

Low-Probability-of-Detection Transmission With Power-Domain Binary Embedding

Shallom Ezekiel

Dept. Mobile Convergence Engineering
Hanbat National University
Daejeon 34158, the Republic of Korea
30261262@o365.hanbat.ac.kr

Refat Khan

Dept. Mobile Convergence Engineering
Hanbat National University
Daejeon 34158, the Republic of Korea
30245109@o365.hanbat.ac.kr

Jihwan Moon

Dept. Mobile Convergence Engineering
Hanbat National University
Daejeon 34158, the Republic of Korea
anschino@staff.hanbat.ac.kr

Abstract—This paper considers low-probability-of-detection transmission enabled by power-domain binary embedding. A source node sends a public message to a destination through conventional constellation-domain modulation while embedding a binary covert message by slightly changing its transmit power. A radiometer-type covert receiver decodes the embedded bits from received-power variations, whereas the destination attempts to detect the existence of the covert signal under noise uncertainty. For this system, we formulate the joint probability of covert transmission and successful decoding and summarize the optimization of the covert-transmission probability, power ratio, and receiver threshold. Compared with our previous work, this paper provides additional numerical results that show how the joint probability changes with the minimum detection-error probability threshold and the required public-rate threshold.

Index Terms—Covert communications, low probability of detection (LPD), physical layer security (PLS), side channel, detection error probability (DEP)

I. INTRODUCTION

Power-domain binary embedding has recently been analyzed as a side-channel method for covert communications in [1]. Its motivation follows from low-probability-of-detection (LPD) communications, where the goal is not only to protect the content of a message but also to hide the existence of the transmission itself [2]. Although conventional physical layer security focuses on preventing unauthorized decoding, it does not automatically guarantee covertness when a warden can infer the presence of a hidden message from received-signal statistics.

Covert links can be formed within the same radio-frequency protocol [3], [4] or through side channels generated by physical effects such as power, timing, electromagnetic leakage, or backscatter [5]–[7]. In particular, power-domain embedding is attractive for cross-technology or air-gapped settings because a simple radiometer or low-complexity Internet-of-Things (IoT) device can recover information from power variations without full baseband decoding. Practical experiments have demonstrated electromagnetic or power-based covert channels [8], while recent theoretical studies have examined covert

This work was supported by the IITP(Institute of Information & Communications Technology Planning & Evaluation)-ITRC(Information Technology Research Center) grant funded by the Korea government(Ministry of Science and ICT)(IITP-2026-RS-2024-00437886, 100%)

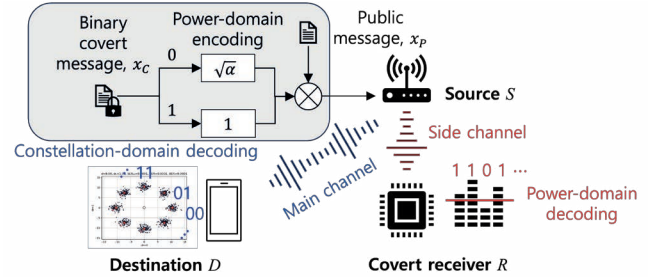


Fig. 1: System model

communications over backscatter, timing, and phase-based mechanisms [9]–[11].

In this paper, we revisit the system model of [1] and present a compact result focused on numerical insight. A source transmits a public symbol using the standard constellation-domain waveform and simultaneously embeds a covert bit by selecting one of two transmit-power levels. Under noise uncertainty [12], [13], we maximize the joint probability (JP) of covert transmission (CT) and successful decoding (SD) at the covert receiver subject to a public-rate constraint and a destination-side detection error probability (DEP) constraint. In addition to the results reported in [1], we evaluate the JP with respect to the minimum DEP threshold and the public-rate threshold, which directly quantify the covertness-reliability and public-service trade-offs.

II. SYSTEM MODEL

As shown in Fig. 1, a source S communicates with a public destination D and a covert receiver R at the same time. The public message x_p is transmitted through conventional constellation-domain modulation, whereas the covert message $x_c \in \{0, 1\}$ is embedded in the power domain. If x_c is bit 1, the source uses power P_s ; if x_c is bit 0, it uses αP_s , where $\alpha \in [0, 1]$ is the power proportion for bit 0. Thus,

$$P(x_c) = \begin{cases} \alpha P_s, & \text{if } x_c = 0, \\ P_s, & \text{if } x_c = 1. \end{cases} \quad (1)$$

A smaller α makes the covert bits more distinguishable at R , but it also creates a larger power fluctuation that may be detected by D .

