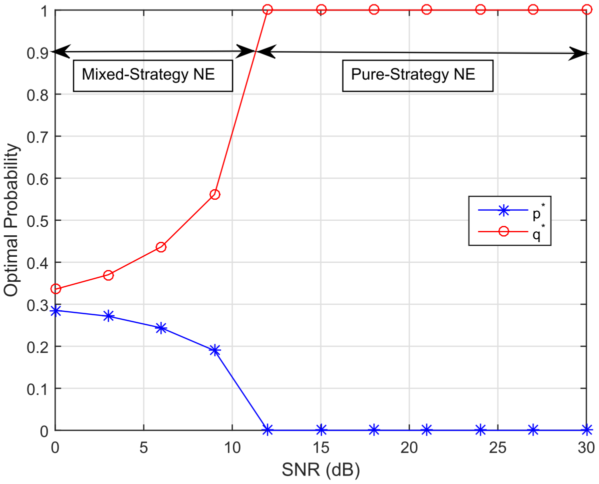

FIGURE 6. **Optimal weak and strong users mixed-strategy probabilities.**

user's eavesdropping power is sufficient to intercept the weak user's message, users should adopt the mixed-strategy NE (mixed-strategy region). Once the power is high enough and hence the power allocated to the AS is sufficient to prevent the strong user of eavesdropping, the mixed-strategy is not optimal anymore and users have to use the deterministic strategies (pure-strategy region). $p^* = 0$ implies that weak user should play the 'AS' strategy and $q^* = 1$ implies that strong user should play the 'Eavesdrop' strategy which lead to the pure-strategy NE profile.

V. CONCLUSION

This paper exploits physical layer security in downlink NOMA system, to impair the strong user capability of decoding the weak user's information. To this end, the weak user's information-bearing signal is merged with an artificial signal. The interactions between the legitimate and malicious user are modeled as strategic non-cooperative two-player zero-sum game. The weak user is trying to maximize the secrecy rate while the strong user attempts to minimize it. A non-cooperative NE profile is obtained in pure and mixed-strategy scenarios. The secrecy outage probability of the weak user is provided in closed-form expression. Furthermore, numerical results demonstrate that injecting AS technique enhances information security, without compromising the NOMA superiority over OMA systems. The proposed AS-aided secure scheme can be extended as a future work, to imperfect or partial CSI scenarios by introducing robust secure schemes and algorithms.

REFERENCES

[1] A. Benjebbovu, A. Li, Y. Saito, Y. Kishiyama, A. Harada, and T. Nakamura, "System-level performance of downlink NOMA for future LTE enhancements," in *Proc. Globecom Workshops (GC Wkshps)*, Dec. 2013, pp. 66–70.

[2] Z. Ding, M. Peng, and H. V. Poor, "Cooperative non-orthogonal multiple access in 5G systems," *IEEE Commun. Lett.*, vol. 19, no. 8, pp. 1462–1465, Aug. 2015.

[3] Y. Saito, Y. Kishiyama, A. Benjebbour, T. Nakamura, A. Li, and K. Higuchi, "Non-orthogonal multiple access (NOMA) for cellular future radio access," in *Proc. IEEE 77th Veh. Technol. Conf.*, Jun. 2013, pp. 1–5.

[4] Z. Yang, Z. Ding, Y. Wu, and P. Fan, "Novel relay selection strategies for cooperative NOMA," *IEEE Trans. Veh. Technol.*, vol. 66, no. 11, pp. 10114–10123, Nov. 2017.

[5] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.

[6] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.

[7] J. Xiong, K.-K. Wong, D. Ma, and J. Wei, "A closed-form power allocation for minimizing secrecy outage probability for MISO wiretap channels via masked beamforming," *IEEE Commun. Lett.*, vol. 16, no. 9, pp. 1496–1499, Sep. 2012.

[8] 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.

[9] N. Li, X. Tao, H. Wu, J. Xu, and Q. Cui, "Large-system analysis of artificial-noise-assisted communication in the multiuser downlink: Ergodic secrecy sum rate and optimal power allocation," *IEEE Trans. Veh. Technol.*, vol. 65, no. 9, pp. 7036–7050, Sep. 2016.

[10] H. Lei *et al.*, "On secure NOMA systems with transmit antenna selection schemes," *IEEE Access*, vol. 5, pp. 17450–17464, 2017.

[11] Y. Zhang, H.-M. Wang, Q. Yang, and Z. Ding, "Secrecy sum rate maximization in non-orthogonal multiple access," *IEEE Commun. Lett.*, vol. 20, no. 5, pp. 930–933, May 2016.

[12] Z. Qin, Y. Liu, Z. Ding, Y. Gao, and M. Elkashlan, "Physical layer security for 5G non-orthogonal multiple access in large-scale networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2016, pp. 1–6.

[13] Y. Liu, Z. Qin, M. Elkashlan, Y. Gao, and L. Hanzo, "Enhancing the physical layer security of non-orthogonal multiple access in large-scale networks," *IEEE Trans. Wireless Commun.*, vol. 16, no. 3, pp. 1656–1672, Mar. 2017.

