Encryption-Aided Physical Layer Security via Cooperative Jamming: Beyond Secrecy Capacity with Noisy Ciphertext

Tarig Sadig, Mehdi Maleki, Nghi H. Tran, and Hamid Reza Bahrami
Department of Electrical & Computer Engineering, The University of Akron, Akron, OH, USA

2023 IEEE Wireless Communications and Networking Conference (WCNC) | 978-1-6654-9122-8/23/$31.00 ©2023 IEEE | DOI: 10.1109/WCNC55385.2023.10118748

***Abstract*—In this work, we propose a joint security approach based on physical layer security (PhySec) and noisy ciphertext to improve the secrecy rate of a relay network with cooperative jamming via two trusted relays. While the secrecy capacity has been considered as the maximum limit for a perfect secrecy at the physical layer, we demonstrate that the consideration of error-prone ciphertext in encryption and its interaction with PhySec allows us to transmit above the PhySec capacity without any leakage. By formulating and solving a non-convex encryption-aided secrecy rate maximization problem, it is shown that beyond PhySec capacity performances can be achieved even in a simple jamming scenario in which the two jammers just send independent jamming signals. The optimal encryption-aware power allocation and the secrecy rate maximization solution are also established in the case of common jamming signals to further increase the secrecy rate. Numerical results are finally provided to demonstrate the superiority of the proposed joint security framework over traditional PhySec.**

***Index Terms*—Cooperative jamming; Encryption; Error-prone ciphertext; PHY security; Rate-equivocation region; Secrecy capacity.**

I. Introduction

While encryption-based security mechanisms have traditionally been designed and implemented at higher layers of protocol stacks [1]–[3], recently, security schemes at the physical layer (PHY) have been proposed and studied. Physical layer security (PhySec), also known as information-theoretic security, generally refers to exploiting the unique properties of the communication systems, such as noise, interference and fading, to provide secrecy and address security threats [4]–[8]. For instance, benefiting from information theoretic studies in cooperative relaying communications, relaying strategies have received considerable attention in the context of PhySec over wireless network. Relay nodes can be used as trusted nodes to support a secured transmission from a source to a destination in the presence of one or more eavesdroppers. Another method is to generate weighted jamming signals from the relays to confound the adversaries. This technique is usually referred to as cooperative jamming (CJ) [9]–[11].

Nevertheless, despite many advances in PhySec, there is still no clear path to connect the PhySec to conventional security approaches at higher layers. In fact, information-theoretic and cryptographic security (CryptoSec) approaches generally neglect one another in the design of a secure communication system. PhySec relies on better channel condition at the legitimate receiver compared to the eavesdropper, and CryptoSec depends on imposing high-complexity computation on the eavesdropper to break the cipher. In fact, classical encryption schemes ignore the properties of the channel and assume that the eavesdropper can detect all parts of the cipher message without any error. Instead, the design of encryption schemes is based on the assumption of limited computational power at the adversary. Interestingly, PhySec assumes the exact opposite; i.e., all the designs are based on the assumption of unlimited computational power at the eavesdropper, which means that the presence of the encryption is completely ignored. On the other hand, unlike in classical cryptography, it is assumed that the eavesdropper cannot, at all, retrieve the correct cipher message. In other words, in CryptoSec, the eavesdropper is assumed to be weak in computation but strong in interception (e.g., equipped with powerful receivers), while in PhySec, the assumption is exactly the opposite. Since in practice, either or none of these assumptions can be true, it is important to consider both approaches and bridge up the gap between PhySec and CryptoSec schemes to come up with more efficient and flexible security mechanisms. By establishing a level of coordination between the layers, cross-layer security design is a promising solution to achieve higher secrecy in communication networks and provide a more flexible trade-off between critical system resources.

While several efforts have been made to design variety of processes jointly in different layers [12]–[16], security schemes in physical and application layers are still designed and executed separately. Recently, there have been some limited efforts to come up with cross-layer security designs by establishing coordination between physical and higher layers [17], [18]. These techniques use the fact that PhySec introduces a theoretical secure transmission rate limit to be employed in higher layers to execute scheduling or packetizing in a more efficient way. In [17], a joint framework involving both physical and application layers for security designs is proposed for wireless multimedia delivery. In [18], a cross-layer packet scheduling is proposed with PhySec employing beamforming and artificial noise. One of the rare attempts to bridge up the gap between PhySec and CryptoSec is reported in [19], [20], where new security metrics based on the cryptographic definition of security are introduced, and the mutual connection between such metrics is studied. Despite considering a cryptographic treatment of wiretap channels, no assumption on the computational power is considered, and

978-1-6654-9122-8/23/$31.00 ©2023 IEEE

key-based encryption is completely ignored. PhySec has also been introduced as an alternative method for key exchange allowing the use of cryptographic algorithms [21], [22]. The idea is based on measuring the characteristics of a highly correlated wireless channel, and then using them as shared random sources to generate a shared key.

