WIRELESS COMMUNICATIONS AND MOBILE COMPUTING
*Wirel. Commun. Mob. Comput.* (2013)
Published online in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/wcm.2446

RESEARCH ARTICLE

# Improved auxiliary particle filter-based synchronization of chaotic Colpitts circuit and its application to secure communication

Zhiguo Shi[1,2*], Songjie Bi[1], Hongtao Zhang[2], Rongxing Lu[2] and Xuemin (Sherman) Shen[2]

[1] Department of Information and Electronic Engineering, Zhejiang University, Hangzhou, 310027, China
[2] Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, N2L 3G1, Canada

## ABSTRACT

In this paper, we propose a synchronization scheme based on an improved auxiliary particle filter (IAPF) for chaotic Colpitts circuit and conduct an experimental study on the synchronization performance with application to secure communications. Specifically, with the synchronization scheme, when the chaotic signals generated by an analog Colpitts circuit are transmitted through a nonideal channel, the distorted signals are processed digitally by the novelly designed IAPF at the receiver, in order to obtain the synchronized signals of the transmitter circuit. Experimental results indicate that synchronization can be achieved over both the additive white Gaussian noise channel and the multipath fading channel with low signal-to-noise ratio, even if there exist severe circuit parameter mismatches between the transmitter and the receiver. Furthermore, a chaos-masking secure communication system is constructed and verified over both the additive white Gaussian noise channel and the multipath fading channel, and the bit error rate is evaluated versus different signal-to-noise ratios and symbol periods. It is shown that the achievable bit error rate can reach the order of magnitude of $10^{-4}$ without error correction coding techniques. In addition, security analysis demonstrates that the proposed chaotic secure communication system is resistant to the brute-force attack. Copyright © 2013 John Wiley & Sons, Ltd.

**KEYWORDS**

chaotic Colpitts circuit; improved auxiliary particle filter; chaos synchronization; secure communication

***Correspondence**

Zhiguo Shi, Department of Information and Electronic Engineering, Zhejiang University, Hangzhou, 310027, China.
E-mail: shizg@zju.edu.cn

## 1. INTRODUCTION

Since the seminal work of Pecora and Carroll on chaos synchronization in the sense of drive–response configuration [1], chaos synchronization has been an active research topic for its potential usage in communications [2–4], radars [5,6], and other related applications [7] over the past two decades. Generally speaking, under the drive–response configuration, chaos synchronization refers to that the response (receiver) system adjusts its state to have precisely identical trajectories as the drive (transmitter) system by different approaches [8–10]. Chaos synchronization plays an important role in chaos-based communications because it offers theoretical advantages over noncoherent detections in terms of noise performance and data rate when the information signal is recovered from the noisy, distorted received signal [11].

However, the chaos synchronization performance is very sensitive to channel conditions and system parameter mismatches, which has become one of the major barriers to apply chaos in the real-world communications. The channel conditions mainly include the additive white Gaussian noise (AWGN) and the multipath fading effect where several signals arriving from different signal paths have different amplitudes and phases [12]. The system parameter mismatches mainly come from device model mismatches and circuit component fabrication errors. Chaos synchronization under different channel conditions along with parameter mismatches in transmitter and receiver remains a very challenging problem.

Nevertheless, plentiful research efforts continue on the study of chaos synchronization for communication because of its potentially attractive performance. Recently, many researchers have focused on utilizing digital signal for

transmission or digital signal processing at the receiver to eliminate the negative effects from channels and system parameter mismatches for achieving better synchronization performance [13–16]. These approaches include parameter estimation, parameter identification, and observer-based digital filter [8,17–19], among which the digital-filter-based schemes show good synchronization performance when both the channel effects and parameter mismatches are considered. This is because signal in its digital form, compared with its analog counterpart, is more resistant to distortions caused by channels and circuit parameters and more convenient for applying various kinds of powerful digital signal processing techniques.

Although a number of digital-filter-based synchronization schemes have appeared in the literature, there are very few reports on their experimental study that is very important for evaluating the feasibility of synchronization scheme in practice. In [18], Shi *et al*. conducted an experimental study on the synchronization of Chua's circuit by using particle filtering (PF), which is a state-of-the-art solution for nonlinear and non-Gaussian problems, at the receiver. This is the first time that the digital-filter-based chaos synchronization scheme is verified by experiment. However, the nonlinearity of Chua's circuit is formed by piece-wise linear current–voltage ($I$–$V$) relationship in which the nonlinearity is not very severe. On the contrary, the nonlinearity of the famous Colpitts circuit is in an exponential form [20], which means much more complexity and diversity existing in dynamics and waveforms. Chaotic secure communication system uses chaotic signal to mask information signal [21]. Intuitively, the more complex and diverse the chaotic signal is, the better it is for chaotic secure communications [22]. Therefore, the chaotic Colpitts circuit is a good candidate for chaotic secure communication systems.

In [23], we have proposed a PF-based synchronization and communication scheme for the chaotic Colpitts circuit over the AWGN channel. In this paper, we extend the work in [23] by fully studying the synchronization and communication over both the AWGN channel and the multipath fading channel, proposing an improved auxiliary particle filter (IAPF) algorithm considering the feature that the chaotic attractor is confined in a bounded state space and conducting a security analysis of the proposed communication system. The main contribution of this paper can be summarized as follows.

- First, we propose a synchronization scheme based on the novel IAPF for chaotic Colpitts circuit and build a prototype board of chaotic Colpitts circuit and an IAPF-based synchronization experimental platform.
- Second, we conduct extensive experiments to show that synchronization can be achieved and maintained with low signal-to-noise ratio (SNR) over both the AWGN channel and the multipath fading channel, even when severe parameter mismatches are considered.
- Third, we demonstrate by experiment the feasibility of a chaos-masking communication system based on the synchronization scheme and evaluate the bit-error-rate (BER) performance versus different SNRs and symbol rates, where both the AWGN channel and the multipath fading channel are considered.
- Fourth, we carry out a security analysis by studying the size of the key space of the chaos-masking secure communication system and show that it is resistant to the brute-force attack.

The remainder of this paper is organized as follows. In Section 2, we propose the synchronization scheme for the chaotic Colpitts circuit by utilizing the novelly designed IAPF. In Section 3, we present the experimental results on the synchronization performance over both the AWGN channel and the multipath fading channel with system parameter mismatches considered. In Section 4, we implement a chaos-masking secure communication system with the synchronization scheme and study its BER performance. In Section 5, we conduct security analysis of the chaos-masking secure communication system. Finally, we conclude this paper in Section 6.

## 2. PROPOSED SYNCHRONIZATION SCHEME OF CHAOTIC COLPITTS CIRCUIT

In this section, we first give a systematic structure of the proposed synchronization scheme and present the implementation details of the chaotic Colpitts circuit. After that, we describe how the receiver is constructed, including how to obtain the measurement for the receiver, how to establish the digitalized state and measurement equations for the filter, and how to design the IAPF algorithm for the synchronization problem.

### 2.1. Structure of the improved auxiliary particle filter-based synchronization scheme

The systematic structure of the proposed synchronization scheme is depicted in Figure 1. The chaotic signal is first generated by a physically implemented Colpitts circuit and passed through an AWGN channel or a multipath fading channel. Then, the signal is sampled by an analog-to-digital converter, and the obtained digital signal is fed to a digital filter for chaos synchronization. The AWGN channel can be implemented by mixing the sampled signal with the manually generated noise according to different SNR conditions. The multipath fading channel with AWGN can be implemented by applying an autoregressive (AR) model to the sampled signal and then mixing the signal with the manually generated noise according to different SNR conditions.

In Figure 1, we use the IAPF at the receiver for the synchronization of the chaotic Colpitts circuit. In comparison

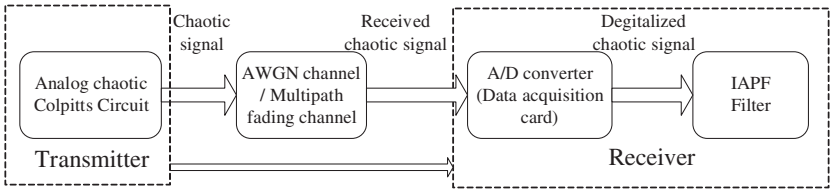



**Figure 1.** Synchronization structure of analog chaotic Colpitts circuit utilizing improved auxiliary particle filter (IAPF). AWGN, additive white Gaussian noise; A/D, analog to digital.

with PF, the auxiliary particle filter (APF) [24] is more suitable for chaos synchronization. In this work, we improve the APF by incorporating the feature that chaotic attractor is bounded in the state space into the design of the initialization and sampling of the IAPF.

## 2.2. Chaotic signal generation by Colpitts circuit

The Colpitts circuit is a third-order autonomous chaotic circuit, and its inherent dynamics leading to chaos was reported for the first time in 1994 [25]. The mathematical model and the nonlinear analysis of the chaotic Colpitts oscillator have been studied in [20]. The design, implementation, and synchronization of chaotic Colpitts circuit has been an active topic in recent years.

