Covert Communications Versus Physical Layer Security
Moslem Forouzesh, Paeiz Azmi, Senior Member, IEEE, Nader Mokari, Member, IEEE, and Kai Kit Wong, Fellow, IEEE

Abstract—This letter studies and compares the physical-layer security approach and the covert communication approach for a wiretap channel with a transmitter, an intended receiver and an eavesdropper. In order to make the comparison, we investigate the power allocation problems for maximizing the secrecy/covert rate subject to the transmit power constraint. Simulation results illustrate that if the eavesdropper is not noisy or it is near to the transmitter, covert communication is more preferable.

Index terms—Covert communication, physical-layer security, optimal power allocation.

I. INTRODUCTION

Security is a major challenge in communications networks, particularly over wireless due to its broadcasting nature. Cryptographic security is the current state-of-the-art but in recent years there appears to be strong interest for providing security in the physical layer to have an additional layer of defence.

Physical-layer security (PLS) has been widely studied since Wyner introduced the wiretap channel in [1]. In his pioneering work, Wyner demonstrated that if an eavesdropper’s channel is a degraded version of the legitimate user’s channel, then the communication channel can achieve a positive information rate at which the message is kept completely confidential from the eavesdropper, which is known as the secrecy rate.

More recently, there emerges another approach, referred to as covert communication, which aims to hide the existence of a communication channel from an observing eavesdropper. In [2], the authors studied the capability of a source to transmit covertly and reliably to a destination with the help of a friendly jammer in the presence of an adversary. Most recently, covert communication with channel uncertainty was also investigated in [3]. Obviously, both PLS and covert communication provide security for communications but literature lacks comparison of the two approaches.

Motivated by this, this letter has made the following major contributions:

• For the basic wiretap channel, we study and compare the secrecy rate and covert rate for the two approaches.
• We show that covert rate does not depend on the distance between the source and eavesdropper.

Moslem Forouzesh is with the Department of Electrical and Computer Engineering, Tarbiat Modares University, Tehran, Iran (e-mail: m.Forouzesh@modares.ac.ir).

Paeiz Azmi is with the Department of ECE, Tarbiat Modares University, Tehran, Iran (e-mail: pazmi@modares.ac.ir).

Nader Mokari is with the Department of ECE, Tarbiat Modares University, Tehran, Iran (e-mail: nader.mny@gmail.com).

Kat-Kit Wong is with the Department of Electronic and Electrical Engineering, University College London, WC1E 7JE, United Kingdom (e-mail: kai-kit.wong@ucl.ac.uk).

In addition, we also obtain the optimal power threshold in closed-form from the perspective of the eavesdropper, for the case of covert communication.

To have meaningful comparison between PLS and covert communication, the optimal power allocation problems for maximizing the secrecy rate and covert rate need to be addressed. To solve these, we exploit a property in the transmit power constraint and illustrate that the problems can be transformed into geometric programming (GP), so that they can be solved by convex approaches.

II. SYSTEM MODEL

The system model under consideration consists of a single transmitter (Alice), an intended receiver (Bob), and an eavesdropper (Eve). Alice aims to send a private message to Bob by transmitting a jamming signal to mask the message to Bob. We consider two approaches for providing the required secret communication: 1) PLS, and 2) covert communication. The distance from Alice to Bob, and that from Alice to Eve are donated by $d_{ab}$, and $d_{ae}$, respectively. Moreover, we denote the channel coefficients between Alice and Bob, and between Alice and Eve as $h_{ab}$ and $h_{ae}$, respectively.

The channel coefficients are assumed to be circularly symmetric complex Gaussian with zero mean and unit variance. We consider a discrete-time channel with $Q$ time slots, each with length of $n$ symbols. The transmit signal to Bob and the jamming signal in each time slot can be written, respectively, as $x_b = [x_b^1, x_b^2, \ldots, x_b^n]$ and $x_j = [x_j^1, x_j^2, \ldots, x_j^n]$.

