A Secure Chaos-Based Communication Scheme in Multipath Fading Channels using Particle Filtering

S. Shaerbaf* and S. A. Seyedin**

Abstract: In recent years chaotic secure communication and chaos synchronization have received ever increasing attention. Unfortunately, despite the advantages of chaotic systems, such as, noise-like correlation, easy hardware implementation, multitude of chaotic modes, flexible control of their dynamics, chaotic self-synchronization phenomena and potential communication confidence due to the very dynamic properties of chaotic nonlinear systems, the performance of most of such designs is not studied and so is not still suitable for wireless channels. To overcome this problem, in this paper a novel wide-band chaos-based communication scheme in multipath fading channels is presented, where the chaotic synchronization is implemented by particle filter observer. To illustrate the effectiveness of the proposed scheme, numerical simulations based on particle filter are presented in different channel conditions and the results are compared with two other EKF and UKF based communication scheme. Simulation results show the remarkable BER performance of the proposed particle filter-based system in both AWGN and multipath fading channels condition, causes this idea act as a good candidate for asynchronous wide band communication.

Keywords: Chaos-based communication; particle filter; unscented kalman filter; multipath fading channel.

1 Introduction

Since the important work by Pecora and Carrol [1], synchronization of chaotic systems has aroused much interest [2-9]. In particular, chaos synchronization has been widely investigated for applications in secure communication today and is an open problem [10-15]. After this time, a number of single-user analog and digital chaos-based communication systems have been proposed, among them the most widely studied are chaos masking [16], chaos-shift keying (CSK) [17, 18], differential CSK (DCSK) [19, 20] and frequency-modulated DCSK (FM-DCSK) [21]. The main idea is that chaotic signal, as a “non- periodic processes produced by a deterministic dynamic system with high sensitivity to the primary conditions” [22], can be used as a carrier and transmitted together with an information signal to a receiver. At the receiver end chaos synchronization is employed to recover the information signal. Although secure communication can be implemented through many ways, but A simple method is to add the information signal to the chaotic carrier [3, 23] and use the combined signal to drive the receiver. This approach suffers from the disadvantage that distortion and noise introduced by the channel are indistinguishable from the signal. Furthermore, if the amplitude of the signal is too large relative to the carrier's, synchronization cannot be maintained.

In recent years, much attention has been devoted to a group of techniques known as particle filtering methods (also referred as sequential Monte Carlo (SMC) algorithms) [24]. All of these techniques are aimed at building a recursive Bayesian filter, which estimates the posterior probability density function (pdf) based on Monte Carlo simulations. Particle filter is an important alternative for predicting and estimating unknown parameters and states in real-time applications, especially in systems with nonlinearities and non-Gaussianities where classical approaches based on the well-known EKF provide solutions that may be far from optimal. The idea of using particle filtering to a chaotic system is given perhaps for the first time in [25, 26] whereas their main work was to estimate the constant bifurcation parameter of chaotic system but in this paper, a novel particle filter based communication scheme is introduced that can act in different multipath fading channel condition. To illustrate the effectiveness of the proposed scheme, numerical simulations based on particle filter are presented and the results are compared with two other EKF and UKF based communication scheme.
The paper is organized as follows. In Section 2, the proposed communication scheme is presented. Section 3 describes the particle filtering and synchronization algorithm. In Section 4, the simulation parameters and final simulation results have been presented. And finally, conclusion is given in Section 5.

2 Chaotic Communication Scheme

In this section, a modified model for digital data modulation using chaotic masking algorithm in transmitter will be expressed and then the proposed structures for particle filter based receiver in both AWGN and Multipath channels will be presented separately.

