IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received November 1, 2018, accepted November 14, 2018, date of publication January 2, 2019,
date of current version January 16, 2019.

Digital Object Identifier 10.1109/ACCESS.2018.2889494

A Game-Theoretical Modelling Approach for Enhancing the Physical Layer Security of Non-Orthogonal Multiple Access System

YAMEN ALSABA, (Student Member, IEEE), CHEE YEN LEOW, (Member, IEEE), AND SHARUL KAMAL ABDUL RAHIM, (Senior Member, IEEE)
Wireless Communication Centre, Faculty of Engineering, School of Electrical Engineering, Universiti Teknologi Malaysia, Johor Bahru 81310, Malaysia
Corresponding author: Chee Yen Leow (bruceleow@utm.my)

This work was supported in part by H2020-MSCA-RISE-2015 under Grant 690750 and Grant 4C094, and in part by Universiti Teknologi Malaysia under Grant 19H58, Grant 04G37, Grant 17H23, and Grant 13H08.

ABSTRACT This paper investigates the physical layer security of a downlink non-orthogonal multiple access (NOMA) communication system, wherein a base station is communicating with two paired active users in the presence of an eavesdropper and multiple idle nodes (helpers). In order to enhance the secrecy performance, a two-phase harvest-and-jam null-steering jamming technique is deployed. In the first phase, the base station provides the helper with power in addition to active users and eavesdropper's information via simultaneous wireless information and power transfer technique. The helpers exploit the harvested energy and the information received in the first phase to build a null-steering beamformer and jam the eavesdropper, during the information exchange between the base station and the legitimate users in the second phase. A game theory is introduced to the proposed scheme, and the base station-helpers interactions are modeled as a Stackelberg game, where the helpers play the leader role and the base station is the follower. The utility functions of both the leader and follower are formed, and the Stackelberg equilibrium is reached by means of the backward induction technique. The proposed scheme demonstrates better secrecy performance when compared with the artificial noise-aided secure NOMA system.

INDEX TERMS Non-orthogonal multiple access, physical layer security, game theory, Stackelberg game, null-steering beamforming, harvest-and-jam.

I. INTRODUCTION

The anticipated functionalities of the future communication systems pose new challenging requirements such as low latency, massive connectivity and high spectral efficiency [1]. Being an answer for the fifth generation (5G) communication system's essentials, non-orthogonal multiple access (NOMA) has been recognised as the potential multiple access scheme for the future 5G systems [2]. Unlike previous multiple access schemes that utilize time, frequency or code domains to serve multiple users, NOMA exploits power domain to access different users according to their channel condition. NOMA users are allocated with power levels inversely proportional to their channel gain, hence NOMA strong user (user with good channel condition) is allocated with lower power level than that of the weak user (user with poor channel condition) [3]. In order to deploy downlink NOMA system, two major techniques are involved namely superposition-coding at the base station and successive interference cancellation (SIC) at the strong user terminal. NOMA strong user decodes the weak user message firstly, then subtracts from the superimposed base station message by means of SIC to decode his own. While being allocated with higher level, NOMA weak user decodes his message directly by considering the strong user information-bearing signal as interference [4].

However, information secrecy is expected to be compromised in the future 5G communication due to the wide coverage area and the enormous number of users served. Hence, security measure should be taken to protect the information messages [5]. One of the most vulnerable information safeguarding strategy is the physical layer (PHY) security. PHY security exploits the imperfect physical qualities of the communication such noise and interference to boost the security performance of the communication scheme. PHY security has been widely utilized in wireless communication systems in favour of the pioneering work of Wyner [6]. By introducing the concept of wire-tap channel,

Wyner proved that secrecy capacity is always positive if the eavesdropper channel is worse than that of the legitimate users. Hence, most of the PHY security enhancing schemes focus on impairing the eavesdropper channel condition by different techniques such as artificial noise (AN) and jamming. In the AN approach, a noise signal is broadcast in the legitimate user's orthogonal subspace, thus only the eavesdropper will be affected by the transmitted noise [7]. Jamming techniques [8] refer to transmitting a noise signal whether by the base station itself [9], or with the aid of external nodes (helpers) [10] in order to mitigate the malicious node abilities of intercepting the legitimate users' information messages. Cooperative helpers scheme is compromised by the limited energy at the wireless communication network as users are selfish and prefer to keep the available energy for their own functionalities. Thus, as an incentive for the helpers to collaborate in transmitting the jamming signal, the base station provides them with power wirelessly, this technique is referred to as harvest-and-jam (HJ) [11]. One of the adopted techniques for building the jamming beamforming vector is the null-steering scheme, where the jamming signal is directed towards the malicious node while being nulled in the legitimate users' directions, hence only the eavesdropper channel will be degraded [12]. Furthermore, null-steering is proved as the optimal beamforming scheme for maximizing the secrecy rate in wireless networks in [13].

Enhancing the PHY security of NOMA communication systems has gained a lot of attention recently. Zhang *et al.* [14] maximize the secrecy rate in a downlink NOMA system, where a base is communicating with multiple trusted users with the existence of an active eavesdropper. While the secrecy outage probability is derived in [15] for NOMA communication system under different base station antenna-selection schemes. NOMA internal or legitimate eavesdropper case has been considered in [16], where the base station is communicating with two NOMA users under the malicious attempt of the weak user to intercept the strong user information-bearing signal. Secure large-scale NOMA communication system is considered in [17] and [18], and the PHY security is enhanced by means of protected zone and AN respectively. In the AN-aided secure NOMA system proposed in [18], a base station is communicating with paired NOMA user in the presence of an eavesdropper. To impair the eavesdropper capabilities of intercepting the legitimate users' data, two AN signals are transmitted in the orthogonal subspace of each user. The eavesdropper will suffer from both users' AN signals while each legitimate user will suffer from the other user's AN signal yielding to better secrecy performance. However, broadcasting the AN signal in one legitimate user's orthogonal subspace will affect both the eavesdropper and the other user channels, resulting in incorrect SIC execution and faulty information decoding at the strong user terminal and degraded signal-to-interference-and-noise ratio (SINR) at the weak receiver. Hence, other jamming techniques are needed to be investigated in NOMA communication systems, wherein only the eavesdropper is affected by the jamming signal.