[14] Y. Li, M. Jiang, Q. Zhang, Q. Li, and J. Qin, "Secure beamforming in downlink MISO nonorthogonal multiple access systems," *IEEE Trans. Veh. Technol.*, vol. 66, no. 8, pp. 7563–7567, Aug. 2017.

[15] M. Kaosar and X. Yi, "Privacy preserving data gathering in wireless sensor network," in *Wireless Technologies: Concepts, Methodologies, Tools and Applications*. Hershey, PA, USA: IGI Global, 2012, pp. 239–253.

[16] D. Fudenberg and J. Tirole, *Game Theory*. Cambridge, MA, USA: MIT Press, 1991.

[17] J. F. Nash, Jr., "Equilibrium points in n-person games," *Proc. Nat. Acad. Sci. USA*, vol. 36, no. 1, pp. 48–49, 1950.

[18] Z. Han, D. Niyato, W. Saad, T. Başar, and A. Hjørungnes, *Game Theory in Wireless and Communication Networks: Theory, Models, and Applications*. Cambridge, U.K.: Cambridge Univ. Press, 2012.

[19] Z. Wang, L. Jiang, and C. He, "Optimal price-based power control algorithm in cognitive radio networks," *IEEE Trans. Wireless Commun.*, vol. 13, no. 11, pp. 5909–5920, Nov. 2014.

[20] E. G. Larsson and E. A. Jorswieck, "Competition versus cooperation on the MISO interference channel," *IEEE J. Sel. Areas Commun.*, vol. 26, no. 7, pp. 1059–1069, Sep. 2008.

[21] X. Kang, R. Zhang, and M. Motani, "Price-based resource allocation for spectrum-sharing femtocell networks: A Stackelberg game approach," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 3, pp. 538–549, Apr. 2012.

[22] X. Liang and Y. Xiao, "Game theory for network security," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 1, pp. 472–486, 1st Quart., 2013.

[23] A. Al-Talabani, Y. Deng, A. Nallanathan, and H. X. Nguyen, "Enhancing secrecy rate in cognitive radio networks via multilevel Stackelberg game," *IEEE Commun. Lett.*, vol. 20, no. 6, pp. 1112–1115, Jun. 2016.

[24] A. Mukherjee and A. L. Swindlehurst, "Jamming games in the MIMO wiretap channel with an active eavesdropper," *IEEE Trans. Signal Process.*, vol. 61, no. 1, pp. 82–91, Jan. 2013.

[25] M. Yuksel, X. Liu, and E. Erkip, "A secure communication game with a relay helping the eavesdropper," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 818–830, Sep. 2011.

[26] C. A. Coelho, "The generalized integer gamma distribution—A basis for distributions in multivariate statistics," *J. Multivariate Anal.*, vol. 64, no. 1, pp. 86–102, 1998.

[27] T. Basar and G. J. Olsder, *Dynamic Noncooperative Game Theory*, vol. 23. Philadelphia, PA, USA: SIAM, 1999.

YAMEN ALSABA received the B.Eng. degree in electrical and telecommunication engineering from the Higher Institute of Applied Science and Technology, Damascus, Syria, in 2005, and the M.S. degree from Supelec, Paris, France, in 2010. He is currently pursuing the Ph.D. degree with the Wireless Communication Centre, Universiti Teknologi Malaysia (UTM), Johor Bahru, Malaysia. His research interests include simultaneous wireless information and power transfer, non-orthogonal multiple access, beamforming, physical layer security, large-scale wireless network analysis, game theory, and 5G communication systems.

CHEE YEN LEOW (S'08–M'12) received the B.Eng. degree in computer engineering from Universiti Teknologi Malaysia (UTM), Malaysia, and the Ph.D. degree from Imperial College London, U.K., in 2007 and 2011, respectively. He is currently a Senior Lecturer with the School of Electrical Engineering, Faculty of Engineering, UTM, where he is also a Research Fellow with the Wireless Communication Centre, Higher Institution Centre of Excellence, and the UTM-Ericsson Innovation Centre for 5G. His research interests include cooperative communication, MIMO, UAV communication, physical layer security, convex optimization, communications theory, wireless power transfer, millimeter wave communication, and non-orthogonal multiple access, for 5G and IoT applications.

SHARUL KAMAL ABDUL RAHIM received the degree in electrical engineering from the University of Tennessee, USA, in 1996, the M.Sc. degree in engineering (communication engineering) from Universiti Teknologi Malaysia (UTM) in 2001, and the Ph.D. degree in wireless communication system from the University of Birmingham, U.K., in 2007. He is currently an Associate Professor with the Wireless Communication Centre, Faculty of Electrical Engineering, UTM Skudai. His research interest is smart antenna on communication system. He is also a member of the IEEE Malaysia Section, the Member Board of Engineer Malaysia, the Member of Institute of Engineer Malaysia (MIEM), and the Eta Kappa Nu Chapter (International Electrical Engineering Honour Society, University of Tennessee). He has published over 50 journal papers and technical proceedings on rain attenuations, smart antenna system, microwave design, and reconfigurable antenna in national and international journals and conferences.