2.1 Modified Chaotic Masking for Digital Transmission

At the transmitter, the dynamics of the chaotic carrier is governed by the one dimensional discrete chaotic map described below:

\[ c(n) = f(c(n-1)) \]  

(1)

where \( c \) is the state variable at time instant \( n \) and \( f(\cdot) \) is a nonlinear chaotic map. If we consider the modulation method, as done in classic analog chaos masking scheme [16], some little modification must be done for transmission of digital information data, since the information signal, \( m(n) \), has been assumed as a sampled bipolar binary sequence in this paper. If we define \( \alpha \) as a “data scale” parameter and \( m(n) \) as an discrete time form of data, the discrete form of transmitter output, \( s(n) \), can be expressed as:

\[ s(n) = c(n) + \alpha m \left( \frac{n}{N_s} \right) \]  

(2)

where \( N_s \) is the number of transmitted samples per information bit and \( \left[ \cdot \right] \) symbol represent the bracket function. \( N_s \) and \( \alpha \) are two main parameters of this modified chaotic masking transmitter, that must be selected carefully, because of significant impact of their value on Bit Error Rate (BER) and security of proposed design. Simulation results of the communication scheme confirm this idea.

2.2 Particle Filter Based Receiver for AWGN Channels

When the transmission signal in (2) passes through an additive white Gaussian noise (AWGN) channel, the received signal can be represented by following equation:

\[ y(n) = s(n) + v(n) \]  

(3)

where \( v(n) \) is a white Gaussian channel noise with zero mean and variance \( \sigma_v^2 \) at time instant \( n \). Obviously, from the predefined equations, the received signal can also be presented as:

\[
\begin{align*}
\hat{c}_n &= f(\hat{c}_{n-1}) \\
y_n &= c_n + \alpha m \left( \frac{n}{N_s} \right) + v_n
\end{align*}
\]  

(4)

Based on the above equation, the following residual signal can be defined:

\[ v_n' = \alpha m \left( \frac{n}{N_s} \right) + v_n \]  

(5)

According to (4), (5) and by using (1) as a chaotic map equation, state-space representation of received signal can be described as:

\[
\begin{align*}
\hat{c}_n &= f(\hat{c}_{n-1}) + w_n \\
y_n &= h(c_n) + v_n'
\end{align*}
\]  

(6)

With the above mentioned equations and with assumption \( w_n = 0 \), (very low value in numerical simulations), (6) can be rewritten as:

\[
\begin{align*}
\hat{c}_n &= f(\hat{c}_{n-1}) + w_n \\
y_n &= \hat{c}_n + v_n'
\end{align*}
\]  

(7)

It is straightforward that (7) has the form of classical state-space and observation equations of one system, where \( y \) is a vector of observations, \( c \) is a state vector, \( f(\cdot) \) is a system transition function, \( h(x) = x \) is a measurement function of (6), \( w \) and \( v \) are noise vectors, and the subscript \( n \) denotes time index. It is important note that although \( v_n \), as a communication channel noise, has a Gaussian pdf but the predefined residual signal in (5), doesn’t have Gaussian distribution, unless the data scale value can be omitted.

In numerical simulations low value of this parameter can lead to establishment of Gaussian PDF assumption and so better convergence and better security conditions of communication scheme.

A sketch designed for our communication scheme in AWGN channel using PF is shown in Fig. 1. The signal of information, which is up sampled with \( N_s \) factor, and its amplitude multiplied by \( \alpha \) factor, is added to the chaotic sequence, generated by one dimensional discrete map variable. The modulated signal is transmitted to the receiver. At the receiver end, received variable serves as a driving signal that enables the particle filter to synchronize pure states.

If we define \( \hat{c}_n \) as an estimated state, the information signal can be recovered by definition:

\[ k_n = \alpha^{-1} (y_n - \hat{c}_n) \]  

(8)

As it seen in Fig. 1 by using (8) and passing \( k_n \) signal through integrator and dump system with zero threshold, information bits can be recovered.
Moreover the main properties of all chaotic systems, such as wide-band spectrum and low cost implementation comparing to conventional spread spectrum systems [27, 28, 29], the proposed scheme have two other main properties; self-synchronization that is compatible for asynchronous communication and using single state for both data-modulation and observer synchronization. This two property cause significant difference of this idea from some other chaotic-masking systems proposed for AWGN channels [16, 17, 18].