In this paper, a joint security approach based on PhySec and noisy ciphertext is introduced for a relay-based network for beyond-secrecy-capacity performances. While the focus is on a relay network with two trusted relays, the results can be extended to more general networks. From the PhySec point of view, we can achieve any transmission rate below PhySec capacity with perfect secrecy. On the other hand, if we transmit any rate above the PhySec capacity, there is a leakage. With encryption, such a result still holds true if the eavesdropper can decode the ciphertext without error. However, with error-prone ciphertext, it is more difficult for the eavesdropper to break the cipher, which leaves room for improvement in PhySec. Therefore, under the consideration of error-prone ciphertexts, we address the encryption-aided secrecy rate maximization problem and show that beyond PhySec capacity performances can be achieved even when the jammers just send independent jamming signals. The secrecy rate can also be enhanced by utilizing cooperative jamming in which the two relays use a common jamming signal. Our simulation results show the superiority of the proposed joint security framework over traditional PhySec.

II. Encryption-Aided Physical Layer Security with Cooperative Jamming: System Model and Secrecy Rate Maximization

In this section, we first present the relay-based wiretap channel of interest. We then introduce the proposed security approach and formulate the secrece rate maximization problem under error ciphertext constraints.

A. Channel Model and PhySec Capacity

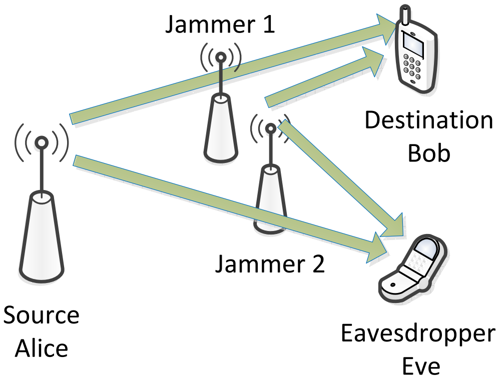

Fig. 1. A cooperative jamming wiretap channel with two trusted jammers.

In this work, we consider a cooperative jamming wiretap channel that includes a source Alice, a destination Bob, an eavesdropper Eve, and two trusted jammers J_1 and J_2. The source Alice transmits a Gaussian signal x_s to Bob under the power constraint ρ_s. Each of the jammers assists Alice to confuse Eve by transmitting Gaussian signals x_1 and x_2, respectively, to the channel. We assume that the two jammers can share power with a total available jamming power budget of P_t, i.e., $E[|x_1|^2 + |x_2|^2] = \rho_1 + \rho_2 \leq P_T$.

Let h_0 and g_0 be the complex channel gains of Alice-Bob and Alice-Eve channels, respectively. The channel gains of J_i-Bob and jammer J_i-Eve are h_i and g_i, respectively, with $i \in \{1, 2\}$. Thus, the received signals at destination Bob and eavesdropper Eve can be written, respectively, as

$$Y = h_0 x_s + h_1 x_1 + h_2 x_2 + n_B, \tag{1}$$

$$Z = g_0 x_s + g_1 x_1 + g_2 x_2 + n_E, \tag{2}$$

where n_B and n_E are additive white Gaussian noise (AWGN) at Bob and Eve with zero mean and normalized unit variance. For a given power scheme $\boldsymbol{\rho} = (\rho_1, \rho_2)$, the achievable secrecy rate R_s is calculated as

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

where $R_b(\boldsymbol{\rho})$ is Alice-Bob channel rate, $R_e(\boldsymbol{\rho})$ is Alice-Eve channel rate, and $[x]^+ = max\{0, x\}$. Furthermore, γ_B and γ_E are the signal to interference plus noise ratios at the Bob and Eve, respectively. In this work, we consider two different types of jamming signals as follows.