Game theory [19] is a mathematical discipline used to model, analyse and study the possible interactions among various rational decision makers referred to as players that have potentially conflicting goals. The framework is first developed to model competition among companies in the field of economics. Recently, game theory has been applied to wireless networks especially to address the problem of distributed resource allocation [20]–[22]. Game theory is introduced to NOMA in [23] and [24], where power allocation problem in NOMA system using game theoretical approach is investigated. In [25], game theory has been introduced to PHY security in cognitive radio network, where a Stackelberg game model is adopted to increase the secrecy rate. The authors in [26] investigate wireless powered communication network (WPCN)-based secure communication scheme consisting of multiple power beacons powering the transmitter in the first phase, to guarantee secure communication with the legitimate users in the second phase. The interactions among the power beacons and the information transmitter are modelled as Stackelberg game. The transmitter plays the leader role while the power beacons are considered as the follower. The Stackelberg equilibrium of the proposed game is derived and provided in closed-form expressions. Secure device-to-device (D2D) communication is addressed in [27], where a hybrid base station powers the transmitter in the first phase. During the D2D device communication in the second phase, the base station jams the eavesdroppers existed in the network. A Stackelberg game is formulated in the corresponding scenario, wherein the transmitter plays the leader role who buys energy from the base station that plays the follower role. The work in [27] is extended in [28] to study the reversed role between the base station and the transmitter, in addition to investigating the social welfare problem and solving it optimally. Fang *et al.* [29] investigate the PHY security of multiple relays, single source and single destination network with the presence of multiple eavesdroppers. Stackelberg model is adopted to model the source and the relays behaviour and the corresponding optimal price allocation algorithm is presented. The model in [29] is extended in [30] to active full-duplex eavesdropper that is capable of both intercepting and jamming. A three-stage Stackelberg game is exploited to model the users' interactions, encourage the cooperation and protect the data from the active eavesdropper attacks. Game theory is introduced to enhance the PHY security in NOMA systems in [31], where a zero-sum game has been adopted to protect the information message of the weak user from being intercepted by the strong user.

In this work, the PHY security of downlink NOMA system is enhanced by means of the two-phase harvest-and-jam technique. In the first phase, the base station provides the helpers with power and the channel state information (CSI) of both eavesdropper and legitimate users via the simultaneous wireless information and power transfer (SWIPT) scheme. The helpers deploy power splitting scheme to divide the

signal received between information decoding and energy harvesting processes. In the second phase, the helpers exploit the information and the harvested energy to build a null-steering beamformer, to direct the jamming signal towards the eavesdropper while being suppressed in the legitimate users' directions, during the base station communication with the intended users. In order to enhance the secrecy performance and the economic revenues, a game-theoretical approach is introduced to the proposed model. The complex interactions between the base station and the helpers are modelled as a Stackelberg game, where the helpers play the leader role who buys energy from the base station that plays the follower role to enhance the secrecy rate of the system. The utility functions at both leader and follower levels are formulated and the Stackelberg equilibrium is achieved by means of the backward induction technique, so both players maintain their equilibrium reaching strategies to guarantee the system stability. This work exploits null-steering jamming and game theory techniques for enhancing the PHY security of NOMA system. The proposed game-theoretical null-steering jamming illustrates better secrecy performance than that of the AN-aided secure NOMA system proposed in [18], in addition to enhancing the base station's economical revenues.

II. SYSTEM MODEL

We consider secure downlink NOMA system, wherein a base station equipped with N antenna is communicating with two active users under the malicious attempts of an external eavesdropper of intercepting the legitimate users information with the existence of L helper. All nodes are equipped with a single antenna and the channel represents Rayleigh fading channel multiplied by the free path loss. The total transmission time T is divided into power and CSI information exchange with the helpers in the first phase of time τT, and information exchange phase $(1-\tau)T$, where $0 \leq \tau \leq 1$. The base station divides the total available power P_T between the two phases with ratio θ, $0 \leq \theta \leq 1$, where if $\theta = 0$ all power is used to information exchange with active users, and $\theta = 1$ means that all power is used to transmit information and power to the helpers and no information is sent to the active users in the second phase.

We assume that the eavesdropper is an active node which communicates with the base station for his own services. Thus, the eavesdropper CSI is assumed to be available at the base station which is a basic assumption in the literature on PHY security [32]. In addition, we consider that the eavesdropper is capable of detecting multi-user data and hence can differentiate the messages of the intended users easily [14]. Eavesdropper's strong decoding capability assumption overestimates the eavesdropper decoding abilities, so our results represent lower bounds of the practical ones. The proposed system model is illustrated in Figure 1.

A. PHASE ONE: WIRELESS INFORMATION AND POWER TRANSFER

In this phase, the base station transmits the information needed by the helper to build the beamforming scheme in addition to wireless power to be used in transmitting the jamming signal. The signal received at the helper number i can be written as

$$y_i = \sqrt{\theta P_T}\mathbf{h}_i\mathbf{s}_h + n_i, \quad i = 1, 2, \ldots, L, \tag{1}$$

where $\mathbf{s}_h$ represents the information-bearing signal with $\mathcal{E}(\|\mathbf{s}_h\|^2) = 1$, $\mathbf{h}_i$ is the complex channel gain between the base station and the helper number i and n_i is the additive white Gaussian noise (AWGN) signal at the helper i.