Figure 2 shows the schematic diagram of the chaotic Colpitts circuit studied in this work. The circuit parameters are as follows: $L = 2.2$ mH, $C_1 = C_2 = 220$ nF, $R = 100\ \Omega$, $R_e = 2$ k$\Omega$, $V_{cc} = 9.3$ V, and $V_{ee} = -5$ V. The bipolar junction transistor (BJT) used is Philips (Amsterdam, The Netherlands) MMBT2222A. PSpice simulations demonstrate the generation of chaotic oscillation from the chaotic Colpitts circuit with the aforementioned parameters, as shown in Figure 3. Also, the time-domain waveforms of $V_{C_1}$ and $V_{C_2}$ are plotted in Figure 4, where $V_{C_1}$ and $V_{C_2}$ denote the voltage across the capacitors $C_1$ and $C_2$, respectively.

The prototype board of the physically implemented Colpitts circuit is shown in Figure 5. Note that there are several differences between the schematic in Figure 2 and the prototype board. First, besides the basic circuit components shown in Figure 2, the physically implemented

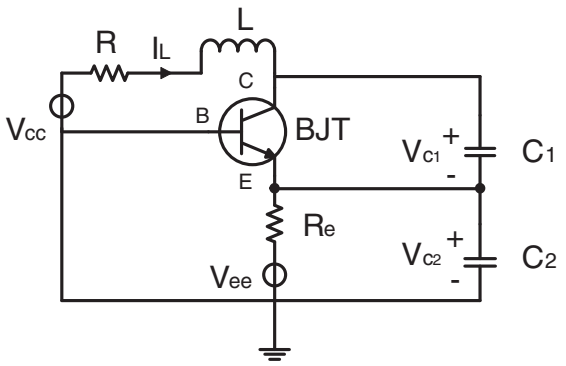



**Figure 2.** Schematic diagram of the Colpitts circuit.

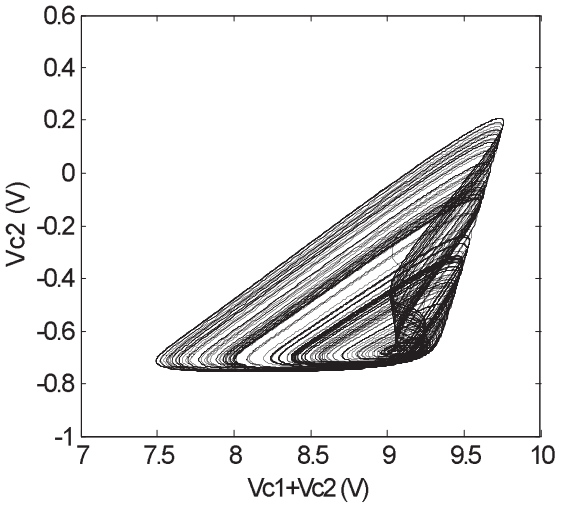



**Figure 3.** Chaotic attractor of the Colpitts circuit from PSpice simulation.

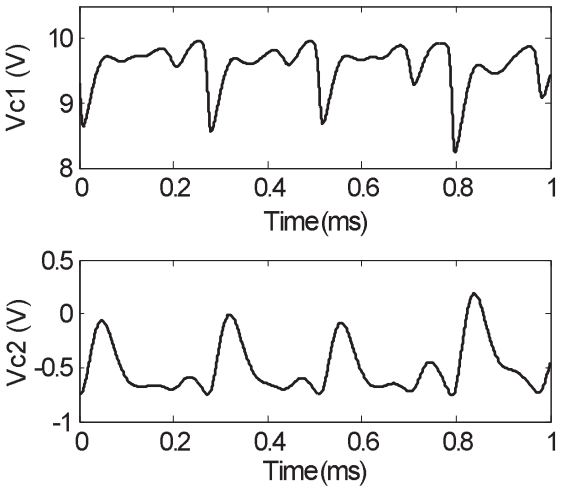



**Figure 4.** Time-domain waveforms of $V_{C1}$ and $V_{C2}$ from PSpice simulation.

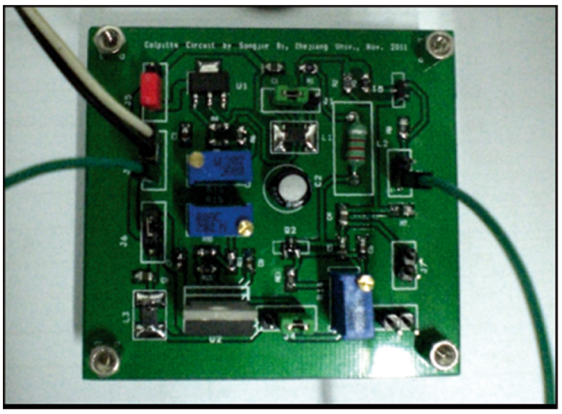


**Figure 5.** Prototype board of the chaotic Colpitts circuit.

**Table I.** Error percentage of circuit components.

| | Resistance | Inductance | Capacitance |
|---|---|---|---|
| Percentage (%) | ± 1 | ± 5 | ± 5 |

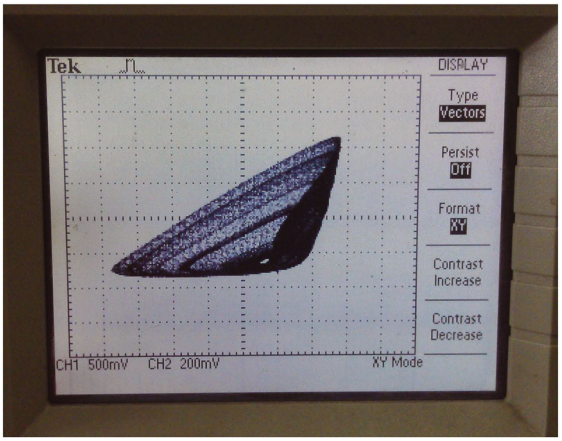



**Figure 6.** Chaotic attractor observed on oscilloscope.

circuit has two voltage regulator modules that aim to provide stable voltage sources and an output buffer that is used to minimize the loading impact of the oscilloscope probe or data acquisition card. Additionally, the real values of the circuit components always deviate from the marked values. The inherent possible deviations from the marked values to the real values obtained from the circuit components manufactures are listed in Table I.

The prototype board exhibits chaotic oscillation when using the same circuit parameters as those in PSpice simulation. Figure 6 shows the chaotic attractor observed from a Tektronix (Beaverton, OR, United States) oscilloscope TDS 1002. The overall shape is very similar to that in Figure 3. Figure 7 plots the time-domain waveforms of $V_{C_1}$ and $V_{C_2}$ obtained by the data acquisition card RBH-8578 with 5 MHz sampling frequency. The RBH-8578 is capable of simultaneously sampling two channels of analog signals

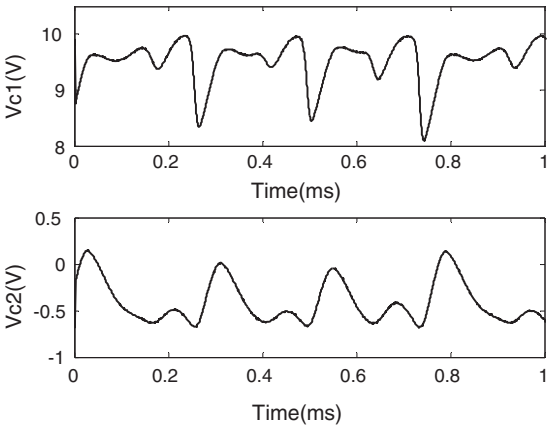



**Figure 7.** Time-domain waveforms of $V_{C1}$ and $V_{C2}$ acquired by the data acquisition card.

into their digital forms and sending the transformed digital signals to a computer via a universal serial bus interface.

## 2.3. Digitalized state and measurement equations

As shown in Figure 1, when the data acquisition card RBH-8578 completes the sampling of analog chaotic signal and sends the transformed digital signal to the computer, an IAPF is designed at the receiver to process these discrete time signals to track the state of the transmitter circuit for achieving chaos synchronization. For comparative study, signals from the prototype board and that from the PSpice simulation are both sent to the IAPF, which is implemented in MATLAB (Natick, Massachusetts, United States) on a Lenovo (Beijing, China) computer.

The state equation of the analog Colpitts circuit is [20]

$$\begin{cases} \frac{dV_{C_1}(t)}{dt} = \frac{1}{C_1}(-f(-V_{C_2}(t)) + I_L(t)) \\ \frac{dV_{C_2}(t)}{dt} = \frac{1}{C_2}\left(I_L(t) - \frac{V_{C_2}(t)-V_{ee}}{R_e}\right) \\ \frac{dI_L(t)}{dt} = \frac{1}{L}\left(-V_{C_1}(t) - V_{C_2}(t) - I_L(t)R + V_{cc}\right) \end{cases} \tag{1}$$

where $f(\cdot)$ is the driving-point characteristic of the nonlinear resistor of the BJT, which is usually described as

$$\begin{aligned} f(x) &= I_s\left[exp\left(\frac{x}{V_T}\right) - 1\right] \\ &\approx I_s[exp\left(\frac{x}{V_T}\right)], \text{ when } x \gg V_T \end{aligned} \tag{2}$$

where $I_s$ is the inverse saturation current of the BJT and $V_T \simeq 26$ mV at room temperature.

