Performance Analysis of Channel-Coding-Based Covert Channels in Physical-Layer Wireless Communications

Haijun Tan[1] and Ning Xie[2, 3]
[1]Control and Network Foundation Laboratory, Department of Strategic and Advanced Interdisciplinary Research, Peng Cheng Laboratory, Shenzhen 518107, China.
[2]School of Intelligent Science and Engineering, Qinghai Minzu University, Xining 810007, Qinghai, China
[3]State Key Laboratory of Radio Frequency Heterogeneous Integration and the Guangdong Key Laboratory of Intelligent Information Processing, College of Electronics and Information Engineering, Shenzhen University, Shenzhen 518060, China

Channel-coding-based covert channels in physical-layer wireless communications enable hidden transmission by embedding covert bits into coded cover signals after channel coding. While existing studies mainly focus on covert-channel construction, the corresponding performance limits remain insufficiently characterized. This paper analyzes such covert channels from the two complementary viewpoints of robustness and security. For robustness, a BER-based effective covert-rate metric is adopted and specialized to the considered channel-coding-based covert embedding framework, and the effects of the hidden payload per cover-code codeword, the error-correction capabilities of the cover and hidden codes, the modulation order, the fading severity, and the coding structure are characterized. For security, two passive statistical attack scenarios, based on corrected-error distributions across codeword positions and embedding-induced Bit Error Rate (BER) variation, are analyzed, and the corresponding security capacities are derived. The results show that the achievable covert capacity is nonincreasing with the number of hidden coded bits embedded in each cover-code codeword and enlarges with the error-correction capability of the cover code. They further show that codeword-wide uniform random embedding minimizes the systematic positional footprint under the corrected-error-statistics attack scenario, and that positive overall security capacity is achievable only when the statistical constraints of both attack scenarios are simultaneously satisfied. Numerical results validate the analysis and demonstrate that block-coded systems are markedly more suitable than convolutional-coded systems under the considered bit-flip embedding rule, and that viable covert transmission can arise in both low- and high-SNR regimes.

***Index Terms*—Covert channel, channel coding, performance analysis, robustness, security.**

I. Introduction

Steganography aims to conceal the existence of communication, whereas cryptography protects the content of the transmitted message [1]. Most existing covert channels are constructed over upper-layer carriers, such as images, audio, and video. By contrast, covert communication at the physical layer of wireless communications has received much less attention. This carrier domain is nevertheless of practical interest because the hidden information is embedded directly into transmitted coded symbols or waveforms, so many steganalytic tools developed for upper-layer carriers are no longer directly applicable.

Interest in covert communication in wireless networks has grown in recent years, driven by the increasing complexity of wireless protocol stacks and by the emergence of new physical-layer hiding opportunities [2], [3]. Existing physical-layer covert schemes can be broadly classified according to the resource used to carry the hidden message. One class embeds hidden information into fixed or semi-fixed protocol structures, such as padding bits [4] and cyclic prefixes [5]. These methods are easy to implement, but the modified fields are often highly structured in legitimate transmissions, so even small perturbations may leave detectable traces. A second class embeds hidden bits during the modulation-mapping stage [6], [7]. These approaches avoid explicit protocol-field manipulation, but they may distort the induced symbol statistics. A third class embeds the hidden message after channel coding, thereby exploiting both coding redundancy and naturally occurring channel impairments. This channel-coding-based design is attractive because the overt channel and the covert channel can coexist within the same transmission [8].

The channel-coding-based covert channel considered in this paper should also be distinguished from two related physical-layer paradigms. The first is physical-layer security [9], whose objective is to protect message content by exploiting an advantage in channel quality at the legitimate receiver. Such methods protect confidentiality, but they do not conceal the existence of the transmission itself. The second is low-probability-of-detection communication [10], [11], which hides transmissions below the noise floor and therefore departs from the normal communication setting. By contrast, the channel-coding-based covert channel studied here preserves a normal overt transmission while embedding a hidden message into the coded overt signal.

Existing studies have mainly addressed covert-channel construction, signal-level detection, or protocol-level vulnerability analysis. For example, physical-layer information hiding can be detected through signal inconsistency and decodability degradation after reencoding and remodulation [12]. Recent studies have also examined the susceptibility of modern wireless protocols, such as Fifth-Generation New Radio, to

Manuscript received April 30, 2026; revised August 18, 2026. Corresponding author: Ning Xie (email: ningxie89@gmail.com).

steganographic channels and have developed protocol design rules to reduce such vulnerabilities [13], [14]. However, these studies do not directly characterize the performance limits of channel-coding-based covert embedding from the joint viewpoints of overt reliability, hidden-message recoverability, and statistical undetectability. As a result, the feasibility conditions and achievable covert rate of post-coding covert transmission remain insufficiently characterized.

Motivated by this gap, this paper develops a performance-analysis framework for channel-coding-based covert channels in physical-layer wireless communications. The analysis is carried out from the two complementary viewpoints of robustness and security. Here, robustness means that covert embedding does not degrade the overt channel and that the hidden message remains decodable at the intended receiver, whereas security means that the embedding operation does not introduce statistical traces that allow a passive adversary to infer the presence of covert communication. These two requirements jointly determine the effective covert rate that can be supported by the system.

The main contributions of this paper are summarized as follows.

- We derive a robustness analysis for channel-coding-based covert transmission and prove two basic monotonicity properties: the achievable covert capacity is nonincreasing with the number of hidden coded bits embedded in each cover-code codeword, and the robustness-feasible region enlarges with the error-correction capability of the cover code.
- We derive a security analysis under two statistical attack scenarios. For the corrected-error-statistics scenario, we prove that codeword-wide uniform random embedding minimizes the systematic positional footprint. For the joint-security case, we prove that positive overall security capacity is achievable only when the constraints of both attack scenarios are simultaneously satisfied.
- We analyze numerically the effects of the hidden-code parameters, modulation order, fading severity, and coding structure, and connect the observed trends directly to the analytical results. The results show in particular that block-coded systems are markedly more suitable than convolutional-coded systems under the considered bit-flip embedding rule, and that viable covert transmission can arise in both low- and high-SNR regimes.

The remainder of this paper is organized as follows. Section II introduces the system model and the performance metrics. Section III presents the robustness analysis. Section IV develops the security analysis under the two statistical attack scenarios. Section V provides simulation results and validates the analytical findings. Section VI concludes the paper.

II. System Model

A. Signal Model and Channel Setup

We consider a typical channel-coding-based covert-channel framework shown in Fig. 1. The overt channel carries the normal cover message, whereas the covert channel secretly conveys the hidden message. Alice and Bob communicate over the overt channel while simultaneously exchanging hidden information through the covert channel. Eve is a passive adversary who observes the transmitted stego signal and attempts to determine whether covert communication is present.

At Alice, the cover message s_{cover} is first encoded by a channel encoder to produce the coded cover sequence u_{cover}. The hidden message s_{hide} is also channel encoded and then embedded into u_{cover} by an embedding module controlled by a shared stego key, yielding the stego sequence u_{stego}. For block-coded cover transmission, let l_h denote the number of coded hidden bits embedded into one cover-code codeword. Thus, $l_h = 0$ corresponds to overt-only transmission, whereas a larger l_h implies a larger covert payload carried by each cover-code codeword. Both Alice and Bob possess identical pseudo-random number generators seeded by the shared stego key, which determines the coded positions used for embedding. The embedding rule considered in this paper is a bit-flip operation: a hidden bit is embedded by flipping the selected coded cover bit if and only if the two bits differ. The resulting stego sequence is modulated to produce the transmitted waveform x_{stego}.