The helper nodes deploy power splitting strategy to divide the power of the received signal into information-decoding and energy harvesting processes with ratio ρ_i $(0 \leq \rho_i \leq 1)$. If $\rho = 1$ all power is used for energy harvesting process, while if $\rho = 0$ then all power is used for the information decoding process. In order that the helper i is capable of performing the information decoding successfully the ratio ρ_i should be equal to

$$\rho_i = \max\left\{0, 1 - \frac{(2^{R_i/\tau} - 1)\sigma_i^2}{\theta P_T \|\mathbf{h}_i\|^2}\right\}, \quad i = 1, 2, \ldots, L, \tag{2}$$

where R_i is the target rate for the helper i, $i = 1, 2, \ldots, L$ to decode the base station information message. As can be seen from Eq. 2 higher data rate implies that power splitting ratio will be higher. Hence, more power portion will be allocated to information decoding process and less to the harvesting energy circuits in the power splitting receiver. The lower levels of harvested energy lead to less jamming signal power and degraded secrecy capacity and performance.

The harvested energy at the helper i can be written as

$$E_i = P_T\theta T\tau\eta_i\rho_i\|\mathbf{h}_i\|^2, \quad i = 1, \ldots, L, \tag{3}$$

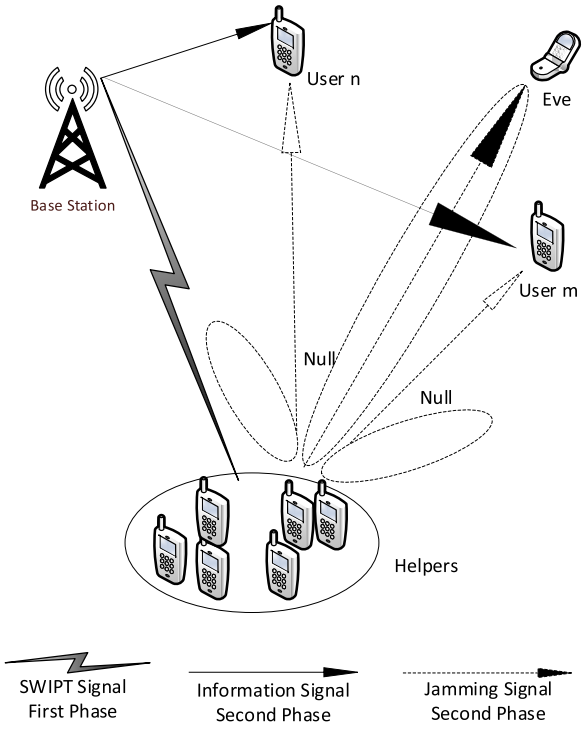

FIGURE 1. The proposed harvest-and-jam null-steering jamming NOMA system.

where η_i is the energy conversion efficiency at the helper i, without loss of generality we will assume that $\eta_i = 1$, $\forall i = 1, .., L$. Hence, the harvested power during the first phase at the helper number i is given by

$$P_{hi} = P_T \theta \rho_i \|\mathbf{h}_i\|^2. \tag{4}$$

And the maximum jamming power of the ith helper in the second phase can be presented as

$$P_i = P_T \theta \tfrac{\tau}{1-\tau} \rho_i \|\mathbf{h}_i\|^2. \tag{5}$$

The harvested energy of the noise signal is considered small and hence ignored ([33], [34]).

The helpers exploit the CSI information to build the null-steering precoder to direct the jamming signal towards the eavesdropper, while being nulled in the active users' directions. The transmit null-steering beamformer at the helpers side in the second phase is written in the following form

$$\mathbf{w}_e = \frac{(\mathbf{I}_L - \mathbf{G})\mathbf{g}_e}{\|(\mathbf{I}_L - \mathbf{G})\mathbf{g}_e\|}, \tag{6}$$

where $\mathbf{I}_L$ is the $L * L$ identity matrix, $\mathbf{G} \triangleq \mathbf{B}(\mathbf{B}^H\mathbf{B})^{-1}\mathbf{B}^H$ is $L * L$ orthogonal projection matrix onto the subspace spanned by the columns of $\mathbf{B}$, with $\mathbf{B} \triangleq [\mathbf{g}_n \ \ \mathbf{g}_m]$, and $g_n = [g_{1n}, g_{2n}, \dots \ \ g_{Ln}]$, $g_m = [g_{1m}, g_{2m}, \dots \ \ g_{Lm}]$ and $g_e = [g_{1e}, g_{2e}, \dots \ \ g_{Le}]$ represent the complex channel between the set of the helpers and the legitimate users n, m and the eavesdropper respectively.

B. PHASE 2: INFORMATION AND JAMMING SIGNALS TRANSMISSION

In the second phase, the base station transmits the legitimate users information, while the helpers are jamming the eavesdropper using the information and the power received at the first phase. The base station implements maximum ratio transmission (MRT) to transmit the intended users information messages, and hence the NOMA superimposed base station message can be expressed as

$$x = \sqrt{(1-\theta)P_T a_n}\mathbf{w}_n s_n + \sqrt{(1-\theta)P_T a_m}\mathbf{w}_m s_m, \tag{7}$$

where a_n and a_m represents NOMA power allocation ratio with $a_n < a_m$ (user n is considered as the strong user) and $a_n + a_m = 1$, s_n and s_m are the information-bearing of users n and m respectively, with $\mathcal{E}(|\ s_n\ |^2) = \mathcal{E}(|\ s_m\ |^2) = 1$, $\mathbf{w}_n, \mathbf{w}_m$ are the MRT beamforming vector for user n and m respectively given by $\mathbf{w}_k = \frac{\mathbf{h}_k^\dagger}{\|\mathbf{h}_k\|}$, $k = n, m$, where $\mathbf{h}_k$ represents channel between the base station and user k.

The signal received at the user n in the second phase can written in the form

$$y_n = \sqrt{P_T(1-\theta)a_n}\mathbf{h}_n\mathbf{w}_n s_n + \sqrt{P_T(1-\theta)a_m}\mathbf{h}_n\mathbf{w}_m s_m + z_n, \tag{8}$$

where z_n is the AWGN signal the user n terminal with zero mean and σ^2 variance. The strong user decodes the weak user's information message and suppresses it by mean of SIC, hence the SINR at the strong user n can be expressed as

$$\begin{aligned}\gamma_n &= P_T(1-\theta)a_n\|\mathbf{h}_n\|^2/\sigma^2 \\ &= \gamma\ (1-\theta)a_n\|\mathbf{h}_n\|^2,\end{aligned} \tag{9}$$

where $\gamma = P_T/\sigma^2$ the total signal to noise ratio (SNR).

