Encryption-Aware PHY Security for Wiretap Channels with Multiple Independent Jammers

Tarig Sadig, *Student Member, IEEE,* Mehdi Maleki, Nghi H. Tran, *Senior Member, IEEE,*
Hamid Reza Bahrami, *Senior Member, IEEE*
Department of Electrical & Computer Engineering, The University of Akron, Akron, OH, USA

2023 Wireless Telecommunications Symposium (WTS) | 978-1-6654-9092-4/23/$31.00 ©2023 IEEE | DOI: 10.1109/WTS2023685.2023.10131796

***Abstract*—In conventional physical layer security schemes no leakage of private information to adversary nodes is tolerated, and no assumption on the encryption of information is considered. This is a limiting assumption in physical layer security, which compromises the efficiency of such schemes. This paper introduces an approach in which a prior knowledge of encryption can be used to improve the security performance of cooperative jamming in Gaussian wiretap channels as an example of physical layer security approached. The proposed approach, however, is not limited to the considered scenario of cooperative jamming and can be applied to other scenarios. We consider a system composed of a transmitter, a receiver, and eavesdropper and several jamming nodes that work independently, and formulate an optimization problem to maximize the secrecy rate with the knowledge of encryption and attempt to solve it by driving the rate-equivocation region to constrain and determine the feasibility of the solution. We then exploit a linear approximation to solve the resulted nonconvex optimization problem to maximize the secure transmission rate. Our numerical results show that prior knowledge of encryption can be exploited to allocate the available power to the jamming nodes to significantly increase the secure transmission rate.**

***Index terms*— Physical layer security; encryption; Gaussian wiretap channel; rate-equivocation region; secrecy capacity; cooperative jamming.**

I. Introduction

Physical layer (PHY) security has emerged as a strategy that guarantees an information-theoretic secrecy, regardless of eavesdropper's computational power. The main objective of PHY security is to exploit channel randomness to ensure that an eavesdropper cannot successfully decode the confidential message, while at the same time, guaranteeing a reliable transmission between the source and the legitimate destination. In other words, the goal is to obtain the secrecy capacity which refers to the maximum transmission rate that is both reliable and secure. One approach to improve the performance of PHY security is to utilize additional cooperative jamming nodes. Cooperative jamming makes use of additional nodes as aides in order to achieve higher transmission rates, while ensuring perfect secrecy. Assuming plain-text transmission, the jamming nodes cooperatively work to perform relaying [1], jamming [2], [3] or both in a hybrid fashion [4].

On the other hand, conventional cryptography schemes are made to be robust against attackers with full access to *error-free* ciphertext [5]–[7]. However, in practice, erroneous reception is inevitable. Toward a practical cryptographic design, the authors in [8]–[10] introduce the concept of noisy ciphertext and show its effectiveness from an application layer perspective. In [11], we introduce a general framework to study the joint impact of PHY security and encryption. Particularly, we show that, having a prior knowledge of encryption, one can deliberately allow leakage to the eavesdropper to be able to securely transmit at a rate beyond the conventional secrecy capacity.

In this paper, we apply the framework that we have first introduced in [11] to a Gaussian wiretap channel with multiple independent jammers. First, we drive a general rate-equivocation region. We then use the approach to maximize the secure transmission rate. Our numerical results show a significant improvement in the secure transmission rate when encryption is taken into account. The rest of the paper has been organized as follows. In Section II, we introduce the system model for a Gaussian wiretap channel with multiple jamming nodes. In Section III, we briefly summarize and formulate the secrecy rate maximization in conventional PHY security. In Section IV, we introduce and characterize the rate-equivocation region as well as the encryption-aware secrecy capacity. In Section V, we formulate and solve the optimization problem to maximize the encryption-aware secrecy rate for the considered wiretap channel with multiple independent jammers. Section VI presents some insightful numerical results and discussions, and Section VII concludes the paper.

II. System Model

Fig. 1 depicts a cooperative jamming system with a transmitter Alice, a receiver Bob, an eavesdropper Eve, and a group of M jammers, $J_1, J_2, \cdots, J_M$. It is assumed that all the nodes are equipped with single antenna. Alice desires to transmit private message to the legitimate destination Bob without any leakage of information to the eavesdropper. The jammers help the source by deliberately introducing noise to confuse Eve's observation. The transmitter sends a zero mean complex Gaussian codeword $x_s \sim \mathcal{CN}(0, \rho_s)$, where ρ_S is Alice's power budget. The group of jammers broadcasts $\mathbf{x} \sim \mathcal{CN}(\mathbf{0}, \mathbf{Q})$, where $\mathbf{0}$ is the mean vector and $\mathbf{Q}$ is the covariance matrix of $\mathbf{x}$; each jammer sends a zero mean complex Gaussian noise signal x_i whose power is $\rho_i = |x_i|^2$. h_0 and g_0 denote the complex gains of the source-destination and source-eavesdropper, respectively. We also have the column vectors $\boldsymbol{h} = [h_1, h_2, \cdots, h_M]^T$ and $\boldsymbol{g} = [g_1, g_2, \cdots, g_M]^T$, where h_i denotes the complex channel gain between the jammer J_i and the destination, while g_i represents the complex channel gain between the jammer J_i and the eavesdropper. Thus, the

