A Game-theoretic Approach to Covert Communications in the Presence of Multiple Colluding Wardens

Abbas Arghavani, Anders Ahlén, André Teixeira, Subhrakanti Dey
Division of Signals and Systems, Department of Electrical Engineering, Uppsala University, Sweden
Email: {abbas.arghavani, anders.ahlen, andre.teixeira, subhrakanti.dey}@angstrom.uu.se

***Abstract*—In this paper, we address the problem of covert communication under the presence of multiple wardens with a finite blocklength. The system consists of Alice, who aims to covertly transmit to Bob with the help of a jammer. The system also consists of a Fusion Center (FC), which combines all the wardens' information and decides on the presence or absence of Alice. Both Alice and jammer vary their signal power randomly to confuse the FC. In contrast, the FC randomly changes its threshold to confuse Alice. The main focus of the paper is to study the impact of employing multiple wardens on the trade-off between the probability of error at the FC and the outage probability at Bob. Hence, we formulate the probability of error and the outage probability under the assumption that the channels from Alice and jammer to Bob are subject to Rayleigh fading, while we assume that the channels from Alice and jammer to the wardens are not subject to fading. Then, we utilize a two-player zero-sum game approach to model the interaction between joint Alice and jammer as one player and the FC as the second player. We derive the pay-off function that can be efficiently computed using linear programming to find the optimal distributions of transmitting and jamming powers as well as thresholds used by the FC. The benefit of using a cooperative jammer is shown by means of analytical results and numerical simulations to neutralize the advantage of using multiple wardens at the FC.**

I. Introduction

Background & Motivations: To prevent eavesdroppers (i.e., wardens) from accessing the content of the packets, wireless communication protocols highly rely on encryption algorithms. However, their vulnerabilities have been revealed by manipulating non-computational techniques such as side-channel attacks [1]. Moreover, in some applications of wireless networks (e.g., military applications), the detection of transmission enables the adversary to discover the location of the transmitter for further attacks. Motivated by this, the idea of covert communication (also known as Low Probability Detection (LPD)) has been introduced to provide a higher tier of security via hiding wireless transmissions in noise so that: (1) the outage probability at the legitimate receiver is acceptably low; (2) the probability of error at an eavesdropper in detecting the transmission is arbitrary close to a random guess. The probability of error at the eavesdropper is defined as $\mathbb{P}_{FA}+\mathbb{P}_{MD}$ where $\mathbb{P}_{FA}$ is the probability that the warden raises the alarm while the transmitter (Alice) is not transmitting (i.e., false alarm), and $\mathbb{P}_{MD}$ is the probability that the eavesdropper (warden) does not detect Alice's transmission (i.e., missed detection). Hence, covertness is defined as below:

$$\mathbb{P}_{FA}+\mathbb{P}_{MD}\geq 1-\epsilon,\ \forall\epsilon>0.$$

The Direct Sequence Spread Spectrum (DSSS) [2] approach is probably the best practical example of covert communication. DSSS spreads the transmission bandwidth by modulating the information on pseudo-noise waves and suppressing the average Power Spectral Density (PSD) of the transmitted signal below the noise level, thus making it difficult to distinguish the transmitted signal from the noise. However, the performance of DSSS systems with additive white Gaussian noise (AWGN) between all parties is limited by the square root law [1]. That is, Alice can covertly transmit $O(\sqrt{N})$ bits in N channel uses to the receiver (Bob), where $N\to\infty$, which results in zero information-theoretic capacity as $\lim_{N\to\infty}O(\sqrt{N})/N$ [1]. In other words, to remain covert, Alice has to adjust her per-symbol transmit power to $O(1/\sqrt{N})$, which goes to 0 as $N\to\infty$.

The square root law is the case under the assumption that the warden knows the exact statistical characteristics of the background noise. That is, the law can be broken and a positive rate can be achieved (i.e., $O(N)$ bits in N channel uses can be transmitted) when there is uncertainty in the Signal to Interference plus Noise Ratio (SINR) at the warden's receiver [3]. Inspired by this, many research efforts have demonstrated the significant advantages of employing a jammer [4]–[6]. A jammer is a node that produces artificial noise by randomly varying its transmit power (or using a constant but randomized power by the fading channel) to increase uncertainty at the warden's SINR. The jammer may also cooperate with Alice and transmit the jamming signal when Alice is silent, and keep silent when Alice transmits [7].

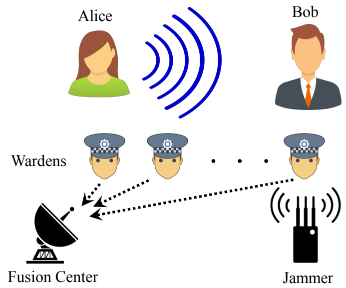


Figure 1: Illustration of the system model - with the help of jammer, Alice transmits covertly to Bob in the presence of multiple wardens.

This project is financed by the Swedish Foundation for Strategic Research.

Besides the asymptotic results given under infinite block length, the case with finite blocklength has been considered. In [8] Alice is suggested to vary its transmit power following a uniform distribution to confuse warden (i.e., increase uncertainty at warden). Leong *et al*. [9] considers the situation where the warden (in response to Alice's randomized power strategy), can randomly change its threshold. Following this situation, the interaction between Alice and the warden is formulated using a game-theoretic approach. Then, a utility function is introduced to make a trade-off between the achievable rate and the probability of error. Finally, the optimal distribution of Alice and jammer's power, as well as the warden's threshold, is computed using linear programming. This paper also shows that at a given achievable rate, utilizing a friendly jammer can significantly increase $\mathbb{P}_{FA} + \mathbb{P}_{MD}$.

