sensors

*Article*

# Realizing Efficient Security and Privacy in IoT Networks

**Joseph Henry Anajemba** [1], **Yue Tang** [1] , **Celestine Iwendi** [2], **Akpesiri Ohwoekevwo** [3], **Gautam Srivastava** [4,5,*,†] and **Ohyun Jo** [6,*]

[1] Department of Communication Engineering, College of Internet of Things, Hohai University, Nanjing 210098, China; herinopallazo@ieee.org (J.H.A.); 20141933@hhu.edu.cn (Y.T.)
[2] Department of Electronics BCC of Central South University of Forestry and Technology, Changsha 410004, China; celestine.iwendi@ieee.org
[3] Computer Science and Technology, Xidian University, Shaanxi 710126, China; gamaliel@stu.xidian.edu.cn
[4] Research Centre of Interneural Computing, China Medical University, Taichung 404472, Taiwan
[5] College of Information and Electrical Engineering, Asia University, Taichung 41354, Taiwan
[6] Department of Computer Science, College of Electrical and Computer Engineering, Chungbuk National University, Cheongju-si 28644, Korea
* Correspondence: srivastavag@brandonu.ca (G.S.); ohyunjo@chungbuk.ac.kr (O.J.)
† Department of Math and Computer Science, Brandon University, Brandon, R7A 6A9, Canada.

Received: 22 March 2020; Accepted: 30 April 2020; Published: 3 May 2020

**Abstract:** In recent times, security and privacy at the physical (PHY) layer has been a major issue of several communication technologies which comprise the internet of things (IoT) and mostly, the emerging fifth-generation (5G) cellular network. The most real-world PHY security challenge stems from the fact that the passive eavesdropper's information is unavailable to the genuine source and destination (transmitter/receiver) nodes in the network. Without this information, it is difficult to optimize the broadcasting parameters. Therefore, in this research, we propose an efficient sequential convex estimation optimization (SCEO) algorithm to mitigate this challenge and improve the security of physical layer (PHY) in a three-node wireless communication network. The results of our experiments indicate that by using the SCEO algorithm, an optimal performance and enhanced convergence is achieved in the transmission. However, considering possible security challenges envisaged when a multiple eavesdropper is active in a network, we expanded our research to develop a swift privacy rate optimization algorithm for a multiple-input, multiple-output, multiple-eavesdropper (MIMOME) scenario as it is applicable to security in IoT and 5G technologies. The result of the investigation show that the algorithm executes significantly with minimal complexity when compared with nonoptimal parameters. We further employed the use of rate constraint together with self-interference of the full-duplex transmission at the receiving node, which makes the performance of our technique outstanding when compared with previous studies.

**Keywords:** privacy capacity; IoT; 5G; physical layer security; MIMOME; jamming

## 1. Introduction

With the recent swift advancement of wireless communication networks and the advent of the fifth generation (5G) cellular network, interconnected devices are embedded into the environment through the IoT paradigm to enhance constant quality of service (QoS) and connectivity [1]. However, security of wireless transmissions has become a vital concern [2]. Unfortunately, in wireless technology, security risks are unavoidably inherent. Recently, network intrusion and eavesdropping, known as Eves, has become the major cradle of security risks in 5G wireless communications. The resources (e.g., battery) of most IoT devices (such as handheld/mobile communicating devices) are constrained, thus resulting in the devices having limited power for transmission, which may warrant the use of frailer cryptographic techniques as power savers. Therefore, devices may be prone to several attacks by some prevailing adversaries.

Security in wireless networks is typically employed through cryptographic methods using the upper layers of the open system interconnection (OSI) model [2,3]. However, these adversaries, which are considered as unauthorized users or network Eves, may infiltrate the network system, exhaust the networks bandwidth, taint the transmission data, reduce transmission performance, and inject data harms that thwart easy access of network data by authentic users. As a result of wireless link's unprotected nature, most wireless connectivity is susceptible which makes it easy for them to be attacked by jamming technology. These jamming attacks can result in a problem of Denial-of-Service (DoS), which can cause numerous other higher-layer security glitches in IoT and 5G technologies [3].

The 5G wireless network is predicted to activate the smart hyperlinked environment, enhancing the evolution and the growth of several sectors, such as energy and railway, where huge amounts of accessibility and reliability is essential. In contrast, this evolution may warrant that future mobile transmitting devices be exposed to cyber-attacks, which can destabilize system accessibility [4]. Because of the nature of wireless communications, vulnerability to Eve's attacks is inevitable. Therefore, transmission confidentiality cannot be guaranteed. In this paper, our work is focused on utilizing the networks physical layer to address countermeasures towards tackling confidentiality attacks in wireless network.

5G communications will headline what is being called the $4^{th}$ Industrial Revolution, where the mobile wireless broadband, pervasive sensing, and artificial intelligence (AI) promises to lead to major changes in academia, industry, and society itself. This coming generation of wireless communications globally focuses on many aspects as standards, policy, and infrastructure are still being shaped. 5G definitely promises to make the IoT network a reality.

In wireless networks, confidentiality attacks mostly stem from jamming. This is considered as the interruption of the flow in wireless transmissions by diminishing the signal-to-noise ratio (SNR) at the receiver end over a wireless signal's transmission interference. This clearly varies from normal network interferences because it explains a deliberate injection of wireless signals into an existing transmission with the intention of interrupting communications. However, network interference is said to be an accidental kind of disruption during transmission [5]. Recently, through conventional means, the implementation of different encryption approaches has been used to handle this security challenge at the advanced communications layers. That being said, a lot of attention has been drawn towards the security of the physical (PHY) layer lately. From a PHY security perspective, the authors of [6] investigated the impact of saturation nonlinear energy harvesting (EH) and activation threshold on the multiuser wireless powered sensor networks (WPSNs) from the physical layer security (PLS) perspective, and with respect to the generalized multiuser scheduling (GMS), they examined the improvement in the secrecy performance in WPNs. Their work explored and presented an exact closed-form expressions for secrecy outage probability (SOP) under linear EH (LEH), saturation nonlinear EH (SNEH), and saturation nonlinear EH with activation threshold (SNAT), respectively, through finding a solution for the maximization problem of secure energy efficiency (SEE).

The basis for tackling jamming attacks is hinged on Wyner's architecture. This architecture presented and demonstrated a wiretap channel when the channel of the eavesdropper (Eve) is a tainted version of the authentic receiver's channel, a secret message can be sent from the transmitter to the destination, while Eve is kept unaware of the content of the transmitted message [7]. The concept of privacy capacity is described as the optimal attainable rate of transmission of private data from the transmitting source (node) to its receiving destination. In [8], the Wyner's wiretap method was generalized by assuming the private message transmission over channels broadcast. Lately, substantial studies have analyzed privacy in wiretap channels under multiple antennas networks [9–11]. Particularly, the authors of [11,12] described the performance capacity of privacy in a multiple-input, multiple-output (MIMO) wiretap transmission channel. However, the authors of [13] investigated a joint effect of multiple jamming signals and noise at the eavesdropper in a MIMO network by assuming the implementation of antenna selection technique by the transmitter, while both the eavesdropper and legitimate receiver make use of a maximal-ratio combining scheme to achieve spatial diversity in reception. Their results show the effects of imperfect feedback and other key system parameters on the secrecy performance.

Basically, security at the PHY layer guarantees an optimal level of transmission privacy against Eve's as well as establishing an anticipated reception standard and quality as expected by the receiver(s). This research area comprises both signal processing analysis and theoretical information study. Although the latter involves more bounds and asymptotical limits, the former inclines towards innovating primal designs of algorithms and architectures to tackle security issues in a wireless network. Therefore, the focus and motivations of this paper is wrapped around the former with respect to Eve's growing quantity of transmitting antennas on privacy.

All the above-mentioned studies, except for [10,11], failed to explore a MIMOME scenario wish illustrates the effects of Eve's growing quantity of transmitting antennas on privacy. Although the authors of [6,11,13] proposed proficient privacy, their technique is reliant only on the assumption of a scenario where several factors such as the quantity of Eve's antennas that are accessible for transmitter usage for artificial noise subspace, are constrained in a MIMO and MIMOME network. By implication, it is essential that Eve's multiple antenna usage needs be considered and addressed. In this research, this is believed to be an issue of importance, therefore these problems are first extensively described, then techniques to tackle such problems are investigated and proposed.The main contributions of this research are as follows.

- A primal outlook into the investigation and optimization of wireless communications security with respect to IoT networks is presented.
- Using a mathematical model, an analysis of a novel transmission system where the eavesdroppers attack is tackled by injecting artificial noise which is transmitted by the receiver who has full-duplex aptitude with the same frequency in the channel, which reduces Eve's reception quality.
- Proposal of a new jamming mitigation technique and developed a sequential convex estimation and optimization (SCEO) algorithm for an optimized and enhanced privacy to solve the optimization problem in a three-node network where network users do not have knowledge of Eve's channel state information (CSI).
- The vulnerability of the proposed privacy enhancing scheme to Eve's increasing number of antennas is characterized and explored, while the performance of the proposed algorithm in a three-node network is established.
- Finally, because privacy capacity in a three-node network have been over-studied by several authors, this research is expanded to cover a MIMOME scenario, justifying its applicability in secured IoT network transmission.

The remainder of this paper is organized as follows. The privacy capacity model in wireless networks is described in Section 2. Review of recent works related to the research is presented in Section 3. System model is described in Section 4. Numerical analysis and results are provided in Section 5, and finally conclusions are outlined in Section 6.

## 2. Privacy Capacity Model in Wireless Networks

In this section, the privacy capacity model of the transmitting network is expressed. In the privacy capacity model of the network, it is assumed that the malicious node may eavesdrop the source as well as well as the receiver. However, in order to get a full use of the signals transmitted from the transmitter, the eavesdropper must be fully synchronized in the network. According to traditional privacy definitions in [8], the channel of communication can be modeled as a channel of broadcast in line with the wiretap channel as illustrated in Figure 1.

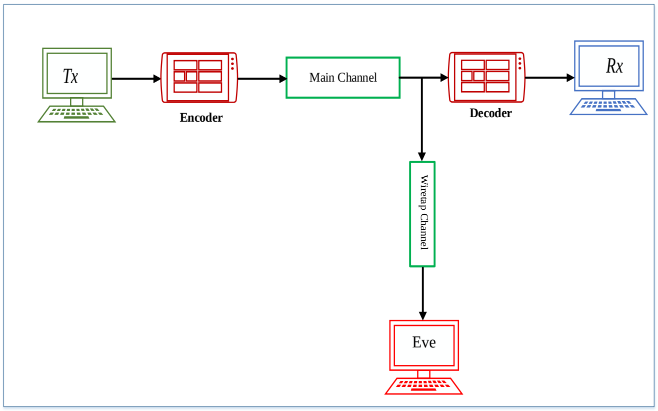

**Figure 1.** A Wiretap Channel for Privacy Capacity model

Considering the wiretap channel, the transmitting channel's message is represented as $a^n \in \mathrm{A}^n$ and is encoded and broadcasted as a codeword $c^m \in C^m$. The receiver $(R_x)$ and eavesdropper (Eve) receive $b^m \in \mathbf{B}^m$ and $e^m \in \mathrm{E}^m$, respectively. Eve's received information via her receiving signal is then modeled and described as in Equation (1),

$$I\left(e^m; a^n\right) = g\left(a^n\right) - g\left(a^n \left| e^m \right.\right) \tag{1}$$

where $I(e^m; a^n)$ represents the mutual information shared by the transmitter and the legitimate receivers, while $g$ is considered as the entropy. As long as Eve cannot decode any bit of the transmitted information, then perfect privacy is achieved. Thus, Equation (2),

$$I\left(e^m; a^n\right) = 0 \leftrightarrow g\left(a^n\right) = g\left(a^n \left| e^m \right.\right) \tag{2}$$

This implies that the quantity of uncertainty about Eve's private information is not altered after $e^m$ is received.

