IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received July 14, 2020, accepted July 23, 2020, date of publication August 5, 2020, date of current version August 21, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3014426

Analysis of Blind Frame Recognition and Synchronization Based on Sync Word Periodicity

YONG-SUNG KIL[1], (Graduate Student Member, IEEE), HYUNJAE LEE[1], (Graduate Student Member, IEEE), SANG-HYO KIM[1], (Member, IEEE), AND SEOK-HO CHANG[2], (Senior Member, IEEE)

[1]Department of Electrical and Computer Engineering, Sungkyunkwan University, Suwon 16419, South Korea
[2]Department of Smart ICT Engineering, Konkuk University, Seoul 05029, South Korea

Corresponding author: Sang-Hyo Kim (iamshkim@skku.edu)

This work was supported by the research fund of Signal Intelligence Research Center supervised by Defense Acquisition Program Administration and Agency for Defense Development of Korea.

ABSTRACT Blind recognition of communication parameters has been studied for various applications including cognitive radios, non-cooperative communications, electronic warfare, etc. In this article, the identification of frame information, such as frame length and synchronization word (SW), and frame synchronization, is addressed over the wiretap channel, where no prior information of the frame structure is available, but only the existence of a repeated SW is known. Modifying the previous study, we propose two blind frame recognition and synchronization algorithms based on the correlation between two distinct windows of the received signal as well as the mean of periodic samples. The algorithms run in two steps. A multiple of frame length is estimated via the correlation and then other frame parameters are acquired using the mean of periodic samples with the estimate. Asymptotic analysis of the first algorithm shows that the error probability of estimation vanishes as the received data increases both in noiseless and noisy transmissions. The second algorithm improves the performance in the limited received data scenario. Simulation results as well as complexity analysis of the proposed algorithm are also shown.

INDEX TERMS Blind frame synchronization, correlation, frame recognition, non-cooperative communication, synchronization word.

I. INTRODUCTION

In digital communication systems, data are transmitted in units of frames, and they are recovered at the receiver through proper digital signal processing techniques. Among these techniques, frame synchronization is a process that identifies the time alignment of frames in the received signal stream [1]–[4]. Frame synchronization should be acquired before data recovery at the receiver. A usual assumption pertaining in most of the previous works on frame synchronization is that the receiver has the knowledge of frame information such as the frame length, the synchronization word (SW), and the specification of employed channel codes. However, if a receiving end is an adversary or a cognitive device with non-cooperative services, blind recognition of communication parameters should precede the information acquisition [5]–[14].

Electronic and information warfare is a typical scenario where data from adversary is a crucial resource that gives advantage in battlefield. Electronic warfare consists of actions such as electronic support, electronic attack, and electronic protect [15]. Among them, the electronic support refers to actions intercepting transmissions of adversary, which may contain helpful information for conducting tactical operations. To leverage such intercepted signals, locating data from a stream of intercepted signal is required. As data

The associate editor coordinating the review of this manuscript and approving it for publication was Abdel-Hamid Soliman.

are transmitted in frames, it is necessary to identify the frame structure blindly above all else.

In this article, we deal with the signal intercepted from a communication source. Such a scenario can be modeled by a wiretap channel where a source and a destination are communicated while an eavesdropper tries to listen to ongoing transmission [16]. Various studies have considered the wiretap channel model for the eavesdropping attack scenario [16]–[25]. The secrecy capacity of wiretap channels were analyzed in [16]–[18]. Secrecy enhancement of transmitted signals in multiple antenna systems were developed in [19], [22], where the key idea is to increase the difference between the signal strength for the legitimate receiver and that for the eavesdropper using beamforming techniques. Cooperative jamming for the wireless medium by other helper nodes can increase the security [23]. Secure coding schemes also provide security and can achieve the secrecy capacity [24]. As opposed to the secrecy schemes, the pilot spoofing attack were presented in [25], where an eavesdropper recognizes the training sequence and transmits the estimated one for the purpose of signal leakage to the eavesdropper. In this article, the wiretap channel model is considered where the receiver and the eavesdropper receive the transmitted signal possibly corrupted by Gaussian noise.

Before addressing the blind setting, we review frame synchronization techniques under normal communication environment. Early studies on frame synchronization assumed that a frame consists of a single SW and data of a fixed length, and that the frame structure is known or provided beforehand via a control channel to the receiver [1]–[4]. Barker [1] showed that the optimal metric of frame synchronization over binary symmetric channel is the correlation between the SW and the received signal stream. Massey [2] found that the correlation rule is suboptimal for additive white Gaussian noise (AWGN) channels. He proposed the optimal maximum likelihood (ML) rule for the AWGN channel, which is a modification of the standard correlation rule with a nonlinear correction term that accounts for the presence of random data surrounding the SW. High and low signal-to-noise ratio (SNR) approximation rules were also proposed in [2]. Massey's frame synchronization rules [2] were extensively simulated by Nielsen [3], and it was shown that the high-SNR approximation rule exhibits a similar performance to the optimal rule over a wide range of SNR. It was also shown in [3] that the probability of frame synchronization error is lower-bounded by the probability of the occurrence of the SW pattern in the data region. The ML rule and the lower bound were generalized to M-ary phase-coherent and phase-noncoherent signalings [4].

In addition to the above works on generic frame synchronization, a number of frame synchronization techniques were developed for frames with some special features [26]–[33]. Specifically, frames with variable length were considered in [26]–[28], where sequential hypothesis tests were conducted to determine the presence of the SW pattern in the observation window. Especially, unknown and asymmetric data distributions were assumed in [27] and [28], respectively. Identification and location detection of SW by means of a predefined set of candidate SWs was addressed in [29]. Joint synchronization and channel decoding for the purpose of improving the synchronization performance was studied in [30], [31]. Frame synchronization with no SW but with only the decoding results was proposed in [32], [33].

The above frame synchronization techniques require a presharing of communication parameters such as the frame structure and transmission schemes by using a separate control channel. In contrast, there are various scenarios in which the communication parameters are not known at the receiver, and thus they should be blindly recognized [5]–[8]. For example, in cognitive radio systems, the receiver adapts to a specific transmission context and blindly estimates transmitter parameters for self-reconfiguration purposes [5], [6]. As another example, in adaptive modulation and coding schemes, the transmitter changes its modulation and coding schemes on the fly according to the state of the channel, and this can be conducted without explicit signaling of related parameters [7]. In non-cooperative applications such as electronic warfare, signal interception and processing via wiretap channels are key tasks for tactical operations [8].

Numerous studies have been conducted to blindly recognize communication parameters, where methodologies therein can readily be applied to the eavesdropping attack scenario. Methods for detecting the number of transmit antennas were studied in [34]. For blind modulation recognition, likelihood-based and feature-based modulation classification schemes were proposed in [6], [9], respectively. A comprehensive summary for blind modulation recognition was provided in [35]. On the other hand, the blind estimation of channel coding parameters have been studied for binary linear codes [36], convolutional codes [5], and Reed-Solomon codes [14]. Meanwhile, blind interleaver detection and blind equalization were also investigated in [38] and in [39], respectively.

Regarding frame synchronization, some blind frame recognition methods were devised in [10]–[12] where the unknown parameters of interest there in are only the frame length, SW, and delay. In [10], the blind recognition of frame length and SW pattern was first introduced. A two-step algorithm was proposed, in which the cross-correlation of two windows of the received signal was used to estimate the frame length first, and the SW was estimated from the mean of the received symbols that are sampled with the period of the estimated frame length. However, explicit rules for estimating the frame information and the analysis of the algorithm were missing. The algorithms proposed in [11], [12] are mainly based on the mean of periodically sampled symbols [10]. Their algorithms, however, assumed the knowledge of the minimum length of frame, which cannot be utilized in purely non-cooperative communications, and analysis on the algorithms were also missing.

In this article, we present an extended work related to the algorithm proposed in [10]. Specifically, we mathematically

analyze the correlation function and mean of periodic samples. We then propose a frame parameter estimation and frame synchronization algorithm. In contrast to the method proposed in [10], we estimate a multiple of frame length instead of the exact frame length, and estimate all frame parameters using the mean of periodically sampled symbols. The error performance of the proposed algorithm and its asymptotic behavior are also analyzed. We also present another frame parameter estimation algorithm, which is a practical modification of the first algorithm for the purpose of use in the limited received data scenario. The modified algorithm improves the estimation performance.

The remainder of this article is organized as follows. In Section II, some relevant notations and the system model are given. In Section III, we present our blind frame recognition algorithm (Algorithm 1) and two key functions, i.e., the correlation function and the mean of periodic samples. We then prove the asymptotic behavior of the proposed algorithm under the noiseless wiretap channel and provide complexity analysis of the algorithm in Section IV. Our theoretical results are extended to Gaussian wiretap channel in Section V. Subsequently, we propose a more practical algorithm for the limited data scenario (Algorithm 2) in Section VI. The simulation results are presented in Section VII, both for Algorithms 1 and 2. Section VIII concludes the study.

II. PRELIMINARIES

A. NOTATIONS

An italic letter indicates a scalar (e.g., a or A). A boldface lower-case letter represents a vector (e.g., $\mathbf{a}$). A calligraphic letter shows a set of scalar values (e.g., $\mathcal{A}$), and $|\cdot|$ denotes the set cardinality. The n-th smallest element of $\mathcal{A}$ is written as $\mathcal{A}_{(n)}$, satisfying $\mathcal{A}_{(1)} \le \mathcal{A}_{(2)} \le \ldots \le \mathcal{A}_{(|\mathcal{A}|)}$. For two vectors $\mathbf{a} = (a_0, \ldots, a_{N-1})$ and $\mathbf{b} = (b_0, \ldots, b_{N-1})$ of length N, the correlation between $\mathbf{a}$ and b is written as

$$C(\mathbf{a}, \mathbf{b}) = \frac{1}{N} \sum_{i=0}^{N-1} a_i b_i.$$

For $0 \le j \le N$, the aperiodic correlation, or the partial correlation function, of $\mathbf{a}$ and b is given by

$$C(\mathbf{a}, \mathbf{b}; j) = \frac{1}{N} \sum_{i=0}^{N-j-1} a_i b_{i+j}.$$

For an integer i and a positive integer j, a modulo operation is defined as $(i)_j = (i + kj) \mod j$, where k is the smallest non-negative integer that satisfies $i + kj \ge 0$. A binomial random variable with n trials and a probability of success 0.5 is denoted by B_n. A sign function of a real number x is defined as

$$\mathrm{sgn}(x) = \begin{cases} -1, & \text{for } x < 0, \\ 0, & \text{for } x = 0, \\ 1, & \text{for } x > 0. \end{cases}$$

B. SYSTEM MODEL

We address the blind frame recognition problem in the Gaussian wiretap channel depicted in Fig. 1. The system model is shown in Figs. 1 and 2, where communication frames of the same size, each of which contains the same SW, are continuously transmitted from a source to the legitimate receiver. Meanwhile, the eavesdropper, who is aware of the existence of SW but does not know the frame length, SW, and its length, observes the transmitted signal passing through the wiretap channel. The eavesdropper estimates the frame parameters to acquire synchronization from the received data stream. The transmitted signal stream is denoted by $\mathbf{x}$, and an eavesdropper and the legitimate receiver receive the signal stream $\mathbf{y}$ and $\mathbf{z}$, respectively.

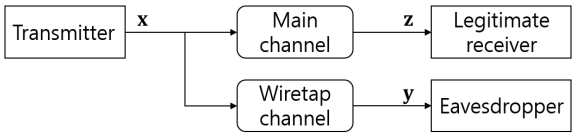


FIGURE 1. A wiretap channel model: a transmitter sends signal stream x to the legitimate receiver and an eavesdropper and the legitimate receiver receive the signal stream y and z through main and wiretap channels, respectively.

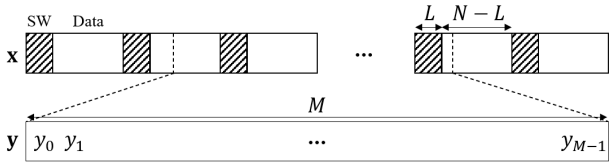


FIGURE 2. Frame structure, transmitted signal stream and received signal stream.

The frame structure, transmitted signal, and received signal are depicted in Fig. 2. A frame of length N consists of SW, denoted by $\mathbf{s} = (s_0, s_1, \ldots, s_{L-1}) \in \{1, -1\}^L$, of length L and the following data of length $N - L$. The ratio of SW is denoted by $r = L/N$. Assume that the data symbols are independent and identically distributed (i.i.d.) equiprobable binary random variables taken from $\{1, -1\}$.