The received signal at D is

$$y_D = h_{SD} \sqrt{P(x_C)} x_P + z_D, \quad (2)$$

where $x_P \sim \text{CN}(0, 1)$, h_{SD} denotes the channel from S to D , and $z_D \sim \text{CN}(0, \sigma_D^2)$. For node $X \in \{D, R\}$, the noise power is uncertain in the dB scale as

$$\sigma_{X,\text{dB}}^2 \sim \text{U}(\bar{\sigma}_{X,\text{dB}}^2 - \zeta_{X,\text{dB}}, \bar{\sigma}_{X,\text{dB}}^2 + \zeta_{X,\text{dB}}). \quad (3)$$

For a given σ_D^2 , the public achievable rate is

$$r_D = \log_2 \left(1 + \frac{|h_{SD}|^2 P(x_C)}{\sigma_D^2} \right). \quad (4)$$

At the covert receiver, the signal is

$$y_R = h_{SR} \sqrt{P(x_C)} x_P + z_R, \quad (5)$$

and the received power conditioned on x_C is $\mathbb{E}[|y_R|^2 | x_C] = |h_{SR}|^2 P(x_C) + \sigma_R^2$. The covert receiver decides the embedded bit by comparing the measured power with a threshold τ_R . With $q = \Pr(x_C = 1) = 1/2$, the bit error probability (BEP) is

$$\Pr(e_R) = (1 - q) \Pr(|h_{SR}|^2 \alpha P_S + \sigma_R^2 \geq \tau_R) + q \Pr(|h_{SR}|^2 P_S + \sigma_R^2 < \tau_R). \quad (6)$$

The destination is also modeled as a passive radiometer that tests whether the covert embedding exists. Using the long-term received power $T = \lim_{N \rightarrow \infty} (1/N) \sum_{n=1}^N |y_D[n]|^2$, the null and alternative hypotheses are

$$\begin{aligned} H_0 : T &= |h_{SD}|^2 P_S + \sigma_D^2, \\ H_1 : T &= \frac{1 + \alpha}{2} |h_{SD}|^2 P_S + \sigma_D^2. \end{aligned} \quad (7)$$

The destination declares that the covert message is present if $T < \tau_D$ and absent otherwise. Therefore, with p denoting the CT probability, the DEP is

$$\Pr(e_D) = (1 - p) \Pr(T < \tau_D | H_0) + p \Pr(T \geq \tau_D | H_1), \quad (8)$$

where the first and second terms are the false-alarm and miss-detection events, respectively.

III. PROBLEM FORMULATION

The performance metric is the JP of CT and SD, defined as $p(1 - \Pr(e_R))$. This metric increases when the source transmits covertly more often and when R decodes the embedded bits more reliably. The design variables are the CT probability p , the power proportion α , and the classification threshold τ_R . The optimization problem is written as

$$(P1): \max_{p, \alpha, \tau_R} p(1 - \Pr(e_R)), \quad (9a)$$

$$\text{s.t.} \min_{x_C} r_D |_{\sigma_D^2 = \zeta_D \bar{\sigma}_D^2} \geq \bar{r}_D, \forall \zeta_D \in \mathcal{Z}_D, \quad (9b)$$

$$\min_{\tau_D} \Pr(e_D) \geq \varepsilon_D, \forall \zeta_D \in \mathcal{Z}_D, \quad (9c)$$

$$p \in [0, 1], \alpha \in [\bar{\alpha}, 1]. \quad (9d)$$

Here, $\bar{r}_D$ is the public-rate requirement and $\varepsilon_D \in [0, 0.5]$ is the minimum DEP threshold. Constraint (9b) protects the

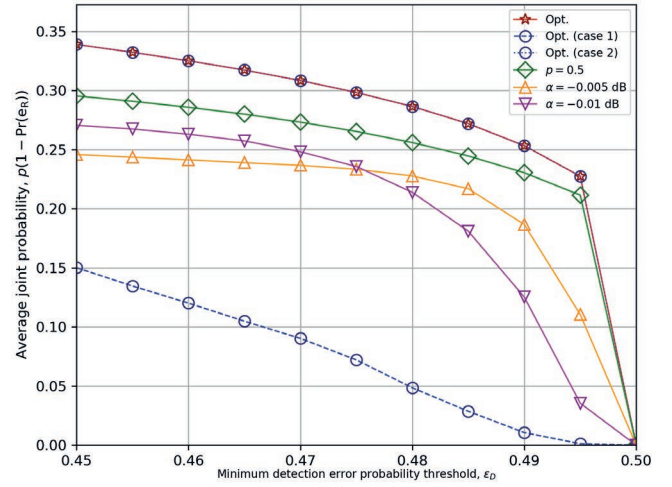


Fig. 2: The JP versus the minimum DEP threshold for $d_{SR} = d_{SD} = 20$ m

public link even when bit 0 is transmitted and the destination noise takes an unfavorable value from $\mathcal{Z}_D$. Constraint (9c) guarantees covertness by forcing the minimum DEP at the destination to remain above ε_D . The lower bound $\bar{\alpha}$ prevents excessive public-rate fluctuation and limits the power-domain signature of the covert message.