2.3 Particle Filter Based Receiver for Multipath Fading Channels

Generally, in multipath fading channels, discrete time representation of channel output can be in the form:

\[
y_n = \sum_{i=0}^{L-1} a_i s_{n-i} + v_n
\]

(9)

where \( L \) is the number of channel paths and \( a_i \) denotes the coefficient of \( i^{th} \) path. Assumed that transmitter output has an equation like (2), channel output can be described as:

\[
y_n = \sum_{i=0}^{L-1} a_i c_{n-i} + \sum_{i=0}^{L-1} a_i m\left( \frac{n-i}{N_s} \right) + v_n
\]

(10)

Based on (10) we can define residual signal like (5) but with little difference:

\[
v'_n = \alpha \sum_{i=0}^{L-1} a_i m\left( \frac{n-i}{N_s} \right) + v_n
\]

(11)

According to (10), (11) and by using (1) as a chaotic map equation, state-space representation of received signal can be described as (6), where \( w'_n = 0 \) (very low value in numerical simulations), \( v'_n \) denotes the predefined residual signal in (11) and \( h(c_n) \) has the form

\[
h(c_n) = \sum_{i=0}^{L-1} a_i c_{n-i}
\]

(12)

According to (12), at the receiver, the synchronization and communications can be simultaneously realized by using the PF to estimate chaotic state we define as \( \hat{c}_n \). Similar to expression in (8) we can define \( k_n \) in multipath channel in the form of:

\[
k_n = \alpha^{-1}(y_n - h(\hat{c}_n))
\]

(13)

It should be noted that we can calculate \( k_n \) from (13) if we know channel coefficients from channel estimation procedure but in this paper we suppose that channel condition is known at receiver. It is obviously clear that \( k_n \) in noiseless condition will be in the form of:

\[
k_{noiseless}(n) = \sum_{i=0}^{L-1} a_i m\left( \frac{n-i}{N_s} \right)
\]

(14)

Information data bits can be recovered by passing \( k_n \) through an equalizer. In this stage we used LMS-based equalizer, whose coefficients vary from training bits with MSE minimization criterion. Detailed information of LMS-based equalizer can be found in [30]. As it seen in Fig. 2 by using (14) and passing \( k_n \) signal through an adaptive equalizer and an integrator and dump system, information bits can be recovered.

2.4 Particle Filter Based Receiver for AR(1) Time Variant Multipath Fading Channels

Under a multipath propagation environment, which is usually modeled by Rayleigh distribution or Rician distribution, fast fading loss occurs as the rate of change of the multipath environment can be relatively high.

Three types of fast fading loss can be identified, namely, space selective fading, frequency selective fading and time selective fading.
They correspond to different fading features in space, frequency and time [30]. In a real communication environment, generally, a fast fading channel can be modeled as:

$$y_n = \sum_{i=1}^{L} a_{n,i} s_{n,i} + v_n$$

(15)

where $a_n$ is the time-varying channel coefficients. Using the AR model, we can express the time-varying channel coefficient as:

$$a'_n = \sum_{j=1}^{p} c_{n,j} a'_{n-j} + w'_n, \quad i = 0,1,...,L-1$$

(16)

where $p$ is the order of the AR model, $C_{i,j}$ is the corresponding coefficient and $w_n$ is AWGN. Generally, in the state space, we can formulize the problem of blind Channel estimation for a wireless communication system with a fast fading channel in terms of a set of state and measurement equations. Thus, the channel equalization problem can be translated to an estimation problem for an extended state space model, in which each time-varying channel coefficient can be modeled by using the predefined AR model. The problem is now changed into the estimation of the mixed state and channel parameter in the state space. We used this idea for signal transmission in time-variant channels.

