How Does Repetition Coding Enable Reliable and Covert Communications?

Jinglu Cui, Student Member, IEEE, Shihao Yan, Member, IEEE, Jinsong Hu, Member, IEEE, Na Li, Riqing Chen, Member, IEEE, and Jinghu Li, Member, IEEE

Abstract—This letter tackles whether and how repetition coding enables reliable and covert communications by considering binary phase shift keying. Communication reliability and covertness are analyzed in terms of the bit error rate $P_e$ and the minimum detection error probability $\xi$. Our examination shows that, when a warden Willie knows the codeword structure, both $P_e$ and $\xi$ are determined by the total power $nP$ and do not depend on the codeword length $n$ or the transmit power $P$ individually. However, this conclusion does not hold for the unknown codeword structure, where increasing $n$ can significantly improve the communication reliability under the same covertness constraint, and vice versa.

Index Terms—Covert communications, BPSK, repetition code, interleaver, communication reliability.

I. INTRODUCTION

CRUCIAL concerns on the security and privacy of wireless communications are emerging due to the fact that an increasing amount of confidential information is currently transmitted through wireless medium. Against this background, covert communication technology is emerging as a promising approach to resolve such security and privacy concerns in wireless networks, since this technology has the ability to hide the very existence of wireless transmissions [1]–[3]. In a covert communication system, a transmitter (Alice) intends to send information to a receiver (Bob) covertly, i.e., avoiding such a transmission being detected by a warden Willie.

Covert communications have received considerable attention recently. For example, the square root law on covert communication rate has been presented in [4] for additive white Gaussian noise (AWGN) channels, where it is proved that no more than $O(n)$ bits of information can be transmitted from Alice to Bob reliably and covertly in $n$ channel uses as $n \to \infty$. The authors of [5] investigated a low-complexity coding scheme for covert communication. A method of embedding messages on a given broadcast code was provided in [6], where the coding scheme proved feasibility of covert communications and summarized some necessary conditions for using covert communications. An optimal low-complexity coding scheme was developed in [7], which can achieve the information-theoretic limits of covert communications over binary-input discrete memoryless channels (BI-DMCs). In [8], the optimality of Gaussian signalling was examined in covert communications. A covert communication system under block fading channels was examined in [9], where transceivers have uncertainty on the related channel state information (CSI). Covert communications with random interference from non-cooperative transmitters were studied in [10]. The letter [11] showed that a relay can transmit information to a destination covertly on top of forwarding the source’s message. This letter has been extended into a self-sustained relay network [12].

Recently, the authors of [13] extended single-antenna covert communications to multi-antenna systems with centralized and distributed antennas. In addition, covert communications through Device-to-Device (D2D) links were achieved by exploiting co-channel interference in D2D content sharing systems in [14]. The authors of [15] extended the applications of covert communications from static scenarios to dynamic ones. In order to eliminate the requirement of CSI, [16] adopted channel inversion power control (CIPC) to achieve covert communications and this CIPC scheme has been extended into IoT scenarios for achieving covert communications [17]. In addition, following [16], the authors of [18] developed an optimal power adaptation strategy for the CIPC scheme under different covertness constraints. Furthermore, covert communications were examined by considering a cognitive jammer [19], 3-dimensional beamforming [20], delay constraints [21], [22], and THz bandwidth [23].

Although covert communications have been studied in a wide range of scenarios, there are still many technical challenges for deploying this technology into practice. These challenges include but not limit to: 1) how to optimally design multi-hop large-scale covert communication networks, 2) what are the optimal interference signals to maximize covert communication performance, and 3) how to eliminate the prior information on Willie in analyzing the achievable covertness level. Furthermore, in covert communications, transmit power is normally in its low regime due to the covertness constraint, which may lead to low transmission reliability. In communications without covertness constraints, channel coding has the capability to increase reliability at the cost of extra redundancy. However, in covert communications, this redundancy increases the number of observations at Willie, which may improve his detection accuracy and thus violate the covertness constraints.

