A Counter-Eavesdropping Technique for Optimized Privacy of Wireless Industrial IoT Communications.

***Abstract*—The Industrial Internet of Things (IIoTs) is a key component of the fourth industrial revolution (Industry 4.0) which is faced with privacy issues as the scale and sensitivity of user and system data constantly increases. Eavesdropping attack is one of such privacy issues of the IIoT system especially when the number of transmitting antennas is increased. Thus, the focus of this paper is on establishing efficient privacy in an IIoT-MIMOME communications scenario. To achieve this, a closed-form derivation for asymptotic regularized prompt privacy rate is first formulated for IIoT network system. Then, the study further examines the design of optimal jamming parameters by proposing a model referred as Optimal Counter-Eavesdropping Channel Approximation (OPCECA) technique for tackling eavesdropping attack in IIoT. The simulated performance of the proposed model clearly shows that provided that the channel coherence time is less than two times number of transmitting nodes, a high privacy precision is achieved even without deploying any artificial noise.**

***Index Terms*—IIoTs, Industry 4.0 , MIMOME, CSI, Artificial Noise, Privacy Capacity**

I. Introduction

THe fourth industrial revolution (Industry 4.0) has an enormous potential of providing massive connectivity and smart industrial scheme where humans, machine (physical system) and internet lumped collaboratively [1]. It provides adequate connectivity for contemporary sensor technology, fog-to-cloud computation platforms, and artificial intelligence (AI) to generate smart, self-optimizing industrial devices and services [2]. The operational physical data transmission has been enabling the performance of IIoTs [3] which is assumed as a key component of the Industry 4.0. Different from previous industrial revolutions, the performance of Industry 4.0 is more concentrated on data transmission [4]. For instance, the Machine to Machine (M2M) and Device to device (D2D) technologies are equipped with the capacities of producing, preserving and transmitting several personal user information [5]. However while the physical data of the IIoTs technology provides essential information for multiple smart connected devices, it is also prone to several privacy concerns for both the manufactures, networks and devices, thus resulting in privacy issues of data transmission. The more the personal information is generated and accrued, the more vulnerable and subtle to eavesdropping and other network attacks they become.

Eavesdropping attacks can pose a challenging threat to the IIoT structure and operations with respect to their conventional privacy prospects [6]. It is very important that the privacy concerns which stems from such attacks like the eavesdropper is addressed, because they have consequent effects on rudimentary user rights and overall aptitude to lay confidence on the devices and the entire Internet space they connect to. Recently, several strategies have attempted to abridge the performances of networks participants for improved theoretical analysis, but have failed to extensively tackle this particular privacy issue in IIoTs where transmitted confidential data is exposed and accessed by an unwanted entity (eavesdropper). This have over time become a major problem of IIoT transmission. Also, esteeming user privacy in an IIoTs setup is essential in guaranteeing trust and confidence in the internet activities. This also influences the user's aptitude in expressions, [7] selecting and connecting in exceptional traditions.

Although some previous researches (such as [8], [9]) have attempted to resolve the issue of privacy on this scale by considering the small-scale fading channel state information (CSI) of the eavesdropper, however, privacy concern with respect to the eavesdroppers location (which implies large-scale fading CSI) is still understudied. Therefore, in order to attain an improved privacy standard, this research considers the most harmful scenario of the eavesdropper's location. Thus, the investigation established a closed-form expression for asymptotic regularized prompt privacy rate when utilizing artificial noise at both the transmitting and receiving nodes.

The study focus is to establish that as long as the quantity of antennas for every transmitting nodes is increased, the regularized prompt rates and the prompt privacy rate joins to a constant. In this case, the derived closed-form constant is not reliant on the channel actualization's; thus, it is suitable when no definite data for the channels actualization's is accessible. With respect to the results of the asymptotic approach, a controllable expression optimization problem is proposed notwithstanding the position of either the eavesdropper or the CSI. The study establishes a closed-form presentation for asymptotic regularized prompt privacy rate when utilizing artificial noise at both the transmitting and receiving nodes.

A. Research contributions

In order to realize the study objective which is to establish that as long as the quantity of antennas for every transmitting nodes is increased, the regularized prompt rates and the prompt privacy rate joins to a constant. The following contributions are established;

1 With respect to the results of the asymptotic expression, the research propose a controllable expression of an optimization problem irrespective of the eavesdroppers' position or the channel state information.

2 The study establishes a closed-form presentation for asymptotic regularized prompt privacy rate when utilizing artificial noise at both the transmitting and receiving nodes.

3 Finally, the study proposes a Prompt Privacy Rate Optimization algorithm which proves to achieve empirically improved performance than conventional stochastic techniques which are based on mere gradient at no additional

signaling cost, because it exploits the convex state of the objective function, (if any).

B. Structure

The remain parts of this research is structured as follows. In section II, several previously related works and revised and compared against the present research idea. The network model which consists of the network framework for an IIoT multiple-input multiple-output multiple-antenna eavesdropping (MIMOME) , an analyzed scenario of Eavesdropper's Worst Location, Asymptotic Prompt Privacy Rate expression, Prompt Privacy Rate Optimization model and the Models for Short and Long Channel Coherence Time Expression are all expressed in III. Simulation parameters and their respective preceding results and analysis are presented in IV and finally conclusions and findings are discussed in V.

II. Related Works

Secured data transmission in the industry 4.0 technologies (which the internet of things is a key component) has always been a primary considerable prerequisite for enabling the efficiency of IIoTs [10]. Recently, several studies have conducted different investigations to illustrate data transmission as regards IIoT schemes. Most of these studies paid adequate attention on proposing novel techniques for mutual data transmission, the allocation of resources while data transmission is in process [11] and also to design several unified scheme which can enable for free data transmission. However, one principal weakness of most of these researches is their obvious neglect of privacy concerns, which in the real sense is more severe owing to the contribution of uncertain physical layer data [12].

On the other hand, several studies have been conducted towards tackling privacy preservation issues in the Industrial Internet of Things (IIoTs). Data location, as a characteristic for several physical data, has been systematically considered to frustrate attacks from diverse intruders. Both the subtle locations and the isolated information below these positions are examined and appropriately controlled [13]. One significant method for enhancing privacy-preservation in IoT transmission at the physical layer was established in [14]. In other to tackle privacy authentication issues in wireless IIoT, the study of [15] designed a novel authentication model referred as Authentication Transfer Learning empowered Blockchain (ATLB). The proposed ATLB utilizes blockchains approach to attain the desired privacy protection of user data in Industrial applications of Internet of Things. The ATLB utilizes a supervisory deep deterministic strategy gradient algorithm (DDSGA) to train the user authentication framework of a precise area. Results of their experiments indicates that the proposed ATLB approach is viable for providing precise authentications for IIoT systems and user as well as attains low latency and optimal throughput.

The study of [2], investigated the implementation of a secured IoT-based healthcare scheme. The scheme functions via an architecture of body sensor networks (BSN) and the key aim of the paradigm is to simultaneously achieve system sturdiness of broadcast and efficiency within openly communicating IoT-based transmission systems. Employing a dynamic crypto-primitives approach, their study fabricated two transmission protocols to safeguard communication confidentiality and maintain viable authentication of entity between smart communicating devices. Because most IIoT information are applicable to individual privacy, it is essential to give maximum consideration to the security of data broadcast. Thus, the study of [16] explored an IoT-adapted offloading scheme (IOS) which is enhanced with optimal privacy preservation to tackle privacy concerns in Cloudlet-assisted Wireless Metropolitan Area Networks (CWMAN). The findings of their investigation assumed the non-dominated cataloguing disparity progression algorithm (NCDPA) with the intention of improving the multi-objective problem which exists in the transmission protocol.On the other hand, several other studies have investigated and established diverse opinions on the privacy rate maximization problem of IoT transmission in the existence of single or multiple eavesdroppers in proportion to varied standards on the settings of antennas of both the transmitter, receiver and eavesdropper and that of the broadcasts CSI. Nevertheless, there are only a few research which considered a scenario whereby the eavesdroppers CSI is unknown to either the transmitter or receivers.

