SYNCHRONIZATION AND MESSAGE RECOVERY SCHEME FOR HYPERCHAOTIC SYSTEM USING EXTENDED KALMAN PARTICLE FILTER

B. B. Sharma¹, Sharad Mathur²,
¹Faculty, ²Post-graduate student
Department of Electrical Engineering,
NIT Hamirpur (HP), India
bbs.iit@gmail.com, Sharadmathur0@gmail.com
Contact No.: +91-1972-254540

August 6, 2018

Abstract
In the field of secure communication and information recovery, applications of chaos theory have seen a tremendous growth over the last few years. More recently, hyperchaotic systems with more than four dimensions in have been developed which offers more complex topological structures compared to traditional hyperchaotic systems. Such systems, therefore, may be more suitable for secure communication. This paper aims to present a synchronization mechanism for recently developed novel 5D hyperchaotic systems along with an information signal recovery scheme. The proposed approach frames the synchronization problem in probabilistic framework, utilizing Extended Kalman Particle Filter (EKPF) as estimators. Chaotic masking is used for the secure transmission of information signal and the security is further enhanced by employing multi-shift encryption/decryption algorithms. The performance evaluation of
EKPF estimators is done using performance measures such as root mean square error (RMSE), signal to noise ratio (SNR) etc.

**Key Words:** Bayesian filtering, novel 5D hyperchaotic systems, Extended Kalman particle filters, multi-shift ciphering

1 INTRODUCTION

In the field of communication, secured message transmission and effective information recovery are the main key issues which are to be addressed. In recent times, applications of chaotic systems in communication are explored a great deal, keeping in view their complexity which offers many advantages in hiding the information in the communication channel. Chaotic systems are complex dynamical systems which have deterministic, nonlinear, and aperiodic description wherein initial conditions are of paramount importance [1]. Although chaotic systems are deterministic but there are many traits that are common between chaotic signals and stochastic signals such as uncorrelated states, wide band spectrum and noise like characteristics [2]. These properties of chaotic systems can be well capitalized in developing secure communication schemes based on chaotic systems.

Initially introduced by Rossler [3], there has been a continuous and sustained effort [4-6] in developing Hyperchaotic systems. Hyperchaotic systems generally have 4th order and have at least two positive Lyapunov exponents and a negative Lyapunov exponent. More recently, there has been a keen interest in developing higher dimension hyperchaotic systems such as novel 5-D Hyperchaotic systems [7-9] which have five dimensions in state space resulting in more complicated dynamical behavior of the chaotic systems and hence making them an even better candidate for secure communication.

Synchronization of identical chaotic systems is essentially a problem of dynamic state estimation. A number of techniques for synchronization of identical chaotic systems with different control strategies like sliding mode control, feedback linearization, backstepping, adaptive control etc are available in literature[10-15]. However, in
majority of these contributions, impact of process and measurement noises are ignored. This is a serious assumption for many practical applications. In case of probabilistic state space framework, chaos synchronization has been discussed in [16-18]. In this framework, majority of approaches utilize Kalman filter and its variants based on Bayesian estimation [19-25].

The Bayesian approach of dynamical state estimation works on construction of posterior probability density function (pdf) recursively as the new measurement becomes available. It can be noted that analytical solution for Bayesian algorithm is intractable unless some weak assumptions like linear and Gaussian nature of probabilistic state space framework hold which eventually leads to famous Kalman filter [19-20]. If valid, no filter can perform better than Kalman filter but nonlinearity can’t be avoided in practical problems. Suboptimal Bayesian filters like Extended Kalman filter (EKF) [21] and Unscented Kalman filter (UKF) [22-25] can be used to tackle nonlinearity but the assumption of Gaussian distribution remains mandatory.

Particle filtering [19, 26-28] is a mechanism that integrates Monte Carlo sequential techniques with the Bayesian filtering algorithm and can be implemented in nonlinear/non-Gaussian probabilistic framework. The idea is to approximate the posterior pdf by a number of randomly chosen weighted samples (particles). It has been shown [19] that as the number of particles approach infinity, Particle filters give true representation of posterior pdf but this comes at the cost of tremendous computational burden.