Manuscript received October 30, 2020; accepted December 7, 2020. Date of publication December 14, 2020; date of current version March 9, 2021.

The associate editor coordinating the review of this article and approving it for publication was J. Lee (Corresponding author: Shihao Yan.)

Jinglu Cui, Riqing Chen, and Jinghu Li are with the School of Computer and Information Sciences, Fujian Agriculture and Forestry University, Fuzhou 350002, China (e-mail: jinglu@fafu.edu.cn; riqing.chen@fafu.edu.cn; jhlee@eochip.com).

Shihao Yan is with the School of Engineering, Macquarie University, Sydney, NSW 2109, Australia (e-mail: shihao.yan@mq.edu.au).

Jinsong Hu is with the College of Physics and Information Engineering, Fuzhou University, Fuzhou 350116, China (e-mail: jinsong.hu@fzu.edu.cn).

Na Li is with the Aerospace Information Research Institute, Chinese Academy of Sciences, Beijing 100094, China (e-mail: xwnaruto@163.com).

Digital Object Identifier 10.1109/LWC.2020.3044305
constraint. Against this background, whether or how channel coding improves covert communication performance becomes an urgent research question. In this letter, we take the initial step to tackle this challenge question by considering the repetition channel coding together with the binary phase shift keying (BPSK) modulation. Based on our performance analysis on Willie’s detection, we prove that, 1) when Willie knows the code structure, increasing the repetition code length cannot improve covert communication performance at all, and 2) when Willie does not know the code structure, increasing the repetition code length improves reliability subject to the same covertness constraint and vice versa.

II. SYSTEM MODEL

A. System Model and Adopted Assumptions

In this letter, we consider a simple scenario, where Alice tries to send messages to Bob covertly under the surveillance of Willie, who intend to determine whether Alice sends signal to Bob. The channel from Alice to Willie is denoted by \( h_{aw} \) and the channel from Alice to Bob is denoted by \( h_{ab} \). It is assumed that Alice adopts BPSK with the repetition code of length \( n \) to send information to Bob. Specifically, Alice has two possible symbols to transmit, i.e., \( s_0 = \sqrt{2P} \) for transmitting ‘0’ and \( s_1 = -\sqrt{2P} \) for transmitting ‘1’, where \( P \) is the transmit power of Alice. With the repetition code, Alice sends \([s_1^2, s_2^2, \ldots, s_n^2]\) to improve communication reliability, where \( i \) is the index for each symbol, \( k = 0 \) or \( k = 1 \) denotes Alice’s transmitted symbol for sending the information bit ‘0’ and ‘1’, respectively.

B. Binary Hypothesis Testing at Willie

The received signal at Willie in the \( i \)-th symbol period is given by

\[
\begin{align*}
H_0 &: y_w[i] = n_w[i], \\
H_1 &: y_w[i] = \sqrt{L_{aw}}h_{aw}s_k[i] + n_w[i],
\end{align*}
\]

where \( H_0 \) denotes the null hypothesis where Alice did not transmit signal, \( H_1 \) denotes the alternative hypothesis where Alice transmitted signal, \( L_{aw} \equiv \psi(d_{aw})^{-m} \) is the path loss, \( m \) is the path loss exponent, \( \psi \) is a constant depending on carrier frequency, which is commonly set as \( (\frac{c}{f_c})^2 \) with \( c = 3 \times 10^8 \) m/s and \( f_c \) as the carrier frequency, \( d_{aw} \) is the distance from Alice to Willie, \( s_k \) is the signal transmitted by Alice satisfying \( \mathbb{E}[(s_k[i])^2] = P, \), \( i = 1, \ldots, n, \) and \( n_w[i] \) is the AWGN at Willie with \( \sigma_w^2 \) as its variance, i.e., \( n_w[i] \sim \mathcal{CN}(0, \sigma_w^2) \). Then, the likelihood function of \( y_w \) under \( H_0 \) is given by

\[
f(y_w|H_0) = \prod_{i=1}^{n} f(y_w[i]|H_0) = \frac{1}{\pi n \sigma_w^2} e^{-\frac{\sum_{i=1}^{n}|y_w[i]|^2}{\sigma_w^2}}.
\]