3 Nonlinear Adaptive Filters

3.1 Extended Kalman Filter

The Kalman filter is an optimal algorithm for recursive estimation of the states (or any other parameters) of a linear system with Gaussian noise [31]. A distinctive feature of this filter is that its mathematical formulation is described in terms of state-space concepts. One of the key features of the kalman filter is its applicability to both stationary and non-stationary environments. EKF is an extension of the kalman filtering algorithm to nonlinear systems. The nonlinearity of the system is linearized using a first order Taylor series approximation. To this approximated system, the kalman filter is applied to obtain an estimate of the states [32].

3.2 The Unscented Kalman Filter

The UKF algorithm was first introduced by Julier and Uhlmann in 1997 [33], [34]. It works on the principle of unscented transform (UT). UT is a method for calculating the statistics of a random variable which undergoes a nonlinear transformation. Here, instead of approximating the nonlinear function, the underlying posterior probability is approximated using properly chosen sigma points. These sigma points are propagated through the nonlinear function and the resulting points are used to estimate the mean and covariance. It is shown that the UKF based approximation is equivalent to a third order Taylor series approximation [33, 34].

3.3 Particle Filter

The PF is to use sequential Monte Carlo based method. These methods allow for a complete representation of the posterior distribution of the states using sequential importance sampling and resampling [24]. Unlike the standard EKF and UKF algorithms, PF make no assumptions on the form of the probability densities, i.e., nonlinear, non-Gaussian estimation. The key idea in PF is to represent the required posterior density function by a set of random samples (particles) with associated weights and to compute estimates based on these samples and weights. As the number of samples becomes very large, this Monte Carlo characterization becomes an equivalent representation to the usual functional description of the posterior probability density function (pdf), and the PF approaches the optimal Bayesian estimate. If we know the posterior density function, we can easily derive various estimates of the system’s states including means, modes, medians and confidence intervals. We can approximate the posterior distribution with a function on a finite discrete support. It is, however, usually difficult to sample directly from a given posterior distribution. Some detailed information for particle filters can be found in [35].

4 Simulation Results

In this section, we will illustrate the performance of algorithm by applying it to chaos-based communications. Our aim is to demonstrate that the PF algorithm can achieve synchronization, and estimate the message symbols concurrently. In our simulation, the following logistic map is used to generate chaotic signals:

$$c_n = r c_{n-1} (1 - c_{n-1})$$

(17)

where $r \in [3.7, 4]$ is the chaotic region.

We select $r = 3.8$ in the simulation. Both modified chaos masking schemes in AWGN and multipath fading channel are simulated, in which a bipolar binary data is used for transmission, number of samples per bit ($N_s$) fixed to 50, the data scale parameter $\alpha$ selected to be 0.05 and the total energy of multipath channel coefficients normalized to unity . Fig. 3 illustrates time representation of the chaotic map, bit sequence and modulated output signal with default data scale 0.05, where normalized spectrum of these signals are shown in Fig. 4. We can see that the wide spectrum of chaotic signal and low value of data scale cause wide band spectrum of modulated data, which is suitable for high security and broad band communication.

It can be noted that the value of data scale must be selected properly since the large values of this parameter decrease security and very low value of it, degrade bit error rate performance of proposed scheme.

For the simulation of multipath fading condition, two different channels with two and three propagation
paths are considered. In Fig. 5 magnitude and phase diagram of these channels are shown versus normalized frequency. As it seen in this figure, both simulated channels are frequency selective and so can impose significant distortion to modulated signal. This result can be recovered from Fig. 6 where returning map diagrams of main chaotic sequence, modulated signal, received signal after two path channel and estimated state are shown. As it seen in this figure the phase space of the modulated sequence differs slightly comparing with the pure chaotic sequence. This difference caused by the chaos masking with data sequence in the modulator.