It is assumed that $\mathbf{x} = (x_0, x_1, \ldots)$ is transmitted continuously, where $x_i \in \{1, -1\}$, and the eavesdropper takes a truncated signal of length M to process. Let the received signals at the eavesdropper, $\mathbf{y} = (y_0, y_1, \ldots, y_{M-1})$, be

$$y_i = x_{jN-T+i} + n_i, \quad i = 0, 1, \ldots, M-1, \tag{1}$$

where $\mathbf{n} = (n_0, n_1, \ldots, n_{M-1})$ is a Gaussian noise vector with i.i.d. elements of zero mean and variance σ^2, so that SNR is given by $E_s/N_0 = 1/(2\sigma^2)$, where $N_0/2$ is the two-sided noise power spectral density. In (1), j is a positive integer, and $T \in \{0, 1, \ldots, N-1\}$ is the delay, which corresponds to the time difference between the first received symbol and the earliest symbol in the next frame. We assume that the received signal length is much longer than the frame length; that is, $M \gg N$. Our goal is to estimate the repetitive SW $\mathbf{s}$ and

its length L, the frame length N, and the delay T from the received signal $\mathbf{y}$ at the eavesdropper side.

III. BLIND FRAME RECOGNITION AND SYNCHRONIZATION

In the past works on frame synchronization for the scenario where frame structures are known at the receiver [1]–[4], the cross-correlation of known SW and the received symbols is the key metric to acquire frame synchronization. However, in blind scenarios where the receiver has no information on the frame structure, the detection of the frame length and SW should precede the synchronization process.

In a previous work on blind frame recognition [10], a two-step blind frame recognition and synchronization technique was proposed. In the first step, the receiver exploits the cross-correlation of two non-overlapping windows of the received signal stream to estimate the frame length. In the second step, the mean of symbols sampled with the period of the estimated frame length is used to locate and estimate the SW sequence, and finally to acquire frame synchronization.

In this section, we investigate the correlation function and the mean of periodic samples in the noise-free channel. Then, we propose a new blind frame recognition and synchronization method, which is a refined version of our previous scheme [13]. The analysis of the proposed algorithm and extension to noisy channel are presented in the following subsections.

Under the noise-free channel assumption, the received signal at the eavesdropper is represented as

$$y_i = x_{jN-T+i}, \quad i = 0, 1, \ldots, M-1. \tag{2}$$

Let $\mathcal{S}$ and $\mathcal{D}$ be the sets of indices in y indicating the SW and data symbols, respectively. For $i \in \mathcal{S}$, y_i is an SW symbol, and for $i \in \mathcal{D}$, y_i is a data symbol. It is clear that $\mathcal{S} \cup \mathcal{D} = \{0, 1, \ldots, M-1\}$, and $\mathcal{S} \cap \mathcal{D} = \varnothing$. The received SW symbol can be expressed as

$$y_i = s_{(i-T)_N}, \quad i \in \mathcal{S}. \tag{3}$$

For example, when $N = 10, L = 3, M = 15$, and $T = 2$, we have $\mathcal{S} = \{2, 3, 4, 12, 13, 14\}$ and $y_2 = y_{12} = s_0, y_3 = y_{13} = s_1$, and $y_4 = y_{14} = s_2$.

A. CORRELATION FUNCTION

In this subsection, we investigate the characteristics and asymptotic behaviors of the cross-correlation of sliding windows. Let $\mathbf{w}_m$ be the sequence contained in a window of length W $(0 < W < M)$ in the received symbol stream $\mathbf{y}$, and $m \in \{0, 1, \ldots, M-W\}$ be the index of the earliest symbol in the window. Then, we obtain

$$\begin{aligned}\mathbf{w}_m &= (w_{m,0}, w_{m,1}, \ldots, w_{m,W-1}) \\ &= (y_m, y_{m+1}, \ldots, y_{m+W-1}).\end{aligned}$$

We define $\mathbf{w}_0$ as the reference window. The received symbol stream and window structure are depicted in Fig. 3, where SW is shaded with stripes.

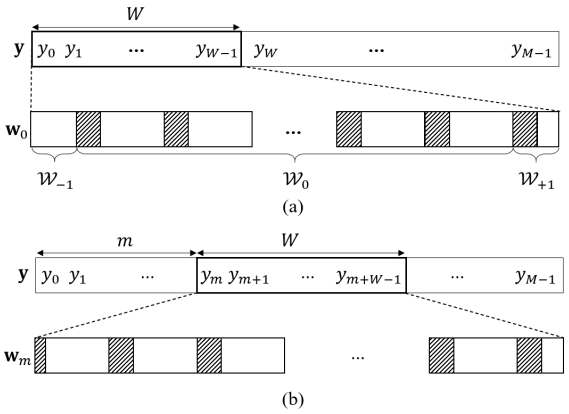


FIGURE 3. Received signal stream and the windows. (a) The reference window $\mathbf{w}_0$. (b) The sliding window $\mathbf{w}_m$.

Let $\mathcal{S}_m$ and $\mathcal{D}_m$ be the sets of indices in $\mathbf{w}_m$ indicating SW and data symbols of $\mathbf{w}_m$, respectively. For $i \in \mathcal{S}_m$, $w_{m,i}$ is an SW symbol, and for $i \in \mathcal{D}_m$, $w_{m,i}$ is a data symbol. Clearly, we have $\mathcal{S}_m \cup \mathcal{D}_m = \{0, 1, \ldots, W-1\}$, and $\mathcal{S}_m \cap \mathcal{D}_m = \varnothing$. We define $\mathcal{W} = \{0, 1, \ldots, W-1\}$ as the index set of a window. Then, $\mathcal{S}_m \cup \mathcal{D}_m = \mathcal{W}$.

We analyze the correlation between the reference window, $\mathbf{w}_0$, and sliding window, $\mathbf{w}_m$ $(1 \le m \le M - W)$. Assuming that window length is greater than frame length (i.e., $W > N$), we first divide the reference window $\mathbf{w}_0$ into two parts of complete frames and residual frames as depicted in Fig. 3(a), where $\mathcal{W}_0$, $\mathcal{W}_{-1}$, and $\mathcal{W}_{+1}$ denote their index sets. Here, $\mathcal{W}_0$ corresponds to the complete frame region (CFR), and $\mathcal{W}_{-1}$ and $\mathcal{W}_{+1}$ correspond to the parts of a frame, which we refer to as the residual frame region (RFR). As shown in Fig. 3(a), we have $\mathcal{W} = \mathcal{W}_{-1} \cup \mathcal{W}_0 \cup \mathcal{W}_{+1}$. Let k be the number of frames in CFR. Then, it can be shown that

$$k = \begin{cases} \lfloor W/N \rfloor - 1, & \text{for } W - N\lfloor W/N \rfloor < T \le N-1, \\ \lfloor W/N \rfloor, & \text{for } 0 \le T \le W - N\lfloor W/N \rfloor, \end{cases} \tag{4}$$

and $|\mathcal{W}_0| = kN$. For RFR, it is clear that $0 \le |\mathcal{W}_{-1}|, |\mathcal{W}_{+1}| \le N-1$ and $|\mathcal{W}_{-1}| = T$. Although any sliding window can be divided into CFR and RFR, we use the terms only for the reference window. From $|\mathcal{W}_0| = kN$ and $0 \le |\mathcal{W}_{-1}|, |\mathcal{W}_{+1}| \le N-1$, we obtain $kN \le W < (k+2)N$. Thus, the number of frames in CFR, k, is bounded as

$$\frac{W-2N}{N} < k \le \frac{W}{N}. \tag{5}$$

The cross-correlation between the reference window $\mathbf{w}_0$ and a sliding window $\mathbf{w}_m$ is given by

$$C(\mathbf{w}_0, \mathbf{w}_m) = \frac{1}{W} \sum_{i=0}^{W-1} w_{0,i} w_{m,i}, \tag{6}$$

and the aperiodic auto-correlation of the SW, $\mathbf{s}$, is given by

$$C(\mathbf{s}, \mathbf{s}; j) = \frac{1}{L} \sum_{i=0}^{L-j-1} s_i s_{i+j}. \tag{7}$$

For $m = 0$, a sliding window is the same as the reference window, and thus we have $C(\mathbf{w}_0, \mathbf{w}_0) = 1$. For $m \geq 1$, $C(\mathbf{w}_0, \mathbf{w}_m)$ is a function of random variables as the data symbols are random.

Theorem 1: For the received signal without any additive noise, given by (2), we have

$$\lim_{W\to\infty} C(\mathbf{w}_0, \mathbf{w}_m) = \begin{cases} 1, & \text{for } m = 0, \\ H(\mathbf{s}; (m)_N), & \text{for } 1 \leq m \leq M - W, \end{cases}$$

where

$$H(\mathbf{s}; j) = \begin{cases} \frac{L}{N} C(\mathbf{s}, \mathbf{s}; j), & \text{for } 0 \leq j < L, \\ 0, & \text{for } L \leq j \leq N - L, \\ \frac{L}{N} C(\mathbf{s}, \mathbf{s}; N - j), & \text{for } N - L < j < N. \end{cases} \quad (8)$$

Proof: It is clear that for $m = 0$, we obtain $C(\mathbf{w}_0, \mathbf{w}_0) = 1$. We next consider the case of $1 \leq m \leq M - W$. The correlation (6) can be split as

$$C(\mathbf{w}_0, \mathbf{w}_m) = \frac{1}{W}\left(\sum_{i\in\mathcal{S}_0\cap\mathcal{S}_m} w_{0,i}w_{m,i} + \sum_{i\in\mathcal{W}\setminus\{\mathcal{S}_0\cap\mathcal{S}_m\}} w_{0,i}w_{m,i} \right). \quad (9)$$

Note that the summand of the first sum is the product of two SW symbols. The first sum can be split into CFR and RFR parts:

$$\sum_{i\in\mathcal{S}_0\cap\mathcal{S}_m} w_{0,i}w_{m,i} = \sum_{i\in\{\mathcal{S}_0\cap\mathcal{S}_m\}\cap\mathcal{W}_0} w_{0,i}w_{m,i} + \sum_{i\in\{\mathcal{S}_0\cap\mathcal{S}_m\}\setminus\mathcal{W}_0} w_{0,i}w_{m,i}. \quad (10)$$

As the SW is repeated in $\mathbf{y}$ with a period N, it follows that $w_{m,i} = w_{(m)_N,i}$ for $i \in \mathcal{S}_{(m)_N}$. The first sum in the right hand side of (10) can be expressed in terms of the aperiodic auto-correlation of the SW given by (7):

$$\begin{aligned} &\sum_{i\in\{\mathcal{S}_0\cap\mathcal{S}_m\}\cap\mathcal{W}_0} w_{0,i}w_{m,i} \\ &= \sum_{i\in\{\mathcal{S}_0\cap\mathcal{S}_{(m)_N}\}\cap\mathcal{W}_0} w_{0,i}w_{(m)_N,i} \\ &= \begin{cases} kLC(\mathbf{s}, \mathbf{s}; (m)_N), & \text{for } 0 \leq (m)_N < L, \\ 0, & \text{for } L \leq (m)_N \leq N - L, \\ kLC(\mathbf{s}, \mathbf{s}; N - (m)_N), & \text{for } N - L < (m)_N < N \end{cases} \\ &= kNH(\mathbf{s}; (m)_N), \end{aligned} \quad (11)$$

where the last line follows from the definition of $H(\mathbf{s}; j)$ given by (8). The second term in the right hand side of (10) is a sum within RFR, and the number of summands is smaller than $2L$. We have $-2L < \sum_{i\in\{\mathcal{S}_0\cap\mathcal{S}_m\}\setminus\mathcal{W}_0} w_{0,i}w_{m,i} < 2L$.