i) Independent jamming signals: In the case that the jammers send out independent Gaussian signals x_1 and x_2, we have:

$$\gamma_B = \gamma_B^I = \frac{\rho_s \alpha_0}{\rho_1 \alpha_1 + \rho_2 \alpha_2 + 1}, \tag{4}$$

$$\gamma_E = \gamma_E^I = \frac{\rho_s \beta_0}{\rho_1 \beta_1 + \rho_2 \beta_2 + 1}, \tag{5}$$

where $\alpha_i = |h_i|^2$ and $\beta_i = |g_i|^2$, $i \in \{1, 2\}$.

ii) Common jamming signals: If the jammers use a common Gaussian signal x, the signal to interference plus noise ratios at Bob and Eve, respectively, can be expressed as

$$\gamma_B = \gamma_B^C = \frac{\rho_s \alpha_0}{|w_1 h_1 + w_2 h_2|^2 + 1}, \tag{6}$$

$$\gamma_E = \gamma_E^C = \frac{\rho_s \beta_0}{|w_1 g_1 + w_2 g_2|^2 + 1}, \tag{7}$$

where w_1 and w_2 are refered to as complex jamming powers, and $\rho_1 = |w_1|^2$ and $\rho_2 = |w_2|^2$.

In both cases, the secrecy capacity C_S is the solution of the following optimization problem

$$\begin{aligned} C_S = &\underset{\boldsymbol{\rho}}{\text{maximize}} \quad R_s(\boldsymbol{\rho}), \\ &\text{subject to} \quad \rho_1 + \rho_2 \leq P_T. \end{aligned} \tag{8}$$

This optimization problem is non-convex, but it can be solved effectively using iterative two-layer approaches [9], [23], [24].

B. Encryption-Aided Rate Maximization with Error-Prone Ciphertexts

In PhySec, transmitting above C_S is not possible without leakage. However, under a practical assumption of errors that come from the physical layer, it makes it harder for Eve to break the cipher. The mutual impact between physical-layer errors encryption has been studied in [25]–[32], and it has been well documented that Eve needs to be computationally stronger or equipped with more sophisticated attacks in order to successfully break encryption. On the other hand, such interaction can also be interpreted via the connection between noisy ciphertext and secrecy rate. In particular, following the analysis in [25], let define P_{cipher} be the error probability limit that causes Eve to fail in breaking the cipher. We can then define an encryption factor λ that can be used to reflect the strength of encryption. More specifically, it is clear that a stronger encryption leads to a larger λ, or equivalently, a smaller P_{cipher}. Thus, we can define λ as follows

$$\lambda = \frac{1}{P_{cipher}}. \tag{9}$$

It is clear that when λ is 1, we can assume that there is no encryption. When a more powerful encryption scheme is used, we have a larger λ. This newly defined parameter can be applied to PhySec to lead to a larger security region. Specifically, in the asymtotic block length regime, the message error rate at Eve, denoted as P_{Eve} satisfies $P_{Eve} \geq \frac{R_e}{R}$. In addition, setting the ratio $\frac{R_e}{R}$ as an upper bound for P_{cipher} will ensure that $P_{Eve} \geq P_{cipher}$. This means that, in this case, the system is secure. Therefore, from (9), we have

$$\frac{R_e}{R} \geq \frac{1}{\lambda}. \tag{10}$$

The secrecy rate maximization problem can now be defined by considering the new constraint $R \leq \lambda R_e$, which is

$$\bar{R}_S \triangleq \sup_{R} \left\{ R : \left(R, \frac{R}{\lambda} \right) \in \bar{\mathcal{R}}^{WTC} \right\}, \tag{11}$$

where $\bar{\mathcal{R}}^{WTC}$ is the so-called rate-equivocation region. For a typical rate-equivocation region that contains all possible rate pairs (R, R_e), with R_e be the equivocation rate, there exist five important boundary points, which are $(R, R_e) = \{(0,0), (C_S, C_S), (C'_B, C_S), (C_B, C'_S), (C_B, 0)\}$. Here, C_B is the main Alice-Bob channel capacity with no jamming. In addition, C'_B is the maximum possible rate of Alice-Bob channel at which we still have $R_e = C_S$. Equivalently, we have $C'_B = R_b(\boldsymbol{\rho}^{(S)})$ or equivalently, $C'_B = R_b(\boldsymbol{\rho}^{(S)})$, where $\boldsymbol{\rho}^{(S)}$ is the power allocation scheme. Finally, C'_S is the maximum possible equivocation rate when $R = C_B$. To simplify the problem further, we can define two thresholds on encryption strength as $\lambda_{T1} = C'_B / C_S$ and $\lambda_{T2} = C_B / C'_S$. While not showing in detail here for brevity of the presentation, it can be proved that when $1 \leq \lambda \leq \lambda_{T1}$, the encryption-aware secrecy capacity can readily be found as $\bar{C}_S = \lambda C_S$. When $\lambda > \lambda_{T2}$, we can securely transmit at the main channel capacity, i.e., $\bar{C}_S = C_B$. Finally, when $\lambda_{T1} < \lambda < \lambda_{T2}$, $\bar{C}_S$ is the solution of the following problem