The phase space of the multipath channel output show that the communication channel generate considerable amount of distortion in phase space which can be reduced by state observer estimation algorithm. Phase space of estimated sequence produced by the particle filter observer shows that the channel distortion in modulated signal can be reduced effectively during observer-based state estimation algorithm. Eb/N_0 value fixed to 40 dB in this figure.

Fig. 7 shows the original and estimated states of proposed system in Ideal and AWGN channel condition using PF when E_b/N_0 ratio of AWGN channel is fixed to 30 dB. The convergence of state is so fast and after a very short time the estimations are synchronized to the original state.

In general case MSE between the estimated chaotic signal in receiver and the ideal generated signal, which is used to measure the state estimation performance, is defined by:

\[
MSE = \frac{1}{N} \sum_{n=1}^{N} (\hat{c}_n - c_n)^2
\]  

where \( N \) is the total number of time samples.

For simulation of the time-varying channels, as a compromise between computational complexity and tracking capability, we used the AR (1) model to model these Coefficients. The following two channels will be used to demonstrate the equalization performance of the algorithm [30]:

\[
a_n = [1 - 0.7(1+0.1\cos(\frac{n}{100})) + 0.3(1+0.1\sin(\frac{n}{50}))]
\]  

\[
a_n = [1.05\cos(\frac{n}{100}), 0.7(1+0.1\cos(\frac{n}{100})) + 0.3(1+0.1\sin(\frac{n}{50}))]
\]

Equations (19) and (20) are the simulated time-varying coefficients. The second model in (20) differs from the first one only in the main path.

Figures 8 and 9 show the equalization performance for the two time-varying channels using the PF-based Receiver. In the simulations, the SNR of each channel is fixed to 30 dB. We can see that the algorithms are able to track the time-varying fading channels properly. Fig. 10 shows MSE of state estimation algorithm in AWGN channel using three different state observer, EKF, UKF and particle filter in AWGN channel.

\[
\text{Fig. 3} \quad \text{a) amplitude of chaotic sequence, b) amplitude of bit sequence and c) amplitude of modulated signal modulated with data scale 0.05 versus time samples.}
\]

\[
\text{Fig. 4} \quad \text{a) Spectrum of chaotic sequence, b) Spectrum of bit sequence and c) Spectrum of modulated signal with data scale 0.05 versus normalized frequency.}
\]

\[
\text{Fig. 5} \quad \text{Magnitude and phase diagram of two and three path simulated channels versus normalized frequency.}
\]
Fig. 6 Returning map diagrams — $x_n$ versus $x_{n-1}$ — for pure chaotic sequence, modulated, received and estimated sequences, $E_b/N_0 = 40$ dB.

Fig. 7 Original and estimated states for ideal and AWGN channels. Solid line denoted to pure state and dashed lines denoted to estimated states. $E_b/N_0$ is fixed to 30 dB and $N_c = 50$.

Fig. 8 Equalization performances for the time-varying fading channels in (19) using PF based observer, in which SNR of each channel is controlled to 30 dB, and the dotted line corresponds to the estimated coefficients.

Fig. 9 Equalization performances for the time-varying fading channels in (20) using PF based observer, in which SNR of each channel is controlled to 30 dB, and the dotted line corresponds to the estimated coefficients.

Fig. 10 MSE of state estimation for EKF, UKF and PF based observer in AWGN channels versus $E_b/N_0$ value. Data scale value fixed to 0.05, number of particles fixed to $N=100$ and $N_s = 100$.

Ratio of Bit energy to noise power ($E_b/N_0$) varies from 10 to 40 dB in all simulations where each point calculated from averaging over $10^5$ data bit. As it seen in this figure, MSE value of particle filter observer outperforms other kalman based estimators. Data scale value for this simulation fixed to 0.05 and $N_c$ equals to 100. Figure 11 shows the BER performance of the system by using the EKF, UKF and the PF algorithms, respectively. The number of particles in PF is configured as $N=100$, Data scale value fixed to 0.05 and $N_s = 100$. In this figure different results of proposed system in different channel conditions plotted. We can see that the BER of the proposed scheme by using the PF algorithm is lower than that by using the EKF and UKF algorithm in all channel condition.