By definition, the probability of experiencing an error $P_i$ in the message estimation of message $a^n$, and $\hat{a}^n$ is defined as the estimate of $a^n$; therefore,

$$P_i = P\left\{a^n \neq \hat{a}^n\right\}. \tag{3}$$

Eve's rate of uncertainty about message $a^n$ is term as the rate of equivocation and can be described as

$$Q_i = \frac{1}{m} g\left(a^n \left| e^m \right.\right) \tag{4}$$

where

$$0 \leq Q_i \leq g(a^n)/m \tag{5}$$

Evidently, if $Q_i = g(a^n)/m$, then perfect privacy, which is related to perfect privacy rate $Q_s$, is realized. For each $\varepsilon > 0$, a particular $Q_s$ is assumed to be realizable, and there is a sequence of $(2^{mQ_s}, m)$ codes such that for any $m > m(\varepsilon)$ the following states are obtained.

$$\begin{cases} P_i < \varepsilon \\ \\ Q_s - \varepsilon < Q_i \end{cases} \tag{6}$$

The first state is the constraint for the realizable rate, whereas the second is the equivocation rate constraint which guarantees prefect privacy. In summary, privacy capacity $S_c$ is the optimal realizable rate of privacy in a network transmission. Thus, in [8], it is established that the difference between the main channel capacity $C_{mc}$ and the wiretap channel capacity $C_{wc}$ is the privacy capacity $S_c$, in other words,

$$S_c = (C_{mc} - C_{wc})^+, \tag{7}$$

as $(.)^+ \overset{\Delta}{=} \max(0, .)$, where negative rate is meaningless. Although Wyner demonstrated this for the distinct no-memory channel, the principle that the capacity of privacy is the difference of the capacity of the legitimate channel and that of the eavesdropper's is established to be accurate for several systems like in multiple-input, multiple-output (MIMO) set-ups [12,13].

*Notations*

We denoted the column vectors and matrices by boldface letters (both at upper and lower cases), while the determinant, inverse of a matrix and column-wise vectorization of the matrix **X** are all represented as $X^H, X^{-1}$, |X|, respectively. In a diagonal vectorization, Y is denoted as the column vector of y , whereas the random variable of y is represented as $\mathrm{C}_y[.]$ and the probability of event occurrence is denoted as $\mathrm{P}\{X\}$. Using the same probability space, we defined the random variables Y and $\mathrm{Y}_m$, if $\mathrm{Y}_m$ converges to Y, we transposed $Y_m \overset{a.s}{\to} Y$ as $m \to \infty$. We used $I$ to represent the matrix identity of supplied size, as $I(y; z)$ represents the information which is mutually and randomly transmitted between y and x variables.

## 3. Related Works

In a wireless network, jammers intentionally introduce radio frequency (RF) interference to distort wireless communications. This is achieved by occupying the transmitting channel and keeping it busy, thereby triggering the transmitter to withdraw each time it senses a busy wireless channel, or a tainted signal acknowledged at the receiver's end. In this section, in an attempt to understand the jamming attack on wireless networks, different kinds of jamming in wireless communications as proposed by several researchers are explored. Primarily, network jamming can occur in different ways based on the type of jammer. Therefore, different kinds of jammers and their jamming mechanisms are reviewed in this section.

The established secrecy capacity rate principle by Wyner in [8] preceded several other theoretical proposals by different researchers. So far, the wireless channels rate of secrecy has been explored from several perspectives like in [9,10]. The different perspectives explored are as follows, the fading channels secrecy [9–11], the analysis of Gaussian wiretap channels secrecy of [11], the multiple antenna systems secrecy [13–15], the broadcast channels secrecy [16], the analysis of secure degrees of freedom [17–21], and the secrecy of cooperative jamming techniques coupled with helpers or relays [22–29].

Additionally, the theoretical information [30] forms guarantees defined by secrecy capacity of the communication channel; the nodes that legitimate can also assume active approaches to improve their communication secrecy. One important approach for improving the secrecy of wireless communication was developed in [31]. The approach proposes that the transmitter (Alice) injects artificial noise into legitimate channels null-space together with the data signal. This scheme is intended to actively reduce the reception quality of any Eve's presence without altering the quality of legitimate receivers (Bobs) channel. Several other works [32,33] have also investigated this approach. Equipping Bob with the capacities of full-duplex radio aptitude, which enables him broadcast jamming noise counter to Eve, while both Bob and Eve attempt to acquire information from Alice [34,35] is another approach. The combination of the aforementioned two jamming approaches is investigated in most part of this study to attain secrecy at higher levels. Moreover, this combination was examined in [36], as it proposed a cooperative optimization algorithm to generate decent parameters for the transmission. Separately, two different sets of antennas are considered for broadcasting and for full-duplex reception. Meanwhile, the research did not fully consider the residual self-interference at Bob. Further, several other works were interested with comparable systems in [37,38]. The system proposed in [39] presents a scenario with Alice and Bob communicating simultaneously and are furnished with full-duplex radio with full consideration of residual self-interference. The study target was to discover the maximum beamforming transmit trajectories for artificial noise and signal considering some constraints of quality of service (QoS) with Eve's CSI recognizable to users. With Eve's exact CSI unrecognizable to the user in [40], a closed-form lower bound on the ergodic rate of secrecy is realized. The authors of [41,42] considered a case of a single-antenna Bob and multiple antenna base station coupled with a colluding and non-colluding single-antenna Eves. As an alternative to beamforming, an antenna selection scheme is used by the study and it is of the research assumption that Eves are dispersed in accordance to the process of Poisson point.

For cooperative relaying networks, several authors have also investigated different techniques for the security of systems physical layers [43]. In cooperative relaying networks, even destinations or relays are used as assistants to offer jamming signals to complicate the eavesdropper's transmission. This method is known as cooperative jamming. The noise-forwarding approach which was introduced in [24], and applied in a channel comprising of four-terminal relay-eavesdropper also considered a full-duplex relay, which independently transmits secret messages codewords which are targeted at complicating the eavesdropper's transmission. The authors of [44] investigated a two-stage cooperative jamming scheme (TSCS) which involves multiple relay nodes acting as the single-antenna's source node extension. The relays in this study do not transmit the information signals as they only function as a helper. However, for a single-antenna relay network, the authors of [45] proposed three different cooperative communication methods. On the other hand, for the second hop, they attempted to optimize secrecy by deriving a power allocation approach and its corresponding relay weights. The study in [46] investigated a decode-and-forward (DF) relays performance based on an optimal beamforming strategy; however, the investigation is limited because it only considered a transmission where the Eve monitors just a single connection linking the transmission destination and relay. The investigation of [47] was based on different privacy enhancing technologies (PETs) for IoT devices which have resulted in a much efficiency and convenience to our daily life. Their survey claim to have identified current state of improvement of the PETs in several turfs and also analyzed how the current technologies adhere with the modern legal ideologies and privacy criteria in curtailing the threats to privacy. A secured IoT-based healthcare system, which operates through the body sensor networks (BSN) architecture, was examined by the authors of [48]. The main focus of their system is to concurrently realize system robustness of transmission and efficiency within publicly transmitting IoT-based communication networks. Utilizing a vigorous utilize crypto-primitives, they constructed two communication schemes to ensure confidentiality in transmission and support entity authentication among smart objects. As most of the IoT data is relevant to personal privacy, it is necessary to pay attention to data transmission security. The authors of [49] investigated an IoT-oriented offloading method (IOM) which is enclave with privacy preservation to solve the problem of privacy in Cloudlet-enabled Wireless Metropolitan Area Networks (CWMAN). Their research and that of [50] adopted the non-dominated sorting differential evolution algorithm (NSDE) in order to optimize the multi-objective problem.

By contrast to the works analyzed above, the work in [51] proposed a cooperative jamming approach for a half-duplex two-hop wireless MIMO relay scheme where the eavesdropper can bug the channels throughout the phases of transmission. The study investigation considered both single and multiple streams of data transmissions. However, for jamming support, due to the absence of an "outer" helpers, the relay, destination, and source must depend on themselves. Whether the eavesdropper is in proximity to the source or the destination, the strategy guarantees that it is jammed. In this strategy, both the source and the destination nodes perform as provisional assistants for transmitting jamming signals throughout the phases of transmission where they are generally inactive.

In summary, the event of optimizing privacy without the users recognizing Eve's CSI is sparsely contained in literature; however, a few works like [52–57] gave more attention to the use of only enough energy to authenticate a particular QoS for Bob and is this energy is estimated in terms of signal-to-interference-plus-noise-ratio (SINR). Using the remaining energy, artificial interference is generated to jam Eve not minding the effect of Eve's location. This process is implemented in place of making attempts to optimize the rate of secrecy, which is impossible without the users having a knowledge of Eve's CSI [58,59]. Furthermore, as new telecommunication technologies emerge, the use of several security and privacy techniques proposed earlier becomes over exploited and obsolete; therefore, it is vital to develop advanced state-of-the-art techniques and algorithms that can mitigate against network jamming and eavesdropping attacks and ensure constant quality of service (QoS) in the network. Considering that this is the optimal focus of this research, therefore, the relevance of this research to cutting-edge telecommunication technologies like the IoT and 5G cellular network cannot be underestimated.

## 4. System Model

In this section, the system model is described. There are similarities in the model to what was given in [8]. For the set-up, a three-node-based wireless transmission is illustrated in Figure 2.