Now, we consider the second sum in (9) where at least one of $w_{0,i}$ and $w_{m,i}$ is a data symbol. Each summand becomes an independent and equiprobable binary random variable and the number of summands is $|\mathcal{W}\setminus\{\mathcal{S}_0 \cap \mathcal{S}_m\}| = W - |\mathcal{S}_0 \cap \mathcal{S}_m|$. The sum can be represented in terms of a binomial random variable as

$$\sum_{i\in\mathcal{W}\setminus\{\mathcal{S}_0\cap\mathcal{S}_m\}} w_{0,i}w_{m,i} = 2\mathrm{B}_{W-|\mathcal{S}_0\cap\mathcal{S}_m|} - (W - |\mathcal{S}_0 \cap \mathcal{S}_m|), \quad (12)$$

where $\mathrm{B}_{W-|\mathcal{S}_0\cap\mathcal{S}_m|} \sim \mathcal{B}\left(W - |\mathcal{S}_0 \cap \mathcal{S}_m|, \frac{1}{2}\right)$. Then, the cross-correlation is represented as

$$\begin{aligned} C(\mathbf{w}_0, \mathbf{w}_m) = \frac{1}{W}\Bigg(&kNH(\mathbf{s}; (m)_N) + \sum_{i\in\{\mathcal{S}_0\cap\mathcal{S}_m\}\setminus\mathcal{W}_0} w_{0,i}w_{m,i} \\ &+ 2\mathrm{B}_{W-|\mathcal{S}_0\cap\mathcal{S}_m|} - (W - |\mathcal{S}_0 \cap \mathcal{S}_m|) \Bigg), \end{aligned} \quad (13)$$

where $\mathrm{B}_{W-|\mathcal{S}_0\cap\mathcal{S}_m|}$ is the only random variable. By the law of large numbers, we have

$$\lim_{W\to\infty} \frac{1}{W}\left(2\mathrm{B}_{W-|\mathcal{S}_0\cap\mathcal{S}_m|} - (W - |\mathcal{S}_0 \cap \mathcal{S}_m|)\right) = 0.$$

Finally, we obtain

$$\begin{aligned} &\lim_{W\to\infty} C(\mathbf{w}_0, \mathbf{w}_m) \\ &= \lim_{W\to\infty} \frac{1}{W}\Bigg(kNH(\mathbf{s}; (m)_N) + \sum_{i\in\{\mathcal{S}_0\cap\mathcal{S}_m\}\setminus\mathcal{W}_0} w_{0,i}w_{m,i} \\ &\quad + 2\mathrm{B}_{W-|\mathcal{S}_0\cap\mathcal{S}_m|} - (W - |\mathcal{S}_0 \cap \mathcal{S}_m|) \Bigg) \\ &= H(\mathbf{s}; (m)_N). \end{aligned}$$

■

Note that $C(\mathbf{w}_0, \mathbf{w}_m)$ can be divided into a deterministic part and a random part as in (13). If $m = 0$, the correlation marks the inphase auto-correlation of the reference window and the random part is empty, indicating that $C(\mathbf{w}_0, \mathbf{w}_0) = 1$, and we call this as the trivial peak. If $m \neq 0$, the correlation function remains a random variable being biased by the deterministic part. Some properties of $H(\mathbf{s}; j)$ are easily derived.

Proposition 1: For $0 < j < L$, we obtain $|H(\mathbf{s}; j)| \leq (L - j)/N$, and $H(\mathbf{s}; 0) = L/N$.

Due to Proposition 1, $H(\mathbf{s}; j)$ has a unique peak at $j = 0$, irrelevant to the SW realization. Lemma 1 shows that the correlation of SW-matched windows is distinguishable with a high probability asymptotically.

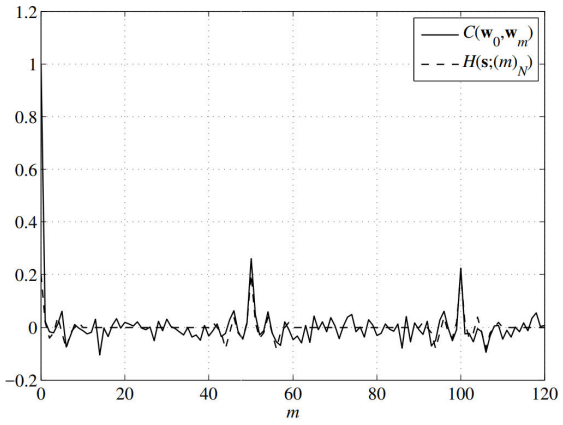
Lemma 1: For nonzero integers m_1 and m_2 satisfying $(m_1)_N = 0$ and $(m_2)_N \neq 0$, we have

$$\lim_{W\to\infty} (C(\mathbf{w}_0, \mathbf{w}_{m_1}) - C(\mathbf{w}_0, \mathbf{w}_{m_2})) \geq \frac{1}{N}.$$

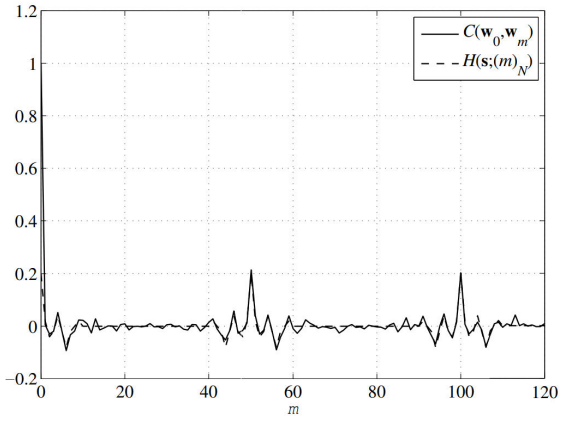
Proof: From Theorem 1 and Proposition 1, it follows that

$$\begin{aligned} &\lim_{W\to\infty} (C(\mathbf{w}_0, \mathbf{w}_{m_1}) - C(\mathbf{w}_0, \mathbf{w}_{m_2})) \\ &= H(\mathbf{s}; 0) - H(\mathbf{s}; (m_2)_N) \\ &\geq \frac{1}{N}. \end{aligned}$$

■



(a)



(b)

FIGURE 4. Convergence behavior of $C(\mathbf{w}_0, \mathbf{w}_m)$ to $H(\mathbf{s}; (m)_N)$ for (a) $W = 1000$, (b) $W = 5000$.

Note that the properties hold for an arbitrary choice of $\mathbf{s}$. The convergence of $C(\mathbf{w}_0, \mathbf{w}_m)$ to $H(\mathbf{s}; (m)_N)$ for $m > 0$ is shown in Fig. 4. The frame length and pseudo random SW are set as $N = 50$, $\mathbf{s} = (-1, 1, 1, 1, -1, 1, 1, -1, -1, -1)$, and $L = 10$. The size of the windows is set to $W = 1000$ for Fig. 4(a) and $W = 5000$ for Fig. 4(b). In the figures, both correlations have the trivial peak $C(\mathbf{w}_0, \mathbf{w}_0) = 1$. The overall difference between $C(\mathbf{w}_0, \mathbf{w}_m)$ and $H(\mathbf{s}; (m)_N)$ becomes smaller as W increases. The peaks of $H(\mathbf{s}; (m)_N)$ appear periodically with a period of the frame length N. Hence, if W is sufficiently large, the index of the highest peak, or the most reliable peak, of $C(\mathbf{w}_0, \mathbf{w}_m)$ apart from the trivial one is the frame length or its multiple with high probability.

Corollary 1: For $m > 0$, the expectation and variance of the correlation are

$$E\left[C(\mathbf{w}_0, \mathbf{w}_m)\right] = \frac{1}{W}\left(\sum_{i\in\mathcal{S}_0\cap\mathcal{S}_m} w_{0,i}w_{m,i}\right), \tag{14}$$

and

$$\mathrm{VAR}\left[C(\mathbf{w}_0, \mathbf{w}_m)\right] = \frac{W - |\mathcal{S}_0 \cap \mathcal{S}_m|}{W^2}. \tag{15}$$

Proof: The correlation can be split as (9). For $i \in \mathcal{S}_0 \cap \mathcal{S}_m$, both $w_{0,i}$ and $w_{m,i}$ are SW symbols.

$$E\left[\sum_{i\in\mathcal{S}_0\cap\mathcal{S}_m} w_{0,i}w_{m,i}\right] = \sum_{i\in\mathcal{S}_0\cap\mathcal{S}_m} w_{0,i}w_{m,i},$$
$$\mathrm{VAR}\left[\sum_{i\in\mathcal{S}_0\cap\mathcal{S}_m} w_{0,i}w_{m,i}\right] = 0.$$

For $i \in \mathcal{W}\backslash\{\mathcal{S}_0 \cap \mathcal{S}_m\}$, at least one of $w_{0,i}$ and $w_{m,i}$ is a data symbol, where we can exploit (12).

$$E\left[\sum_{i\in\mathcal{W}\backslash\{\mathcal{S}_0\cap\mathcal{S}_m\}} w_{0,i}w_{m,i}\right] = 0,$$
$$\mathrm{VAR}\left[\sum_{i\in\mathcal{W}\backslash\{\mathcal{S}_0\cap\mathcal{S}_m\}} w_{0,i}w_{m,i}\right] = W - |\mathcal{S}_0 \cap \mathcal{S}_m|.$$

■

The following corollary presents a lower bound of the difference of expected the SW-matched correlation to the SW-mismatched correlation.

Corollary 2: For nonzero integers m_1 and m_2 satisfying $(m_1)_N = 0$ and $(m_2)_N \neq 0$, we have

$$E\left[C(\mathbf{w}_0, \mathbf{w}_{m_1})\right] - E\left[C(\mathbf{w}_0, \mathbf{w}_{m_2})\right] > \frac{1}{N} - \frac{2}{W}. \tag{16}$$

Proof:

$$\begin{aligned}
&E\left[C(\mathbf{w}_0, \mathbf{w}_{m_1})\right] - E\left[C(\mathbf{w}_0, \mathbf{w}_{m_2})\right] \\
&\overset{(a)}{=} \frac{1}{W}\left(\sum_{i\in\mathcal{S}_0\cap\mathcal{S}_{m_1}} w_{0,i}w_{m_1,i} - \sum_{i\in\mathcal{S}_0\cap\mathcal{S}_{m_2}} w_{0,i}w_{m_2,i}\right) \\
&\overset{(b)}{=} \frac{1}{W}\Bigg(kNH(\mathbf{s};(m_1)_N) + \sum_{i\in\{\mathcal{S}_0\cap\mathcal{S}_{m_1}\}\cap\mathcal{W}_0} w_{0,i}w_{m_1,i} \\
&\qquad - kNH(\mathbf{s};(m_2)_N) - \sum_{i\in\{\mathcal{S}_0\cap\mathcal{S}_{m_2}\}\cap\mathcal{W}_0} w_{0,i}w_{m_2,i}\Bigg) \\
&\overset{(c)}{\geq} \frac{1}{W}\left(k + |\mathcal{S}_0| - \left|\mathcal{S}_0 \cap \mathcal{S}_{m_2}\right|\right) \\
&\overset{(d)}{>} \frac{1}{N} - \frac{2}{W},
\end{aligned}$$

where (a) follows from Corollary 1, (b) follows from (10) and (11), (c) follows from Proposition 1 and $\mathcal{S}_m = \mathcal{S}_{(m)_N}$, and (d) follows from (5). ■

B. MEAN OF PERIODIC SAMPLES

In this subsection, we investigate the mean of periodic samples of the received signal $\mathbf{y}$, which was used in [10] for

detecting the values of the SW $\mathbf{s}$ and its length L. The mean of periodic samples is defined as

$$D_p(l) = \frac{1}{d}\sum_{i=0}^{d-1} y_{l+ip},$$

where $0 \le l \le p-1$, p is the sampling period, and $d = \lfloor \frac{M}{p} \rfloor$ is the number of samples in the sum. The following theorem presents the asymptotic convergence of $D_p(l)$.

Theorem 2: For the received signal without additive noise, given in (2), if $(p)_N = 0$, we have

$$\lim_{M\to\infty} D_p(l) = \begin{cases} s_{(l-T)_N}, & \text{for } l \in [0, p-1] \cap \mathcal{S}, \\ 0, & \text{for } l \in [0, p-1] \cap \mathcal{D}. \end{cases}$$

Otherwise (i.e., $(p)_N \neq 0$), we obtain

$$\left| \lim_{M\to\infty} D_p(l) \right| \le \frac{\lceil L/\gcd(p,N) \rceil}{N/\gcd(p,N)}.$$

Proof: We first consider the case of $(p)_N = 0$. If $l \in [0, p-1] \cap \mathcal{S}$, then $y_{l+ip} = s_{(l-T)_N}$ follows from (3). Hence, for $l \in [0, p-1] \cap \mathcal{S}$, we have $D_p(l) = s_{(l-T)_N}$, and

$$\lim_{M\to\infty} D_p(l) = s_{(l-T)_N}.$$

If $l \in [0, p-1] \cap \mathcal{D}$, then y_{l+ip} is an independent and equiprobable binary random variable. We can represent $D_p(l)$ as

$$D_p(l) = \frac{1}{d}\left(2\mathrm{B}_d - d\right). \tag{17}$$

By the law of large numbers,

$$\lim_{M\to\infty} D_p(l) = \lim_{d\to\infty} \tfrac{1}{d}\left(2\mathrm{B}_d - d\right) = 0.$$

Now, we consider the case of $(p)_N \neq 0$. We are interested in the frame indices of the sampled symbols and the fraction of fixed SW symbols that contribute to the sample sum. Let $b = (l - T)_N$, which is the frame perspective bias of the sampling. If $\gcd(p, N) = 1$, as p is a generator of the cyclic group $\{0, 1, \ldots, N-1\}$, then

$$\{(qp+b)_N \,|\, 0 \le q \le N-1\} = \{0, 1, \ldots, N-1\} = Z_N, \tag{18}$$

for any $b \in \{0, 1, \ldots, N-1\}$ (we can use the notation Z_n instead). The sampler in (18) accesses all the symbol indices in the frame regularly with the period of N. More generally, assume $g = \gcd(p, N)$ and let $p = gp_1$ and $N = gN_1$, where p_1 and N_1 are coprime. We have

$$\{(qp)_N \,|\, 0 \le q \le N-1\} = \{0, g, \ldots, N-g\},$$

where $G = \{0, g, \ldots, N-g\}$ is a subgroup of Z_N of order N/g. Therefore,

$$\{(qp+b)_N \,|\, 0 \le q \le N-1\} = \{b', g+b', \ldots, N-g+b'\},$$

where $b' = b \mod g$. Hence, the sampler accesses only N_1 symbol indices of the frame regularly. The fraction of sampling of SW symbols is smaller than or equal to $\lceil L/g \rceil / N_1$, which is smaller than one if $L < N/2$. It is apparent that