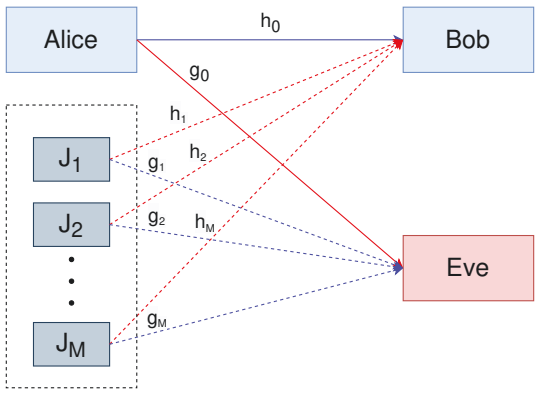

Figure 1. A wiretap channel model with multiple jammers

received signals at Bob and Eve can be written, respectively, as

$$Y = h_0 x_s + \sum_{i=1}^{M} h_i x_i + n_B \tag{1}$$

$$Z = g_0 x_s + \sum_{i=1}^{M} g_i x_i + n_E, \tag{2}$$

where n_B and n_E are independent identically distributed (i.i.d) additive white Gaussian noise (AWGN) samples with variances σ_B^2 and σ_E^2, respectively. We shall assume that $\sigma_B^2 = \sigma_E^2 = 1$.

III. Secrecy Capacity for Multiple Jammers Scheme

The achievable secrecy rate can be written as

$$\begin{aligned} R_s &= [R_b - R_e]^+ \\ &= \left[\log_2(1+\gamma_B) - \log_2(1+\gamma_E)\right]^+, \end{aligned} \tag{3}$$

where R_b is the main channel rate and R_e is the eavesdropper channel rate, and

$$\gamma_B = \frac{\rho_s \left|h_0\right|^2}{\boldsymbol{h}^\dagger \mathbf{Q} \boldsymbol{h} + 1} \tag{4}$$

$$\gamma_E = \frac{\rho_s \left|g_0\right|^2}{\boldsymbol{g}^\dagger \mathbf{Q} \boldsymbol{g} + 1}, \tag{5}$$

are the signal to interference plus noise ratios at Bob and Eve, respectively, where $\dagger$ denotes the Hermitian transpose. For a fixed transmission power, the main channel capacity and the secrecy capacity are to be obtained via maximizations over $\mathbf{Q}$. On the one hand, the main channel capacity R_B is achieved by the covariance matrix $\mathbf{Q}^{(B)}$, which can be readily found by eliminating interference caused by the jammers at the legitimate destination; i.e., $\mathbf{Q}^{(B)} \in \{\mathbf{Q} : \boldsymbol{h}^\dagger \mathbf{Q} \boldsymbol{h} = 0, \quad \mathbf{Q} \succeq \mathbf{0}\}$. On the other hand, the secrecy capacity R_S is achieved by $\mathbf{Q}^{(S)}$ which, under joint power constraint, can be obtained by solving

$$\begin{aligned} R_S = \underset{\mathbf{Q}}{\text{maximize}} \quad & R_s(\mathbf{Q}) \\ \text{subject to} \quad & \text{tr}(\mathbf{Q}) \le P_T, \end{aligned} \tag{6}$$

where P_T is the total available jamming power. In order to solve (6), one should first develop the condition(s) under which a nonzero secrecy rate is achievable (i.e., $R_s > 0$). In order to solve (6), the first step is to maximize the interference caused by the jammers at Eve, while at the legitimate receiver, the interference is fixed to a scalar $t \ge 0$; that is

$$\begin{aligned} \underset{\mathbf{Q}}{\text{maximize}} \quad & \boldsymbol{g}^\dagger \mathbf{Q} \boldsymbol{g} \\ \text{subject to} \quad & \boldsymbol{h}^\dagger \mathbf{Q} \boldsymbol{h} = t, \\ & \text{tr}(\mathbf{Q}) \le P_T. \end{aligned} \tag{7}$$

Assuming $\mathbf{Q}^{(t)}$ is the solution to (7), the secrecy capacity problem becomes

$$R_S = \underset{t}{\text{maximize}} \quad \log_2 \left(\frac{1 + \frac{\rho_s |h_0|^2}{t+1}}{1 + \frac{\rho_s |g_0|^2}{\boldsymbol{g}^\dagger \mathbf{Q}^{(t)} \boldsymbol{g} + 1}} \right), \tag{8}$$

which can be solved numerically by a one-dimensional search over t. The two problems (6) and (7) are then to be solved iteratively to obtain the optimal covariance matrix $\mathbf{Q}^{(S)}$ and the corresponding optimal jammers induced interference $t^* = \boldsymbol{h}^\dagger \mathbf{Q}^{(S)} \boldsymbol{h}$. It is worth mentioning that $t^* \neq 0$ which means $\mathbf{Q}^{(S)} \notin \{\mathbf{Q} : \boldsymbol{h}^\dagger \mathbf{Q} \boldsymbol{h} = 0, \quad \mathbf{Q} \succeq \mathbf{0}\}$. In other words, it is not possible to achieve both main channel and secrecy capacity using the same covariance matrix.