III. PLS

The received signal at receiver $m$ (Bob or Eve) is $y_m = \sum_{k=1}^{Q} h_{am} x_k + \sum_{j=1}^{Q} h_{aj} x_j + \eta_m$, where $p_j$ and $p_{ab}$ are the power allocated for jamming and transmitting Alice’s message to Bob, respectively, $\alpha$ denotes the path-loss exponent, and $\eta_m \sim CN \left(0, \sigma_m^2 I_n \right)$ represents the received noise vector at user $m$. As a consequence, the signal-to-interference-plus-noise ratio (SINR) at Eve and Bob can be expressed as $\text{SINR}_e = \frac{p_{ab} |h_{ae}|^2}{p_{ab}|h_{ae}|^2 + p_j |h_{aj}|^2}$, $\text{SINR}_b = \frac{p_{ab} |h_{ab}|^2}{p_{ab}|h_{ab}|^2 + p_j |h_{aj}|^2}$, respectively. Therefore, the secrecy rate at Bob can be written as $R_{sec} = \frac{1}{2} \log \left(1 + \text{SINR}_b \right) - \frac{1}{2} \log \left(1 + \text{SINR}_e \right)$, where $[x]^+ = \max \{x,0\}$ and $p \triangleq [p_{ab}, p_j]$.

A. Optimization Problem

Considering PLS, the system aims to maximize the secrecy rate at Bob subject to a transmit power constraint. That is,

$$\max_{p_{ab}, p_j} R_{sec} (p) \quad \text{s.t.} \quad p_{ab} + p_j \leq p_{max}. \quad (1)$$
IV. COVERT COMMUNICATION

For the case of covert communication, based on the received signal power, Eve decides on whether Alice sends a message. In this case, the received signal at receiver \( m \) (Bob or Eve) is

\[
y_m = \begin{cases} 
\frac{\sqrt{P_f}h_{am,x_1}}{d_{am}^{\frac{\alpha}{2}}} + \eta_m, & \text{if } \Psi_0, \\
\frac{\sqrt{P_f}h_{am,x_2}}{d_{am}^{\frac{\alpha}{2}}} + \frac{\sqrt{P_m}h_{am,x_2}}{d_{am}^{\frac{\alpha}{2}}} + \eta_m, & \text{if } \Psi_1,
\end{cases}
\]

(2)

where \( \Psi_0 \) specifies the case where Alice does not transmit any message to Bob, while \( \Psi_1 \) states that Alice indeed transmits a message to Bob. Each symbol of the received signal at Eve, \( y_e \), follows \( CN(0, \sigma_e^2 + \gamma) \), in which the probability density function (PDF) of \( \gamma \) for \( \gamma > 0 \) is given by \[2\]

\[
fr_{\psi}(\gamma) = \begin{cases} 
\frac{1}{\sqrt{2\pi}\psi_0} \exp\left(-\frac{\gamma^2}{2\psi_0^2}\right), & \text{if } \Psi_0, \\
\frac{1}{\sqrt{2\pi}\psi_1} \exp\left(-\frac{\gamma^2}{2\psi_1^2}\right), & \text{if } \Psi_1,
\end{cases}
\]

(3)

where \( \psi_0 = \frac{p_f}{d_{ae}^{\alpha}} \) and \( \psi_1 = \frac{p_f + p_m}{d_{ae}^{\alpha}} \). The SINR at Bob is

\[
\text{SINR}_b = \begin{cases} 
0, & \text{if } \Psi_0, \\
\frac{p_{ab}h_{ab}|^2}{d_{ae}^{\alpha}\sigma_e^2 + p_j|h_{ab}|^2}, & \text{if } \Psi_1.
\end{cases}
\]

(4)

When Eve mistakenly decides \( \Psi_1 \) while \( \Psi_0 \) is true, false alarm (FA) with probability \( P_{FA} \) occurs, while Eve decides \( \Psi_0 \) while \( \Psi_1 \) is true, miss detection (MD) with probability \( P_{MD} \) appears. Alice is said to have covert communication to Bob when the following constraint is satisfied \[2\]:

For any \( \varepsilon \geq 0 \), \( P_{MD} + P_{FA} \geq 1 - \varepsilon \), as \( n \to \infty \). (5)

As illustrated in \[2\], for minimal detection error at Eve, the optimal decision rule is written as \( Y_e \Psi_1 \geq \vartheta \), where \( Y_e = \sum_{l=1}^{n} |y_{l}^e|^2 \) is defined as the total power received by Eve in a time slot, \( y_{l}^e \) denotes the \( l \)th symbol of \( y_e \), and \( \vartheta \) is the threshold for decision at Eve, and \( n \) is the number of symbols used in a time slot. The FA and MD probabilities are given by \[3\]

\[
P_{FA} = P\left( \frac{Y_e}{n} > \vartheta | \Psi_0 \right) = P\left( \sigma_e^2 + \gamma \chi_n^2/n > \vartheta | \Psi_0 \right),
\]