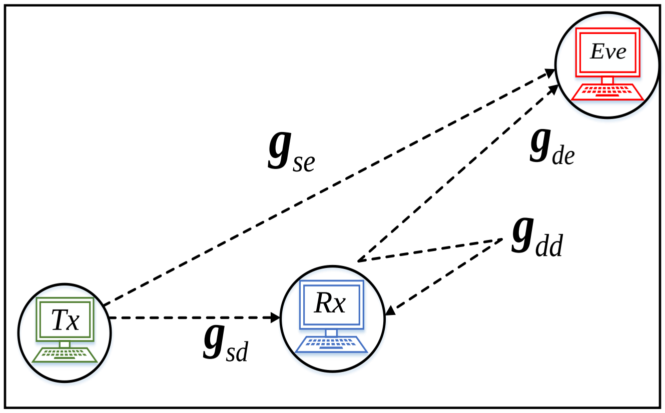

**Figure 2.** A single-antenna three-node wireless transmission with a full-duplex destination.

In the set-up, all three nodes are attached to a single transmitting antenna. The intention of the transmitter (Source) is to broadcast some private information to the receiver (Destination) while Eve (a passive eavesdropper) attempts to gain access to the sensitive private information. We assume that each link channel entails several $M$ orthogonal subcarriers and each subcarrier fading is flat. Tackling eavesdropping attacks in this set-up entails that artificial noise is broadcasted by $R_x$ with the same frequency and in the same channel, which reduces Eve's reception quality. Considering that this jamming attack operates at the same frequency and time in which information is transmitted from $T_x$ to $R_x$; thus, it is assumed that $R_x$ has full-duplex aptitude. It is well known that there is no perfect full-duplex system, therefore $R_x$ always manifests some level of residual self-interference.

Considering $y_s(x) \in {}^{Mx1}$ is the signal vector independent and identically distributed (i.i.d) zero mean cyphers and unit variance that the $T_x$ will be transmitting while $y_d(x) \in {}^{Mx1}$ is assumed to be the jamming noise vector of i.i.d. zero mean cyphers and unit variance the transmitter ($T_x$) will be transmitting. Thus, the signal vectors $R_x$ and Eve received can be individually described,

$$z_d(x) = \mathbf{g}_{sd} * \sqrt{\mathbf{p}_s} * y_s(x) + \sqrt{\delta}\mathbf{g}_{dd} * \sqrt{\mathbf{p}_d} * y_d(x) + \mathbf{m}_d(x), \tag{8}$$

$$z_e(x) = \mathbf{g}_{se} * \sqrt{\mathbf{p}_s} * y_s(x) + \mathbf{g}_{de} * \sqrt{\mathbf{p}_d} * y_d(x) + \mathbf{m}_e(x), \tag{9}$$

where ${}^{Mx1}$ comprises the vector, $\mathbf{g}_{sd}, \mathbf{g}_{se}, \mathbf{g}_{de}$, and $\mathbf{g}_{dd}$ are explicitly described in Figure 2, and $\mathbf{p}_s$ and $\mathbf{p}_d$ vectors, respectively, represent the power of transmission between the $T_x$ and $R_x$. $\mathbf{m}_d(x) \in {}^{Mx1}$ and $\mathbf{m}_e(x) \in {}^{Mx1}$ are considered as the mean of independent white Gaussian noise of zero and unit variance, respectively. The multiplication and square root are used as element-wise operators, and $\delta$ represents the attenuation factor of self-interference.

Denoting the superscript $(m)$ as a vector $m$th element, we formulate the respective signal-to-noise-ratios (SNRs) of the $m$th subcarrier at $R_x$ and Eve as

$$\gamma_d^{(m)} = \tfrac{A_m y_m}{1+B_m z_m} \text{and} \gamma_e^{(m)} = \tfrac{C_m y_m}{1+D_m z_m}, \tag{10}$$

where $A_m = \left|\mathbf{g}_{sd}^{(n)}\right|^2$, $B_m = \delta\left|\mathbf{g}_{dd}^{(n)}\right|^2$, $C_m = \left|\mathbf{g}_{se}^{(n)}\right|^2$, $D_m = \left|\mathbf{g}_{de}^{(n)}\right|^2$, $y_m = \mathbf{p}_s^{(m)}$ and $z_m = \mathbf{p}_d^{(m)}$. Recall that as stated earlier, Eve's CSI ($C_m$ and $D_m \forall m$) is only supposed to be recognizable by legitimate users in this Section.

Thus, the privacy capacity of this model is defined as

$$S_c(\mathrm{y}, \mathrm{z}) = \frac{1}{M} \sum_{m=1}^{M} \max\{0, \Delta S_m(y_m, z_m)\}, \tag{11}$$

where

$$\Delta S_m(y_m, z_m) = \log\left(1 + \gamma_d^{(m)}\right) - \log\left(1 + \gamma_e^{(m)}\right). \tag{12}$$

### *4.1. Formulated Optimization Problem*

In this subsection, our objective is to boost the privacy capacity of the scheme using power and rate constraints with cooperative power distribution between $T_x$ (source) and $R_x$ (destination). As compared with the conventional physical layer security techniques, the proposed SCEO and swift privacy rate optimization algorithms are suitable for the Internet of Things, because the optimization algorithms are energy efficient; therefore, the low-energy consumption necessities of IoT is enormously satisfied. Specifically, in a wireless channel transmission scheme, intrinsic noise is deployed which degrades the quality of the eavesdropper's received signal; thus, privacy in transmission is guaranteed with no cost of supplementary power. In summary, the application of the proposed technique in IoT technologies is low power capable as it does not necessitated the use of additional energy to guarantee privacy in transmission. The authors in [38] attempted to solve this low power problem through the bisection approach by swapping the source and destination powers optimizations, iteratively. However, in this work, we provided an improved solution by jointly assigning source and destination powers, thereby formulating the first optimization problem as (13):

$$\begin{aligned}
&\begin{matrix} max \\ x,y \end{matrix} \; \frac{1}{M} \sum_{m \in \Psi z} \left( \log(1 + \tfrac{A_m y_n}{1+B_m z_m}) - log(1 + \tfrac{C_m y_m}{1+D_m z_m}) \right) \\
&s.t. \frac{1}{M} \sum_{m \in \Psi z} \log(1 + \tfrac{A_m y_n}{1+B_m z_m}) \geq C_{sd} \\
&\sum_{m \in \Psi z} z_m \leq \mathbf{p}_d, z_m \geq 0 \forall m \in \Psi_z \\
&\sum_m y_m \leq \mathbf{p}_s, y_m \geq 0 \forall m \in \aleph \\
&z_m = 0, \forall m \in \Psi \overset{\perp}{\underset{z}{}}
\end{aligned} \tag{13}$$

where

$$\begin{aligned}
&\Psi_z = \Theta_z \cap \Phi \\
&\Theta_z = \left\{ m \,\middle|\, \tfrac{A_m}{1+B_m z_m} > \tfrac{C_m}{1+D_m z_m}, \forall m \in \aleph \right\} \\
&\Phi = \left\{ m \,\middle|\, \tfrac{A_m}{C_m} > \tfrac{B_m}{D_m}, \tfrac{B_m}{D_m} < 1, \forall m \in \aleph \right\} \\
&\Psi \overset{\perp}{\underset{z}{}} = \{ m \,| m \in \aleph, m \notin \Psi_z \}
\end{aligned} \tag{14}$$

The privacy capacity of our system is considered as the objective function, and the approximation is performed over the privacy capacity of the group of subcarriers which warrants a positive capacity of $\psi_z$. First, the rate constraint which guarantees the quality of service (QoS) of the network is considered. Although the techniques warrant data exchange or channel feedback between the authentic users, which can result in a slight rate performance degradation, typically IoT devices and applications have very low data rates. Therefore, this setback of low rate performance does not alter the adoption of the scheme in IoT operations. Second, the jamming mitigation power constraint which has its summation over the set of subcarriers $\psi_z$ is considered. This is due to the need to properly manage power so no power waste is experienced by subcarriers which might not guarantee a positive gain of privacy. Last, the third constraint which is the power constraint at Source is taken into consideration. Furthermore, the minimum expected rate is represented as $C_{sd}$, whereas $\mathbf{p}_s$ and $\mathbf{p}_d$ are set to represent the optimal sum of powers at Source and Destination.

With the aim of exploring the Karush–Kuhn–Tucker (KKT) conditions, we formulated the Lagrangian function of the problem as

$$\begin{aligned}
&\mathcal{L}(y, z, \lambda, \mu_y, \mu_z, v_y, v_z) = \\
&-\frac{1}{M} \sum_{m \in \psi_z} \left( \log(1 + \tfrac{A_m y_m}{1+B_m z_m}) - \log(1 + \tfrac{C_m y_m}{1+D_m z_m}) \right) \\
&-\mu_y^R \mathrm{y} - \mu_z^R \mathrm{z} + \mu_y (\sum_m y_m - \mathbf{p}_s) + v_z (\sum_{m \in \psi_z} y_m - \mathbf{p}_d) \\
&+\lambda \left( \tilde{C}_{sd} - \frac{1}{M} \sum_{m \in \psi_z} \log(1 + \tfrac{A_m y_m}{1+B_m z_m}) \right)
\end{aligned} \tag{15}$$

Considering the KKT conditions as

$$\begin{cases} \forall m \in \psi_z \begin{cases} \frac{\partial l}{\partial y_m} = -\varphi_m(y_m, z_m) - \frac{1}{M}\frac{A_m}{1+B_m z_m A_m y_m} - \mu_y(m) + v_y = 0 \\ \frac{\partial l}{\partial z_m} = -\varphi_m(y_m, z_m) - \frac{1}{M}\left(\frac{B_m}{1+B_m z_m A_m y_m} - \frac{B_m}{1+B_m z_m}\right) - \mu_z(m) + v_z = 0 \end{cases} \\ y_m \geq 0, \mu_y(m)0, y_m \mu_y(m) = 0, \forall m \in \aleph \\ z_m \geq 0, \mu_z(m)0, z_m \mu_z(m) = 0, \forall m \in \psi_z \\ v_y \geq 0, \sum_m y_m \leq \mathbf{p}_s, v_y \left(\sum_m y_m - \mathbf{p}_s\right) = 0 \\ v_z \geq 0, \sum_{\in \psi_y} y_m \leq \mathbf{p}_d, v_z \left(\sum_{\in \psi_y} y_m - \mathbf{p}_d\right) = 0 \\ \lambda \geq 0, \tilde{C}_{sd} \leq \frac{1}{M}\sum_{m \in \psi_z} \log(1 + \frac{A_m y_m}{1+B_m z_m}) \\ \lambda \left(\tilde{C}_{sd} - \frac{1}{M}\sum_{m \in \psi_z} \log(1 + \frac{A_m y_m}{1+B_m z_m})\right) = 0 \end{cases} \tag{16}$$

where

$$\varphi(y_m, z_m) = \frac{1}{M}\frac{A_m}{1+B_m z_m + A_m y_m} - \frac{1}{M}\frac{C_m}{1+D_m z_m + C_m y_m} \tag{17}$$

$$\vartheta_m(y_m, z_m) = \frac{1}{M}\left(\frac{B_m}{1+B_m z_m + A_m y_m}) - \frac{B_m}{1+B_m z_m} - \frac{D_m}{1+D_m z_m + C_m y_m} + \frac{D_m}{1+D_m z_m}\right) \tag{18}$$

Equations (16)–(18) above are the derivations of the KKT conditions which the Lagrangian function of the problem must satisfy for optimal solution to be achieved.

Apparently, attempting to find solution to the source-to-destination KKT conditions, a two-dimensional (2-D) bisection search estimation is performed on parameters $\lambda, \nu$, and $\mu$ as analyzed in Algorithm 1.