Similarly, the signal received by the user m can be written on the following form

$$\begin{aligned}y_m = \sqrt{P_T(1-\theta)a_m}\mathbf{h}_m\mathbf{w}_m s_m \\ + \sqrt{P_T(1-\theta)a_n}\mathbf{h}_m\mathbf{w}_n s_n + z_m,\end{aligned} \tag{10}$$

where z_m is the AWGN signal the user m terminal with zero mean and σ^2 variance. Hence, the SINR at the weak user terminal is expressed as

$$\begin{aligned}\gamma_m &= \frac{P_T(1-\theta)a_m\|\mathbf{h}_m\|^2}{P_T(1-\theta)a_n\ |\ \mathbf{h}_m\frac{\mathbf{h}_n^\dagger}{\|\mathbf{h}_n\|}\ |^2 + \sigma^2} \\ &= \frac{\gamma\ (1-\theta)a_m\|\mathbf{h}_m\|^2}{\gamma\ (1-\theta)a_n\ |\ \mathbf{h}_m\frac{\mathbf{h}_n^\dagger}{\|\mathbf{h}_n\|}\ |^2 + 1}.\end{aligned} \tag{11}$$

The eavesdropper receives both the base station signals and the helpers jamming signal

$$\begin{aligned}y_e = \sqrt{P_T(1-\theta)a_n}\mathbf{h}_e\mathbf{w}_n s_n + \sqrt{P_T(1-\theta)a_m}\mathbf{h}_e\mathbf{w}_m s_m \\ + \sum_{i=1}^{L}\sqrt{P_i}g_{ie}w_{ie}v + z_e,\end{aligned} \tag{12}$$

where g_{ie} represents the channel between the helper i and the eavesdropper, w_{ie} denotes the component i of the jamming null-steering beamforming vector $\mathbf{w}_e$, v is an artificial Gaussian jamming signal with zero mean and unit variance, P_i is the transmission power of the helper i, and z_e is the AWGN signal the eavesdropper with zero mean and σ^2 variance.

The SINR at the eavesdropper terminal to intercept the user $k, k \in n, m$ messages under the assumption of strong detection capability can be expressed as

$$\gamma_{ek} = \frac{\gamma\ (1-\theta)a_k\ |\ \mathbf{h}_e\frac{\mathbf{h}_k^\dagger}{\|\mathbf{h}_k\|}\ |^2}{\gamma\theta\frac{\tau}{1-\tau}\sum_{i=1}^{L}\rho_i\|\mathbf{h}_i\|^2\|\mathbf{g}\mathbf{w}_e\|^2 + 1}, \quad k \in \{n, m\}. \tag{13}$$

C. THE SECRECY RATE

The secrecy rate is defined as the difference between the legitimate user rate and that of the eavesdropper and expressed as

$$\begin{aligned}\mathcal{C}_k = [(1-\tau)\log_2(1+\gamma_k) - (1-\tau)\log_2(1+\gamma_{ek})]^+, \\ k \in \{n, m\},\end{aligned} \tag{14}$$

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

III. PHYSICAL LAYER SECURITY GAME FORMULATION

In this section, game theory approach is exploited to analyse the PHY security performance of the proposed model. The relation between the base station and the helpers is modelled as a Stackelberg game. In the Stackelberg model, the helpers move first by expressing their willingness to buy wireless power from the base station with an optimal price that maximizes the utility function. The feature of moving first gives the helpers a priority in the game hierarchy and hence considered as the leader of the game. The base station plays the follower role who trades wireless energy with the leader for money in the corresponding game model. We will start by formulating both leader and follower utility function that each player is trying to maximize.

A. LEADER UTILITY FUNCTION

The leader aims to maximize his utility function $\mathcal{U}_{Lk}$ which is formulated as the gain in terms of secrecy rate for the legitimate user $k, k \in \{n, m\}$ minus the price paid for purchasing wireless energy from the follower. Hence, the optimization problem of the leader can be expressed on the following form

$$\begin{aligned} &\underset{\tau,\alpha}{\text{maximize}}\ \mathcal{U}_{Lk}(\theta, \alpha, \tau) = \zeta \mathcal{C}_k - \alpha P_T \theta \sum_{i=1}^{L} \rho_i \|\mathbf{h}_i\|^2, \\ &\qquad k \in \{n, m\}, \\ &\text{subject to } 0 < \tau < 1, \alpha \geq 0. \end{aligned} \tag{15}$$

where ζ is the gain per secrecy capacity unit and α represents the price per harvested energy unit.

B. FOLLOWER UTILITY FUNCTION

The utility function of the base station is modelled as the price of the power sold to the leader minus its production cost. Thus, the follower utility function can be expressed as

$$\begin{aligned} &\underset{\theta}{\text{maximize}}\ \mathcal{U}_{BS}(\theta, \alpha, \tau) = \tau \left(\alpha P_T \theta \sum_{i=1}^{L} \rho_i \|\mathbf{h}_i\|^2 - \mathcal{F}(P_T \theta) \right), \\ &\text{subject to } 0 \leq \theta \leq 1. \end{aligned} \tag{16}$$

where $\mathcal{F}(P_T\theta)$ is a function models the cost of power production per unit at the base station. The power cost function will be modelled as a quadratic form given by [35]

$$\mathcal{F}(P_T\theta) = a(\theta P_T)^2 + b\theta P_T, \tag{17}$$

where $a, b > 0$ are constants.