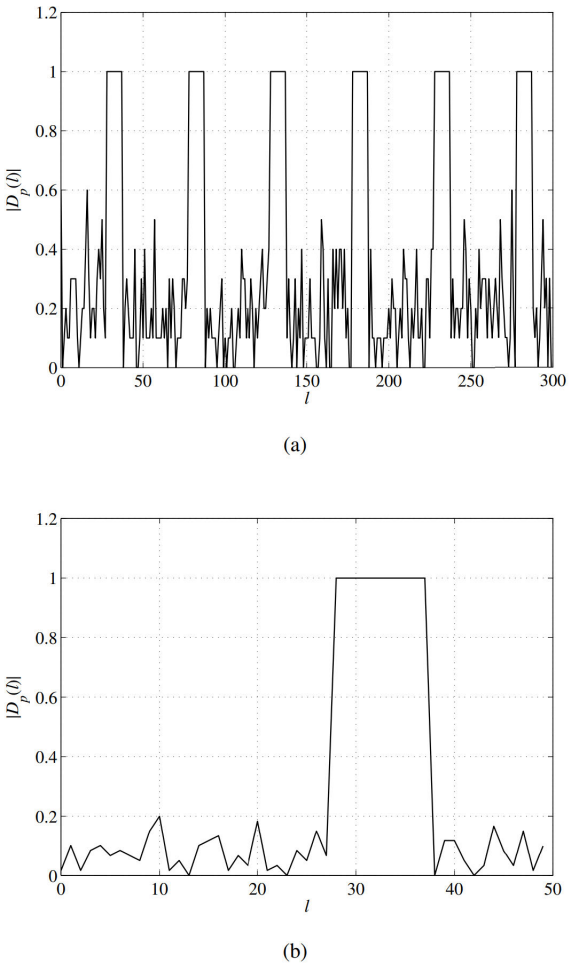


FIGURE 5. Absolute mean of periodic samples $|D_p(l)|$ for (a) $p = 300$, (b) $p = 50$.

the absolute value of the mean of periodic samples does not exceed $\lceil L/g \rceil / (N/g)$ asymptotically:

$$\left| \lim_{M\to\infty} D_p(l) \right| \le \frac{\lceil L/g \rceil}{N/g},$$

with equality if the SW is the all-ones sequence. ■

It has been shown that, if the sampling period is a multiple of the frame length, the mean of periodic samples converges to the corresponding SW or zero. Assuming that we can obtain a sufficiently long signal and a small multiple of the frame length, this converging behavior guarantees the acquisition of the SW, its position, and interval, which is equal to the exact frame length.

The convergence behavior of $|D_p(l)|$, which is related to Theorem 2, is exhibited in Fig. 5. We consider the same frame length and SW as those used in Fig. 4. Here, we set the sampling period p to 300 and 50, which are 5 times as large as and equal to the frame length, respectively. As the sampling periods p are multiples of the frame length (or frame length itself), if $l \in \mathcal{S}$, then the periodically collected samples are all SW symbols with the same sign. In contrast, if $l \in \mathcal{D}$, then the samples to be averaged are

all randomly generated data symbols. Note that, a smaller p draws a larger d, which is the number of samples to be averaged out. Hence, a smaller p, being a multiple of the frame length, leads to a smaller average $|D_p(l_{\in\mathcal{D}})|$ and makes the discrimination between $|D_p(l_{\in\mathcal{D}})|$ and $|D_p(l_{\in\mathcal{S}})|$ easier.

Until now, we have discussed the asymptotic behavior of the correlation and the mean of periodic samples. In the following section, a blind frame recognition method will be proposed, which utilizes these results.

C. PROPOSED BLIND FRAME RECOGNITION METHOD

We propose an algorithm that targets an asymptotic setting first. The algorithm is a two-step approach, which is a modified version of that proposed in [10]. In [10], the exact frame length was estimated by averaging the intervals of consecutive peaks through the correlation function. Other frame parameters, such as the SW and the length of a frame, and the delay were estimated using the absolute mean of periodic samples subsequently. However, while choosing the successive peaks of correlation, if some of the successive peaks are not selected or some improper peaks are included, the estimation of frame length may fail. Furthermore, as neither the number nor the minimum value of the proper peaks are provided to the eavesdropper, no explicit method to select helpful peaks from all the peaks for some frame information was provided. We claim through Algorithm 1 that setting a frame length multiple by choosing a single peak of the correlation first, and then estimating all other parameters with the mean of periodic samples is an effective approach.

The proposed blind frame recognition algorithm is described in Algorithm 1. The algorithm is designed for estimating the information of finite-length frames so that it is assumed that $N \le N_{\max}$ for a finite $N_{\max}$. The algorithm takes the input of the received signal stream $\mathbf{y}$ and parameters $N_{\max}$ and η, and outputs an estimation of the frame length $\hat{N}$, the delay $\hat{T}$, the SW $\hat{\mathbf{s}}$ and its length $\hat{L}$. In the first step, the algorithm estimates a small multiple of the frame length p. The window length is set to $M - N_{\max}$ in line 1. In line 2, p is set to the index of the largest peak of $C(\mathbf{w}_0, \mathbf{w}_m)$ excluding $C(\mathbf{w}_0, \mathbf{w}_0) = 1$. This is one of differences from [10] in that we choose the single highest peak instead of multiple peaks from $C(\mathbf{w}_0, \mathbf{w}_m)$ for $m > 0$, which improves the performance of the first step of the algorithm.

In the second step, the frame parameters are estimated with $D_p(l)$. If the first step is successful, p is an integer multiple of N. Then, for $l \in [0, p-1] \cap \mathcal{S}$, $|D_p(l)| = 1$ because the summands of $|D_p(l)|$ are all the same SW symbols. For $l \in [0, p-1] \cap \mathcal{D}$, $|D_p(l)| < 1$ with a high probability as the summands of $|D_p(l)|$ are all random data. We detect the rising and falling edges of $|D_p(l)|$ to estimate the SW and frame length. In line 3, the index sets of the rising and falling edges, $\mathcal{R}$ and $\mathcal{F}$, respectively, are determined with an edge detection threshold η:

$$\mathcal{R} = \{l \,|\, |D_p((l-1)_p)| < \eta \le |D_p(l)|, l \in [0, p-1]\},$$
$$\mathcal{F} = \{l \,|\, |D_p(l)| < \eta \le |D_p(l-1)_p|, l \in [0, p-1]\}.$$

Algorithm 1 Blind Frame Recognition and Synchronization

Input: $\mathbf{y}, N_{\max}, \eta$;
Output: $\hat{N}, \hat{T}, \hat{L}, \hat{\mathbf{s}}$;
\\ Step 1: Estimation of frame length multiple p
1: $W \leftarrow M - N_{\max}$, compute $C(\mathbf{w}_0, \mathbf{w}_m)$ for $m \in [0, N_{\max}]$;
2: $p \leftarrow \arg \max_{m \in [1, N_{\max}]} C(\mathbf{w}_0, \mathbf{w}_m)$, compute $D_p(l)$ for $l \in [0, p-1]$;
\\ Step 2: Detection of frame length, SW, and delay
3: set the index sets of rising and falling edges, $\mathcal{R}$ and $\mathcal{F}$, from $|D_p(l)|$;
4: **if** $|\mathcal{R}| = 1$ **then**
5: $\quad \hat{N} \leftarrow p$;
6: **else if** $|\mathcal{R}| > 1$ **then**
7: $\quad \hat{N} \leftarrow \mathcal{R}_{(2)} - \mathcal{R}_{(1)}$;
8: **end if**
9: $\hat{T} \leftarrow \mathcal{R}_{(1)}$;
10: $\hat{L} \leftarrow \left(\mathcal{F}_{(1)} - \mathcal{R}_{(1)}\right)_{\hat{N}}$;
11: **for** $l = 0, \ldots, \hat{L} - 1$ **do**
12: $\quad \hat{s}_l \leftarrow \mathrm{sgn}(D_p((\hat{T} + l)_p))$;
13: **end for**

The above predicates provide the same number of rising and falling edges. The rising and falling edge instants provide the start and end indices of the SWs in the received signals, respectively. For $p = N$ with proper η, there is a single rising edge and a single falling edge regarding SW. If $p = iN$ where $i > 1$, there are more than one rising and falling edges. Hence, depending on the size of $\mathcal{R}$, the frame length estimate $\hat{N}$ is obtained in lines 4-8. The delay is estimated by the value of the first rising edge instant in line 9. The length of the SW is estimated by the distance from the first rising edge to the nearest falling edge and the SW is estimated by corresponding signs of $D_p(l)$ in lines 10-13.

IV. ANALYSIS OF ALGORITHM 1

In this section, we analyze the estimation error probability of Algorithm 1. Subsequently, it is proved that the proposed algorithm works well asymptotically; the error probability approaches zero. Then the computational complexity of Algorithm 1 is given.

Let the estimation error probability of Algorithm 1 be P_{e} and the probability of correct estimation be $P_{\mathrm{c}} = 1 - P_{\mathrm{e}}$. Then, P_{e} is bounded as

$$\begin{aligned} P_{\mathrm{e}} &= 1 - P_{\mathrm{c}} \\ &= 1 - P\left(\hat{N} = N, \hat{L} = L, \hat{\mathbf{s}} = \mathbf{s}, \hat{T} = T\right) \\ &\le 1 - P\left((p)_N = 0\right) \\ &\quad \times P\left(\hat{N} = N, \hat{L} = L, \hat{\mathbf{s}} = \mathbf{s}, \hat{T} = T \,|\, (p)_N = 0\right), \end{aligned} \tag{19}$$

where $(p)_N = 0$ is the desired condition for the output of the first step of Algorithm 1. An upper bound of (19) can be

derived with Lemmas 2 and 3, whose proofs are provided in Appendices A and B, respectively.

Lemma 2: The probability that p is a multiple of N is bounded as

$$P\left((p)_N = 0\right) \geq 1 - \frac{4N_{\max}^3 W}{(W - 2N_{\max})^2}. \tag{20}$$

Lemma 3: Given $(p)_N = 0$, the probability of correct estimation of N, L, $\mathbf{s}$, and T is bounded as

$$P\left(\hat{N} = N, \hat{L} = L, \hat{\mathbf{s}} = \mathbf{s}, \hat{T} = T | (p)_N = 0\right) \geq \left(1 - 2\exp\left(-\frac{\eta^2\left(\frac{M}{N_{\max}} - 1\right)}{2}\right)\right)^{N_{\max}}.$$

The following theorem confirms that the error probability of Algorithm 1 converges to zero as the received data increases.

Theorem 3: For the noiseless reception (2), the error probability of estimating $N, L, \mathbf{s}$, and T by Algorithm 1 diminishes as M increases:

$$\lim_{M\to\infty} P_{\mathrm{e}} = 0.$$

Proof: From (19) and Lemmas 2 and 3, we have

$$\begin{aligned}
&\lim_{M\to\infty} P_{\mathrm{e}} \\
&\leq 1 - \lim_{M\to\infty} P\left((p)_N = 0\right) \\
&\quad \times P\left(\hat{N} = N, \hat{L} = L, \hat{\mathbf{s}} = \mathbf{s}, \hat{T} = T | (p)_N = 0\right) \\
&\leq 1 - \lim_{M\to\infty} \left(1 - \frac{4N_{\max}^3 W}{(W - 2N_{\max})^2}\right) \\
&\quad \times \left(1 - 2\exp\left(-\frac{\eta^2}{2}\left(\frac{M}{N_{\max}} - 1\right)\right)\right)^{N_{\max}} \\
&= 0.
\end{aligned}$$

■

Now the analysis of computational complexity of Algorithm 1 is given. The number of computations in Algorithm 1 is affected not only by the length of received signal M and the input parameters $N_{\max}$ and η but also from p, which is determined by the realization of the received signals. Instead of providing the exact number of operations, we evaluate the complexity using $\mathcal{O}(\cdot)$, the big omicron, to show the limiting behaviors.