$$\begin{aligned} \bar{C}_S = \underset{\boldsymbol{\rho}}{\text{maximize}} \quad & R_b(\boldsymbol{\rho}), \\ \text{subject to} \quad & \rho_1 + \rho_2 \leq P_T, \\ & R_b(\boldsymbol{\rho}) = \lambda R_s(\boldsymbol{\rho}). \end{aligned} \tag{12}$$

III. Encryption-Aided Rate Maximization: Optimal Power Allocation and Secrecy Capacity

In the following, we shall address the optimization problem in (12) for the two cases of using independent jamming signals and common jamming signals, respectively. It should be noted that we only need to focus on the region $\lambda_{T1} < \lambda < \lambda_{T2}$. The solutions for other regions are rather trivial as we discussed earlier.

A. Independent Jamming Signals

Consider the first case that the two jamming signals x_1 and x_2 are independent. For convenience, let $K_1 = \rho_s |h_0|^2$ and $K_1 = \rho_s |g_0|^2$. After some manipulations, the problem in (12) can be equivalently written as

$$\begin{aligned} \underset{\boldsymbol{\rho}}{\text{minimize}} \quad & \rho_1 \alpha_1 + \rho_2 \alpha_2, \\ \text{subject to} \quad & \rho_1 + \rho_2 \leq P_T, \\ & \rho_1 \alpha_1 + \rho_2 \alpha_2 = \frac{K_1}{\left(1 + \frac{K_2}{1 + \rho_1 \beta_1 + \rho_2 \beta_2}\right)^{\xi} - 1} - 1. \end{aligned} \tag{13}$$

Observe that (13) is a $2-$dimensional optimization problem with a linear objective function, one linear inequality constraint, and another non-linear equality constraint. This problem can be approximated as a linear programming (LP) problem by simply approximating the non-linear equality constraint with a linear function as follows. First, let $t_1 = \rho_1 \alpha_1 + \rho_2 \alpha_2$ and $t_2 = \rho_1 \beta_1 + \rho_2 \beta_2$. We can write the equality constraint as

$$t_1 = \frac{K_1}{\left(1 + \frac{K_2}{1 + t_2}\right)^{\xi} - 1} - 1. \tag{14}$$

The curve in (14) is approximated with the line $t_1 = m t_2 + c$, where $m > 0$ is the slope and $c < 0$ is the t_1 intercept value. Given this approximation, (13) can be written as

$$\begin{aligned} \underset{\boldsymbol{\rho}}{\text{minimize}} \quad & t_1, \\ \text{subject to} \quad & \rho_1 + \rho_2 \leq P_T, \\ & t_1 = m t_2 + c. \end{aligned} \tag{15}$$

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

$$\begin{aligned} \underset{\nu_1, \nu_2}{\text{maximize}} \quad & -P_T \nu_1 - c \nu_2, \\ \text{subject to} \quad & \nu_1 + (\alpha_i - m \beta_i) \nu_2 \geq -\alpha_i, \qquad i = 1, 2, \\ & \nu_1 \geq 0, \end{aligned} \tag{16}$$

where $\nu_1$and ν_2 are the dual variables. The three lines, $\nu_1 = 0$ and $\nu_1 + (\alpha_i - m\beta_i)\nu_2 = -\alpha_i$ for $i = 1, 2$, define a super-set of the lines that determine the boundary of this region. For this linear programming, strong duality is achieved, which results in

$$\text{minimum} \quad t_1 = \text{maximum} \quad -P_T\nu_1 - c\nu_2 \geq 0. \tag{17}$$

Furthermore, complementary slackness conditions are satisfied. Therefore, we have:

$$\nu_1^* \left(\rho_1^* + \rho_2^* - P_T\right) = 0, \tag{18}$$
$$\rho_i^* \left(\nu_1^* + (\alpha_i - m\beta_i)\nu_2^* + \alpha_i\right) = 0, \qquad i = 1, 2. \tag{19}$$