The wireless links from Alice to Bob and from Alice to Eve are modeled as independent Nakagami-m fading channels. The Nakagami-m model is adopted because its shape parameter m can represent a wide range of fading conditions: smaller values of m correspond to more severe fading, the special case $m = 1$ yields Rayleigh fading, and the limit $m \to +\infty$ recovers the Additive White Gaussian Noise (AWGN) channel [15]. The received signals at Bob and Eve are

$$y_{\mathrm{stego}}^{(b)} = h_m^{(b)} x_{\mathrm{stego}} + z^{(b)}, \tag{1}$$

$$y_{\mathrm{stego}}^{(e)} = h_m^{(e)} x_{\mathrm{stego}} + z^{(e)}, \tag{2}$$

where $h_m^{(b)}$ and $h_m^{(e)}$ are the complex fading coefficients, and $z^{(b)} \sim \mathcal{CN}(0, \sigma_b^2)$ and $z^{(e)} \sim \mathcal{CN}(0, \sigma_e^2)$ are independent complex Gaussian noise samples.

Bob demodulates the received signal, applies the extraction module with the shared stego key to recover the hidden message $\hat{s}_{\mathrm{hide}}$, and decodes the cover message $\hat{s}_{\mathrm{cover}}$. Eve, being unaware of the stego key, knows only the parameters of the overt channel, including the channel code and the modulation format, and performs statistical inference on her received signal to detect whether a covert channel has been established. To further protect the hidden message, encryption can be applied before embedding. For clarity, the encryption module is omitted in the following analysis.

Two coding structures are considered in the analysis. For block coding, the cover code is denoted by $C_b(n_c, k_c)$, where n_c and k_c are the coded length and information length of one cover-code codeword, and t_c denotes the corresponding error-correction capability. The hidden message may also be encoded by a block code, denoted by $C_b(n_h, k_h)$, where n_h and k_h are the coded length and information length of one hidden-code codeword, and t_h denotes its error-correction capability. For convolutional coding, the encoder is denoted by $C_c(n, k, K)$, where K is the encoder memory length. These definitions will be used repeatedly in Sections III and IV.

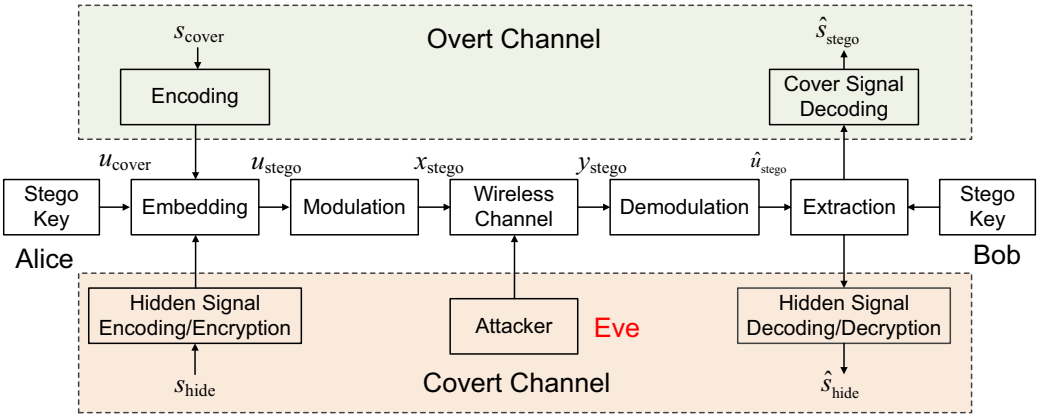

Fig. 1. Overview of the considered coded covert-channel framework, where the overt channel and the covert channel coexist within a physical-layer wireless communication system.

B. Performance Metrics

Following [8], [16], we adopt the following BER-based effective covert-rate metric for the considered channel-coding-based covert embedding framework:

$$C_{\text{hide}} = \frac{Lk_h(1-2p_{\text{hide}})^2}{2n_h \ln 2}, \tag{3}$$

where p_{hide} is the BER of the covert channel after hidden-message decoding at Bob, $L = \log_2 M$ is the number of bits carried by one M-ary modulation symbol, and k_h/n_h is the code rate of the hidden-message encoder. The BERs of the overt channel are denoted separately by p_{normal} and p_{stego}, where p_{normal} is the post-decoding BER without embedding and p_{stego} is the post-decoding BER in the presence of embedding. These two BER quantities are used in the robustness and security constraints to characterize the reliability degradation and detectability caused by covert embedding, whereas p_{hide} determines the effective rate of the hidden channel in (3).

In this paper, the capacity terminology is used as an operational performance metric for channel-coding-based covert embedding. Following [8], [16], (3) is adopted as a BER-based covert-rate metric for a hidden message carried by an existing overt link. This metric reflects the hidden-channel BER, the hidden-code rate, and the modulation order. It is therefore different from the information-theoretic covert capacity in low-probability-of-detection communications, where the capacity is defined under asymptotic reliability and detection constraints and yields the square-root-law throughput over n channel uses [10], [11]. Accordingly, the terms covert capacity, robustness capacity, and security capacity in this paper refer to the BER-based metric in (3) under the corresponding robustness and security constraints, rather than to the square-root-law covert throughput.

III. Robustness Analysis

This section analyzes the coded covert channel from the viewpoint of robustness. Unless otherwise specified, we focus on the bit-flip embedding rule introduced in Section II and on the post-decoding BER observed at Bob. The objective is to characterize when covert embedding can be supported without degrading the overt transmission after decoding. Under this requirement, the hidden transmission is evaluated through the effective covert-rate metric in (3). The corresponding robustness capacity is defined as

$$C_{\text{hide}}^{\text{R}} = \begin{cases} C_{\text{hide}}, & \text{if } p_{\text{stego}} = p_{\text{normal}}, \\ 0, & \text{otherwise.} \end{cases} \tag{4}$$

Note that (4) is an analytical reliability criterion, which requires that covert embedding should not increase the post-decoding BER of the overt channel. We first examine how the number of embedded hidden coded bits l_h and the cover-code error-correction capability t_c affect the robustness-feasible operating region.