IV. Rate-Equivocation Region Derivation and Encryption-Aware Secrecy Capacity

In this section, before delving into the effect of encryption, we first characterize the rate-equivocation region of the considered multi-jammer system.

A. Rate-Equivocation Region Characterization

For a specific covariance matrix, we define a subregion denoted as $\bar{\mathcal{R}}^{WTC}(\mathbf{Q})$ within which the rate-equivocation pair (R, R_e) is achievable as

$$\bar{\mathcal{R}}^{WTC}(\mathbf{Q}) = \left\{ \begin{matrix} 0 \le R \le R_b(\mathbf{Q}) \\ (R, R_e) : 0 \le R_e \le R_s(\mathbf{Q}) \\ R_e \le R \end{matrix} \right\}. \tag{9}$$

Altogether, the convex rate-equivocation region can be expressed as

$$\mathcal{R}^{WTC} = \bigcup_{\mathbf{Q} \in \{\mathbf{Q}: \text{tr}(\mathbf{Q}) \le P_T, \ \mathbf{Q} \succeq \mathbf{0}\}} \bar{\mathcal{R}}^{WTC}(\mathbf{Q}). \tag{10}$$

Identifying special boundary points is the first step in characterizing the rate-equivocation region. For a 4-node system, these points are $(R, R_e) = \{(0,0), (R_S, R_S), (R'_B, R_S), (R_B, R'_S), (R_B, 0)\}$, where R'_B is the maximum transmission rate that $R_e = R_S$ is achievable; i.e., $R'_B = R_b(\mathbf{Q}^{(S)})$, and R'_S is the maximum achievable equivocation rate for $R = R_B$, and it can be achieved by

$$\begin{aligned} R'_S = \underset{\mathbf{Q}}{\text{maximize}} \quad & \log_2 \left(\frac{1 + \frac{\rho_s |h_0|^2}{\boldsymbol{h}^\dagger \mathbf{Q} \boldsymbol{h} + 1}}{1 + \frac{\rho_s |g_0|^2}{\boldsymbol{g}^\dagger \mathbf{Q} \boldsymbol{g} + 1}} \right) \\ \text{subject to} \quad & \boldsymbol{h}^\dagger \mathbf{Q} \boldsymbol{h} = 0, \\ & \text{tr}(\mathbf{Q}) \le P_T. \end{aligned} \tag{11}$$

The solution to (11) can analytically be found by the covariance matrix $\mathbf{Q}^* = \boldsymbol{\varphi}^\dagger \boldsymbol{\varphi}$, where

$$\boldsymbol{\varphi} = \mu \|\boldsymbol{h}\|^2 \boldsymbol{g} - \mu \boldsymbol{h}^\dagger \boldsymbol{g} \boldsymbol{h}, \tag{12}$$

and μ is given by

$$\mu = \sqrt{\frac{P_T}{\|\boldsymbol{h}\|^4 \|\boldsymbol{g}\|^2 - \|\boldsymbol{h}\|^2 |\boldsymbol{h}^\dagger \boldsymbol{g}|^2}}. \tag{13}$$

The solution to (11) can result in a nonzero or a zero R'_S. As a consequence, two different typical rate-equivocation regions are depicted in Fig .2.

B. Encryption-Aware Secrecy Capacity

The above results on the secrecy capacity R_S still hold true with encryption under the extreme assumption that Eve can completely recover the entire ciphertext without error. However, with error-prone ciphertexts, it is more difficult for Eve to intercept the ciphertext. We define the encryption strength λ parameter to establish a connection between PHY security and encryption. The interested reader is referred to [11]. To ensure secrecy with the added parameter, we relate the equivocation to transmission rate by the following bound

$$\frac{R_e}{R} \geq \frac{1}{\lambda}. \tag{14}$$

The rate maximization problem at the physical layer can now be modified by taking into account an additional constraint imposed by the encryption; i.e., $R \leq \lambda R_e$. This new security condition applied at the physical layer can therefore lead to a larger secrecy region. The new encryption-aware secrecy rate is the solution to the following optimization problem

$$\bar{R}_S \triangleq \sup_R \left\{ R : \left(R, \frac{R}{\lambda} \right) \in \bar{\mathcal{R}}^{WTC} \right\}. \tag{15}$$