Novelty & Contributions: Instead of the achievable rate, the current paper considers the trade-off between the outage probability at Bob (under a desired achievable rate) and the probability of error at FC. The paper also generalizes the game-theoretic approach in [9] to a scenario with multiple wardens, where the channel between Alice and Bob, as well as the channel between jammer and Bob, are subject to block Rayleigh fading. This is the worst-case scenario for Alice as the channel between Alice and wardens as well as the channel between jammer and wardens is AWGN and not subject to fading. The main contribution of the paper is as follows:

- We investigate the presence of multiple wardens, where they share their observations (i.e., their measurements) with a FC. The expressions for $\mathbb{P}_{FA}$ and $\mathbb{P}_{MD}$ are derived for (a) wardens with identical noise variance; (b) wardens with different noise variance.
- A zero-sum game formulation is provided where Alice optimizes a utility function achieving a trade-off between the outage probability and the probability of error at the FC, and the FC optimizes the negative of this utility. Optimal distributions of the joint Alice and jammer transmission powers and the thresholds at the FC are obtained via linear programming.
- We present some analytical results in the case of no jammer and an arbitrary number of wardens, showing that the optimal strategy at the FC is to use a unique threshold, whereas Alice randomizes her transmission power between at most two levels. We also show that in the presence of a jammer, increasing the number of wardens has a negligible benefit for the FC when the number of transmission blocks (channel uses) is sufficiently large.
- Extensive numerical results illustrate the benefit of having a coordinated jammer and Alice optimally choosing the joint distribution of their transmission powers in the presence of multiple wardens.

Section II details the system model and derives the general expressions for the probability of error as well as the outage probability. Section III gives the game-theoretic formulation of utility function. Section IV considers a special case scenario with identical noise variance at wardens. Section V derives the analytical results and Section VI presents numerical results via simulation. Finally, Section VII draws concluding remarks.

II. System Model and Metrics

A. Channel Model

Fig. 1 illustrates the system model, where Alice aims to covertly send a finite block of N complex-valued symbols to Bob. N can also be seen as the number of channel uses. To increase uncertainty at the wardens' noise level, the jammer, in cooperation with Alice, generates noise. We assume the channel from Alice to Bob and the channel from the jammer to Bob are (pessimistically, from Alice's perspective) subject to Rayleigh block fading, where the channels vary independently between blocks but remains unchanged within a block of N channel uses. Hence, denoting the absence and presence of Alice's transmission by H_0 and H_1, respectively, the received signal at Bob ($y_{b,k}$) is expressed as:

$$\begin{aligned} H_0 &: y_{b,k} = n_{b,k} + h_{jb} j_k \\ H_1 &: y_{b,k} = h_{ab} x_k + n_{b,k} + h_{jb} j_k \end{aligned} \tag{1}$$

where $n_{b,k} \sim CN(0, \sigma_b^2)$ is a zero-mean complex Gaussian noise at Bob. $x_k \sim CN(0, P^{(A)})$ and $j_k \sim CN(0, P^{(J)})$ denote the complex Gaussian signal to be transmitted by Alice and jammer, with power $P^{(A)}$ and $P^{(J)}$, respectively. h_{ab} and h_{jb} are Rayleigh fading coefficients with $E[|h_{ab}|^2] = E[|h_{jb}|^2] = 1$, and $k = 1, \ldots, N$. The channels from Alice and jammer to wardens are AWGN, and not subject to fading.

This paper assumes wardens employ a typical energy detector where they passively measure the energy over the channel from Alice and share their measurements with the FC. To detect the presence of Alice's transmission, the FC aggregates the received channel measurements (also known as a soft combination of decisions) and decides between the two hypotheses, given that the received signal at the warden w is

$$\begin{aligned} H_0 &: y_{w,k} = n_{w,k} + j_k \\ H_1 &: y_{w,k} = x_k + n_{w,k} + j_k \end{aligned} \tag{2}$$

where $n_{w,k} \sim CN(0, \sigma_w^2)$ is complex Gaussian noise at warden w and $w = 1, \ldots, W$. $y_{w,k} \sim CN(0, P^{(A)} + \sigma_w^2)$ and $y_{w,k} \sim CN(0, P^{(A)} + P^{(J)} + \sigma_w^2)$ is the received signal by warden w over the k^{th} channel in use under H_0 and H_1, respectively.

B. Detection of Covert Communication

To transmit each block of symbols, Alice randomly selects a power level $P^{(A)}$ from a finite set of powers (i.e., $P^{(A)} \in \{P_1^{(A)}, \ldots, P_I^{(A)}\}$). Likewise, jammer randomly takes jamming power $P^{(J)}$ on $\{P_1^{(J)}, \ldots, P_J^{(J)}\}$. The joint probability of transmitting and jamming power is defined as:

$$\pi_{i,j}^{A,J} = \mathbb{P}(P^{(A)} = P_i^{(A)} \wedge P^{(J)} = P_j^{(J)}).$$

Please note that the exact transmit and jamming power in each block is only known by Bob via a pre-shared codebook, but that FC only knows the joint distribution of $P^{(A)}$ and $P^{(J)}$. Once the FC receives all measurements from wardens, the test statistic T is produced by taking the weighted average of the measured channel samples:

$$T = \sum_{w=1}^{W} \omega_w T_w = \frac{1}{N} \sum_{w=1}^{W} \sum_{k=1}^{N} \omega_w |y_{w,k}|^2 \tag{3}$$

where ω_w is the weighting factor proportional to the $SINR$ at warden w:

$$\omega_w = \frac{SINR_w}{\sum_{i=1}^{W} SINR_i} \tag{4}$$

FC's optimal test to minimize the probability of error is the likelihood ratio test (LRT) [8]. Hence, assuming the probability that Alice transmits or not is equally likely (i.e., $\mathbb{P}(H_0) = \mathbb{P}(H_1) = 1/2$) the LRT is:

$$T \underset{H_1}{\overset{H_0}{\lessgtr}} t \tag{5}$$

where t is the threshold at FC which is randomly selected from a finite set $\{t_1, \dots, t_M\}$ with:

$$\pi_m^t = \mathbb{P}(t = t_m), \quad m \in \{1, \dots, M\}$$

Note that $\omega_w T_w$ given in Eq. 3 is a chi-squared distributed random variable with scaling factor $\omega_w(\sigma_w^2 + P^{(J)})/2N$ under H_0 and scaling factor $\omega_w(\sigma_w^2 + P^{(J)} + P^{(A)})/2N$ under H_1.