Considering that \( s_0 \) and \( s_1 \) are equally like to be transmitted by Alice, the likelihood function of \( y_w[i] \) under \( H_1 \) is

\[
f(y_w[i]|H_1) = \frac{1}{2\pi \sigma_w^2} e^{-\frac{|y_w[i] - \sqrt{70P}|^2}{\sigma_w^2}} + \frac{1}{2\pi \sigma_w^2} e^{-\frac{|y_w[i] + \sqrt{70P}|^2}{\sigma_w^2}},
\]

where \( P_0 = PL_{aw}|h_{aw}|^2 \). The likelihood function of \( y_w \) under \( H_1 \) depends on whether Willie knows the structure of codeword or not, which is denoted as \( f(y_w|H_1) \) and will be specified later.

The optimal detector that minimizes the detection error probability \( \xi \) is the likelihood ratio test, which is given by

\[
\Lambda(y_w) = \frac{f(y_w|H_1)}{f(y_w|H_0)} \frac{D_1}{D_0} \frac{Pr(H_0)}{Pr(H_1)},
\]

where \( \Lambda(y_w) \) is the likelihood ratio, \( D_1 \) and \( D_0 \) denote the binary decisions that infer whether Alice’s transmission occurs or not, respectively, \( Pr(H_0) \) and \( Pr(H_1) \) are the prior probabilities for \( H_0 \) and \( H_1 \), respectively. In this letter, we consider equal prior probabilities, i.e., \( Pr(H_0) = Pr(H_1) = 1/2 \). As such, the total error probability is given by \( Pr(H_0) + Pr(H_1) = \alpha + \beta = 1/2 \), where \( \alpha \equiv Pr(D_1|H_0) \) is the false alarm probability and \( \beta \equiv Pr(D_0|H_1) \) is the miss detection probability. For clarity, considering \( Pr(H_0) = Pr(H_1) = 1/2 \) define \( \xi = \alpha + \beta \), which is referred to as the detection error probability in this letter. Willie’s ultimate goal is to detect the presence of Alice’s transmission with the minimum detection error probability \( \xi^* \). Then, the covertness constraint can be written as \( \xi^* \geq 1 - \epsilon \), where \( \epsilon \) is normally a small value to determine the required covertness.

C. Bit Error Rate at Bob

The received signal at Bob for the \( i \)-th symbol is

\[
y_b[i] = \sqrt{L_{ab}}h_{ab}s_k[i] + n_b[i], \tag{5}
\]

where \( n_b[i] \) is the AWGN at Bob with \( \sigma_b^2 \) as its variance, \( L_{ab} \equiv \psi(d_{ab})^{-m} \) is the path loss, and \( d_{ab} \) is the distance from Alice to Bob. In this letter, we consider soft decoding at Bob, where Bob combines all the received symbols for each codeword and then conducts the decoding. Then, with the repetition code of length \( n \), the bit error rate (BER) of the BPSK modulation is

\[
P_e = Q\left(\sqrt{\frac{nPL_{ab}|h_{ab}|^2}{\sigma_b^2}}\right) = \frac{1}{2} \text{erfc}\left(\sqrt{\frac{n\gamma_b}{2}}\right), \tag{6}
\]

where \( \gamma_b = \frac{nPL_{ab}|h_{ab}|^2}{\sigma_b^2} \) is the signal-to-noise ratio (SNR) of the channel from Alice to Bob, \( Q(\cdot) \) is the Q-function, and \( \text{erfc}(\cdot) \) is the complementary error function.

III. COVERT COMMUNICATIONS WITH AND WITHOUT AN INTERLEAVER

In this section, we tackle the performance of covert communications with and without an interleaver and explicitly reveal the necessity of using an interleaver to keep the codeword structure secrecy from Willie in covert communications.