**Algorithm 1** Algorithm to solve problem (15) by solving the KKT conditions of (16), using **2-D** search approach for $\mu$, $\nu$, and $\lambda$.

```
Initialize:
$A_m, B_m, C_m, D_m, y_m, \forall m \in \aleph; \mathbf{p}_s; sd; C_{SOD}; \varepsilon, \zeta$.
Generate:
Initiate $\lambda$ = 0 therefore, eliminating the rate constraint), perform search for $\nu$ and $\mathbf{y}$.
Compute $C(y)$ as $sd$ capacity.
if $C(y) > C_{SOD}$ then
    revert y (meaning the rate constraint is achieved).
else    2-D search: perform search for $\nu$= 0 to satisfy power constraint till precision $\varepsilon$ is achieved.
    Perform search $\lambda > 0$ for every given $\nu$ to achieve the rate constraint until precision $\zeta$ is achieved.
    Given each pair of $\lambda$ and $\nu$, $y_m \geq 0$ is achieved as the solution of (24) for every $m \in \aleph$.
    revert y (meaning the rate constraint is achieved).
end if
```

Considering Algorithm 1 (bisection algorithm), the following set of equations which require solution will be encountered. These represent two nonlinear systems of equations:

$$\begin{cases} \frac{\partial l}{\partial y_m} = -\varphi_m(y_m, z_m) - \frac{\lambda}{M}\frac{A_m}{1+B_m z_m A_m y_m} - \mu_y(m) + v_y = 0 \\ \frac{\partial l}{\partial z_m} = -\varphi_m(y_m, z_m) - \frac{\lambda}{M}\left(\frac{B_m}{1+B_m z_m A_m y_m} - \frac{B_m}{1+B_m z_m}\right) - \mu_z(m) + v_z = 0 \end{cases}. \tag{19}$$

Finding solution for the KKT conditions which contains these two nonlinear equations appears to be unnerving; therefore, we consider applying the approach of sequential convex approximation.

### *4.2. Sequential Convex Approximation*

In attempt to realize a sequential convex approximation, the rate constraint and the objective function which constitute the optimization problem formulated in (13) is rewritten as (20) below.

$$
\begin{aligned}
& f(\mathrm{y},\mathrm{z}) = \frac{1}{M}\sum_{m\in\Theta z}\left(\log(1+\tfrac{A_m y_m}{1+B_m z_m}) - \log(1+\tfrac{C_m y_m}{1+D_m z_m})\right) \\
& = \frac{1}{M}\sum_{m\in\Theta z}(\log(1+B_m z_m + A_m y_m) + log(1+D_m z_m)) \\
& - \frac{1}{M}\sum_{m\in\Theta z}(\log(1+D_m z_m + C_m y_m) + log(1+B_m z_m)) \\
& = f_1(\mathrm{y},\mathrm{z}) + f_2(\mathrm{y},\mathrm{z})\frac{1}{M}\sum_{m}(\log(1+B_m z_m + A_m y_m)) \\
& -\frac{1}{M}\sum_{m}(\log(1+B_m z_m)) \geq C_{sd} \\
& f_3(\mathrm{y}) + f_4(\mathrm{y},\mathrm{z}) \geq C_{sd}
\end{aligned}
\tag{20}
$$

Evidently, $f_1$ and $f_4$ functions are concave while $f_2$ and $f_3$ functions are convex. Considering first-order Taylor series expansion of convex functions as the function's underestimator. By denoting the first-order Taylor series expansion of $f_2$ and $f_3$ around $(\mathrm{y}^{(h)}, \mathrm{z}^{(h)})$ points and expressing them, respectively, as $\tilde{f}_2^{(h)}, \tilde{f}_3^{(h)}$, the following was realized,

$$
\begin{aligned}
f_1(\mathrm{y},\mathrm{z}) + f_2(\mathrm{y},\mathrm{z}) &\geq f_1(\mathrm{y},\mathrm{z}) + \tilde{f}_2^{(h)}(\mathrm{y},\mathrm{z}) \forall \mathrm{y},\mathrm{z} \in {}^{M} \\
f_4(\mathrm{y},\mathrm{z}) + f_3(z) &\geq f_4(\mathrm{y},\mathrm{z}) + \tilde{f}_3^{(h)}(z) \forall \mathrm{y},\mathrm{z} \in {}^{M}
\end{aligned}
\tag{21}
$$

where

$$
\begin{aligned}
& \tilde{f}_2^{(h)}(\mathrm{y},\mathrm{z}) = f_2(\mathrm{y}^{(h)},\mathrm{z}^{(h)}) + \nabla f_2(\mathrm{y}^{(h)},\mathrm{z}^{(h)})^R(\begin{bmatrix} \mathrm{y} \\ \mathrm{z} \end{bmatrix} \\
& - \begin{bmatrix} \mathrm{y}^{(h)} \\ \mathrm{z}^{(h)} \end{bmatrix}) \\
& \tilde{f}_3^{(h)}(\mathrm{z}) = f_3(z^{(h)}) + \nabla f_3(z^{(h)})^R(\mathrm{z} - \mathrm{z}^{(h)}) \\
& \nabla f_2(y,z) = -\frac{1}{M}\begin{bmatrix} \frac{C_1}{1+D_1 z_1 + C_1 y_1} \\ \vdots \\ \frac{C_M}{1+D_M z_M + C_M y_M} \\ \frac{D_1}{1+D_1 z_1 + C_1 y_1} + \frac{B_1}{1+B_1 z_1} \\ \vdots \\ \frac{D_M}{1+D_M z_M + C_M y_M} + \frac{B_M}{1+B_M z_M} \end{bmatrix} \\
& \nabla f_3(z) = -\frac{1}{M}\begin{bmatrix} \frac{B_1}{1+B_1 z_1} \\ \vdots \\ \frac{B_M}{1+B_M z_M} \end{bmatrix}
\end{aligned}
\tag{22}
$$

Based on work done in [34] and assuming $\frac{B_m}{D_m} < 1$ we further simplify $\Theta_z$ and obtain

$$\begin{aligned}
&\Theta_z = \left\{ m \,\middle|\, z_m \geq 0, \tfrac{A_m}{1+B_m z_m} > \tfrac{C_m}{1+D_m z_m}, \forall m \in \aleph \right\} \\
&= \{ m \,|\, (B_m C_m - A_m D_m) z_m > A_m - C_m, \forall m \in \aleph \} \\
&= \left\{ m \,\middle|\, z_m \geq \tfrac{A_m - C_m}{B_m C_m - A_m D_m}, 1 > \tfrac{A_m}{C_m} > \tfrac{B_m}{D_m}, \forall m \in \aleph \right\} \\
&\cup \left\{ m \,\middle|\, z_m \geq 0, 1 < \tfrac{A_m}{C_m} > \tfrac{B_m}{D_m}, \forall m \in \aleph \right\}
\end{aligned} \tag{23}$$

Thus, following iteration $h$, we formulate the optimization problem as follows,

$$\begin{aligned}
&\max_{y,z} \; f_1(y,z) + \tilde{f}_2^{(h)}(y,z) \\
&s.t. f_4(y,z) + \tilde{f}_3^{(h)}(z) \geq C_{sd} \\
&\sum_m z_m \leq \mathbf{p}_d, z_m \geq 0 \forall m \in \aleph \\
&z_m = 0 \forall m \in \left\{ m \,\middle|\, \tfrac{A_m}{C_m} < \tfrac{B_m}{D_m} < 1, \forall m \in \aleph \right\} \\
&\cup \left\{ m \,\middle|\, \tfrac{B_m}{D_m} > 1, \forall m \in \aleph \right\} \\
&z_m \geq \tfrac{A_m - C_m}{B_m C_m - A_m D_m} \forall m \in \left\{ m \,\middle|\, 1 > \tfrac{A_m}{C_m} > \tfrac{B_m}{D_m}, \forall m \in \aleph \right\} \\
&\sum_m y_m \leq \mathbf{p}_s, y_m \geq 0 \forall m \in \aleph
\end{aligned} \tag{24}$$

It is observed that a convex optimization problem occurs at each point of iteration. This attempts to optimize a lower bound on the primal objective function and guarantees the rate constraint. As the iterative Algorithm reaches convergence, a decent approximation on the optimal values is expected. The optimization process is detailed in Algorithm 2.

**Algorithm 2** Sequential Convex Estimation Optimization Algorithm for solving optimization problem.

```
Initialize:
$(A_m, B_m, C_m, D_m) : \forall_m \in \aleph, \mathbf{p}_d, \mathbf{p}_s, C_{sd}, \zeta.$
Generate:
$y^{(0)} = \frac{1}{M}\mathbf{p}_s 1_M$
$z^{(0)} = \frac{1}{|\Theta_x|}\mathbf{p}_d \mathbf{a}(i) = 1$
if $(i \in \Theta_x)$
else $\mathbf{a}(i) = 0, t = 1$
While True do
end if
    Perform the convex optimization problem in (18) to realize $y^{(t)}$ , $z^{(t)}$,
    if ($\left\| [y^{(t)}; z^{(t)}] - [y^{(t-1)}; z^{(t-1)}] \right\| < \zeta$) then
        break.
    else
        $t = t + 1$
    end if
end
return $y^{(t)}$ , $z^{(t)}$;
```

### *4.3. Optimization of Swift Privacy Rate in a MIMOME*

Considering a network scenario where multiple eavesdroppers operate, the first assumption in realizing a swift privacy rate will be that Eve has full knowledge of her covariance matrix of noise and interference $(\mathbf{M}_E)$ just as she has full knowledge of all her entire CSIs (as earlier stated); then, she can make use of the optimal receiving antenna and her achievable rate would be derived as

$$R_{TE} = \log \left| \mathbf{M}_E + a\mathbf{A}_1 \mathbf{Z}_r \mathbf{A}_1^G \right| - \log |\mathbf{M}_E| \tag{25}$$

where

$$\mathbf{M}_E = \mathbf{I} + \frac{aPm}{A_{Tx} - r} \mathbf{A}_2 \mathbf{A}_2^G + \frac{eP_B}{A_{Rx}} \mathbf{B}\mathbf{B}^G \tag{26}$$

Then, the swift realizable privacy rate would be expressed as

$$P_R = (R_{TR} - R_{TE})^+ \tag{27}$$

However, for a multiple-input multiple-output multiple-antenna eavesdropping (MIMOME) system, assuming there is a constraint on the number of Eve's antenna $(A_E)$, one major issue of the system will be on how can to optimize the parameters of the transmission in such a way that Eve's interference in the transmission is made difficult. This becomes our focus in this subsection.

In this MIMOME system, if there is great increase in of $(A_E)$, the artificial noise does not have a significant impact on the rate of transmission between $T_x$ and Eve $(R_{TE})$. Therefore, the assumption in this subsection is that there is a constraint on Eve's maximum number of antennas; therefore, for the reason of optimization, a worst case is assumed, and thus this maximum number of antennas is considered as $(A_E)$.