$$\omega_w T_w = \begin{cases} H_0 : \ \frac{\omega_w(\sigma_w^2 + P^{(J)})}{2N} \sum_{k=1}^{N} \frac{\left|y_{w,k}\right|^2}{\sigma_w^2 + P^{(J)}} \\ H_1 : \ \frac{\omega_w(\sigma_w^2 + P^{(J)} + P^{(A)})}{2N} \sum_{k=1}^{N} \frac{\left|y_{w,k}\right|^2}{\sigma_w^2 + P^{(J)} + P^{(A)}} \end{cases} \tag{6}$$

Thus, T is the sum of W independent scaled chi-squared distributed random variables with different parameters, and its likelihood function under H_0 is [10]:

$$f(T|H_0) = \sum_{i=1}^{I} \sum_{j=1}^{J} \sum_{k=0}^{\infty} c_j \delta_{j,k} \frac{T^{\rho+k-1} \exp(-\frac{T}{\theta_j^\star})}{\Gamma(\rho+k) \theta_j^{\star\rho+k}} \pi_{i,j}^{A,J} \tag{7}$$

where $\rho = WN$, $\theta_{j,w} = \omega_w(\sigma_w^2 + P_j^{(J)})/N$, $\theta_j^\star = \min_w \theta_{j,w}$, $c_j = \prod_{w=1}^{W} \left(\theta_j^\star / \theta_{j,w}\right)^N$ and $\delta_{j,k}$ is found by recursion from:

$$\delta_{j,k+1} = \frac{1}{k+1} \sum_{l=1}^{k+1} l \zeta_{j,l} \delta_{j,k+1-l}, \ k = 0, 1, 2, \dots, \ \delta_{j,0} = 1$$

and $\zeta_{j,k} = \sum_{w=1}^{W} N\big(1 - \theta_j^\star/\theta_{j,w}\big)^k/k, \ k = 1, 2, 3, \dots.$ In the same way, the likelihood function of T under H_1 can be expressed as:

$$f(T|H_1) = \sum_{i=1}^{I} \sum_{j=1}^{J} \sum_{k=0}^{\infty} C_{i,j} \Delta_{i,j,k} \frac{T^{\rho+k-1} \exp(-\frac{T}{\Theta_{i,j}^\star})}{\Gamma(\rho+k) \Theta_{i,j}^{\star\rho+k}} \pi_{i,j}^{A,J} \tag{8}$$

where $\Theta_{w,i,j} = \frac{\omega_w(P^{(A)} + P^{(J)} + \sigma_w^2)}{N}$, $\Theta_{i,j}^\star = \min_w \theta_{w,i,j}$, $C_{i,j} = \prod_{w=1}^{W} \left(\frac{\Theta_{i,j}^\star}{\Theta_{w,i,j}}\right)^N$, and $\Delta_{i,j,k}$ is recursively calculated:

$$\Delta_{i,j,k+1} = \frac{1}{k+1} \sum_{l=1}^{k+1} l Z_{i,j,l} \Delta_{i,j,k+1-l}, \ k = 0, 1, 2, \dots, \quad \Delta_{i,j,0} = 1$$

and $Z_{i,j,k} = \sum_{w=1}^{W} \frac{N\left(1 - \frac{\Theta_{i,j}^\star}{\Theta_{i,j,w}}\right)^k}{k}, \ k = 1, 2, 3, \dots.$

The detection performance of FC is subject to two types of error probabilities: (I) $\mathbb{P}_{FA}$ denoting the probability of rejecting H_0 when it is true (i.e., $\mathbb{P}_{FA} = \mathbb{P}(decide H_1 | H_0)$); and (II) $\mathbb{P}_{MD}$ denoting the probability of rejecting H_1 when it is true (i.e., $\mathbb{P}_{MD} = \mathbb{P}(decide H_0 | H_1)$). Thus, for a given distribution of detection thresholds (π^t) and joint transmit and jamming power ($\pi^{A,J}$), $\mathbb{P}_{FA}$ and $\mathbb{P}_{MD}$ are defined as follows:

$$\mathbb{P}_{FA}(\pi^{A,J}, \pi^t) = \mathbb{P}(T > t | \pi^{A,J}, \pi^t, H_0) = \sum_{i=1}^{I} \sum_{j=1}^{J} \sum_{m=1}^{M} \sum_{k=0}^{\infty} c_j \delta_{j,k} \frac{\Gamma\big(\rho+k, \frac{t_m}{\theta_j^\star}\big)}{\Gamma(\rho+k)} \pi_{i,j}^{A,J} \pi_m^t \tag{9}$$

$$\mathbb{P}_{MD}(\pi^{A,J}, \pi^t) = \mathbb{P}(T < t | \pi^{A,J}, \pi^t, H_1) = 1 - \sum_{m=1}^{M} \sum_{i=1}^{I} \sum_{j=1}^{J} \sum_{k=0}^{\infty} C_{i,j} \Delta_{i,j,k} \frac{\Gamma\big(\rho+k, \frac{t_m}{\Theta_{i,j}^\star}\big)}{\Gamma(\rho+k)} \pi_{i,j}^{A,J} \pi_m^t \tag{10}$$

where $\Gamma(.)$ and $\Gamma(.,.)$ are complete and upper incomplete gamma function.