The research of [17] proposed a location privacy protection technique which fulfills differential privacy limitation to exploit the usefulness of data and algorithm and secure location data privacy in IIoT system. Considering the enormous importance and low density of location data, the researchers conglomerated the effectiveness with the privacy and designed an information tree model based on a multilevel location. However, their proposed technique could only guarantee a chunk level of improvement with respect to applicability and privacy. Using machine learning (ML) approach, [18] designed an ML-based privacy-preserving model which leverages on microservice technique for securing healthcare Industrial IoT schemes. Precisely, the authors utilized the combination of the Radial Basis Function Network (RBFN) and Differential Privacy (DP) approach in designing a microservice-based distributed privacy-preserving scheme in an attempt to achieve a balance between model performance and privacy preservation in edge networks. Results of their experiments showed that data preservation is enhanced but only through the execution of microservices.

In summary, from all the above analyzed studies, the unique feature of our research is that unlike other previously established techniques, the proposed privacy optimization model is equipped with the capacity of averting any hostile effect of the eavesdroppers notwithstanding their position in the network while optimal privacy preservation is achieved as well. Also, the investigation established a clarity between the scenarios of short and long channel coherence time and further examined the eavesdroppers optimal performance coupled with how her method influences privacy. Finally, the study illustrates the performance advantage of the proposed technique and presents that the use of artificial noise is effective when the technique is employed.

III. Network Model

This system model in this chapter explores a network framework for an IIoT multiple-input multiple-output multiple-antenna eavesdropping (MIMOME) is presented in Fig. 1.

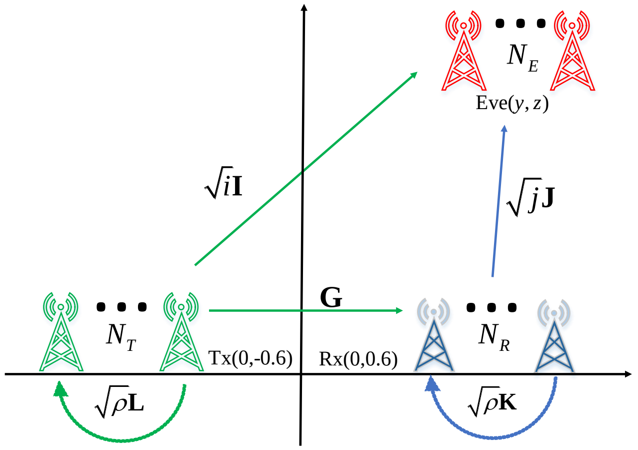

Fig. 1. Illustration of an IIoT-MIMOME network model

In the setup, the Transmitters antennas which are denoted as N_T attempts to transmit confidential personal data through a means of a wireless frequency to the Receiver whose number of antennas is described as N_R with probably lots of inert number of Eavesdroppers antennas represented as N_E which might jam with each other only at the network layer as it is very difficult in real terms for jamming to occur at the physical layer between disseminated Eavesdroppers. In [6], setup parameters are regularized in a way that the factors of large-scale-fading from the transmitter to Eavesdropper is demonstrated as $t = d_T^{-\alpha} = \left(\sqrt{(y+0.6+z^2)^2}\right)^{-\alpha}$, while that of the Receiver to Eavesdropper is expressed as $r = d_R^{-\alpha} = \left(\sqrt{(y+0.6+z^2)^2}\right)^{-\alpha}$. In this regard, the exponent of path loss is represented as α . Virtually, we suppose that the proximity between any of the Eavesdropper to the Transmitter is not beyond a precise interval which is; $d_T \geq \Delta$.

We used ρ to represent the regularized factor of large-scale-fading of the Transmitter's and Receiver's self-interference, while the matrix of small-scale-fading channel from Transmitter to Eavesdropper is signified as $\mathbf{I}$, that of Receiver to Eavesdropper is $\mathbf{J}$, while $\mathbf{K}$ and $\mathbf{L}$ represents the respective channels of self-interference between the Receiver and Transmitter (recall that the transmitter does not utilize a full-duplex capacity). $\mathbf{G}$ is used to denote the matrix of Transmitter and Receiver matrix, and the singular value decomposition (SVD) is represented as:

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

where $\mathbf{M}$ and $\mathbf{N}$ represents the inflexible matrices, while $\sqrt{\lambda_a, a \in \{1, ..., N_R\}}$ which represents the SVD values of $\mathbf{G}$ are confined in $\sqrt{\mathbf{\Lambda}}$ and are expressed in a descending sequence on its foremost transverse with a presumption that $N_R \leq N_T$. It is assumed that the whole elements of the entire channel matrices are i.i.d. and circularly symmetric complex Gaussian with zero mean and unit variance. In the setup, the transmitter and Receiver are only knowledgeable of $\mathbf{G}$, but Eavesdropper is aware of the entire parameters if not otherwise stated. Thus, the transmitter conveys the preceding signal which comprises of i flows of confidential data and noise at time space l

$$\mathbf{y}_T(l) = \mathbf{N}_1\mathbf{d}\left(l\right) + \mathbf{N}_2\mathbf{c}_T\left(l\right) \tag{2}$$

where $\mathbf{N}_1$ represents the matrix, $N_T \times i$ and $\mathbf{N}_2$ denotes the matrix, $N_T \times (N_T - i)$ which are illustrated as $\mathbf{N} = [\mathbf{N}_1, \mathbf{N}_2]\,, \mathbf{d}\left(l\right)$. $\mathbf{U}_i$ is the covariance matrix3. of the Transmitter's data trajectory and $\mathrm{Hi}\left(\mathbf{U}_i\right) = P_d$ while $\mathbf{c}_T\left(l\right)$ represents the $(N_T - i) \times 1$ trajectory of artificial noise with allocation format as $\mathcal{CN}\left(0, \frac{P_n}{N_T - i}\mathbf{A}\right)$, thus $P_b + P_n = P_T \leq P_T^{\max}$.

In the process whereby Rx obtains data from Tx , jamming noise is also transmitted and presented as

$$\mathbf{x}_R\left(l\right) = \mathbf{c}_R\left(l\right) \tag{3}$$

representing $\mathbf{c}_R\left(l\right)$ as an $N_R \times 1$ trajectory of artificial noise with allocation format as $\mathcal{CN}\left(0, \frac{P_R}{N_R}\mathbf{A}\right)$. The regularized powers regarding the path loss from Tx to Rx is denoted as P_T and P_D , respectively. Then, the following signals are respectively received by Rx and Eavesdropper

$$\mathbf{z}_R\left(l\right) = \mathbf{G}\mathbf{N}_1\mathbf{d}\left(l\right) + \mathbf{G}\mathbf{N}_2\mathbf{c}_T\left(l\right) + \sqrt{\rho}\mathrm{K}\bar{\mathbf{c}}_R\left(l\right) + \mathbf{n}_R\left(l\right) \tag{4}$$

$$\mathbf{z}_E\left(l\right) = \sqrt{i}\mathbf{I}_1\mathbf{d}\left(l\right) + \sqrt{i}\mathbf{I}_2\mathbf{c}_T\left(l\right) + \sqrt{r}\mathbf{J}\mathbf{c}_R\left(l\right) + \mathbf{n}_E\left(l\right), \tag{5}$$

considering self-interference attributes in a full-duplex wireless transmission, $\bar{\mathbf{c}}_R\left(l\right)$ is not reliant on $\mathbf{c}_R\left(l\right)$ and is Gaussian with unit variance and zero mean, similarly $[\mathbf{I}_1, \mathbf{I}_2] = [\mathbf{I}\mathbf{N}_1, \mathbf{I}\mathbf{N}_2] = \mathbf{I}\mathbf{N}$, and the fundamentals of both matrices are i.i.d. composite Gaussian with unit variance and zero mean [19]. Additionally, $\mathbf{n}_E$ and $\mathbf{n}_R$ are $\mathcal{CN}\left(0, \mathbf{A}\right)$. So, the privacy capacity of this transmission is expressed as

$$S_P = \max_{p(\mathbf{b})}(A(\mathbf{d};\mathbf{z}_R) - A(\mathbf{d};\mathbf{z}_E))^{+} \tag{6}$$

Due to maximization throughout all allocations, it is somewhat complex to realize this formulation, nevertheless, assuming a Gaussian input character, such as, $\mathbf{d} \sim \mathcal{CN}\left(0, \mathbf{U}_i\right)$ is utilized, then, the attainable privacy rate and rates which is a lower bound on privacy capacity can be employed, thus, $\mathbf{d} \sim \mathcal{CN}\left(0, \mathbf{U}_i\right)$ is implicit.