Proposition 1. *Consider block-coded cover transmission with error-correction capability t_c. For fixed channel conditions, fixed modulation order, and fixed cover and hidden channel codes, the robustness capacity $C_{\text{hide}}^{\text{R}}$ is a nonincreasing function of the number of embedded hidden coded bits l_h.*

Proof. Let N_{ch} denote the number of channel-induced errors in one received cover-code codeword before decoding, and define

$$P_{\text{ch}}(e) = \Pr\{N_{\text{ch}} = e\}, \qquad e = 0, 1, \ldots, n_c. \tag{5}$$

Under the considered replacement rule, an embedding-induced flip occurs at a selected position if and only if the corresponding coded hidden bit differs from the selected coded cover bit. The binomial model is obtained under the standard statistical assumption that, over the selected embedding positions, the coded hidden bits and the selected coded cover bits are mutually independent and approximately equiprobable. This assumption is consistent with uniformly distributed cover messages, pseudo-random embedding positions, and a scrambled or encrypted hidden bit stream. Accordingly, the mismatch indicator at each selected position can be modeled as an independent Bernoulli random variable with parameter $1/2$, and the number of embedding-induced flips in one cover-code codeword follows

$$N_{\text{em}}(l_h) \sim \text{Binomial}(l_h, 1/2). \tag{6}$$

For a given l_h, the cover decoder may fail when the residual number of coded-bit errors exceeds the correction capability t_c. For binary coded bits, a channel-induced flip and an embedding-induced flip occurring at the same coded position may cancel each other because two consecutive flips restore the original bit. Therefore, the direct sum $N_{\mathrm{ch}} + N_{\mathrm{em}}(l_h)$ is used as a conservative no-cancellation error count, which upper-bounds the actual residual error count. Under this conservative model, the decoder-overload probability is upper-bounded as

$$\begin{aligned} P_{\mathrm{ov}}(l_h, t_c) &\le \Pr\{N_{\mathrm{ch}} + N_{\mathrm{em}}(l_h) > t_c\} \\ &= \sum_{e=0}^{n_c} P_{\mathrm{ch}}(e) \Pr\{N_{\mathrm{em}}(l_h) > t_c - e\} \\ &= \sum_{e=0}^{n_c} P_{\mathrm{ch}}(e) \sum_{j=(t_c-e+1)^+}^{l_h} \binom{l_h}{j} 2^{-l_h}, \end{aligned} \tag{7}$$

where $(x)^+ = \max\{x, 0\}$. Thus, (7) should be interpreted as a conservative upper bound rather than a no-overlap assumption. The actual bit-level simulations apply the channel errors and embedding operations directly to the coded bits, and therefore naturally include possible cancellations at the same coded position.

To study the dependence on l_h, for each fixed e we define

$$\Psi_e(l_h) = \Pr\{\mathrm{Binomial}(l_h, 1/2) > t_c - e\}. \tag{8}$$

Next, from the binomial recursion

$$\mathrm{Binomial}(l_h + 1, 1/2) = \mathrm{Binomial}(l_h, 1/2) + B, \tag{9}$$

where $B \sim \mathrm{Bernoulli}(1/2)$ is independent of $\mathrm{Binomial}(l_h, 1/2)$, we get

$$\begin{aligned} \Psi_e(l_h + 1) &= \Pr\{\mathrm{Binomial}(l_h, 1/2) + B > t_c - e\} \\ &= \frac{1}{2} \Pr\{\mathrm{Binomial}(l_h, 1/2) > t_c - e\} \\ &\quad + \frac{1}{2} \Pr\{\mathrm{Binomial}(l_h, 1/2) > t_c - e - 1\} \\ &\ge \Psi_e(l_h). \end{aligned} \tag{10}$$

Hence, for every fixed e, the tail probability in (8) is nondecreasing with l_h. Substituting (10) into the right-hand side of (7), we find that the conservative decoder-overload bound induced by the no-cancellation error count is nondecreasing with l_h. In other words, under the adopted conservative analytical model, increasing the number of embedded coded hidden bits cannot reduce the upper bound on the probability that the residual error count exceeds the cover-code correction capability. Since a larger conservative decoder-overload bound cannot improve the post-decoding reliability of the overt channel, increasing l_h cannot enlarge the robustness-feasible region under the adopted analytical model. Therefore, from the robustness-capacity definition in (4), $C_{\mathrm{hide}}^{\mathrm{R}}$ is nonincreasing with l_h. This completes the proof.

Remark 1. *The binomial model in* (6) *is appropriate when the selected cover coded bits and hidden coded bits are approximately independent and equiprobable, which can be supported by pseudo-random embedding positions and a scrambled or encrypted hidden stream. If the mismatch probability is biased or position dependent, the parameter* $1/2$ *can be replaced by the corresponding mismatch probabilities. If the mismatch indicators are correlated, the exact overload probability becomes system dependent and should be calibrated under the actual code, interleaver, channel, and receiver.*

Corollary 1. *For any fixed SNR, modulation format, and cover/hidden code pair, there exists an integer threshold* $l_h^\star \ge 0$ *such that* $C_{\mathrm{hide}}^{\mathrm{R}} = 0$ *for all* $l_h > l_h^\star$.

Proof. Only a finite number of coded positions can be modified in one cover-code codeword. Therefore, the admissible values of l_h form a finite ordered set. From Proposition 1, we know that $C_{\mathrm{hide}}^{\mathrm{R}}$ is nonincreasing in l_h. It then follows that there exists a largest feasible payload, denoted by $l_h^\star$, such that the robustness condition $p_{\mathrm{stego}} = p_{\mathrm{normal}}$ still holds. For any $l_h > l_h^\star$, this equality is violated. From (4), we get $C_{\mathrm{hide}}^{\mathrm{R}} = 0$ for all $l_h > l_h^\star$. This completes the proof.

Proposition 2. *For fixed channel conditions, fixed modulation order, and fixed embedding payload* l_h*, increasing the error-correction capability* t_c *of the cover code enlarges the robustness-feasible region.*

Proof. For fixed l_h, the conservative decoder-overload bound can be written as

$$P_{\mathrm{ov}}(l_h, t_c) = \sum_{e=0}^{n_c} P_{\mathrm{ch}}(e) \Pr\{N_{\mathrm{em}}(l_h) > t_c - e\}. \tag{11}$$

Now consider two cover codes with correction capabilities $t_c^{(1)}$ and $t_c^{(2)}$, where $t_c^{(2)} \ge t_c^{(1)}$. For each fixed e, the tail probability $\Pr\{N_{\mathrm{em}}(l_h) > t_c - e\}$ is nonincreasing in t_c, because increasing the correction capability raises the allowable error threshold before decoder failure occurs. Therefore, for every e, we have

$$\Pr\{N_{\mathrm{em}}(l_h) > t_c^{(2)} - e\} \le \Pr\{N_{\mathrm{em}}(l_h) > t_c^{(1)} - e\}. \tag{12}$$

Multiplying both sides of (12) by the nonnegative weight $P_{\mathrm{ch}}(e)$ and then summing over $e = 0, 1, \ldots, n_c$, we get

$$P_{\mathrm{ov}}(l_h, t_c^{(2)}) \le P_{\mathrm{ov}}(l_h, t_c^{(1)}). \tag{13}$$

Hence increasing t_c cannot increase the conservative decoder-overload bound. As a consequence, the post-decoding BER of the overt channel under the stronger cover code cannot exceed that under the weaker cover code. Therefore, every operating point satisfying $p_{\mathrm{stego}} = p_{\mathrm{normal}}$ under $t_c^{(1)}$ also satisfies it under $t_c^{(2)}$. From (4), we conclude that the robustness-feasible region enlarges with t_c. This completes the proof.