One of the major issues in Particle filtering is proper choice of proposal density function [26-27]. Considering this only, a number of variants of Particle filters have been proposed. In filtering/estimation problems, Extended Kalman Particle filter (EKPF) [27] is quite commonly used. In EKPF, an EKF is employed to generate a Gaussian proposal density for each particle. Since EKF is based on first order linearization of nonlinearity, large errors are expected if the nonlinearity is severe. Plus, EKF involves calculation of Jacobians/Hessians at each step which are nontrivial in most cases making it difficult to tune [21]. In literature, applications of Extended Kalman Particle filter (EKPF) are not explored much in meeting out synchronization requirements in case of chaotic/hyperchaotic systems.
Keeping in view the above, in present manuscript, a strategy of chaotic synchronization in transmitter-receiver configuration using Extended Kalman Particle filter is proposed. For this purpose, a recently developed novel 5D hyperchaotic system [9] is considered in probabilistic state space framework. Some results for the same system are presented in [30]. At transmitter end, a novel 5D hyperchaotic system is used as the master system which transmits some of the states as synchronization signal via insecure public channel whereas at the receiver end, stochastic nonlinear dynamic state estimators viz. Extended Kalman Particle Filter (EKPF) is used as slave system to reconstruct the master system states using noisy synchronization signal and random initialization. The problem is further extended to develop a secure chaotic communication system by employing an information signal recovery scheme. The information signal is secured by chaotic masking by considering state of chaotic system as carrier signal. The security is further enhanced by using multi-shift ciphering techniques for encryption/decryption. The key used for encryption is not transmitted via insecure public channel, rather generated independently at receiver end using synchronization signals. EKPF is used to recover the information signal for first and second case, respectively. Performance of both the estimators is tested and the comparative study is illustrated with numerical examples.

The detailed simulation results are presented in the end while quantifying the performance using measures like root mean square error (RMSE), total root mean square error (TRMSE) and signal to noise ratio (SNR).

The rest of the paper is organized as: In section 2, the novel 5D Hyperchaotic system is described and the proposed chaotic communication scheme is discussed with suitable block diagrams. In section 3, EKPF algorithm is discussed in detail along with basic idea of Particle filtering. In section 4, simulation results are presented for the proposed scheme. In section 5, concluding remarks along with future possibilities are discussed.
2 SYSTEM DESCRIPTION AND PROPOSED CHAOTIC COMMUNICATION SCHEME

This section introduces the novel 5D hyperchaotic system dynamics and further presents the proposed communication scheme. The 5D hyperchaotic system system description involves five ordinary differential equations out of which four have 4th order nonlinearities and one has second order nonlinearity as follows [9]:

\[
\begin{align*}
\dot{x}_1 &= a_1(x_2 - x_1) + x_2x_3x_4x_5 \\
\dot{x}_2 &= a_2(x_1 + x_2) - x_1x_3x_4x_5 \\
\dot{x}_3 &= -x_3 + 0.1x_1^2 \\
\dot{x}_4 &= -a_3x_4 + x_1x_2x_3x_5 \\
\dot{x}_5 &= -a_4(x_3 - x_4) - a_5x_1 + x_1x_2x_3x_4
\end{align*}
\]

Here \((x_1, x_2, x_3, x_4, x_5)\) are system states and \((a_1, a_2, a_3, a_4, a_5)\) are real positive parameters. For parameter values \(a_1 = 37, a_2 = 14.5, a_3 = 10.5, a_4 = 15,\) and \(a_5 = 9.5\) the system exhibits hyperchaotic behavior as described in [9].