As long as Rx has a good knowledge of the matrix of covariance matrix for the existing noise coupled with the interference S_R in his received signal $\mathbf{z}_R$, Rx can utilize an optimal receiving channel, thus, the rate at Rx can be expressed as

$$C_{TR} = \log\left|\mathbf{S}_R + \mathbf{G}\mathbf{N}_1\mathbf{U}_i\mathbf{N}_1^G\mathbf{G}^G\right| - \log\left|\mathbf{S}_R\right| \tag{7}$$

Similarly, assuming the covariance matrix of noise coupled with interference $\mathbf{S}_E$ of Eavesdropper is well known to her just like her entire CSI, then, Eavesdropper can utilize an optimal receiving channel and her transmission rate can be expressed as;

$$C_{TE} = \log\left|\mathbf{S}_E + t\mathbf{I}_1\mathbf{U}_i\mathbf{I}_1^G\right| - \log\left|\mathbf{S}_E\right| \tag{8}$$

In conclusion, the swift attainable privacy capacity is expressed as

$$C_D = (C_{TR} - C_{TE})^+ \tag{9}$$

This is a stochastic quantity and liable upon Eavesdropper's small-scale-fading CSI and her unidentified location, thus making it inappropriate for optimization, however, a possible solution to this issue will be proposed in the later part of this research.

Alternatively, average privacy rate can be utilized as one other procedure for privacy and is expressed as

$$\bar{C}_D = \mathbb{E}_{\mathbf{G},\mathbf{K},\mathbf{I},\mathbf{J}}\left[C_D\right] \tag{10}$$

For further reading about realization of a closed-form for $\bar{C}_D$, we refer to [9]; but, this kind of closed-form is inappropriate for neither optimization nor analysis (because of its convexity) which explains why we did not express it in this research. Therefore, the investigation in this research is focused on asymptotic rates which eradicates the issue of reliance on the CSI small-scale-fading and our analysis is based on the achievements of the asymptotic procedures.

Although the reliance of privacy on the small-scale fading CSI of Eavesdropper has been resolved, however, privacy reliance on the location of Eavesdropper (which implies large-scale fading CSI) is yet to be removed. So as to attain a more controllable investigation, the most harmful scenario of Eavesdropper's position is considered following subsection.

A. A Scenario of Eavesdropper's Worst Location

Because C_{TR} is not variant to position of Eavesdropper, her worst scenario is that one whose location optimizes C_{TE} . Then C_{TE} can be expressed as

$$C_{TE} = \log\left|\mathbf{A} + \left(\tfrac{1}{t}\mathbf{A} + \tfrac{P_n}{N_T - i}\mathbf{I}_2\mathbf{I}_2^G + \tfrac{rP_R}{tM}\mathbf{J}\mathbf{J}^G\right)^{-1}\mathbf{I}_1\mathbf{U}_i\mathbf{I}_1^G\right| \tag{11}$$

On a lighter note we observe that with respect to this formulation, for a fixed $t = d_T^{-\alpha}$ (which implies that if Eavesdropper loops about the Transmitter with fixed area), C_{TE} is optimized when r is minimal (minimum channel degradation as a result of jamming at the Receiver's end) that is, $r = (1 + d_T)^{-\alpha}$. Using the optimized r , we formulate

$$\mathrm{C}_{TE} = \log\left|\mathrm{A} + \left(d_T^{\alpha}\mathbf{A} + \tfrac{P_n}{N_T - i}\mathbf{I}_2\mathbf{I}_2^G + \tfrac{d_T^{\alpha}P_R}{(1+d_T)^{\alpha}N_R}\mathbf{J}\mathbf{J}^G\right)^{-1}\mathbf{I}_1\mathbf{U}_i\mathbf{I}_1^G\right| \tag{12}$$

Assuming $d_T \geq \Delta$ is constrained, then C_{TE} is optimized if $d_T = \Delta$. So, Eavesdropper's worst location is at $y^* = -0.6 - \Delta$, $z^* = 0$. Henceforth, t and r are considered to be equivalent to the location (y^*, z^*) . For future referencing in the simulation, Δ is set at 0.2. As the number of transmitting antennas increases, it is important to find the asymptotic state of the rates. This is one approach towards eliminating the reliance of C_B on the CSI of Eavesdropper. Therefore, the closed-form for asymptotic regularized prompt privacy rate is derived in the preceding section.

1) A Closed-form Expression: Our focus here is to establish that as long as the quantity of antennas for every transmitting nodes is increased, the regularized prompt rates $\frac{C_{TR}}{N_R}$ and $\frac{C_{TE}}{N_E}$ coupled with the prompt privacy rate $\frac{C_D}{N_R}$ joins to a constant. Thus, in order to generate this constant and for an ease of analysis we assume that $N_R < N_T$, $\mathbf{U}_i = \frac{P_b}{N_R}\mathbf{A}$ and $i = N_R$, consequently, the null-space of $\mathbf{G}$ is represented as $\mathbf{N}_2$. So, we realize

$$\begin{aligned} C_{TR} &= \log\left|\mathbf{A} + \tfrac{\rho P_R}{N_R}\mathbf{K}\mathbf{K}^G + \tfrac{P_d}{N_R}\mathbf{G}\mathbf{G}^G\right| - \log\left|\mathbf{A} + \tfrac{\rho P_R}{N_R}\mathbf{K}\mathbf{K}^G\right| \\ &= \log\left|\mathbf{A} + \mathbf{B}_1\Theta_1\mathbf{B}_1^G\right| - \log\left|\mathbf{A} + \mathbf{B}_2\Theta_2\mathbf{B}_2^G\right| \end{aligned} \tag{13}$$

considering that $\mathbf{B}_1 = \frac{1}{\sqrt{N_R}}\left[\mathbf{G}, \mathbf{K}\right], \mathbf{B}_2 = \frac{1}{\sqrt{N_R}}\mathbf{K}, \Theta_2 = \rho P_R\mathbf{A},.$

The amount of diagonal element of Θ is represented by Q_Θ while, $\delta > 0$ describes the derivation of the computation

$$1 - \delta = \frac{\beta_\delta}{Q_\Theta}\sum_{v=1}^{Q_\Theta}\tfrac{\Theta_{v,v}}{1+\delta\Theta_{v,v}}. \tag{14}$$

Therefore, assuming the number of Eavesdropper's antennas is increased so much while the numbers of both the transmitters and receivers' antennas remains constant, the number of Eavesdropper's antennas goes to infinity ($N_E \to \infty$, although the asymptotic performance converges faster however, N_E should not be overly increased in practical application).