C. Outage Probability

To support a target achievable rate (R_T), the threshold $SINR$ at Bob (τ) is required to satisfy the given equality [9]:

$$R_T \approx log_2(1+\tau) - \sqrt{\frac{1}{N} \frac{1}{(1+\tau)^2}} \frac{Q^{-1}(\upsilon)}{ln(2)}$$

where $Q^{-1}(.)$ is the inverse Q-function, and υ is the coding probability of error. The outage probability under the constraint of satisfying a target achievable rate R_T is the probability that the $SINR$ at Bob falls below τ. Following the fact that (a) both Alice and jammer randomize on a set of transmit powers; and (b) the channel from Alice to Bob, as well as the channel from jammer to Bob, is subject to Rayleigh fading, the outage probability is as given below:

$$\mathbb{P}_{out}(\pi^{A,J}, \tau) = \mathbb{P}\left(\frac{|h_{ab}|^2 P^{(A)}}{\sigma_b^2 + |h_{jb}|^2 P^{(J)}} < \tau\right) = 1 - \sum_{i=1}^{I} \sum_{j=1}^{J} \frac{e^{-\frac{\tau \sigma_b^2}{P_i^{(A)}}}}{1 + \frac{\tau P_j^{(J)}}{P_i^{(A)}}} \pi_{i,j}^{A,J} \tag{11}$$

III. Game-theoretic Formulation

Following the proposed approach in [9], this section formulates the interaction between Alice, jammer, and the FC as a two-player zero-sum game. Alice and jammer, on one side, cooperatively randomize on a finite set of power levels aiming to confuse the FC, and accordingly, increase the probability of error. In parallel, Alice wishes to minimize the $\mathbb{P}_{out}$ (equivalently maximize $1 - \mathbb{P}_{out}$) satisfying a minimum required achievable rate. We can conclude this into Alice's utility function as below:

$$U = 1 - \mathbb{P}_{out}(\pi^{A,J}, \tau) + \beta\Big(P_{FA}(\pi^{A,J}, \pi^t) + P_{MD}(\pi^{A,J}, \pi^t)\Big) \tag{12}$$

where β signifies the trade-off between outage probability and the probability of error. In other words, β allows Alice to trade the probability of error for a desirable outage probability.

On the other side, the FC confuses Alice by randomizing between a finite set of thresholds aiming to minimize the probability of error (i.e., maximize the negative of the probability of error). It is also reasonable that the FC prefers a higher $\mathbb{P}_{out}$ at Bob. Motivated by this, a utility function for FC can be the negative of the utility function in Eq. (12). That is, the gain of the FC is equivalent to Alice's loss. Thus, the competitive conflict between Alice and FC can be formulated as a two-player zero-sum game. The Nash equilibrium mixed strategy for Alice can be found by solving the linear program:

$$\begin{aligned} &\max_{\{\pi_{i,j}^{A,J}\}} U \\ &s.t. \sum_{i=1}^{I}\sum_{j=1}^{J}\Bigg[\frac{e^{-\frac{\tau\sigma_b^2}{P_i^{(A)}}}}{1+\frac{\tau P_j^{(J)}}{P_i^{(A)}}}+\beta\Bigg(\sum_{k=0}^{\infty}c_j\delta_{j,k}\frac{\Gamma\big(\rho+k,\frac{t_m}{\theta_j^\star}\big)}{\Gamma(\rho+k)} \\ &+1-\sum_{k=0}^{\infty}C_{i,j}\Delta_{i,j,k}\frac{\Gamma\big(\rho+k,\frac{t_m}{\Theta_{i,j}^\star}\big)}{\Gamma(\rho+k)}\Bigg)\Bigg]\pi_{i,j}^{A,J}>U \\ &m=1,\dots,M,\quad \sum_{i=1}^{I}\sum_{j=1}^{J}\pi_{i,j}^{A,J}=1,\quad \pi_{i,j}^{A,J}\geq 0. \end{aligned} \tag{13}$$

Likewise, a Nash equilibrium mixed strategy for FC can be found by solving the linear program:

$$\begin{aligned} &\min_{\{\pi_m^t\}} U \\ &s.t. \sum_{m=1}^{M}\Bigg[\frac{e^{-\frac{\tau\sigma_b^2}{P_i^{(A)}}}}{1+\frac{\tau P_j^{(J)}}{P_i^{(A)}}}+\beta\Bigg(\sum_{k=0}^{\infty}c_j\delta_{j,k}\frac{\Gamma\big(\rho+k,\frac{t_m}{\theta_j^\star}\big)}{\Gamma(\rho+k)} \\ &+1-\sum_{k=0}^{\infty}C_{i,j}\Delta_{i,j,k}\frac{\Gamma\big(\rho+k,\frac{t_m}{\Theta_{i,j}^\star}\big)}{\Gamma(\rho+k)}\Bigg)\Bigg]\pi_m^t<U \\ &i=1,\dots,I,\quad j=1,\dots,J,\quad \sum_{m=1}^{M}\pi_m^t=1,\quad \pi_m^t\geq 0 \end{aligned} \tag{14}$$

Please note that although the linear program in (13) does not follow the standard form of linear programs, it can be put into the standard form by vectorization of the joint probability distribution matrix $\pi_{i,j}^{A,J}$.

IV. A Special Case Scenario with Identical Noise Variance at Wardens

Consider the case where all wardens experience the same noise variance:

$$\sigma_w^2=\sigma_{w'}^2,\quad \forall w,w'\in\{1,2,\dots,W\}.$$

Thus:

$$\omega_w=\frac{1}{W},\quad w=1,\dots,W.$$

Replacing ω_w by $1/W$ in Eq. (3), the average measured energy at the FC can be written as follows:

$$T=\frac{1}{W}\sum_{w=1}^{W}T_w=\frac{1}{WN}\sum_{k=1}^{N}|y_{w,k}|^2. \tag{15}$$

The test statistic T is a scaled chi-squared distributed random variable with scaling factor $(\sigma_w^2+P^{(J)})/2\,WN$ under H_0 and scaling factor $(\sigma_w^2+P^{(J)}+P^{(A)})/2\,WN$ under H_1. Therefore, the likelihood function of T under H_0 and H_1 is defined respectively:

$$\begin{aligned} f(T|H_0)=&\frac{T^{WN-1}}{\Gamma(WN)}\sum_{i=1}^{I}\sum_{j=1}^{J}\Bigg[\Big(\frac{WN}{P_j^{(J)}+\sigma_w^2}\Big)^{WN} \\ &\times exp\Big(-\frac{WNT}{P_j^{(J)}+\sigma_w^2}\Big)\Bigg]\pi_{i,j}^{A,J} \end{aligned} \tag{16}$$

$$\begin{aligned} f(T|H_1)=&\frac{T^{WN-1}}{\Gamma(WN)}\sum_{i=1}^{I}\sum_{j=1}^{J}\Bigg[\Big(\frac{WN}{\sigma_w^2+P_j^{(J)}+P_i^{(A)}}\Big)^{WN} \\ &\times exp\Big(-\frac{WNT}{\sigma_w^2+P_j^{(J)}+P_i^{(A)}}\Big)\Bigg]\pi_{i,j}^{A,J}. \end{aligned} \tag{17}$$