The Stackelberg equilibrium will be reached to guarantee that none of the players will diverse individually, as moving alone to another strategy rather than the equilibrium strategy will not render any benefits to the player. In Stackelberg game, the leader moves first and chooses his optimal strategies $(\alpha^{opt}, \tau^{opt})$ that maximize its utility function. The follower observes the leader strategy and chooses his best strategy (θ^{opt}) referred to as best response. Stackelberg equilibrium is reached with the help of backward induction by finding the best response of the follower first, and then by maximizing the leader utility function based on the follower best response the optimal stratifies will be found.

C. FOLLOWER LEVEL SOLUTION

The optimal power allocation ratio θ^{opt} by the base station for a given price per energy unit α and time allocation ratio τ will be found first by solving the follower optimization problem. The objective function $\mathcal{U}_{BS}$ is quadratic in terms of θ with linear constraint and hence the optimization problem is convex, and the optimal power allocation ratio θ^{opt} can be obtained by making the first derivatives equals to zero.

$$\begin{aligned} &\frac{\partial \mathcal{U}_{BS}}{\partial \theta} = \tau \left(\alpha P_T \sum_{i=1}^{L} \rho_i \|\mathbf{h}_i\|^2 - 2\, a\theta P_T - b P_T \right) = 0 \\ &\implies \theta^{opt} = \begin{cases} \frac{\alpha \sum_{i=1}^{L} \rho_i \|\mathbf{h}_i\|^2 - b}{2a}, & \text{if } \alpha \sum_{i=1}^{L} \rho_i \|\mathbf{h}_i\|^2 - b > 0, \\ 0, & \text{if } \alpha \sum_{i=1}^{L} \rho_i \|\mathbf{h}_i\|^2 - b \leq 0. \end{cases} \end{aligned} \tag{18}$$

Hence, for a given α and τ values, the follower's best response θ^{opt} is given by

$$\theta^{opt} = \left[\frac{\alpha \sum_{i=1}^{L} \rho_i \|\mathbf{h}_i\|^2 - b}{2a} \right]^{+}. \tag{19}$$

D. LEADER LEVEL SOLUTION

After observing the best response of the follower, the leader will choose his best strategies for the best response θ^{opt}, and hence the optimization problem of the leader can be rewritten as

$$\begin{aligned} &\underset{\tau,\alpha}{\text{maximize}}\ \mathcal{U}_{Lk}(\alpha, \tau, \theta^{opt}) = \zeta [R_k - R_{ek}]^{+} \\ &\qquad - \alpha \theta^{opt} P_T \sum_{i=1}^{L} \rho_i \|\mathbf{h}_i\|^2, \quad k \in \{n, m\}, \\ &\text{subject to } 0 < \tau < 1, \quad \alpha \geq 0. \end{aligned} \tag{20}$$

The optimization problem is NP-hard and the optimal values for both α and τ can not be found in polynomial time, thus a suboptimal two-step alternating optimization approach will be adopted. In the first step, α is fixed in terms of optimization parameter, and the optimal value for τ^{opt} is derived. Then the optimal value α^{opt} is found by performing one-dimensional search over all its possible values for the optimized value τ^{opt}.

The relaxed optimization problem can be expressed as

$$\begin{aligned} &\underset{\tau}{\text{maximize}}\ \mathcal{U}_{Lk}(\alpha, \tau, \theta^{opt}) = \zeta [R_k - R_{ek}]^{+} \\ &\qquad - \alpha \theta^{opt} P_T \sum_{i=1}^{L} \rho_i \|\mathbf{h}_i\|^2, \quad k \in \{n, m\}, \\ &\text{subject to } 0 < \tau < 1. \end{aligned} \tag{21}$$

The optimization function is concave with respect to τ, and the optimal value τ^{opt} by making its first derivative equal zero.

The legitimate user data rate is given by

$$R_k = (1 - \tau) \log_2(1 + \gamma_k) \quad k \in \{n, m\} \tag{22}$$

Similarly, the eavesdropper data rate can be written on the following form

$$R_{ek} = (1-\tau)\log_2(1+\gamma_{ek}) = (1-\tau)\log_2\left(1+\frac{\gamma_{ekk}}{\gamma_j\frac{\tau}{1-\tau}+1}\right) \quad k\in\{n,m\}, \quad (23)$$

where $\gamma_{ekk} = \gamma\ (1-\theta^{opt})a_k \ \left|\ \mathbf{h}_e\frac{\mathbf{h}_k^{\dagger}}{\|\mathbf{h}_k\|}\right|^2$, $\gamma_j = \gamma\theta^{opt}\sum_{i=1}^{L}\rho_i\|\mathbf{h}_i\|^2\|\mathbf{g}\mathbf{w}_e\|^2$ calculated at $\theta^{opt} = \frac{\alpha\sum_{i=1}^{L}\rho_i\|\mathbf{h}_i\|^2-b}{2a}$.

Hence the optimization function can be written on the following form

$$\mathcal{U}_{Lk} = \zeta\ (1-\tau)\left[\log_2(1+\gamma_k)-\log_2\left(1+\frac{\gamma_{ekk}}{\gamma_j\frac{\tau}{1-\tau}+1}\right)\right] - \alpha\theta^{opt}P_T\sum_{i=1}^{L}\rho_i\|\mathbf{h}_i\|^2, \quad k\in\{n,m\} \quad (24)$$

As it is difficult to obtain a closed-formula for the optimal value τ, the optimization function will be approximated with its Taylor's series expansion.

$$\mathcal{U}_{Lk} \approx \zeta\left[\log_2(1+\gamma_k)-\log_2(1+\gamma_{ekk}) + \left(-\frac{\gamma_{ekk}\gamma_j}{1+\gamma_{ekk}}-\log_2(1+\gamma_k)+\log_2(1+\gamma_{ekk})\right)\tau - \frac{\gamma_{ekk}\gamma_j^2(2+\gamma_{ekk})}{2(1+\gamma_{ekk})^2}\tau^2\right] - \alpha\theta^{opt}P_T\sum_{i=1}^{L}\rho_i\|\mathbf{h}_i\|^2, \quad k\in\{n,m\} \quad (25)$$

The second order partial derivative of the optimization function with respect to τ is given by

$$\frac{\partial^2\mathcal{U}_{Lk}}{\partial^2\tau} = -\frac{\gamma_{ekk}\gamma_j^2(2+\gamma_{ekk})}{(1+\gamma_{ekk})^2}, \quad k\in\{n,m\} \quad (26)$$

The second derivative is always negative and hence the optimization function is concave. Therefore, the optimal value can be found be putting the first derivative equal to zero.