A. Channel Coding Without an Interleaver

In this subsection, we first examine Willie’s detection performance when Alice does not employ an interleaver with channel coding, which means that Willie knows the codeword structure. As such, the likelihood function of \( y_w \) under \( H_1 \) is given by
Following (2) and (7), the likelihood ratio defined in (4) can be rewritten as

$$
\Lambda(y_w) = \frac{e^{-\frac{n\lambda}{\sigma^2}}}{2} \left( e^{2\sqrt{T_0} \sum_{i=1}^{n} \Re \{y_{w[i]}\}} + e^{-2\sqrt{T_0} \sum_{i=1}^{n} \Re \{y_{w[i]}\}} \right),
$$

where $\Re \{x\}$ denotes the real part of $x$. Then, the optimal decision rule given in (4) can be rewritten as $h(t) \equiv \frac{D_1}{D_0} \lambda$, where

$$
h(t) = t + \frac{1}{t}, \quad \text{with} \quad t = e^{rac{2\sqrt{T_0} \sum_{i=1}^{n} \Re \{y_{w[i]}\}}}{\sigma^2},$$

$$
\lambda = 2e^\frac{n\lambda}{\sigma^2}.
$$

We note the term $2\sqrt{T_0} \left( \sum_{i=1}^{n} \Re \{y_{w[i]}\} \right)$ under $H_0$ follows a normal distribution, of which the probability distribution function (pdf) is given by $N(t, 2n\lambda \sigma^2)$. Hence, $t$ under $H_0$ follows a log-normal distribution, of which the cumulative distribution function (cdf) is given by

$$
F_t|H_0(x) = \frac{1}{2} \left[ 1 + \text{erf} \left( \frac{\ln x - 2n\lambda}{2\sqrt{n\lambda \sigma^2}} \right) \right].
$$

Likewise, the cdf of $t$ under $H_1$ is given by

$$
F_t|H_1(x) = \frac{1}{2} \left[ 1 + \text{erf} \left( \frac{\ln x + 2n\lambda}{2\sqrt{n\lambda \sigma^2}} \right) \right].
$$

We present the false alarm probability and miss detection probability at Willie in the following theorem.

**Theorem 1:** Without an interleaver, the false alarm and miss detection probabilities at Willie are respectively given by

$$
\alpha = 1 - \frac{1}{2} \text{erf} \left( \frac{\ln \left( t_\lambda^+ \right)}{2\sqrt{\frac{n\lambda \sigma^2}{\alpha^2}}} \right) + \frac{1}{2} \text{erf} \left( \frac{\ln \left( t_\lambda^- \right)}{2\sqrt{\frac{n\lambda \sigma^2}{\alpha^2}}} \right),
$$

$$
\beta = \frac{1}{4} \left[ \text{erf} \left( \frac{\ln \left( t_\lambda^+ \right) - 2n\lambda}{2\sqrt{\frac{n\lambda \sigma^2}{\alpha^2}}} \right) + \text{erf} \left( \frac{\ln \left( t_\lambda^- \right) + 2n\lambda}{2\sqrt{\frac{n\lambda \sigma^2}{\alpha^2}}} \right) \right]
- \frac{1}{4} \left[ \text{erf} \left( \frac{\ln \left( t_\lambda^+ \right) - 2n\lambda}{2\sqrt{\frac{n\lambda \sigma^2}{\alpha^2}}} \right) + \text{erf} \left( \frac{\ln \left( t_\lambda^- \right) + 2n\lambda}{2\sqrt{\frac{n\lambda \sigma^2}{\alpha^2}}} \right) \right],
$$

where $t_\lambda^\pm$ are two different solutions to $h(t) = \lambda$, given by

$$
t_\lambda^\pm = \frac{\lambda \pm \sqrt{\lambda^2 - 4}}{2}.\tag{14}
$$

**Proof:** We derive the first derivative of $h(t)$ with respect to $t$

$$
\frac{\partial h(t)}{\partial t} = 1 - \frac{1}{t^2}.
$$

As per (8) and (15), we have $t > 0$ and conclude that $\partial h(t)/\partial t < 0$ for $0 < t < 1$ and $\partial h(t)/\partial t > 0$ for $t > 1$. We recall that $\lambda > 2$ as per (9) and thus we have $t_\lambda^+ = \sqrt{\lambda^2 - 4}/2 > 1$, $t_\lambda^- = \frac{\lambda - \sqrt{\lambda^2 - 4}}{2} < 1$.