Figure 1: Phase portrait on the plane \((x_2 - x_4)\)
The divergence of this system is:

\[ \Delta V = \frac{x_2}{x_2} + \frac{x_4}{x_4} + \frac{x_5}{x_5} \]  

(2)

\[ \Delta V = - (a_4 - a_5 + 1 + a_3 + a_4) \]  

(3)

For given choice of parameters, \(< 0\) hence system converges to zero exponentially as \(t \to \infty\). Thus the system is dissipative in nature and bounded. Fig. 1 and Fig. 2 are phase portraits of the hyperchaotic system for \((x_2 - x_4)\) and \((x_2 - x_4 - x_5)\) states, respectively. The graphs are with initial conditions taken as \([-0.4, -0.2, 2, -3, -2]\).

The chaotic communication system presented here adopts the basic structure as given in [16]. The major advantage of using this scheme is that the key signal used for encryption/decryption is not transmitted via insecure communication channel, rather it is generated separately by the estimator using noisy synchronization signal which boosts the security level compared to traditional chaotic communication schemes [29]. The chaotic communication scheme used here is presented in Fig. 3. The transmitter-receiver pair scheme utilizes encryption/decryption algorithms based on multi-shift ciphering methods. Some of the states except for those used as key signal and carrier signal, i.e. except for first and fourth state, are sent as synchronization signal along with encrypted signal via inse-
cure noisy communication channel.

The receiver part consists of an EKPF as a stochastic nonlinear dynamic state estimator and a decryption unit. The decryption unit is exactly the inverse process of the encryption unit. The estimator attempts to synchronize the transmitter with the receiver. When the estimated states exactly match the true states, the original information signal can be recovered by implementing the decryption algorithm on the received noisy encrypted signal.

For chaotic masking, let \( m(t) \) be the information signal which is to be chaotically masked with \( x_4(t) \) state variable of a given novel 5D hyperchaotic system. Then chaotically masked signal \( c(t) \) can be formulated as:

\[
c(t) = m(t) + x_4(t) \quad \text{(4)}
\]

To achieve this purpose, both the information signal and the hyperchaotic system state used for chaotic masking are firstly discretized with proper sampling time and algebraically added thereafter. For encryption, a multi-shift ciphering algorithm is used. The chaotically masked signal \( c(t) \) is encrypted using a key signal \( k(t) \) which is the state \( x_1(t) \) of the hyperchaotic system. The encryption and decryption rules are based on the nonlinear function as shown in Fig. 4.
Here, \( c \) and \( k \) represent the values of \( c(t) \) and \( k(t) \) at time instant 't' and \( M \) is the threshold value of the shift ciphering. For this function to work efficiently, \( c(t) \) and \( k(t) \) must lie between \(-M\) and \( M\). The encrypted signal \( \theta_n(c, k) \) can be obtained as explained in equations (5), (6) and (7) where \( 'n' \) represents the number of shifts.

For \( n = 1 \),

\[
e_{1}(c,k) = \begin{cases} (c + k) + 2M : & -2M \leq (c + k) \leq -M \\ (c + k) : & -M < (c + k) < M \\ (c + k) - 2M : & M \leq (c + k) \leq 2M \end{cases}
\]

(5)

For \( n = 2 \),

\[
e_{2}(c,k) = e(e(c,k) + k) = \begin{cases} (e(c,k) + k) + 2M : & -2M \leq (e(c,k) + k) \leq -M \\ (e(c,k) + k) : & -M < (e(c,k) + k) < M \\ (e(c,k) + k) - 2M : & M \leq (e(c,k) + k) \leq 2M \end{cases}
\]

(6)

Likewise, after 'n' shifts, the encrypted signal will be represented as:

\[
e_{n}(c,k) = e(\ldots e(e(c,k) + k) + k) \ldots + k)
\]

(7)

At the receiver end, the estimator attempts to reproduce transmitter end hyperchaotic system states. Let the estimated key signal be denoted as \((t)\), which is equivalent to \( \hat{x}_1(t) \) then the decryption rule, can be formulated as:

For \( n = 1 \),

\[
d_{1}(e_{n}\hat{k}) = \begin{cases} (e_{n} - \hat{k}) + 2M : & -2M \leq (e_{n} - \hat{k}) \leq -M \\ (e_{n} - \hat{k}) : & -M < (e_{n} - \hat{k}) < M \\ (e_{n} - \hat{k}) - 2M : & M \leq (e_{n} - \hat{k}) \leq 2M \end{cases}
\]