B. Prompt Privacy Rate Optimization

Relating to the illustrations in the earlier section, assuming N_E is increased to a very large degree, then the impact of artificial noise on C_{TE} will be inconsequential. So, the assumption in this section is that there is a limitation on the maximum number of antennas Eavesdropper can possess and for optimization purposes, it is supposed that the most harmful scenario and considering N_E as the maximum number of antennas. So as to achieve the desired optimization, Tx and Rx cannot utilize the Eavesdropper's prompt CSI, thus, for the optimization, based on the previous derivations, it is not appropriate to employ C_B . With reference to the section before, it is established that Eavesdropper's asymptotic rate is a decent approximation to the fixed rate therefore, this fact can be employed to achieve optimization.

With respect to this approximation, we propose an objective function that obtains $-C_B$ approximation. This proposed objective function is independent of the CSI of Eavesdropper's and considers the Eavesdropper's approximate prompt rate. Similarly, since $\mathbf{G}$ (which is the transmitted information) is supposed to be acknowledgeable by Tx and Rx , the fixed rate of Rx is utilized instead of its asymptotic state. Consequently, the proposed objective function is established and expressed as

$$\begin{aligned} k\left(\mathbf{u}_i, P_n, P_R\right) = -\log\left|\mathbf{S}_R + \mathbf{G}\mathbf{N}_1\mathbf{U}_i\mathbf{N}_1^G\mathbf{G}^G\right| + \log\left|(\mathbf{S}_R)\right| \\ + N_E\Phi\left(\bar{\delta}_3, \bar{\Theta}_3, \bar{\beta}_3\right) - N_E\Phi\left(\bar{\delta}_4, \bar{\Theta}_4, \bar{\beta}_4\right), \end{aligned} \tag{15}$$

note that $\mathbf{S}_R$ is already derived in (7), $\bar{\beta}_3 = \frac{N_T + N_R}{N_E}$, $\bar{\beta}_4 = \frac{N_{T-i} + N_R}{N_E}$ while, $\bar{\delta}_3$ and $\bar{\delta}_4$ denotes the solutions for the problem in (14) using $\left\{\beta = \bar{\beta}_3, \Theta = \bar{\Theta}_3\right\}$ and $\left\{\beta = \bar{\beta}_4, \Theta = \bar{\Theta}_4\right\}$ as their respective parameters. Therefore, to realize an optimal prompt privacy rate, the subsequent optimization problem is proposed;

$$\begin{aligned}\min_{i} \min_{\mathbf{u}_i, P_n, P_R} & \; k\left(\mathbf{u}_i, P_n, P_R\right) \\ & \text{s.t.} \sum_{a=1}^{i} \mathbf{u}_i\left(a\right) + P_n \leq P_T^{\max} \\ & \mathbf{u}_i\left(a\right) \geq 0, \forall a = 1, ..., i \\ & P_n \geq 0 \\ & 0 \leq P_R \leq P_R^{\max}.\end{aligned} \tag{16}$$

The constraints of the optimization problem are convex, however, $k\left(.\right)$ is a non-convex expression. By using the first-order-Taylor-series expansion, we can linearize the fragment of $k\left(.\right)$ that is not convex $\left(\text{i.e.}, \log\left|S_R\right| + \sum_{v=1}^{Q_{\Theta_3}} \log\left(1 + \bar{\delta}_3\left(\bar{\Theta}_3\right)v, v\right)\right)$ at every iteration point of the optimization algorithm. In the same way, the reliance of $k\left(.\right)$ on $\bar{\delta}_3$, thus $\bar{\delta}_3$ is solvable as long as they are kept constant depending on their values from the initial iteration and updating them in the last part of every iteration by finding the solution of (17) using the updated parameters and expressing the result as

$$1 - \bar{\delta}_a^{h+1} = \frac{\bar{\beta}_a \bar{\delta}_a^{h+1}}{Q_{\Theta_a}} \sum_{v=1}^{Q_{\Theta_a}} \frac{\left(\bar{\Theta}_a^{h+1}\right)v, v}{1 + \bar{\delta}_a^{h+1}\left(\bar{\Theta}_a^{h+1}\right)v, v}, a = 3, 4. \tag{17}$$

considering that the superscript $\left(h+1\right)$ represents the parameters at $h+1$ iteration. Thus, the subsequent convex function ought to be optimized at iteration h. It is worth noting that the constant terms are omitted in (17) as they do not affect optimization. Now $g^h\left(.\right)$ is a convex function and can be optimized by the following optimization

$$\begin{aligned}\mathbf{y}_i^{h+1} = & \arg\min_{\mathbf{y}_i} g^h\left(\mathbf{y}_i\right) \\ & \text{s.t.} \sum_{a=1}^{i} \mathbf{u}_i\left(a\right) + P_n \leq P_T^{\max} \\ & \mathbf{u}_i\left(a\right) \geq 0, \forall a = 1, ..., i \\ & P_n \geq 0 \\ & 0 \leq P_R \leq P_R^{\max}\end{aligned} \tag{18}$$

In the same way, the optimal value of can be established by exploring all its likely values. The detail of our proposed optimization technique is presented in **Algorithm 1**. It is important to state that dissimilar optimization methods for solving this kind of problem was discussed in [20] which examined a stochastic optimization technique with respect to Eavesdropper's rate anticipation. The technique here almost has the same result as that of [20] , however, a very meaningful lower complexity is achieved by using **Algorithm 1**.

Practically, Algorithm 1 represents the first equivalent optimal-response (such as non-gradient somewhat response) pattern for problems of non-convex stochastic sum-utility. This implies that the strategies of all the smart communicating devices will be update in parallel (perhaps with a memory) resolving an order of decoupled (sturdily) convex sub-problems. The algorithm achieves empirically improved performance than conventional stochastic techniques which are based on mere gradient at no additional signaling cost, because it exploits the convex state of the objective function, (if any). Furthermore, assuming varying occurrences of the set of $\mathbf{y}_i^h$ is selected, a sub-problem which assumes a convex polynomial form will be obtained. This convex problem may display a dissimilar trade-off between speed of convergence and cost of each iteration. Finally, the algorithm guarantees optimal convergence notwithstanding any frail norms while providing some elasticity in the selection of the permissible parameters.

Algorithm 1 Proposed Prompt Privacy Rate Optimization performance .

```
Input: actual $\bar{\delta}_3^0$ , $\bar{\delta}_4^0$ , $\in$
Data: Initialize $k^{\min} = 0$.
for $i = 1 : N_T$ do
    initiate $\mathbf{y}_i$ making sure the constraints are satisfied
     Set $h = 0$
    while $\frac{\left\|\mathbf{y}_i^h - \mathbf{y}_i^{h-1}\right\|}{\left\|\mathbf{y}_i^{h-1}\right\|} > \in$ do
        Find the solution of (18) to realize $\mathbf{y}_i^{h+1}$
         Update $\bar{\delta}_3$ , $\bar{\delta}_4$ by finding the solution of (17) utilizing $\mathbf{y}_i^{h+1}$.
         $h = h + 1$
    end
    end while
     if $k\left(\mathbf{y}_i^h\right) < k^{\min}$ then
        $k^{\min} = k\left(\mathbf{y}_i^h\right)$
         $\mathbf{y}^{\min} = \left(\mathbf{y}_i^h\right)$
         end If
    end
end
end For
 Repeat $\mathbf{y}^{\min}$
```

C. Analysis of computational complexity

The computational complexity of our proposed OPCECA algorithm is established in this subsection. Firstly, the discrete iterations compute JK allocating sub-channel to $k\text{th}$ transmitting smart devices. The iteration is performed to assign only one antenna to individual K of the transmitting smart devices. Therefore, the overall realized complexity in the first phase is expressed as JK^2. Secondly, by means of sub-gradient method each iteration attains a complexity of $O\left(JK\right)$ which converges swiftly in $O\left(\left(JK\right)^2\right)$ iterations. Assuming the sub-gradient method is estimated further, it produces a complexity of $O\left(JK(J+1)^2\right)$. Considering ω as the vital precision which supports the bisection search, the realized computational complexity in the second phase is established as $O\left(JK(J+1)^2.\log_2(1/\omega)\right)$. Thirdly, assuming a constant data is transmitted from $j\text{th}$ antenna to $k\text{th}$ smart devices, we assume the computation complexity as $O\left(J\right)$ for individual iteration. Therefore, the attained complexity at the third phase is expressed as $O\left(K(J+1)^2.\log_2(1/\omega)\right)$. From the above stated analysis, it is observed that the iteration at the first phase has a K constraint since the smart devices selects just a single antenna. This implies that the proposed OPCECA algorithm realizes a computational complexity only with the second and the third iterations. As a result, the overall computational complexity is established as $O\left(K(J+1)^3.\log_2(1/\omega)\right)$. This supports the claim that the complexity of the proposed OPCECA algorithm is polynomial time complexity and can enable real-world operation in Industrial IoT structures.