Comparing EKF and UKF-based receivers, UKF has the better BER performance, due to nonlinear structure of it. As it can be considered the system has the better
performance in AWGN channel comparing multipath communication channels.

In Fig. 12 the BER performance of particle filter receiver calculated in all channel condition. As it can be seen in this figure, the performance of the first AR(1) channel with fixed coefficient in the first path is slightly better than the second AR(1) channel. Data scale value fixed to 0.05, number of particles fixed to N=100, N_s = 100.

As it mentioned before, data scale parameter must be selected properly. In Fig. 13, BER performance of all observers calculated versus data scale parameter when E_b/N_0 value fixed to 30 dB in AWGN channel and N_s = 100.

As it seen in Fig. 13, the best value of data-scale parameter lies between 0.08 and 0.11 for all observers. Although minimum value for BER exists in larger value of data scale, but low values of this parameter lead to better security and wide band property of communication scheme. Hence the optimum value of data scale is about 0.1 and this value selected as a simulation parameter for modulation of information data over AWGN and multipath channels for all observers.

Figure 14 shows the BER performance of the system in all channel condition when the data scale parameter fixed to 0.1. As it mentioned before, the value of about 0.1 for scale parameter is a good candidate for optimum performance in all observers especially if we want to use low value to enhance the security of system. Simulation conditions in this figure are the same with the Fig.9 where N=100, and N_s = 100. As it can be seen in this figure, BER of the proposed scheme by using the PF algorithm is lower than that by using the EKF and UKF algorithm in all channel condition. In addition The BER value of system reduced comparing with the Fig.9 results particularly in AWGN channel for new particle filter receiver.
In Fig. 15 the BER performance of particle filter receiver for optimum data scale parameter calculated. Remarkable result of PF-based scheme in all channel condition causes this idea act as a good candidate for asynchronous wide band communication.

5 Conclusion

In this paper a novel wide band communication scheme method based on particle filtering is proposed. Two different receivers for AWGN and multipath communication channel designed using PF-based state estimation. At the receiver end, after estimation process, the signal passed through integrator and dump system in AWGN case and LMS-based equalizer for Multipath channel. Also the value of data scale parameter in transmitter selected properly to enhance the overall performance of system. Simulation results show the Remarkable BER performance of the proposed particle filter-based system in both results AWGN and multipath fading channels condition. A comparison with EKF and UKF–Based receivers confirmed this enhancement in the terms of BER and MSE for both schemes.

Acknowledgment

The authors wish to thank khorasan higher institute of education for the financial paper support.

References


Saeed Shaerbaf received his B.S. degree in Electrical Engineering from Ferdowski University of Mashhad in 2003 and M.S. degree in Communication Engineering from Ferdowsi University of Mashhad in 2006 respectively. He received the Ph.D. Degree from the Ferdowsi University of Mashhad in 2011. His research interests are in the field of chaos-based communication systems, design of spread spectrum systems, advanced signal processing techniques and pattern recognition area.

Seyed Alireza Seyedin received the B.S. degree in Electronics Engineering from Isfahan University of Technology, Isfahan, Iran in 1986, the M.S. degree in Control and Guidance Engineering from Roorkee University, Roorkee, India in 1992, and the Ph.D. degree from the University of New South Wales, Sydney, Australia in 1996. Since 1996, he has been with the faculty of engineering, Ferdowsi University of Mashhad, Mashhad, Iran as an assistant professor and since 2007 as an associate professor. He was the head of the department of the electrical engineering for the period 1998-2000. He is a member of technical committee of the Iranian Conference on Machine Vision and Image Processing (MVIP). Dr. Seyedin's research activities focus on the Machine vision, DSP-based signal processing algorithms and digital image processing techniques.