The preceding propositions characterize the roles of the embedding payload and the cover-code correction capability. The effects of the remaining parameters are less amenable to a clean monotonic statement under the adopted metric, but their roles can still be understood from (3) together with

the structure of the coded covert channel. When the embedding payload is fixed, increasing the hidden-code correction capability t_h reduces p_{hide} but also lowers the hidden-code rate k_h/n_h. Therefore, its net effect on $C^{\text{R}}_{\text{hide}}$ depends on the balance between improved hidden-message reliability and reduced coding efficiency. The modulation order M also has a regime-dependent effect. In the high-SNR regime, increasing M is beneficial because the spectral-efficiency gain dominates. In the low-SNR regime, increasing M is harmful because the reduced Euclidean distance between constellation points increases the channel error rate. Similarly, increasing the Nakagami parameter m improves the covert capacity because the channel becomes less severe. Finally, under the considered bit-flip embedding rule, block coding is structurally more suitable than convolutional coding because a flipped coded bit affects only its own codeword in block coding, whereas in convolutional coding the encoder memory spreads the perturbation across multiple trellis relations. These trends are further examined numerically in Section V.

IV. Security Analysis Under Two Statistical Attack Scenarios

This section analyzes the coded covert channel from the viewpoint of security. Unless otherwise specified, Eve is assumed to be a passive adversary who knows the overt-channel parameters but not the stego key. The analysis focuses on whether post-coding embedding leaves statistical traces that reveal the presence of covert communication. To this end, we consider two attack scenarios. In Scenario 1, Eve exploits the corrected-error statistics across coded positions. In Scenario 2, Eve estimates the BER variation induced by embedding. We first introduce the security metrics associated with these two scenarios and then derive the overall security capacity under the joint attack model.

More generally, Eve's security test can be written as a binary hypothesis test

$$\begin{aligned} &\mathcal{H}_0: \text{ normal overt transmission,} \\ &\mathcal{H}_1: \text{ post-coding covert embedding.} \end{aligned} \tag{14}$$

Let $\mathbf{Z}$ denote the set of statistics available to Eve from the received codeword blocks. Depending on Eve's capability, $\mathbf{Z}$ may include corrected-error profiles, BER variation, syndrome patterns, decoder-failure events, HD statistics, and soft demodulation information. A general detector compares a scalar test statistic $T(\mathbf{Z})$ with a threshold η, namely

$$T(\mathbf{Z}) \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \eta. \tag{15}$$

If the distributions of $\mathbf{Z}$ under $\mathcal{H}_0$ and $\mathcal{H}_1$ are known, the Neyman–Pearson detector is the likelihood-ratio test

$$T_{\text{LRT}}(\mathbf{Z}) = \frac{p(\mathbf{Z}|\mathcal{H}_1)}{p(\mathbf{Z}|\mathcal{H}_0)} \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \eta. \tag{16}$$

When some parameters are unknown, the corresponding generalized likelihood-ratio test can be obtained by replacing the unknown parameters with their maximum-likelihood estimates. These hypothesis-testing based detectors are more general than the two scalar tests analyzed below, because they may jointly exploit several code-domain and receiver-domain statistics.

The two attack scenarios considered in this paper can be interpreted as tractable special cases of (15). In Scenario 1, the test statistic is the corrected-error positional-footprint statistic, i.e., $T(\mathbf{Z}) = \lambda$, and Eve declares a detectable embedding footprint if $\lambda > \varepsilon_1$. In Scenario 2, the test statistic is the normalized BER variation, i.e., $T(\mathbf{Z}) = \delta$, and Eve declares a detectable BER footprint if $\delta > \varepsilon_2$. Thus, the joint detector induced by the two considered statistics is

$$\lambda > \varepsilon_1 \quad \text{or} \quad \delta > \varepsilon_2. \tag{17}$$

Equivalently, the security-feasible event is $\lambda \le \varepsilon_1$ and $\delta \le \varepsilon_2$, which is the condition used later in **Proposition 5**. Hence, the security capacities derived below should be understood as performance measures under two code-aware necessary tests. If either condition in (17) holds, the covert embedding is already detectable by a simple passive hypothesis test and cannot be expected to remain secure against stronger detectors based on richer observations.

A. Security Scenario 1: Corrected-Error Statistics

Let $N_{\text{stego}}(i)$ and $N_{\text{normal}}(i)$ denote the average numbers of corrected errors at coded position i per codeword block with and without embedding, respectively. Define the expected positional increment

$$\Delta_i = \mathbb{E}\{N_{\text{stego}}(i) - N_{\text{normal}}(i)\}, \qquad i \in \{1, 2, \ldots, n_c\}, \tag{18}$$

and the corresponding positional-footprint variance

$$\lambda_\Delta = \frac{1}{n_c}\sum_{i=1}^{n_c}(\Delta_i - \bar{\Delta})^2, \qquad \bar{\Delta} = \frac{1}{n_c}\sum_{i=1}^{n_c}\Delta_i. \tag{19}$$

The quantity λ_Δ captures the systematic position-dependent component of the corrected-error-statistics attack.

Let q_i denote the probability that coded position i is selected for embedding when one embedding opportunity is used in a codeword block, so that $q_i \ge 0$ and $\sum_{i=1}^{n_c} q_i = 1$. Under the considered bit-flip embedding rule, a selected coded position is actually flipped with probability $1/2$. Let β denote the average increase in Eve's corrected-error statistic caused by one actual embedding-induced flip at a selected coded position, after averaging over the channel, demodulation, and decoding operations. Thus, β measures the per-flip contribution of embedding to the corrected-error profile. When the coded positions are statistically equivalent, this contribution does not depend on the position index i. This position-independent approximation is valid for symmetric channels and modulation/demodulation models with approximately uniform bit-error behavior across coded positions, or when interleaving/randomization removes persistent position-dependent reliability differences. Hence, there exists a constant $\beta > 0$, independent of i, such that

$$\Delta_i = \frac{\beta}{2} q_i. \tag{20}$$

Remark 2. *The position-independent coefficient β in* (20) *is an averaged model for statistically equivalent coded positions. In practical systems with persistent position-dependent*

reliability differences, such as insufficient interleaving over frequency-selective channels or unequal protection between different coded-bit classes, β can be replaced by a position-dependent coefficient β_i, leading to

$$\Delta_i = \frac{\beta_i}{2} q_i, \qquad i = 1, 2, \ldots, n_c. \tag{21}$$

*In this generalized model, the uniform embedding law is not necessarily optimal; the embedding distribution should be calibrated according to the reliability profile $\{\beta_i\}_{i=1}^{n_c}$. The uniform result in **Proposition 3** is recovered when $\beta_i = \beta$ for all coded positions.*

Proposition 3. *Among all embedding-position distributions $\{q_i\}_{i=1}^{n_c}$ satisfying $q_i \geq 0$ and $\sum_{i=1}^{n_c} q_i = 1$, the positional-footprint variance λ_Δ is minimized if and only if*

$$q_i = \frac{1}{n_c}, \qquad i = 1, 2, \ldots, n_c.$$

Equivalently, codeword-wide uniform random embedding uniquely minimizes the systematic positional footprint under the corrected-error-statistics scenario.

