A Secure Multiuser Privacy Technique for Wireless IoT Networks Using Stochastic Privacy Optimization

Joseph Henry Anajemba, *Member, IEEE*, Tang Yue, *Member, IEEE*, Celestine Iwendi, *Senior Member, IEEE*, Pushpita Chatterjee, *Member, IEEE*, Desire Ngabo, and Waleed S. Alnumay

***Abstract*—With the exponential increase of interconnected communicating devices which make up the Internet of Things (IoT), securing the network transmission and the fifth generation (5G) systems which is the bedrock for IoT concept actualization is becoming more and more challenging. One of the major attacks which poses a great risk to data transmission is the eavesdropper (Eve) attack which occurs in both single input, single output (SISO), multiple input and multiple output (MIMO) systems. Thus, in this study, our focus is to establish a secured connection in a multiple-antenna transmission when the channel state information (CSI) of Eve is unknown to the network users. Our model comprises a secure wireless communication standard where Eve performs either optimal matched filtering (OMF) or a basic matched filtering (BMF) while the transmitting IoT node employs smart jamming strategy in order to compromise the activities of Eve. With respect to this and in attempt to realize maximum privacy, we examined the design of optimal jamming parameters. In the end, the numerical analysis of our investigation indicates that a substantial privacy advantage is achievable while utilizing only full-duplex jamming against using artificial noise from the transmitter only. However, a joint performance of both results shows a higher privacy improvement.**

***Index Terms*—Basic matched filtering (BMF), full-duplex, Internet of Things (IoT), multiple input and multiple output (MIMO), optimal matched filtering (OMF), privacy capacity.**

Manuscript received October 25, 2020; revised December 12, 2020; accepted January 6, 2021. Date of publication January 11, 2021; date of current version February 4, 2022. This work was supported by the Researchers Supporting Project through King Saud University, Riyadh, Saudi Arabia, under Grant RSP-2020/250. *(Corresponding author: Joseph Henry Anajemba.)*

Joseph Henry Anajemba and Tang Yue are with the Department of Communication Engineering, School of Internet of Things, Hohai University, Changzhou 211100, China (e-mail: herinopallazo@ieee.org; 362996892@qq.com).

Celestine Iwendi is with the Department of Electronics BCC, Central South University of Forestry and Technology, Changsha 410004, China (e-mail: celestine.iwendi@ieee.org).

Pushpita Chatterjee is with the Future Networking Research Group and the Faculty of Electrical and Electronics Engineering, Ton Duc Thang University, Ho Chi Minh City, Vietnam (e-mail puspitachatterjee@tdtu.edu.vn).

Desire Ngabo is with the College of Computer Science and Electronics Engineering, Hunan University, Changsha 410082, China (e-mail: dngabo@hnu.edu.cn).

Waleed S. Alnumay is with the Computer Science Department, King Saud University, Riyadh 12533, Saudi Arabia (e-mail: wnumay@ksu.edu.sa).

Digital Object Identifier 10.1109/JIOT.2021.3050755

I. Introduction

IN A WIRELESS communication, resource security and data privacy preservation are fundamental necessities. Particularly, wireless communications of the Internet of Things (IoT) which entail an intelligent data analysis and transmission, pervasive sensing and resourceful data management are extremely vulnerable to eavesdropping attack, because of its wireless broadcasting kind of channel [1]. Lately, IoT applications (e.g., smart devices in fifth generation (5G) systems) have been extensively mounted for data transmission in several multiple-input–multiple-output (MIMO) settings where a given number of users exchange data and vital information such as, data analysis, spatial crowdsourcing, smart cities, crowd dynamics management, environment monitoring and security surveillance [2]. Thus, any inversion of the network by a malicious attacker may impact negatively on the network transmission and can lead to an erroneous judgement, misinterpretation of information or unauthorized access to confidential data. Therefore, the security and privacy preservation of data during transmission and analytical process is vital in systems like single-input–single-output multiantenna eavesdropper (SISOME), multiple-input single-output multiantenna eavesdropper (MISOME) and multiple-input–multiple-output multiantenna eavesdropper (MIMOME).

Generally, eavesdropping has been established as one of the prevalent and frequently occurring attack in wireless networks. Conventionally, cryptographic encryption techniques are applied in managing these security glitches in the upper layers of the network protocol stack [3]. However, these techniques are characterized by hitches and susceptibilities in the distribution of secret key however, not without some extreme complication [4]. Therefore, considering IoT systems with a huge amount of resource constrained actuators and sensors, it is quite challenging to establish privacy and security. Thus, contrarily to the cryptographic encryption-based privacy, this article is focused on utilizing the physical properties of wireless networks (such as interference, noise and fading) which by extention is known as the physical layer security (PLS) approach [5] in combating eavesdropping attacks in IoT and MIMO data transmitting systems and to guarantee the overall security of the network.

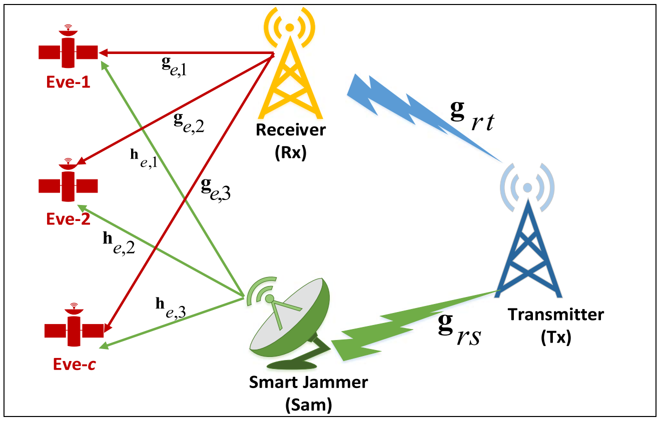

Fig. 1. IoT network transmission with PLS.

The PLS approach is almost a perfect alternative to conventional encryption-based methods and an attractive solution for IoT secure communications due to its capability of assuring security and privacy of information-theoretics notwithstanding the aptitudes of the computing eavesdropper [6], [7]. Thus, by using the PLS approach, Li and Dai [8] proposed a concept of friendly jammer approach with the intention of preventing the eavesdropper from deliberately injecting noise in the network. Before now, virtually all the researchers supposed that the jammer in a network transmission is friendly, that is, the network users possess a complete control of the network activities. But the jammer is not always friendly in the real sense and may assume a malicious part in transmitting noise to interrupt free flow of information in the transmission.

In a wider expression, this article considers a privacy performance in a secure IoT networks transmission as illustrated in Fig. 1, where the transmitting IoT device (Tx) aims to convey a private information to the receiver (Rx), in the presence of numerous noncolluding and passive eavesdroppers (Eves). Additionally, the transmitter uses a smart jammer (Sam) to emit signal interference which complicates Eves operations. We denote the set of Eves as $\mathcal{C} \triangleq \{1, 2, \ldots, C\}$ and the transmitter and Sam are furnished with A_t and A_s number of antennas, respectively. With respect to slow flat fading conditions, we assumed that all the wireless channels are autonomous. With denoted Tx $\rightarrow$ Rx transmitting channels and the Eve ($c \in \mathcal{C}$) by $\mathbf{g}_{tr} \in \mathbb{C}^{A_t}$ and $\mathbf{g}_{e,c} \in \mathbb{C}^{A_t}$, respectively, while Sam to Receivers transmitting signals and the cth Eve are represented by $\mathbf{g}_{rs} \in \mathbb{C}^{A_s}$ and $\mathbf{h}_{e,c} \in \mathbb{C}^{A_s}$, respectively. Finally, we assume that the perfect channel state information (CSI) of the Receivers and the statistical CSIs of the Eves are obtainable.

A. Notations

All matrices and column vectors in this work are denoted using both upper and lowercase boldface letters. Considering matrix $\mathbf{Y}$ with a vectorized form as $\mathbf{y}$, the operational inverse of $\mathbf{y} = \text{vec}(\mathbf{Y})$ is set as ivec($\mathbf{y}$). For a scenario where $\mathbf{y}$ is expressed as a column vector, diag($\mathbf{y}^J$) is used to represent the a diagonal matrix of $\mathbf{y}$ which contains several elements of $\mathbf{y}$ in a diagonal form. We utilized $\mathbb{E}_y[.]$ to denote the expectation regarding random variable $\mathbf{y}$ while, $\mathcal{P}\{T\}$ is used to represent the probability of occurrence T. Assuming the same probability space is used to express the random variables Y_c and Y. If Y_c converges to Y, then $Y_c \overset{\text{a.s.}}{\rightarrow} Y$ is practically as $c \rightarrow \infty$. Furthermore, we used $\mathbf{I}$ to express the identity matrix of presumed size, while $\mathbf{1}_c^J$ denotes the length of vector c all together. Using $I(y; z)$, we expressed the joint information transmitted amongst y and z random variables, while the actual unit of a complex number y is represented as Re(y). log(.) denotes the base 2 logarithm of the entire expressions, whilst the derivative of function $f(y)$ regarding y is signified as $([df(y)]/dy)$. For the intricate matrices $\mathbf{Y}$ and $\mathbf{Z}$, $\langle \mathbf{Y}, \mathbf{Z} \rangle \triangleq \text{Re}(A(\mathbf{Y}^G\mathbf{Z}))$ is established. For the matrices $\mathbf{T}_e, e \in \xi = \{1, \ldots, E_1\}$, $\{\mathbf{T}_e\}e \in \xi$ is used to represent the horizontal and orderly connection of all matrices. Finally, the slope of function $f(\mathbf{y})$ of y vector is classified as $\nabla_{\mathbf{x}} f(\mathbf{x})$.

B. Contributions

Inspired by the aforementioned observations, this article investigates privacy capacity in a MIMOME system where we assume that the perfect CSI of the Receivers and the statistical CSIs of the Eves are obtainable in IoT networks. The major contributions of this work are detailed as follows.

1) The proposed model considers two different conventional jamming approaches for Eve's activities in the transmission. Two respective scenarios where either an optimal matched filtering (OMF) or a basic matched filtering (BMF) is performed by Eve based on whether the transmitter is utilizing a smart jamming approach are analyzed.
2) For both the OMF and the BMF scenarios, a novel stochastic optimization algorithm is proposed to show the improvement in the performance of the jamming parameters.
3) Using mathematical models, we demonstrated the impacts of the main channel superiority and the requirements of minimum privacy capacity for optimal power allocation. Also, our model proved that the objective function in the primal privacy outage probability minimization problem can be changed into a severely concave function. Thus, a unique optimal solution is guaranteed.
4) Several elaborate simulations are performed to assess the exceptional performance of the proposed algorithm. Result of the simulations show the notable outperformance with respect to data rate constrain and transmit power as compared with other algorithms.