(6)

\[
P_{MD} = P\left( \frac{Y_e}{n} < \vartheta | \Psi_1 \right) = P\left( \sigma_e^2 + \gamma \chi_n^2/n < \vartheta | \Psi_1 \right),
\]

(7)

where \( \chi_n^2 \) is a random variable with chi-squared distribution with \( 2n \) degrees of freedom. Therefore, we have

\[
P_{FA} = \begin{cases} 
e^{-\frac{\vartheta - \sigma_e^2}{\psi_0}}, & \text{for } \vartheta - \sigma_e^2 \geq 0, \\
1, & \text{for } \vartheta - \sigma_e^2 < 0,
\end{cases}
\]

(8)

\[
P_{MD} = \begin{cases} 
1 - e^{-\frac{\vartheta - \sigma_e^2}{\psi_1}}, & \text{for } \vartheta - \sigma_e^2 \geq 0, \\
0, & \text{for } \vartheta - \sigma_e^2 < 0.
\end{cases}
\]

(9)

The proof of \[8\] and \[9\] can be found in Appendix A.

A. Optimal Threshold for Eve

The security performance depends on the decoding performance of Eve and from Eve’s viewpoint, the power threshold needs to be optimized by \( \min_{\vartheta} P_{FA} + P_{MD} \). It can be shown in Appendix B that the optimal \( \vartheta \) is given by

\[
\vartheta_{opt} = \begin{cases} 
\vartheta^*, & \text{if } \vartheta - \sigma_e^2 \geq 0, \\
\text{there is no optimal } \vartheta, \text{ if } \vartheta - \sigma_e^2 < 0,
\end{cases}
\]

(10)

where \( \vartheta^* = \ln \left( \frac{\psi_0}{\psi_1} \right) + \sigma_e^2 \left( \frac{\psi_0}{\psi_0 - \psi_1} \right) \left( \frac{\psi_0 - \psi_1}{\psi_0} \right) \). By substituting (10) into (9) and (10), and since \( \vartheta^* \geq \sigma_e^2 \) is always true, we have \( P_{FA} + P_{MD} = 1 - e^{\frac{-\vartheta^*}{\psi_0}} \).

B. Optimization Problem

Our aim in this system model is to maximize the covert rate at Bob subject to the transmit power constraint and the covert communication condition at Bob, i.e., (5) is satisfied. Hence, we consider the following optimization problem:

\[
\max_{p_{ab},p_j} P_{\psi_1} \log \left( 1 + \frac{p_{ab}|h_{ab}|^2}{d_{ae}^{\alpha}\sigma_e^2 + p_j|h_{ab}|^2} \right),
\]

(11a)

s.t. \( p_{ab} + p_j \leq P_{\text{max}}, \) (11b)

\[
\min_{\vartheta} P_{FA} + P_{MD} \geq 1 - \varepsilon. \quad (11c)
\]

Constraint (11b) specifies the total power constraint for Alice while (11c) corresponds to the worst-case covert rate requirement for Bob. For solving (11), we first solve \( \min_{\vartheta} P_{FA} + P_{MD} \) to obtain the optimal \( \vartheta \), denoted by \( \vartheta^* \), for Eve. Then we solve (11) based on \( \vartheta^* \). Note that \( P_{\psi_1} \) refers to the probability of transmission data to Bob. This will be discussed next.

V. SOLUTIONS TO THE OPTIMIZATION PROBLEMS

Problems (1) and (11) are nonconvex because their objective functions are not concave. Also, (11c) is nonconvex. To solve them, we resort to successive convex approximation (SCA), and consider the scenario, in which the summation of jamming and data power is fixed, i.e., \( p_{ab} + p_j = P_{\text{max}} \), which is a common assumption in the security literature, e.g., \[5\]-\[7\].

