Channel-Aware Power Allocation for Enhanced Covert Communication with Friendly Jammer

Emmanuel Kwaning Kwakye, Taehoon Kim[+*], Inkyu Bang[*]
Hanbat National University
ekwakye@edu.hanbat.ac.kr, thkim@hanbat.ac.kr, ikbang@hanbat.ac.kr

Abstract

This paper investigates a jammer-assisted covert communication system where a transmitter (Alice) aims to deliver messages to a legitimate receiver (Bob) without being detected by a passive warden (Willie). To enhance covert throughput under covertness we propose a channel-aware jammer power allocation strategy based on the complementary cumulative distribution function (CCDF) of the jammer-to-receiver channel gain. The scheme adaptively adjusts jamming power to reduce interference at Bob while increasing uncertainty at Willie. We derive the detection error probability (DEP) and evaluate covert throughput, showing via simulations that the CCDF-based method outperforms uniform power allocation

I . INTRODUCTION

The evolution of wireless technologies has enabled the deployment of 5G networks and accelerated research into 6G innovations for massive connectivity, ultra-low latency, and ubiquitous data services [1]. However, the open and dynamic architecture of these networks introduces new security and privacy vulnerabilities. Traditional cryptographic approaches are often inadequate against adversaries who exploit physical-layer characteristics, prompting increased interest in techniques such as physical layer security (PLS) and covert communication. Covert communication, also referred to as low probability of detection (LPD) communication, aims to hide the existence of a transmission rather than protecting its contents as in PLS [3].

The fundamental limit of covert communication is governed by the square-root law, which states that at most $O(\sqrt{n})$ bits can be reliably transmitted over channel uses without detection. Recently, friendly jamming has been explored to enhance covertness by increasing the adversary's uncertainty. Yet, even with a friendly jammer, the detection error probability (DEP) remains a key bottleneck.

Many studies have proposed jammer-assisted strategies (e.g. probabilistic jamming) [2], but often without leveraging channel state information for power control. In this paper, we address this issue. Our contributions are summarized as follows:

- We propose a channel-aware jamming strategy that dynamically adapts jamming power based on the channel gain between the jammer and the receiver.
- We analytically derive the DEP and formulate covert throughput under covertness constraints.
- We perform extensive simulations in Rayleigh fading to compare our scheme with uniform jamming in terms of covert throughput.

* Corresponding Authors: Taehoon Kim and Inkyu Bang

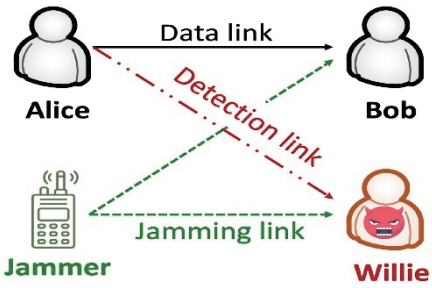

Figure 1: System model for covert communication with a friendly jammer

II. SYSTEM MODEL

We consider a covert communication network with four single-antenna nodes: a transmitter (Alice), a receiver (Bob), a friendly jammer (J), and a passive warden (Willie), as illustrated in Fig. 1. Alice aims to send data to Bob covertly, while the jammer transmits artificial noise to confuse Willie.

Prior to transmission, a pilot-based channel estimation phase is conducted. Bob broadcasts a pilot that allows Alice and the jammer to estimate their downlink channels ($\boldsymbol{h_{ab}}$ and , $\boldsymbol{h_{jb}}$). In return, Alice and the jammer transmit secret uplink pilots to Bob for estimating $\boldsymbol{h_{ba}}$ and, $\boldsymbol{h_{b,j}}$. These pilots are pre-shared and hidden from Willie, preventing him from estimating $\boldsymbol{h_{ab}}$ and, $\boldsymbol{h_{jb}}$. Willie can only estimate h_{bw} from Bob's broadcast

All channels are modeled as i.i.d. Rayleigh fading: $h(x,y) \sim CN(0,1)$ for all $(x,y) \in \{a,b,j,w\}$. We assume nodes are equidistant, and channel reciprocity holds $(e.g., ha,b = hb,a)$ since estimation occurs within a coherence interval.

The received signal at Bob under hypothesis H_0 (Alice silent) is:

$$\boldsymbol{y[t] = \sqrt{P_j} h_{j,b} X_j[t] + n_b[t]} \quad (1)$$

The received signal at Bob under hypothesis H_1 (Alice transmitting) is:

$$y[t] = \sqrt{P_a}h_{a,b}X_a[t] + \sqrt{P_j}\,h_{j,b}X_j[t] + n_b[t] \quad (2)$$

The received signal at Willie under hypothesis H_0 is:

$$z[t] = \sqrt{P_j}h_{j,w}X_j[t] + n_w[t]. \quad (3)$$

The received signal at Willie under hypothesis H_1 is:

$$z[t] = \sqrt{P_a}h_{a,w}X_a[t] + \sqrt{P_j}h_{j,w}X_j[t] + n_w[t]. \quad (4)$$

Based on the observation at Willie, he attempts to determine whether Alice transmits her covert message or remains silent. The detection error probability **(DEP)**, denoted by ζ, is defined as the sum of **False alarm** probability and **Missed detection** probability.