For the Colpitts circuit shown in Figure 2, the driving-point characteristic can be expressed as $I_E = f(V_{BE}) =$

$f(-V_{C_2})$, and from (2), it follows that

$$f\left(-V_{C_2}(t)\right) = I_s\left[exp\left(-\frac{V_{C_2}(t)}{V_T}\right)\right] \tag{3}$$

The transmitted signal is

$$V_T(t) = V_{C_1}(t) + V_{C_2}(t) \tag{4}$$

After the signal is sent through an AWGN channel, it becomes

$$V_{arrive}(t) = V_{C_1}(t) + V_{C_2}(t) + v(t) \tag{5}$$

where $v(t)$ is the zero-mean white Gaussian noise induced by the AWGN channel. The SNR is defined as $10log\left(var\left(V_{C_1}+V_{C_2}\right)/\sigma_v^2\right)$, where $\sigma_v^2$ is the variance of the noise $v(t)$ and the function $var(.)$ returns the variance of its input.

The multipath fading channel is more common than the AWGN channel for wireless communications [26,27]. For the multipath fading channel, the received signal in (5) can be rewritten by using the AR model [28], that is,

$$\tilde{V}_{arrive}(t) = \sum_{i=1}^{p} a_i(t-\tau_i)V_T(t-\tau_i) + w(t) \tag{6}$$

where $a_i(t-\tau_i)$ and $\tau_i$ denote the time-varying coefficient and the time delay of the $i$-th path signal, respectively, $p$ denotes the order of the model, and $w(t)$ is an AWGN. The SNR is defined as $10log(var\left(\sum_{i=1}^{p} a_i(t-\tau_i)V_T(t-\tau_i)\right)/\sigma_w^2)$, where $\sigma_w^2$ denotes the variance of the noise $w(t)$.

To implement the digital filter at the receiver, according to (1), the discrete version of the state equation is formulated as follows:

$$\boldsymbol{x}_k = \boldsymbol{\Phi}\boldsymbol{x}_{k-1} + \boldsymbol{G} \tag{7}$$

where

$$\boldsymbol{x}_k = \begin{pmatrix} V_{C_1}(kT) \\ V_{C_2}(kT) \\ I_L(kT) \end{pmatrix},$$

$$\boldsymbol{G} = \begin{pmatrix} -f(V_{C_2}((k-1)T))T/C_1 \\ V_{ee}T/(C_2R_e) \\ V_{cc}T/L \end{pmatrix},$$

$$\boldsymbol{\Phi} = \begin{pmatrix} 1 & 0 & T/C_1 \\ 0 & 1-T/(C_2R_e) & T/C_2 \\ -T/L & -T/L & 1-RT/L \end{pmatrix}$$

where $k$ is the time index and $T$ is the sampling interval of the acquisition card.

For the AWGN channel, the measurement equation is

$$z_k = \mathbf{x}_k[1] + \mathbf{x}_k[2] + v_k \tag{8}$$

where $z_k$ denotes the measurement at time $k$, $\mathbf{x}_k[i]$ denotes the $i$-th element of the vector $\mathbf{x}_k$ at time $k$, and $v_k$ is the $v(t)$ at time $k$.

For the multipath fading channel, the discrete version of the state equation is the same as that over the AWGN channel. However, when it comes to the measurement equation, it is totally different from the AWGN case. Here, we assume that the channel coefficients of the multipath fading channel can be obtained by means of some channel estimation techniques, and thus, all channel coefficients are known. Thus, the measurement equation is

$$z_k = \sum_{i=1}^{p} \hat{a}_{k-l_i}^{i}\left(\mathbf{x}_{k-l_i}[1] + \mathbf{x}_{k-l_i}[2]\right) + w_k \tag{9}$$

where $l_i$ is the discrete time delay of the $i$-th path, $\hat{a}_{k-l_i}^{i}$ denotes the discrete coefficient of the $i$-th path at time $k-l_i$, and $w_k$ is the discrete version of $w(t)$.

## 2.4. Improved auxiliary particle filter algorithm

From the filtering perspective, particle filter is a combination of the Bayesian filter theory and the Monte Carlo (MC) method, and the system state $\mathbf{x}_k$ can be estimated based on the set of all available measurements $z_{1:k} = \{z_i, i = 1,\ldots,k\}$ up to time $k$. It is known that $\mathbf{x}_k$ can be estimated by constructing the posterior probability density function $p(\mathbf{x}_k|z_{1:k})$. Taking advantage of the MC method, the posterior probability density function can be approximated as

$$p(\mathbf{x}_k|z_{1:k}) \approx \sum_{i=1}^{N_s} w_k^i \delta\left(\mathbf{x}_k - \mathbf{x}_k^i\right) \tag{10}$$

where $\delta(\cdot)$ is the Dirac delta function and $\left\{\mathbf{x}_k^i, i = 0,\ldots, N_s\right\}$ denotes a set of supporting particles with associated weights $\left\{w_k^i, i = 1,\ldots,N_s\right\}$.

In this work, to achieve better synchronization performance, we design the IAPF at the receiver. In comparison with PF, the APF naturally generates particles from the sample at the previous iteration conditioned on the current measurement, and thus, the particles are most likely to be closer to the true state. Also, the APF can be viewed as adding another resampling procedure according to the measurement at next iteration, which includes information from the future. These characteristics of the APF make it very suitable for tracking dynamic systems that have small process noise [24], similar to the chaotic Colpitts circuit (1) studied in this work. Thus, we select the APF as the filter algorithm basis and try to improve it for the synchronization of the chaotic Colpitts circuit.

Because the chaotic trajectories generated from a chaotic circuit are generally confined in a bounded state space, we can make use of this feature and improve the APF for chaos synchronization. At the receiver, because the circuit parameters are known, the possible maximum and minimum

**Algorithm 1** IAPF algorithm for chaos synchronization

**BEGIN:**

1) Loop Initialization: $k = 0$

**for** $i = 1, 2, ..., N_s$ **do**
  Draw $\mathbf{x}_0^i$ using the procedure proposed in [17];
  Assign particle weight $w_k^i = 1/N_s$;
**end for**

2) Main Loop:

**for** k=1,2,... **do**
  **for** $i = 1, 2, ..., N_s$ **do**
    Calculate $\mu_k^i$;
    **while** $\mu_k^i$ outside the attractor boundary **do**
      $\mu_k^i = 0.99\mu_k^i$;
    **end while**
    $w_k^i = q(i|z_{1:k}) \propto p(z_k|\mu_k^i) w_{k-1}^i$;
  **end for**
  Calculate total wight $t = \sum_{i=1}^{N_s} w_k^i$;
  **for** $i = 1, 2, ..., N_s$ **do**
    Normalize: $w_k^i = t^{-1} w_k^i$;
  **end for**
  Do resampling using systematic resampling algorithm:
  {-,-,$i^j$}=RESAMPLING($\{\mathbf{x}_k^i, w_k^i\}_{i=1}^{N_s}$);
  **for** $j = 1, 2, ..., N_s$ **do**
    Draw $\mathbf{x}_k^j \sim q(\mathbf{x}_k|i^j, z_{1:k}) = p(\mathbf{x}_k|x_{k-1}^{i^j})$;
    **while** $\mathbf{x}_k^j$ outside the attractor boundary **do**
      $\mathbf{x}_k^j = 0.99\mathbf{x}_k^j$;
    **end while**
    Assign weight $w_k^j$ using (12);
  **end for**
  Calculate total wight $t = \sum_{i=1}^{N_s} w_k^i$;
  **for** $i = 1, 2, ..., N_s$ **do**
    Normalize: $w_k^i = t^{-1} w_k^i$;
  **end for**
  State estimation: $\mathbf{x}_k = \sum_{i=1}^{N_s} \mathbf{x}_k^i w_k^i$;
**end for**

**END;**

values of the state variables $V_{C_1}^{max}$, $V_{C_1}^{min}$,$V_{C_2}^{max}$, $V_{C_2}^{min}$, $I_L^{max}$ and $I_L^{min}$ can be obtained to form the bounded state space. Then, in the IAPF, the information can be used in both the initialization and main iteration loop to improve the synchronization performance. Although the idea has been used in the initialization of PF in [17], we extend the usage of the information to the main iteration loop in this work. The IAPF for chaos synchronization is described in Algorithm 1.