A. The PLS Case

By using the epigraph method \[8\], we can rewrite (11) as

\[
\max_{p_{ab},p_j,\xi} \xi
\]

(12a)

s.t. \( \begin{align} 
\log \left( 1 + \text{SINR}_e^j \right) - \log \left( 1 + \text{SINR}_e^c \right) \leq \xi, \quad (12c) \\
\xi \geq 0. \quad (12d)
\end{align} \)

Next, we solve this problem using SCA and study the scenario when the total jamming and data power is constant.

1) Locally optimal solution: SCA: The objective function, \( \text{(12b)} \) and \( \text{(12d)} \) are affine but \( \text{(12c)} \) is nonconvex. As a result, the problem is unfortunately nonconvex. To tackle this, we employ the SCA approach to approximate \( \text{(12c)} \) by a convex constraint. This is done by rewriting \( \text{(12c)} \) as

\[
\Xi(P) = \log \left( p_{ab}|h_{ab}|^2 + d_{ae}^{\alpha}\sigma_e^2 + p_j|h_{ae}|^2 \right) - \\
\log \left( d_{ae}^{\alpha}\sigma_e^2 + p_j|h_{ae}|^2 \right) - \log \left( d_{ae}^{\alpha}\sigma_e^2 + p_j|h_{ae}|^2 \right) - \log \left( d_{ae}^{\alpha}\sigma_e^2 + p_j|h_{ae}|^2 \right) - \xi \leq 0, \quad (13)
\]
where the equation belongs to the difference of two concave functions. We now adopt the difference of convex functions (DC) method to approximate (13) to a convex constraint. To this end, we rewrite (13) as
\[
\Xi (P) = \Xi (P) - \Phi (P),
\]
where
\[
\begin{aligned}
\Xi (P) &= - \log \left( \frac{d_{ae}^2 \sigma_e^2 + p_j |h_{ae}|^2 + p_{ab} |h_{ae}|^2}{|h_{ab}|^2} \right) - \xi \\
\Phi (P) &= - \log \left( \frac{p_{ab} |h_{ab}|^2 + \alpha^2 \sigma_b^2 + p_j |h_{ab}|^2}{|h_{ab}|^2} \right) - \log \left( \frac{d_{ae}^2 \sigma_e^2 + p_j |h_{ae}|^2}{|h_{ae}|^2} \right).
\end{aligned}
\]
By using a linear approximation, we have
\[
\Phi (P) \simeq \Phi (P) = \Phi (P (s - 1)) + \nabla^T \Phi (P (s - 1)) (P - P (s - 1)),
\]
where \((.)^T\) denotes the transpose operator and \(\nabla\) is the gradient operator. Moreover, we have \(\nabla^T \Phi (P (s - 1)) = - \frac{d_{ae}^2 \sigma_e^2 + p_j |h_{ae}|^2}{|h_{ab}|^2} \), \(\frac{p_{ab} |h_{ab}|^2 + \alpha^2 \sigma_b^2 + p_j |h_{ab}|^2}{|h_{ab}|^2} \), and \(- \frac{d_{ae}^2 \sigma_e^2 + p_j |h_{ae}|^2}{|h_{ae}|^2} \). Therefore, after utilization of DC, (12) can be approximated to a convex optimization problem, which can be solved by available softwares as CVX solver [9].

2) Equality transmit power constraint: Globally optimal solution: From numerical results, it can be observed that at the optimum, the total transmit power consumption is almost the same as the power constraint. As such, we can replace the inequality constraint (11b) by the equality constraint, which is in fact a common trick in the literature [5]–[7]. Moreover, if we consider the case that Alice always spends all the available power for transmission, i.e., \(p_{ab} + p_j = P_{\text{max}}\), then this scenario has an optimal solution. Now, we define
\[
\gamma_b \triangleq \frac{p_{ab} |h_{ab}|^2}{d_{ab}^2 \sigma_b^2}, \quad \gamma_c \triangleq \frac{p_{max} |h_{ae}|^2}{d_{ae}^2 \sigma_e^2}, \quad p_j \triangleq (1 - \lambda) P_{\text{max}}.
\]
Then, the secrecy rate becomes
\[
R_{\text{sec}} (\lambda) = \left( \log \left( \frac{1 + \gamma_b}{1 + (1 - \lambda) \gamma_b} \right) - \log \left( \frac{1 + \gamma_c}{1 + (1 - \lambda) \gamma_c} \right) \right)^+.
\]
When \(\lambda = 0\), the secrecy rate is zero. As we aim to find the optimal \(\lambda\), we have \(\forall \lambda_{\text{optimum}} \in [0, 1]\), the argument within the function \([\cdot]^+\) in (17) should be positive. Therefore, the secrecy rate optimization problem can be recast into
\[
\max_{\lambda} \lambda \left( \frac{1 + \gamma_b}{1 + (1 - \lambda) \gamma_b} \right) \left( \frac{1 + \gamma_c}{1 + (1 - \lambda) \gamma_c} \right).
\]
Optimization problem (18) is a generalized posynomial, because it is equivalent to the GP form as follows:
\[
\begin{aligned}
\max_{t \geq 0} t \\
\text{s.t.} \quad t (1 + \gamma_c) (1 + \gamma_b) + \lambda \gamma_c (1 + \gamma_b) \leq t_1, \\
(1 + \gamma_c) (1 + \gamma_b) + t \lambda \gamma_b (1 + \gamma_c) \leq t_1.
\end{aligned}
\]
For solving the GP problem (19), which is convex, we can exploit available softwares such as CVX solver [9].