Proof. From (20) and (19), we get

$$\bar{\Delta} = \frac{\beta}{2n_c}, \qquad \lambda_\Delta = \frac{\beta^2}{4n_c} \sum_{i=1}^{n_c} \left(q_i - \frac{1}{n_c} \right)^2. \tag{22}$$

From (22), we find that λ_Δ is a nonnegative scaled sum of squared deviations between the embedding-position probabilities q_i and the uniform probability $1/n_c$. Hence, for any feasible distribution $\{q_i\}_{i=1}^{n_c}$, we have $\lambda_\Delta \geq 0$.

Moreover, the minimum value $\lambda_\Delta = 0$ is attained if and only if every squared deviation in (22) is equal to zero. This happens if and only if

$$q_i - \frac{1}{n_c} = 0, \qquad i = 1, 2, \ldots, n_c,$$

which is equivalent to $q_i = 1/n_c$ for all coded positions. Hence the uniform distribution over the entire codeword uniquely minimizes the positional-footprint variance. This completes the proof.

Corollary 2. *Any embedding strategy restricted to a proper subset of codeword positions, including fixed-position embedding and random embedding confined to only information bits or only parity-check bits, yields $\lambda_\Delta > 0$ and is therefore strictly less secure than codeword-wide uniform random embedding under the corrected-error-statistics scenario.*

Proof. Any embedding strategy restricted to a proper subset of codeword positions cannot assign probability $1/n_c$ to every coded position. Hence, under such a restricted strategy, there exists at least one index i for which $q_i \neq 1/n_c$. From (22), we then get

$$\lambda_\Delta = \frac{\beta^2}{4n_c} \sum_{i=1}^{n_c} \left(q_i - \frac{1}{n_c} \right)^2 > 0.$$

By **Proposition 3**, the minimum value $\lambda_\Delta = 0$ is attained only by the codeword-wide uniform law $q_i = 1/n_c$ for all i. Therefore any embedding strategy confined to a proper subset of coded positions is strictly less secure under the corrected-error-statistics scenario. This completes the proof.

Proposition 4. *Under the corrected-error-statistics scenario, any embedding-position distribution $\{q_i\}_{i=1}^{n_c}$ satisfying $\lambda_\Delta \leq \varepsilon_1$ must satisfy*

$$\sum_{i=1}^{n_c} \left(q_i - \frac{1}{n_c} \right)^2 \leq \frac{4n_c \varepsilon_1}{\beta^2}. \tag{23}$$

If the embedding positions are uniformly selected from a subset of s coded positions and are not selected outside this subset, then

$$\lambda_\Delta(s) = \frac{\beta^2}{4n_c} \left(\frac{1}{s} - \frac{1}{n_c} \right). \tag{24}$$

Therefore, the condition $\lambda_\Delta(s) \leq \varepsilon_1$ requires

$$s \geq \left\lceil \frac{n_c \beta^2}{\beta^2 + 4n_c^2 \varepsilon_1} \right\rceil. \tag{25}$$

Proof. From (22), the condition $\lambda_\Delta \leq \varepsilon_1$ directly gives (23). For subset-based uniform embedding, we have $q_i = 1/s$ on the selected subset and $q_i = 0$ outside it. Hence,

$$\begin{aligned} \sum_{i=1}^{n_c} \left(q_i - \frac{1}{n_c} \right)^2 &= s \left(\frac{1}{s} - \frac{1}{n_c} \right)^2 + (n_c - s) \left(\frac{1}{n_c} \right)^2 \\ &= \frac{1}{s} - \frac{1}{n_c}. \end{aligned} \tag{26}$$

Substituting (26) into (22) yields (24). Solving $\lambda_\Delta(s) \leq \varepsilon_1$ with respect to the integer variable s yields (25). This completes the proof.

In the first attack scenario, Eve compares the corrected-error profile of the overt channel with that of the received signal. The positional-footprint variance λ_Δ in (19) is a population-level quantity defined from the expected increments $\{\Delta_i\}_{i=1}^{n_c}$, and is therefore used in **Proposition 3** to analyze the systematic footprint induced by the embedding-position distribution. In practice, Eve cannot directly observe these expectations and can only estimate the footprint from finite received blocks. Hence, the statistic used for the security test is the empirical counterpart of λ_Δ, given by

$$\lambda \triangleq \widehat{\lambda}_\Delta = \mathrm{var}_i\big\{ N_{\mathrm{stego}}(i) - N_{\mathrm{normal}}(i) \big\}, \tag{27}$$

where $\mathrm{var}_i\{\cdot\}$ denotes the variance over the coded positions. Thus, λ_Δ and λ characterize the same position-dependent corrected-error footprint at the theoretical and empirical levels, respectively. As the number of observed codeword blocks increases, λ converges to λ_Δ up to finite-sample fluctuations. Based on this empirical statistic, the security capacity under Scenario 1 is defined as

$$C_{\mathrm{hide}}^{\mathrm{S1}} = \begin{cases} C_{\mathrm{hide}}, & \text{if } \lambda \leq \varepsilon_1, \\ 0, & \text{if } \lambda > \varepsilon_1, \end{cases} \tag{28}$$

where ε_1 is the detection threshold of the corrected-error-statistics scenario.

B. Security Scenario 2: BER Variation and Overall Security Capacity

In the second attack scenario, Eve estimates the overt-channel BER in the presence of embedding and compares it against the no-embedding baseline. The normalized BER variation induced by embedding is defined with a denominator floor as

$$\delta = \frac{|p_{\text{normal}} - p_{\text{stego}}|}{\max\{p_{\text{normal}}, p_{\text{floor}}\}}, \tag{29}$$

where $p_{\text{floor}} > 0$ is a small BER floor used to avoid numerical instability when p_{normal} is very small or zero. When $p_{\text{normal}} \gg p_{\text{floor}}$, (29) reduces to the conventional normalized BER variation. The corresponding security capacity is defined as

$$C_{\text{hide}}^{\text{S2}} = \begin{cases} C_{\text{hide}}, & \text{if } \delta \le \varepsilon_2, \\ 0, & \text{if } \delta > \varepsilon_2, \end{cases} \tag{30}$$

where ε_2 is the detection threshold of the BER-variation scenario. The thresholds ε_1 and ε_2 are detector operating parameters associated with the corrected-error positional-footprint statistic λ and the normalized BER-variation statistic δ, respectively. In practical implementations, they can be calibrated from overt-only transmissions according to prescribed false-alarm probabilities. In the numerical results, representative fixed thresholds are used and kept unchanged across the compared cases, so that different system configurations are evaluated under a common detector operating point.