The overall computational complexity of Algorithm 1 is $\mathcal{O}(MN_{\max})$, which is explained as follows. At first, the correlation, $C(\mathbf{w}_0, \mathbf{w}_m)$, is computed for all $m \in [0, N_{\max}]$. As the size of window is $W = M - N_{\max}$, where $M > N_{\max}$, the computation of $C(\mathbf{w}_0, \mathbf{w}_m)$ for all m requires $\mathcal{O}(MN_{\max})$. The following computations have smaller complexity. The search of p and computation of $D_p(l)$ for all $l \in [0, p-1]$ are conducted with the complexity of $\mathcal{O}(N_{\max})$ and $\mathcal{O}(M)$, respectively. The rest of the algorithm can be computed in $\mathcal{O}(N_{\max})$.

V. ANALYSIS OF BLIND FRAME RECOGNITION IN GAUSSIAN WIRETAP CHANNELS

In this section we consider Gaussian wiretap channel and analyze the blind frame recognition by showing the asymptotic behaviors of the correlation function and the mean of periodic samples. The wiretap channel is assumed to be an AWGN channel with $\sigma \neq 0$, and the received signal was given in (1). Let the noiseless component of the received signal $\mathbf{y}' = (y'_0, y'_1, \ldots, y'_{M-1})$ and the sliding window $\mathbf{w}'_m = (w'_{m,0}, w'_{m,1}, \ldots, w'_{m,W-1})$ be

$$y'_i = x_{tj-T+i} = y_i - n_i,$$

and

$$w'_{m,i} = w_{m,i} - n_{m+i} = y'_{m+i},$$

respectively. The following theorem shows the asymptotic behavior of $C(\mathbf{w}_0, \mathbf{w}_m)$ for increasing W.

Theorem 4: For the transmission over an AWGN channel as in (1), $C(\mathbf{w}_0, \mathbf{w}_m)$ converges as

$$\lim_{W\to\infty} C(\mathbf{w}_0, \mathbf{w}_m) = \begin{cases} 1, & \text{for } m = 0, \\ H(\mathbf{s}; (m)_N), & \text{for } 1 \leq m \leq M - W, \end{cases}$$

Proof: When $m = 0$, $C(\mathbf{w}_0, \mathbf{w}_0) = 1$ as noted. Let us consider the case of $m > 0$. The correlation function can be expressed as

$$\begin{aligned}
&C(\mathbf{w}_0, \mathbf{w}_m) \\
&\quad = C(\mathbf{w}'_0, \mathbf{w}'_m) + \frac{1}{W}\sum_{i=0}^{W-1}\left(n_i w'_{m,i} + w'_{0,i} n_{m+i} + n_i n_{m+i}\right).
\end{aligned}$$

As n_i is a Gaussian random variable, $n_i w'_{m,i}$, $w'_{0,i} n_{m+i}$, and $n_i n_{m+i}$ are random variables with zero mean. By the law of large numbers, we have

$$\lim_{W\to\infty} \frac{1}{W}\sum_{i=0}^{W-1}\left(n_i w'_{m,i} + w'_{0,i} n_{m+i} + n_i n_{m+i}\right) = 0.$$

From Theorem 1, we have

$$\lim_{W\to\infty} C(\mathbf{w}_0, \mathbf{w}_m) = \lim_{W\to\infty} C(\mathbf{w}'_0, \mathbf{w}'_m) = H(\mathbf{s}; (m)_N).$$

■

Now we consider the mean of periodic samples of $\mathbf{y}$. The following theorem shows the asymptotic behavior of $D_p(l)$ over $\mathbf{y}$.

Theorem 5: For the transmission over an AWGN channel as in (1), if $(p)_N = 0$, $D_p(l)$ converges as

$$\lim_{M\to\infty} D_p(l) = \begin{cases} s_{(l-T)_N}, & \text{for } l \in [0, p-1] \cap \mathcal{S}, \\ 0, & \text{for } l \in [0, p-1] \cap \mathcal{D}, \end{cases}$$

and if $(p)_N \neq 0$, $D_p(l)$ is bounded as

$$\left|\lim_{M\to\infty} D_p(l)\right| \leq \frac{\lceil L/g \rceil}{N/g}.$$

Proof: The mean of periodic samples can be written as

$$D_p(l) = \frac{1}{d}\sum_{i=0}^{d-1} y'_{l+ip} + \frac{1}{d}\sum_{i=0}^{d-1} n_{l+ip}.$$

By the law of large numbers, we have

$$\lim_{M\to\infty} \frac{1}{d}\sum_{i=0}^{d-1} n_{l+ip} = 0,$$

and

$$\lim_{M\to\infty} D_p(l) = \lim_{M\to\infty} \frac{1}{d}\sum_{i=0}^{d-1} y'_{l+ip}.$$

The rest of the proof is straightforward in regard to the proof of Theorem 2. ■

From Theorems 4 and 5, it was proven that the convergence of $C(\mathbf{w}_0, \mathbf{w}_m)$ and $D_p(l)$ for a noisy signal is similar to that in the noiseless case, indicating that the channel noise does not affect their asymptotic behaviors. From these properties, the asymptotic error probability of Algorithm 1 over Gaussian channel is 0 with proof omitted.

VI. MODIFIED BLIND FRAME RECOGNITION AND SYNCHRONIZATION

From Theorem 3, we show that the SW and the frame length are estimated with diminishing error probability when the received symbol stream size increases. However, it is realistic to assume that the received signal is finite in length, which may result in estimation errors. In this section, we analyze the possible errors in the finitely long received signal case and we present Algorithm 2, a modified version of Algorithm 1, which estimates the frame information with lower error probability.

Algorithm 2 Modified Blind Frame Recognition and Synchronization

Input: $\mathbf{y}, N_{\max}, J$;
Output: $\hat{N}, \hat{L}, \hat{T}, \hat{\mathbf{s}}$;
1: $N'_{\max} \leftarrow N_{\max}$;
2: **repeat**
3: $W \leftarrow M - N'_{\max}$, compute $C(\mathbf{w}_0, \mathbf{w}_m)$ for $m \in [0, N'_{\max}]$;
4: $p \leftarrow \arg\max_{m\in[1,N'_{\max}]} C(\mathbf{w}_0, \mathbf{w}_m)$, compute $D_p(l)$ for $l \in [0, p-1]$;
5: $\eta^* \leftarrow \arg\max_{\eta} \Lambda(\eta)$;
6: $(\mathcal{R}, \mathcal{F}) \leftarrow$ `EdgeDetection`(J, η^*);
7: $N'_{\max} \leftarrow p - 1$;
8: **until** $|\mathcal{R}| = 1$
9: $\hat{N} \leftarrow p$;
10: $\hat{T} \leftarrow \mathcal{R}_{(1)}$;
11: $\hat{L} \leftarrow \left(\mathcal{F}_{(1)} - \mathcal{R}_{(1)}\right)_{\hat{N}}$;
12: **for** $l = 0, \ldots, \hat{L} - 1$ **do**
13: $\hat{s}_l \leftarrow \mathrm{sgn}(D_p((\hat{T} + l)_p))$;
14: **end for**

In Algorithm 1, the estimate of frame length multiple p is set to the index of the maximum of $C(\mathbf{w}_0, \mathbf{w}_m)$ except the trivial peak $C(\mathbf{w}_0, \mathbf{w}_0) = 1$, and all the frame information is estimated with $|D_p(l)|$. The estimation is performed based on the rising and falling edges of $|D_p(l)|$. To improve the estimation performance, we modify Algorithm 1 in three perspectives; optimization of edge detection threshold, stricter detection of edges, and minimization of an estimate of frame length multiple.

We first address the optimization of edge detection threshold, η, of $|D_p(l)|$ for maximizing the edge detection probability. For the correct estimate of a frame length multiple p, the probability of detection of all edges in $|D_p(l)|$ is given as

$$\begin{aligned} P&\left(\bigcap_{l\in[0,p-1]\cap\mathcal{S}} \left|D_p(l)\right| \geq \eta, \bigcap_{l\in[0,p-1]\cap\mathcal{D}} \left|D_p(l)\right| < \eta\right) \\ &= P\left(\left|D_p(l)\right| \geq \eta | l \in [0, p-1]\cap\mathcal{S}\right)^{rp} \\ &\quad \times P\left(\left|D_p(l)\right| < \eta | l \in [0, p-1]\cap\mathcal{D}\right)^{(1-r)p}, \end{aligned} \tag{21}$$

where $D_p(l)$'s for all $l \in [0, p-1]$ are independent to each other, the SW ratio is $r = L/N$, $|[0, p-1]\cap\mathcal{S}| = rp$, and $|[0, p-1]\cap\mathcal{D}| = (1-r)p$. Although r is unknown, as $C(\mathbf{w}_0, \mathbf{w}_m)$ converges to r for $(m)_N = 0$ by Theorem 1, we use $C(\mathbf{w}_0, \mathbf{w}_p)$ as an estimate of r. The absolute mean of periodic samples in each factor of (21) is given as

$$D_p(l) = \frac{1}{d}\sum_{i=0}^{d-1} \left(y_{l+ip} + n_{l+ip}\right),$$

and is well approximated to Gaussian random variable by the central limit theorem.

Let $\Lambda(\eta)$ denote an approximation of correct detection probability, given as

$$\Lambda(\eta) = \Lambda_{\mathcal{S}}(\eta)\,\Lambda_{\mathcal{D}}(\eta), \tag{22}$$

where $\Lambda_{\mathcal{S}}(\eta)$ and $\Lambda_{\mathcal{D}}(\eta)$ denote approximations of correct detection probability in SW region and data region, respectively. They are the factors of (21) and given as

$$\begin{aligned} \Lambda_{\mathcal{S}}(\eta) &= \left(1 - Q\left(-(1+\eta)\frac{\sqrt{d}}{\sigma}\right)\right. \\ &\quad \left. + Q\left(-(1-\eta)\frac{\sqrt{d}}{\sigma}\right)\right)^{\lfloor C(\mathbf{w}_0,\mathbf{w}_p)p\rfloor} \\ &\approx P\left(\left|\frac{1}{d}\sum_{i=0}^{d-1}\left(y_{l+ip} + n_{l+ip}\right)\right|\right. \\ &\quad \left. \geq \eta | l \in [0, p-1]\cap\mathcal{S}\right)^{rp}, \end{aligned} \tag{23}$$

and likewise,

$$\Lambda_{\mathcal{D}}(\eta) = \left(Q\left(-\eta\sqrt{\frac{d}{1+\sigma^2}}\right) - Q\left(\eta\sqrt{\frac{d}{1+\sigma^2}}\right)\right)^{p-\lfloor C(\mathbf{w}_0,\mathbf{w}_p)p\rfloor}. \quad (24)$$

The optimized threshold is given as

$$\begin{aligned}\eta_{\text{opt}} &= \arg\max_{\eta} \Lambda(\eta) \\ &= \arg\max_{\eta} \Lambda_{\mathcal{S}}(\eta)\,\Lambda_{\mathcal{D}}(\eta).\end{aligned} \quad (25)$$

As the frame length and SW are acquired by the edges of $|D_p(l)|$, false edge detection may lead to estimation error. Hence a stricter criterion that can prevent such false edge detection is required. One way of achieving this is to observe more consecutive sampled values of $|D_p(l)|$ than the number of samples that observed in Algorithm 1 for detecting an edge. Since the length of SW is more than a few symbols, a stricter condition is to check if there are $J > 1$ consecutive low or high samples after a high or low sample for determining rising or falling edges, respectively. We define an edge detecting function $\Phi(J, \eta, l)$, which observes $J+1$ symbols and outputs 1, -1, and 0, meaning l is an index of either rising or falling edges of $|D_p(l)|$ or neither of them, as

$$\Phi(J,\eta,l) = \begin{cases} 1, & \text{for } |D_p((l-1)_p)| < \eta, |D_p(l)| \geq \eta, \\ & \quad \ldots, |D_p(l+J-1)| \geq \eta, \\ -1, & \text{for } |D_p((l-1)_p)| \geq \eta, |D_p(l)| < \eta, \\ & \quad \ldots, |D_p(l+J-1)| < \eta, \\ 0, & \text{otherwise.} \end{cases} \quad (26)$$

The minimization of the randomness in $|D_p(l)|$ can be achieved by increasing the number of samples to be summed, d, or with a smaller p. Given that p is a multiple of N obtained from $C(\mathbf{w}_0, \mathbf{w}_m)$, $|\mathcal{R}| = 1$ is a sufficient condition for $p = N$, which is the optimal p for detecting the edges of $|D_p(l)|$. Therefore, we modify Algorithm 1 to choose p iteratively until $|\mathcal{R}| = 1$.