(8)

For \( n = 2 \),

\[
d_{2}(e_{n}\hat{k}) = d(d(e_{n}\hat{k}), \hat{k}) = \begin{cases} (d(e_{n}\hat{k}) - \hat{k}) + 2M : & -2M \leq (d(e_{n}\hat{k}) - \hat{k}) \leq -M \\ (d(e_{n}\hat{k}) - \hat{k}) : & -M < (d(e_{n}\hat{k}) - \hat{k}) < M \\ (d(e_{n}\hat{k}) - \hat{k}) - 2M : & M \leq (d(e_{n}\hat{k}) - \hat{k}) \leq 2M \end{cases}
\]

(9)

Similarly, after 'n' shifts, the decrypted signal must come out as:
Here $\hat{c}(t)$ is recovered chaotically masked signal and if $\hat{x}_4(t)$ the estimated fourth state, the estimated message signal is $\hat{m}(t)$ can be obtained as:

$$\hat{m}(t) = \hat{c}(t) - x_4(t)$$  \hspace{1cm} (10)

If the estimator is really synchronized with the transmitter, estimated message signal must match with the original message signal precisely i.e. $m(t) - \hat{m}t \to 0$

3 NONLINEAR STATE ESTIMATORS

Consider the probabilistic nonlinear discrete time state space model whose state evolution and measurement model are defined as:

$$x_k = f_{k-1}(x_{k-1}, w_{k-1})$$
$$z_k = h_k(x_k, v_k)$$  \hspace{1cm} (11)

Where $f_k$ and $h_k$ are nonlinear functions such that $f_k : R^{nx} \times R^{nw} \to R^{nx}$ and $h_k : R^{nx} \times R^{nv} \to R^{nz}$ where $x \in R^{nx}$ is the state vector, $W \in R^{nw}$ is the i.i.d (independent and identically distributed) process noise vector, $Z \in R^{nz}$ is the measurement vector and $v \in R^{nv}$ is the i.i.d measurement noise vector.

In the Bayesian approach of dynamic state estimation, if the posterior pdf of states at $(k-1)^{th}$ instant $p(x_{k-1}|Z_{1:k-1})$ is known (given all measurements available up to $(k-1)^{th}$ instant), the posterior pdf of states at $k^{th}$ instant $p(x_k|z_{1:k})$ can be computed in a recursive way as the new measurement $Z_k$ becomes available. Here, $\{Z_{1:k}\}$ implies measurement values up to time k Bayesian filtering is a two-step process as described below:

**Prediction:** This step involves prediction of prior pdf at instant using famous ChapmanKolmogorov equation [22]:

$$p(x_k|z_{1:k-1}) = \int p(x_k|x_{k-1})p(x_{k-1}|z_{1:k-1})dx_{k-1}$$  \hspace{1cm} (12)

Update: Once the measurement at $k^{th}$ instant becomes available, the prior pdf is updated to posterior pdf as per Bayes' rule [22]:
Unlike arbitrary pdfs, complete description of Gaussian pdf can be obtained by only first two moments i.e. mean and covariance. It can be seen in (12) that if \( p(x_{k-1} | Z_{1:k-1}) \) is Gaussian, and if we linearize \( f_k \) at each iteration about mean and covariance of \( p(x_{k-1} | Z_{1:k-1}) \), (12) and (13) make a closed loop resulting in popular EKF [21]. On the same lines, if unscented transformation [25-26] is applied about mean and covariance of \( p(x_{k-1} | Z_{1:k-1}) \), analytical solution exists for (12) and (13) which is widely known as UKF [22-24]. However, if the \( p(x_{k-1} | Z_{1:k-1}) \) is non-Gaussian, analytical solution becomes intractable as the complete description of \( p(x_{k-1} | Z_{1:k-1}) \) may need unbounded number of parameters. For such scenarios, Particle filters remain the best solution.