The first derivative of optimization function with respect to τ is given by

$$\frac{\partial\mathcal{U}_{LK}}{\partial\tau} = \zeta\left[-\frac{\gamma_{ekk}\gamma_j}{1+\gamma_{ekk}}-\log_2(1+\gamma_k)+\log_2(1+\gamma_{ekk}) - \frac{\gamma_{ekk}\gamma_j^2(2+\gamma_{ekk})}{(1+\gamma_{ekk})^2}\tau\right], \quad k\in\{n,m\} \quad (27)$$

The optimal value for time allocation ratio is given by

$$\tau_k^{opt} = \frac{(1+\gamma_{ekk})((1+\gamma_{ekk})(\log(1+\gamma_{ekk})-\log(1+\gamma_k))-\gamma_{ekk}\gamma_j)}{\zeta\gamma_{ekk}(2+\gamma_{ekk})\gamma_j^2}, \times k\in\{n,m\} \quad (28)$$

Once the optimal time allocation ratios for both users' utility functions are calculated, the corresponding optimal price per energy unit value for each user will be found by performing one-dimensional search over all possible values of α. The helpers will naturally choose to pay the minimum price between the two optimal values α_k^{opt}, $k\in\{n,m\}$, i.e., $\alpha^{opt} = \min(\alpha_m^{opt},\alpha_n^{opt})$ and the corresponding time allocation value τ^{opt}.

The Stackelberg equilibrium profile is hence given by the following strategies $\{\theta^{opt},\alpha^{opt},\tau^{opt}\}$.

IV. NUMERICAL SIMULATIONS

In this section, numerical results are provided to demonstrate the performance evaluation in terms of the secrecy rate in the proposed secure NOMA system. The representative results in the proposed scheme are drawn according to the values shown in Table 1.

TABLE 1. Simulation parameters.

Parameter	Value
Strong user coefficient power	0.2
Weak user coefficient power	0.8
Users locations	uniformly distributed
Total transmission power	46 dBm
Path Loss model	128.1 + 37.6 log(r) dB
Channel model	slow fading Rayleigh channel
Receiver noise density	-169 dBm
Power conversion efficiency factor	1
Secrecy capacity threshold	1 bps

The curves shown in Figure 2 illustrate the secrecy rate versus total transmit power to noise ratio for the proposed null-steering jamming and the AN-aided scheme introduced in [18]. The figure shows that the secrecy rate performance enhances with the SNR, as the increased total power increases the harvested energy at the helpers and the jamming power consequently, in addition to boosting the SINR level at the legitimate users' terminals. The comparisons between null-steering jamming and AN-aided scheme yield that null-steering approach provides better secrecy performance than

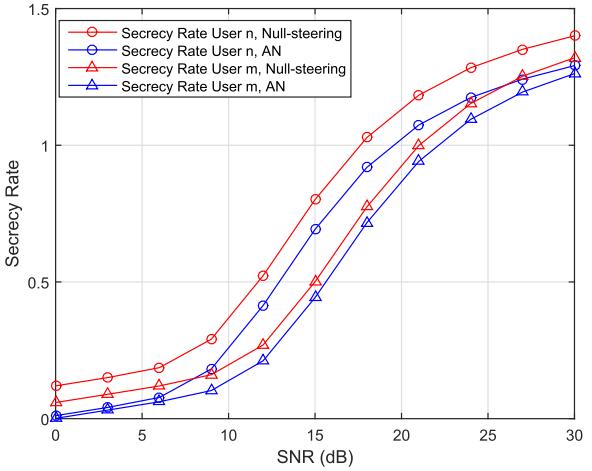

FIGURE 2. Secrecy rate versus transmit SNR.

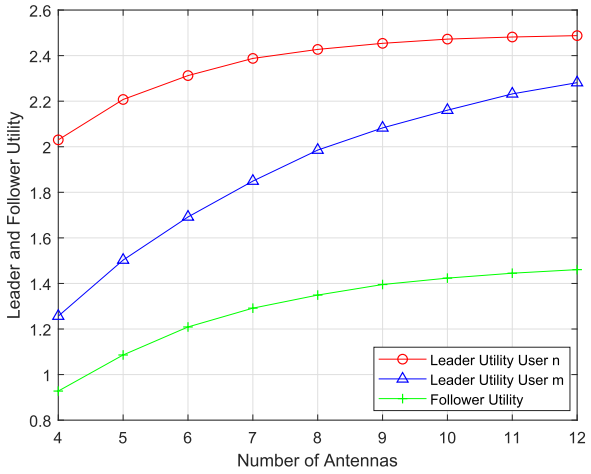

FIGURE 3. Leader and follower utility functions versus number of antennas.

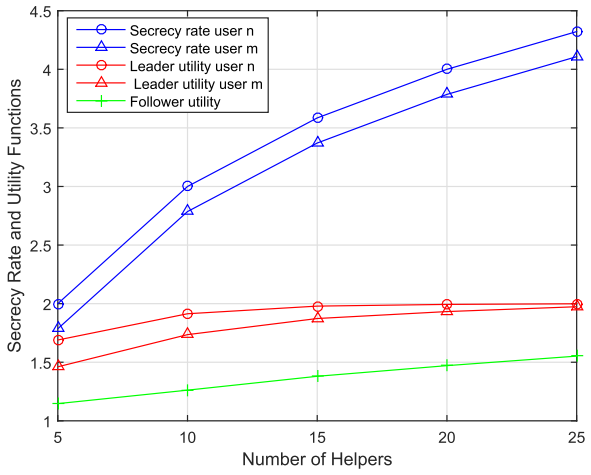

FIGURE 4. Secrecy rate and utility functions versus number of helpers.