The efficient out-performance of the proposed optimization is shown in Fig. 3 in comparison to the parameters that are not optimal. Hence, $N_E = N_T$, $\beta_1 = 5$, and $P_T^{\max} = P_R^{\max} = 30$dB are the optimization parameters. Regarding the optimized model, contrarily to the parameters that are not optimal, the optimal parameters curve which is realized by numerical analysis is invalid for the asymptotic regularized prompt privacy rate. The analysis in this study failed to illustrate any evident forms in the values of the optimal parameters, and their values are derived from the actualization of $\mathbf{G}$. But P_d can be said to be frequently and evenly distributed amongst diverse communication flows and assuming N_E is increased further, then, lesser i and lesser P_R are favored by the optimization, respectively. Based on the performance of the simulation in Fig. 3, it could be determined that even if the advanced and optimized technique is applied to battle the activities of the eavesdropper, privacy is still undermined in the Eavesdropper's most harmful scenario, especially if her number of antennas is somewhat increased more than that of Tx and Rx . This has been a very overlooked factor in previous researchers, and it is important to design novel ideas and models which could provide lasting solution to this issue. The OPCECA concept is believed to be a good foundation for solving this kind of problem. Therefore, the efficacy of this concept with respect to tackling eavesdropping attacks is explored in the next subsection.

D. Models for Short and Long Channel Coherence Time Expression

There are two stages that forms the framework of the OPCECA model. In the first stage which is referred as the training stage, the Tx and Rx concurrently transmits pilots in such a way that they can approximate their mutual channel. Utilizing $N_T = N_R$ antennas and for time frame L_1 , both the Tx and Rx respectively transmits the following signals

$$\mathbf{y}_T\left(l\right) = \mathbf{y}_R\left(l\right) = \mathbf{p}\left(l\right), l = 1, ..., L_1 \tag{19}$$

Firstly, the signals received by the Eavesdropper at the training stage is established as

$$\mathbf{z}_E\left(l\right) = \left(\sqrt{t}\mathbf{I} + \sqrt{r}\mathbf{J}\right) = \mathbf{p}\left(l\right) + \mathbf{n}_E\left(l\right), l = 1, ..., L_1 \tag{20}$$

considering $\mathbf{n}_E\left(l\right)$ to be a spatial white and also sequential with unit variance, while $\mathbf{P}$, $\mathbf{Z}_E$, and $\mathbf{N}_E$ are described as the subsequent matrices of the horizontal piling of L_1 column vectors $\mathbf{p}\left(l\right)$, $\mathbf{z}_E\left(l\right)$ and $\mathbf{n}_E\left(l\right)$, correspondingly. Hence, the linear minimum mean square error (LLMSE) approximation of $\mathbf{g}_T$ and $\mathbf{g}_R$ are presented as follows

$$\begin{aligned} \hat{\mathbf{g}}_T &= \mathbb{E}\left[\mathbf{g}_T\mathbf{z}_E^G\right]\mathbb{E}\left[\mathbf{z}_E\mathbf{z}_E^G\right]^{-1}\mathbf{z}_E \\ &= \sqrt{t}\mathbf{H}^G\left(\left(t+r\right)\mathbf{H}\mathbf{H}^G + \mathbf{A}\right)^{-1}\mathbf{z}_E \\ &= \sqrt{t}\left(\left(t+r\right)\mathbf{H}^G\mathbf{H} + \mathbf{A}\right)^{-1}\mathbf{H}^G\mathbf{z}_E, \end{aligned} \tag{21}$$

$$\begin{aligned} \hat{\mathbf{g}}_R &= \mathbb{E}\left[\mathbf{g}_R\mathbf{z}_E^G\right]\mathbb{E}\left[\mathbf{z}_E\mathbf{z}_E^G\right]^{-1}\mathbf{z}_E \\ &= \sqrt{r}\left(\left(t+r\right)\mathbf{H}^G\mathbf{H} + \mathbf{A}\right)^{-1}\mathbf{H}^G\mathbf{z}_E. \end{aligned} \tag{22}$$

For this approximation, the matrix of the mean square error (MSE) is expressed as follows

$$\begin{aligned} \mathbf{S}_\Delta^T &= \mathbb{E}\left[\mathbf{g}_T\mathbf{g}_T^G\right] - \mathbb{E}\left[\mathbf{g}_T\mathbf{z}_E^G\right]\mathbb{E}\left[\mathbf{z}_E\mathbf{z}_E^G\right]^{-1}\mathbb{E}\left[\mathbf{z}_E\mathbf{g}_T^G\right] \\ &= \mathbf{A} - t\psi\mathbf{A} = \left(1 - t\psi\right)\mathbf{A}. \end{aligned} \tag{23}$$

Also,

$$\hat{\mathbf{g}}_R = \sqrt{tr}\psi\mathbf{g}_T + r\psi\mathbf{g}_R\frac{\psi\sqrt{r}}{E_H}\mathbf{H}^G\mathbf{n}_E, \tag{24}$$

and

$$\mathbf{S}_\Delta^R = \left(1 - r\psi\right)\mathbf{A}. \tag{25}$$

Because $\hat{\mathbf{g}}_T$ is a linear function acquired from the Gaussian variables $\mathbf{g}_T$, $\mathbf{g}_R$, $\mathbf{n}_E$, they are all mutually Gaussian, so, the approximation error $\Delta\mathbf{g}_T$ which represents the variance of the Gaussian variables is Gaussian.

The second stage of the model illustrates a scenario where Tx transmits the confidential message and Rx jams concurrently. transmits a signal produced in (2), while the signal transmitted by Rx is represented in (3) for $L_2 \leqslant N_T$ time frames. Then the rate for Tx to Rx is similar to the rate established in (7). It is important to generate Eavesdropper's rate bearing in mind the approximation of her imperfect channel. So, Eavesdropper obtains

$$\bar{\mathbf{z}}_E\left(l\right) = \sqrt{t}\mathbf{I}\mathbf{N}_1\mathbf{d}\left(l\right) + \sqrt{t}\mathbf{I}\mathbf{N}_2\mathbf{c}_T\left(l\right) + \sqrt{r}\mathbf{I}\mathbf{c}_R\left(l\right) - \mathbf{n}_E\left(l\right) \tag{26}$$