For a given distribution of detection thresholds (π^t) and joint transmit and jamming power levels ($\pi^{A,J}$), $\mathbb{P}_{FA}$ and $\mathbb{P}_{MD}$ are defined as follows:

$$\mathbb{P}_{FA}(\pi^{A,J},\pi^t)=\sum_{m=1}^{M}\sum_{i=1}^{I}\sum_{j=1}^{J}\frac{\Gamma(WN,\frac{WNt_m}{\sigma_w^2+P_j^{(J)}})}{\Gamma(WN)}\pi_{i,j}^{A,J}\pi_m^t \tag{18}$$

$$\begin{aligned} \mathbb{P}_{MD}(\pi^{A,J},\pi^t)=&\sum_{i=1}^{I}\sum_{j=1}^{J}\sum_{m=1}^{M}\Bigg[1- \\ &\frac{\Gamma(WN,\frac{WNt_m}{\sigma_w^2+P_j^{(J)}+P_i^{(A)}})}{\Gamma(WN)}\Bigg]\pi_{i,j}^{A,J}\pi_m^t. \end{aligned} \tag{19}$$

V. Analytical Results

Theorem 1. *With an arbitrary number of W wardens but without the presence of the jammer (i.e., $P^{(J)}=0$), the Nash equilibrium strategy at the FC includes only one threshold with probability one while, Alice's Nash equilibrium strategy involves randomizing between at most two transmit powers.*

Proof. Consider the utility function in Eq. (12). To find the support set of optimal thresholds of the FC for a given Alice's transmit power distribution, we can calculate the first derivative of the utility function w.r.t the threshold t and set it equal to zero as:

$$\begin{aligned} \frac{\partial U}{\partial t}=&\sum_{i=1}^{I}\sum_{m=1}^{M}\Big[\exp\Big(-\frac{WNt_m}{\sigma_w^2+P_i^{(A)}}\Big)\Big(\frac{WNt_m}{\sigma_w^2+P_i^{(A)}}\Big)^{WN} \\ &-\exp\Big(-\frac{WNt_m}{\sigma_w^2}\Big)\Big(\frac{WNt_m}{\sigma_w^2}\Big)^{WN}\Big]\times\frac{\pi_i^A\pi_m^t}{t_m\Gamma(WN)}=0. \end{aligned} \tag{20}$$

After simplifying Eq. (20), we can get the following equality, solving which gives the optimal thresholds ($t^\star$).

$$\sum_{i=1}^{I}\Big(\frac{\sigma_w^2}{\sigma_w^2+P_i^{(A)}}\Big)^{WN}\exp\Big(\frac{WNt^\star P_i^{(A)}}{\sigma_w^2(\sigma_w^2+P_i^{(A)})}\Big)\pi_i^A=1 \tag{21}$$

At a given Alice's transmit power distribution, each summand in Eq. (21) is a strictly increasing function of t, thus, the whole sum in the left-hand side is a strictly increasing function of t, which guarantees the uniqueness of the solution ($t^\star$). One can also show that the second derivative at this point is positive. Hence we can conclude that $t^\star$ minimizes the utility function. Thus, it is the optimal choice for the FC.

On the other hand, since there is only one optimal threshold for FC, then from Caratheodory's theorem [11] the Alice's Nash equilibrium has at most two transmit powers. In other words, since the utility of each power level $P_i^{(A)}$ at a given $t^\star$ is a one-dimensional real value and Alice's utility U is a convex combination of utilities of power levels (i.e., lies in the convex hull of the utility of power levels), Alice's utility can be written as a convex combination of utilities achieved by at most 2 power levels. □

Remark. The range of the optimal threshold $t^\star$*: Consider a scenario without the presence of the jammer where multiple wardens experience the same noise variance. Given that* $\mathbb{P}_{FA} + \mathbb{P}_{MD} > 1 - \epsilon$*, it can be shown that the range of* $t^\star$ *is:*[1]

$$t^\star \in [\sigma_w^2 - \frac{\sigma_w^2}{2WN}\sqrt{\frac{2}{\epsilon}}, \sigma_w^2 + P_1^{(A)} + \frac{\sigma_w^2 + P_i^{(A)}}{2WN}\sqrt{\frac{2}{\epsilon}}].$$

Theorem 2. *Let* $1 - \mathbb{P}(E)$ *and* $1 - \mathbb{P}(E)'$ *be the probability that* $\mathbb{P}_{FA} + \mathbb{P}_{MD} > 1 - \epsilon$ *at a desirable* $1 - \mathbb{P}_{out}$ *in scenarios with* W *and* W' *wardens, respectively, where* $W < W'$*. Then, by choosing* $N > N_\mu$, $\mathbb{P}(E) - \mathbb{P}(E)' < \mu$ *for any* $\mu > 0$*, as long as* N_μ *is sufficiently larger than* $\sqrt{\frac{2}{\epsilon}}$.

Proof. For the sake of simplicity, we consider the multiple-warden case scenario with identical noise variance. A similar approach can be applied to the case with non-identical noise variance. Assume a desirable $1 - \mathbb{P}_{out} = \gamma$ is required to be satisfied. Therefore, following Eq. (11), $P^{(J)}$ turns out to be a strictly increasing function of $P^{(A)}$ so that there is a unique $P_i^{(J)} > 0$ corresponding to any $P_i^{(A)} > -\frac{\tau\sigma_b^2}{ln(\gamma)}$ that satisfies the equation below:

$$P_i^{(J)} = \frac{P_i^{(A)}}{\tau}\Bigg(\frac{e^{-\frac{\tau\sigma_b^2}{P_i^{(A)}}}}{\gamma} - 1\Bigg). \tag{22}$$

Since $\mathbb{P}_{FA} = \mathbb{P}(T > t|H_0)$, the following can be derived from Chebyshev's inequality:

$$\mathbb{P}\big(2WN - \epsilon_0 \leq \chi^2_{2WN} \leq 2WN + \epsilon_0\big) \geq 1 - \frac{2}{\epsilon_0^2}. \tag{23}$$