To achieve this optimization, $T_x$ and $R_x$ cannot utilize the swift CSI at Eve, so as earlier mentioned, $P_R$ is inappropriate for this optimization. From some previous research [6,13,18], it is observed that Eve's symptotic rate is a decent approximation to the tangible rate; thus, we adopted this fact in order to achieve optimization. Suppose that the we make no assumption on the realizable random parameter $(r)$ and assuming that $\mathbf{z}_r$ is a vector encompassing the transverse elements of $\mathbf{Z}_r$, and $(A_E)$ is discreetly huge. Then, by rewriting (26), we obtained

$$\begin{aligned} R_{TE} &= \log \left| \mathrm{I} + \tfrac{aPm}{A_{Tx}-r} \mathrm{A}_2 \mathrm{A}_2^G + \tfrac{eP_B}{A_{Rx}} \mathrm{B}\mathrm{B}^G + a\mathrm{A}_1 \mathrm{z}_r \mathrm{A}_1^G \right| \\ &- \log \left| \mathrm{I} + \tfrac{aPm}{A_{Tx}-r} \mathrm{A}_2 \mathrm{A}_2^G + \tfrac{eP_B}{A_{Rx}} \mathrm{B}\mathrm{B}^G \right| \\ &= \log \left| \mathrm{I} + \mathrm{K}_3 \bar{\Theta}_3 \mathrm{K}_3^G \right| - \log \left| \mathrm{I} + \mathrm{K}_4 \bar{\Theta}_4 \mathrm{K}_4^G \right|, \end{aligned} \tag{28}$$

as $K_3$ and $K_4$ are expanded as $K_3 = \frac{1}{\sqrt{A_E}} [\mathrm{A}_1, \mathrm{A}_2\mathrm{A}_3]$, and $K_4 = \frac{1}{\sqrt{A_E}} [\mathrm{A}_2, \mathrm{B}]$. where

$$\bar{\Theta}_3 = A_E \text{trans} \left( \left[ az_r^P, \tfrac{aP_m}{A_{Tx}-r} 1 A_{Tx} - r, \tfrac{bP_B}{A_{Rx}} 1 A_{Rx} \right] \right), \tag{29}$$

$$\bar{\Theta}_4 = A_E \text{trans} \left( \left[ \tfrac{aP_m}{A_{Tx}-r} 1 A_{Tx} - r, \tfrac{bP_B}{A_{Rx}} 1 A_{Rx} \right] \right), \tag{30}$$

Deriving from the approximation of $R_{TE}$, an objective function which entails the approximation of $P_R$ is proposed. Note that the proposed objective function does not depend on the CSI of Eve; however, it considers the approximate swift rate of Eve. Likewise, as it is assumed that the transmitter and receiver has full knowledge of the null space $(\mathbf{G})$, the receivers exact rate is applied but not in its asymptotic form. The objective function is expressed as follows,

$$\begin{aligned} & h(\mathbf{z}_r, P_m, P_B) = -\log\left|\mathbf{M}_B + \mathbf{G}\mathbf{V}_1\mathbf{Z}_r\mathbf{V}_1^G\mathbf{G}^G\right| + \log|\mathbf{M}_B| \\ & + A_E\Omega\left(\bar{\beta}_3, \bar{\Theta}_3, \bar{\sigma}_3\right) - A_E\Omega\left(\bar{\beta}_4, \bar{\Theta}_4, \bar{\sigma}_4\right), \end{aligned} \tag{31}$$

where $\mathbf{M}_B$ implies that the receiver has full knowledge of her covariance matrix of noise and interference, $\bar{\beta}_3 = \frac{A_{Tx}+A_{Rx}}{A_E}$, $\bar{\beta}_4 = \frac{A_{Tx}-r+A_{Rx}}{A_E}$, while $\bar{\sigma}_3$ and $\bar{\sigma}_4$ are solutions to the formulated problem. In order to optimize the swift privacy rate, we proposed an optimization problem as stated below.

$$\begin{aligned} & \overset{\min}{r}\ \mathbf{z}_r, \overset{\min}{P_m}, P_B\, h\left(\mathbf{z}_r, P_m, P_B\right) \\ & \text{s.t.} \sum_{i=1}^{r} \mathbf{z}_r(i) + P_m \leq P_A^{\max} \\ & \mathbf{z}_r(i) \geq 0, \forall i = 1, ..., r \\ & P_m \geq 0 \\ & 0 \leq P_B \leq P_B^{\max} \end{aligned} \tag{32}$$

In the optimization problem above, the constraints are in their convex form; nevertheless, $h(.)$ is yet to assume a convex form. We can achieve this by rewriting the function

$$\begin{aligned} & h(\mathbf{z}_r, P_m, P) = -\log\left|\mathbf{M}_B + \mathbf{G}\mathbf{V}_1\mathbf{Z}_r\mathbf{V}_1^G\mathbf{G}^G\right| + \log|\mathbf{M}_B| \\ & + A_E\bar{\beta}_3 v_{\Theta_3}(\bar{\sigma}_3) - A_E\bar{\beta}_4 v_{\Theta_4}(\bar{\sigma}_4) \\ & + A_E\log\left(\frac{\bar{\sigma}_4}{\bar{\sigma}_3}\right) + A_E\left(\bar{\sigma}_3 - \bar{\sigma}_4\right)\log(c) \\ & = -\log\left|\mathbf{M}_B + \mathbf{G}\mathbf{V}_1\mathbf{Z}_r\mathbf{V}_1^G\mathbf{G}^G\right| + \log|\mathbf{M}_B| \\ & + \sum_{k=1}^{N_{\bar{\Theta}_3}} \log\left(1 + \bar{\sigma}_3(\bar{\Theta}_3)k, k\right) - \sum_{k=1}^{N_{\bar{\Theta}_4}} \log\left(1 + \bar{\sigma}_4(\bar{\Theta}_4)k, k\right) \\ & + A_E\log\left(\frac{\bar{\sigma}_4}{\bar{\sigma}_3}\right) + A_E\left(\bar{\sigma}_3 - \bar{\sigma}_4\right)\log(c) \end{aligned} \tag{33}$$

From Equation (33), we can linearize $+\sum_{k=1}^{N_{\bar{\Theta}_3}} \log\left(1 + \bar{\sigma}_3(\bar{\Theta}_3)k, k\right)$, which is the convex form of $h(.)$ at every iteration point of the optimization algorithm using the expansion method of first-order Taylor series. Similarly, we can resolve the reliance state of $h(.)$ on the $\bar{\sigma}_3, \bar{\sigma}_4$ parameters by making them constant with respect to their values and the upgrading them at the end to achieve the following,

$$1 - \bar{\sigma}_i^{j+1} = \frac{\bar{\beta}_i\bar{\sigma}_i^{j+1}}{N_{\bar{\Theta}_i}} \sum_{k=1}^{N_{\bar{\Theta}_i}} \frac{(\bar{\Theta}_i^{j+1})k, k}{1 + \bar{\sigma}_i^{j+1}(\bar{\Theta}_i^{j+1})k, k}, i = 3, 4. \tag{34}$$

note that $j+1$ represents the parameter value at $j+1$ iteration. Thus, we optimized the preceding convex function at $j$ iteration,

$$\begin{aligned} & g^j(\mathbf{y}_r) = -\log\left|\mathbf{M}_B + \mathbf{G}\mathbf{V}_1\mathbf{Z}_r\mathbf{V}_1^G\mathbf{G}^G\right| \\ & - \sum_{k=1}^{N_{\bar{\Theta}_4}} \log\left(1 + \bar{\sigma}_3^j(\bar{\Theta}_4)k, k\right) + \left(\mathbf{y}_r - \mathbf{y}_r^j\right)^J \nabla_{\mathbf{y}_r} f^j \Big|_{\mathbf{y}_r = \mathbf{y}_r^j}, \end{aligned} \tag{35}$$

denoting $\mathbf{y}_r = \left[\mathbf{z}_r^J, P_m, P_B\right]^J$ and $f^j(\mathbf{y}_r) = \log|\mathbf{M}_B| + \sum_{k=1}^{N_{\bar{\Theta}_3}} \log\left(1 + \bar{\sigma}_3^j(\bar{\Theta}_3)k, k\right)$. Recall that terms that are constant were not used in (25) because they do not have any effect in the optimization. However, at this point, $h(.)$ has assumed a convex function and we can then optimize it using the preceding optimization

$$\begin{aligned}
&\mathbf{y}_r^{j+1} = \overset{\arg\min}{\mathbf{y}_r} \; g^j(\mathbf{y}_r) \\
&\text{s.t.} \sum_{i=1}^{r} \mathbf{z}_r(i) + P_m \leq P_A^{\max} \\
&\mathbf{z}_r(i) \geq 0, \forall i = 1, \ldots, r \\
&P_m \geq 0 \\
&0 \leq P_B \leq P_B^{\max}.
\end{aligned} \tag{36}$$

Similarly, at this point, if any possible values of $r$ is deployed, an optimal output will be recorded. The summary of our proposed optimization procedure can be seen in Algorithm 3. Although different optimization methods to tackle this kind of problem were proposed in [13,18] comparatively, these methods give almost similar outcome, nonetheless, our proposed Algorithm 3 significantly executes with minimal complexity. Our figures illustrate the efficiency and out-performance of our swift optimization algorithm as compared with nonoptimal parameters.

**Algorithm 3** Swift privacy rate optimization algorithm.

```
Input actual:
$\varepsilon$, $\bar{\sigma}_3^0$, $\bar{\sigma}_4^0$, and initiate $h^{\min}= 0$
for $r = 1 : A_{Tx}$ do
    Set $\mathbf{y}_r$ to satisfy the constraints
    while $\frac{\left\|\mathbf{y}_r^j - \mathbf{y}_r^{j-1}\right\|}{\left\|\mathbf{y}_r^{j-1}\right\|} > \varepsilon$ do
        execute (28) till $\mathbf{y}_r^{j+1}$ is realized
        execute (25) using $\mathbf{y}_r^{j-1}$ till $\bar{\sigma}_3^0$ , $\bar{\sigma}_4^0$ is updated
        $j = j + 1$.
    end while
    if $h\left(\mathbf{y}_r^j\right) < h^{\min}$ then
        $h^{\min} = h\left(\mathbf{y}_r^j\right)$
        $\mathbf{y}^{\min} = \mathbf{y}_r^j$
    end if
end for
Revert $\mathbf{y}^{\min}$.
```

## 5. Numerical Analysis and Results

In this section, MATLAB simulation results based on our proposed SCEO algorithm and the Swift privacy rate optimization algorithm is presented. Our investigations show that the magnitudes of all transmission channels are distributed in a Rayleigh form with an even unit of mean square, while the attenuation factor of the transmission self-interference $\rho$ is set to be 0.8, except where slight changes are required. The transmission power constraints were set at $20db$ except where otherwise stated.

### *5.1. Realized Privacy Capacity*

We performed a transmission performance evaluation for a three-node transmission under power and rate constraints as shown in Figures 3 and 4. A comparison of three separate transmission scenarios with respect to the privacy capacity of their transmissions is shown in the experiment.