The encryption-aware rate, denoted as $\bar{R}_S$, must be within the rate-equivocation region $\mathcal{R}^{WTC}$. In order to obtain $\bar{R}_S$, we proceed by defining two thresholds on encryption strength as $\lambda_{T1} = R'_B/R_S$ and $\lambda_{T2} = R_B/R'_S$. Clearly, for Fig. 2.b, since $R'_S = 0$, we have $\lambda_{T2} = \infty$. The line segments $R = \lambda_{T1} R_e$ and $R = \lambda_{T2} R_e$ divide the region in Fig. 2.a into three subregions, while for Fig. 2.b, the rate-equivocation region is divided into two subregions by the line $R = \lambda_{T1} R_e$. Obviously, for the subregion $1 \leq \lambda \leq \lambda_{T1}$, the encryption-aware secrecy can readily be found as $\bar{R}_S = \lambda R_S$, and for the subregion $\lambda > \lambda_{T2}$, we can securely transmit at the main channel capacity (i.e., $\bar{R}_S = R_B$). On the other hand, for the subregion $\lambda_{T1} < \lambda < \lambda_{T2}$, to evaluate $\bar{R}_S$, we need to solve the following optimization problem

$$\begin{aligned} \bar{R}_S = \underset{\mathbf{Q}}{\text{maximize}} \quad & R_b(\mathbf{Q}) \\ \text{subject to} \quad & \text{tr}(\mathbf{Q}) \leq P_T, \\ & R_b(\mathbf{Q}) = \lambda R_s(\mathbf{Q}). \end{aligned} \tag{16}$$

In summary, letting $\mathbf{Q}^{(\lambda)}$ be the solution to (16), the encryption-aware rate can be obtained as

$$\bar{R}_S = \begin{cases} \lambda R_S & 1 \leq \lambda \leq \lambda_{T1} \\ \lambda R_s\left(\mathbf{Q}^{(\lambda)}\right) & \lambda_{T1} < \lambda < \lambda_{T2} \\ R_B & \lambda \geq \lambda_{T2} \end{cases}. \tag{17}$$

Now, we focus our attention on solving the problem (16). It is easy to check that, by simple manipulations and letting $K_1 = \rho_s |h_0|^2$ and $K_1 = \rho_s |g_0|^2$, the matrix $\mathbf{Q}^{(\lambda)}$ can equivalently be obtained as a solution to

$$\begin{aligned} \underset{\mathbf{Q}}{\text{minimize}} \quad & \boldsymbol{h}^\dagger \mathbf{Q} \boldsymbol{h} \\ \text{subject to} \quad & \text{tr}(\mathbf{Q}) \leq P_T, \\ & \boldsymbol{h}^\dagger \mathbf{Q} \boldsymbol{h} = \frac{K_1}{\left(1 + \frac{K_2}{1 + \boldsymbol{g}^\dagger \mathbf{Q} \boldsymbol{g}}\right)^\xi - 1} - 1, \end{aligned} \tag{18}$$

where $\xi = \frac{\lambda}{\lambda - 1}$.

V. Multiple Jammers with Independent Transmission

In this section, we shall consider a special case of (18) under the assumption that the jammers send completely independent signals. As we shall demonstrate shortly, the obtained results shed new light on the optimal power allocation at the jammers, which will be beneficial in generalizing the results to the general optimization problem in (18).

A. Secrecy Problem Modification

With the independent jamming assumption, we consider the individual jammer powers $\boldsymbol{\rho} = [\rho_1, \rho_2, \cdots, \rho_M]^T$ instead of the covariance matrix. We define $\alpha_i = |h_i|^2$ and $\beta_i = |g_i|^2, \quad \forall i = \{0, 1, 2, 3, \cdots, M\}$, to represent the power gain corresponding to each complex channel gain. Then, we can write

$$\gamma_B^I = \frac{\rho_s \alpha_0}{\sum_{i=1}^M \rho_i \alpha_i + 1} \tag{19}$$

$$\gamma_E^I = \frac{\rho_s \beta_0}{\sum_{i=1}^M \rho_i \beta_i + 1}, \tag{20}$$

where γ_B^I and γ_E^I are the signal to interference plus noise ratios at the destination and eavesdropper, respectively. The superscript I refers to independent jamming. The corresponding secrecy capacity R_S^I can be obtained by solving

$$\begin{aligned} R_S^I = \underset{\boldsymbol{\rho}}{\text{maximize}} \quad & R_s^I(\boldsymbol{\rho}) \\ \text{subject to} \quad & \sum_{i=1}^M \rho_i \leq P_T, \end{aligned} \tag{21}$$

where $R_s^I(\boldsymbol{\rho})$ is the secrecy rate and is obtained by

$$\begin{aligned} R_s^I &= \left[R_b^I - R_e^I \right]^+ \\ &= \left[\log_2(1 + \gamma_B^I) - \log_2(1 + \gamma_E^I) \right]^+, \end{aligned} \tag{22}$$

When Encryption awareness is taken into consideration, we can utilize the rate-equivocation region to obtain the encryption-aware secrecy capacity $\bar{R}_S^I$. However, for the special subregion, $\lambda_{T1} < \lambda < \lambda_{T2}$, we seek the optimal power