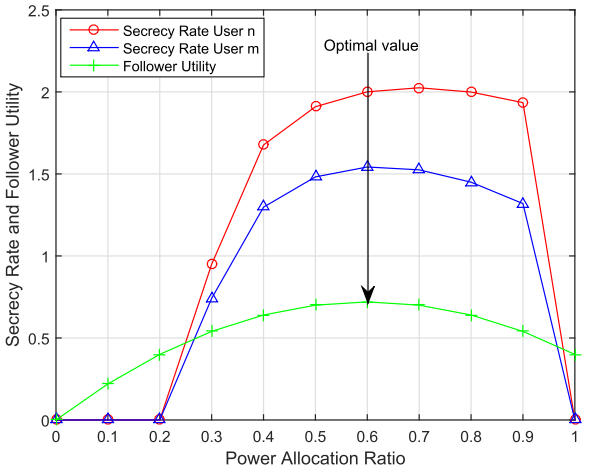

FIGURE 5. Secrecy rate versus power allocation ratio.

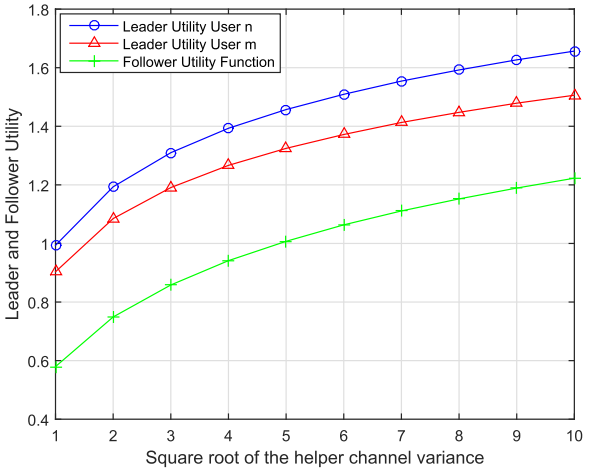

FIGURE 6. Leader utility function versus the square root of the helper channel variance.

that of the AN-aided scheme, since in the AN scheme legitimate users are affected by each other AN signal while in the null-steering only the eavesdropper is prone to the jamming signal. The curves illustrate that the strong user provides better secrecy performance than the weak user, this is due to the assumption made that the eavesdropper has strong decoding abilities and can decode the weak user information message directly while the legitimate weak user treats the strong user information message as interference in order to decode the own.

Figure 3 plots both leader and follower utility functions with respect to the base station number of antenna. Increasing the antennas number enhances the received signal at the intended legitimate users, in addition to the quality of the harvested energy at the helpers and the secrecy rate eventually. Furthermore, increasing the number of transmitting antennas enhances the follower utility function as well, since it leads to an increased level of harvested energy at the helpers and higher economical revenues.

Figure 4 illustrates the secrecy rate, leader utility function, and the follower utility function with respect to the number of helpers. The curves demonstrate that the increased number of helpers in the network enhances the secrecy rate and the leader utility function for both users. This is due to the fact that the increased number of the helpers will increase the power level of the jamming signal, resulting in better secrecy performance and leader utility function as a consequence. In addition, more helpers existed in the network means more buyers, this boosts the economic revenues of the base station as the energy production cost is the same regardless of the number of helpers.

The curves illustrated in Figure 5 draw the secrecy rate and the follower utility function with respect to the power allocation values θ. $\theta = 0$ means that all power is used for information exchange and the helpers are not powered with energy to jam the eavesdropper (“no-helper” scheme). While $\theta = 1$ means that all power is assigned to helpers and no information exchange between the base station and the intended legitimate users. The secrecy rate increases

significantly at the value θ^{opt}, this illustrates that the proposed null-steering jamming scheme does enhance the PHY security of NOMA system when compared to the no-helper scheme ($\theta = 0$). The increased value of the power allocation ratio θ boosts the harvested energy and the jamming signal power level, and hence the secrecy performance of the system.

Figure 6 plots the utility function for both the leader and the follower with respect to helper channel gain $\|h_i\|$. The curves demonstrate that both utility functions increase with the channel gain of the helper. Better helper's channel condition yields higher level of harvested energy resulting in higher jamming levels and better secrecy performance in terms of leader utility function. On the other hand, higher helpers channel gain increased the amount of the harvested energy and its price, leading to better follower function. Hence, it is more efficient to choose nodes with good channel conditions to play the helpers role from both leader and follower perspectives.

V. CONCLUSION

A game-theoretical approach is exploited in this work to model the relation between the base station and helpers in a secure downlink NOMA communication system. In the proposed scheme, the helpers are utilizing the harvested energy of the SWIPT technique to jam the eavesdropper channel and impair its decoding capabilities. Modelled as Stackelberg game, the helpers buy energy from the base station to transmit the jamming signal towards the eavesdropper without affecting the legitimate users' channels by exploiting the null-steering beamforming technique. The optimised null-steering scheme demonstrates a higher secrecy rate than that of the conventional AN-aided NOMA scheme and proved to enhance the economic revenue of the system.

REFERENCES

[1] Y. Liu, Z. Qin, M. Elkashlan, Z. Ding, A. Nallanathan, and L. Hanzo, "Nonorthogonal multiple access for 5G and beyond," *Proc. IEEE*, vol. 105, no. 12, pp. 2347–2381, Dec. 2017.

[2] Y. Alsaba, C. Y. Leow, and S. K. A. Rahim, "Full-duplex cooperative non-orthogonal multiple access with beamforming and energy harvesting," *IEEE Access*, vol. 6, pp. 19726–19738, 2018.

[3] A. Benjebbour, A. Li, Y. Kishiyama, H. Jiang, and T. Nakamura, "System-level performance of downlink NOMA combined with SU-MIMO for future LTE enhancements," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Dec. 2013, pp. 706–710.