Algorithm 2 starts by setting $N'_{\max} = N_{\max}$ where $N_{\max}$ is an input argument to the algorithm. We set $N'_{\max}$ smaller as the inner loop of the algorithm iterates. An iterative search of W, p, η, $\mathcal{R}$, and $\mathcal{F}$ is conducted in lines 2-8 where lines 3 and 4 are the same as Algorithm 1. In line 5, η is optimize with (25). The rising and falling edges are set by Algorithm 3 where the first edge is determined in line 1-6 and remaining edges are determined in line 7-13. At the end of each iteration, the cardinality of $\mathcal{R}$ for rising edges is checked in line 8 of Algorithm 2. If $|\mathcal{R}| \neq 1$, $N_{\max}$ is set to $p-1$ for narrowing the search range for N and the subsequent iteration begins. The iteration proceeds until $|\mathcal{R}| = 1$. After the iteration terminates, the frame information is estimated as in Algorithm 1 in lines 9-13. Note that, throughout the iteration, W increases gradually. This improves the accuracy of determining η with the approximations and p such that $(p)_N = 0$, as $C(\mathbf{w}_0, \mathbf{w}_m)$ converges to $H(\mathbf{s}; (m)_N)$ with increase in W. The iteration stops in some finite number of loops.

Algorithm 3 EdgeDetection(J, η)

Input: J, η;
Output: $\mathcal{R}, \mathcal{F}$;
1: $\mathcal{R} \leftarrow \varnothing, \mathcal{F} \leftarrow \varnothing$;
2: **for** $l = 0, \ldots, p-1$ **do** \\ Detection of the first edge
3: **if** $\Phi(J, \eta, l) \neq 0$ **then**
4: $l_0 \leftarrow l$, break;
5: **end if**
6: **end for**
7: **for** $l = l_0, \ldots, l_0 + p - 1$ **do** \\ Detection of all edges
8: **if** $\Phi(J, \eta, (l)_p) = 1$ **then**
9: $\mathcal{R} \leftarrow \mathcal{R} \cup \{(l)_p\}$;
10: **else if** $\Phi(J, \eta, (l)_p) = -1$ **then**
11: $\mathcal{F} \leftarrow \mathcal{F} \cup \{(l)_p\}$;
12: **end if**
13: **end for**

The computational complexity of Algorithm 2 is $\mathcal{O}\left(MN_{\max}{}^2\right)$, which is shown as follows. The maximum number of iterations of the loop in lines 2–8 of Algorithm 2 is $N_{\max}$. During an iteration, lines 3 and 4, which are the same process as in Algorithm 1, require the complexity of $\mathcal{O}(MN_{\max})$ and $\mathcal{O}(M)$, respectively. The optimization of η can be easily performed by a single table lookup. Then the detection of edges by Algorithm 3 requires $\mathcal{O}(N_{\max})$. Hence, the complexity in lines 2–8 is $\mathcal{O}\left(MN_{\max}{}^2\right)$. The rest of the algorithm can be computed with the complexity of $\mathcal{O}(N_{\max})$.

VII. NUMERICAL RESULTS

The simulation results for the proposed blind frame recognition algorithms are provided in this section to evaluate their validness. Throughout the simulations, the recognition error performance of the algorithms is of interest. It is regarded as a recognition error event if any of the outputs of the algorithms, $\hat{N}$, $\hat{T}$, and $\hat{s}$, are not correct.

The simulation setting is as follows. The frame length N is set to 50. Practically used SWs usually have a good aperiodic correlation property to avoid synchronization errors [1]–[4]. As the proposed algorithms are designed for arbitrary realization of a SW, we try two types of SWs of length $L = 15$; one from the m-sequence and the other randomly generated. Throughout the comparisons, the maximum length of the frame to be estimated is set as $N_{\max} = 100$. We consider the transmission of BPSK modulated signals through noiseless or Gaussian wiretap channels with high or low-SNR.

We first present the sensitivity of the edge detection probability of $D_p(l)$ to the detection threshold by showing $\Lambda(\eta)$, the closed form approximation of edge detection probability, for various η's and E_s/N_0's in Fig. 6. Then in Figs. 7, 8, and 9, Algorithms 1 and 2 are evaluated for different values

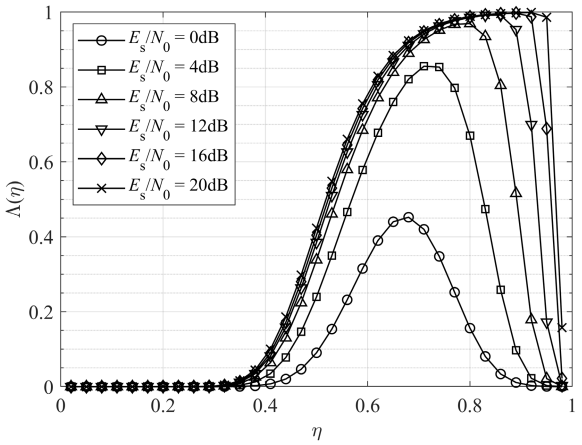


FIGURE 6. The approximate correct detection probability (22) for frame structure $N = 50$, m-sequence SW of $L = 15$, and received signal length is $M = 1000$ where the transmit signals are the same, but the realization of the channel noise is different for different E_s/N_0's.

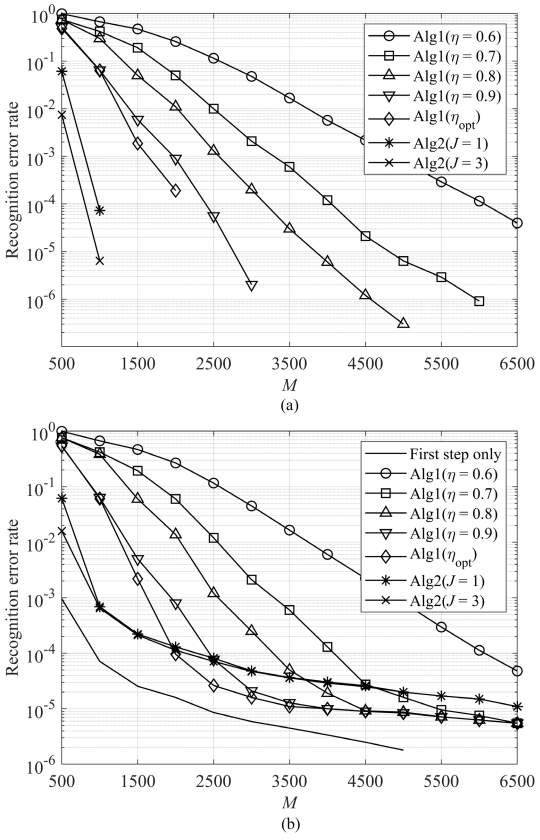


FIGURE 7. Recognition error rate of Algorithms 1 and 2 with $N_{max} = 100$ for $N = 50$ and $L = 15$ over a noiseless channel: (a) m-sequence SW and (b) randomly generated SW.

of η and J in the noiseless wiretap channel, Gaussian wiretap channels of $E_s/N_0 = 10$ dB and $E_s/N_0 = 0$ dB, respectively. The recognition error performance as well as the estimation error performance for each frame information, such as frame length, SW, and delay, over a Gaussian wiretap channel of $E_s/N_0 = 10$ dB is shown in Fig. 10. Then, the simulation results for a wider search space for the frame length,

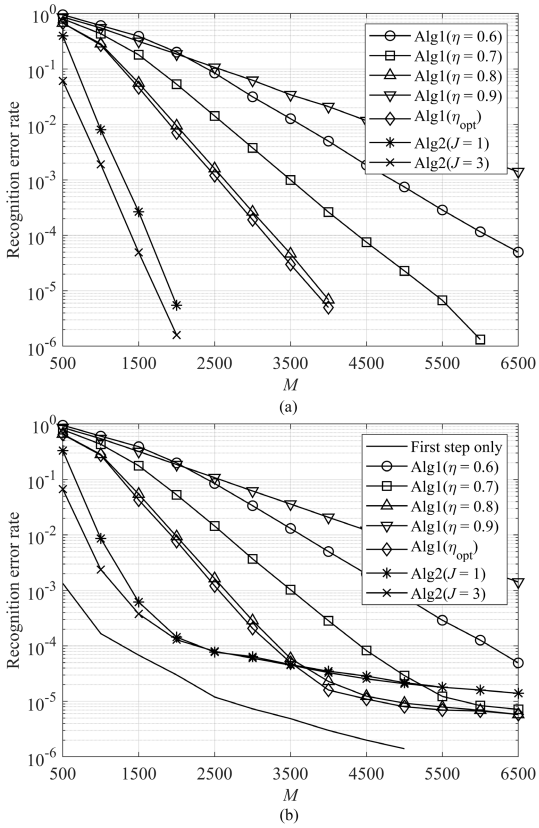


FIGURE 8. Recognition error rate of Algorithms 1 and 2 with $N_{max} = 100$ for $N = 50$ and $L = 15$ over a Gaussian channel with SNR $E_s/N_0 = 10$ dB: (a) m-sequence SW and (b) randomly generated SW.

$N_{max} = 200$, is shown in Fig. 11. In Fig. 12, the recognition error rate for Algorithms 1 and 2 are presented for various E_s/N_0's. We also present the error performance of a modified version of Algorithm 1 in which the optimization step of η is inserted as Algorithm 2, and these cases are labeled by Alg1(η_{opt}). In fact, the recognition error rate of Alg1(η_{opt}) is the performance limit of Algorithm 1 with constant η's.

1) EDGE DETECTION THRESHOLD η OF ALGORITHM 2

In Algorithm 2, the edge detection threshold η is optimized. Fig. 6 shows $\Lambda(\eta)$ for various η's and channel SNRs with the same realization of the received signal and simulation parameters, such as d and N_{max}. In the figure, as E_s/N_0 increases, η maximizing $\Lambda(\eta)$ converges to 1. The recognition error rate of Algorithm 1 for various η's confirms this observation. In Figs 7, 8, and 9, as channel SNR increases, η minimizing the error rate of Algorithm 1 also increases.

2) PERFORMANCE FOR THE SWs OF M-SEQUENCE AND RANDOM GENERATION

In this subsection, we discuss the performances of the proposed algorithms for the SW of the m-sequence and the random sequence. For the random SW, the rate of $(p)_N \neq 0$, the error performance of the first step only, is also drawn for Algorithm 1 for comparison purpose. The recognition error

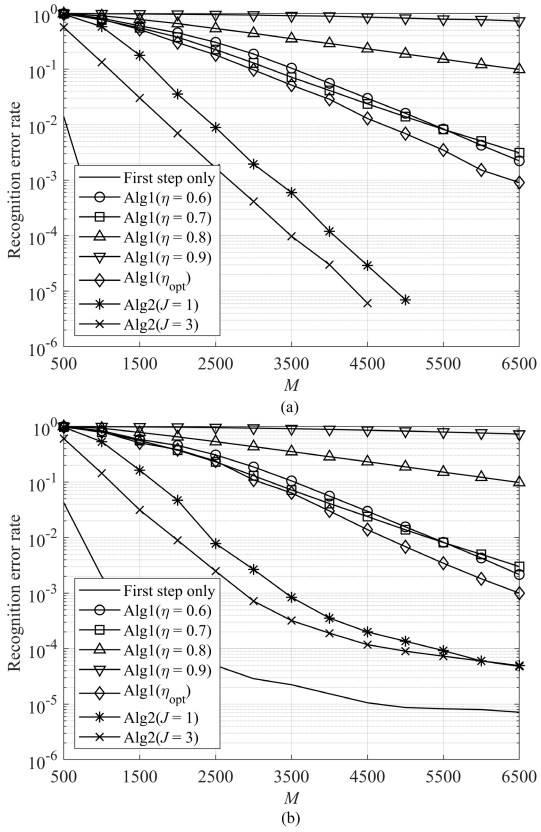


FIGURE 9. Recognition error rate of Algorithms 1 and 2 with $N_{max} = 100$ for $N = 50$ and $L = 15$ over a Gaussian channel with SNR $E_s/N_0 = 0$ dB: (a) m-sequence SW and (b) randomly generated SW.

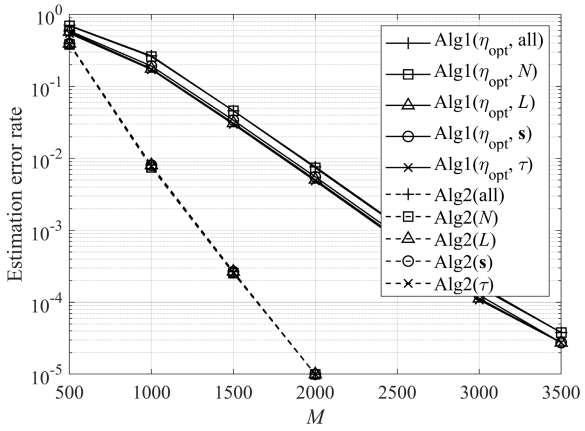


FIGURE 10. Estimation error rate of Algorithms 1 and 2 for all frame parameters with $J = 1$ for $N = 50$ and m-sequence SW of $L = 15$ in Gaussian channel with SNR $E_s/N_0 = 10$ dB.

performance of Algorithm 1 cannot surpass the error rate of the first step because if $(p)_N \neq 0$, the edge detection step fails. Hence, the performance of the first step is the algorithmic limit of Algorithm 1. In general, the recognition error rates monotonically decrease as the length of the received signal increases in all cases. This observation is consistent with the result of Theorem 3.