On the other hand, the Eavesdropper employs the LMMSE approximation approximate so as to approximate $\mathbf{d}\left(l\right)$ from $\bar{\mathbf{z}}_E\left(l\right)$. This approximation is derived as

$$\hat{\mathbf{d}}\left(l\right) = \mathbf{X}^G\mathbf{E}^{-1}\bar{\mathbf{z}}_E\left(l\right) \tag{27}$$

where,

$$\mathbf{X} = \mathbb{E}\left[\bar{\mathbf{z}}_E\mathbf{d}^G\left|\hat{\mathbf{g}}_T\right.\right] = \sqrt{t}\mathbb{E}\left[\mathbf{I}\left|\hat{\mathbf{g}}_T\right.\right]\mathbf{N}_1\mathbf{U}_i = \sqrt{t}\hat{\mathbf{I}}\mathbf{N}_1\mathbf{U}_i, \tag{28}$$

and

$$\begin{aligned} \mathbf{E} &= \mathbb{E}\left[\bar{\mathbf{z}}_E\bar{\mathbf{z}}_E^G\left|\hat{\mathbf{g}}_T, \hat{\mathbf{g}}_R\right.\right] \\ &= \mathbb{E}\left[t\mathbf{I}\left(\mathbf{N}_1\mathbf{U}_i\mathbf{N}_1^G + \tfrac{P_n}{N_T-i}\mathbf{N}_2\mathbf{N}_2^G\right)\mathbf{I}^G\left|\hat{\mathbf{g}}_T\right.\right] \\ &+ \mathbb{E}\left[\tfrac{rP_R}{N_R}\mathbf{J}\mathbf{J}^G\left|\hat{\mathbf{g}}_T\right.\right] + \mathbf{A} \\ &= t\mathbb{E}\left[\mathbf{I}\mathbf{W}\mathbf{I}^G\left|\hat{\mathbf{g}}_T\right.\right] + \tfrac{rP_R}{N_R}\mathbb{E}\left[\mathbf{J}\mathbf{J}^G\left|\hat{\mathbf{g}}_R\right.\right] + \mathbf{A}, \end{aligned} \tag{29}$$

In order to achieve a significant comparison against the preceding results, suppose that $\mathbf{U}_i = \frac{P_d}{i}\mathbf{A}$. Therefore, $C_{TE}^{(2)}$ can be derived as follows

$$\begin{aligned} C_{TE}^{(2)} &= \log\left|\mathbf{A} + \tfrac{tP_n}{\gamma(N_T-i)}\hat{\mathbf{I}}_2\hat{\mathbf{I}}_2^G + \tfrac{rP_R}{\gamma N_R}\hat{\mathbf{J}}\hat{\mathbf{J}}^G + \tfrac{tP_d}{\gamma i}\hat{\mathbf{I}}_1\hat{\mathbf{I}}_1^G\right| \\ &- \log\left|\mathbf{A} + \tfrac{tP_n}{\gamma(N_T-i)}\hat{\mathbf{I}}_2\hat{\mathbf{I}}_2^G + \tfrac{rP_R}{\gamma N_R}\hat{\mathbf{J}}\hat{\mathbf{J}}^G\right| \end{aligned} \tag{30}$$

In conclusion, Eavesdropper's asymptotic rate can be realized as

$$\frac{C_{TE}^{(2)}}{N_E} \overset{a.s.}{\to} \left(\Phi\left(\delta_3, \Theta_3, \beta_3\right) - \Phi\left(\delta_4, \Theta_4, \beta_4\right)\right), \tag{31}$$

$$C_{TE}^{(2)} \simeq i \log\left(1 + \frac{N_E t P_d \omega_T}{\gamma i}\right). \tag{32}$$

In order to compare our results with preceding findings, assuming $i = N_R$, we have

$$C_{TE}^{(2)} \simeq \hat{C}_{TE} \triangleq N_R \log\left(1 + \frac{N_E t P_d \omega_T}{\gamma N_R}\right). \tag{33}$$

Also, the following measure is established to prove the outperformance of the proposed OPCECA.

$$\begin{aligned} \Delta C_{TE} &\triangleq \tilde{C}_{TE} - \hat{C}_{TE} \\ &= N_R \log\left(\frac{1+\frac{N_E t P_d}{N_R}}{1+\frac{N_E t P_d \omega_T}{\gamma N_R}}\right) \simeq N_R \log\left(\frac{\gamma}{\omega_T}\right) \end{aligned} \tag{34}$$

and it is the estimated decrease of the asymptotic rate of Eavesdropper as a result of the engagement of OPCECA technique. Thus, it is easier to demonstrate that as t and E_H are increased, respectively. Apparently, assuming P_T or P_R is randomly increased (desirably P_T as C_{TR} is growing alongside P_T different from P_R), then this decrease can be increased to attain anticipated privacy in most harmful scenarios with enormous number of antennas belonging to the eavesdropper.

IV. Simulation and Results

In Fig. 4, the reliance of OPCECA performance on the Eavesdropper's proximity from the transmitter (Δ) is illustrated using $N_T = N_B = 16$, $i = 1$, $P_T = P_R = 2P_d = 40$dB, with a shortest time of channel coherence. Using 1000 channel actualization's, the average rate computed. The simulation indicates that as the proximity between Eavesdropper and Tx gets nearer, likewise, increase is not only observed at her rate, but better accuracy is likewise witnessed at her channel estimation (as seen from the slope of the curves). For example, when $t \gg r$, $\sqrt{t}\mathbf{I} + \sqrt{r}\mathbf{J} \simeq \sqrt{t}\mathbf{I}$ is realized and at the training stage $\mathbf{I}$ can be estimated by Eavesdropper using higher precision. In the same way, analysis in the figure demonstrates the outperformance OPCECA, considering that privacy rate is only compelled to zero as N_E is significantly large unlike N_T or N_R (over 10 times in the most harmful scenario). Table I presents the simulation parameters and their respective derivations.

TABLE I
SIMULATION PARAMETERS AND DESCRIPTION

Parameters	Descriptions
Overall system bandwidth	6 MHz
Number of receiving antennas	16
Number of transmitting antennas	16
Channel frequency	3.0 GHz
Minimum required data rate	150 kbps/Hz
Regularized power for path loss	40 dB
Channel bandwidth	15MHz

The precision of the approximation is illustrated in Fig. 2 where $N_E\varphi_{TE}$ is measured against $\tilde{C}_{TE}$ assuming that $N_T = 2$, $N_R = 8$, and $P_T = P_R = 2P_d = 2P_n$. The result indicates that as N_E increases while the number of antennas for the transmitting and receiving channels remain constant, the Eavesdropper's rate is not impacted by the artificial noise, hence, user privacy could still be undermined without difficulty.

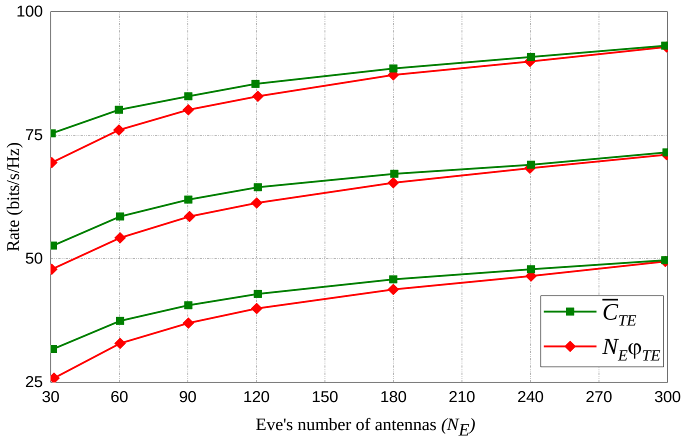

Fig. 2. Performance of the convergence of $\bar{C}_{TE}$ to $N_E\varphi_{TE}$ using parameters $P_T = 20\text{dB}, 30\text{dB}$ and 40dB

With the purpose of analyzing this susceptibility better, we scout for the Eavesdropper's least number of antennas that results in zero privacy $\left(\tilde{N}_E\right)$ by using mathematical analysis to explain the nonlinear classification of equations that results in $\sum = 0$. The performance of $\tilde{N}_E$ against N_A is compared in Fig. 3 when $\beta_1 = 5$ and by utilizing either the optimal parameters (which will be derived later) or non-optimal parameters selected as $P_d = P_n = \frac{P_T}{2}$, $P_T = P_R$, $i = N_R$, $\mathbf{U}_i = \frac{P_d}{N_R}\mathbf{A}$.