In the proposed IAPF, the first step is to initialize the particle $\mathbf{x}_0^i$. This is conducted by using the bounded state space information, and the details of the procedure can be found in [17]. Then, in the main iteration loop, we sample the pair $\left\{\mathbf{x}_k^j, i^j\right\}_{j=1}^{N_s}$, where $i^j$ denotes the index of the particle at $k-1$, from an importance density $q(\mathbf{x}_k, i|z_{1:k})$ that is defined to satisfy the proportionality

$$q(\mathbf{x}_k, i|z_{1:k}) \propto p\left(z_k|\mu_k^i\right) p\left(\mathbf{x}_k|\mathbf{x}_{k-1}^i\right) w_{k-1}^i \quad (11)$$

where $\mu_k^i \sim p\left(\mathbf{x}_k|\mathbf{x}_{k-1}^i\right)$ is a sample of $\mathbf{x}_k$ with a given $\mathbf{x}_{k-1}^i$. Note that when each $\mu_k^i$ is generated, they are also confined in the bounded state space.

After $\mu_k^i$ and its corresponding $w_k^i$ are generated, systematic resampling is conducted to obtain the $\left\{\mathbf{x}_k^j, i^j\right\}$ according to $w_k^i$. Then, from the resampling results, one can sample the particles in the current time with the corresponding weight update equation formulated as [24]:

$$\begin{aligned} w_k^j &\propto w_{k-1}^{i_j} \frac{p\left(z_k|\mathbf{x}_k^j\right) p\left(\mathbf{x}_k^j|\mathbf{x}_{k-1}^{i_j}\right)}{q\left(\mathbf{x}_k^j, i^j|z_{1:k}\right)} \\ &= \frac{p\left(z_k|\mathbf{x}_k^j\right)}{p\left(z_k|\mu_k^{i_j}\right)} \end{aligned} \quad (12)$$

After the weights are normalized, state estimation can be obtained from the particles and their corresponding weights.

## 3. EXPERIMENTAL STUDY OF CHAOS SYNCHRONIZATION

It is well known that digital-filter-based synchronization schemes for analog chaotic circuits have various kinds of advantages. However, it is highly necessary to conduct an experimental study on the feasibility of them for the following reasons.

From the circuits and systems point of view, firstly, the state equation used in digital filters is generally a simplified version of its physical circuit implementation and may far or less deviate from the true circuit parameter/model conditions; secondly, the parameters in physical circuits cannot be obtained accurately because they always deviate from the marked values with time-varying characteristics; last but not least, the influences of inherent small noises in circuits cannot be neglected because of the sensitivity of chaotic systems. In addition, from the communication point of view, both the AWGN channel and the multipath fading channel have to be considered to evaluate the synchronization performance and the applicability to communications.

In this section, we present the experimental results of the synchronization performance over the AWGN channel and the multipath fading channel. The effects of circuit parameter mismatches between the transmitter and the receiver are considered for both cases.

### 3.1. Synchronization over the additive white Gaussian noise channel

In this section, we present the experimental results of the IAPF-based synchronization over the AWGN channel. A series of experiments are conducted to study the effects of parameter mismatches and different noise levels (described in terms of SNR) on the synchronization performance, which is evaluated by defining the average attractor distance (AAD) as

$$D = \lim_{t_s \to \infty} \frac{\int_{t_0}^{t_s} \sqrt{e_1^2 + e_2^2}\, dt}{t_s - t_0} \tag{13}$$

where $e_1 = V_{C_1} - \tilde{V}_{C_1}$, $e_2 = V_{C_2} - \tilde{V}_{C_2}$, and $t_0$ denotes the settling time during which the transient parts of the signals have passed. The value of $D$ will be zero if the transmitter and the receiver are exactly synchronized; otherwise, a bigger value of $D$ indicates a worse synchronization performance.

#### 3.1.1. Time evolution of synchronization.

For comparison reason, we send signals generated from the PSpice simulation and the prototype board to the receiver to see whether the synchronization can be achieved. Figures 8 and 9 show the experimental results to demonstrate the time evolution of synchronization for the data from both the PSpice simulation and the prototype board, respectively, where the SNR equals 10 dB. It can be seen that the transmitter's state can be estimated and tracked, which means synchronization can be achieved and maintained no matter the transmitted signals are from the PSpice simulation or prototype board. And the synchronization is achieved in a very short settling time even when the initial state of the receiver is far apart from that of the transmitter, which means that the synchronization scheme features rapid convergence characteristics.

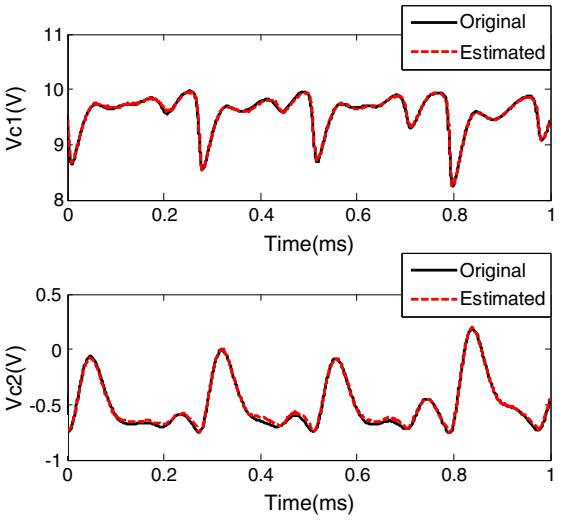



**Figure 8.** Synchronization process based on the PSpice data over additive white Gaussian noise channel.

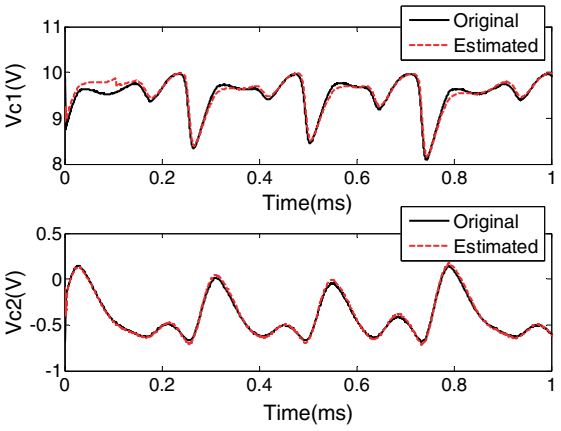



**Figure 9.** Synchronization process based on data from the prototype board over additive white Gaussian noise channel.

#### 3.1.2. Synchronization performance versus different signal-to-noise ratios.

By observing the values of AAD, we conduct a set of experiments to find out whether the scheme can satisfactorily dispel the sensitivity to noise. The AAD versus different SNRs over the AWGN channel is plotted with squared line in Figure 10. It can be seen that the synchronization performance becomes better with the increment of SNR.

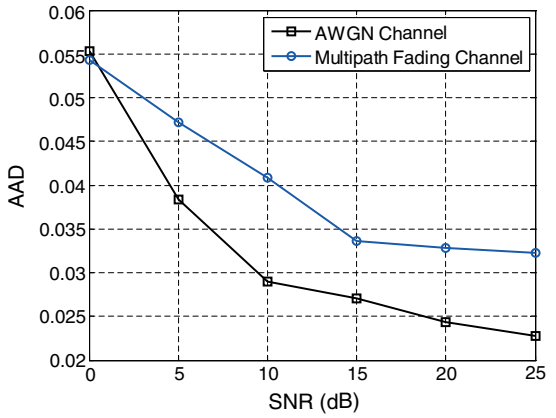



**Figure 10.** The average attractor distance (AAD) versus different signal-to-noise ratios (SNRs) over additive white Gaussian noise (AWGN) channel and multipath fading channel.

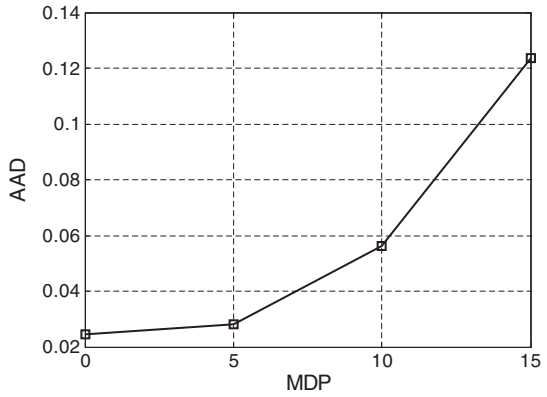



**Figure 11.** The average attractor distance (AAD) versus different maximum deviation percentages (MDPs) over additive white Gaussian noise channel.

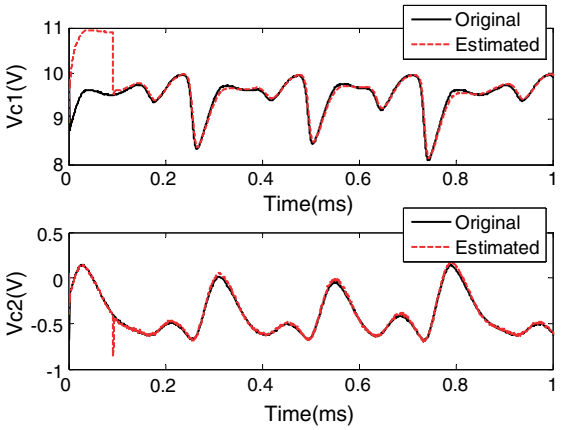



**Figure 12.** Time-domain waveform of $V_{C1}$ and $V_{C2}$ in transmitter and receiver with a maximum deviation percentage of 10% over additive white Gaussian noise channel.