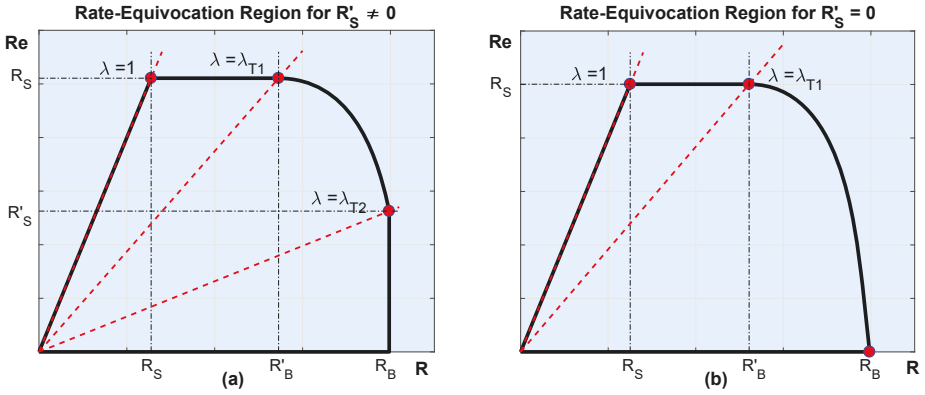

Figure 2. Typical rate-equivocation regions for multi-jammer scenario when (a) $R'_S \neq 0$ and (b) $R'_S = 0$ [11].

allocation $\boldsymbol{\rho}^{(\lambda)}$ that achieves $\bar{R}_S^I$. The problem in (18) can be modified such that we can find $\boldsymbol{\rho}^{(\lambda)}$ by solving

$$\begin{aligned} \underset{\boldsymbol{\rho}}{\text{minimize}} \quad & \sum_{i=1}^{M} \rho_i \alpha_i \\ \text{subject to} \quad & \sum_{i=1}^{M} \rho_i \leq P_T, \\ & \sum_{i=1}^{M} \rho_i \alpha_i = \frac{K_1}{\left(1+\frac{K_2}{1+\sum_{i=1}^{M}\rho_i\beta_i}\right)^{\xi}-1} - 1. \end{aligned} \tag{23}$$

Notably, (23) is an $M-$ dimensional optimization problem with a linear objective function, one linear inequality constraint, and another nonlinear equality constraint. This problem can be approximated as a linear programming (LP) problem by simply approximating the nonlinear equality constraint with a linear function, as we shall see next.

B. Linear Approximation and Duality

Here, we aim to modify the optimization problem in (23) by approximating the nonlinear equality constraint with a linear one. First, let $t_1 = \sum_{i=1}^{M} \rho_i \alpha_i$ and $t_2 = \sum_{i=1}^{M} \rho_i \beta_i$; thus, we can write the equality constraint as

$$t_1 = \frac{K_1}{\left(1+\frac{K_2}{1+t_2}\right)^{\xi}-1} - 1. \tag{24}$$

The curve in (24) is best approximated with the line $t_1 = mt_2 + c$, where $m > 0$ is the slope and $c < 0$ is the t_1 intercept value. Given the approximation, (23) can be written as

$$\begin{aligned} \underset{\boldsymbol{\rho}}{\text{minimize}} \quad & t_1 \\ \text{subject to} \quad & \sum_{i=1}^{M} \rho_i \leq P_T, \\ & t_1 = mt_2 + c. \end{aligned} \tag{25}$$

We now have a linear programming problem with two constraints, whose two-dimensional dual problem can be formulated as

$$\begin{aligned} \underset{\nu_1,\nu_2}{\text{maximize}} \quad & -P_T\nu_1 - c\nu_2 \\ \text{subject to} \quad & \nu_1 + (\alpha_i - m\beta_i)\nu_2 \geq -\alpha_i \qquad i = 1,2,3,\cdots,M, \\ & \nu_1 \geq 0, \end{aligned} \tag{26}$$

where $\nu_1$and ν_2 are the dual variables. The $M+1$ lines, $\nu_1 = 0$ and $\nu_1 + (\alpha_i - m\beta_i)\nu_2 = -\alpha_i$ for all $i \in 1,2,3,\cdots,M$, define a superset of the lines that determine the boundary of this region. Generally, for linear programing, strong duality is achieved; hence

$$\text{minimum} \quad t_1 = \text{maximum} \quad -P_T\nu_1 - c\nu_2 \geq 0, \tag{27}$$

and also complementary slackness conditions are satisfied; we have

$$\nu_1^* \left(\sum_{i=1}^{M} \rho_i^* - P_T\right) = 0 \tag{28}$$

$$\rho_i^* \left(\nu_1^* + (\alpha_i - m\beta_i)\nu_2^* + \alpha_i\right) = 0, \tag{29}$$

The first condition in (28) implies that if $\nu_1^* \neq 0$, then the power constraint in the primal problem should be achieved with equality. Whereas the condition in (29) implies that, at most, *only two* jammers can have nonzero power. Since (26) is a linear programming, the optimal solution (ν_1^*, ν_2^*) lies on the boundary of the feasible region. Therefore, we next develop an approach to identify the set of candidate jammer(s) that are involved in defining the boundary of the feasible region.