When both scenarios are active, the overall security capacity is defined as

$$C_{\text{hide}}^{\text{Overall}} = \min\big(C_{\text{hide}}^{\text{S1}}, C_{\text{hide}}^{\text{S2}}\big). \tag{31}$$

Proposition 5. *Under the joint detector in* (17) *and the capacity definitions in* (28)–(31)*, the overall security capacity is positive if and only if*

$$\lambda \le \varepsilon_1 \qquad \textit{and} \qquad \delta \le \varepsilon_2.$$

In that case,

$$C_{\text{hide}}^{\text{Overall}} = L\frac{k_h}{n_h}\frac{(1-2p_{\text{hide}})^2}{2\ln 2};$$

$$C_{\text{hide}}^{\text{Overall}} = C_{\text{hide}};$$

otherwise,

$$C_{\text{hide}}^{\text{Overall}} = 0.$$

Proof. Let

$$Q = C_{\text{hide}}, \tag{32}$$

and define the indicator variables

$$I_1 = \mathbf{1}_{\{\lambda \le \varepsilon_1\}}, \qquad I_2 = \mathbf{1}_{\{\delta \le \varepsilon_2\}}. \tag{33}$$

Then, from (28) and (30), we get

$$C_{\text{hide}}^{\text{S1}} = QI_1, \qquad C_{\text{hide}}^{\text{S2}} = QI_2. \tag{34}$$

Substituting (34) into the overall-security definition in (31), we obtain

$$\begin{aligned} C_{\text{hide}}^{\text{Overall}} &= \min(QI_1, QI_2) \\ &= Q\min(I_1, I_2). \end{aligned} \tag{35}$$

Because I_1 and I_2 take values only in $\{0,1\}$, we have

$$\min(I_1, I_2) = I_1 I_2. \tag{36}$$

Combining (35) and (36), we get

$$C_{\text{hide}}^{\text{Overall}} = QI_1 I_2. \tag{37}$$

From (37), we find that $C_{\text{hide}}^{\text{Overall}} > 0$ holds if and only if both indicators are equal to one, that is, if and only if $\lambda \le \varepsilon_1$ and $\delta \le \varepsilon_2$. When both conditions are satisfied, $I_1 I_2 = 1$ and (37) reduces to $C_{\text{hide}}^{\text{Overall}} = Q$. Otherwise, at least one indicator is zero, and hence $C_{\text{hide}}^{\text{Overall}} = 0$. This completes the proof.

Corollary 3. *Any operating point satisfying the robustness condition $p_{\text{stego}} = p_{\text{normal}}$ also satisfies $\delta = 0$ and therefore automatically passes the BER-variation scenario for any threshold $\varepsilon_2 > 0$.*

Proof. If the robustness condition $p_{\text{stego}} = p_{\text{normal}}$ holds, then substituting this equality into (29) yields

$$\delta = \frac{|p_{\text{normal}} - p_{\text{stego}}|}{\max\{p_{\text{normal}}, p_{\text{floor}}\}} = 0. \tag{38}$$

Therefore, for any threshold $\varepsilon_2 > 0$, the inequality $\delta \le \varepsilon_2$ is automatically satisfied. This means that every robustness-feasible operating point necessarily passes the BER-variation attack scenario. This completes the proof.

The preceding results provide the formal feasibility conditions. They also explain the operating-regime behavior examined later in Section V: in the low-SNR regime, channel uncertainty can mask the embedding footprint and make both λ and δ small, whereas in the high-SNR regime the overt decoder can often absorb the embedding perturbation so that $p_{\text{stego}} \approx p_{\text{normal}}$ and the BER-variation scenario becomes inactive. The intermediate SNR range is generally the least favorable operating region because the overt channel becomes reliable while the embedding-induced statistical perturbations remain visible.

V. Numerical Results

A. Simulation Setup

We consider the coded covert-channel model described in Section II. The wireless channel is modeled as a Nakagami-m fading channel. Unless otherwise specified, BCH block codes are used for both the cover signal and the hidden signal, while convolutional coding is considered only in the structural-comparison experiment. The performance is evaluated from the viewpoints of robustness and security. For robustness, we use the capacity $C_{\text{hide}}^{\text{R}}$ in (4). For security, we examine the corrected-error profile across coded positions, the two scenario-specific security capacities in (28) and (30), and the overall security capacity in (31). For the BER-variation

TABLE I
KEY SIMULATION PARAMETERS.

Parameter	Value	Parameter	Value
N_{MC}	10	N_{blk}	5×10^4
$C_b(n_c, k_c)$	$C_b(63, 24)$	t_c	7
$C_b(n_h, k_h)$	$C_b(31, 16)$	t_h	3
l_h	3	Modulation	MPSK
M	4	m	1
ε_1	10^{-5}	ε_2	0.1
BCH decoder	HDD	Conv. decoder	Viterbi
$C_c(n, k, K)$	$C_c(2, 1, 4)$	Traceback length	35

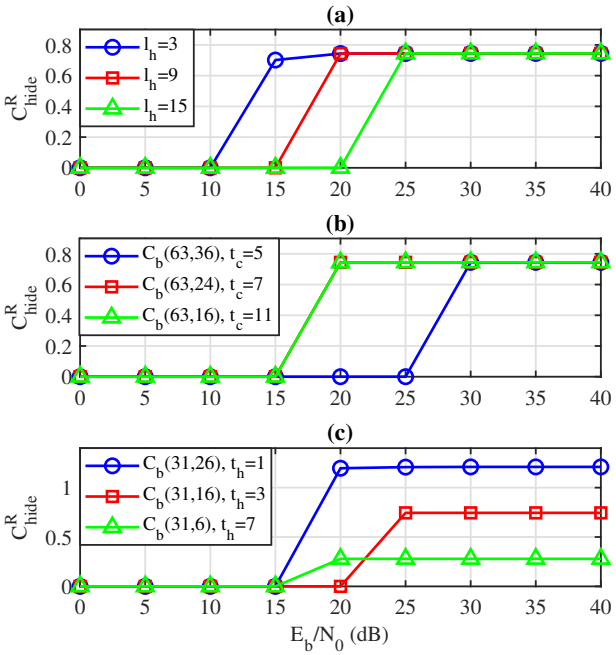

Fig. 2. Covert channel capacity $C^{\mathrm{R}}_{\mathrm{hide}}$ as a function of SNR for: (a) different numbers of hidden coded bits l_h embedded in each cover-code codeword; (b) different error-correction capabilities t_c of the cover code; and (c) different error-correction capabilities t_h of the hidden code.

statistic in (29), p_{floor} is set to the BER resolution of the corresponding Monte Carlo estimate, so that zero-error overt-channel realizations remain well defined in high-SNR regimes. The key default simulation parameters are summarized in Table I, where HDD denotes hard-decision decoding, and Viterbi denotes the hard-decision Viterbi decoder.

Unless otherwise specified, the simulations use independent message, fading, and noise realizations, and all plotted curves are obtained by Monte Carlo averaging. Since the BERs in the simulations are estimated from a finite number of decoded bits, the analytical condition $p_{\mathrm{stego}} = p_{\mathrm{normal}}$ in (4) is evaluated numerically using $|p_{\mathrm{stego}} - p_{\mathrm{normal}}| \leq \epsilon_{\mathrm{R}}$, where ϵ_{R} is set to the BER resolution of the corresponding Monte Carlo estimate.

B. Simulation Results

1) Robustness Results

We first examine the effects of the embedding payload l_h, the cover-code error-correction capability t_c, and the hidden-code error-correction capability t_h on the robustness capacity, where a larger value of $C^{\mathrm{R}}_{\mathrm{hide}}$ indicates a more favorable operating point. The results are shown in Fig. 2. Figure 2(a) shows that the covert capacity decreases monotonically as l_h increases. For $C_b(63, 7)$ with $M = 4$, $m = 1$, and $t_h = 3$, the feasible SNR region gradually shrinks and eventually disappears as the embedding payload becomes sufficiently large, consistent with **Proposition 1** and **Corollary 1**. Figure 2(b) shows that increasing the cover-code error-correction capability t_c raises the achievable covert capacity and enlarges the feasible SNR region, in agreement with **Proposition 2**. This trend is consistent with (11), under which a larger t_c reduces the decoder-overload probability. Figure 2(c) shows that, under the considered parameter setting, increasing t_h does not improve the covert capacity. In this case, the reduction in the hidden-code rate k_h/n_h dominates the benefit brought by the smaller value of p_{hide}, which is consistent with the discussion at the end of Section III.