C. Structure

The remaining parts of this work is structured as follows. In Section II, related literature about privacy performance and PLS are reviewed and summarized. The system model which includes the formulation of the optimization models, proposed algorithms, and the proposed stochastic optimization method are described in Section III. Simulations and numerical analysis are provided in Section IV. Finally, the conclusion is presented in Section V.

II. Related Works

The study of privacy capacity has gained enormous attention in recent time. Hu *et al.* [9] and several other research works have dwelt on the maximization problem of privacy rate in the presence of single or multiple eavesdroppers in line with diverse norms on both transmitter, receiver and eavesdropper antenna settings and that of the transmissions CSI. However, there have been a limited number of researches which focused on the case whereby CSI of Eve is not known to both the transmitter and receivers. The study of [10] presents scrambling outcome on the per-node secure throughput in a network of transmitter-receiver pairs. On the other hand, [11] utilized a stochastic cooperative jamming approach (SCJA) to frustrate Eves activities at any location in the network. Where compared this approach to our proposed technique, the stochastic optimization technique we propose in this work is void of data rate degradation to the inherent IoT devices. Xu *et al.* [12] examined and presented an approach for rewarding nonaltruistic secondary users (SUs) for offering adequate jamming service by offering adjustable range of resources. This approach is established to be very useful in combination with stochastic protocols for the optimization of cognitive radio (CR) performance [13].

Adopting a stochastic geometry technique (SGT), Wang and Zhang [14] analyzed the privacy performance of full-duplex device-to-device (D2D) transmission in multitier wireless communication using optimal spectrum partition amongst cellular modes and D2D. Similarly, based on the advantage of posing spatial degrees of diversity gains and freedom, the multiantenna approach is utilized as a resourceful and consistent means of enhancing privacy in a wireless communication [15]. Particularly with the unavailability of the when the eavesdropper's instantaneous CSI, to this effect, a privacy beamforming with artificial noise (AN) was proposed in [16]. With respect to a multiantenna concept, AN aided transmit strategies were considered for both slow and fast fading channels in [17], [18] where secrecy outage probability (SOP), SOP constrained secrecy rate and secrecy throughput are frequently assumed as the performance metrics for slow fading channels [19], [20], while ergodic secrecy rate is frequently applied as the privacy metric for fast fading channels [21]. Precisely, in order to minimize SOP, power allocation between information-bearing signal and AN signal were improved for the single eavesdropper in [22], and for multiple eavesdroppers in [23].

Anajemba *et al.* [24] examined privacy performance of a single-hop MIMO system using AN and beamforming approaches where AN is communicated over the signal bearing the information to depreciate the eavesdropper's medium. All nodes in their experiment operated in half-duplex mode and for the multiantenna eavesdroppers, they assumed a poisson point process (PPP) distribution. Employing full-duplex relay under a total power constraint, the research of [25] investigated the realizable privacy capacity. Their result proved that full-duplex powered relays can attain a substantial performance improvement over half-duplex relays. But they measured only a single eavesdropper setting. They also examined privacy outage probability for multi-input single-output (MISO) channels, while [26] presented a privacy performance MIMO channels with and without AN.

Although all the above works have analyzed both the single and multiple streams of transmission in the presence of both single and multiple eavesdroppers, with a single antenna or multiple antennas, all the research made use of preset system parameters as constants and could not fit into some available channel states. The distinguishing factor of our research is that privacy capacity is achievable with both optimal and nonoptimal parameters of jamming. Considering this, the output of our investigation shows that a substantial benefit is achievable while utilizing only full-duplex jamming against using AN from the Transmitter only, however, a joint performance of both results shows a higher privacy improvement.

III. System Model

In the network setup of our MIMOME model, the transmitting station (TS) which is made up of multiple smart antenna's (A) attempts to communicate private message through the receivers wireless channel of multiple smart antenna's (B) in a scenario where possibly several inactive Eves (with C number of antennas) may interconnive at the network layer rather than at the physical layer. With reference to [19], in a MIMO system setup, network parameters are stabilized such that the factor of large-scale-fading from the Transmitter to the Receiver is $t = d_T^{-\alpha} = \left(\sqrt{(y+0.5)^2+z^2}\right)^{-\alpha}$, while from the Receiver to Eve is estimated as $r = d_R^{-\alpha} = \left(\sqrt{(y+0.5)^2+z^2}\right)^{-\alpha}$.

Considering as the exponent coefficient of the path loss. Practically, we assumed that the distance from any of Eve's to the transmitting device is not more than a particular distance which is, $d_T \geq \Delta$. Thus, ρ represents the stabilized factor of large-scale-fading factor of the Receiver's self-interference. The parameter $\mathbf{I}$ denotes the Transmitter to Receiver matrix of small-scale-fading channel, and $\mathbf{R}$ represents that of Receiver to Transmitter, while $\mathbf{H}$ denotes the Receivers self-interference. The Receiver to Transmitter channel matrix is then represented as $\mathbf{G}$, denoting its singular value decomposition (SVD) as

$$\mathbf{G} = \mathbf{M}\sqrt{\Lambda}\mathbf{N}^G \tag{1}$$

while $\mathbf{M}$ and $\mathbf{N}$ represents the respective unitary matrices, $\sqrt{\Lambda}$ denotes the transverse matrix which encompasses the singular values $\sqrt{\lambda_s}$, $s = 1, \ldots, \min(B, A)$ of $\mathbf{G}$ in a downward order on its main transverse. It is important to note that all the channel matrix elements are identically-independently-distributed (i.i.d.) circular composite Gaussian form with zero mean and unit variance. Therefore, the following signal comprising private message and noise is transmitted by Tx

$$\mathrm{y}_t = \sqrt{\phi P_t \mathbf{n}_1 i} + \sqrt{\tfrac{(1-\phi)P_t}{A-1}}\mathbf{N}_1\mathbf{x}_t \tag{2}$$

as the definition of $\mathbf{n}_1$ and $\mathbf{N}_1$ is obtained by $\mathbf{N} = [\mathbf{n}_1, \mathbf{N}_1]$, i denotes the information symbol of Tx with unit variance (for easy clarity of major concept, we study a single stream of data, but will be extended further to the concept of multiple stream of data), while $\mathbf{x}_t$ represents the $(A-1)x1$ i.i.d. composite Gaussian noise vector form with zero mean and unit variance. Likewise, ϕ denotes the ratio of power P_t assigned to data at Tx. While receives messages from Tx, Tx also transmits jamming noise. While we will later introduce the concept of smart jamming, this noise is represented in a simplified form as

$$y_R = \sqrt{\frac{P_R}{B}}\mathbf{x}_R \tag{3}$$

where $\mathbf{x}_R$ is an i.i.d. form of Bx1 and a composite Gaussian noise vector with zero mean and unit variance. P_T and P_R represents the normalized powers pertaining to Tx $\rightarrow$ Rx path loss. As long as all related contextual noises at all terminals are normalized to assume the same unit variance, then, the following signals will be, respectively, received by Tx and Rx

$$z_R = \sqrt{\phi\lambda_1 P_T}\mathbf{m}_1 i + \sqrt{\frac{(1-\phi)P_T}{A-1}}\mathbf{M}_1\sqrt{\Lambda_1}\mathbf{x}_T + \tilde{\mathbf{v}}_R \tag{4}$$

$$z_K = \sqrt{t\phi P_T}\mathbf{t}_1 i + \sqrt{\frac{t(1-\phi)P_T}{A-1}}\mathbf{T}_1\mathbf{x}_T + \sqrt{\frac{rP_R}{B}}\mathbf{R}\mathrm{x}_R + \mathbf{c}_K \tag{5}$$

considering $\mathbf{TN} = [\mathbf{Tn}_1, \mathbf{TN}_1] = [\mathbf{t}_1, \mathbf{T}_1]$, $\mathbf{M} = [\mathbf{m}_1, \mathbf{M}_1]$ and $\tilde{\mathbf{n}}_R = \sqrt{\frac{\rho P_R}{B}}\mathbf{R}\mathrm{x}_R + \mathbf{n}_K$. Based on the analysis in [19], $\tilde{\mathbf{n}}_R$ can be expressed as $\mathcal{CN}(0, (\rho P_R + 1)\mathbf{S})$, while $\sqrt{\Lambda_1}$ is the matrix of $(B-1)x(A-1)$ with $\sqrt{\lambda_s}, s \in \{2, \ldots, \min(B, A)\}$ on the core transverse, and $\mathbf{c}_K$ is an $C \times 1$ i.i.d. composite Gaussian noise vector with zero mean and unit variance.