Note that $\nu_1 \geq 0$ in (16). Now, let first consider the case that $\nu_1^* \neq 0$. The first condition in (20) implies that the power constraint in the primal problem should be achieved with equality. On the other hand, if $\nu_1^* = 0$, to satisfy the conditions in (21), we can verify that we have $\rho_1^* = 0$, $\rho_2^* = 0$ or $\rho_1^* = \rho_2^* = 0$. So, to solve (13), we consider the following

$$\begin{aligned} \underset{\boldsymbol{\rho}}{\text{minimize}} \quad & \rho_1\alpha_1 + \rho_2\alpha_2, \\ \text{subject to} \quad & \rho_1 + \rho_2 = P_T, \\ & \rho_1\alpha_1 + \rho_2\alpha_2 = \frac{K_1}{\left(1 + \frac{K_2}{1+\rho_1\beta_1+\rho_2\beta_2}\right)^{\xi} - 1} - 1. \end{aligned} \tag{20}$$

Note that the above problem is the system of equations with the two equality constraints, and its solution results in the optimal powers (ρ_1^*, ρ_2^*). It should be noted that if no solution is found for this system of equation, we need to proceed by checking

$$\begin{aligned} \underset{\rho}{\text{minimize}} \quad & \rho_i\alpha_i, \\ \text{subject to} \quad & \rho_i \leq P_T, \\ & \rho_i\alpha_i = \frac{K_1}{\left(1 + \frac{K_2}{1+\rho_i\beta_i}\right)^{\xi} - 1} - 1, \end{aligned} \tag{21}$$

for $i = 1, 2$. It is obvious that the optimal power allowcation $\boldsymbol{\rho}^*$ can be found directly by solving the non-linear equation depicted by the equality constraint. Furthermore, if no solution to be found for this equality constraint, we conclude that $\rho_1^* = \rho_2^* = 0$, i.e., it is optimal to silence both jammers to achieve the optimal secrecy.

B. Common Jamming Signals

In this subsection, we address the case that the two jammers transmit common signals $x_1 = x_2 = x$. Under this jamming scenario, it is not hard to verify that the power constraint at the two jammers can be achieved with equality. In a similar manner as in the independent jamming signals, the main optimization problem in (12) can be re-formulated over two complex variables w_1 and w_2 as follows:

$$\begin{aligned} \underset{w_1,w_2}{\text{minimize}} \quad & |w_1g_1 + w_2g_2|^2, \\ \text{subject to} \quad & |w_1|^2 + |w_2|^2 = P_T, \\ & |w_1h_1 + w_2h_2|^2 = \frac{K_1}{\left(1 + \frac{K_2}{1+|w_1g_1+w_2g_2|^2}\right)^{\xi} - 1} - 1. \end{aligned} \tag{22}$$

In (22), $|w_1h_1 + w_2h_2|^2$ and $|w_1g_1 + w_2g_2|^2$ are the interferences caused by the jammers at Bob and Eve, respectively. Because of the logarithmic equality constraint in (22), it is extremely difficult, if not possible, to obtain the optimal values of w_1 and w_2. Our method is to approximate this constraint by a line with a tolerable error. As a result, we can formulate the following optimization problem to obtain an approximated solution as

$$\begin{aligned} \underset{w_1,w_2}{\text{minimize}} \quad & |w_1g_1 + w_2g_2|^2, \\ \text{subject to} \quad & |w_1|^2 + |w_2|^2 = P_T, \\ & |w_1h_1 + w_2h_2|^2 = m\,|w_1g_1 + w_2g_2|^2 + c. \end{aligned} \tag{23}$$

By letting $w_1 = |w_1|\angle\eta_1$ and $w_2 = |w_2|\angle\eta_2$, for $h_1 = |h_1|\angle\theta_1$, $h_2 = |h_2|\angle\theta_2$, $g_1 = |g_1|\angle\phi_1$ and $g_2 = |g_2|\angle\phi_2$, (23) can further be written as

$$\begin{aligned} \underset{w_1,w_2}{\text{minimize}} \; & 2|w_1||g_1||w_2||g_2|\cos(\eta_2 - \eta_1 + \phi_1 - \phi_2) \\ & + (|w_1||g_1|)^2 + (|w_2||g_2|)^2, \\ \text{subject to} \quad & |w_1|^2 + |w_2|^2 = P_T, \\ & 2|w_1||h_1||w_2||h_2|\cos(\eta_2 - \eta_1 + \theta_1 - \theta_2) \\ & + (|w_1||h_1|)^2 + (|w_2||h_2|)^2 = \\ & 2m|w_1||g_1||w_2||g_2|\cos(\eta_2 - \eta_1 + \phi_1 - \phi_2) \\ & + m(|w_1||g_1|)^2 + m(|w_2||g_2|)^2 + c. \end{aligned} \tag{24}$$