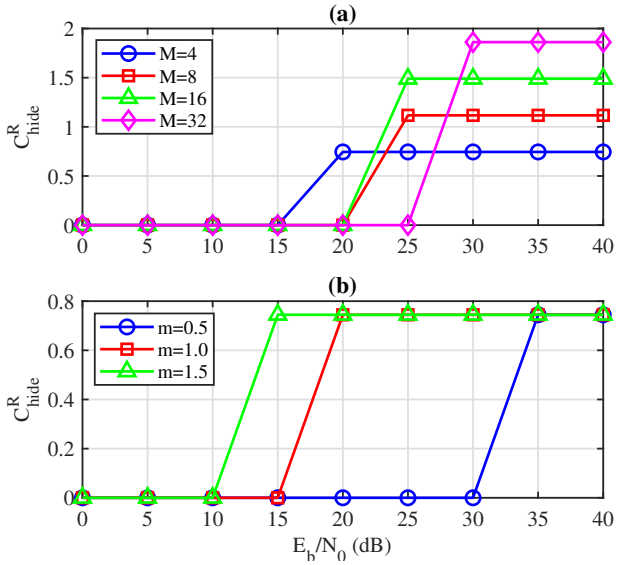

Fig. 3. Covert channel capacity $C^{\mathrm{R}}_{\mathrm{hide}}$ as a function of SNR for: (a) different modulation orders M; and (b) different Nakagami fading parameters m.

We next examine the effects of the modulation order M and the fading parameter m on the robustness capacity. The results are shown in Fig. 3. Figure 3(a) shows that the effect of M depends strongly on the operating SNR. In this example, a larger modulation order requires a higher SNR before a positive covert capacity becomes achievable, whereas it yields a higher covert rate once the system enters the robustness-feasible regime. This trend is consistent with Section III: increasing M improves the factor $L = \log_2 M$ in (3), but it also reduces the Euclidean distance between constellation points. Figure 3(b) shows that increasing the Nakagami parameter m improves the covert capacity by reducing the severity of fading, which again agrees with the analysis in Section III.

We then compare block coding and convolutional coding under the considered bit-flip embedding rule. The results are shown in Fig. 4, where the coded output lengths are matched for fairness. Figure 4(a) shows that the overt BER in the

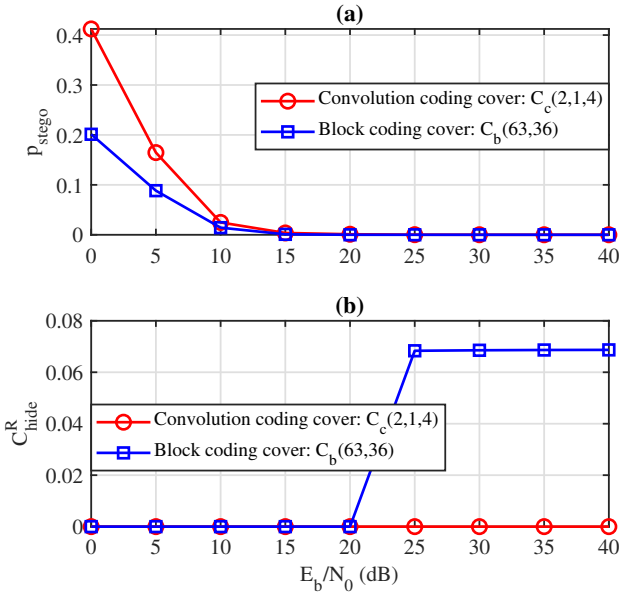

Fig. 4. BER and covert capacity as functions of SNR for block coding $C_b(63, 36)$ and convolutional coding $C_c(2, 1, 4)$ applied to the cover signal, with $m = 1$, $M = 4$, and $l_h = 3$.

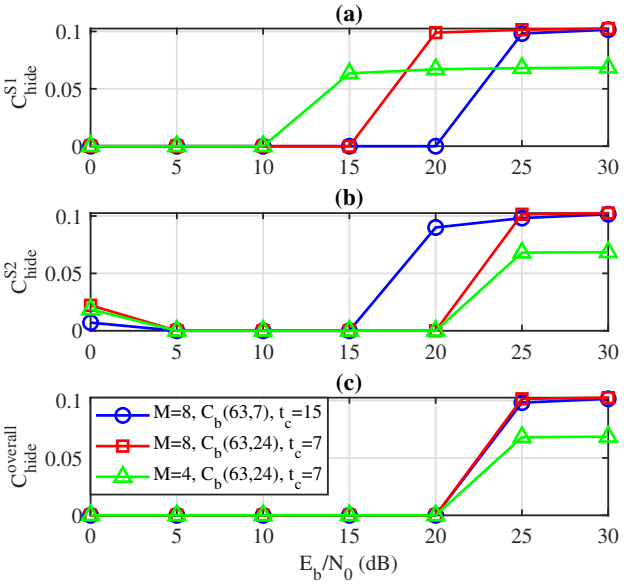

Fig. 6. Covert capacity under the considered security constraints as a function of SNR, for different modulation orders M and cover-code error-correction capabilities t_c. Parameters: $m = 1$, $l_h = 3$, $\varepsilon_1 = 10^{-5}$, and $\varepsilon_2 = 0.1$.

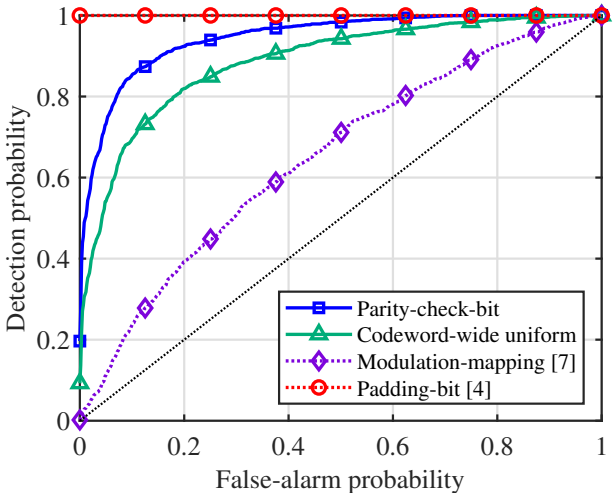

Fig. 5. ROC comparison of different physical-layer covert embedding schemes under Rayleigh fading with imperfect CSI, where $m = 1$ and channel estimation error variance 10^{-2}.

convolutional-coded case increases much faster than that in the block-coded case. Figure 4(b) shows that the covert capacity of the convolutional-coded system collapses much earlier than that of the block-coded system. These results indicate that convolutional coding is substantially more sensitive than block coding to embedding-induced perturbations under the considered rule. This trend agrees with the analysis in Section III: in convolutional coding, one embedding-induced perturbation affects multiple trellis relations because of encoder memory, whereas in block coding the perturbation remains confined to its own codeword.