As long as the noise covariance matrix and interference in the received signal z_R in (4) is recognizable by the Receiver, then an OMF can be performed by T_x. However, as a result of the orthogonality which exist among $\mathbf{m}_1$ and $\mathbf{M}_1$, the receivers OMF corresponds to its BMF, this implies that $\mathbf{m}_1^G z_R$ satisfies the estimation of i given z_R. Considering that $\mathbf{m}_1^G z_R = \sqrt{\phi\lambda_1 P_T} i + \mathbf{m}_1^G \tilde{\mathbf{c}}_R$, then, R_x optimized SNR is achieved as

$$\mathrm{SNR}_{TR} = \frac{\phi\lambda_{1P_T}}{1+\rho P_R}. \tag{6}$$

A. Case of Eve Utilizing OMF

Assuming Rx utilizes the simplified noise, which is represented (3), then, Eve may obtain a complete information to regulate the co-variance matrix $\mathbf{Q}_K$ of the interference and noise z_K in (5), therefore

$$\mathbf{Q}_K = \mathbf{S} + \frac{t(1-\phi)P_T}{A-1}\mathbf{T}_1\mathbf{T}_1^G + \frac{rP_R}{B}\mathbf{R}\mathbf{R}^G. \tag{7}$$

Using the covariance matrix $(\mathbf{Q}_K)$, the OMF of the received signal z_K can be performed by Eve using the premultiplication of a $\mathbf{t}_1^G\mathbf{Q}_K^{-1}$. This results in an SNR optimization at Eve

$$\mathrm{SNR}_{TK} = t\phi P_T \mathbf{t}_1^G \mathbf{Q}_K^{-1}\mathbf{t}_1. \tag{8}$$

Thus, the achievable privacy rate of Tx $\rightarrow$ Rx channel against all colluding Eves at the network layer rather than the physical layer is

$$I = \min_{\mathrm{Eves}}(\log(1+\mathrm{SNR}_{TR}) - \log(1+\mathrm{SNR}_{TK}))^+ \tag{9}$$

where $(.)^+ \overset{\Delta}{=} \max(0, .)$. Although we can statistically model the small-scale-fading CSI of Eve to correspond to a classification of packets in multiple channel coherent time of mobile computing environment. However, Eve's CSI large-scale-fading is according to Eve's large-scale position in line with the Transmitter and the Receiver. In most real-life scenario, during the time of interest which is based on seconds or minutes, Eve's distribution is practically described as deterministic and unidentified (thus, not stochastically and obviously not Poisson distributed). Considering this, a perfect way of tackling the unidentified Eve's CSI large-scale-fading is to study Eve's most destructive position in the network [19]. Hence, SNR_{TR} is not variant to the position and location of Eve, therefore, in a multiple eavesdropping scenario, the most destructive Eve is the one whose position maximizes SNR_{TK}. Thus, (3) can be rewritten as

$$\mathrm{SNR}_{TK} = \phi P_T \mathbf{t}_1^G\left(\frac{1}{t}\mathbf{S} + \frac{(1-\phi)}{A-1}\mathbf{T}_1\mathbf{T}_1^G + \frac{rP_R}{tB}\mathbf{R}\mathbf{R}^G\right)^{-1_{\mathbf{t}_1}}. \tag{10}$$

As long as r is minimum for a fixed $t = r_T^{-\alpha}$, SNR_{TK} is maximized, that is, $r = (1+d_T)^{-\alpha}$. Thus, substituting the r in (10) we achieved

$$\mathrm{SNR}_{TK} = \phi P_T \mathbf{t}_1^G\left(d_T^{\alpha}\mathbf{S} + \frac{(1-\phi)P_T}{A-1}\mathbf{T}_1\mathbf{T}_1^G + \frac{d_T^{\alpha}P_R}{(1+d_T)^{\alpha}B}\mathbf{R}\mathbf{R}^G\right)^{-1_{\mathbf{t}_1}}. \tag{11}$$

Considering that $d_T \geq \Delta$, if $d_T \geq \Delta$ then, SNR_{TK} is maximized. Consequently, Eve's most destructive position is set as $y^* = -0.6 - \Delta$, $z^* = 0$. Henceforth, the $\min_{\mathrm{Eves}}$ in (9) will no longer be considered, however, t and r will be referred as the Eves matching to points (y^*, z^*). For the entire simulations, $\Delta = 0$ will be utilized.

B. Formulated Optimization Problem for OMF of Eve

Although it is simple to demonstrate that I is a cumulative function of P_T, however, it is inconsequential to prove the dependency of I on P_R and ϕ. At this point, our focus is to establish the optimal P_R and ϕ by maximizing the objective function below

$$I_A(P_R, \phi) = \left(\log(1+\mathrm{SNR}_{TR}) - \varepsilon_{\mathbf{T},\mathbf{R}}\left[\log(1+\mathrm{SNR}_{TR})\right]\right)^+ \tag{12}$$

where $\varepsilon_y[.]$ represents expectation with regard to y, while $I_A(P_R, \phi) \leq \varepsilon_{\mathbf{T},\mathbf{R}}[I]$ preceding the observation $(\varepsilon[y])^+ \leq \varepsilon[(y)]^+$. By utilizing the proposed technique in [19], we will stochastically maximize $I_A(P_R, \phi)$. Thus, our proposed stochastic optimization technique is initiated by first defining

$$\begin{aligned} -I_A(P_R, \phi|\mathbf{T}, \mathbf{R}) &= \log(1+\rho P_R + \phi\lambda_1 P_T) - \log|\mathbf{Q}_K| \\ &\quad + \log(1+\rho P_R) - \log\left|\mathbf{Q}_K + t\phi P_T \mathbf{t}_1\mathbf{t}_1^H\right| \\ &= f_1(\mathbf{y}) + f_2(\mathbf{y}, \mathbf{T}, \mathbf{R}) + f_3(\mathbf{y}) + f_4(\mathbf{y}, \mathbf{T}, \mathbf{R}) \end{aligned} \tag{13}$$

considering that f_1, f_2, f_3, and f_4 are obviously defined, the first two expressions of the jamming parameter $\mathbf{y} = [P_R, \phi]^J$ are in convex form, while the last two assumed concave functions. Using their first-order Taylor series of expansion, the latter can be iteratively upper bounded and approximated. We realized a random realization of $\mathbf{T}$ and $\mathbf{R}$ at iteration j, thus, since $y^j = [P_R^j, \phi^j]^J$, and $\mathbf{T}^j$, $\mathbf{R}^j$, let

$$\hat{y}^j \triangleq \arg\min_{y\in\gamma} \hat{f}^j(\mathrm{y}) \tag{14}$$

where $\gamma \triangleq \{y | 0 \leq \phi \leq 1, 0 \leq P_R \leq P_R^{\max}\}$ and denoting $\beta^j \in [0, 1]$ as the sequence which is to be selected properly

$$\begin{aligned}\hat{f}^j(y) \triangleq\ & \beta^j\big(f_1(y) + f_2\big(y, \mathbf{T}^j, \mathbf{R}^j\big)\big) + \beta^j\big(y - y^j\big)^J \Pi^j \\ & + \big(1 - \beta^j\big)\big(y - y^j\big)^J\Big(\mathbf{f}^{j-1}\Big) + \tau\big\|y - y^j\big\|^2 \end{aligned} \tag{15}$$

whereby

$$\begin{aligned}\Pi^j &= \nabla_y\big(f_3(y) + f_4\big(y, \mathbf{T}^j, \mathbf{R}^j\big)\big)|_{y=y^f} \\ &= \frac{1}{1n(2)}\left[\begin{array}{c} \Big(\mathrm{Jq}\Big(\mathbf{Q}_K^j + tP_T\phi^j\mathbf{t}_1^j\mathbf{t}_1^{jG}\Big)^{-1}\Big(-\frac{tP_T}{A-1}\mathbf{T}_1^j\mathbf{T}_1^{jG}\Big)\Big) \\ \frac{\rho}{1+\rho P_R} + \mathrm{Jq}\Big(\Big(\mathbf{Q}_K^j + tP_T\phi^j\mathbf{t}_1^j\mathbf{t}_1^{jG}\Big)^{-1}\big(\frac{r}{B}\mathbf{R}^j\mathbf{R}^{jG}\big)\Big) \end{array}\right]\end{aligned} \tag{16}$$

since the vector $\mathbf{f}^j$ is updated iteratively as

$$\mathbf{f}^j = (1 - \beta^j)\mathbf{f}^{j-1} + \beta^j\big(\Pi^j + \nabla_y\big(f_1(y) + f_2\big(y, \mathbf{T}^j, \mathbf{R}^j\big)\big)|_{y=y^j}\big). \tag{17}$$

Then

$$\begin{aligned}&\nabla_y\big(f_1(y) + f_2\big(y, \mathbf{T}^j, \mathbf{R}^j\big)\big)|_{y=y^j} \\ &= \frac{1}{1n(2)}\left[\begin{array}{c} \frac{\lambda_1 P_t}{1+\rho P_R^j+\phi^j\lambda_1 P_T} + \mathrm{Jq}\Big(\Big(\mathbf{Q}_K^j\Big)^{-1}\Big(\frac{tP_T}{A-1}\mathbf{T}_1^j\mathbf{T}_1^{jG}\Big)\Big) \\ -\frac{\rho}{1+\rho P_R^j+\phi^j\lambda_1 P_T} - \mathrm{Jq}\Big(\Big(\mathbf{Q}_K^j\Big)^{-1}\big(\frac{r}{B}\mathbf{R}^j\mathbf{R}^{jG}\big)\Big) \end{array}\right].\end{aligned} \tag{18}$$

In (15), the first expression denotes the convex fragment of (13) and the linearizing effect of the nonconvex fragment is represented by the second expression. Likewise, the third expression is included to determine the unidentified gradient of $I_A(P_R, \phi)$ [as long as $I_A(P_R, \phi) > 0$] according to its models which are received during iterations and which assume better accuracy with each iteration. On the other hand, the third expression is the regularization parameter. In conclusion, the updated form of $\hat{y}^j, y^j$ as $\chi^j \in (0, 1]$ is utilized as the sequence which is to be selected properly is given as follows:

$$y^{j+1} = \Big(1 - \chi^{j+1}\Big)y^j + \chi^{j+1}\hat{y}^j. \tag{19}$$

Recall that the objective function in (14) is extremely convex and its optimization is made very simple. Therefore, with respect to the conditions in [26] and applying such in our technique, convergence is guaranteed in our problem by the following parameters: $\beta^0 = \beta^1 = \chi^1 = 1$, $\beta^j = [2/(j+2)^{0.6}]$ $\forall j \geq 2$, $\chi^j = [2/(j+2)^{0.6}]$ $\forall j \geq 2$ and $\tau = 10^{-4}$. Algorithm 1 illustrates the detailed computation procedure for the proposed stochastic optimization. However, the following procedure is proposed to determine an effective initialization of the algorithm. First, if we assumed that $\rho P_R \ll 1$ and realized

$$I_A(P_R, \phi) \approx \big[\log(1 + \phi\lambda_1 P_R) - \varepsilon_{\mathbf{T},\mathbf{R}}\big[\log(1 + \mathrm{SNR}_{TK})\big]\big]^+ \tag{20}$$