C. Solution Algorithm by Characterizing a Pool of Candidate Jammers

Here, we develop the necessary and sufficient conditions that each candidate jammer should satisfy. In addition, we optimally solve the problem (23) for the simplified network. We start by removing redundancy from the feasible region. Since ν_1 and P_T are non-negative and $c < 0$, from (27), we get $\nu_2 \geq 0$; therefore, the optimal solution is to be found in the first quadrant of the dual 2D plane. Moreover, on the feasible region boundary, inequality constraints are satisfied with equality (i.e. $\nu_1 + (\alpha_i - m\beta_i)\nu_2 = -\alpha_i$), and since both ν_1 and ν_2 are non-negative, the slope of these linear constraints $s_i = (m\beta_i - \alpha_i)$ must be positive. For the channel between a jammer J_i and the eavesdropper, we define the encryption-augmented power gain $\tilde{\beta}_i = m\beta_i$. Thus, all selected jammers should satisfy $\tilde{\beta}_i > \alpha_i$. Furthermore, the constraint line, for each jammer J_i, intersects with $\nu_1 = 0$ at the point $\bar{\nu_2}^{(i)} = \alpha_i/(\tilde{\beta}_i - \alpha_i)$. However, the line segment from $\nu_2 = 0$ to $\nu_2 = \min(\bar{\nu_2}^{(i)})$ mandates the lower boundary of the feasible region. Therefore, we sort the jammers satisfying $(\tilde{\beta}_i > \alpha_i)$ in ascending manner based on $\bar{\nu_2}^{(i)}$, which is

an equivalent ordering based on $\frac{\alpha_i}{\beta_i}$. The jammer with the minimum $\frac{\alpha_i}{\beta_i}$ is the first contributor to the feasible region. The remaining candidates will be determined based on the slope s_i. In order to see that, for each J_i whose $(\tilde{\beta}_i > \alpha_i)$, we define the region Ψ_i as

$$\begin{aligned}\Psi_i &= \{(\nu_1, \nu_2) : \nu_1 + (\alpha_i - m\beta_i)\nu_2 \geq -\alpha_i\} \\ &= \{(\nu_1, \nu_2) : \nu_2 \leq \frac{\nu_1}{s_i} + \bar{\nu_2}^{(i)}\}\end{aligned} \tag{30}$$

The whole feasible region Ω can then be given by

$$\Omega = \bigcap_{i=1}^{\bar{M}} \Psi_i, \tag{31}$$

where $\bar{M}$ is the number of jammers that satisfy $(\tilde{\beta}_i > \alpha_i)$. For any two consecutive jammers in the $\bar{\nu_2}^{(i)}$ ordering if $\Psi_i \subset \Psi_{i+1}$ (i.e. $\Psi_i \bigcap \Psi_{i+1} = \Psi_i$), the latter jammer (J_{i+1}) is redundant in obtaining the whole region Ω.

Proposition 1: For a set of $\bar{\nu_2}^{(i)}$-ordered jammers and a J_k candidate jammer, if $s_k > s_j$ (for k and $j \in \{1, 2, 3, \cdots, \bar{M}\}$, and $k < j$), then $\Psi_k \subset \Psi_j$. (i.e., the jammer J_j is not a candidate).

Proof: Let $(\nu_1, \nu_2) \in \Psi_k$; then, we have

$$\nu_2 \leq \frac{\nu_1}{s_k} + \bar{\nu_2}^{(k)}. \tag{32}$$

Indeed, $s_k > s_j$, and since the jammers are in an ascending order, $\bar{\nu_2}^{(k)} < \bar{\nu_2}^{(j)}$. Therefore, we have

$$\nu_2 \leq \frac{\nu_1}{s_k} + \bar{\nu_2}^{(k)} < \frac{\nu_1}{s_j} + \bar{\nu_2}^{(j)}. \tag{33}$$

which means that $(\nu_1, \nu_2) \in \Psi_j$, and hence, $\Psi_k \subset \Psi_j$. ■

In summary, the following steps summarize our algorithm in identifying the pool of the candidate jammers:

(a) In the first step, we discard the jammers that do not satisfy $(\tilde{\beta}_i > \alpha_i)$. If all the jammers are to be discarded, they all should be silenced.
(b) We order the remaining jammers in ascending manner based on $\frac{\alpha_i}{\beta_i}$ and pick the first one to be our dominant candidate.
(c) The rest of the candidates are picked such that the slopes s_i be as well in ascending order.

D. Optimal Power Allocation for the Simplified Network

Although the pool of candidate jammers can contain any number of $\bar{M}$ jammers where $0 \leq \bar{M} \leq M$, only two of which, at most, can actually transmit as outlined by the condition in (29). As a result, we adopt the following approach by deeming that either one or two jammers are needed to maximize the encryption-aware secrecy rate. Essentially, we modify the optimization problem (23) with $M = 1$ or $M = 2$.