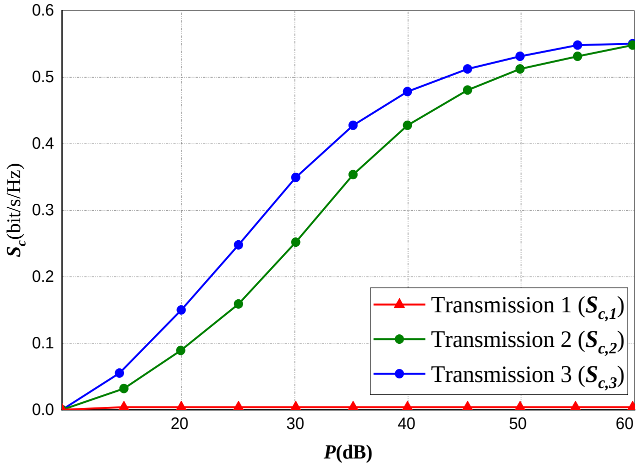

**Figure 3.** Realized privacy capacity against eavesdroppers under power and rate constraints.

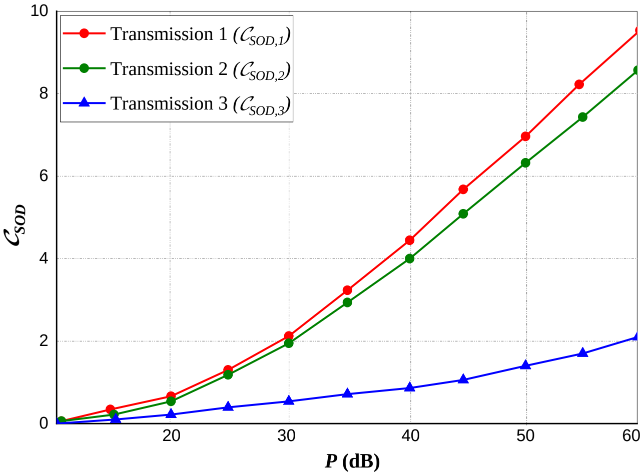

**Figure 4.** Realized privacy capacity for Source-to-Destination $(C^*_{SOD} = 0.8C_{SOD,1})$ transmission under power and rate constraints.

Figure 3 indicates privacy capacity against Eve, whereas Figure 4 represents the data rate of the transmission between the source and destination *(Source-to-Destination)* specifically realizing for the entire $A_m < C_m, \forall m \in \aleph$. This clearly implies that, for the entire set of subcarriers, the Eve's channel is stronger from the Source $(T_x)$ than the Destination $(R_x)$ has from the Source.

For Transmission 1 (the first transmission scenario), at the Source and Destination terminals, data rate is optimized subject to power constraints. However, this occurs without the constraint for privacy capacity. The subsequent obtainable data rate is signified by $C_{SOD,1}$. On the other hand, as expected for this channel, the subsequent privacy capacity $S_{c,1}$ is realized as zero.

For Transmission 2, the transmissions privacy capacity is optimized subject to power constraints at *Source* and *Destination* likewise a rate constraint of *Source-to-Destination*. Setting the lesser bound on the rate (i.e., the constrained rate) at $C^*_{SOD} = 0.8C_{SOD,1}$, the equivalent rate realized at the channel transmission is signified by $C_{SOD,2}$, as anticipated, the curve is vague from that of $C^*_{SOD}$. $S_{c,2}$ represents the subsequent attained transmission privacy capacity and it is huge and quite close to Transmission 3.

In Transmission 3 (the third transmission scenario), the privacy capacity is optimized with only power constraint at *Source* and *Destination* without considering any rate constraint. Subsequently, we represented the privacy capacity as $S_{c,3}$ while the data transmission rate is signified as $C_{SOD,3}$.

Considering the three transmission scenarios, it is observed that the result obtained at the second scenario *(Transmission 2)* outperform the other two transmission scenarios in terms of *source-to-destination* data rate trade-off and the transmission's privacy capacity.

### 5.2. Joint Power Assignment for Multiple Destinations

For a multiple transmission destinations scenario, we considered $C_n = \chi C^*_n$, representing $C^*_n$ as the optimal data rate attainable from *Source* to *Destination* when power $\frac{\mathbf{P}_s}{N}$ is assigned to *Source* for data broadcast to the *n*th destination. Considering $\chi = 0.8$ and $N = 4$, Figures 5 and 6, respectively, represent the maximum attained privacy capacities and data rates from the *source-to-destination*. Likewise, the equivalent outputs with no rate constraint are represented in the two figures. It is observed that if rate constraints are applied, a small measure of privacy capacities is lost, however, significant data rates are gained and maintained. For both Figures 5 and 6, under rate constraint, both the achieved and constrained rates are separable.

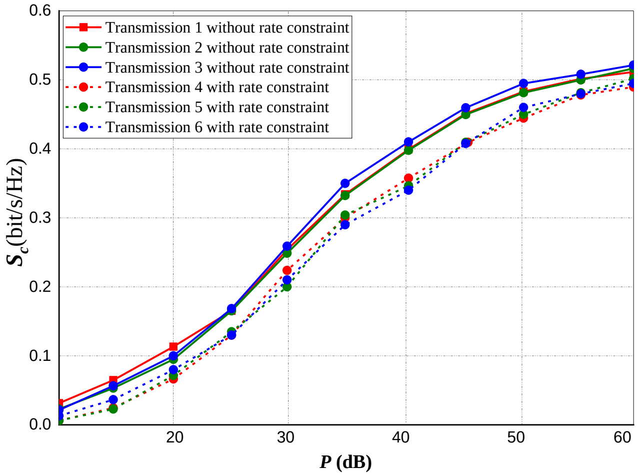

**Figure 5.** Maximum realized privacy capacity for multiple destinations transmission.

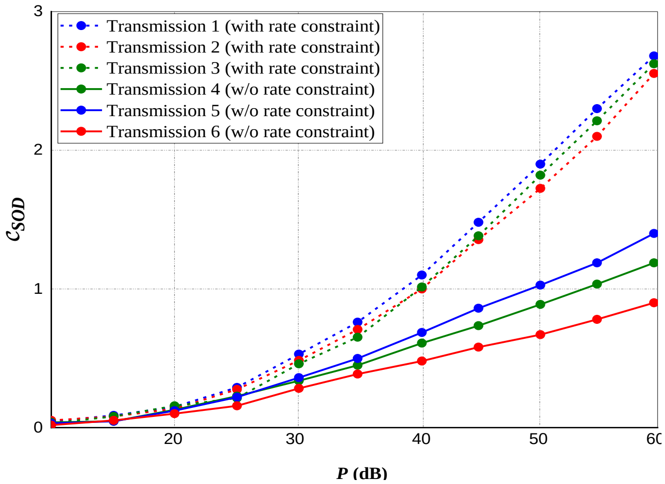

**Figure 6.** *Source-to-Destination* data rate for multiple destinations transmission.

## *5.3. Joint Power Assignment for Multiple Sources*

For a multiple transmission source scenario, considering the $n$th transmission source, we set the rate constraint as $C_n = \chi C_n^*$, representing $C_n^*$ as the optimal data rate attainable from *Source* to *Destination* when power $\mathbf{p}_{s,n} = \frac{\mathbf{p}_s}{M}$ is assigned to *Destination* for data broadcast from the $n$th *Source*. Figures 7 and 8 present the data rates and privacy capacities for all three different sources. The subsequent result shows that although a small measure of privacy capacity is lost in the absence of rate constraint, significant data rates are gained and maintained.

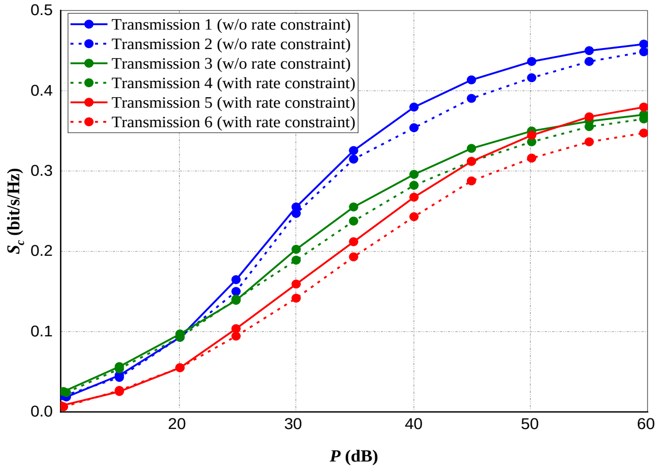

**Figure 7.** Maximum realized privacy capacity for multiple sources transmission.

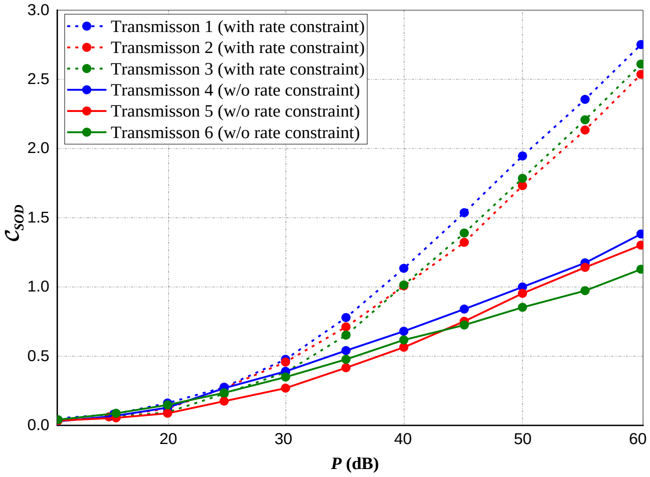

**Figure 8.** *Source-to-Destination* data rate for multiple sources transmission.

### 5.4. Performance Comparison of Difference Algorithms

In Figures 9 and 10, we compared our proposed sequential convex estimation optimization (SCEO), which is intended to mitigate the optimization problem in (15) against the Bisection method in [38] and the two-stage cooperative jamming scheme (TSCS) in [44]. A total of 60 transmitting antennas were selected for both experiments. For the rate constraints, about 0.8 of optimal attainable capacity (OAA) was selected for Figure 9, whereas for Figure 10, the power constraint $(\mathbf{p}_s = \mathbf{p}_d = \mathbf{p})$ is set at 20 dB.

Figure 9 indicates that mostly if the power constraints are low, our proposed *SCEO* technique is latent enough to obtain optimal values. Comparing the three different techniques in Figure 10 at different variations of rate constraint. Our technique is observed to outperform the other two compared techniques notwithstanding severe rate constraints. Moreover, as the rate constraints becomes more severe, convergence might be difficult for the TSCS and Bisection techniques but our algorithm converges almost seamlessly.