### 3.1 PARTICLE FILTERING AS STATE ESTIMATION

Particle filtering is a dynamic state estimation technique based on Monte Carlo simulation methods which applies the Bayesian algorithm in a recursive manner. This method is more general as probabilistic nonlinear/non-Gaussian models can be dealt with this approach. The fundamental idea is to approximate \( p(x_{k-1} | Z_{1:k-1}) \) by randomly chosen weighted samples, called particles. Using this approximation, any statistical parameter can be computed that is needed to describe \( p(x_{k-1} | Z_{1:k-1}) \). These particles are propagated through state evolution model to predict \( p(x_{k-1} | Z_{1:k-1}) \) and their weights (probabilities) are modified to approximate \( p(x_{k-1} | Z_{1:k-1}) \) when the measurement \( Z_k \) becomes available. Thus a closed loop between (12) and (13) exists for sequential state estimation. The estimate of states can be evaluated by computing convenient statistical parameter like mean, mode, MAP etc. of these posterior pdfs at each iteration.

Let \( \{x_{0:k}', \omega_k\}_{i=1}^{N_S} \) is a parametric representation of sampled approximation of posterior pdf of states at \( k^{th} \) instant where \( \{x_{0:k}'\}_{i=1}^{N_S} \) is the set of samples drawn from posterior pdf of states at \( k^{th} \) instant with \( \{k = 1, 2, ..., N\} \) and \( \{\omega_k\}_{i=1}^{N_S} \) are the weights associated with each particle at \( k^{th} \) instant such that \( \sum_{i=1}^{N_S} \omega_k^i = 1 \). The problem of sequential dynamic state estimation can then be summarized as:
In order to approximate the posterior \( p(x_k|Z_1:k) \), challenge is how to draw particles from \( p(x_k|x_{k-1}) \) and then how to evaluate and update weights (probabilities) of each particle that would give the true representation of posterior pdf. In many situations, it may not be possible to draw samples from the posterior directly [19]. In such cases the concept of importance density [26-27] is utilized.

Let \( q(x) \) be the importance density (proposal) function that can be sampled easily and \( P(x) \) is the normalized target (actual, posterior) density function which is not so easy to sample but can be evaluated at samples. Since, \( P(x) \) is normalized pdf, \( q(x) \) can be thought of as a scaled version of \( P(x) \) and we can define weight ratio as:

\[
\omega'_i = \frac{P(x_i)}{q(x_i)} \quad \text{(15)}
\]

Using Bayes’ rule, this weight equation can be modified as [19]:

\[
\omega'_i = \omega'_i + \frac{P(x_i|Z_1:k)}{q(x_i|x_{k-1})} \quad \text{(16)}
\]

This is the weight update equation that is used to approximate the posterior pdf recursively.

**Degeneracy:** It has been seen that the variance of the weights only increases with time [19, 26] and hence after some iterations, very few particles are left that have significant weights. This leads to poor approximation of the posterior. One measure of Degeneracy is ‘Effective sample size’ [19] whose estimate can be formulated as:

\[
\hat{N}_{eff} = \frac{1}{\sum_{i=1}^{N} \omega_i^k} \quad \text{(17)}
\]

Here, \( \omega_i^k = \frac{\omega_i^k}{\sum_{i=1}^{N} \omega_i^k} \) is normalized weight sequence. Larger the \( \hat{N}_{eff} \), smaller the degeneracy. Degeneracy can’t be eliminated completely, however, it can be controlled by: 1) Resampling and 2) Good choice of proposal density. The major drawback of resampling is that the diversity among the particles is lost (sample impoverishment [19, 27]) which can be severe for small process noises.