Hence, for T under H_0 (see Eq. (6)) it can be concluded that:

$$\mathbb{P}\big(\sigma_w^2 + P_i^{(J)} - \psi_1(i) \leq T \leq \sigma_w^2 + P_i^{(J)} + \psi_1(i)\big) \geq 1 - \epsilon \tag{24}$$

where $\epsilon = \frac{2}{\epsilon_0^2}$ and $\psi_1(i) = \frac{\sigma_w^2 + P_i^{(J)}}{2WN}\epsilon_0$. That is, for any $t_i < \sigma_w^2 + P_i^{(J)} - \psi_1(i)$, $P_{FA} > 1 - \epsilon$. Likewise, following analogous arguments, for any $t_i > \sigma_w^2 + P_i^{(J)} + P_i^{(A)} + \psi_2(i)$, $P_{MD} > 1 - \epsilon$, where $\psi_2(i) = \frac{\sigma_w^2 + P_i^{(J)} + P_i^{(A)}}{2WN}\epsilon_0$. Therefore, it can be concluded that if either (I) $t_i > \sigma_w^2 + P_i^{(J)} + P_i^{(A)} + \psi_2(i)$ or (II) $t_i < \sigma_w^2 + P_i^{(J)} - \psi_1(i)$ is correct, $\mathbb{P}_{FA} + \mathbb{P}_{MD} > 1 - \epsilon$. Let E be the event that neither of (I) or (II) happens. That is, $E : \sigma_w^2 + P_i^{(J)} - \psi_1(i) < t_i < \sigma_w^2 + P_i^{(J)} + P_i^{(A)} + \psi_2(i)$. Let $\mathbb{P}(E)$ be the probability that event E happens. Hence, $1 - \mathbb{P}(E)$ represents the probability $\mathbb{P}_{FA} + \mathbb{P}_{MD} > 1 - \epsilon$. For any $P_i^{(A)}$ and $P_i^{(J)}$ that satisfies Eq. (22), FC can achieve $\mathbb{P}(E) = 1$ by adjusting its threshold to:

$$t_i = \sigma_w^2 + P_i^{(J)} - \psi_1(i) + \phi_i = \sigma_w^2 + P_i^{(J)} + P_i^{(A)} + \psi_2(i) - \phi_i \tag{25}$$

where $\phi_i = (P_i^{(A)} + \psi_1(i) + \psi_2(i))/2$. Alice and jammer can avoid this by switching to a different pair of transmit and jamming power $(P_{i+1}^{(A)}, P_{i+1}^{(J)})$ satisfying either (I) or (II) as well as Eq. (22). To this end, it is enough to set $P_{i+1}^{(J)}$ as:

$$P_{i+1}^{(J)} = P_i^{(J)} + \phi_i + \psi_1(i+1) - \psi_1(i) \tag{26}$$

and accordingly set $P_{i+1}^{(A)}$ based on Eq. (22). Similarly, the FC can take the corresponding threshold t_{i+1}. Assume there are n pairs of $(P_{i+1}^{(A)}, P_{i+1}^{(J)})$ that satisfies Eq. 22. Since Alice, jammer, and FC randomly select the transmission power levels and thresholds, respectively, $\mathbb{P}(E)$ is calculated as follows:

$$\mathbb{P}(\mathbb{E}) = \sum_{i=1}^{n} \pi_{i,i}^{A,J} \times \pi_i^t. \tag{27}$$

The FC knows Alice and Jammer's distribution of power levels, so it can maximize $\mathbb{P}(E)$ by taking $\pi_k^t = 1$ where:

$$k = \underset{1 \leq i \leq n}{\operatorname{argmax}}(\pi_{i,i}^{A,J}). \tag{28}$$

Thus, the best strategy for Alice and jammer is to use a uniform distribution ($\pi_{i,i}^{A,J} = 1/n$) under which $\mathbb{P}(E) = 1/n$. Following Eq. (26), n can be obtained by solving the equality below:

$$\sum_{i=1}^{n-1} \phi_i + \psi_1(i+1) - \psi_1(i) = P_J^{(J)} - P_1^{(J)}. \tag{29}$$

Let $N_\lambda >> \epsilon_0 = \sqrt{\frac{2}{\epsilon}}$ be the number of channel uses which results $\psi_1(i+1) - \psi_1(i) = \lambda$, where λ is an arbitrarily small number. By choosing $N > N_\lambda$, Eq. (29) can be written as below:

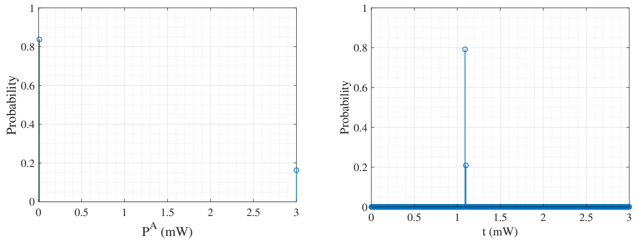
$$0 < P_J^{(J)} - P_1^{(J)} - \frac{1}{2}\sum_{i=1}^{n-1} P_i^{(A)} < \lambda, \ \forall \lambda > 0. \tag{30}$$

As can be shown, n (and consequently $\mathbb{P}(E)$) does not depend on W and σ_w^2, as one can make λ arbitrarily small. □

VI. Numerical Results

In this section, we perform extensive simulations in order to verify the proposed analytical results. We further compare the performance of the proposed approach with uniform distribution as well as a constant transmit power scheme. This section considers the single-warden scenario first. It provides some plots of the Nash equilibrium mixed strategy and examines

[1]The proof is omitted due to space constraints.



(a) (b)

Figure 2: Probability distribution of (a) Alice's transmit power level (b) thresholds at FC; in a single-warden scenario without the jammer.