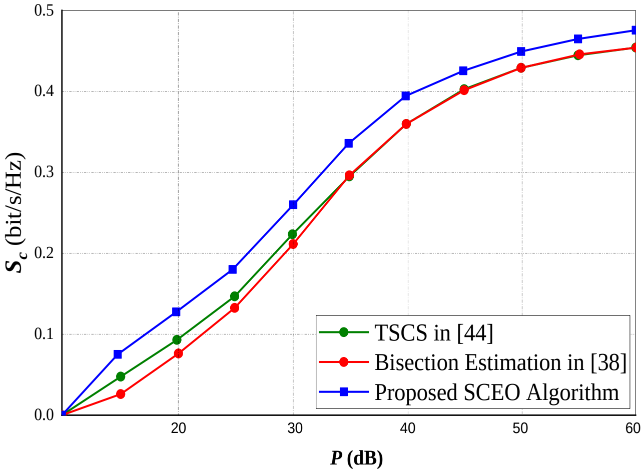

**Figure 9.** Performance of the algorithms under different power constraints.

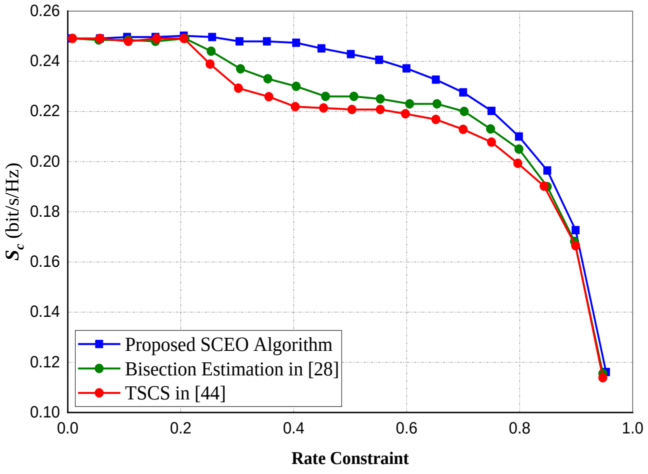

**Figure 10.** Performance of the algorithms with different rate constraints for $\mathbf{p} = 20$ dB.

Finally, the complexity analysis of our swift privacy rate optimization algorithm in a multiple transmission and multiple eavesdropper scenario is shown in Figure 11. We set the optimization parameters as $A_E = A_{Tx}, \beta_1 = 6, P_n^{\max} = P_B^{\max} = 20$ dB. From the result of our investigation, there were no evident patterns in the optimal values, in addition, the optimal parameters are dependent on the outputs of $\mathbf{G}$. Nevertheless, $P_n$ can be assumed to be frequently and approximately distributed evenly among the channels. Finally, it is observed that as $A_E$ becomes larger, the minimal $P_B$ and $r$ are respectively favored by the optimization.

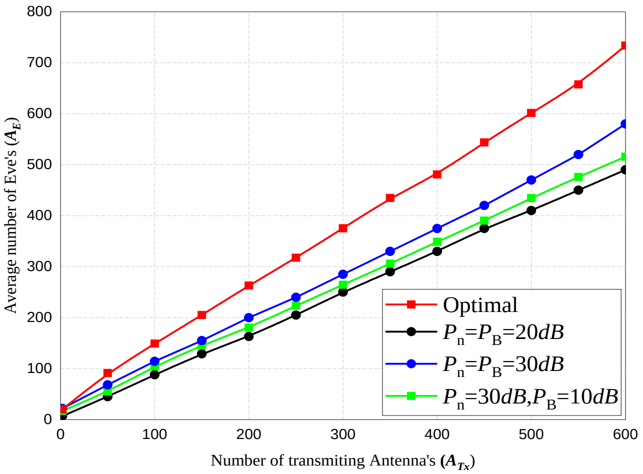

**Figure 11.** Comparison of $\bar{A}_E$ versus $\bar{A}_{Tx}$ with different parameters.

## 6. Conclusions

In this study, we explore the privacy capacity of wireless transmitting networks in several schemes relating to full-duplex jamming. Subject to both the transmission rate and power constraints, we considered and implemented an efficient power allocation optimization algorithm for enhancing privacy capacity in a three-node transmitting network and also in a real life MIMOME scenario. The applications of the resulting research and results can be applied to current wireless communication networks seen in rampant use in both IoT and 5G networks. Our experimental results showed that by using the sequential convex estimation optimization (SCEO) algorithm, a more optimal result and enhanced convergence is achieved.

However, due to possible challenges envisaged when a multiple eavesdropper is active in a network, we expanded our research to develop a swift privacy rate optimization algorithm, which executes significantly with minimal complexity when compared with nonoptimal parameters. The use of the rate constraint together with self-interference of the full-duplex at the receiving node makes the performance of our technique outstanding from the recent studies reviewed. Furthermore, we extended our study to consider a scenario where multiple sources and multiple destinations are in use. Finally, our technique indicates that as the iterative algorithm reaches convergence, a decent approximation on the optimal values is achieved. In a future work, we intend to consider a stochastic optimization approach for privacy capacity with Eve's CSI Unknown to Users.

**Author Contributions:** Conceptualization, J.H.A. and Y.T.; methodology, J.H.A. and C.I.; software, A.O.; validation, J.H.A, Y.T., C.I., and G.S.; formal analysis, Y.T. and J.H.A.; investigation, A.O. and J.H.A; resources, O.J. and G.S.; data curation, J.H.A.; writing—original draft preparation, J.H.A.; writing—review and editing, C.I., and G.S.; visualization, C.I.; supervision, Y.T.; project administration, J.H.A. and O.J.; funding acquisition, O.J. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. NRF-2018R1C1B5045013).

**Acknowledgments:** The authors wish to acknowledge the technical, supervision and material supports received from Tang Yue, Department of Communication Engineering, College of Internet of Things, Hohai University, Changzhou Campus, China.

**Conflicts of Interest:** The authors declare no conflict of interest.

## References

1. Anajemba, J.H.; Tang, Y.; Ansere, J.A.; Iwendi, C. Performance Analysis of D2D Energy Efficient IoT Networks with Relay-Assisted Underlaying Technique. In Proceedings of the IECON 2018—44th Annual Conference of the IEEE Industrial Electronics Society, Washington, DC, USA, 21–23 October 2018; pp. 3864–3869. [CrossRef]
2. Schneider, P.; Horn, G. Towards 5G security. In Proceedings of the 4th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Helsinki, Finland, 20–22 August 2015.
3. Alavi, F.; Mokari, N.; Javan, M.R.; Cumanan, K. Limited Feedback Scheme for Device-to-Device Communications in 5G Cellular Networks with Reliability and Cellular Secrecy Outage Constraints. *IEEE Trans. Veh. Technol.* **2017**, *66*, 8072–8085. [CrossRef]
4. Sun, X.; Yang, W.; Cai, Y. Secure Communication in NOMA-Assisted Millimeter-Wave SWIPT UAV Networks. *IEEE Internet Things J.* **2020**, *7*, 1884–1897. [CrossRef]
5. Yu, W.; Chorti, A.; Musavian, L.; Poor, H.V.; Ni, Q. Effective Secrecy Rate for a Downlink NOMA Network. *IEEE Trans. Wirel. Commun.* **2019**, *18*, 5673–5690. [CrossRef]
6. Shang, X.; Yin, H.; Wang, Y.; Li, M.; Wang, Y. Secrecy Performance Analysis of Wireless Powered Sensor Networks Under Saturation Nonlinear Energy Harvesting and Activation Threshold. *Sensors* **2020**, *20*, 1632. [CrossRef] [PubMed]
7. Zhou, Q.; Chan, C. Secrecy Capacity under Limited Discussion Rate for Minimally Connected Hypergraphical Sources. In Proceedings of the 2018 IEEE International Symposium on Information Theory (ISIT), Vail, CO, USA, 17–22 June 2018; pp. 2664–2668. [CrossRef]
8. Wyner, A.D. The Wire-Tap Channel. *Bell Syst. Tech. J.* **1975**, *54*, 1355–1387. [CrossRef]
9. Khisti, A.; Wornell, G.W. Secure Transmission With Multiple Antennas I: The MISOME Wiretap Channel. *IEEE Trans. Inf. Theory* **2010**, *56*, 3088–3104. [CrossRef]
10. Lin, P.-H.; Lai, S.-H.; Lin, S.-C.; Su, H.-J. On Secrecy Rate of the Generalized Artificial-Noise Assisted Secure Beamforming for Wiretap Channels. *IEEE J. Sel. Areas Commun.* **2013**, *31*, 1728–1740. [CrossRef]
11. Oggier, F.; Hassibi, B. The secrecy capacity of the MIMO wiretap channel. *IEEE Trans. Inf. Theory* **2011**, *57*, 4961–4972 . [CrossRef]