A good number of Resampling methods exist, however, systematic resampling is widely used and its pseudo code is given in Algorithm...
Algorithm 1: Systematic Resampling

```
\begin{algorithm}
\begin{algorithmic}
\State \( [x_i^e, w_i^e] \subseteq \text{Resample}(x_i^e, w_i^e)_{i=1}^N \)
\State \text{Construct the cumulative distribution function of weights.}
\State \text{Set: } \alpha = 0
\FOR \( i = 1 \ldots N \)
\State \( c_i = \alpha + w_i \)
\END FOR
\State \text{Draw: } u \sim \text{UniformDistribution}[0, 1]
\State \text{Set: } i = 1
\FOR \( j = 1 \ldots N \)
\State \( z_j = u, x_j = 1 - i/N \)
\WHILE \( u > c_j \)
\State \( i = i + 1 \)
\END WHILE
\State Set particles: \( x_i^e = x_i \)
\State Set weights: \( w_i^e = 1/N \)
\end{algorithmic}
\end{algorithm}
```

Algorithm 1: Systematic Resampling

Algorithm 2: Extended Kalman Particle Filter (EKPF)

```
\begin{algorithm}
\begin{algorithmic}
\State \text{Prediction}
\FOR \( i = 1 \ldots N \)
\State \( \mathbf{f}_i = \mathbf{f}(\mathbf{x}_i, \mathbf{y}_i) \)
\State \( \mu_i = \mathbf{f}_i \)
\State \( \Sigma_i = \text{cov}(\mathbf{f}_i) \)
\FOR \( j = 1 \ldots N \)
\State \( \mathbf{p}_{ij} = \mathbf{f}_j \)
\State \( \mathbf{K}_ij = \Sigma_i^{-1} \mathbf{p}_{ij} \)
\State \( \mathbf{p}_{ij} = \mathbf{p}_{ij} - \mathbf{K}_ij \mathbf{p}_{ij} \)
\END FOR
\State \( \mathbf{x'} = \mathbf{x} + \mathbf{K}_i (\mathbf{y} - \mathbf{f}(\mathbf{x}, \mathbf{y})) \)
\State \( \mathbf{p'} = \mathbf{p} - \mathbf{K}_i \mathbf{p} \)
\FOR \( j = 1 \ldots N \)
\State \( \mathbf{p}_{ij} = \mathbf{p}_{ij} - \mathbf{K}_ij \mathbf{p}_{ij} \)
\END FOR
\State \text{Update}
\State \text{Resample}
\FOR \( i = 1 \ldots N \)
\State \( w_i = \frac{1}{N \mathbf{p}_{i}} \)
\State \( \text{Set weights: } w_i = w_i \)
\END FOR
\end{algorithmic}
\end{algorithm}
```

Algorithm 2: Extended Kalman Particle Filter (EKPF)
Second approach to avoid degeneracy is good choice of importance density [19, 26-27]. In general, transition prior density is taken as the importance density (Bootstrap particle filter) because of simplicity but it is surely suboptimal because it doesn’t employ present measurement while updating weights which is a vital parameter in weight updating and hence can cause weights to die after some iterations. The process of general Particle filter can be summarized as:
Step 1: Choose an importance density q(x) and draw $x_k^i \sim q(x)$.
Step 2: Calculate weights according to (16).
Step 3: Resample using Algorithm 1.
Step 4: Approximate the posterior pdf using (14).
Step 5: Evaluate necessary statistics from this posterior pdf.

3.2 EXTENDED KALMAN PARTICLE FILTER (EKPF)

To overcome the degeneracy problem, in EKPF, an EKF is used to generate and propagate importance density by evaluating first two moments of the Gaussian distribution for each particle. While doing this, present measurements are incorporated which is important for particles to fall in the regions of high likelihood [27]. In EKF step, the nonlinear system is linearized by 1st order Taylor expansion. The mean and covariance of posterior pdf at $(k-1)^{th}$ instant for each particle are recursively propagated to predict prior pdfs at $k^{th}$ instant. When the measurement at $k^{th}$ instant becomes available, the prior pdfs are updated using present measurement to give approximation of posterior pdfs at $k^{th}$ instant. New particles sampled from these posterior pdfs are obtained at $k^{th}$ instant.