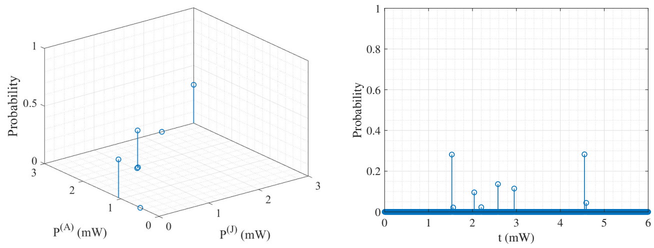
the covert performance of the game-theoretic approach in a trade-off with the outage probability. The rest of this section discusses the impact of utilizing multiple wardens on the mentioned trade-off.

In most of the simulations throughout this section, we assume Alice's transmit powers are quantized from 0.01 mW to 3 mW in steps of 0.001 mW. Likewise, the jamming power is discretized from 0 mW to 3 mW in steps of 0.001 mW. The detection threshold at FC ranges from 0.01 mW to 6 mW with a step size of 0.001 mW. The number of channel uses (N) is set to 200, and the noise variance at Bob (σ_b^2) and wardens (σ_w^2) is 0 dBm. We also set the target achievable rate to $R_T = 0.4$ bits per channel uses and υ = 0.1, turns out the threshold SINR (i.e., τ) to be almost 0.407.

A. *Single-warden case Scenario*

For the sake of simplicity of analysis, we first consider a scenario with a single warden without the presence of a cooperative jammer. Let $\beta = 1$. Fig. 2a and Fig. 2b illustrates the distribution (i.e., the Nash equilibrium) of Alice's transmit power and the thresholds at the FC, respectively. The results show that Alice's Nash equilibrium is to randomize between the minimum and the maximum transmit power level, while the Nash equilibrium strategy for FC is to randomize between two adjacent thresholds close to $\sigma_w^2 + P_1^{(A)}$. However, as expected, repeating the simulation reveals that the two thresholds of FC overlap when the granularity level of thresholds is increased. We also repeated the simulation under different values of β ranging from 0.1 to 4, which leads to three key observations: (1) Increasing β (i.e., emphasising more on the probability of error) motivates Alice to select her minimum power level with a higher probability so that, for large βs Alice's mixed strategy is replaced by a pure strategy with $\mathbb{P}(P^{(A)} = P_1^{(A)}) = 1$; (2) Decreasing the value of β motivates Alice to increase the probability of transmission with the maximum power level. Accordingly, for small values of βs, Alice's mixed strategy is changed to a pure strategy with $\mathbb{P}(P^{(A)} = P_I^{(A)}) = 1$; (3) At some βs close to 1, Alice randomizes between her maximum transmit power and another power level very close to her minimum transmit power.

We repeated the simulations under the presence of the jammer. Fig. 3a illustrates the joint distribution of Alice and jammer's transmit power. Unlike the case without the jammer, Alice and jammer jointly randomize on several transmit powers in equilibrium. This is also the case for the FC. As is shown in Fig 3b, the Nash equilibrium mixed strategy of FC



(a) (b)

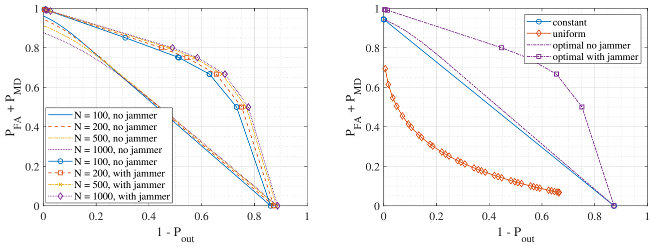
Figure 3: (a) Joint probability distribution of Alice and jammer's transmit powers; (b) probability distribution of thresholds at FC; under a single-warden case scenario and presence of jammer.

includes several thresholds. We also repeated the simulation for different βs ranging from 0.1 to 4, based on which we plotted the trade-off between $1 - P_{out}$ and probability of error in Fig. 4. As is expected, increasing β enables Alice to gain a higher probability of error, though, at the cost of lower $1-\mathbb{P}_{out}$. We further plotted the simulation results for different N ranging from 100 to 1000 channel uses. The key observation is that regardless of the length of the blocks, the presence of the jammer results in a significantly better performance for Alice (i.e., a higher probability of error at a given $1 - \mathbb{P}_{out}$). It can also be observed that at a desired $1 - \mathbb{P}_{out}$ in scenarios without the presence of the jammer, utilizing larger N provides a lower probability of error. This is reasonable due to the fact that the larger blocks provide FC with more observations and accordingly, less erroneous decisions [1]. This is the other way around under the presence of the jammer. As is shown, utilizing larger blocks results in a slightly better performance for Alice which is consistent with the results of [5].

We further compare the proposed approach with a constant power scheme and the scheme with uniformly distributed transmit powers [8] in Fig. 4b. For constant power scheme, Alice considers different transmit powers from 0.01mW to 3 mW, for each of which, the FC finds the optimal threshold that minimizes the utility. Among them, Alice selects the power level that maximizes the utility as its transmit power level. For uniform distribution scheme, to find the best range of transmit powers, Alice considers $N-1$ different range of transmit powers identified by $\{0.01, \ldots, 0.01k\}$ where $k \in \{2, ..., N\}$. Note that $k \neq 1$ otherwise it turns out to a constant power scheme. Under each range of transmit powers, the optimal threshold at the FC is calculated. Among them, Alice selects the range with the maximum utility. As can be seen, unlike the uniform distribution scheme which has the worst performance, the constant power scheme is almost as good as the proposed approach in the case of no jammer. This is expected as the optimal distribution is also a pure strategy (i.e., a constant transmit power) under many values of β. That is, choosing any power with uniform probability is bound to be sub-optimal.