Note that even when the value of the AAD is 0.03 (the corresponding SNR is about 10 dB), synchronization performance is good according to the corresponding time-domain waveform of the transmitter and the receiver in Figure 9. Consequently, the proposed scheme can be regarded as an effective way for chaos synchronization with the existence of AWGN distortions.

### 3.1.3. Synchronization performance versus parameter mismatches.

The sensitivity to parameter mismatches is another important issue. Synchronization performance of some traditional schemes degrades severely because of parameter mismatches. To investigate whether the IAPF-based synchronization scheme is resistive to parameter mismatches, a series of experiments are conducted with an additional error-introducing process, which can artificially introduce errors within a certain degree in order to imitate the parameter mismatches in practice. The concrete process of it is described as follows.

Firstly, we set a maximum deviation percentage (MDP), namely $p\%$, and the circuit component parameters including $L$, $C_1$, $C_2$, $R$, and $R_e$ are all confined in an interval between a minimum value and a maximum value determined by the MDP. Specifically, for a given circuit parameter with marked value $x$, its maximum and minimum values are $(1+p\%)x$ and $(1-p\%)x$, respectively. Then, the parameter interval is formed in the interval $((1+p\%)x, (1-p\%)x)$, and the parameter is assumed to be uniformly distributed in this interval each time when generated. In other words, each time a synchronization experiment is conducted, each component parameter is randomly generated with equal probability from the corresponding parameter interval.

When one set of parameters are generated, we use them in the IAPF and calculate the AAD. We conduct 100 MC experiments to obtain the average AAD for each MDP, and the results are shown in Figure 11, where the SNR equals 20 dB. It can be seen that the AAD increases with the increment of the MDP. As the parameter mismatches increase, the synchronization performance will be degraded. The best synchronization performance is achieved when the MDP equals 0, which means there is no parameter mismatch.

To further provide a better insight of the synchronization performance, Figure 12 shows the time-domain waveform of the transmitter and the receiver with the MDP of 10%, with the corresponding AAD approximately equaling 0.055, as shown in Figure 11. From Figure 12, it can be seen that even when the MDP is 10%, the synchronization performance seems good. Therefore, the proposed synchronization scheme is capable of obtaining a good synchronization performance when taking parameter mismatches into consideration. However, further experiments show that when the MPD increases to more than 15%, desynchronization may occur.

### 3.2. Synchronization over multipath fading channel

According to the AR model, we have obtained the measurement equation for the multipath fading channel as (9). It is assumed that conditions of all the signal transmission paths are known, and the paths in (6) are described by

$$P_i = \{a_i, \tau_i\}, i = 1, \ldots, p \tag{14}$$

In the experiment, we define a total of six transmission paths: $P_1 = \{1, 0 \text{ ms}\}$, $P_2 = \{0.6 + 0.1cos(t), 0.03 \text{ ms}\}$, $P_3 = \{0.2 + 0.2sin(t), 0.046 \text{ ms}\}$, $P_4 = \{0.55 - 0.3cos(t), 0.142 \text{ ms}\}$, $P_5 = \{0.1 - 0.1sin(t), 0.178 \text{ ms}\}$, $P_6 = \{0.28, 0.2 \text{ ms}\}$. Note that channel coefficients of the second to the fifth paths are time-varying. This makes the measurement equation (9) a highly nonlinear function.

The AAD versus different SNRs over the multipath fading channel is depicted in Figure 10. It can be seen that the synchronization performance becomes better with the increment of SNR. However, when comparing the AAD results over the multipath fading channel with that over the AWGN channel, the synchronization performance over the AWGN channel is better than that over the multipath fading channel. This can be explained as that, over the multipath fading channel, both the state equation of the system (1) and the measurement equation (9) are highly nonlinear functions, and the time-varying amplitudes and delays of channel coefficients make it even more difficult for synchronization. Consequently, the synchronization performance is relatively not as good as that over the AWGN channel.

Although the synchronization performance over the multipath fading channel is not as good as that over the AWGN channel, it is still considerably good, as shown in Figure 13, which plots the time-domain waveform of the transmitter and the receiver over the multipath fading channel, where the SNR is 15 dB, and we obtain an AAD of 0.034. Although the synchronization performance degrades a little bit in comparison with that over the AWGN channel, it is acceptable for chaotic communications.

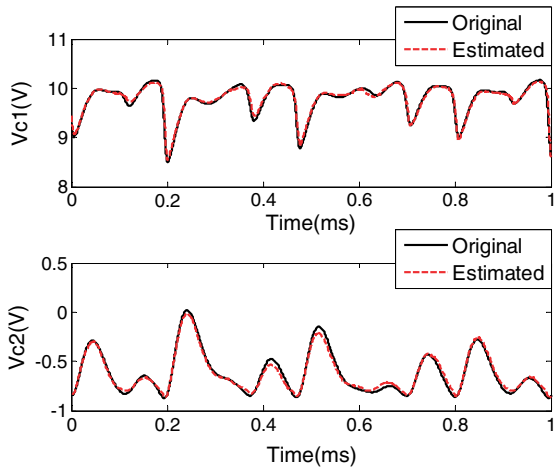



**Figure 13.** Time-domain waveform of $V_{C1}$ and $V_{C2}$ in the transmitter and the receiver over multipath fading channel.

## 4. APPLICATION TO SECURE COMMUNICATION

In chaos-based secure communications, security is achieved by embedding information signal into the complex dynamic behaviors provided by chaotic systems. In this section, we consider the chaos-masking secure communication system based on the synchronization of chaotic Colpitts circuit. The reason of using chaos masking for secure communication experiment is that the effect of chaos masking on synchronization performance is much significant that in other chaos modulation schemes, such as chaos shift keying or chaotic parameter modulation. Thus, if the chaos-masking secure communication system is feasible, it is most probably that communication with other modulation schemes is also feasible. In this section, the system configuration is described first, and then, the experimental results of communication over both the AWGN channel and the multipath fading channel are given, where the time domain transmitted and decoded signal, the BER performance versus SNR, and the symbol period (SP) are illustrated in detail.

### 4.1. Chaotic secure communication configuration

Figure 14 shows the chaos-masking communication system with the synchronization scheme over the AWGN channel. The transmitter modulates the chaotic carrier $x(t)$ by adding the information signal $s(t)$ to the chaotic signal and then forms the transmitted signal

$$z(t) = x(t) + s(t) \tag{15}$$

After passing through an AWGN channel, the received signal becomes

$$r(t) = x(t) + s(t) + v(t) \tag{16}$$

According to (4), the received signal is

$$r(t) = V_T(t) + s(t) + v(t) \tag{17}$$

When $r(t)$ is received, the IAPF at the receiver synchronizes and recovers the chaotic carrier $V_T(t)$. Then, we obtain the recovered information signal as

$$s'(t) = r(t) - V_T(t) \tag{18}$$

In the experiment, the prototype board shown in Figure 5 acts as the chaos generator, and the IAPF implemented

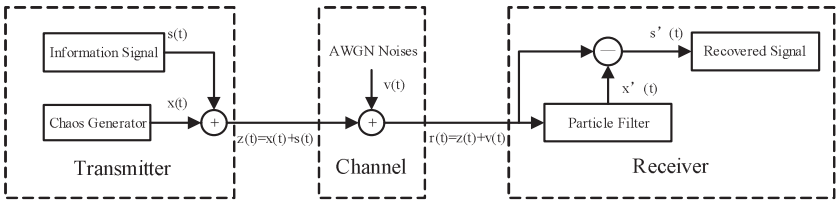



**Figure 14.** Chaos-masking communication system over additive white Gaussian noise (AWGN) channel.

in MATLAB is responsible for synchronizing the chaotic carrier that has been contaminated by channel noises, modulated signal, and quantization error. Here, the information symbol set contains only two symbols, that is,

$$s = \{0, 1\} \tag{19}$$

and the information signal $s(t)$ is a rectangular digital waveform with a peak-to-peak amplitude of 0.15 V, which is approximately one-tenth of the peak-to-peak value of the carrier. During the "1" information SP, the signal level of $s(t)$ is high; otherwise, it is low. After passing through the AWGN channel, the received signal is sampled by the data acquisition card and sent to the IAPF to obtain the recovered carrier $V_T(t)$. Then, $s'(t)$ is obtained by subtracting $V_T(t)$ from $r(t)$, as shown in (18). Finally, decoding can be conducted by averaging $s'(t)$ during each SP and comparing the mean value with a threshold. According to the feature of information signal and noise, it is recommended to take half of the peak-to-peak amplitude of the information signal as the threshold.