The Bayesian solution (12) and (13) by EKF is definitely suboptimal since higher order nonlinearities are ignored. The algorithm for the EKPF is given as Algorithm-2.

4 SIMULATION RESULTS

This section briefs about the numerical data used for the implementation purpose. The State space Model of novel 5D hyperchaotic
The continuous time system was integrated by using fourth order Runge-Kutta method with sampling time $T=0.0015$ for $N = 1000$ time steps. The novel 5D hyperchaotic system given in (1) can be represented as:

$$\dot{x}(t) = A(x)x(t) + w$$

where $x = [x_1, x_2, x_3, x_4, x_5]$ and $A(x)$ is the process noise vector.

States $x_2, x_3, x_5$ were sent as synchronization signals while state $x_4$ was used to chaotically mask the information signal and state $x_1$ was used as the key signal. The output description for the proposed scheme can be given as:

$$z(t) = Cx(t) + v_k$$

where $v_k$ is the measurement noise vector. Parameter values $(a_1, a_2, a_3, a_4, a_5)$ are chosen as in section 2. With these choice of parameters, the pair $(A, C)$ always remains observable. Process noise was drawn from a Gamma distribution $(3, 0.01)$ and measurement noise was drawn from a Normal distribution and experiments were conducted for different variance values $\sigma_v^2 = (0.3, 0.8, 1.2, 3, 5, 6, 7)$. Initial conditions used at transmitter end were $[4 -2 1 -3.5 6]$ and at receiver end were $[15 -10 -2 -10 -10]$. For EKPF, $N_s = 1000$ particles were used and threshold for resampling was taken as $N_T = 0.7N_s$.

The information signal was chosen as a sine wave with following description:

$$m(t) = Asin(2\pi ft)$$

Where $A = 8$, $f = 1.2$Hz and for the encryption, parameter values were taken as $M = 10$, $n =3$. If $x$ is true state and $\hat{x}$ is the estimated state, to check the accuracy of the estimator, following performance...
measures were used:

a) Root mean square error (RMSE): \( \text{RMSE} = \sqrt{\frac{1}{N} \sum_{i=1}^{N} (x_i - \hat{x}_i)^2} \)

b) Total RMSE (TRMSE): \( \text{TRMSE} = \sum_{i=1}^{N} \left( \frac{1}{N} \sum_{j=1}^{N} (x_{ij} - \hat{x}_{ij})^2 \right) \)

The value of observation noise variance was varied between 0.3 and 7. Table 1 depicts a comparative study of RMSE and TRMSE for chaotic system states and message signal for EKPF for different variances. It can be noticed that an increase in noise variance is causing RMSE and TRMSE to grow in case of EKPF.