In the single jammer scenario $(M = 1)$, we allocate power to the jammer with the smallest $\frac{\alpha_i}{\beta_i}$; the problem (23) becomes

$$\begin{aligned}\underset{\rho}{\text{minimize}} \quad & \rho\alpha \\ \text{subject to} \quad & \rho \leq P_T, \\ & \rho\alpha = \frac{K_1}{\left(1 + \frac{K_2}{1+\rho\beta}\right)^{\xi} - 1} - 1,\end{aligned} \tag{34}$$

We drop the index i for simplicity since only one jammer is selected. However, it is obvious that the optimal power ρ^* can be found directly by solving the nonlinear equation depicted by the equality constraint. On the other hand, for the two jammer scenario $(M = 2)$, as the condition in (28) suggests, the total available power P_T is consumed. Therefor, we can formulate the problem as

$$\begin{aligned}\underset{\rho_1, \rho_2}{\text{minimize}} \quad & \rho_1\alpha_1 + \rho_2\alpha_2 \\ \text{subject to} \quad & \rho_1 + \rho_2 = P_T, \\ & \rho_1\alpha_1 + \rho_2\alpha_2 = \frac{K_1}{\left(1 + \frac{K_2}{1+\rho_1\beta_1+\rho_2\beta_2}\right)^{\xi} - 1} - 1.\end{aligned} \tag{35}$$

Here, the indices 1 and 2, respectively, refer to i and $i + 1$. Note that the optimal powers (ρ_1^*, ρ_2^*) in this case can also be readily found by solving the system of equations depicted by the two equality constraints.

VI. Numerical Results

In this section, with numerical simulations using MATLAB software, we study the effect of encryption awareness on secure transmission rate with the aid of multiple jammers. In particular, we use ten jamming nodes with power gains to Bob and Eve as $\boldsymbol{\alpha} = \{0.06, 0.3, 0.7, 1.3, 2.1, 3, 4.2, 5.52, 7, 8.7\}$ and $\boldsymbol{\beta} = \{0.6, 1.8, 3.4, 5.4, 7.9, 10.7, 13.9, 17.6, 21.6, 26\}$, respectively. We first show the case with $\alpha_0 = 1.5$ and $\beta_0 = 1$, where secrecy is achievable without the help of the jammers, that is $K_1 > K_2$, with a total (normalized) jamming power budget of $10dB$ and a source power of $15dB$. Fig. 3 shows the encryption-aware secrecy rate with and without jammers for different encryption strengths, λ. For small values of encryption strength, we clearly see that the presence of jammers achieves higher secrecy rate, whereas for relatively large λ, even without utilizing the jamming nodes, the secrecy rate saturates at the reliable transmission bound R_B. Further, for the same case where $K_1 > K_2$, Fig. 4 shows the conventional and encryption-aware secure transmission rate for different jamming power budgets, source power of $15dB$, and $\lambda = 3$. Here, we see that the encryption-aware transmission rate always supersedes the conventional secrecy rate. However, we notice that for $P_T \geq 10dB$, more jamming power budget would not result in higher encryption-aware rate, which means that the best jammer is selected and hence the highest possible secure transmission rate is achieved.

On the other hand, for the case with $\alpha_0 = 1$ and $\beta_0 = 1.5$, where jamming is essential to achieve positive secrecy, i.e., $K_1 < K_2$, Fig. 5 shows the encryption-aware secrecy rate with and without jammers for different λ values with ten jammers, total jamming power budget of $10dB$, and a source power of $15dB$. As shown, in this case, the knowledge of the encryption would not be helpful if the jamming nodes are not used. Finally, for this case, Fig. 6 shows a similar behavior as Fig. 4, while the achievable rate is lower and the required jamming power budget to achieve saturation is slightly higher than those of the previous case.

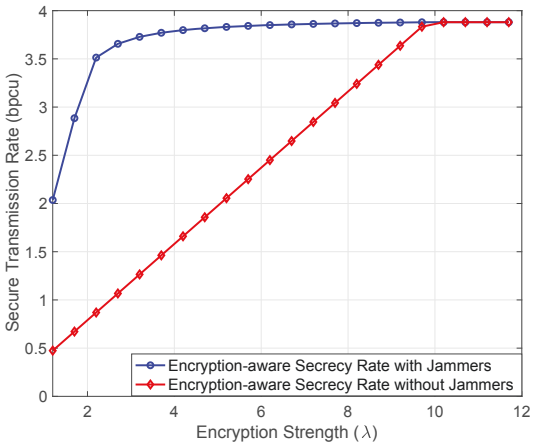

Figure 3. Encryption-aware secrecy rate versus encryption strength ($M = 10$ and $K_1 > K_2$)

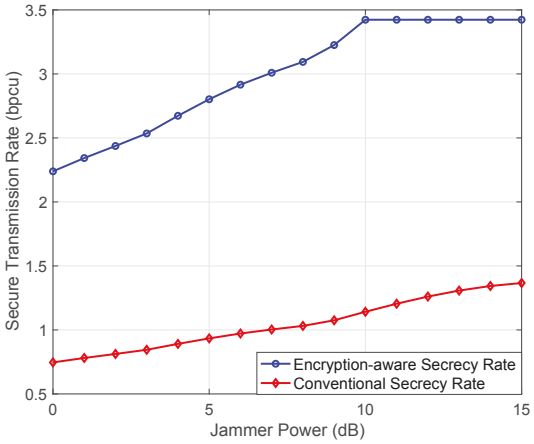

Figure 4. Encryption-aware secrecy rate versus jamming power budget ($M = 10$, $K_1 > K_2$ and $\lambda = 3$)