Algorithm 1 Stochastic Optimization Computation

Set: P_R^0, ϕ^0, allocate $P_R^{-1} = 0$, and select the actual τ, $\in$, β^j, χ^j
Initiate: $j = 0$

while $\frac{|\phi^j - \phi^{j-1}|}{\phi^j} + \frac{|P_R^j - P_R^{j-1}|}{P_R^j} > \in$ **do**
  Compute a random realization of $\mathbf{T}, \mathbf{R}$.
  Estimate $\hat{y}^j$ from (14)
  Update y^{j+1} utilizing (19).
  Update $\mathbf{f}^j$ utilizing (17).
  $j = j + 1$
end
Return $\phi^* = \phi^j, P_R^* = P_R^j$

then, on the average, privacy would be a cumulative function of P_R as cumulative P_R implies maximized Rx jamming and on the average, minimized Eve's SNR. Thus, if $P_R^0 = \frac{\vartheta}{\rho}$ is selected where $\vartheta \ll 1$, P_R^0 is guaranteed to be suboptimal and with respect to the solution in [26], $\mathbf{Q}_K^{-1}$ can be approximated to achieve

$$\mathbf{Q}_K = \mathbf{Q}_1 - \phi\mathbf{Q}_2 \tag{21}$$

$$\mathbf{Q}_K^{-1} \approx \mathbf{Q}_1^{-1} + \phi\mathbf{Q}_1^{-1}\mathbf{Q}_2\mathbf{Q}_1^{-1} \tag{22}$$

where $\mathbf{Q}_1 = \mathbf{S} + (tP_T/A - 1)\ \mathbf{T}\mathbf{N}_1\mathbf{N}_1^G\mathbf{T}^G + (rP_R/B)\ \mathbf{R}\mathbf{R}^G$ and $\mathbf{Q}_2 = (tP_T/A - 1)\ \mathbf{T}\mathbf{N}_1\mathbf{N}_1^G\mathbf{T}^G$. It is important to note that as long as $\phi \in (0, 1)$ is smaller than $\mathbf{Q}_1$ and $\mathbf{Q}_2$, then the approximation is validated. Therefore, the SNR of Eve can be expressed as

$$\mathrm{SNR}_{TK} \approx t\phi P_T\mathbf{t}_1^G\Big(\mathbf{Q}_1^{-1} + \phi\mathbf{Q}_1^{-1}\mathbf{Q}_2\mathbf{Q}_1^{-1}\Big)\mathbf{t}_1 = \phi(d + \phi k) \tag{23}$$

where $d = tP_T\mathbf{t}_1^G\mathbf{Q}_1^{-1}\mathbf{t}_1$, $k = tP_T\mathbf{t}_1^G\mathbf{Q}_1^{-1}\mathbf{Q}_2\mathbf{Q}_1^{-1}\mathbf{t}_1$ and $\mathrm{SNR}_{TR} = [(\phi\lambda_1 P_T)/(1 + \rho P_R^0)] = \phi c$. Therefore

$$I = I_A(\phi, P_R|\mathbf{T}, \mathbf{R}) \approx \left[\log\left(\frac{1 + \phi c}{1 + \phi d + \phi k^2}\right)\right]^+. \tag{24}$$

Thus, in an attempt to optimize privacy, we derived the optimal ϕ from

$$\begin{aligned}\frac{\vartheta I}{\vartheta\phi} &= 0 \to -\phi kc^2 - 2\phi k + c - d \\ &= 0 \to \phi^0 = \frac{-1 + \sqrt{1 + \frac{c(c-d)}{k}}}{c}.\end{aligned} \tag{25}$$

C. Case of Eve Utilizing BMF

In this section, a scenario where Eve makes use of BMF is considered. Assuming that Rx utilizes a smart jamming approach other than the one in (3) as follows:

$$\mathrm{y}_R = \sqrt{\frac{P_R}{c}}\mathbf{Z}\tilde{\mathbf{x}}_R. \tag{26}$$

With respect to the smart jamming approach in (26), $\tilde{\mathbf{x}}_R$ represents the $c \times 1$ i.i.d. vector of composite Gaussian noise with unit variance, where $\mathbf{Z}$ denotes a $B \times c$ random matrix considering $B > c$ as the property that $\mathbf{Z}^G\mathbf{Z} = \mathbf{S}$, at this point Eve cannot acquire the matrix of covariance for the interference and noise in its received signal. Therefore, Eve is unable to make use of the OMF, however, it applies the following BMF:

$$\mathbf{t}_1^G z_K = \sqrt{t\phi P_R}\|\mathbf{t}_1\|^2 i + \sqrt{\frac{t(1-\phi)P_T}{A-1}}\mathbf{t}_1^G\mathbf{T}_1 x_T + \sqrt{\frac{rP_R}{c}}\mathbf{t}_1^G\mathbf{R}\mathbf{Z}_{\tilde{x}_R} + \mathbf{t}_1^G\mathbf{c}_K \tag{27}$$

the SNR of this expression is stated as

$$\mathrm{SNR}_{TK} = \frac{\phi P_R\|\mathbf{t}_1\|^2}{1 + \frac{(1-\phi)}{A-1}tP_T\left\|\mathbf{T}_1^G\tilde{\mathbf{t}}_1\right\|^2 + \frac{rP_R}{c}\left\|\hat{\mathbf{B}}^G\tilde{\mathbf{t}}_1\right\|^2} \tag{28}$$

as $\tilde{\mathbf{t}}_1 = (\mathbf{t}_1/\|\mathbf{t}_1\|)$, where $\tilde{\mathbf{R}} = \mathbf{R}\mathbf{Z}$. Assuming $n_1 \triangleq \|\mathbf{t}_1\|^2$, then, we can establish that $\sqrt{2n_1}$ is identically distributed as $\gamma^2(2C)$. Likewise, assuming $n_2 \triangleq \|\mathrm{T}_1^G\tilde{\mathbf{t}}_1\|^2$, then, $\sqrt{2n_2}$ is accordingly distributed to $\gamma^2(2(A-1))$. Lastly, if $n_3 \triangleq \|\tilde{\mathbf{R}}^G\tilde{\mathbf{t}}_1\|^2$, then, $\sqrt{2n_3}$ is accordingly distributed to $\gamma^2(2c)$. In this scenario, Eve's most dangerous position remains $(y^*, x^*) = (-0.6-\Delta, 0)$. Similarly, the smart jamming from Tx does not affect the SNR_{TR} in (6). To further establish cumulative distribution function (CDF) of I when $I > 0$, the CDF which is conditioned on λ_1 is $\mathcal{F}_I(i) = \mathcal{P}\{I \le i|\lambda_1\} = \mathcal{P}\{\log_2(1+\mathrm{SNR}_{TR}) - \log_2(1+\mathrm{SNR}_{TK}) \le i|\lambda_1\} = \mathcal{P}\{n_1 - X_1 n_2 - X_2 n_3 - X_3 \ge 0|\lambda_1\}$ where

$$X_1 = \frac{(1-\phi)\left(\frac{\phi\lambda_1 P_T}{1+\rho P_R} - 2^i + 1\right)}{(A-1)\left(2^i\phi\right)} \tag{29}$$

$$X_2 = \frac{rP_R\left(\frac{\phi\lambda_1 P_T}{1+\rho P_R} - 2^i + 1\right)}{c\left(2^i\phi P_T t\right)} \tag{30}$$

$$X_3 = \frac{\left(\frac{\phi\lambda_1 P_T}{1+\rho P_R} - 2^i + 1\right)}{\left(2^i\phi P_T t\right)}. \tag{31}$$

This adheres to

$$\begin{aligned}\mathcal{F}_I(i) &= \int_0^\infty\int_0^\infty\int_{X_{1y}+X_{2z}+X_3}^\infty \frac{x^{(C-1)}y^{(A-2)}z^{(c-1)}k^{-w-y-z}}{(C-1)!(A-1)!(c-1)!}dx\,dy\,dz\\ &= \frac{k^{-X_3}}{(1+X_2)^c(1+X_1)^{A-1}(c-1)!(A-2)!}\sum_{e=0}^{C-1}\sum_{s=0}^{e}\sum_{l=0}^{s}\frac{1}{e!}\binom{e}{s}\binom{s}{l}\\ &\quad\times(e-s+A-2)!(s-l+c-1)!\left(\frac{X_1}{1+X_1}\right)^{e-1}\\ &\quad\times\left(\frac{X_2}{1+X_2}\right)^{s-l}X_3^l.\end{aligned} \tag{32}$$

To proof this, we first established the following theorems.

Theorem 1:

$$\int_0^\infty x^c k^{-x}dx = k^{-l}\sum_{e=0}^{c}\frac{c!}{e!}l^e(l > -\infty). \tag{33}$$

Theorem 2:

$$\int_0^\infty x^c k^{-lx}dx = \frac{c!}{l^{c+1}}(l > \infty). \tag{34}$$

Therefore

$$\mathcal{F}_I(i) = \frac{1}{(C-1)!(A-2)!(c-1)!}\int_0^\infty z^{(c-1)}k^{-z}\int_0^\infty y^{(A-2)}k^{-y} \times\int_{X_{1y}+X_{2z}+X_3}^\infty x^{(C-1)}k^{-x}dx\,dy\,dz. \tag{35}$$

By utilizing Theorem 1, we achieve

$$\begin{aligned}\mathcal{F}_I(i) &= \frac{(C-1)!k^{-X_3}}{(C-1)!(A-2)!(c-1)!}\\ &\quad\times\sum_{e=0}^{C-1}\frac{1}{e!}\int_0^\infty z^{(c-1)}k^{-z(X_2+1)}\\ &\quad\times\int_0^\infty y^{(A-2)}k^{-y}(X_1y+X_2z+X_3)^e dy\,dz\\ &= \frac{k^{-X_3}}{(L-2)!(c-1)!}\times\sum_{e=0}^{C-1}\sum_{s=0}^{e}\frac{\binom{e}{s}}{e!}\\ &\quad\times\int_0^\infty z^{(c-1)}k^{-z(X_2+1)}(X_2z+X_3)^s\\ &\quad\int_0^\infty y^{(A-2)}k^{-y(X_1+1)}(X_1y)^{e-s}dy\,dz.\end{aligned} \tag{36}$$