12. Fakoorian, S.A.A.; Swindlehurst, A.L. Solutions for the MIMO Gaussian Wiretap Channel With a Cooperative Jammer. *IEEE Trans. Signal Process.* **2011**, *59*, 5013–5022. [CrossRef]
13. Ortega, Y.R.; Upadhyay, P.K.; Da Costa, D.B.; Bithas, P.S.; Kanatas, A.G.; Dias, U.S.; de Sousa, R.T., Jr. Joint effect of jamming and noise on the secrecy outage performance of wiretap channels with feedback delay and multiple antennas. *Trans. Emerg. Telecommun. Technol.* **2017**, *28*, e3191. [CrossRef]
14. Mahmood, N.H.; Ansari, I.S.; Mogensen, P.; Qaraqe, K.A. On the ergodic secrecy capacity with full duplex communication. In Proceedings of the 2017 IEEE International Conference on Communications (ICC), Paris, France, 21–25 May 2017.
15. Xie, J.; Ulukus, S. Secure Degrees of Freedom of One-Hop Wireless Networks. *IEEE Trans. Inf. Theory* **2014**, *60*, 3359–3378. [CrossRef]
16. Hua,Y.; Zhu, Q.; Sohrabi, R. Fundamental properties of full-duplex radio for secure wireless communications. *arXiv* **2017**, arXiv:1711.10001. Available online: https://arxiv.org/abs/1711.10001 (accessed on 1 May 2020).
17. Hua, Y. Advanced Properties of Full-Duplex Radio for Securing Wireless Network. *IEEE Trans. Signal Process.* **2018**, *67*, 120–135. [CrossRef]
18. Iwendi, C.; Zhang, Z.; Du, X. ACO based key management routing mechanism for WSN security and data collection. In Proceedings of the 2018 IEEE International Conference on Industrial Technology (ICIT), Lyon, France, 20–22 February 2018; pp. 1935–1939. [CrossRef]
19. Zhou, Y.; Xiang, Z.Z.; Zhu, Y.; Xue, Z. Application of Full-Duplex Wireless Technique into Secure MIMO Communication: Achievable Secrecy Rate based Optimization. *IEEE Signal Process. Lett.* **2014**, *21*, 804–808. [CrossRef]
20. Cepheli, O.; Dartmann, G.; Kurt, G.K.; Ascheid, G. A Joint Optimization Scheme for Artificial Noise and Transmit Filter for Half and Full Duplex Wireless Cyber Physical Systems. *IEEE Trans. Sustain. Comput.* **2017**, *3*, 126–136. [CrossRef]
21. Yun, S.; Park, J.; Im, S.; Ha, J. On the Secrecy Rate of Artificial Noise Assisted MIMOME Channels with Full-Duplex Receiver. In Proceedings of the 2017 IEEE Wireless Communications and Networking Conference (WCNC), San Francisco, CA, USA, 19–22 March 2017; pp. 1–6.
22. Masood, M.; Ghrayeb, A.; Babu, P.; Khalil, I.; Hasna, M. A Minorization-Maximization Algorithm for Maximizing the Secrecy Rate of the MIMOME Wiretap Channel. *IEEE Commun. Lett.* **2016**, *21*, 1. [CrossRef]
23. Liu, S.; Hong, Y.; Viterbo, E. Artificial Noise Revisited. *IEEE Trans. Inf. Theory* **2015**, *61*, 3901–3911. [CrossRef]
24. Sohrabi, R.; Hua, Y. A New Look at Secrecy Capacity of Mimome Using Artificial Noise From Alice and Bob Without Knowledge of Eve'S Csi. In Proceedings of the 2018 IEEE Global Conference on Signal and Information Processing (GlobalSIP), Anaheim, CA, USA, 26–29 Novomber 2018; pp. 1291–1295.
25. Yang, Y.; Scutari, G.; Palomar, D.P.; Pesavento, M. A Parallel Decomposition Method for Nonconvex Stochastic Multi-Agent Optimization Problems. *IEEE Trans. Signal Process.* **2016**, *64*, 2949–2964. [CrossRef]
26. Liu, A.; Lau, V.; Kananian, B. Stochastic Successive Convex Approximation for Non-Convex Constrained Stochastic Optimization. CoRR, vol. abs/1801.08266. 2018. Available online: http://arxiv.org/abs/1801.08266 (accessed on 1 May 2020).
27. Zheng, B.; Wen, M.; Wang, C.-X.; Wang, X.; Chen, F.; Tang, J.; Ji, F. Secure NOMA Based Two-Way Relay Networks Using Artificial Noise and Full Duplex. *IEEE J. Sel. Areas Commun.* **2018**, *36*, 1426–1440. [CrossRef]
28. Cepheli, Ö.; Tedik, S.; Kurt, G.K. A High Data Rate Wireless Communication System With Improved Secrecy: Full Duplex Beamforming. *IEEE Commun. Lett.* **2014**, *18*, 1075–1078. [CrossRef]
29. Zhou, Y.; Zhu, Y.; Xue, Z. Enhanced MIMOME wiretap channel via adopting full-duplex MIMO radios. In Proceedings of the 2014 IEEE Global Communications Conference, Austin, TX, USA, 8–12 December 2014; pp. 3320–3325.
30. Zhou, Y.; Li, F.; Guo, P.; Xue, Z. Robust MIMO beamforming and power allocation for artificial noise generated by both transmitter and receiver. In Proceedings of the 9th International Conference on Communications and Networking in China, Maoming, China, 14–16 August 2014.
31. Heo, J.; Kim, J.-J.; Jeongyeup, P.; Saewoong, B. Mitigating stealthy jamming attacks in low-power and lossy wireless networks *J. Commun. Netw.* **2018**, *20* , 219–230.

32. Li, M.; Koutsopoulos, I.; Poovendran, R. Optimal Jamming Attack Strategies and Network Defense Policies in Wireless Sensor Networks. *IEEE Trans. Mob. Comput.* **2010**, *9*, 1119–1133. [CrossRef]
33. Matsushita, T.; Taniguchi, Y. A Method for Selecting Jamming Nodes Considering SINR to Prevent Eavesdropping in Wireless Networks. In Proceedings of the 2017 4th Asia-Pacific World Congress on Computer Science and Engineering (APWC on CSE), Nadi, Fiji, 11–13 December 2017.
34. Dorus, R.; Vinoth, P. Mitigation of jamming attacks in wireless networks. In Proceedings of the 2013 IEEE International Conference ON Emerging Trends in Computing, Communication and Nanotechnology (ICECCN), Tamil Nadu, India, 25–26 March 2013; pp. 168–171, doi: 10.1109/ICE-CCN.2013.6528486 [CrossRef]
35. Chiang, J.T.; Hu, Y.-C. Cross-Layer Jamming Detection and Mitigation in Wireless Broadcast Networks. *IEEE/ACM Trans. Netw.* **2010**, *19*, 286–298. [CrossRef]
36. Li, X.; Dai, H.-N. Friendly-Jamming: An anti-eavesdropping scheme in wireless networks. In Proceedings of the 2017 IEEE 18th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM), Macau, China, 12–15 June 2017, doi: 10.1109/WoWMoM.2017.7974299. [CrossRef]
37. Yu, B.; Zhang, L.-Y. An improved detection method for different types of jamming attacks in wireless networks. In Proceedings of the The 2014 2nd International Conference on Systems and Informatics (ICSAI 2014), Shanghai, China, 15–17 Novomber 2014.
38. Kutia, S.; Chauhdary, S.H.; Iwendi, C.; Liu, L.; Yong, W.; Bashir, A.K. Socio-Technological Factors Affecting User's Adoption of eHealth Functionalities: A Case Study of China and Ukraine eHealth Systems. *IEEE Access* **2019**, *7*, 90777–90788. [CrossRef]
39. Iwendi, C.; Uddin, M.; Ansere, J.A.; Nkurunziza, P.; Anajemba, J.H.; Bashir, A.K. On Detection of Sybil Attack in Large-Scale VANETs Using Spider-Monkey Technique. *IEEE Access* **2018**, *6*, 47258–47267. [CrossRef]
40. Iwendi, C.; AlQarni, M.A.; Anajemba, J.H.; Alfakeeh, A.S.; Zhang, Z.; Bashir, A.K. Robust Navigational Control of a Two-Wheeled Self-Balancing Robot in a Sensed Environment. *IEEE Access* **2019**, *7*, 82337–82348. [CrossRef]
41. Vincent, P.M.D.R.; Deepa, N.; Elavarasan, D.; Srinivasan, K.; Chauhdary, S.H.; Iwendi, C. Sensors Driven AI-Based Agriculture Recommendation Model for Assessing Land Suitability. *Sensors* **2019**, *19*, 3667. [CrossRef]
42. Mittal, M.; Iwendi, C. A Survey on Energy-Aware Wireless Sensor Routing Protocols. *EAI Endorsed Trans. Energy Web* **2019**, *6*. [CrossRef]
43. Iwendi, C.; Allen, A.; Offor, K. Smart security implementation for wireless sensor network nodes. *J. Wirel. Sens. Netw.* **2015**, *1*, 1.
44. Iwendi, C.; Allen, A. Enhanced security technique for wireless sensor network nodes. In Proceedings of the IET Conference on Wireless Sensor Systems (WSS 2012), London, UK, 18–19 June 2012.
45. Iwendi, C.; Ponnan, S.; Munirathinam, R.; Srinivasan, K.; Chang, C.-Y. An Efficient and Unique TF/IDF Algorithmic Model-Based Data Analysis for Handling Applications with Big Data Streaming. *Electronics* **2019**, *8*, 1331. [CrossRef]
46. Li, Z.; Yates, R.; Trappe, W. Secrecy capacity of independent parallel channels. In *Securing Wireless Communications at the Physical Layer*; Springer: Boston, MA, USA, 2010; pp. 1–18. Available online: http://dx.doi.org/10.1007/978-1-4419-1385-21 (accessed on 1 May 2020).
47. Cha, S.-C.; Hsu, T.-Y.; Xiang, Y.; Yeh, K.-H. Privacy Enhancing Technologies in the Internet of Things: Perspectives and Challenges. *IEEE Internet Things J.* **2018**, *6*, 2159–2187. [CrossRef]
48. Yeh, K. A Secure IoT-Based Healthcare System with Body Sensor Networks. *IEEE Access*, **2016**, *4*, 10288–10299. [CrossRef]
49. Xu, Z.; Gu, R.; Huang, T.; Xiang, H.; Zhang, X.; Qi, L.; Xu, X. An IoT-Oriented Offloading Method with Privacy Preservation for Cloudlet-Enabled Wireless Metropolitan Area Networks. *Sensors* **2018**, *18*, 3030. [CrossRef]
50. Iwendi, C.; Jalil, Z.; Javed, A.R.; Thippa, R.G.; Kaluri, R.; Srivastava, G.; Jo, O. KeySplitWatermark: Zero Watermarking Algorithm for Software Protection Against Cyber-Attacks. *IEEE Access* **2020**, *8*, 72650–72660. [CrossRef]
51. Riihonen, T.; Werner, S.; Wichman, R. Mitigation of Loopback Self-Interference in Full-Duplex MIMO Relays. *IEEE Trans. Signal Process.* **2011**, *59*, 5983–5993. [CrossRef]

52. Ng, D.W.K.; Lo, E.S.; Schober, R. Energy-Efficient Resource Allocation for Secure OFDMA Systems. *IEEE Trans. Veh. Technol.* **2012**, *61*, 2572–2585. [CrossRef]
53. Anajemba, J.H.; Yue, T.; Iwendi, C.; Alenezi, M.; Mittal, M. Optimal Cooperative Offloading Scheme for Energy Efficient Multi-Access Edge Computation. *IEEE Access* **2020**, *8*, 53931–53941. [CrossRef]
54. Reddy, G.T.; Sudheer, K.; Rajesh, K.; Lakshmanna, K. Employing data mining on highly secured private clouds for implementing a security-asa-service framework. *J. Theor. Appl. Inf. Technol.* **2014**, *59*, 317–326.
55. Anajemba, J.H.; Tang, Y.; Ansere, J.A.; Sackey, S.H. Efficient Switched Digital Beamforming Radar System based on SIMO/MIMO Receiver. In Proceedings of the 2019 Computing, Communications and IoT Applications (ComComAp), Shenzhen, China, 26–28 October 2019.
56. Al-Hayajneh, A.; Alam Bhuiyan, Z.; McAndrew, I. Improving Internet of Things (IoT) Security with Software-Defined Networking (SDN). *Computers* **2020**, *9*, 8. [CrossRef]
57. Babaei, A.; Schiele, G. Physical Unclonable Functions in the Internet of Things: State of the Art and Open Challenges. *Sensors* **2019**, *19*, 3208. [CrossRef]
58. Reddy, G.T.; Kaluri, R.; Reddy, P.K.; Lakshmanna, K.; Koppu, S.; Rajput, D.S. A Novel Approach for Home Surveillance System Using IoT Adaptive Security. *SSRN Electron. J.* **2019**. [CrossRef]
59. Kumar, M.E.; Reddy, G.T.; Sudheer, K.; Reddy, M.P.K.; Kaluri, R.; Rajput, D.S.; Lakshmanna, K. Vehicle Theft Identification and Intimation Using GSM & IOT. *IOP Conf. Ser. Mater. Sci. Eng.* **2017**, *263*, 42062. [CrossRef]