<table>
<thead>
<tr>
<th>Estimator</th>
<th>(( \sigma_n^2 ))</th>
<th>( x_1(T) )</th>
<th>( x_2(T) )</th>
<th>( x_3(T) )</th>
<th>( x_4(T) )</th>
<th>( x_5(T) )</th>
<th>( x_6(T) )</th>
<th>( x_7(T) )</th>
<th>( x_8(T) )</th>
<th>( x_9(T) )</th>
<th>( x_{10}(T) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>EKPF</td>
<td>0.3</td>
<td>0.3108</td>
<td>0.3279</td>
<td>0.3102</td>
<td>0.6887</td>
<td>0.3271</td>
<td>0.6884</td>
<td>1.4124</td>
<td>1.4124</td>
<td>1.4124</td>
<td>1.4124</td>
</tr>
<tr>
<td></td>
<td>0.6</td>
<td>0.4390</td>
<td>0.5040</td>
<td>0.4863</td>
<td>0.7517</td>
<td>0.5046</td>
<td>0.7519</td>
<td>1.6674</td>
<td>1.6674</td>
<td>1.6674</td>
<td>1.6674</td>
</tr>
<tr>
<td></td>
<td>1.0</td>
<td>0.5452</td>
<td>0.6179</td>
<td>0.5181</td>
<td>0.8148</td>
<td>0.6173</td>
<td>0.8134</td>
<td>2.2381</td>
<td>1.8296</td>
<td>2.2381</td>
<td>1.8296</td>
</tr>
<tr>
<td></td>
<td>2.0</td>
<td>0.5353</td>
<td>0.7286</td>
<td>0.6848</td>
<td>0.7177</td>
<td>0.6846</td>
<td>0.7179</td>
<td>2.3385</td>
<td>2.3385</td>
<td>2.3385</td>
<td>2.3385</td>
</tr>
<tr>
<td></td>
<td>3.0</td>
<td>0.6005</td>
<td>0.8336</td>
<td>0.7275</td>
<td>0.8066</td>
<td>0.7279</td>
<td>0.8066</td>
<td>2.4912</td>
<td>2.4912</td>
<td>2.4912</td>
<td>2.4912</td>
</tr>
<tr>
<td></td>
<td>5.0</td>
<td>0.7893</td>
<td>1.0055</td>
<td>0.8266</td>
<td>1.2551</td>
<td>0.8274</td>
<td>1.2551</td>
<td>2.9431</td>
<td>2.9431</td>
<td>2.9431</td>
<td>2.9431</td>
</tr>
<tr>
<td></td>
<td>6.0</td>
<td>0.8381</td>
<td>1.0270</td>
<td>0.8232</td>
<td>1.3099</td>
<td>0.8229</td>
<td>1.3099</td>
<td>3.1226</td>
<td>3.1226</td>
<td>3.1226</td>
<td>3.1226</td>
</tr>
<tr>
<td></td>
<td>7.0</td>
<td>0.8919</td>
<td>1.0315</td>
<td>0.8287</td>
<td>1.4440</td>
<td>0.8301</td>
<td>1.3437</td>
<td>3.4370</td>
<td>3.4370</td>
<td>3.4370</td>
<td>3.4370</td>
</tr>
</tbody>
</table>

From Fig. 5-9, it can be seen that for the states whose measurements were available i.e., \( x_2, x_3 \) and \( x_5 \) synchronize almost immediately hence RMSE are smaller for them and absolute errors converge to zero rapidly. However, for the states \( x_1 \) and \( x_2 \) RMSE values are comparatively high. This is because their measurements were not available while filtering and the weights were completely updated using available information of synchronization signals only.

It should also be noted that transition period (time before synchronization) also depends on the initial conditions. A closer guess of initial conditions can be handy for achieving fast synchronization. The recovery of information signal is shown in Fig. 10.
Figure 5. First state and its estimation

Figure 6. Second state and its estimation
Figure 7. Third state and its estimation

Figure 8. Fourth state and its estimation
The plot in Fig. 10 clearly shows the effectiveness of the proposed scheme to recover the message signal with reasonable accuracy. The state estimation errors are shown in Fig. 11-15 for all the states of hyperchaotic system under consideration. The proposed EKPF based estimator is able to estimate the true states with good amount of accuracy, though estimate of 4th state takes slightly longer time to settle to the true value of the state. The above detailed simulations highlight the efficacy of EKPF based approach which is clearly reflected in terms of evaluation of error.
measures like RMSE, TRMSE and SNR.

Figure 11 Estimation error in first state

Figure 12 Estimation error in 2\textsuperscript{nd} state
Figure 13. Estimation error in 3\textsuperscript{rd} state

Figure 14. Estimation error in 4\textsuperscript{th} state
5 CONCLUSION

Synchronization of chaotic systems becomes more difficult in presence of process and measurement noise as traditional synchronization schemes cannot be implemented. Here, synchronization strategy based on Extended Kalman Particle filter (EKPF) as an estimator is used to synchronize the novel 5D hyperchaotic system in a non-Gaussian environment. Further, the proposed approach is extended to transmit an information signal and to recover it back in secured way by using chaotic masking and multi-shift ciphering. Detailed performance analysis of EKPF based approach is done on the basis of error measures like RMSE, TRMSE and SNR. The results suggested that EKPF gives reasonable performance in meeting out the synchronization as well as in recovering the message signal.

References