For the multipath fading channel situation, the communication system is the same as that shown in Figure 14 except that the channel contains not only the AWGN noise but also the multipath fading. The received signal under this condition will be described in Section 4.3.

## 4.2. Communication over additive white Gaussian noise channel

We conduct the communication experiment over the AWGN channel first. Figure 15 plots the waveforms of the original information signal $s(t)$ and the recovered information signal $s'(t)$, where the SNR is 20 dB and the SP is 200 μs. From the figure, the recovered information signal $s'(t)$ has been contaminated by channel noises, parameter mismatches, quantization error, and others. However, it can still be recovered from this contaminated signal based on the scheme described earlier.

For the chaotic communication system over the AWGN channel, two factors, namely the SNR and the SP, have significant influences on the communication performance. Experiments are conducted, and the results are shown in Figures 16 and 17.

Figure 16 shows the BER with the increment of information SP when the SNR equals 10 dB. It can be seen that the BER decreases with the increment of the SP. A longer SP is expected to have a lower BER because of the enhancement of resistance to noise, while it results in a lower symbol rate. Therefore, for different applications, proper compromise of the SP is needed according to different system requirements of BER and data rate.

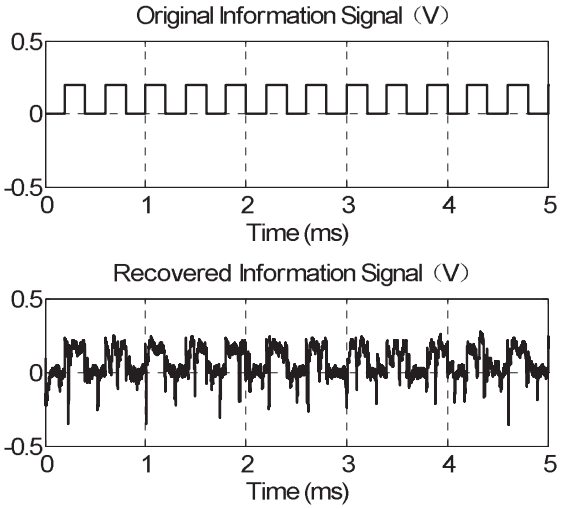



**Figure 15.** Time-domain waveform of $s(t)$ and $s'(t)$ over the additive white Gaussian noise channel.

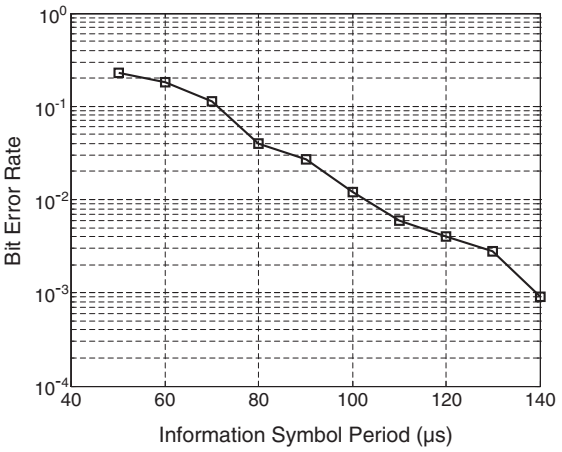



**Figure 16.** Bit error rate versus different information symbol periods ($SNR = 10$ dB).

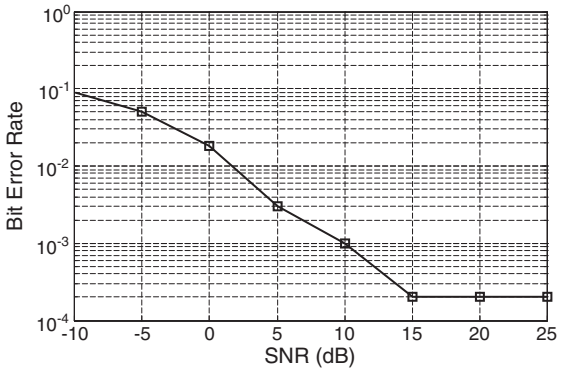



**Figure 17.** Bit error rate versus different signal-to-noise ratios (SNRs) ($SP = 140\ \mu s$).

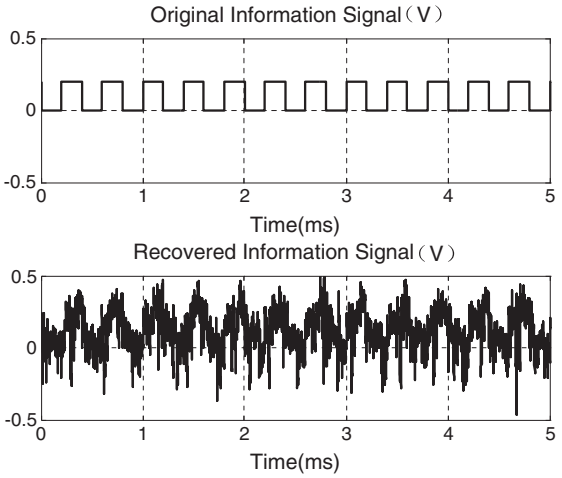



**Figure 18.** Time-domain waveform of $s(t)$ and $s'(t)$ over the multipath fading channel.

Figure 17 shows the BER with different SNRs when the SP equals 140 $\mu$s. It can be seen that the IAPF can efficiently reduce the negative effect caused by channel noises and recover the information signal. As shown in Figure 17, the BER decreases with the increment of SNR when it is below 15 dB, and then, the BER remains at approximately the same level even when the SNR increases. In other words, after the threshold of SNR, the BER reaches its performance floor because in this case, the synchronization error, caused by parameter mismatches other than the channel noise, becomes the dominant factor that affects the communication performance.

### 4.3. Communication over multipath fading channel

Over the multipath fading channel, the received signal is composed of several signals arriving from different paths with different time delays. According to the AR model, the received signal in (16) is

$$r_{multipath}(t) = \sum_{i=1}^{p} a_i(t-\tau_i)[V_T(t-\tau_i)+s(t-\tau_i)]+w(t) \tag{20}$$

In order to obtain the recovered information signal similar to (18), firstly, we have to recover the main path signal by subtracting the branch-path signals from $r_{multipath}(t)$, that is,

$$r_{main}(t) = r_{multipath}(t) - \sum_{i=2}^{p} a_i(t-\tau_i)\left[V_T(t-\tau_i)+s(t-\tau_i)\right] \tag{21}$$

Because the exact $V_T(t-\tau_i)$ and $s(t-\tau_i)$ at the previous time cannot be obtained, we substitute the estimated $V'_T(t-\tau_i)$ and $s'(t-\tau_i)$ into (21) and obtain

$$\tilde{r}_{main}(t) = r_{multipath}(t) - \sum_{i=2}^{p} a_i(t-\tau_i)\left[V'_T(t-\tau_i)+s'(t-\tau_i)\right] \tag{22}$$

Here, $\tilde{r}_{main}(t)$ can be regarded as the received signal $r(t)$ over the AWGN channel. Consequently, the recovered information signal can be obtained, and decoding can be completed by using the same strategies as that over the AWGN channel.

Figure 18 plots the original information signal $s(t)$ and the recovered information signal $s'(t)$ with the SNR of 20 dB when the SP equals 200 $\mu s$ and the MDP equals 1%. The recovered information signal $s'(t)$ has been contaminated more severely over the multipath fading channel in comparison with that over the AWGN channel. The performance degradation is mainly caused by the following reasons. First, the multipath fading with the amplitude of each path varying in a sinusoid format significantly increases the nonlinearity and complexity of the system and thus increases the difficulty of chaos synchronization. Furthermore, because $\tilde{r}_{main}(t)$ is calculated by employing the estimated time-delayed version of signals, that is, $V'_T(t-\tau_i)$ and $s'(t-\tau_i)$, deviation of the two signals may accumulate to enlarge the estimation error at the current iteration. However, even with these unfavorable factors, Figure 18 shows that it is still feasible to decode the transmitted symbol information.

Figure 19 illustrates the BER versus different SNRs over the multipath fading channel with the SP of 140 $\mu s$. By comparing with Figure 17, it can be seen that even though synchronization and recovery of transmitted information signal is much more difficult over the multipath fading channel, the BER does not decrease significantly, and the communication system is capable of obtaining a fairly satisfactory performance.

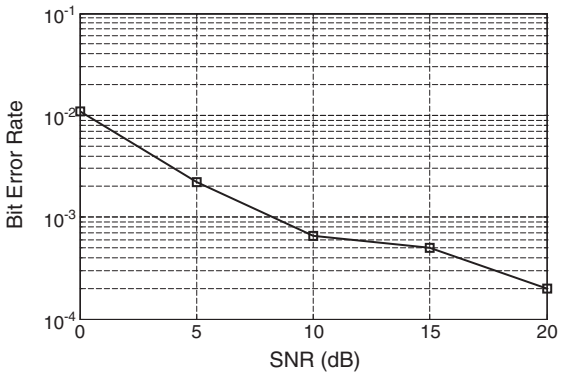



**Figure 19.** Bit error rate versus different signal-to-noise ratios (SNRs) over multipath fading channel ($SP = 140\ \mu s$).