By utilizing Theorem 2 twice, we achieve

$$\begin{aligned}\mathcal{F}_I(i) &= \frac{k^{-X_3}}{(A-2)!(c-2)!}\sum_{e=0}^{C-1}\sum_{s=0}^{e}\frac{\binom{e}{s}}{e!}\int_0^\infty z^{(c-1)}k^{-z(X_2+1)}\\ &\quad\times(X_2z+X_3)^s\frac{X_1^{e-1}(e-s+A-2)!}{(1+X_1)^{e-s+c_1}}dz\\ &= \frac{k^{-X_3}}{(A-2)!(c-2)!(1+X_1)^{c_1}}\\ &\quad\times\sum_{e=0}^{C-1}\sum_{s=0}^{e}\frac{1}{e!}(e-s+A-2)!\binom{e}{s}\left(\frac{X_1}{1+X_1}\right)^{e-s}\\ &\quad\times\int_0^\infty z^{(c-1)}k^{-z(X_2+1)}\sum_{l=0}^{s}\binom{s}{l}(X_2z)^{s-l}(X_3)^l\,dz\\ &= \frac{k^{-X_3}}{(A-2)!(c-2)!(1+X_1)^{c_1}(1+X_2)}\\ &\quad\sum_{e=0}^{C-1}\sum_{s=0}^{e}\sum_{l=0}^{s}\frac{1}{e!}(e-s+A-2)!(s-l+c-1)!\\ &\quad\times\binom{e}{s}\binom{s}{l}\\ &\quad\left(\frac{X_1}{1+X_1}\right)^{e-s}\left(\frac{X_2}{1+X_2}\right)^{s-l}X_3^l.\end{aligned} \tag{37}$$

D. Formulated Optimization Problem for BMF of Eve

To achieve an optimal P_R and ϕ, we employed a focal privacy level I_0 but minimized $\mathcal{F}_I(i_0)$. However, to establish a good level of Quality of Service (QoS), the rate of Tx $\rightarrow$ Rx is constrained to be greater than or equal to C. Therefore, the optimization problem is established as

$$\min_{P_R,\phi}\ \mathcal{F}_I(i_0) \tag{38}$$

s.t. $0 \le P_R \le P_R^{\max}$, $0 \le \phi \le 1$ and $\phi - ([(2^c-1)\rho]/P_T\lambda_1)P_R \ge ([(2^c-1)\rho]/P_T\lambda_1)$ which is generated from the constraint of Tx $\rightarrow$ Rx. These constraints are

Algorithm 2 Stochastic Optimization Algorithm for Estimating the Optimal P_R and ϕ

Input: P_R and ϕ into $\Re$ and initialize the group of active constraints as null

```
while P_R and φ do not converge do
  for each constraint do
    if the action fails to meet (39) conditions, then
      Eliminate the executed constraint from the group of active constraints
    end if
  end for
  Utilize a group of active constraints and estimate P but, initialize P = 0 if all constraints are inactive
  d = −P∇F_I
  ξ = BackTracking - LineSearch(d, φ, F_I P_R)
  P_R = P_R + dξ
  φ = φ + dξ
  for every constraint do
    if unable to satisfy constraint then
    Compute P_R and φ to attain constraint satisfaction
    Add the satisfied constraint to the group of active constraints
end search
end
```

in a linear form and is made up of a convex region $\Re$, thus, for the objective function to be minimized, a gradient projection approach is utilized. In approach, for every level of the gradient lineage, the direction of the search is projected into a direction tangent to the active constraints. Note, for (P_R, ϕ) the constraint $C : \phi t + rP_r + c \geq 0$ is referred as active if the parameter attains the subsequent two conditions

$$\begin{cases} \phi t + rP_r + c = 0 \\ c^J \nabla \mathcal{F}_I \leq 0 \end{cases} \tag{39}$$

where c is used to represent the constraints actual vector which points toward the inward region $\Re$. Assuming the columns of matrix $\mathbf{C}$ is defined as the active constraints gradient, we establish our direction of search as $-\mathbf{P}\nabla\mathcal{F}_I$ considering $\mathbf{P} = \mathbf{S} - \mathbf{C}(\mathbf{C}^J\mathbf{C})^{-1}\mathbf{C}^J$ with $\nabla\mathcal{F}_I$ expressed as follows:

$$\nabla\mathcal{F}_I = \begin{bmatrix} \frac{\delta\mathcal{F}_I}{\delta\phi} \\ \frac{\delta\mathcal{F}_I}{\delta P_R}. \end{bmatrix}.$$

Thus

$$\begin{aligned} \frac{\delta\mathcal{F}_I}{\delta\phi} &= \frac{\delta X_1}{\delta P_R}\left(\frac{1-A}{1+X_1}S(1) + \frac{1}{X_1(1+X_1)}S(e-s)\right) \\ &\quad + \frac{\delta X_2}{\delta\phi}\left(\frac{-B}{1-X_2}S(1) + \frac{1}{X_2(1+X_2)}S\right) \\ &\quad + \frac{\delta X_3}{\delta\phi}\left(-S(1) + \frac{1}{X_3}S(l)\right). \end{aligned} \tag{40}$$

The proposed stochastic optimization algorithm for estimating the optimal P_R and ϕ is illustrated in Algorithm 2.

E. Case of Multiple Information Source

So far, our analysis has been based on a single source of information. However, we briefly extended our research to a privacy scenario where the Transmitter utilizes more than one information source, while the performance of Eve is based on OMF. With respect to these assumptions, the equations for this scenario can be easily simplified. To achieve that, we first established an energy allocation matrix $\mathbf{E} = \mathrm{diag}(e_1, e_2 \cdots e_q)$ considering q as the number of information sources with $\sum e_s \leq \phi$. Therefore, (12) is transformed as

$$\begin{aligned} I_A(P_R, \phi) = \Bigg[& \sum_{s=1}^{q} \log\left(1 + \tfrac{P_T\lambda_s e_s}{1+\rho P_R}\right) \\ & - \varepsilon_{\mathbf{T},\mathbf{R}}\left[\log\left|\mathbf{S}_K + tP_T\bar{\mathbf{Q}}_K^{-1}\bar{\mathbf{T}}_1\mathbf{E}\mathbf{N}_1^Q\right|\right]\Bigg]^+ \end{aligned} \tag{41}$$

where $\bar{\mathbf{T}}_1 = \mathbf{TN}_{1:q}$ (as represents the first qth columns of $\mathbf{N}$) while

$$\bar{\mathbf{Q}}_K = \mathbf{S} + \frac{t(1-\phi)P_T}{A-q}\mathbf{TN}_{q+1:A}\mathbf{N}_{q+1:A}^G\mathbf{T}^G + \frac{rP_R}{B}\mathbf{RR}^G. \tag{42}$$

Since we have derived the equations for multiple information source, then we can derive an optimal $\mathbf{E}$, P_R and ϕ using the objective function alongside Algorithm 1.

F. Computational Complexity

In this section we analyzed the computational complexity of our proposed SPOA algorithm against other existing privacy optimization techniques, such as, SCJA and SGT techniques. First, the discrete iterations are to calculate JK which is allocated to antennas of kth SCDs. The iteration J is implemented to assign only one antenna per K of the SCDs. Thus, the total realized complexity in the primal phase is expressed as JK^2. For the second phase, if a subgradient method is applied for individual iterations, a complexity of $0(JK)$ which converges speedily as $0((JK)^2)$ iterations is achieved. The subgradient method also results in a complexity of $0(JK(J+1)^2)$. With ξ utilized as the crucial precision which support the backtracking-line search, the realizable computational complexity is achieved as $0(JK(J+1)^2.\log_2(1/\xi))$. At the third phase, the computational complexity is $0(K)$ for individual iterations if data is constantly transmitted from Jth antenna to Kth SCDs. Thus, the achievable complexity of this phase is established as $0(K(J+1)^2.\log_2(1/\xi))$. The result show that the first phase iteration contains a constraint K because only one antenna is selected by the transmitting SCDs. Hence, this implies that the computational complexity of the proposed SPOA algorithm is subject to both the second and the third phase of iterations. Thus, the overall complexity of the proposed SPOA algorithm is computed as $0(K(J+1)^3.\log_2(1/\xi))$ and contains polynomial time complexity which can enable an actual and real-life application of the proposed technique in IoT network transmission with a minimized data rate constraint.

IV. Simulation Results and Analysis

In this section, we numerically examined the privacy performance of our proposed stochastic optimization technique. For all the simulation, we set the transmitting IoT

TABLE I
SIMULATION PARAMETERS AND DERIVATIONS

Parameters	**Derivations**
T_x	Transmitting node
R_x	Receiving node
$10\log_{10}^{\phi}$	Estimated SNR
ϕ	Power constraint
$(y_0, 0), \ldots (y_k, 0)$	2D representation of IoT nodes
D_n	Distance between two IoT nodes
I_0	Focal privacy level
P_T	Normalized power of T_x path loss
P_R	Normalized power of R_x path loss
$(P_R = P_R^*, \phi = 1)$	Utilized full duplex jamming
$(P_R = 0, \phi = \phi^*)$	Artificial noise from T_x
α	Exponent path loss
ψ_{SI}	Residual signal interference
ρ	Stabilized factor of large-scale-fading interference

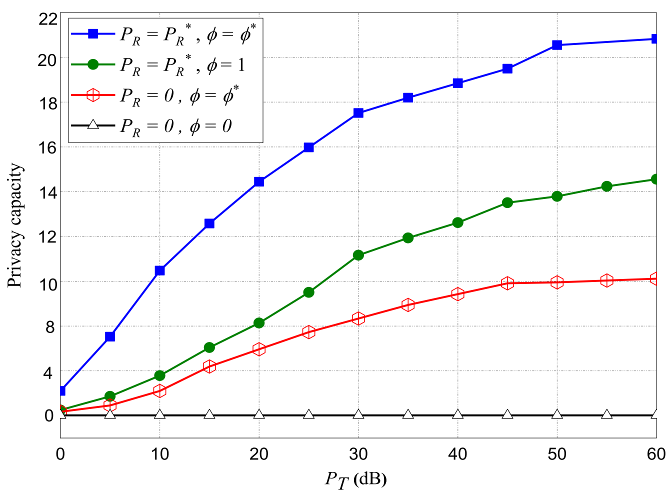

Fig. 2. Result of the performance of optimal jamming parameters on $\varepsilon_{\mathbf{T},\mathbf{R}}[I]$ as Eve utilizes OMF, while all transmitting smart devices are equipped with 4 antennas.

nodes to be positioned in 2-D pattern and represented them as $(y_0, 0), \ldots, (y_k, 0)$ considering $y_0 = 0$. Similarly, the existing distances between two bothering nodes are set as D_n with $D_{n+1} = 3$ m. Furthermore, we set the expected privacy capacity I_c at 0.2 bps/s/Hz, while the exponent of path loss is set as $\alpha = 2$ and the residual signal interference Ψ_{SI} at 15 dB. The simulation paramters and their deriavations are detailed in Table I.