2) Security Results

We further compare the detection performance of different physical-layer covert embedding schemes, including the considered parity-check-bit and codeword-wide uniform schemes, the padding-bit scheme [4], and the modulation-mapping scheme [17]. The corrected-error positional-footprint statistic is used as the detection score, where the overt-only transmission is treated as $\mathcal{H}_0$ and each embedding scheme is treated as $\mathcal{H}_1$. The ROC curves are obtained under Rayleigh fading with imperfect CSI, and the results are shown in Fig. 5. For a fixed false-alarm probability, a larger detection probability indicates that Eve can more easily identify covert embedding and hence implies lower security. Fig. 5 shows that the padding-bit and parity-check-bit schemes are the easiest to detect because their embedding operations are confined to structured or restricted positions, producing strong positional footprints. By contrast, the codeword-wide uniform scheme achieves a lower detection probability by spreading embedding perturbations over the whole codeword, which is consistent with Proposition 3 and Corollary 2. The modulation-mapping baseline gives the lowest response under this detector because its main trace lies in constellation-domain or symbol-distribution statistics rather than corrected-error positions. Fig. 5 verifies the advantage of codeword-wide uniform embedding among the considered code-domain embedding strategies and highlights the need for mechanism-matched detectors when comparing different physical-layer covert schemes.

We finally examine the overall security capacity under the joint statistical attack model. The results are shown in Fig. 6 for $m = 1$, $l_h = 3$, $\varepsilon_1 = 10^{-5}$, and $\varepsilon_2 = 0.1$. Figure 6 shows that, under the adopted thresholds and parameter setting, positive covert capacity may arise in both low-SNR and high-SNR regimes, whereas an intermediate SNR range is less favorable. This trend is consistent with **Proposition 5** and **Corollary 3**. From (37), positive overall security capacity is achievable only

when both statistical constraints are simultaneously satisfied. Moreover, from (29), the BER-variation constraint becomes inactive when the difference between p_{stego} and p_{normal} is negligible. Figure 6 also shows that the effects of the modulation order M and the cover-code error-correction capability t_c depend on the operating regime. In the high-SNR regime, increasing M raises the achievable covert rate through the factor $L = \log_2 M$ in (3), whereas the effect of t_c depends on which statistical constraint dominates at the operating point. These numerical results agree with the analysis in Section IV.

VI. Conclusion

This paper developed a performance-analysis framework for channel-coding-based covert channels in physical-layer wireless communications. Rather than focusing only on covert-channel construction, it characterized the feasibility of such transmission from the joint viewpoints of robustness, security, and covert capacity. A robustness analysis was developed to capture the hidden transmission rate achievable without degrading the overt channel. A security analysis was then established under two statistical attack scenarios, one based on corrected-error distributions across codeword positions and the other based on embedding-induced BER variation.

The analysis yielded several structural conclusions. First, the covert capacity is nonincreasing with the number of hidden coded bits embedded in each cover-code codeword, while increasing the error-correction capability of the cover code enlarges the robustness-feasible region. Second, under the corrected-error-statistics scenario, codeword-wide uniform random embedding uniquely minimizes the systematic positional footprint. Third, positive overall security capacity is achievable only when both statistical constraints are simultaneously satisfied. The simulation results verified these analytical findings and further showed that block-coded systems are substantially more suitable than convolutional-coded systems under the considered bit-flip embedding rule, and that viable covert transmission can arise in both low- and high-SNR regimes.

Future work includes the design of embedding rules tailored to memory codes, the development of more efficient coded embedding strategies under wireless transmission constraints, and the extension of the present analysis to multicarrier and multi-antenna wireless systems.

Acknowledgment

This work was supported by the Natural Science Foundation of Qinghai Province (No. 2026-ZJ-756).

References

[1] R. J. Anderson and F. A. P. Petitcolas, "On the limits of steganography," *IEEE Journal on Selected Areas in Communications*, vol. 16, no. 4, pp. 474–481, 1998.

[2] X. Chen, J. An, Z. Xiong, C. Xing, N. Zhao, F. R. Yu, and A. Nallanathan, "Covert communications: A comprehensive survey," *IEEE Communications Surveys and Tutorials*, vol. 25, no. 2, pp. 1173–1198, 2023.

[3] Y. Jiang, L. Wang, H.-H. Chen, and X. Shen, "Physical layer covert communication in B5G wireless networks—Its research, applications, and challenges," *Proceedings of the IEEE*, vol. 112, no. 1, pp. 47–82, 2024.

[4] K. Szczypiorski and W. Mazurczyk, "Steganography in IEEE 802.11 OFDM symbols," *Security and Communication Networks*, vol. 9, no. 2, pp. 118–129, 2016.

[5] S. Grabski and K. Szczypiorski, "Steganography in OFDM symbols of fast IEEE 802.11n networks," in *Proceedings of the IEEE Security and Privacy Workshops (SPW)*, San Francisco, CA, USA, 2013, pp. 158–164.

[6] P. P. Kumar, R. Amirtharajan, K. Thenmozhi, and J. B. B. Rayappan, "Steg-OFDM blend for highly secure multi-user communication," in *Proceedings of the 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace Electronic Systems Technology (Wireless VITAE)*, Chennai, India, 2011, pp. 1–5.

[7] P. Praveenkumar, S. Vivekhandan, V. Phaneendra, K. Thenmozhi, J. B. B. Rayappan, and R. Amirtharajan, "DS-CDMA in stego pitch," in *Proceedings of the International Conference on Computer Communication and Informatics (ICCCI)*, Coimbatore, Tamil Nadu, India, 2013, pp. 1–6.

[8] A. Marzin, M. Schwartz, and M. Segal, "Covert channel by exploiting error-correcting codes," *Computer Networks*, vol. 266, p. 111314, 2025.

[9] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge, UK: Cambridge University Press, 2011.

[10] 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.

[11] M. R. Bloch, "Covert communication over noisy channels: A resolvability perspective," *IEEE Transactions on Information Theory*, vol. 62, no. 5, pp. 2334–2354, 2016.

[12] N. Xie, Z. Li, J. Tan, and A. X. Liu, "Detection of information hiding at physical layer in wireless communications," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 2, pp. 1104–1117, 2022.

[13] M. Walter and J. Keller, "Design and evaluation of steganographic channels in Fifth-Generation New Radio," *Future Internet*, vol. 16, no. 11, p. 410, 2024.

[14] J. Keller, D. Spiekermann, and M. Walter, "Protocol design rules from hiding patterns to avoid steganographic channels in wireless communication," in *Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC)*, Milan, Italy, 2025, pp. 1–6.

[15] M. K. Simon and M.-S. Alouini, *Digital Communication over Fading Channels*, 2nd ed. Hoboken, NJ, USA: Wiley, 2005.

[16] H. J. Helgert, "On a bound for channel capacity," *IEEE Transactions on Information Theory*, vol. 13, no. 1, pp. 126–127, 1967.

[17] P. Cao, W. Liu, G. Liu, X. Ji, J. Zhai, and Y. Dai, "A wireless covert channel based on constellation shaping modulation," *Security and Communication Networks*, vol. 2018, p. 1214681, 2018.