### 4.4. Remarks

In the simulations of the proposed secure communication system over both the AWGN channel and the multipath fading channel, it is found that the BER has a lower bound around $10^{-4}$ when the SNR increases to a certain threshold value. This is because when the SNR is high enough, the effects of the parameter mismatches other than the channel effects become dominant to the communication performance. For many practical communication systems, it is generally required that the BER is in the order of $10^{-6}$. In the proposed communication system, this is possible when error correction coding techniques are incorporated into the systems. Although the BER improvement by using error correcting coding depends on the system configuration and channel modeling, it is usually easy to lower the BER two to three orders of magnitude [29]. Thus, it is feasible to apply the proposed communication system to real-world scenarios when some error correction coding techniques are incorporated.

The receiver in this work is constructed with a kind of PF. Because PF is based on the MC method, the computational complexity is inherently high and the real-time processing may become an implementation difficulty. Fortunately, some recent researches have shown that with dedicated designed hardware circuits in field programable gate arrays platform, the processing rate can achieve an order of magnitude of 100 kHz [30,31]. This indicates that the proposed communication system can meet the requirements in moderate data rate communications.

The application of the proposed synchronization scheme is not limited to communications. Another potential application is chaos-based radars. As discussed in [5,6], chaos-based radar has many distinguishing features such as excellent electronic counter, countermeasure performance, and the so-called multiuser characteristics, but all of these are highly dependant on robust chaos synchronization. The proposed synchronization scheme may pave a way for the chaos-based radar systems.

## 5. SECURITY ANALYSIS

There exist many types of attacks to chaos-based secure communication systems, among which the brute-force attack is one major type to break the whole secure communication system [2,21]. In this section, we will conduct a security analysis on the secure communication system to see whether it is resistant to the brute-force attack. From the cryptanalysis point of view, the precise values of the circuit parameters can be considered as the secret key of the cryptosystem.

From the previous section, the proposed synchronization scheme can have some degree of resistance to parameter mismatches. As discussed in [21], there is a paradox when considering the security property in the system here. On one hand, from the security requirements, the more the synchronization is sensitive to the parameter mismatches, the higher the security level is; on the other hand, the more the synchronization is insensitive to the parameter mismatches, the better synchronization and communication performance can be achieved. Because of the unavoidable parameter mismatches in circuit components and circuit modeling, the synchronization robustness to parameter mismatches is necessary, although it decreases the security level because it reduces the key space and makes the brute-force attack easier.

In the circuit shown in Figure 2, there are a total of eight parameters related to the chaotic dynamics, that is, $C_1$, $C_2$, $L$, $V_{cc}$, $V_{ee}$, $R$, $R_e$, and $I_s$. Although the normalized state equation contains less normalized parameters [20], we assume that the attacker cannot use the corresponding relationship between the normalized state equation and Equation (1) in this work because of the following reasons: First, the normalized state equation omits the physical meaning of circuit implementation, resulting in difficulty for attack; second, using the relationship will cause much more extra computational cost for the attacker; third, using the relationship requires that the attacker is a very “smart" attacker, not in a sense of brute-force. Thus, we consider the key space to be eight-dimensional under the assumptions.

The available information to the attacker is the fundamental frequency of the system that can be analyzed from the obtained chaotic waveforms. The fundamental frequency of the system is determined by

$$f_0 = (1/2\pi)\sqrt{(C_1 + C_2)/LC_1C_2} \tag{23}$$

In the implementation of the circuit in this paper, by analyzing the fundamental frequency, the attacker can only have the information that the inductor $L$ is approximately of 1 nH to 100 mH level (parameter interval $100 \times 10^{-3}$), and the capacitors $C_1$ and $C_2$ are in the order of 10 nF to 100 mF (parameter interval $100 \times 10^{-3}$). If a brute-force attacker searches the key space with 0.1 nH ($0.1 \times 10^{-9}$) step for the $L$, and 1 nF ($10^{-9}$) step for the $C_1$ and $C_2$, the size of the three-dimensional key space spanned by $L$, $C_1$, and $C_2$ is roughly

$$k_{3d} = \frac{100 \times 10^{-3}}{0.1 \times 10^{-9}} \times \frac{100 \times 10^{-3}}{10^{-9}} \times \frac{100 \times 10^{-3}}{10^{-9}} = 10^{25} \quad (24)$$

For the resistances $R$ and $R_e$, we can assume that they are in the range of 50–150 Ω and 1.5–2.5 kΩ, respectively, and correspondingly use 1 and 10 Ω steps for the brute-force attack. For the positive and negative voltage sources $V_{cc}$ and $V_{ee}$, we assume that for each parameter 100 values can be tried. For the inverse saturation current $I_s$, we assume that 1000 values can be tried because it is very sensitive to the system dynamics (1).

With the aforementioned assumptions, the size of the whole key space can be obtained as

$$k_{wh} = k_{3d} \times 10^2 \times 10^2 \times 100^2 \times 10^3 = 10^{34} \quad (25)$$

From [21], to provide a sufficient level of security against the brute-force attack, the size of the key space should be $\kappa > 2^{100}$. For our case, $k_{wh} = 10^{34} \gg 10^{30} \approx 2^{100}$. That means the communication system based on the proposed synchronization scheme can provide a sufficient level of security against the brute-force attack.

Note that (i) the assumptions about the step and the possible value interval of each parameter are conservative, meaning that the success of attacking the system cannot be guaranteed and (ii) the aforementioned analysis is conducted based on an underlying assumption that the attackers have the knowledge of the type of chaotic system for transmission and reception. If this is not known, the attack will become more difficult.

## 6. CONCLUSIONS

In this paper, we have proposed an IAPF-based synchronization scheme of chaotic Colpitts circuit and conduct experimental study on the synchronization performance over the AWGN channel and the multipath fading channel. Also, a chaos-masking secure communication system has been implemented based on the synchronization scheme. Experimental results show that with the existence of different channel effects and severe parameter mismatches, the proposed synchronization scheme is effective and has good synchronization performance. In addition, secure communication can be achieved with the synchronization scheme. In our future work, we will conduct an experimental study on the feasibility of the proposed synchronization scheme for the chaotic Colpitts circuit when significant channel attenuations are considered. Furthermore, we will explore how to use the proposed synchronization scheme to extract target information from radar echoes in chaos-based radar systems.

## ACKNOWLEDGEMENTS

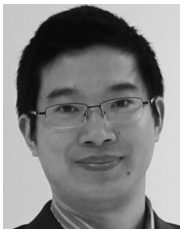
This work was supported in part by the National Science Foundation of China under grant 61171149, the Research Foundation of Chinese State Key Laboratory of Industrial Control Technology under grant ICT1119, the Fundamental Research Funds for the Chinese Central Universities under grant 2013xzzx008-2, and the ORF-RE, Ontario, Canada. Part of this paper was presented at the *2012 International Conference on Wireless Communications and Signal Processing* [23].

## REFERENCES

1. Pecora LM, Carroll TL. Synchronization in chaotic system. *Physics Review Letters* 1990; **64**(8): 821–824.
2. Khadra A, Liu X, Shen X. Application of impulsive synchronization to communication security. *IEEE Transactions on Circuits and Systems I* 2003; **50**(3): 341–351.
3. Chong C, Yong S. UWB direct chaotic communication technology for low-rate wpan applications. *IEEE Transactions on Vehicular Technology* 2008; **57**(3): 1527–1536.
4. Xu W, Wang L, Chen G. Performance of dcsk cooperative communication systems over multipath fading channels. *IEEE Transactions on Circuits and Systems I* 2011; **58**(1): 196–204.
5. Shi Z, Qiao S, Chen K, Cui W, Ma W, Jiang T, Ran L. Ambiguity functions of direct chaotic radar employing microwave chaotic Colpitts oscillator. *Progress In Electromagnetics Research* 2007; **77**: 1–14.
6. Gambi E, Chiaraluce F, Spinsante S. Chaos-based radars for automotive applications: theoretical issues and numerical simulation. *IEEE Transactions on Vehicular Technology* 2008; **57**(6): 3858–3863.
7. Zhang Z, Chau K, Wang Z. Analysis and stabilization of chaos in electric vehicle steering system. *IEEE Transactions on Vehicular Technology* 2012; **57**(6): 3858–3863.
8. Hugues-Salas O, Shore K. An extended kalman filtering approach to nonlinear time-delay systems: application to chaotic secure communications. *IEEE Transactions on Circuits and Systems I* 2010; **57**(9): 2520–2530.
9. Liu X, Shen X, Zhang H. Intermittent impulsive synchronization of chaotic delayed neural networks. *Differential Equations and Dynamical Systems* 2011; **19**(1): 149–169.
10. Zheng H, Hu J, Liu L, He Z. Study on fast synchronization of chaos. *Acta Physica Sinica* 2011; **60**(11): article 110507.
11. Kolumban G, Kennedy MP, Chua LO. The role of synchronization in digital communications using chaos—part ii: chaotic modulation and chaotic synchronization. *IEEE Transactions On Circuits and Systems I* 1998; **45**(11): 1129–1140.