Our previous work in [1] derived the BEP and DEP expressions under noise uncertainty and solved (P1) by separating the zero-BEP and non-zero-BEP regimes. In the zero-BEP regime, the source chooses α so that the two received-power intervals at R do not overlap. In the non-zero-BEP regime, a controlled amount of decoding error is allowed to improve the JP. Closed-form expressions and a global solution procedure are provided in [1], and this paper utilizes those solutions and focuses on the new numerical trends below.

IV. NUMERICAL RESULTS

We evaluate the average JP of power-domain binary embedding. The channel is modeled as $h_{XY} = \sqrt{L_{XY}} \hat{h}_{XY}$, where $\hat{h}_{XY} \sim \text{CN}(0, 1)$ and $L_{XY} = L_0(d_{XY}/d_0)^{-\beta}$ with reference distance $d_0 = 1$ m. Unless otherwise stated, the parameters follow [1]: $W = 20$ MHz, $P_S = 23$ dBm, $\bar{r}_P = 1.5$ bps/Hz, $\bar{\alpha} = 0.95$, $\bar{\sigma}_R^2 = \bar{\sigma}_D^2 = -160$ dBm/Hz, $\zeta_R = 5$ dB, $\zeta_D \in \mathcal{Z}_D = \{4.0, 4.5, 5.0, 5.5, 6.0\}$, $\varepsilon_D = 0.45$, and $\beta = 3.5$. The curve labeled “Opt.” takes the better result between Case 1 with zero BEP and Case 2 with non-zero BEP, and it is compared with fixed- p and fixed- α baselines.

Fig. 2 shows the average JP versus the minimum DEP threshold ε_D for $d_{SR} = d_{SD} = 40$ m. As ε_D increases toward 0.5, the destination must be forced closer to a random-guess detector, and the feasible set of (p, α) becomes increasingly narrow. Therefore, all curves decrease and eventually approach zero near the most stringent covertness requirement. The optimized curve almost coincides with Case 2, which indicates that allowing a non-zero BEP at the covert receiver can be beneficial when the covertness constraint is tight.

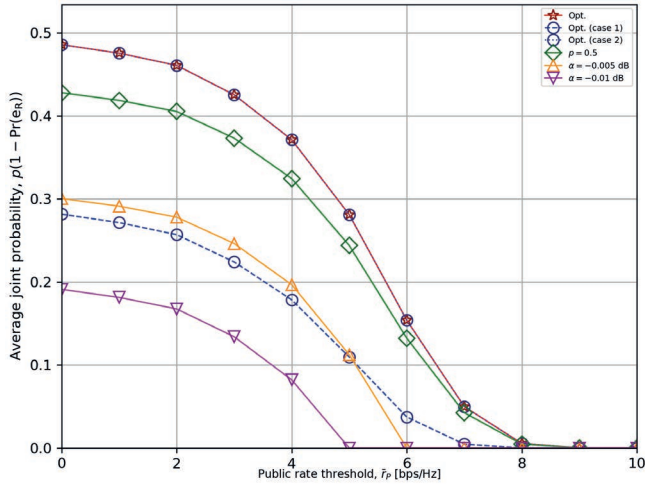


Fig. 3: The JP versus the public rate threshold for $d_{SR} = d_{SD} = 20$ m

Case 1 suffers because enforcing zero BEP requires enough power separation at R , but this same separation makes the embedding easier for D to detect. The fixed- $p = 0.5$ baseline is consistently below the optimum, highlighting the importance of adapting the CT probability. For fixed- α schemes, the larger power separation associated with $\alpha = -0.01$ dB improves reliability at moderate ε_D , but it loses feasibility earlier than $\alpha = -0.005$ dB as the covertness requirement becomes stricter.

Fig. 3 plots the average JP as the public-rate threshold $\bar{r}_P$ increases for $d_{SR} = d_{SD} = 20$ m. A larger $\bar{r}_P$ leaves less margin for transmitting bit 0 with reduced power, so the optimizer must choose α closer to one or reduce the CT probability. Both actions lower the JP: a high α reduces the received-power separation at R , while a low p directly reduces the covert transmission opportunity. The sharp drop in the medium-rate region shows the transition from a covertness-limited regime to a public-rate-limited regime. The optimized scheme remains the upper envelope of Case 1 and Case 2, and Case 2 again dominates over most of the range because a small BEP penalty is preferable to the restrictive zero-BEP condition. Fixed- α baselines lose feasibility earlier, especially for $\alpha = -0.01$ dB, since the larger power reduction for bit 0 violates the public-rate requirement at smaller $\bar{r}_P$.