Without loss of generality, we can assume $\eta_1^* = 0$. Then, the optimal η_2^* that minimizes the objective function in (24) can be given by

$$\eta_2^* = \pi + \phi_2 - \phi_1.$$

Finally, the optimal magnitudes of the complex jamming powers $|w_1|^*$ and $|w_2|^*$ can be readily obtained from the two equality constraints.

IV. Numerical Examples

In this section, we provide several numerical examples to show the significance of the proposed joint security approach.

First, let consider the scenario in which a positive PhySec rate can be achieved without the need of cooperative jamming. This corresponds to the case that the Alice-Bob channel is stronger than the Alice-Eve channel, which is equivalent to $K_1 > K_2$. For this scenario, the channel gains are chosen as follows: $h_0 = 1$, $h_1 = 0.25 + j0.25$, $h_2 = 0.55 + j0.3$, $g_0 = 1.3$, $g_1 = 0.24 + 0.05j$ and $g_2 = 0.54 + j0.2$.

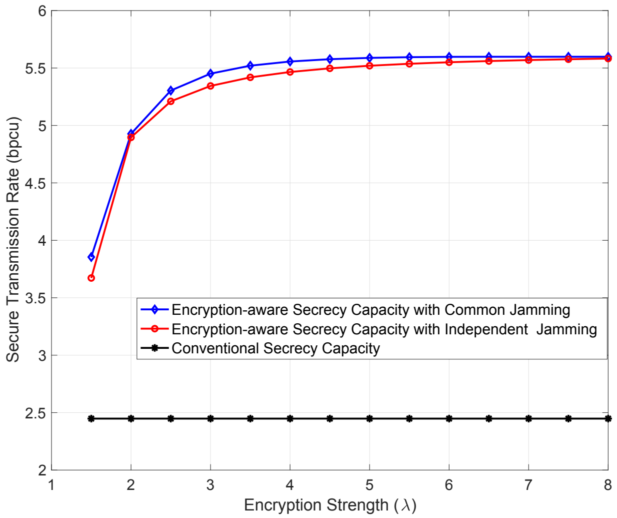

Fig. 2. Encryption-aided secrecy rates achieved by different encryption strengths when $K_1 > K_2$.

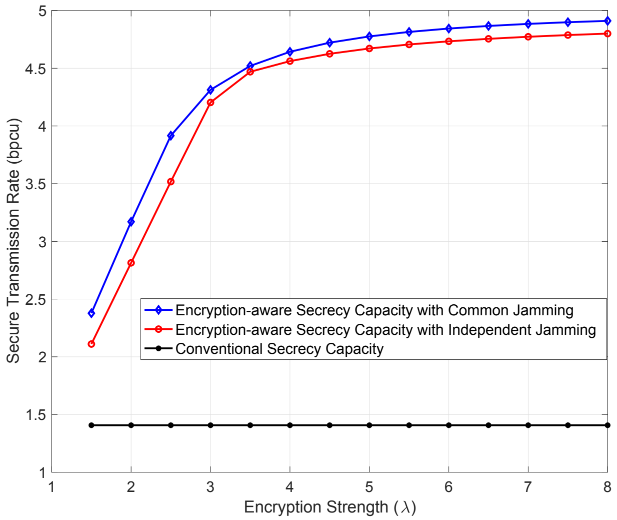

Fig. 3. Encryption-aided secrecy rates achieved by different encryption strengths when $K_1 < K_2$

Assume that we have a source power budget of 15dB and jamming power budget 10dB, Fig.2 shows the encryption-aided secrecy rates achieved by independent jamming as well as common jamming signals for different λ values. It should be again noted that when $\lambda = 1$, we achieve the traditional PhySec capacity, which is also plotted in Fig.2 as a benchmark. It can be observed from Fig.2 that we can achieve significant rate gains over traditional PhySec capacity in both cases of using independent jamming and common jamming signals. It can also be seen that the use of common jamming signals leads to a slight better rate as compared to the case of using independent jamming signals. Finally, it is also worth seeing the effect of λ to the secrecy rate from Fig.2. At sufficiently high values of λ, the encryption-aided PhySec capacity approaches a constant value. The main reason for that is because we approach to the main channel capacity C_B.