12. Chen J, Zhang R, Song L, Han Z, Jiao B. Joint relay and jammer selection for secure two-way relay networks. *IEEE Transactions on Information Forensics and Security* 2012; **7**(1): 310–320.
13. Robilliard C, Huntington EH, Frater MR. Digital transmission for improved synchronization of analog chaos generators in communications systems. *Chaos* 2007; **17**(2): article 023130.
14. Kurian AP, Puthusserypady S. Performance analysis of nonlinear-predictive-filter-based on chaos synchronization. *IEEE transactions on Circuits and Systems II* 2006; **53**(9): 886–890.
15. Yu WW, Cao JD. Synchronization in a class of complex dynamical networks with nonlinear coupling. *International Journal of Nonlinear Science* 2010; **10**(3): 370–377.
16. Sorrentino F, Porfiri M. Chaos synchronization of uncertain genesio-tesi chaotic systems with deadzone nonlinearity. *EPL* 2011; **93**(5): 50002.
17. Shi Z, Hong S, Chen J, Chen K, Sun Y. Particle filter-based synchronization of chaotic Colpitts circuits combating awgn channel distortion. *Circuits, Systems, and Signal Processing* 2008; **27**: 833–845.
18. Shi Z, Hong S, Chen K. Experimental study on tracking the state of analog Chua's circuit with particle filter for chaos synchronization. *Physics Letters A* 2008; **372**(34): 5575–5580.
19. Hong S, Shi Z, Wang L, Gu Y, Chen K. Adaptive regularized particle filter for synchronization of chaotic Colpitts circuits in an AWGN channel. *Circuits, Systems, and Signal Processing* 2013; **32**(2): 825–841.
20. Maggio G, De Feo O, Kennedy M. Nonlinear analysis of the Colpitts oscillator and applications to design. *IEEE Transactions on Circuits and Systems I* 1999; **46**(9): 1118–1130.
21. Alvarez G, Li S. Some basic cryptographic requirements for chaos-based cryptosystems. *International Journal of Bifurcation and Chaos* 2006; **16**(8): 2129–2151.
22. Liu X, Shen X, Zhang H. Multi-scroll chaotic and hyperchaotic attractors from Chen system. *International Journal of Bifurcation and Chaos* 2012; **22**(2): article 1250033.
23. Bi S, Shi Z, Zhang H, Shen X. Experimental study on particle filter based synchronization of chaotic Colpitts circuit with application to secure communications, In *Proceedings of WCSP*, Hangzhou, China, 2012; 1–6.
24. Arulampalam MS, Maskell S, Gordon N, Clapp T. A tutorial on particle filters for online nonlinear/non-Gaussian bayesian tracking. *IEEE Transactions on Signal Processing* 2002; **50**(2): 174–188.
25. Kennedy M. Chaos in the Colpitts oscillator. *IEEE Transactions on Circuits and Systems I* 1994; **41**(11): 771–774.
26. Pack S, Shen X, Mark J. Optimizing truncated ARQ scheme over wireless fading channels. *IEEE Transactions on Vehicular Technology* 2008; **57**(2): 1302–1305.
27. Song L, de Lamare RC, Burr AG. Successive interference cancellation schemes for time-reversal space-time block codes. *IEEE Transactions on Vehicular Technology* 2008; **57**(1): 642–648.
28. Wang S, Feng J. Particle filtering for noisy contaminated chaotic signals and its application in communications, In *IEEE International Conference on Control and Automation*, Guangzhou, China, 2007; 524–528.
29. Berrou C, Glavieux A. Near optimum error correcting coding and decoding: turbo-codes. *IEEE Transactions on Communications* 1996; **44**(10): 1261–1271.
30. Hong S, Shi Z, Chen K. Easy-hardware-implementation MMPF for maneuvering target tracking: algorithm and architecture. *Journal of Signal Processing Systems* 2010; **61**(3): 259–269.
31. Miao L, Zhang J, Chakrabarti C, Papandreou-Suppappola A. Algorithm and parallel implementation of particle filtering and its use in waveform-agile sensing. *Journal of Signal Processing Systems* 2011; **65**(2): 211–227.

## AUTHORS' BIOGRAPHIES



**Zhiguo Shi** (IEEE M'10) received the BSc and PhD degrees both in electronic engineering from Zhejiang University, Hangzhou, China, in 2001 and 2006, respectively. From 2006 to 2009, he was an assistant professor with the Department of Information and Electronic Engineering, Zhejiang University, where currently he is an associate professor. From September 2011, he began a two-year visiting period to the Broadband Communications Research (BBCR) Group, University of Waterloo. His research interests include radar data and signal processing, wireless communication, and security. He received the Best Paper Award of IEEE/CIC ICCC 2013, IEEE WCNC 2013, and IEEE WCSP 2012. He received the Scientific and Technological Award of Zhejiang Province, China, in 2012. He serves as an editor of *KSII Transactions on Internet and Information Systems*. He also serves as a TPC member for IEEE VTC 2013 Fall, IEEE ICCC 2013, MSN 2013, IEEE INFOCOM 2014, IEEE ICNC 2014, and others.

**Songjie Bi** received the BSc degree in electronic engineering from Zhejiang University, Hangzhou, China, in 2012. He is pursuing his PhD degree in the DART lab, Department of Electrical and Computer Engineering, University of California, Davis. His research interests focus on radio frequency microelectromechanical system (RF-MEMS) design and reconfigurable radio systems, nonlinear circuits, and applications.

**Hongtao Zhang** received the BSc degree in power and mechanical engineering from Wuhan University, Wuhan, China, in 2001, the MSc degree in control theory and control engineering from Huazhong University of Science and Technology, Wuhan, China, in 2004, and the PhD degree in electrical and computer engineering from University of Waterloo, Waterloo, Ontario, Canada, in 2010. He is currently a post-doctoral fellow in applied mathematics with mechanical and mechatronics engineering at University of Waterloo. His research interests include hybrid dynamics, chaos control, network synchronization and their potential applications to secure communication, biological systems, and hybrid electric vehicles.

**Rongxing Lu** (IEEE M'10) Rongxing Lu received the PhD degree (with excellent doctoral thesis award) in computer science from Shanghai Jiao Tong University, Shanghai, China, in 2006, and the PhD degree (with Governor General's Gold Medal) in electrical and computer engineering from the University of Waterloo, Canada in 2012. He is currently an assistant professor at the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore. His research interests include wireless network security, applied cryptography, trusted computing, and target tracking.

**Xuemin (Sherman) Shen** (IEEE M'97 SM'02 F'09) received the BSc(1982) degree from Dalian Maritime University (China) and the MSc (1987) and PhD degrees (1990) from Rutgers University, New Jersey (USA), all in electrical engineering. He is a professor and university research chair for the Department of Electrical and Computer Engineering, University of Waterloo, Canada. He was the associate chair for the Graduate Studies from 2004 to 2008. Dr. Shen's research focuses on resource management in interconnected wireless/wired networks, wireless network security, wireless body area networks, vehicular ad hoc, and sensor networks. He is a coauthor/editor of six books and has published more than 600 papers and book chapters in wireless communications and networks, control, and filtering. Dr. Shen served as the technical program committee chair for IEEE VTC'10 Fall, the symposia chair for IEEE ICC'10, the Tutorial Chair For IEEE VTC'11 Spring and IEEE ICC'08, the technical program committee chair for IEEE Globecom'07, the general co-chair for Chinacom'07 and QShine'06, the chair for IEEE Communications Society Technical Committee on Wireless Communications, and P2P Communications and Networking. He also serves/served as the editor-in-chief for *IEEE Network*, *Peer-to-Peer Networking and Application*, and *IET Communications*; a founding area editor for *IEEE Transactions on Wireless Communications*; an associate editor for *IEEE Transactions on Vehicular Technology, Computer Networks*, and *ACM/Wireless Networks*, and others; and the guest editor for *IEEE JSAC*, *IEEE Wireless Communications*, *IEEE Communications Magazine*, and *ACM Mobile Networks and Applications*, and others. Dr. Shen received the Excellent Graduate Supervision Award in 2006; the Outstanding Performance Award in 2004, 2007, and 2010 from the University of Waterloo; the Premier's Research Excellence Award (PREA) in 2003 from the Province of Ontario, Canada; and the Distinguished Performance Award in 2002 and 2007 from the Faculty of Engineering, University of Waterloo. Dr. Shen is a registered professional engineer of Ontario, Canada, an IEEE Fellow, an Engineering Institute of Canada Fellow, a Canadian Academy of Engineering Fellow, and a distinguished lecturer of IEEE Vehicular Technology Society and Communications Society.