When the SW is the m-sequence, the error rate decreases at a constant rate in the semilog plot. The error rate of the first

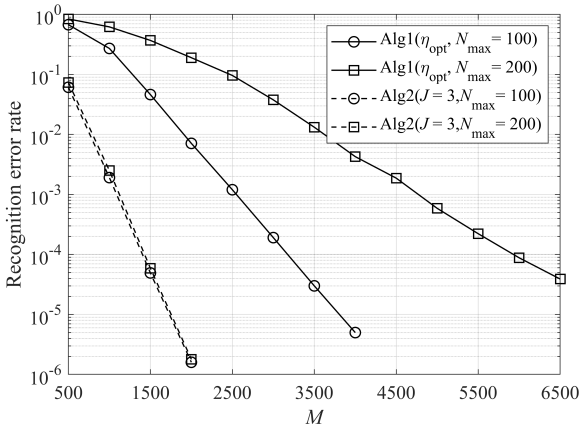


FIGURE 11. Recognition error rate of Algorithms 1 and 2 with two different values of N_{max} for frame structure $N = 50$ and m-sequence SW of $L = 15$ in Gaussian channel with SNR $E_s/N_0 = 10$ dB.

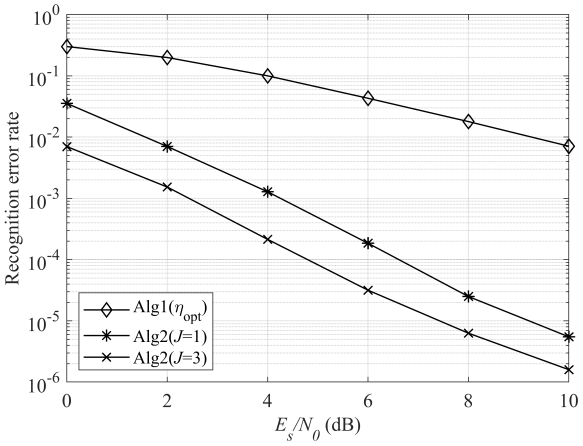


FIGURE 12. Recognition error rate of Algorithms 1 and 2 for $N = 50$ and m-sequence SW of $L = 15$ and $M = 2000$ in Gaussian channel with various E_s/N_0 dB.

step is found to be extremely low for the m-sequence SW, indicating that the recognition error rate is dominated by the incorrect edge detection of the mean of periodic samples in the second step of the algorithms. In contrast, in the random SW case, there appears to be an error floor as M increases due to poor SW patterns. In Fig. 7(b), for example, the error rate of Algorithm 1 decreases quickly for a small M whereas the slope of the error rate curve becomes modest for a larger M. As the edge detection in $|D_p(l)|$ is irrelevant of the SW pattern, the edge detection performs equivalently for both m-sequence and random SW given the same p. In contrast, the performance of the first step is largely dependent on SW's aperiodic correlation. Although the performance is poorer for the random SW, the error rates still gradually decrease as M increases.

3) PERFORMANCE COMPARISON BETWEEN ALGORITHMS 1 AND 2

The recognition performances of the two proposed algorithms can be compared. Algorithm 2 outperforms

Algorithm 1 by following reasons. First, the iterative update of p leads to a smaller integer multiple of N which is better for the second step performance. The strict condition on detecting the rising and falling edges by observing J instants, which can be more than one, also keeps the algorithm from detecting wrong edges. The use of optimal η as a threshold in each iteration also improves the edge detecting performance. In Figs. 7(a), 8(a), 9(a), 11, and 12, Algorithm 2 significantly outperforms Algorithm 1 for all values of M. When the m-sequence is used, proper peaks of correlation are easily distinguishable from other correlation values. This makes Algorithm 2 get $p = N$ with high probability. The estimation error performance of Algorithms 1 and 2 for all frame parameters are compared in Fig. 10. In contrast, in the random SW case, there is a performance crossover between the two algorithms in high-SNR environments as shown in Figs. 7(b) and 8(b). For SWs with a poor aperiodic correlation property, the proper correlation peaks are possibly be indistinguishable from others. In this case, iterative estimations of p can degrade the performance because there are multiple large side lobes in the aperiodic correlation function of the SW resulting in strong false candidates for peak detection.

4) IMPACT OF NOISE

For the noiseless wiretap channel, if p is a multiple of N, $|D_p(l)| = 1$ in the SW region, $l \in \mathcal{S}$. Hence, for edge detection, a higher η provides a better performance generally. In contrast, for a noisy channel, $|D_p(l)|$ in the SW region can be smaller than 1 due to the channel noise and the variance is larger when the SNR is lower. Therefore, a high η does not guarantee a good edge detection performance in the noisy channel and should be set lower for more margin to avoid false edge detection. The simulation results show the performance sensitivity to η as in Figs. 7, 8, and 9. The optimization of η in Algorithm 2 can be explained with Fig. 6, presenting the approximated edge detection probability for various η's and E_s/N_0's.

The recognition error rates of Algorithms 1 and 2 for various E_s/N_0's are shown in Fig. 12. The iterative estimation of frame information in Algorithm 2 gives SNR gain over Algorithm 1 more than 6dB, which can be shown by comparing Alg2($J = 1$) to Alg1(η_{opt}). And also the strict condition on detecting the rising and falling edges of $|D_p(l)|$ by observing $J > 1$ instants gives additional SNR gain, which can be shown by comparing Alg2($J = 3$) to Alg2($J = 1$).

5) PERFORMANCE VERSUS MAXIMUM FRAME LENGTH

As the maximum frame length $N_{\max}$, that can be estimated by the proposed algorithm, is a preset value and also affects the frame recognition performance. The performance in terms of $N_{\max}$ is given in Fig. 11. An increase in $N_{\max}$ causes a significant performance degradation in Algorithm 1 whereas Algorithm 2 shows little or no loss of performance. For Algorithm 1, if $N_{\max}$ is doubled, then the average of p is almost doubled, too. Doubling of M is required to get a similar accuracy in the edge detection of $|D_p(l)|$. In contrast, in Algorithm 2, p gets smaller through iterations and the optimal η for given $C(\mathbf{w}_0, \mathbf{w}_m)$ and p is also obtained. For a similar edge detection performance, M does not need to increase as much as needed in Algorithm 1. Therefore, Algorithm 2 works better for a wider search space of frame length.

VIII. CONCLUSION

In this article, we have studied a blind frame recognition and synchronization problem. It has been shown that, under no prior information other than the existence of unknown SW, reliable blind frame recognition is possible. We proposed an asymptotically good correlation-based algorithm that is designed to determine the frame length and SW. The validness of the algorithm was theoretically proven – the error rate vanishes as the received data size increases. Although this approach originated from [10], we presented an explicit modified algorithm and analyzed the asymptotic behaviors. In fact, this is the first study that conducted the theoretical analysis on the performance of fully blind frame recognition to the authors' knowledge.

We also presented another algorithm, which performs better under the limited data scenario, for practical use. The simulation results showed that regardless of channel impairments or SW pattern, the proposed algorithms estimate the frame parameters consistently improves as the amount of the received signal increases. It is also shown that our algorithms perform better when an SW with a better aperiodic autocorrelation is used. The complexity analysis was also conducted and the iterative estimation of frame information in the improved algorithm results in the complexity increase from $\mathcal{O}(MN_{\max})$ to $\mathcal{O}\left(MN_{\max}{}^2\right)$.

APPENDIX A

In this section, we prove Lemma 2. From line 2 of Algorithm 1, the following hold:

$$\begin{aligned}(p)_N = 0 &\Leftrightarrow \left(\arg \max_{m\in[1,N_{\max}]} C(\mathbf{w}_0, \mathbf{w}_m)\right)_N = 0 \\ &\Leftrightarrow \max_{\substack{m\in[1,N_{\max}],\\ (m)_N\neq 0}} C(\mathbf{w}_0, \mathbf{w}_m) < \max_{\substack{m\in[1,N_{\max}],\\ (m)_N= 0}} C(\mathbf{w}_0, \mathbf{w}_m). \end{aligned} \quad (27)$$

From Corollary 2, $|C(\mathbf{w}_0, \mathbf{w}_m) - E[C(\mathbf{w}_0, \mathbf{w}_m)]| < \frac{1}{2}\left(\frac{1}{N} - \frac{2}{W}\right)$ holding for all $m \in [1, N_{\max}]$ is a sufficient condition for (27).

$$\begin{aligned}&P\left((p)_N = 0\right) \\ &= P\left(\max_{\substack{m\in[1,N_{\max}],\\ (m)_N\neq 0}} C(\mathbf{w}_0, \mathbf{w}_m) < \max_{\substack{m\in[1,N_{\max}],\\ (m)_N= 0}} C(\mathbf{w}_0, \mathbf{w}_m)\right)\end{aligned}$$

$$\geq P\Bigg(\bigcap_{m\in[1,N_{\max}]} |C(\mathbf{w}_0,\mathbf{w}_m) - E[C(\mathbf{w}_0,\mathbf{w}_m)]| < \frac{1}{2}\left(\frac{1}{N}-\frac{2}{W}\right)\Bigg)$$

$$= 1 - P\Bigg(\bigcup_{m\in[1,N_{\max}]} |C(\mathbf{w}_0,\mathbf{w}_m) - E[C(\mathbf{w}_0,\mathbf{w}_m)]| \geq \frac{W-2N}{2NW}\Bigg)$$

$$\geq 1 - \sum_{m\in[1,N_{\max}]} P\Bigg(|C(\mathbf{w}_0,\mathbf{w}_m) - E[C(\mathbf{w}_0,\mathbf{w}_m)]| \geq \frac{W-2N}{2NW}\Bigg),$$

where the last inequality follows from the union bound on probabilities. Since $M \gg N$, we can assume that $W = M - N_{\max} > 2N$. From Corollary 1,

$$E[C(\mathbf{w}_0,\mathbf{w}_m) - E[C(\mathbf{w}_0,\mathbf{w}_m)]] = 0,$$

$$\mathrm{VAR}[C(\mathbf{w}_0,\mathbf{w}_m) - E[C(\mathbf{w}_0,\mathbf{w}_m)]] = \frac{W-|\mathcal{S}_0\cap\mathcal{S}_m|}{W^2}.$$

By the Chebyshev inequality, we conclude the proof as

$$P\left((p)_N = 0\right) \geq 1 - \sum_{m\in[1,N_{\max}]} \frac{W-|\mathcal{S}_0\cap\mathcal{S}_m|}{W^2}\left(\frac{2NW}{W-2N}\right)^2 \geq 1 - \sum_{m\in[1,N_{\max}]} \frac{4N^2W}{(W-2N)^2} \geq 1 - \frac{4N_{\max}^3 W}{(W-2N_{\max})^2}.$$

APPENDIX B

In this section, we first introduce the Chernoff bound [40] and prove Lemma 3.

Lemma 4 (Chernoff Bound [40]): Let $\mathrm{B}_n \sim \mathcal{B}\left(n, \frac{1}{2}\right)$. For any $0 < \epsilon < 1$,

$$P\left(\mathrm{B}_n \geq (1+\epsilon)\frac{n}{2}\right) \leq \exp\left(-\frac{\epsilon^2 n}{2}\right),$$

$$P\left(\mathrm{B}_n \leq (1-\epsilon)\frac{n}{2}\right) \leq \exp\left(-\frac{\epsilon^2 n}{2}\right).$$

Using Lemma 4, we now derive the lower bound in Lemma 3. In line 3 of Algorithm 1, if all the rising and falling edges that discriminate the SW and data are set correctly, all the frame information is estimated without errors:

$$P\left(\hat{N}=N, \hat{L}=L, \hat{\mathbf{s}}=\mathbf{s}, \hat{T}=T \,|(p)_N=0\right) \geq P\Bigg(\bigcap_{l\in[0,p-1]\cap\mathcal{S}} |D_p(l)| \geq \eta, \bigcap_{l\in[0,p-1]\cap\mathcal{D}} |D_p(l)| < \eta \,|(p)_N=0\Bigg)$$

$$= P\Bigg(\bigcap_{l\in[0,p-1]\cap\mathcal{S}} |D_p(l)| \geq \eta \,|(p)_N=0\Bigg) \times P\Bigg(\bigcap_{l\in[0,p-1]\cap\mathcal{D}} |D_p(l)| < \eta \,|(p)_N=0\Bigg). \quad (28)$$

As p is a multiple of the frame length, $|D_p(l)| = 1$ when $l \in [0, p-1]\cap\mathcal{S}$. Hence the first term of (28) is

$$P\Bigg(\bigcap_{l\in[0,p-1]\cap\mathcal{S}} |D_p(l)| \geq \eta \,|(p)_N=0\Bigg) = 1.$$

Furthermore, a lower bound for the second term of (28) is obtained as follows:

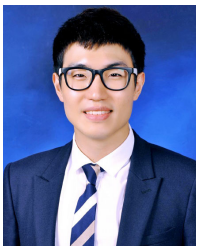
$$P\Bigg(\bigcap_{l\in[0,p-1]\cap\mathcal{D}} |D_p(l)| < \eta \,|(p)_N=0\Bigg) \overset{(a)}{=} \prod_{l\in[0,p-1]\cap\mathcal{D}} P\left(|D_p(l)| < \eta \,|(p)_N=0\right) \overset{(b)}{=} \prod_{l\in[0,p-1]\cap\mathcal{D}} P\left(\left|\frac{1}{d}(2\mathrm{B}_d - d)\right| \leq \eta\right) \overset{(c)}{\geq} P\left(\left|\frac{1}{d}(2\mathrm{B}_d - d)\right| \leq \eta\right)^{N_{\max}} \overset{(d)}{\geq} \left(1 - 2\exp\left(-\frac{\eta^2}{2}\left(\frac{M}{N_{\max}}-1\right)\right)\right)^{N_{\max}},$$

where (a) follows from the independence of $D_p(l)$'s, $l \in [0, p-1]\cap\mathcal{D}$, (b) follows from (17), (c) follows from $N_{\max} \geq p$, and (d) is due to Lemma 4 and $d = \lfloor \frac{M}{p} \rfloor$.