[4] Y. Saito, A. Benjebbour, Y. Kishiyama, and T. Nakamura, "System-level performance evaluation of downlink non-orthogonal multiple access (NOMA)," in *Proc. IEEE 24th Annu. Int. Symp. Pers., Indoor, Mobile Radio Commun. (PIMRC)*, Sep. 2013, pp. 611–615.

[5] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Di Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20–27, Apr. 2015.

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

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

[8] Y. Huo, Y. Tian, L. Ma, X. Cheng, and T. Jing, "Jamming strategies for physical layer security," *IEEE Wireless Commun.*, vol. 25, no. 1, pp. 148–153, Feb. 2017.

[9] P.-H. Lin, S.-H. Lai, S.-C. Lin, and H.-J. Su, "On secrecy rate of the generalized artificial-noise assisted secure beamforming for wiretap channels," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1728–1740, Sep. 2013.

[10] W. Liu, X. Zhou, S. Durrani, and P. Popovski, "Secure communication with a wireless-powered friendly jammer," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 401–415, Jan. 2016.

[11] H. Xing, K.-K. Wong, Z. Chu, and A. Nallanathan "To harvest and jam: A paradigm of self-sustaining friendly jammers for secure AF relaying," *IEEE Trans. Signal Process.*, vol. 63, no. 24, pp. 6616–6631, Dec. 2015.

[12] B. Friedlander and B. Porat, "Performance analysis of a null-steering algorithm based on direction-of-arrival estimation," *IEEE Trans. Acoust., Speech Signal Process.*, vol. 37, no. 4, pp. 461–466, Apr. 1989.

[13] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[14] 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.

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

[16] 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.

[17] 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.

[18] 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.

[19] D. Fudenberg and J. Tirole, *Game Theory*. Cambridge, MA, USA: MIT Press, 1991, p. 86.

[20] 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.

[21] 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.

[22] 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.

[23] C. Li, Q. Zhang, Q. Li, and J. Qin, "Price-based power allocation for non-orthogonal multiple access systems," *IEEE Wireless Commun. Lett.*, vol. 5, no. 6, pp. 664–667, Dec. 2016.

[24] W. Xu, X. Li, C.-H. Lee, M. Pan, and Z. Feng, "Joint sensing duration adaptation, user matching, and power allocation for cognitive OFDM-NOMA systems," *IEEE Trans. Wireless Commun.*, vol. 17, no. 2, pp. 1269–1282, Feb. 2018.

[25] 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.

[26] Z. Chu, H. X. Nguyen, and G. Caire, "Game theory-based resource allocation for secure WPCN multiantenna multicasting systems," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 4, pp. 926–939, Apr. 2018.

[27] Z. Chu *et al.*, "Game theory based secure wireless powered D2D communications with cooperative jamming," in *Proc. Wireless Days*, Mar. 2017, pp. 95–98.

[28] Z. Chu, H. X. Nguyen, T. A. Le, M. Karamanoglu, E. Ever, and A. Yazici, "Secure wireless powered and cooperative jamming D2D communications," *IEEE Trans. Green Commun. Netw.*, vol. 2, no. 1, pp. 1–13, Mar. 2018.

[29] H. Fang, L. Xu, and X. Wang, "Coordinated multiple-relays based physical-layer security improvement: A single-leader multiple-followers Stackelberg game scheme," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 1, pp. 197–209, Jan. 2018.

[30] H. Fang, L. Xu, Y. Zou, X. Wang, and K.-K. R. Choo, "Three-stage Stackelberg game for defending against full-duplex active eavesdropping attacks in cooperative communication," *IEEE Trans. Veh. Technol.*, vol. 67, no. 11, pp. 10788–10799, Nov. 2018.

[31] Y. Alsaba, C. Y. Leow, and S. K. A. Rahim, "A zero-sum game approach for non-orthogonal multiple access systems: Legitimate eavesdropper case," *IEEE Access*, vol. 6, pp. 58764–58773, 2018.

[32] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[33] G. Pan, H. Lei, Y. Yuan, and Z. Ding, "Performance analysis and optimization for SWIPT wireless sensor networks," *IEEE Trans. Commun.*, vol. 65, no. 5, pp. 2291–2302, May 2017.
[34] X. Zhou, R. Zhang, and C. K. Ho, "Wireless information and power transfer: Architecture design and rate-energy tradeoff," *IEEE Trans. Commun.*, vol. 61, no. 11, pp. 4754–4767, Nov. 2013.
[35] A.-H. Mohsenian-Rad, V. W. S. Wong, J. Jatskevich, R. Schober, and A. Leon-Garcia, "Autonomous demand-side management based on game-theoretic energy consumption scheduling for the future smart grid," *IEEE Trans. Smart Grid*, vol. 1, no. 3, pp. 320–331, Dec. 2010.

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 Supélec, Paris, France, in 2010. He is currently pursuing the Ph.D. degree with the Wireless Communication Centre, Universiti Teknologi Malaysia, 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, in 2007, and the Ph.D. degree from Imperial College London, U.K., in 2011. He is currently an Associate Professor with the School of Electrical Engineering, Faculty of Engineering, UTM. He is also a Research Fellow with the Wireless Communication Centre, Higher Institution Centre of Excellence, UTM, and with 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, non-orthogonal multiple access, and so on, for 5G and the 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), Skudai, in 2001, and the Ph.D. degree in wireless communication system from the University of Birmingham, U.K., in 2007. He is currently an Professor with the Wireless Communication Centre, Faculty of Electrical Engineering, UTM. He has published over 50 journal papers and technical proceedings on rain attenuations, smart antenna systems, microwave design, and reconfigurable antenna in national and international journals and conferences. His research interest is smart antenna on communication systems. He is a member of the IEEE Malaysia Section, a member of the Board of Engineer Malaysia, and a member of the Institute of Engineer Malaysia and the Eta Kappa Nu Chapter (International Electrical Engineering Honour Society, University of Tennessee).