The results also hold in a more interesting scenario in which cooperative jamming is needed to achieve a positive PhySec rate, i.e., the Alice-Bob channel is stronger than the Alice-Eve channel that results in $K_1 < K_2$. In particular, we consider the same set of channel gains $h_1 = 0.25+j0.25$, $h_2 = 0.55+j0.3$, $g_1 = 0.24 + 0.05j$ and $g_2 = 0.54 + j0.2$, but different Alice-Bob and Eve-Bob channels with $h_0 = 1.3$ and $g_0 = 1$. Fig. 3 shows a similar behaviour as in Fig. 2, where we can still achieve a significant improvement over the traditional PhySec capacity. It is also clear that jamming using a common signal provides higher rates than jamming using independent signals.

V. Conclusion

This paper presented a new joint security approach to exploit the benefits of physical layer security (PhySec) and noisy ciphertext in encryption for a relay network with cooperative jamming with two trusted relays. The consideration of error prone ciphertext enables us to transmit above the PHYsec capacity without leakage. We formulated and solved non-convex encryption-aided secrecy rate maximization problems for two cases of using independent and common jamming signals from the two relays. Numerical results were provided to confirm that beyond PHYsec capacity performances can be achieved under the consideration of error-prone ciphertext in encryption and its interaction with the physical layer.

As for future works, it is of particular interest to extend the current framework to a general relay network having K relays that include both trusted and untrusted (but friendly) relay nodes. All the relays can assist in providing secure communication against the eavesdropper. However, untrusted relays should not be able to completely extract the cipher message; however, with the aid of encryption, partial decoding might be possible. We can assume that all relays collaborate with each other by sharing channel information to achieve the best transmission scheme. The relays can also employ different encryption schemes; i.e., different encryption strength λ. This interesting research is currently under investigation.

References

[1] I. Marić, S. Shamai, and O. Simeone, *Information Theoretic Perspectives on 5G Systems and Beyond*. Cambridge University Press, 2022.

[2] J.-S. Coron, "What is cryptography?" *IEEE Security & Privacy*, vol. 4, no. 1, pp. 70–73, Jan.-Feb 2006.

[3] E. D. Silva, A. L. D. Santos, L. C. P. Albini, and M. Lima, "Identity-based key management in mobile ad hoc networks: Techniques and applications," *IEEE Trans. Wireless Commun.*, vol. 15, no. 10, pp. 46–52, Oct. 2008.

[4] M. Bloch, J. Barros, M. Rodrigues, and S. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inform. Theory*, vol. 54, no. 6, pp. 2515–2534, June 2008.

[5] J. D. V. Sanchez, D. P. M. Osorio, F. J. Lopez-Martinez, M. C. P. Paredes, and L. F. Urquiza-Aguiar, "Information-theoretic security of MIMO networks under κ-μ shadowed fading channels," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 7, pp. 6302–6318, 2021.

[6] H. Zhou and A. El Gamal, “Network information theoretic security with omnipresent eavesdropping,” *IEEE Transactions on Information Theory*, vol. 67, no. 12, pp. 8280–8299, 2021.

[7] G. Li, H. Luo, J. Yu, A. Hu, and J. Wang, “Information-theoretic secure key sharing for wide-area mobile applications,” *IEEE Wireless Communications*, 2023.

[8] H. Zhou and A. El Gamal, “Network information theoretic security,” in *2020 IEEE International Symposium on Information Theory (ISIT)*. IEEE, 2020, pp. 978–983.

[9] G. Zheng, L.-C. Choo, and K.-K. Wong, “Optimal cooperative jamming to enhance physical layer security using relays,” *IEEE Trans. Signal Process.*, vol. 59, no. 3, pp. 1317–1322, Mar. 2011.

[10] Y. Wu and Y. Huo, “A survey of cooperative jamming-based secure transmission for energy-limited systems,” *Wireless Communications and Mobile Computing*, vol. 2021, 2021.

[11] S. Xu, S. Han, W. Meng, Z. Li, C. Li, and C. Zhang, “Improving secrecy for correlated main and wiretap channels using cooperative jamming,” *IEEE Access*, vol. 7, pp. 23 788–23 797, 2019.