In Fig. 2, a random realization of Eve's channel is utilized for the estimation of ϕ^0. The simulation compared $\varepsilon_{\mathbf{T},\mathbf{R}}[I]$ with respect to optimal and nonoptimal parameters of jamming. For this specific scenario, the result of the experiment indicates that a significant advantage is achieved while employing only full-duplex jamming $(P_R = P_R^*, \phi = 1)$ against utilizing AN from Tx only $(P_R = 0, \phi = \phi^*)$, however, a joint performance of both results shows a higher privacy improvement. For the simulation, we employed a total of 20 000 realizations of $\mathbf{T}$ and $\mathbf{R}$ while the privacy capacity is measured in b/s/Hz.

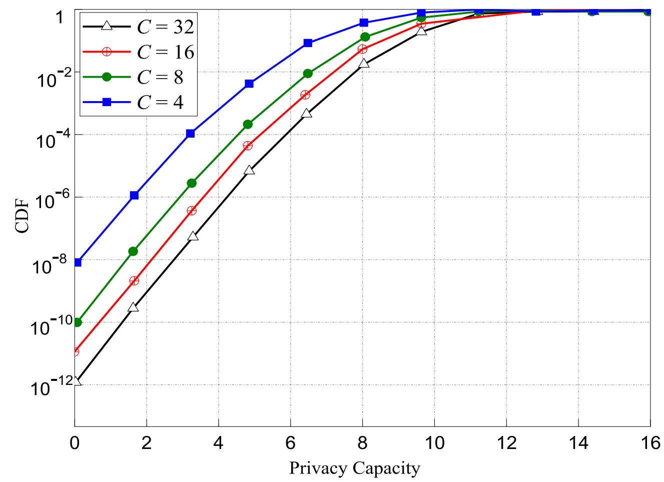

Fig. 3. Performance of Privacy CDF against several number of antennas.

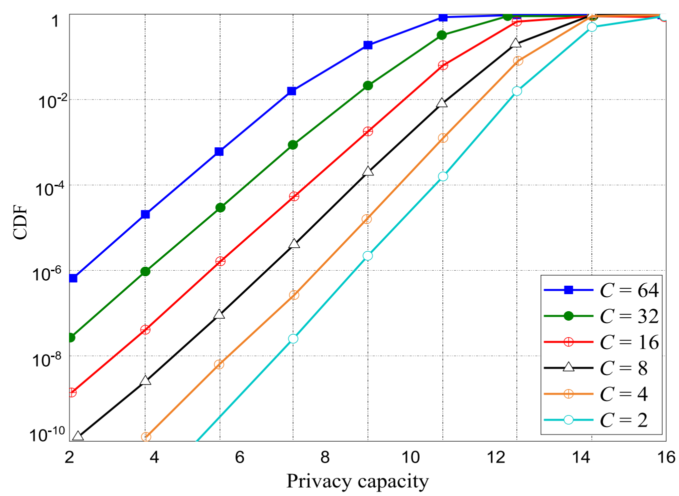

Fig. 4. Performance of Privacy CDF against several number of antennas of Eve.

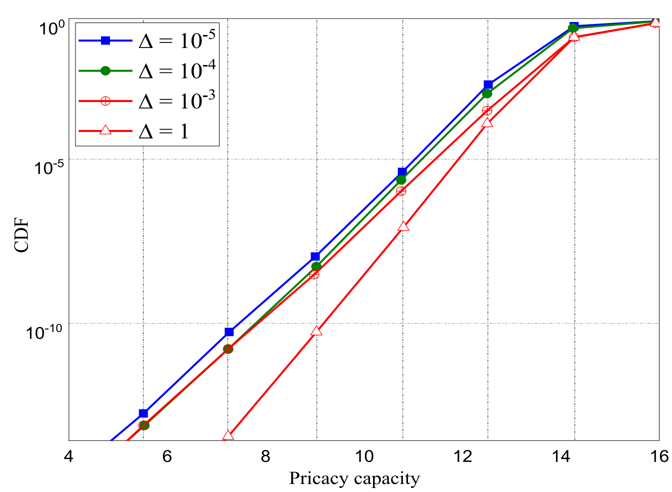

Fig. 5. Performance of Privacy CDF against several number Δ.

In Figs. 3–5, the following parameters, $B = C = A = 32$, $P_T = 60$ dB, $\rho = 10^{-3}$, $\alpha = 4$ and $P_R = 45$ dB are employed to examine the effect of different parameters on the privacy CDF. The results from the figures indicate that

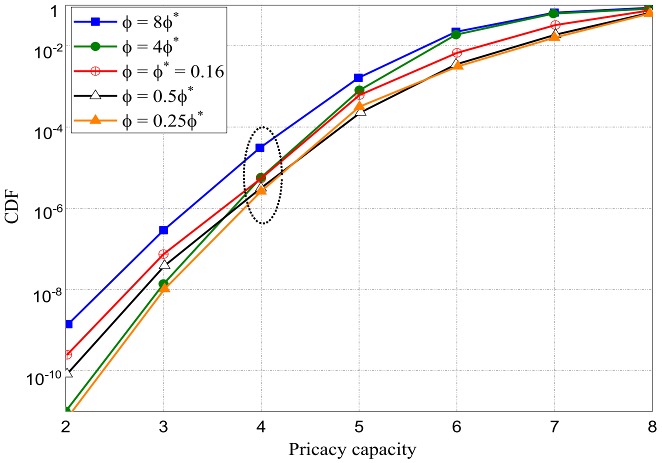

Fig. 6. CDF of $\mathcal{F}_I(i)$ using $\phi = 0.16$ optimal or nonoptimal ϕ with $i_0 = 3$.

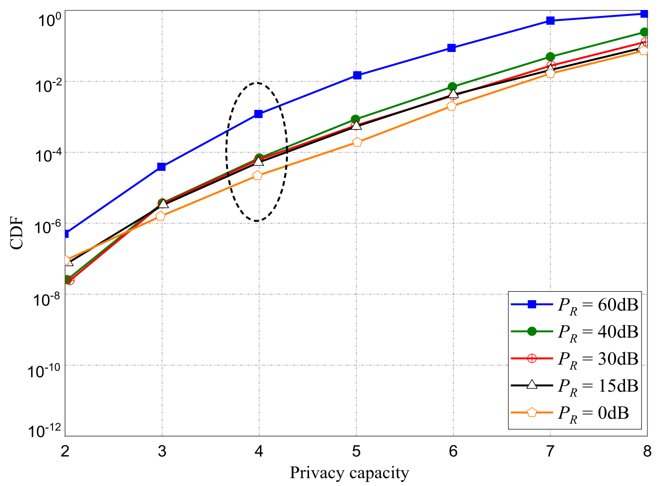

Fig. 7. CDF of $\mathcal{F}_I(i)$ using optimal $P_R = 40$ dB or nonoptimal P_R with $i_0 = 3$.

privacy is optimized as the number of antennas for each node is increased. Similarly, assuming increase is witnessed only at Eve's number of antennas, then Eve's effect on privacy is meager except a scenario where the antenna increase grows very large. Thus, for practical and effective optimization, Eve's number of antennas is expected not to exceed a certain amount, hence, optimization is performed with respect to the maximum number of antennas. To an extent, Eve's distance from the Transmitter has an insignificant effect. Assuming Eve utilizes OMF, then, a closed form of the CDF of privacy (I) is unavailable, while the privacy capacity is measured in bits/s/Hz.

Further, we set the following parameters as, $A = B = C = 32$, $P_T = 45$ dB, $\rho = 4 \times 10^{-3}$, $i_0 = 3$, $k = 8$ and $P_R^{\max} = 60$ dB. Utilizing P_R^* for all the curves, the performance of $\mathcal{F}_I(i)$ with optimal and nonoptimal P_R is shown in Fig. 6 while the performance of $\mathcal{F}_I(i)$ with the optimal and nonoptimal P_R is illustrated in Fig. 7. For all the curves, ϕ^* is utilized. In Fig. 8, the average privacy capacity is compared against P_T with respect to Eve's most harmful state with either BMF or OMF with either 8, 16, 24, or 80 number of antennas while the transmitting and receiving nodes share 8 antennas.

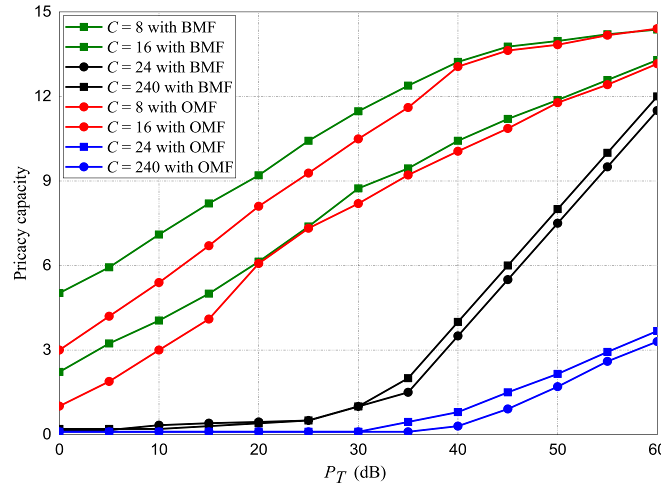

Fig. 8. Averaged privacy performance in four different setups with respect to varying C and Eve's filtering approach.

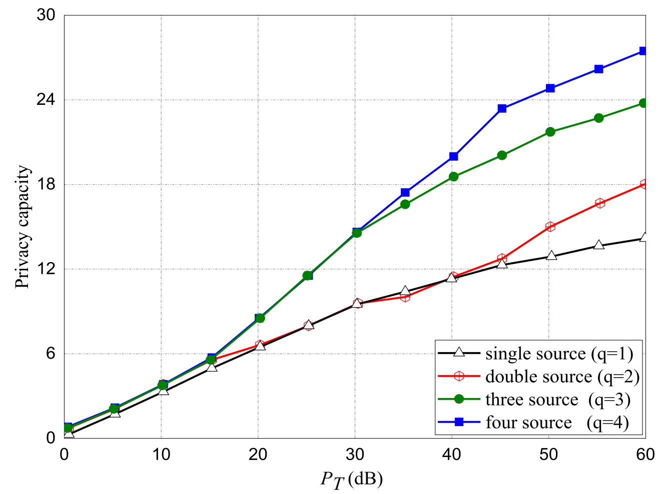

Fig. 9. Performance of averaged privacy for varying sources of information.