Therefore, the false alarm probability and miss detection probability are respectively derived as

$$
\alpha = \Pr \left( t + \frac{1}{t} > \lambda | H_0 \right) = \Pr \left( t > t_\lambda^+ | H_0 \right) + \Pr \left( t < t_\lambda^- | H_0 \right)
= 1 - F_{t|H_0} \left( t_\lambda^+ \right) + F_{t|H_0} \left( t_\lambda^- \right),
$$

$$
\beta = \Pr \left( t + \frac{1}{t} < \lambda | H_1 \right) = \Pr \left( t_\lambda^- < t < t_\lambda^+ | H_1 \right)
= F_{t|H_1} \left( t_\lambda^- \right) - F_{t|H_1} \left( t_\lambda^+ \right).\tag{17}
$$

Then, substituting (10) and (11) into (16) and (17), respectively, we achieve the desired results in (12) and (13).

Based on Theorem 1, we note that the covertsness of the communication system without an interleaver is determined by $n\lambda$. As per (6), the BER also directly depends on $n\lambda$. Therefore, we can conclude that covert and reliable communication may not be achievable without an interleaver (i.e., when Willie knows the codeword structure), since the system BER cannot be reduced by increasing $n$ under a specific covertness constraint that requires $n\lambda$ being fixed.

**B. Channel Coding With an Interleaver**

In this subsection, we examine the detection performance of Willie when Alice employs an interleaver for channel coding, which leads to the fact that Willie does not know the codeword structure and thus the received symbols are independent to Willie. Then, the likelihood function of $y_w$ under $H_1$ is

$$
\Lambda(y_w) = \frac{1}{2} \prod_{i=1}^{n} \left( e^{-\frac{|y_{w[i]}|-\sqrt{T_0}^2}{\sigma^2}} + e^{-\frac{|y_{w[i]}|+\sqrt{T_0}^2}{\sigma^2}} \right).
$$

Following (2) and (18), the likelihood ratio is given by

$$
\Lambda(y_w) = \frac{1}{2} \prod_{i=1}^{n} \left( e^{-\frac{|y_{w[i]}|-\sqrt{T_0}^2}{\sigma^2}} + e^{-\frac{|y_{w[i]}|+\sqrt{T_0}^2}{\sigma^2}} \right).\tag{19}
$$

Then, as per (19) the optimal decision rule can be written as

$$
\sum_{i=1}^{n} \ln |v_i| \geq \frac{D_1}{D_0} \lambda, \text{ where } v_i = t + 1/t, \quad t = e^\frac{2\sqrt{T_0} \sum_{i=1}^{n} \Re \{y_{w_i[i]}\}}{\sigma^2},
$$

and $\lambda = n \ln 2 + \frac{n\lambda \sigma^2}{\sigma^2}$. We present the false alarm and miss detection probabilities in the following theorem.

**Theorem 2:** With an interleaver, the false alarm and miss detection probabilities are respectively approximated as

$$
\alpha = 1 - \frac{1}{2} \text{erfc} \left( \frac{\lambda - n\mu + \sqrt{\frac{2n\mu \sigma^2}{c_0}}}{\sqrt{\frac{2n\mu (\lambda - \mu) + 2n\sigma^2}{c_0}}} \right)
+ 2T \left[ \frac{n\mu + \sqrt{n\mu + 2n\sigma^2}}{c_0}, \sqrt{\frac{\pi}{c_0 + \pi^2}} \right],
$$