[12] S. Toumpis and A. J. Goldsmith, “Capacity regions for wireless ad hoc networks,” *IEEE Trans. Wireless Commun.*, vol. 2, no. 4, pp. 746–748, 2003.

[13] S. Pollin, B. Bougard, and G. Lenoir, “Cross-layer exploration of link adaptation in wireless LANs with TCP traffic,” in *Proc. IEEE Benelux Chapter on Commun. and Veh. Technol.*, 2003.

[14] L. Chen, S. H. Low, and J. C. Doyle, “Joint congestion control and media access control design for ad hoc wireless networks,” in *Proc. INFOCOM*, 2005.

[15] X. Lin and N. B. Shroff, “The impact of imperfect scheduling on cross layer rate control in wireless networks,” in *Proc. INFOCOM*, 2005.

[16] D. Kliazovich and F. Granelli, *Cross layer designs in WLAN systems*. Troubador Publishing Ltd, Nov. 2011, ch. Introduction: Why cross-layer? Its advantages and disadvantages.

[17] L. Zhou, D. Wu, B. Zheng, and M. Guizani, “Joint physical-application layer security for wireless multimedia delivery,” *IEEE Commun. Mag.*, vol. 52, no. 3, pp. 66–72, March 2014.

[18] J. Wang, P. Huang, X. Wang, and Y. Yang, “Cross-layer scheduling for physical layer secrecy and queue stability in a multi-user system,” in *Globecom 2013 - Wireless Networking Symposium*, 2013.

[19] M. Bellare, S. Tessaro, and A. Vardy, *Advances in Cryptology*. Santa Barbara, CA, USA: Springer, 2012, ch. Semantic security for the wiretap channel, pp. 294–311.

[20] M. Bellare, S. Tessaro, and A. Vard, “A cryptographic treatment of the wiretap channel.” [Online]. Available: http://arxiv.org/abs/1201.2205v1

[21] K. Zeng, “Physical layer key generation in wireless networks: challenges and opportunities,” *IEEE Commun. Mag.*, vol. 53, no. 9, pp. 33–39, June 2015.

[22] J. Zhang, R. Woods, T. Q. Duong, Y. Ding, Y. Huang, and Q. Xu, “Experimental study on key generation for physical layer security in wireless communications,” *IEEE Access*, vol. 4, pp. 4464–4477, Aug. 2016.

[23] L. Zhang, R. Zhang, Y.-C. Liang, Y. Xin, and S. Cui, “On the relationship between the multi-antenna secrecy communications and cognitive radio communications,” in *2009 47th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, 2009, pp. 1286–1292.

[24] J. Li, A. Petropulu, and S. Weber, “Optimal cooperative relaying schemes for improving wireless physical layer security,” *IEEE Transactions on Signal Processing*, 01 2010.

[25] W. K. Harrison and S. W. McLaughlin, “Physical-layer security: Combining error control coding and cryptography,” in *2009 IEEE Int. Conf. Commun. (ICC)*, June 2009.

[26] ——, “Tandem coding and cryptography on wiretap channels: EXIT chart analysis,” in *2009 IEEE Int. Symp. on Inform. Theory*. IEEE, June 2009.

[27] ——, “EXIT charts applied to tandem coding and cryptography in a wiretap scenario,” in *2009 IEEE Inform. Theory Workshop*. IEEE, 2009.

[28] W. K. Harrison, J. Almeida, D. Klinc, S. W. McLaughlin, and J. Barros, “Stopping sets for physical-layer security,” in *2010 IEEE Inform. Theory Workshop*. IEEE, Aug. 2010.

[29] W. K. Harrison, J. Almeida, S. W. McLaughlin, and J. Barros, “Coding for cryptographic security enhancement using stopping sets,” *IEEE Trans. Inform. Forensics and Sec.*, vol. 6, no. 3, pp. 575–584, Sept. 2011.

[30] ——, “Physical-layer security over correlated erasure channels,” in *2012 IEEE Int. Conf. Commun. (ICC)*, June 2012.

[31] W. K. Harrison and S. W. McLaughlin, “Equivocations for the simple substitution cipher with erasure-prone ciphertext,” in *2012 IEEE Inform. Theory Workshop*. IEEE, Sept. 2012.

[32] 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 Int. Conf. Commun. (ICC)*, June 2014.