To ensure covert communication, we require that:

$$\zeta \geq 1 - \varepsilon \quad (5)$$

where ε is the covertness parameter.

In Rayleigh fading environments, we can derive the detection error probability at Willie analytically as shown in [5]. Under certain assumptions, the DEP can be expressed as:

$$\zeta = e^{\frac{Pa|hab|^2}{Pj}} \quad (6)$$

This leads to the following constraint relating Alice's power to the jammer's power:

$$P_a(|h_{ab}|^2) \leq \varepsilon P_j. \quad (7)$$

III. POWER ALLOCATION STRATEGIES

Based on the constraint in equation (7), we set Alice's power to $Pa = \varepsilon \cdot Pmax$, where $Pmax$ is the maximum transmit power. We propose a novel CCDF-based jammer power allocation strategy

$$P_j\left(|h_{jb}|^2\right) = P_{max} \cdot e^{-|h_{jb}|^2}. \quad (8)$$

The scheme lowers jamming power when $|h_{jb}|^2$ is high to reduce interference at Bob and increases it when $|h_{jb}|^2$ is low to better jam Willie. For comparison, we consider a uniform jammer that allocates its power according to a uniform distribution over the interval $[0, Pmax]$:

$$P_j\left(|h_{jb}|^2\right) \sim U(0, P_{max}). \quad (9)$$

While the uniform jamming approach provides randomness in power allocation, it fails to exploit channel state information.

IV. SIMULATION RESULTS

We ran Monte Carlo simulations with 10^5 channel realizations, setting $\sigma b^2 = 1$ and $Pmax = 1$. Performance was evaluated across ε values from 0.001 to 0.2. For each strategy, we computed Bob's SINR

$$SINR = \left(\frac{\varepsilon \cdot P_{max} \cdot |h_{ab}|^2}{\sigma_b{}^2 + P_j \cdot |h_{jb}|^2}\right) \quad (10)$$

where **Pmax** is the maximum transmit power. The covert throughput was then determined as the expected value of the achievable rate:

$$\eta = E[\log_2(1 + SINR)] \quad (11)$$

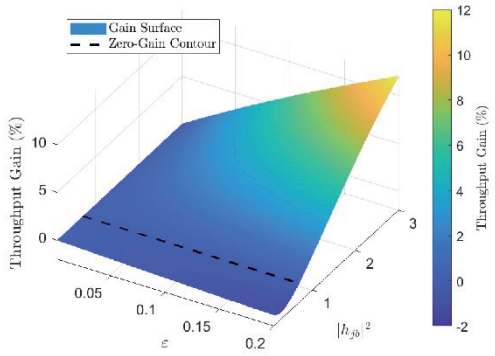

Figure 2: shows the throughput gain of CCDF over uniform jamming versus epsilon and the jammer-to-Bob channel gain. Uniform jamming performs slightly better below the dashed boundary (up to **2%**), while CCDF achieves up to **12%** gain above it. The near-linear boundary highlights CCDF's advantage in high-interference conditions with minimal loss otherwise.

V. CONCLUSION

This paper proposes a CCDF-based power allocation strategy for covert communication with friendly jamming in wireless environments. By adapting jamming power to channel conditions, the approach outperforms uniform jamming, reducing interference at the receiver while maintaining covertness. Future work will explore multi-jammer setups, and ML-based optimization.

VI. ACKNOWLEDGEMENTS

This work was partly supported by the Institute of Information & Communications Technology Planning & Evaluation (IITP) grant funded by the Korea government(MSIT) (No. RS-2024-00444170, Research and international collaboration on trust model-based intelligent incident response technologies in 6G open network environment, 50%) and IITP-ITRC(Information Technology Research Center) grant funded by the Ko rea government(MSIT)(IITP-2025-RS-2024-00437886, 50%).

REFERENCES

[1] S. Yan, X. Zhou, J. Hu, and S. V. Hanly, "Low Probability of Detection Communication: Opportunities and Challenges," IEEE Wireless Communications, vol. 26, no. 5, pp. 19-25, 2019.

[2] X. Chen, F. Gao, M. Qiu, J. Zhang, F. Shu, and S. Yan, "Achieving Covert Communication with a Probabilistic Jamming Strategy," IEEE Transactions on Information Forensics and Security, vol. 19, pp. 5561-5574, 2024.

[3] 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.