$$
\beta = \frac{1}{2} \text{erfc} \left( \frac{\lambda - n\mu + \sqrt{\frac{2n\mu c_0}{c_1}}}{\sqrt{\frac{2n\mu (\lambda - \mu) + 2n\sigma^2}{c_1}}} \right)
- 2T \left[ \frac{n\mu + \sqrt{n\mu + 2n\sigma^2}}{c_1}, \sqrt{\frac{\pi}{c_1 + \pi^2}} \right].\tag{21}
$$
observe that $P_e$ of the scheme with an interleaver monotonically decreases with $n$, which indicates that the communication reliability can be improved by increasing $n$ in the system with an interleaver. This also demonstrates that reliable covert communications can be enabled by increasing $n$ and keeping the code structure unknown to Willie. Finally, we observe that $P_e$ increases as $\epsilon$ decreases, which indicates a tradeoff between communication covertness and reliability.

V. Conclusion

This letter for the first time studied the impact of channel coding on covert communications by considering repetition coding with BPSK modulation. Our analysis shows that, when the codeword structure is known to Willie, channel coding cannot increase the reliability of covert communications, even at the cost of extra redundancies. When the codeword structure is not known to Willie, communication reliability increases with the codeword length subject to the same covertness constraint. We conjecture that this conclusion also holds for other modulations, since, when the codeword structure is unknown, increasing the codeword length allows Alice to transmit with a larger total power to meet the same covertness constraint.

APPENDIX

PROOF OF THEOREM 2

We present our proof in the following 4 steps.

Step 1: Derive the pdfs of $\ln |v[i]|$ under $\mathcal{H}_0$ and $\mathcal{H}_1$. Following (10), the cdfs of $\ln |v[i]|$ under $\mathcal{H}_0$ is given by

$$
\Pr_{\mathcal{H}_0}(f(t) < x) = F_{\ln |v[i]|}(x) = 
\begin{cases} 
\frac{\text{erf}(\sqrt{x/\sigma_w^2})}{2}, & \text{if } x > 0 \\
0, & \text{if } x \leq 0
\end{cases}
$$

As per (10) and (24), the pdf $\ln |v[i]|$ under $\mathcal{H}_0$ is given by

$$
f_{\ln |v[i]|}(x) = \frac{e^{x}}{2\sqrt{\pi P_0} \sqrt{e^{2x} - 4}}
\begin{aligned}
&\left[ \ln \left( \frac{e^{x} + \sqrt{e^{2x} - 4}}{2} \right) \right] \frac{\sigma_w^2}{\sigma_w^2} \\
&+ e^{x} \left[ \ln \left( \frac{e^{x} + \sqrt{e^{2x} - 4}}{2} \right) \right] \frac{\sigma_w^2}{\sigma_w^2}.
\end{aligned}
$$

Likewise, we can derive the pdf of $\ln |v[i]|$ under $\mathcal{H}_1$ as

$$
f_{\ln |v[i]|}(x) = \frac{\sigma_w e^{x}}{4\sqrt{\pi P_0} e^{2x} - 4}
\begin{aligned}
&\left[ \ln \left( \frac{e^{x} + \sqrt{e^{2x} - 4}}{2} \right) \right] \frac{\sigma_w^2}{\sigma_w^2} \\
&+ e^{x} \left[ \ln \left( \frac{e^{x} + \sqrt{e^{2x} - 4}}{2} \right) \right] \frac{\sigma_w^2}{\sigma_w^2}.
\end{aligned}
$$

IV. NUMERICAL RESULTS

Unless stated otherwise, we set $\lambda_{aw} = \lambda_{ab} = 1$ and $d_{aw} = d_{aw} = 10\text{m}$, the path loss exponent $n$ is set to 2, and the carrier frequency $f_c$ is set to 900MHz [12].