V. CONCLUSION

This paper presented a compact result of LPD transmission with power-domain binary embedding. A public constellation-domain message and a binary covert message are transmitted simultaneously by mapping the covert bit to two closely spaced power levels. Under noise uncertainty, the JP of CT and SD was optimized subject to public-rate and DEP constraints. The new numerical results show that stricter covertness and higher public-rate requirements both reduce the achievable JP, but for different reasons: the former limits the detectable power separation and CT probability, while the latter forces the bit-0

power level closer to the bit-1 level. The results also show that the non-zero-BEP regime often gives the best JP because it balances covert reliability against LPD feasibility. Future work may extend this framework to more advanced detectors, imperfect channel knowledge at a passive covert receiver, and adaptive transmit-power control.

REFERENCES

- [1] J. Moon, S. Hwang, J. Park, I. Bang, T. Kim, and Z. Fu, "Achievable Performance of Covert Communications via Power-Domain Binary Embedding," *IEEE Wireless Commun. Lett.*, vol. 15, pp. 2644–2648, 2026.
- [2] X. Chen, J. An, Z. Xiong, C. Xing, N. Zhao, F. R. Yu, and A. Nallanathan, "Covert Communications: A Comprehensive Survey," *IEEE Commun. Surveys Tuts.*, vol. 25, no. 2, pp. 1173–1198, Secondquarter 2023.
- [3] X. Qin, Z. Na, Z. Wen, and X. Wu, "Relaying IRS-UAV Assisted Covert Communications in Uplink C-NOMA Network," *IEEE Commun. Lett.*, vol. 28, no. 9, pp. 2136–2140, September 2024.
- [4] Y. Lei, G. Huang, X. Li, Z. Tian, S. Mumtaz, and M. Asif, "STAR-RIS-NOMA Assisted Power Constrained Covert Communication Systems," *IEEE Trans. Veh. Technol.*, vol. 74, no. 7, pp. 11120–11131, July 2025.
- [5] R. Spolaor, Y. Xu, V. Moonsamy, M. Conti, and X. Cheng, "Covert-Power: A Covert Channel on Android Devices Through USB Power Line," *IEEE Trans. Dependable Secure Comput.*, vol. 22, no. 5, pp. 4911–4926, September–October 2025.
- [6] S. Son, D. Kwon, S. Lee, Y. Jeon, and Y. Park, "A Robust Covert Channel With Self-Bit Recovery for IEEE 802.11 Networks," *IEEE Internet Things J.*, vol. 11, no. 16, pp. 27356–27368, August 2024.
- [7] S. Li, S. Li, Q. Liu, Y. Song, C. Zhang, and L. Lu, "Watch Out Your Thumb Drive: Covert Data Theft From Portable Data Storage via Backscatter," *IEEE Trans. Dependable Secure Comput.*, vol. 21, no. 4, pp. 2434–2447, July–August 2024.
- [8] M. Guri, "Air-Gap Electromagnetic Covert Channel," *IEEE Trans. Dependable Secure Comput.*, vol. 21, no. 4, pp. 2127–2144, July–August 2024.
- [9] J. Liu, J. Yu, X. Chen, R. Zhang, S. Wang, and J. An, "Covert Communication in Ambient Backscatter Systems With Uncontrollable RF Source," *IEEE Trans. Commun.*, vol. 70, no. 3, pp. 1971–1983, March 2022.
- [10] Y. Ma, R. Ma, W. Yang, C. Miao, Y. Cai, and W. Wu, "Covert Communication Using Time Modulated Retrodirective Array," *IEEE Wireless Commun. Lett.*, vol. 13, no. 2, pp. 510–514, February 2024.
- [11] X. Ji, R. Zhu, Q. Zhang, C. Li, and D. Cao, "Enhancing Covert Communication in OOK Schemes by Phase Deflection," *IEEE Trans. Inf. Forensics Security*, vol. 19, pp. 9775–9788, 2024.
- [12] B. He, S. Yan, X. Zhou, and V. K. N. Lau, "On Covert Communication With Noise Uncertainty," *IEEE Commun. Lett.*, vol. 21, no. 4, pp. 941–944, April 2017.
- [13] J. Si, Z. Li, Y. Zhao, J. Cheng, L. Guan, J. Shi, and N. Al-Dhahir, "Covert Transmission Assisted by Intelligent Reflecting Surface," *IEEE Trans. Commun.*, vol. 69, no. 8, pp. 5394–5408, August 2021.