Assuming the number of Eve's antennas is even to that of the Transmitter and Receiver (i.e., $C = 8$) and Eve applies OMF, then, an efficient privacy capacity is realized. A slight decline is also witnessed when the number of antennas employed by Eve is doubled (i.e., $C = 16$), however, if Eve's number of antennas against that of the transmitting and Receiving node is tripled (i.e., $C = 24$), a substantial decline in privacy is witnessed. But, if Eve's number of antennas is ten times bigger than that of the Transmitter and Receiver (i.e., $C = 80$), privacy performance is substantially seen to decrease to zero.

Nevertheless, assuming BMF is used by Eve instead of OMF, then, a substantial privacy performance is still obtainable notwithstanding large number of Eve's antennas. Therefore, this establishes that by utilizing smart jamming from the receiving devices, an efficient privacy performance can be achieved.

With respect to the extension of multiple sources of information, the averaged privacy for varying sources of information is compared and presented in Fig. 9 The comparison indicates that at lower SNR scenario, small q is optimal,

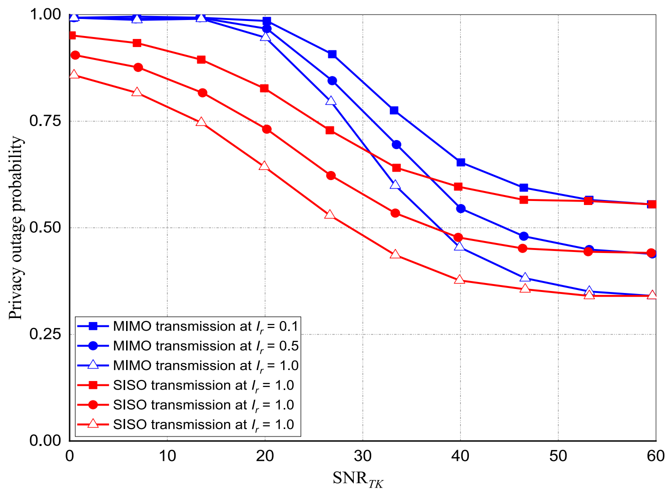

Fig. 10. Performance of privacy outage probability against jamming SNR for both single and multiple transmission scenarios.

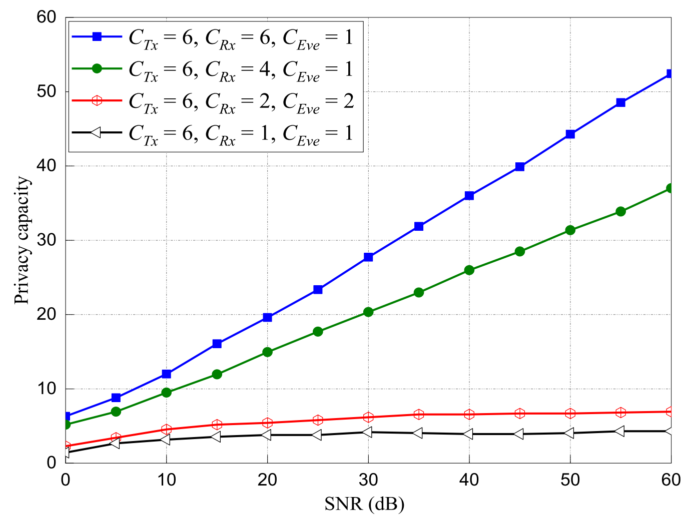

Fig. 11. Privacy capacity versus SNRs with varying number of antennas.

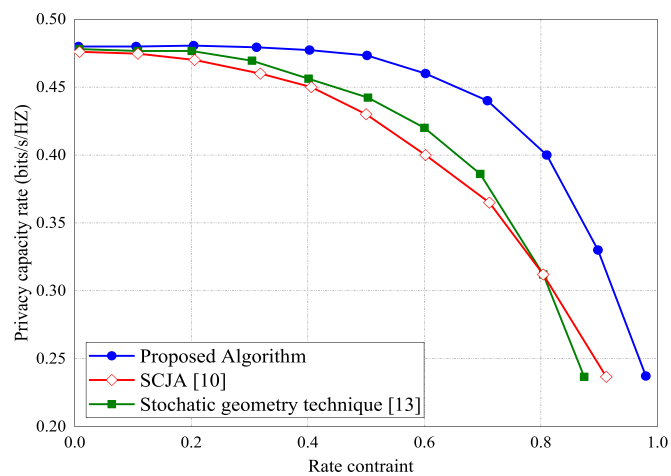

Fig. 12. Comparison of Rate constraint performance under different techniques.

while at higher SNR scenario, greater q is optimal. However, it is not very convenient applying this extension to the case of Eve performing BMF.

Comparing the privacy outage probability of varying transmission against the jamming SNR in Fig. 10, it is observed that privacy performance can be improved at the MIMO range of transmission only at low jamming power gain. However, privacy outage of the transmission at high jamming power gain witness a minimal noise which cannot be improved further because, the initial transmission is void of any jamming signal since both transmitting and receiving smart devices engaged their multiple antennas for a two-way data transmission. This is in contrast to the single input, single output (SISO) system which makes use of full duplex receivers. In this scenario, jamming signal is broadcasted by the receiving node in the initial transmission loop. Moreover, since the evaluations were performed in an interference-limited setting, and considering that there are multiple eavesdroppers in this scenario with the transmitter utilizing smart jamming approach, the results of the compared analysis at high jamming power gain is in line with the simulations considering jamming signal as a main factor.

Subject to the power constraint ϕ and setting the estimated SNR at $10\log_{10}\phi$, the varying SNR scaling of privacy capacity in the MIMOME system is compared and illustrated in Fig. 11. We considered three different combination of antennas as, $(C_{Tx}, C_{\text{Rx}}, C_{\text{Eve}})$ which represents the number of antennas utilized by the transmitter, receiver, and eavesdropper, respectively. In line with the results of [20], when $C_{\text{Rx}} = C_{\text{Eve}} = 1$, privacy capacities do not scale with SNR and convergence is witnessed at high SNR. Therefore, in this scenario, increasing the SNR might warrant in resource wastage which becomes a drawback. However, assuming the set number of transmitting antennas is $C_{Tx} > C_{\text{Eve}}$, then, this drawback can be tackled by increasing the number of receiver antennas C_{Rx} to realize $C_{\text{Rx}} > C_{\text{Eve}}$. Thus, our experiment indicates that for a MIMOME system, extending the number of the receivers antennas (i.e., $C_{\text{Rx}} = 4$ to $C_{\text{Rx}} = 6$) is also vital toward achieving optimal privacy capacities at the high SNR scheme.

In Fig. 12, rate constraint which assures QoS in IoT transmission is measured and experimented. Our proposed stochastic privacy optimization approach (SPOA) which is projected to mitigate the optimization problem in (38) is compared against other recently proposed technique, particularly the SCJA in [11] and the SGT in [14]. We deployed and generated data from a total of 80 IoT devices. Using an optimal achievable capacity of 0.6, we investigated the rate constraint and the result is presented in Fig. 12. Comparing the other techniques with our proposed algorithm, it is realized that the stochastic optimization technique we propose in this work is void of data rate degradation to the inherent IoT devices. The result shows that our algorithm performs better than the other two techniques as compared nonetheless vast rate constraints. Furthermore, the more severe the rate constraints becomes, the more difficult it is for the systems in the SCJA and SGT techniques to converge, however, convergence in the proposed SPOA algorithm is easily achievable.

Finally, the results of our experiment are compared with achievable privacy capacities of other previously proposed technique and the results presented in Fig. 13. The SCJA [11]

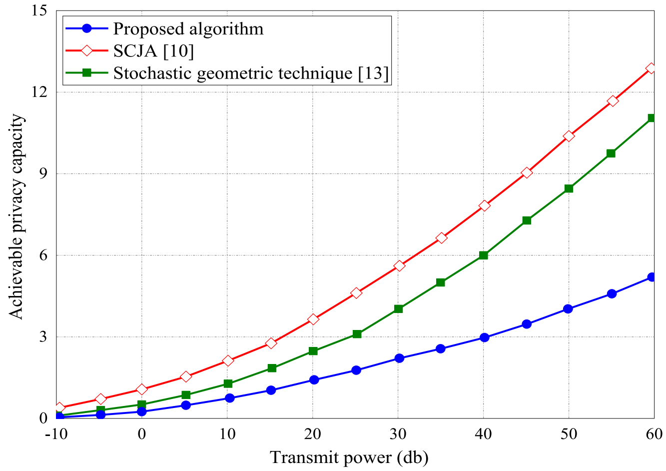

Fig. 13. Comparison of Rate constraint performance under different techniques.

which is applicable in MISOSE channel and the SGT [14] for MIMOME technique are used for comparison against the proposed SPOA algorithm. As anticipated, the capacity of the proposed technique scales better than the two compared technique. At $\phi < 0.1$ regime, all the compared techniques linearly increase with achievable rate for every increase of ϕ. However, as the rate progresses, the performance gap between the proposed algorithm and the compared techniques broaden due to high multiuser interference. However, the proposed SPOA algorithm exploits available resource allocation to fully avoid interference and to realize a significant and minimize power consumption during transmission.

V. Conclusion

In this article, a stochastic optimization algorithm for improved privacy capacity in an IoT mutltiuser scheme with the CSI of the multiple eavesdropper's unknown to both the transmitters and receivers has been investigated. With respect to the particular Eve which assumes the most dangerous position and may interrupt transmission at the network layer depending on the transmitters secured region. Two vital scenarios where Eve either performs its activities using OMF or BMF were considered. However, we realized that in a case where the Receivers utilizes smart jamming, then the BMF approach is inapplicable by Eve. We developed several mathematical models for the optimization of jamming parameters which are utilized by the Transmitters and Receivers for the two scenarios. Furthermore, the proposed algorithm indicated an optimal resilience eavesdropping attacks in a MIMOME transmission, as just a minor loss performance was witnessed with an increase in the number of transmitting antennas. Also, for each of the cases, we derived some essential closed-form expressions with respect to an interference restricted case for the privacy outage probability. Comparing the proposed SPOA against other recent algorithms, it is observed that the stochastic optimization technique is void of data rate degradation to the inherent IoT devices and by exploiting available resource allocation to fully avoid interference, it outperforms the SCJA and SGT and realizes a significant and minimized power consumption during transmission. Finally, the numerical analysis of our scheme with the optimized jamming parameters indicate a very significant privacy capacity enhancement against other existing methods.