REFERENCES

[1] R. H. Barker, "Group synchronization of binary digital systems," in *Communication Theory*. London, U.K.: Butterworth, 1953, pp. 273–287.
[2] J. Massey, "Optimum frame synchronization," *IEEE Trans. Commun.*, vol. COM-20, no. 2, pp. 115–119, Apr. 1972.
[3] P. Nielsen, "Some optimum and suboptimum frame synchronizers for binary data in Gaussian noise," *IEEE Trans. Commun.*, vol. COM-21, no. 6, pp. 770–772, Jun. 1973.
[4] G. Lui and H. Tan, "Frame synchronization for Gaussian channels," *IEEE Trans. Commun.*, vol. COM-35, no. 8, pp. 818–829, Aug. 1987.
[5] M. Marazin, R. Gautier, and G. Burel, "Blind recovery of K/N rate convolutional encoders in a noisy environment," *EURASIP J. Wireless Commun. Netw.*, vol. 2011, no. 1, pp. 1186–1687, Dec. 2011.
[6] J. Tian, Y. Pei, Y.-D. Huang, and Y.-C. Liang, "Modulation-constrained clustering approach to blind modulation classification for MIMO systems," *IEEE Trans. Cognit. Commun. Netw.*, vol. 4, no. 4, pp. 894–907, Dec. 2018.
[7] R. Moosavi and E. G. Larsson, "Fast blind recognition of channel codes," *IEEE Trans. Commun.*, vol. 62, no. 5, pp. 1393–1405, May 2014.
[8] V. Choqueuse, M. Marazin, L. Collin, K. C. Yao, and G. Burel, "Blind recognition of linear Space–Time block codes: A likelihood-based approach," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1290–1299, Mar. 2010.
[9] O. A. Dobre, A. Abdi, Y. Bar-Ness, and W. Su, "Blind modulation classification: A concept whose time has come," in *Proc. IEEE Sarnoff Symp. Adv. Wired Wireless Commun.*, Apr. 2005, pp. 223–228.
[10] P. P. Brahma and K. Bandyopadhyay, "Non-cooperative denial of communication after synchronizing with repeating sequences," in *Proc. DSR*, Aug. 2011, pp. 1–4.

[11] J. Qin, Z. Huang, C. Liu, S. Su, and J. Zhou, "Novel blind recognition algorithm of frame synchronization words based on soft-decision in digital communication systems," *PLoS ONE*, vol. 10, no. 7, pp. 1–8, Jul. 2015.
[12] Y. Xu, Y. Zhong, and Z. Huang, "An improved blind recognition algorithm of frame parameters based on self-correlation," *Information*, vol. 10, no. 64, pp. 1–9, Feb. 2019.
[13] Y. S. Kil, S.-H. Kim, and J. Kim, "A blind frame structure recognition method," in *Proc. ITC-CSCC*, Jul. 2017, pp. 743–745.
[14] C. Li, T.-Q. Zhang, and Y. Liu, "Blind recognition of RS codes based on Galois field columns Gaussian elimination," in *Proc. Int. Congr. Image Signal Process.*, Oct. 2014, pp. 836–841.
[15] R. A. Poisel, *Electronic Warfare Receivers and Receiving Systems*. Norwood, MA, USA: Artech House, 2014.
[16] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.
[17] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 4, pp. 451–456, Jul. 1978.
[18] H. Lei, H. Zhang, I. S. Ansari, Z. Ren, G. Pan, K. A. Qaraqe, and M.-S. Alouini, "On secrecy outage of relay selection in underlay cognitive radio networks over Nakagami-*m* fading channels," *IEEE Trans. Cogn. Commun. Netw.*, vol. 3, no. 4, pp. 614–627, Dec. 2017.
[19] Y.-W.-P. Hong, P.-C. Lan, and C.-C.-J. Kuo, "Enhancing physical-layer secrecy in multiantenna wireless systems: An overview of signal processing approaches," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 29–40, Sep. 2013.
[20] Y. Liu, H.-H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: Theories, technologies, and challenges," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 347–376, 1st Quart., 2017.
[21] S. Shafiee and S. Ulukus, "Achievable rates in Gaussian MISO channels with secrecy constraints," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun. 2007, pp. 2466–2470.
[22] A. Khisti, G. Wornell, A. Wiesel, and Y. Eldar, "On the Gaussian MIMO wiretap channel," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun. 2007, pp. 2471–2475.
[23] R. Bassily, E. Ekrem, X. He, E. Tekin, J. Xie, M. R. Bloch, S. Ulukus, and A. Yener, "Cooperative security at the physical layer: A summary of recent advances," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 16–28, Sep. 2013.
[24] W. K. Harrison, J. Almeida, M. R. Bloch, S. W. McLaughlin, and J. Barros, "Coding for secrecy: An overview of error-control coding techniques for physical-layer security," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 41–50, Sep. 2013.
[25] K.-W. Huang, H.-M. Wang, Y. Wu, and R. Schober, "Pilot spoofing attack by multiple eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 17, no. 10, pp. 6433–6447, Oct. 2018.
[26] M. Chiani and M. G. Martini, "Optimum synchronization of frames with unknown, variable lengths on Gaussian channels," in *Proc. IEEE GLOBECOM*, Dec. 2004, pp. 4087–4091.
[27] M. Chiani and M. G. Martini, "Practical frame synchronization for data with unknown distribution on AWGN channels," *IEEE Commun. Lett.*, vol. 9, no. 5, pp. 456–458, May 2005.
[28] M. G. Martini and M. Chiani, "Optimum metric for frame synchronization with Gaussian noise and unequally distributed data symbols," in *Proc. IEEE SPAWC*, Jul. 2009, pp. 643–647.
[29] C. Stefanovic and D. Bajic, "On the search for a sequence from a predefined set of sequences in random and framed data streams," *IEEE Trans. Commun.*, vol. 60, no. 1, pp. 189–197, Jan. 2012.
[30] P. Robertson, "A generalized frame synchronizer," in *Proc. IEEE GLOBECOM*, Dec. 1992, pp. 365–369.
[31] H. Huh and J. Krogmeier, "A unified approach to optimum frame synchronization," *IEEE Trans. Wireless Commun.*, vol. 5, no. 12, pp. 3700–3711, Dec. 2006.
[32] S. Houcke and G. Sicot, "Blind frame synchronization for block code," in *Proc. IEEE EUSIPCO*, Sep. 2006, pp. 1–4.
[33] R. Imad, S. Houcke, and C. Douillard, "Blind frame synchronization on Gaussian channel," in *Proc. IEEE EUSIPCO*, Sep. 2007, pp. 555–559.
[34] S. Aouada, A. Zoubir, and C. See, "A comparative study on source number detection," in *Proc. IEEE ISSPA*, vol. 1, Jul. 2003, pp. 173–176.
[35] O. A. Dobre, A. Abdi, Y. Bar-Ness, and W. Su, "Survey of automatic modulation classification techniques: Classical approaches and new trends," *IET Commun.*, vol. 1, no. 2, pp. 137–156, Apr. 2007.
[36] A. Valembois, "Detection and recognition of a binary linear code," *Discrete Appl. Math.*, vol. 111, nos. 1–2, pp. 199–218, Jul. 2001.
[37] I.-S. Kang, H. Lee, S.-J. Han, C.-S. Park, J.-H. Soh, and Y.-J. Song, "Reconstruction method for Reed–Müller codes using fast Hadamard transform," in *Proc. ICACT*, Feb. 2011, pp. 793–796.
[38] G. Sicot, S. Houcke, and J. Barbier, "Blind detection of interleaver parameters," *Signal Process.*, vol. 89, no. 4, pp. 450–462, Apr. 2009.
[39] L. Tong, G. Xu, and T. Kailath, "Blind identification and equalization based on second-order statistics: A time domain approach," *IEEE Trans. Inf. Theory*, vol. 40, no. 2, pp. 340–349, Mar. 1994.
[40] M. Mitzenmacher and E. Upfal, "Chernoff bounds," in *Probability and Computing: Randomized Algorithms and Probabilistic Analysis*. New York, NY, USA: Cambridge Univ. Press, 2005.
[41] S. Su, J. Zhou, Z. Huang, C. Liu, and Y. Zhang, "Blind identification of convolutional encoder parameters," *Sci. World J.*, vol. 2014, pp. 1–9, May 2014.
[42] L. Fan, S. Zhang, T. Q. Duong, and G. K. Karagiannidis, "Secure switch-and-stay combining (SSSC) for cognitive relay networks," *IEEE Trans. Commun.*, vol. 64, no. 1, pp. 70–82, Jan. 2016.
[43] P.-H. Lin, F. Gabry, R. Thobaben, E. A. Jorswieck, and M. Skoglund, "Multi-phase smart relaying and cooperative jamming in secure cognitive radio networks," *IEEE Trans. Cognit. Commun. Netw.*, vol. 2, no. 1, pp. 38–52, Mar. 2016.



YONG-SUNG KIL (Graduate Student Member, IEEE) received the B.S. degree in information and communication engineering from Sungkyunkwan University, Suwon, South Korea, in 2015, where he is currently pursuing the Ph.D. degree in information and communication engineering. His research interests include polar codes, wireless communication systems, and deep learning-based communication systems.

HYUNJAE LEE (Graduate Student Member, IEEE) received the B.S. degree in information and communication engineering from Sungkyunkwan University, Suwon, South Korea, in 2014, where he is currently pursuing the Ph.D. degree in information and communication engineering. His research interests include low-density parity-check codes, polar codes, coding theory, and wireless communication systems.

SANG-HYO KIM (Member, IEEE) received the B.Sc., M.Sc., and Ph.D. degrees in electrical engineering from Seoul National University, Seoul, South Korea, in 1998, 2000, and 2004, respectively. From 2004 to 2006, he was a Senior Engineer with Samsung Electronics. He visited the University of Southern California as a Visiting Scholar, from 2006 to 2007. In 2007, he joined the College of Information and Communication Engineering, Sungkyunkwan University, Suwon, South Korea, where he is currently a Professor. In 2015, he had a one-year visit to the University of California at San Diego, San Diego. His research interests include coding theory, wireless communications, and deep learning-inspired communication systems. He has been serving as an Editor for the TRANSACTIONS ON EMERGING TELECOMMUNICATIONS TECHNOLOGIES and the *Journal of Communications and Networks*, since 2013.

SEOK-HO CHANG (Senior Member, IEEE) received the B.S. and M.S. degrees from Seoul National University, Seoul, South Korea, in 1997 and 1999, respectively, and the Ph.D. degree from the University of California at San Diego, San Diego, CA, USA, in 2010, all in electrical engineering. From 1999 to 2005, he was with LG Electronics, South Korea, where he was involved in the development of WCDMA (3GPP) cellular modem chips. In 2006, he was with POSCO ICT, South Korea, where he was involved in mobile WiMax systems. From 2010 to 2011, he was a Postdoctoral Scholar with the University of California, where he was engaged in the cross-layer design of wireless systems. From 2011 to 2012, he was a Staff Engineer with Qualcomm Inc., San Diego, where he was involved in the design and development of 4G cellular modem chips. From 2012 to 2020, he was an Associate Professor (tenured) with Dankook University, Yongin, South Korea. Since 2020, he has been an Associate Professor with Konkuk University, Seoul. His research interests include communication theory, optimization theory, the cross-layer design of wireless systems, and the applications of machine learning and signal processing.