The observations from Fig. 3 shows that Eavesdropper may have an advantage with respect to rate by growing the number of her antennas as bulky as possible in order to realize a sophisticated rate than the Receiver's which basically propels privacy to zero. But then again, assume N_E is constrained, then the arising question will be how to improve the broadcasting parameters in such a way that Eavesdropper's activity is made complex. This becomes the focus of our analysis in the preceding section

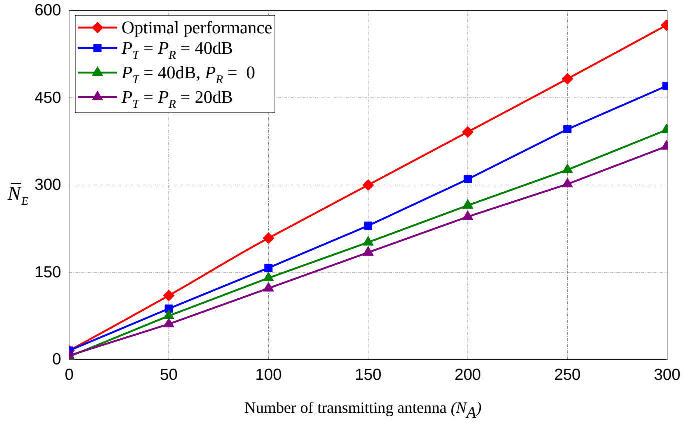

Fig. 3. Evaluating the performance of $\bar{N}_E$ against the number of transmitting antennas using different parameters

Further, Fig. 5 demonstrates the privacy optimization gains of OPCECA, using $N_T = N_R$, $i = 1$, $P_T = P_B = 2P_d$, at a very short time of channel coherence. The findings indicate that

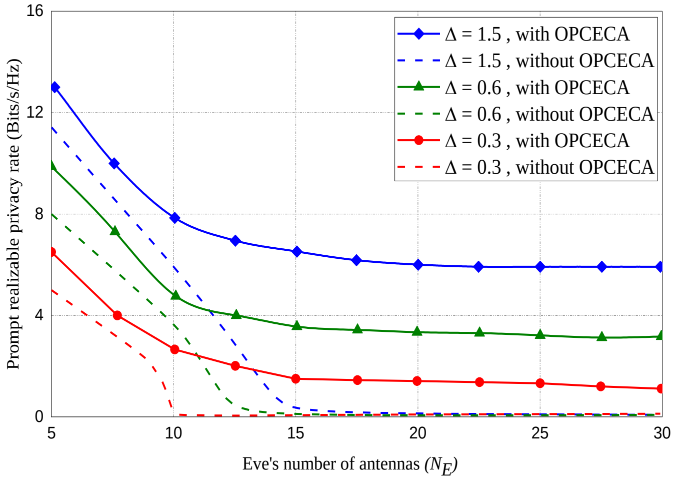

Fig. 4. Evaluating the performance of OPCECA against Δ and N_E .

$\tilde{N}_E$ is enormously huge even for small number of antennas at the legitimate transmission nodes. Therefore, the Eavesdropper compelling privacy to zero is practically achievable.

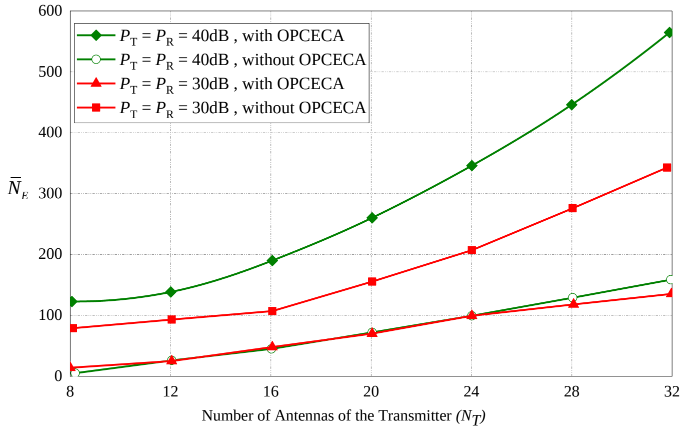

Fig. 5. Evaluating the performance of $\bar{N}_E$ against N_T with and without OPCECA

Assume that the coherence time for all channels is long to facilitate $L_2 \gg N_T$. Consequently, the quantity of data (or ambiguity) transmitted by Eavesdropper's channel turn out to be significantly reduced unlike that transmitted by the data signal, then, Eavesdropper can realize higher rates as against utilizing the approximation technique.

For ease of investigation, it is assumed that instead of utilizing artificial noise at their information stage, Tx and Rx utilized OPCECA in the training stage with the intention of ensuring that the Eavesdropper does not have a precise knowledge of $\mathbf{I}$. At the information stage, the signal the Eavesdropper received at time frame $l = 1, ..., L_2$ is defined as $\mathbf{z}_E(l) = \sqrt{t}\mathbf{Id}_T(l) + \mathbf{n}_E(l)$

The performance of privacy in the unknown structure is compared against the scenario where Eavesdropper's channel is completely known to her, and the result illustrated in Fig.6. For this simulation, we set $N_T - N_R = 8$, while the average rate is computed by 1,000 different channel actualization's. For each actualization, $\mathbf{D}$ is autonomously actualized based on a 4-QAM combination. Clearly, we observe that provided that the channel coherence time is less than two times N_T , a high privacy is achieved even without deploying any artificial noise. It is important to note that in a scenario whereby the channel coherence time is extended, Tx and Rx can utilize recurrence ciphers to refute Eavesdropper of the gain which comes as a result of an extended coherence time.

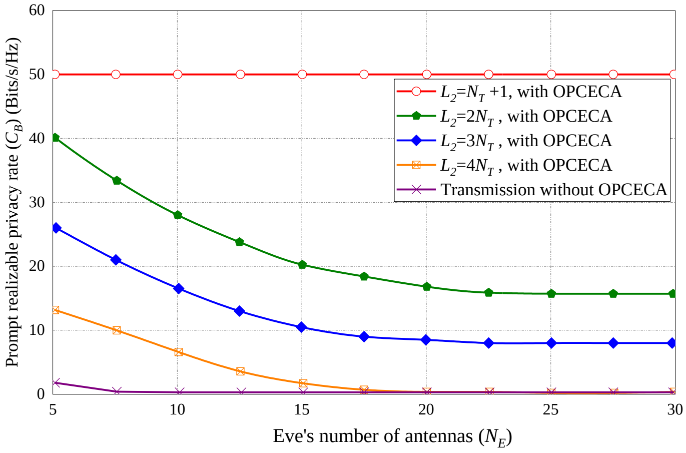

Fig. 6. Illustration of OPCECA performance against N_T and L_2 using Long channel coherence time expression

Lastly, the demonstration which shows that with the increase of L_2 , the proximity of the blind rate becomes nearer to Eavesdropper's rate when she has a complete knowledge of her CSI.

For this simulation, we set $N_T - N_R = 16$, $N_T - N_R = 8$ while the average rate is computed by 1,000 different channel actualization's. Hence, for each actualization, $\mathbf{D}$ is autonomously actualized based on a 4-QAM combination.

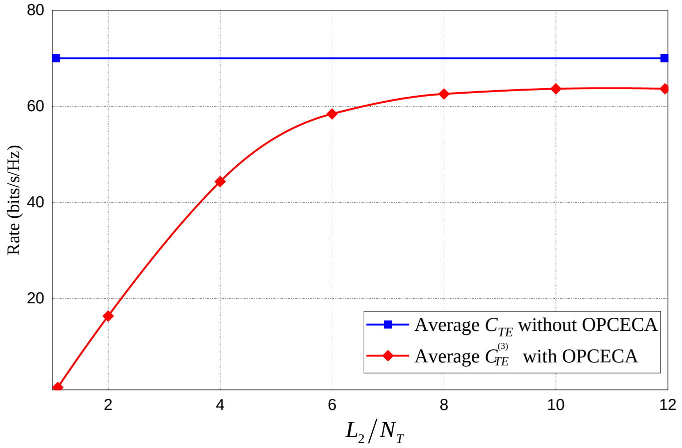

Fig. 7. Illustration of OPCECA performance against N_T and L_2 using Long channel coherence time expression

Assuming statistical information about Eavesdropper's CSI is not known to her, then, it is difficult for Eavesdropper to engage the approximation techniques which was earlier illustrated. Thus, the parameters of the multiple of N_T are completely secured, and it is impossible for Eavesdropper to estimate them. Let's say Tx and Rx concurrently sends information, there is an increase of this number as $(N_T + N_R) \times (N_T + N_R)$.