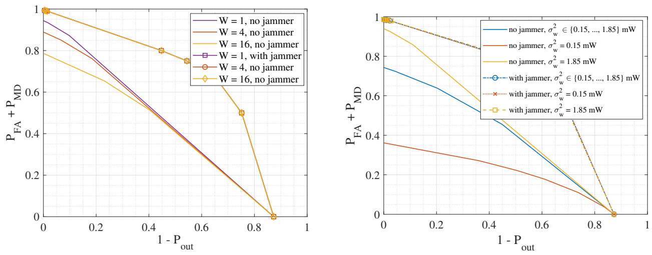
B. *Multiple-wardens Case Scenario*

Fig. 5 illustrates the trade-off between the outage probability and the probability of error under the utilization of multiple wardens. For the sake of simplicity of analysis, we first assume wardens experience identical noise variance with $\sigma_w^2 = 1$ mW. As is shown in Fig. 5a, increasing the number of wardens in



(a) (b)

Figure 4: (a) Impact of increasing N on the expected $1 - \mathbb{P}_{out}$ vs. $\mathbb{P}_{FA} + \mathbb{P}_{MD}$, with and without jammer; (b) Constant, optimal, and uniform distribution scheme (β varies from 0.1 to 4).



(a) (b)

Figure 5: Expected $1 - \mathbb{P}_{out}$ vs. $\mathbb{P}_{FA} + \mathbb{P}_{MD}$ in soft combination of decisions, with and without jammer, (a) with multiple wardens and the same noise variance; (b) with 4 wardens and different noise variances (β varies from 0.1 to 4).

scenarios without the presence of the jammer monotonically reduces Alice's performance. Generally, utilizing multiple wardens enable the FC to collect more observations. From the perspective of the FC only, this is analogous to increasing N (i.e., number of observations). Thus, the results presented in Fig. 5a almost match to that of the Fig. 4. Introducing the jammer to the environment significantly improves Alice's performance, however, the results under the different number of wardens overlap. That is, increasing the number of wardens from 1 to 16 under the presence of the jammer, does not lead to a significant change in the trade-off between the probability of error and outage probability. This illustrates the analytical result presented in *Theorem* 2.

To further investigate the impact of utilizing multiple wardens, simulation scenarios are repeated with four wardens, each of which has a different noise variance ($\sigma_w^2 \in \{0.15, 0.715, 1.28, 1.85\}$ mW) where the arithmetic mean of the noise variances is 1 mW. The results with and without the presence of the jammer are shown in Fig. 5b. To provide a better analogy, we also include some simulation results with identical noise variance at wardens. As is shown, except for very high outage probability requirements, increasing the noise variance at wardens always results in a higher probability of error at the FC. Additionally, the presence of the jammer not only increases the error probability at the FC but also neutralizes the impact of using multiple wardens. This indicates that the analytical results presented in *Theorem* 2 applies to scenarios with non-identical noise variance as well.

VII. Conclusions

In this paper, we examined the impact of utilizing multiple colluding wardens on covert communication. The considered system consisted of Alice, Bob, a friendly jammer, and multiple wardens that provide channel observations to a FC which is in charge of deciding on the presence of Alice. To confuse the FC, Alice and jammer randomly vary their transmit power and jamming power according to a joint distribution, respectively. Likewise, the FC randomly varies its threshold to confuse Alice. We formulate the interaction between Alice and the jammer (one player) and the FC (second player) as a zero-sum game where Alice and the jammer cooperatively optimize a utility function reflecting a trade-off between Alice's outage probability at Bob and the probability of detection error at the FC, while the FC optimizes the negative of this utility. The optimal probability distributions for the transmission powers and the thresholds are found via linear programming.

Analytical results reveal that without the presence of the jammer, the optimal threshold distribution (i.e., the Nash equilibrium strategy) for FC includes only one threshold while Alice randomizes between at most two transmit powers. Furthermore, we also show that increasing the number of wardens significantly reduces the outage probability under high covertness requirements. However, utilizing a friendly jammer can effectively neutralize the advantage of using multiple wardens for FC. In addition, compared to the uniformly distributed transmit power scheme and constant power scheme, the game-theoretic approach significantly enhances Alice's performance, especially under the presence of a jammer.

References

[1] B. A. Bash, D. Goeckel, and D. Towsley, "Limits of reliable communication with low probability of detection on awgn channels," *IEEE journal on selected areas in communications*, vol. 31, no. 9, pp. 1921–1930, 2013.

[2] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt, *Spread Spectrum Communications Handbook*. McGraw-Hill, 1994.

[3] S. Lee, R. J. Baxley, M. A. Weitnauer, and B. Walkenhorst, "Achieving undetectable communication," *IEEE Journal of Selected Topics in Signal Processing*, vol. 9, no. 7, pp. 1195–1205, 2015.

[4] K. Li, P. A. Kelly, and D. Goeckel, "Optimal power adaptation in covert communication with an uninformed jammer," *IEEE Transactions on Wireless Communications*, vol. 19, no. 5, pp. 3463–3473, 2020.

[5] T. V. Sobers, B. A. Bash, S. Guha, D. Towsley, and D. Goeckel, "Covert communication in the presence of an uninformed jammer," *IEEE Transactions on Wireless Communications*, vol. 16, no. 9, pp. 6193–6206, 2017.

[6] R. Soltani, D. Goeckel, D. Towsley, B. A. Bash, and S. Guha, "Covert wireless communication with artificial noise generation," *IEEE Transactions on Wireless Communications*, vol. 17, no. 11, pp. 7252–7267, 2018.

[7] W. Xiong, Y. Yao, X. Fu, and S. Li, "Covert communication with cognitive jammer," *IEEE Wireless Communications Letters*, vol. 9, no. 10, pp. 1753–1757, 2020.

[8] S. Yan, B. He, X. Zhou, Y. Cong, and A. L. Swindlehurst, "Delay-intolerant covert communications with either fixed or random transmit power," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 1, pp. 129–140, 2019.

[9] A. S. Leong, D. E. Quevedo, and S. Dey, "A game-theoretic approach to covert communications," *arXiv preprint arXiv:1911.00156*, 2019.

[10] P. G. Moschopoulos, "The distribution of the sum of independent gamma random variables," *Annals of the Institute of Statistical Mathematics*, vol. 37, no. 3, pp. 541–544, 1985.

[11] C. Carathéodory, "Über den variabilitätsbereich der fourier'schen konstanten von positiven harmonischen funktionen," *Rendiconti Del Circolo Matematico di Palermo (1884-1940)*, vol. 32, no. 1, pp. 193–217, 1911.