B. The Covert Communication Case

As the optimization problem (11) is nonconvex, we will adopt similar approaches as in the PLS case described above.

1) Locally optimal solution: SCA: Similar to Section V-A1, we can approximate the objective function as \(\Phi (P) - \Omega (P)\). Hence, constraint (11b) can be rewritten as
\[
\begin{aligned}
\max_{p_{ab}, p_j} & \quad \Phi (P) - \Omega (P) \leq 0, \\
\text{s.t} & \quad (11b), \quad (11c) \leq 0,
\end{aligned}
\]
Again, the objective function is increasing, we can maximize (21a)
\[
\begin{aligned}
\max_{p_{ab}, p_j} & \quad \lambda \gamma_b \leq \lambda \gamma_c \leq \lambda \gamma_b + (1 - \lambda) \gamma_b \leq \lambda \gamma_c + (1 - \lambda) \gamma_b \leq \lambda \gamma_b + (1 - \lambda) \gamma_b,
\end{aligned}
\]
which is convex and can be solved by solvers as CVX [9].

2) Equality total transmit power constraint: Globally optimal solution: In this part, similar to Section V-A2, we consider the case that \(p_{ab} + p_j = P_{\text{max}}\). Hence, (11) is rewritten as
\[
\begin{aligned}
\max_{\lambda} & \quad \lambda \gamma_b \leq \lambda \gamma_c \leq \lambda \gamma_b + (1 - \lambda) \gamma_b \leq \lambda \gamma_c + (1 - \lambda) \gamma_b \leq \lambda \gamma_b + (1 - \lambda) \gamma_b,
\end{aligned}
\]
which is convex and can be solved by solvers as CVX [9].

VI. SIMULATION RESULTS

In this section, we present the computer simulation results to evaluate and compare PLS and covert communication. In the simulations, we set the parameters as \(p_{\text{max}} = 5\) W, \(d_{ab} = 5\) m, \(\sigma_b^2 = -10\) dB, \(\alpha = 4\), \(\varepsilon = 0.1\), \(F_{\tilde{e}_1} = 0.7\).

Fig. 1(a) compares the proposed solutions with optimal values which are obtained from the exhaustive search method. As seen, in the proposed system model, Alice uses all the available power mostly, and hence the consideration of a fixed total power scenario, leading to the optimization problems. (11) and (11b) solved by SCA, appears to be reasonable.

Fig. 1(b) shows the covert and secrecy rate versus the distance from Alice to Eve. The main results in this figure are: 1) When Eve is near to Alice, covert communication has higher rate than PLS, but when Eve gets further away from Alice, the secrecy rate increases while the covert rate is fixed. The reason is that constraints (11b, 11c) and the objective function (11) are not function of \(d_{ae}\). 2) When the noise power
TABLE I: PLS versus covert communication

| Items             | Covet communication | PLS       |
|-------------------|---------------------|-----------|
| CSI               | Not necessary       | Necessary |
| Security level    | Medium              | High      |
| Legitimate jamming| Increase covertness | Increase security |
| Eve jamming       | Increase covertness | Decrease security |

at the eavesdropper is low or the eavesdropper is near to the source, covert communication outperformed PLS. Also, our results revealed that the optimality gap between the proposed methods and the exhaustive search method is inappreciable.