The gains to the Eavesdropper which might be false in some scenarios were presented in preceding sections. Bearing this in mind, one question that arise at this point is, assuming OPCECA is not utilized, then, what impact will be felt when the Eavesdropper is knowledgeable of her own CSI instead of $\mathbf{G}$? For this scenario, let us examine the information that can be known by the Eavesdropper. In (27), $\bar{\mathbf{z}}_E$ is received by the Eavesdropper. Utilizing the knowledge of $\sqrt{t}\mathbf{I}$, the approximate of $\mathbf{N}_1\mathbf{d}\left(l\right)$ can be achieved by the Eavesdropper. Along with the ambiguities connected to $\mathbf{N}_1\mathbf{d}\left(l\right)$, if $i = N_R$, then the parameters of Tx can be said to be completely secured, contrarily to OPCECA's parameters. So, a new benefit of OPCECA is expressed.

V. Conclusion

In summary, privacy optimization in wireless IIoTs communications using different setups have been examined in this research. The major focus of the investigation in this study is about establishing efficient privacy in a IIoTs-MIMOME communications scenario where the Eavesdroppers are equipped with multi-antenna (jamming at the network layer) at unidentified positions. Also, the study considers a scenario where both the Transmitter and Receiver transmits unidentified CSI coupled with artificial noise with the intention of minimizing the activities of the eavesdroppers. Firstly, a closed-form derivation for asymptotic regularized prompt privacy rate is presented for this system. Consistent with the derived result, methods to attain a controllable optimization problem which enables both the Transmitter and Receiver to estimate optimal broadcasting parameters were proposed. The simulations of the asymptotic investigation show that if the eavesdropper possess sufficient CSI knowledge, she can force privacy to zero by accumulating the number of her antennas notwithstanding the use of optimal parameters. In order to tackle this challenge, a new model which is referred as Optimal Counter-Eavesdropping Channel Approximation (OPCECA) is proposed as a new channel approximation method which permits legitimate nodes to transmit inform without the Eavesdropper obtaining precise channel approximations, thus, leaving her incapacitated. This model is capable of averting any hostile effect of Eavesdropper's location as well as preserve privacy. The investigation established a clarity between the scenarios of short and long channel coherence time and further examined the Eavesdropper's optimal performance coupled with how her method influences privacy. Finally, the study illustrates the performance advantage of OPCECA and presents that the use of artificial noise is effective when the proposed OPCECA technique is employed. In a future study, we will be investigating the diverse theoretical and other real-world applications of the OPCECA model.

References

[1] A. S. Lalos, E. Vlachos, K. Berberidis, A. P. Fournaris, and C. Koulamas, "Privacy preservation in industrial iot via fast adaptive correlation matrix completion," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 12, pp. 7765–7773, 2020.

[2] I. Razzak, M. K. Khan, and G. Xu, "Privacy-preserving federated machine learning solutions for enhanced security of critical energy infrastructures," *IEEE Transactions on Industrial Informatics*, pp. 1–1, 2021.

[3] W. Wang, H. Xu, M. Alazab, T. R. Gadekallu, Z. Han, and C. Su, "Blockchain-based reliable and efficient certificateless signature for iiot devices," *IEEE Transactions on Industrial Informatics*, pp. 1–1, 2021.

[4] M. Zhang, J. Chen, S. He, L. Yang, X. Gong, and J. Zhang, "Privacy-preserving database assisted spectrum access for industrial internet of things: A distributed learning approach," *IEEE Transactions on Industrial Electronics*, vol. 67, no. 8, pp. 7094–7103, 2020.

[5] T. Gebremichael, L. P. I. Ledwaba, M. H. Eldefrawy, G. P. Hancke, N. Pereira, M. Gidlund, and J. Akerberg, "Security and privacy in the industrial internet of things: Current standards and future challenges," *IEEE Access*, vol. 8, pp. 152 351–152 366, 2020.

[6] C. Iwendi, J. H. Anajemba, C. Biamba, and D. Ngabo, "Security of things intrusion detection system for smart healthcare," *Electronics*, vol. 10, no. 12, 2021. [Online]. Available: https://www.mdpi.com/2079-9292/10/12/1375

[7] J. Xiong, R. Ma, L. Chen, Y. Tian, Q. Li, X. Liu, and Z. Yao, "A personalized privacy protection framework for mobile crowdsensing in iiot," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 4231–4241, 2020.

[8] 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, 2020. [Online]. Available: https://www.mdpi.com/1424-8220/20/9/2609

[9] J. H. Anajemba, T. Yue, C. Iwendi, P. Chatterjee, D. Ngabo, and W. S. Alnumay, "A secure multi-user privacy technique for wireless iot networks using stochastic privacy optimization," *IEEE Internet of Things Journal*, pp. 1–1, 2021.

[10] Y. Huo, C. Meng, R. Li, and T. Jing, "An overview of privacy preserving schemes for industrial internet of things," *China Communications*, vol. 17, no. 10, pp. 1–18, 2020.

[11] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas i: The misome wiretap channel," *IEEE Transactions on Information Theory*, vol. 56, no. 7, pp. 3088–3104, 2010.

[12] S. Siboni, V. Sachidananda, Y. Meidan, M. Bohadana, Y. Mathov, S. Bhairav, A. Shabtai, and Y. Elovici, "Security testbed for internet-of-things devices," *IEEE Transactions on Reliability*, vol. 68, no. 1, pp. 23–44, 2019.

[13] J. Heo, J. Kim, J. Paek, and S. Bahk, "Mitigating stealthy jamming attacks in low-power and lossy wireless networks," *Journal of Communications and Networks*, vol. 20, no. 2, pp. 219–230, 2018.

[14] M. Li, I. Koutsopoulos, and R. Poovendran, "Optimal jamming attack strategies and network defense policies in wireless sensor networks," *IEEE Transactions on Mobile Computing*, vol. 9, no. 8, pp. 1119–1133, 2010.

[15] X. Wang, S. Garg, H. Lin, M. J. Piran, J. Hu, and M. S. Hossain, "Enabling secure authentication in industrial iot with transfer learning empowered blockchain," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 11, pp. 7725–7733, 2021.

[16] N. Kolokotronis and M. Athanasakos, "Improving physical layer security in df relay networks via two-stage cooperative jamming," in *2016 24th European Signal Processing Conference (EUSIPCO)*, 2016, pp. 1173–1177.

[17] C. Yin, J. Xi, R. Sun, and J. Wang, "Location privacy protection based on differential privacy strategy for big data in industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3628–3636, 2018.

[18] N. Bugshan, I. Khalil, N. Moustafa, and M. S. Rahman, "Privacy-preserving microservices in industrial internet of things driven smart applications," *IEEE Internet of Things Journal*, pp. 1–1, 2021.

[19] U. Tefek, A. Tandon, and T. J. Lim, "Malicious relay detection using sentinels: A stochastic geometry framework," *Journal of Communications and Networks*, vol. 22, no. 4, pp. 303–315, 2020.

[20] R. Nirala, S. S. Chauhan, and G. Verma, "Improving physical layer security in full-duplex relaying system," in *2017 2nd IEEE International Conference on Recent Trends in Electronics, Information Communication Technology (RTEICT)*, 2017, pp. 997–1001.