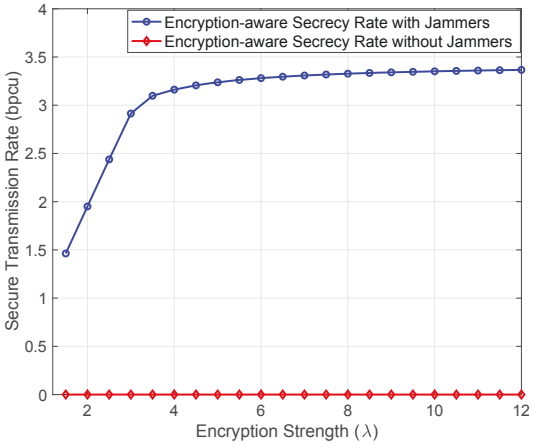

Figure 5. Encryption-aware secrecy rate versus encryption strength ($M = 10$ and $K_1 < K_2$)

VII. Conclusion

We proposed an encryption-aware PHY security approach for a Gaussian wiretap channel with multiple jammers. We first characterized the rate-equivocation region for different scenarios, and for an independent jamming case, we derived an approach to optimally allocate the power under an additional encryption-awareness constraint. We showed that, at most, only two jammers are needed to achieve optimal encryption-aware secrecy rate. We also introduced an ordering mechanism by which we were able to accurately determine the candidate jammers. Our numerical results showed that the knowledge of encryption can significantly improve the transmission rate compared to the case that the encryption is ignored.

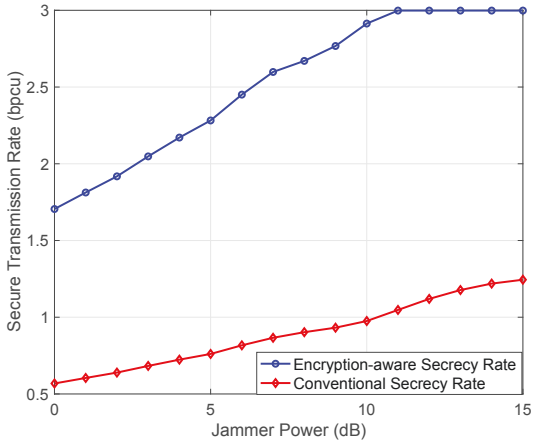

Figure 6. Encryption-aware secrecy rate for different jamming power budgets ($M = 10$, $K_1 < K_2$ and $\lambda = 3$)

VIII. Acknowledgment

This material is based upon work supported in part by the National Science Foundation under Grant No. SaTC-1956110.

References

[1] G. Zhang, Y. Gao, H. Luo, S. Wang, M. Guo, and N. Sha, "Security performance analysis for best relay selection in energy-harvesting cooperative communication networks," *IEEE Access*, vol. 8, pp. 26–36, 2020.

[2] Z. Cao, X. Ji, J. Wang, W. Wang, K. Cumanan, Z. Ding, and O. A. Dobre, "Artificial noise aided secure communications for cooperative NOMA networks," *IEEE Transactions on Cognitive Communications and Networking*, vol. 8, no. 2, pp. 946–963, jun 2022.

[3] J. Hu, Y. Cai, N. Yang, X. Zhou, and W. Yang, "Artificial-noise-aided secure transmission scheme with limited training and feedback overhead," *IEEE Transactions on Wireless Communications*, vol. 16, no. 1, pp. 193–205, Jan. 2017.

[4] T. Hu, F. Ma, Y. Shang, and Y. Cheng, "Physical layer security of untrusted UAV-enabled relaying NOMA network using SWIPT and the cooperative jamming," in *2021 IEEE 94th Vehicular Technology Conference (VTC2021-Fall)*. IEEE, sep 2021.

[5] D.-S. Lee, "Substitution deciphering based on HMMs with applications to compressed document processing," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 24, no. 12, pp. 1661–1666, Dec. 2002.

[6] Siegenthaler, "Decrypting a class of stream ciphers using ciphertext only," *IEEE Transactions on Computers*, vol. C-34, no. 1, pp. 81–85, Jan. 1985.

[7] T. Johansson and F. Jonsson, "Theoretical analysis of a correlation attack based on convolutional codes," *IEEE Transactions on Information Theory*, vol. 48, no. 8, pp. 2173–2181, Aug. 2002.

[8] W. K. Harrison and S. W. McLaughlin, "Physical-layer security: Combining error control coding and cryptography," in *2009 IEEE International Conference on Communications*. IEEE, Jun. 2009.

[9] ——, "Equivocations for the simple substitution cipher with erasure-prone ciphertext," in *2012 IEEE Information Theory Workshop*. IEEE, Sep. 2012.

[10] N. L. Gross and W. K. Harrison, "An analysis of an HMM-based attack on the substitution cipher with error-prone ciphertext," in *2014 IEEE International Conference on Communications (ICC)*. IEEE, Jun 2014.

[11] T. Sadig, M. Maleki, N. H. Tran, and H. R. Bahrami, "An encryption-aware PHY security framework for 4-node gaussian wiretap channels with joint power constraint," *IEEE Transactions on Communications*, vol. 68, no. 12, pp. 7837–7850, 2020.