APPENDIX A

According to the strong law of large numbers (SLLN), $\chi^2_{2n}$ converges to 1, and based on the Lebesgues dominated convergence theorem [10], we can replace $\chi^2_{2n}$ with 1, when $n \to \infty$. Hence, we can rewrite (7) as

$$\begin{align*}
\mathbb{P}_{FA} &= \mathbb{P} \left( \sigma^2_e + \gamma > \vartheta | \Psi_0 \right), \\
\mathbb{P}_{MD} &= \mathbb{P} \left( \sigma^2_e + \gamma < \vartheta | \Psi_1 \right).
\end{align*}$$

(23)

By using the distribution of $\gamma$ as explained in [3], we calculate (23) and we reach to (9) and (9).

APPENDIX B

There are two cases for finding $\vartheta_{op}$. Case 1: When $\vartheta - \sigma^2_e < 0$, we have $\mathbb{P}_{FA} + \mathbb{P}_{MD} = 1$. Hence in this case, there is no optimal $\vartheta$. Case 2: When $\vartheta - \sigma^2_e \geq 0$, we have $\mathbb{P}_{FA} + \mathbb{P}_{MD} = 1 - e^{-\frac{\vartheta - \sigma^2_e}{\sigma_e^2}} + e^{-\frac{\vartheta - \sigma^2_e}{\sigma^2_e}}$. For obtaining $\vartheta^*$, we calculate $\vartheta^* = \left( \ln \left( \frac{\sigma_e^2}{\vartheta - \sigma^2_e} \right) + \sigma^2_e \right) \left( \frac{\vartheta - \sigma^2_e}{\sigma^2_e} \right)$. After some simplification, we have $\vartheta^* = \left( \ln \left( \frac{\sigma_e^2}{\vartheta - \sigma^2_e} \right) + \sigma^2_e \right) \left( \frac{\vartheta - \sigma^2_e}{\sigma^2_e} \right)$.

REFERENCES

[1] A. D. Wyner, “The wire-tap channel,” Bell Syst. Tech. J., vol. 54, no. 8, pp. 1355-1387, Oct. 1975.
[2] T. Sobers, B. Bash, S. Guha, D. Towsley, and D. Goeckel, “Covert communication in the presence of an uninformued jammer,” IEEE Trans. on Wireless Commun., vol. 16, no. 9, pp. 6193-6206, Sep. 2017.
[3] K. Shahzad, X. Zhou, and S. Yan, “Covert communication in fading channels under channel uncertainty,” arXiv: 1703.02169 [cs.IT]. 2017.
[4] M. Bloch, J. Barros, M. Rodrigues, and S. McLaughlin, “Wireless information-theoretic security,” IEEE Trans. Inf. Theory, vol. 54, no. 6, pp. 2515-2534, June 2011.
[5] L. Wang, M. Elkashlan and J. Huang, “Secure transmission with optimal power allocation in untrusted relay networks,” IEEE Wireless Commun Lett, vol. 3, no. 3, pp. 289 - 292, June 2014.
[6] A. Kuhestani, A. Mohammadni, and M. Mohammadni, “Joint relay selection and power allocation in large-scale MIMO systems with untrusted relays and passive eavesdroppers,” IEEE Trans. Inf. Forensics and Security, vol. 13, no. 2, pp. 341-355, Feb. 2018.
[7] A. Kuhestani, A. Mohammadni, K. K. Wong, P. L. Yeh, M. Moradikia, and M. R. Khandaker, “Optimal power allocation by imperfect hardware analysis in untrusted relaying networks,” arXiv: 1709.01334, 2017.
[8] S. Boyd and L. Vandenberghe, Convex Optimization, Cambridge University Press, 2004.
[9] I. CVX Research, CVX: Matlab software for disciplined convex programming, version 2.0, [http://cvxr.com/cvx] Aug. 2012.
[10] A. Browder, Mathematical Analysis: An Introduction, Springer-Verlag, 1996.
[11] M. Forouzesh, P. Azmi and N. Mokari, “Reduce impact of false detection of adversary states on the secure cooperative network,” in Proc. Int. Symp. on Telecommun. Tehran, Iran. Sept. 2016, pp. 261-265.