In Fig. 1, we plot the BER $P_e$ of the schemes with and without an interleaver versus $n$ with different values of the covertness parameter $\epsilon$. In this figure, we first observe that $P_e$ of the scheme without an interleaver does not change with $n$ and is the same as the $P_e$ of the scheme with an interleaver for $n = 1$, which is proved in Theorem 1. Meanwhile, we
Step 2: Determine the mean, variance, and skewness of $\ln v[i]$ under $H_0$ and $H_1$.

Following its definition, we know $\ln v[i] \geq \ln 2$. Then, as per their definitions, $m_j$, $v_j$ and $s_j$, where $j=\{0,1\}$ corresponding to $H_0$ and $H_1$, are respectively given by

$$m_j = \frac{\theta_j^2}{2\sqrt{\pi}} \int_{-\infty}^{+\infty} \left(2 \cosh \frac{2\sqrt{\theta_j^2}}{\sigma_w} t\right) e^{-t^2} \left(e^{-2\theta_j t} + e^{2\theta_j t}\right) dt,$$

$$v_j = \frac{\theta_j^2}{2\sqrt{\pi}} \int_{-\infty}^{+\infty} \left(2 \cosh \frac{2\sqrt{\theta_j^2}}{\sigma_w} t\right)^2 e^{-t^2} \times \left(e^{-2\theta_j t} + e^{2\theta_j t}\right) dt - m_j^2,$$

$$s_j = \frac{\theta_j^2}{2\sqrt{\pi}} \int_{-\infty}^{+\infty} \left(2 \cosh \frac{2\sqrt{\theta_j^2}}{\sigma_w} t\right)^3 e^{-t^2} \times \left(e^{-2\theta_j t} + e^{2\theta_j t}\right) dt - (m_j v_j + m_j^2) v_j^{-\frac{3}{2}},$$

where $\theta_0 = 0$ and $\theta_1 = \sqrt{P_0/\sigma_w^2}$. By approximating the Hyperbolic cosine as $\cosh x \approx \frac{x^2}{2}$ for $0 < x < 1$ and $\ln \cosh x \approx x - \ln 2$ for $x > 1$, $m_j$, $v_j$ and $s_j$ can be obtained in closed-form expressions, which are eliminated here due to the space limitation.

Step 3: Determine the distribution of $\sum_{i=1}^{n} \ln v[i]$.

Following [24], we approximate $\sum_{i=1}^{n} \ln v[i]$ as skew-normal distributed random variables. A skew-normal distribution is determined by the positive real scale parameter $\sigma$, the location parameter $\mu$, and the shape parameter $\alpha$. They are respectively given by

$$\mu_j = M_j - \frac{2V_j}{\sqrt{2(4-\pi)}} \sqrt{\frac{s_j}{S_j}} \frac{\pi}{\pi - 2},$$

$$\alpha_j^2 = \frac{\sqrt{2(4-\pi)}}{S_j} \left(\frac{\sqrt{2(4-\pi)}}{S_j}\right)^{\frac{3}{2}} \theta_j^2 - \pi^2 + 2,$$

where $M_j$, $V_j$, and $S_j$ are respectively the mean, variance, and skewness of $\sum_{i=1}^{n} \ln v[i]$. Since $\ln v[i]$ are independent and identically distributed random variables, we have $M_j = nm_j$, $V_j = n v_j$ and $S_j = \frac{\sigma_j^2}{n}$.

Following (27), the cdf of $\sum_{i=1}^{n} \ln v[i]$ under $H_j$ is

$$F_{\sum_{i=1}^{n} \ln v[i]|H_j}(x) = \frac{1}{2} \text{erfc} \left[ - \frac{x - nm_j + \sqrt{2\nu v_j (c_j + 2)}}{\sqrt{2\nu v_j (c_j + 2)}} \right] - 2T \left[ \frac{x - nm_j + \sqrt{2\nu v_j (c_j + 2)}}{\sqrt{\nu v_j (c_j + 2)}}, \frac{\pi}{c_j - \pi^2 + 2} \right].$$

Step 4: Following (28), for a fixed threshold $\lambda$, we derive the false alarm probability in (20) and miss detection probability in (21). This completes the proof of this theorem.