References

[1] J. A. Stankovic, "Research directions for the Internet of Things," *IEEE Internet Things J.*, vol. 1, no. 1, pp. 3–9, Feb. 2014.

[2] Y. Kawamoto, N. Yamada, H. Nishiyama, N. Kato, Y. Shimizu, and Y. Zheng, "A feedback control-based crowd dynamics management in IoT system," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1466–1476, Oct. 2017.

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

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

[5] H. Wen, *Physical Layer Approaches for Securing Wireless Communication Systems*. New York, NY, USA: Springer, 2013.

[6] J. H. Anajemba, Y. Tang, J. A. Ansere, and C. Iwendi, "Performance analysis of D2D energy efficient IoT networks with relay-assisted underlaying technique," in *Proc. IECON 44th Annu. Conf. IEEE Ind. Electron. Soc.*, Washington, DC, USA, Oct. 2018, pp. 3864–3869.

[7] K. Wang, L. Yuan, T. Miyazaki, D. Zeng, S. Guo, and Y. Sun, "Strategic antieavesdropping game for physical layer security in wireless cooperative networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 10, pp. 9448–9457, Oct. 2017.

[8] X. Li and H.-N. Dai, "Friendly-jamming: An anti-eavesdropping scheme in wireless networks," in *Proc. Int. Symp. World Wireless (WoWMoM)*, Jun. 2017, pp. 1–3.

[9] J. Hu, N. Yang, and Y. Cai, "Secure downlink transmission in the Internet of Things: How many antennas are needed?"Ì *IEEE J. Sel. Areas Commun.*, vol. 36, no. 7, pp. 1622–1634, Jul. 2018.

[10] L. Hu, H. Wen, B. Wu, J. Tang, and F. Pan, "Adaptive secure transmission for physical layer security in cooperative wireless networks," *IEEE Commun. Lett.*, vol. 21, no. 3, pp. 524–527, Mar. 2017.

[11] G. Zheng, I. Krikidis, J. Li, A. P. Petropulu, and B. Ottersten, "Improving physical layer secrecy using full-duplex jamming receivers," *IEEE Trans. Signal Process.*, vol. 61, no. 20, pp. 4962–4974, Oct. 2013.

[12] X. Xu, B. He, W. Yang, X. Zhou, and Y. Cai, "Secure transmission design for cognitive radio networks with poisson distributed eavesdroppers," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 2, pp. 373–387, Feb. 2016.

[13] I. Stanojev and A. Yener, "Improving secrecy rate via spectrum leasing for friendly jamming," *IEEE Trans. Wireless Commun.*, vol. 12, no. 1, pp. 134–145, Jan. 2013.

[14] Y. Z. Y. Wang and X. Zhang, "Joint spectrum partition and performance analysis of full-duplex D2D communications in multi-tier wireless networks," *Comput. Mater. Continua*, vol. 61, no. 1, pp. 171–184, 2019.

[15] T.-X. Zheng, H.-M. Wang, J. Yuan, D. Towsley, and M. H. Lee, "Multi-antenna transmission with artificial noise against randomly distributed eavesdroppers," *IEEE Trans. Commun.*, vol. 63, no. 11, pp. 4347–4362, Nov. 2015.

[16] T.-X. Zheng and H.-M. Wang, "Optimal power allocation for artificial noise under imperfect CSI against spatially random eavesdroppers," *IEEE Trans. Veh. Technol.*, vol. 65, no. 10, pp. 8812–8817, Oct. 2016.

[17] Y. Yang, G. Scutari, D. P. Palomar, and M. Pesavento, "A parallel decomposition method for nonconvex stochastic multi-agent optimization problems," *IEEE Trans. Signal Process.*, vol. 64, no. 11, pp. 2949–2964, Jun. 2016.

[18] X. Zhang, X. Zhou, and M. R. McKay, "On the design of artificial-noise-aided secure multi-antenna transmission in slow fading channels," *IEEE Trans. Veh. Technol.*, vol. 62, no. 5, pp. 2170–2181, Jun. 2013.

[19] J. H. Anajemba, Y. Tang, C. Iwendi, A. Ohwoekevwo, G. Srivastava, and O. Jo, "Realizing efficient security and privacy in IoT networks," *Sensors*, vol. 20, no. 9, p. 2609, 2020,

[20] D. Chen *et al.*, "S2M: A lightweight acoustic fingerprints-based wireless device authentication protocol," *IEEE Internet Things J.*, vol. 4, no. 1, pp. 88–100, Feb. 2017.

[21] J. H. Anajemba, C. Iwendi, M. Mittal, and T. Yue, “Improved advance encryption standard with a privacy database structure for IoT nodes,” in *Proc. IEEE 9th Int. Conf. Commun. Syst. Netw. Technol. (CSNT)*, Gwalior, India, 2020, pp. 201–206, doi: 10.1109/CSNT48778.2020.9115741.

[22] J. H. Anajemba, Y. Tang, J. A. Ansere, and S. H. Sackey, “Efficient switched digital beamforming radar system based on SIMO/MIMO receiver,” in *Proc. Comput. Commun. IoT Appl. (ComComAp)*, Shenzhen, China, 2019, pp. 411–416, doi: 10.1109/ComComAp46287.2019.9018789.

[23] A. Behnad, M. B. Shahbaz, T. J. Willink, and X. Wang, “Statistical analysis and minimization of security vulnerability region in amplify-and-forward cooperative systems,” *IEEE Trans. Wireless Commun.*, vol. 16, no. 4, pp. 2534–2547, Apr. 2017.

[24] J. H. Anajemba, T. Yue, C. Iwendi, M. Alenezi, and M. Mittal, “Optimal cooperative offloading scheme for energy efficient multi-access edge computation,” *IEEE Access*, vol. 8, pp. 53931–53941, 2020, doi: 10.1109/ACCESS.2020.2980196.

[25] N. Yang, M. Elkashlan, T. Q. Duong, J. Yuan, and R. Malaney, “Optimal transmission with artificial noise in MISOME wiretap channels,” *IEEE Trans. Veh. Technol.*, vol. 65, no. 4, pp. 2170–2181, Apr. 2016.

[26] J. Yao, S. Feng, X. Zhou, and Y. Liu, “Secure routing in multihop wireless ad-hoc networks with decode-and-forward relaying,” *IEEE Trans. Commun.*, vol. 64, no. 2, pp. 753–764, Feb. 2016.

Joseph Henry Anajemba (Member, IEEE) is currently pursuing the Ph.D. degree in information and communication engineering with the College of Internet of Things, Department of Communication engineering, Hohai University, Nanjing, China, (under the Chinese University FULL scholarship).

His research interests include cellular wireless communications, antenna and V2V technology, 5G cellular networks and security, and several other IoT related areas.

Tang Yue (Member, IEEE) received his B.Eng. degree from Tianjin University, Tianjin, China, in 2004, the M.Eng. degree from Shanghai Spaceflight Technology Institute, Shanghai, China, in 2008, and the Ph.D. degree from Nanyang Technological University, Singapore, in 2014.

From September 2014 to July 2017, he worked with Hohai University, Nanjing, China, as an Assistant Professor, and from August 2017 to January 2020 as an Associate Professor. Since January 2020, he has been working with the Binjiang College, Nanjing University of Information Science and Technology, Nanjing, China, as an Associate Professor. His current research interests include DBF radar system, MIMO radar system, random space array based radar system, array signal processing, and antennas.

Celestine Iwendi (Senior Member, IEEE) received the second master’s degree in communication hardware and microsystem engineering from Uppsala University, Uppsala, Sweden, in 2008, ranked under 100 in the world university ranking, and the Ph.D. degree in electronics from the University of Aberdeen, Aberdeen, U.K., in 2013.

He is currently a Visiting Professor with Coal City University Enugu, Enugu, Nigeria. He is also an ACM Distinguished Speaker and a Senior Lecturer with the Bangor College China, Bangor, U.K., where he has strong teaching emphasis on communication, hands-on experience, willing-to-learn, and 20 years technical expertise and currently teaches with strong research emphasis in Engineering team Project, circuit theory, data networks and distributed systems, artificial intelligence, cybersecurity, machine learning, and control systems.

Dr. Iwendi is currently a board member of IEEE Sweden Section, a Wireless Sensor Network Chief Evangelist, a Researcher, and a Designer. He is a highly motivated and hardworking researcher with a Wireless Sensor Network Security book, and more than 100 publications. He is Fellow of the Higher Education Academy, U.K.

Pushpita Chatterjee (Member, IEEE) received the M.Tech. degree in computer engineering and the M.S. degree in computer and information science from the University of Calcutta, Kolkata, India, in 2004 and 2002, respectively, and the Ph.D. degree from the Indian Institute of Technology Kharagpur, Kharagpur, India, in 2013.

She was a Senior Research Lead with the SRM Institute of Science and Technology, (a Unit of SRM University, Chennai), Bengaluru, India, and a Research Consultant with Old Dominion University, Norfolk, VA, USA. She is currently a Research Consultant with Future Networking Research Group, Ton Duc Thang University, Ho Chi Minh City, Vietnam. She has a good number of publications to her credit in international journals, conferences, and books. Her research interests include smart health, machine learning, distributed and trust computing, wireless sensor networks, network security, and software-defined networking.

Desire Ngabo is currently pursuing the Ph.D. degree with the College of Computer Science and Electronics Engineering, Hunan University, Changsha, China.

He is an Assistant Lecturer with the University of Rwanda, Kigali, Rwanda, and an Assistant Research with the African Center of the Excellence in the Internet of Things. His research interests are Internet of Things, wireless sensor network, and embedded Computing systems.

Waleed S. Alnumay received the bachelor’s degree in computer science from King Saudi University, Riyadh, Saudi Arabia, in 1993, the master’s degree in computer science from the University of Atlanta, Atlanta, GA, USA, in 1996, and the Ph.D. degree in computer science from Oklahoma University, Norman, OK, USA, in 2004.

He is currently working as an Associate Professor of Mobile Networking with the Computer Science Department, King Saud University, Riyadh, Saudi Arabia. He has published research papers in reputed international conferences and journals. His main research interests are computer networks and distributed computing that includes but not limited to mobile ad-hoc and sensor networks, information-centric networking, and software-defined networking.