WSN-BASED SMART GRID SECURITY USING CHAOTIC SYNCHRONIZATION

Komeil Nosrati
Tehran Electrical Distribution – Iran
komeilnosrati@gmail.com

Morteza Bahadori
Tehran Electrical Distribution – Iran
bahadori@tbtb.ir

Mohammad Hashemi
Tehran Electrical Distribution – Iran
hashemi@tbtb.ir

ABSTRACT

In this study, we will evaluate the application of encryption design based on a new chaotic synchronization algorithm to the Smart Grid. Chaotic cryptosystem has the advantages of high security and low cost of time and space which can be useful for security goals in WSN-based smart grid. We present a new synchronization method of fractional chaotic system based on unscented Kalman filter (UKF) which is applicable in a secure protocol for WSN to overcome the drawbacks of small key space and weak security in the used integer order systems. Analyses on analog and digital signal show that the synchronization algorithm can recover the encrypted data successfully with high accuracy and low time.

INTRODUCTION

Smart grid as a modern electric power grid infrastructure for improved efficiency, reliability, and safety through automation control and modern two-way communication and electricity flows, can provide predictive power information to both utilities and consumers and diagnose power disturbances and outages to avoid the effect of equipment failure and natural accidents [1].

Recently, Wireless Senor Network (WSN) has been widely recognized as a vital component of the electric power system [2]. It contains a large number of low cost, low power, and multifunctional sensor nodes which can be of benefit to electric system automation applications, especially entire process of smart grid from the generation, transmission and distribution, and the consumer side. Through WSN, it can capture and analyze data related to power usage, delivery, and generation efficiently. Load management and control, wireless automatic meter reading, equipment fault diagnostic, remote monitoring, fault detection, advanced metering infrastructure and residential energy management are some of the applications WSN in smart grid. They can reduce operational costs by eliminating the need for human readers and provide an automatic pricing system for customers.

The WSN brings cyber security and privacy challenges to smart grid [3]. For example, eavesdropping or unauthorized modification of the communications if not protected by authentication and encryption, accessing illegally through wireless sensing network of smart grid customers' privacy information can be highly dangerous to the grid and thus fail the critical mission of the supervisory control and data acquisition systems. Therefore, a secure WSN with high capacity must be addressed to ensure a reliable and efficient smart grid.

Encryption is a cryptographic method to achieve secure communication for any information system. As the Smart Grid communication network consists of millions of embedded computing systems with limited computational ability, computational efficiency becomes an important factor for an encryption scheme [4-5]. Thus, in this study, we will evaluate the applications of encryption design based on a new chaotic synchronization algorithm to the Smart Grid.

The features of Chaos, complexity, sensitivity to initial values and inscrutability, make it adaptable to encryption [6]. Chaotic cryptosystem has the advantages of high security and low cost of time and space which can be useful for security goals in WSN-based smart grid. We present a new synchronization method of fractional chaotic system based on unscented Kalman filter and apply it in a secure protocol for WSN to overcome the drawbacks of small key space and weak security in the used integer order systems. The secure protocol is based on symmetric chaotic encryption. Since WSN suffer from limited resources, asymmetric cryptosystem which consumes more resources is not suitable for WSN, so symmetric encryption is used in secure protocol [6].

Analyses on analog and digital signal show that the synchronization algorithm can recover the encrypted data successfully with high accuracy and low time and can be used in secure protocol. Our work includes further reducing especially the cost in chaos synchronization. Fractional Chaotic system is able to provide a large and sensitive key space, so it is sufficient for encryption of WSN.

This paper is organized as follows: In section 2, a review of fractional chaotic systems, principles and algorithms of UKF is presented. The proposed chaotic secure communication scheme is provided in section 3. In section 4, the results of simulation on fractional Lorenz chaotic system with using of UKF and their application in proposed WSN-based chaotic secure communication scheme are presented. Section 5 deals with concluding remarks.

CHAOTIC SYSTEM SYNCHRONIZATION

Fractional-order chaotic system

Fractional calculus is a generalization of integration and differentiation of the non-integer order fundamental operator ${}_aD_t^{\alpha}$, where a and t are the limits of the operation. The two most important definitions generally used for the fractional integral are the Grunwald–Letnikov (GL) and the Riemann–Liouville (RL) definitions for discrete systems and continuous systems, respectively [7]. The RL integral definition is:

$$I^{(\alpha)}f(t)=\frac{1}{\Gamma(\alpha)}\int_0^t (t-\tau)^{1-\alpha}f(\tau)d\tau, \qquad \alpha,t>0 \tag{1}$$

With this definition of integral, the two equations, the Riemann–Liouville and Caputo fractional derivatives can be defined as (2) and (3), respectively.

$$D^{(\alpha)}f(t)=\frac{d^m}{dt^m}(I^{(m-\alpha)}f(t)) \tag{2}$$

$$D^{(\alpha)}f(t)=I^{(m-\alpha)}\left(\frac{d^m}{dt^m}f(t)\right) \tag{3}$$

m is a positive integer variable and $m-1<\alpha\le m$.

Lorenz system is a nonlinear chaotic one, found in the process of chaotifying continuous systems, described by

$$\begin{cases}\dot{x}=-\sigma(x-y)\\ \dot{y}=-xz+\rho x-y\\ \dot{z}=xy-\beta z\end{cases} \tag{4}$$

When $(\sigma,\rho,\beta)=(10,28,8/3)$, (4) exists a chaotic attractor. The fractional-order Lorenz system is described as follows:

$$\begin{cases}\dfrac{d^{(q_1)}x}{dt^{q_1}}=-\sigma(x-y)\\ \dfrac{d^{(q_2)}y}{dt^{q_2}}=-xz+\rho x-y\\ \dfrac{d^{(q_3)}y}{dt^{q_3}}=xy-\beta z\end{cases} \tag{5}$$

When $(q_1,q_2,q_3)=(0.96,0.98,1.1)$ system (5) behaves chaotically.

The standard definitions of fractional differential equations do not allow direct implementation of the fractional operators in time domain simulations. To solve a fractional differential equation numerically, two approximation methods, namely, frequency domain approximation and Adams–Bashforth–Moulton algorithm, have been proposed. Simulation results by proposed Adams–Bashforth–Moulton algorithm are more reliable than simulation results of the first method, due to specificity of the error estimation bound in this method. So the second method was selected for our simulations. The next section describes the unscented Kalman filter, which is used in the estimation of fractional system states.

Unscented Kalman Filter

The problem of propagating Gaussian random variables through a nonlinear function can be approached using the unscented transform (UT) which is used in the UKF [8]. A set of weighted sigma points is deterministically chosen so that the sample mean and sample covariance of these points match those of a priori distribution. The nonlinear function is applied to each of these points in turn to yield transformed samples, and the predicted mean and covariance are calculated from the transformed samples as shown in Fig. 1. This strategy typically does both decrease the computational complexity, while at the same time increasing estimate accuracy, yielding faster, more accurate results. Basically, the UKF captures the posterior mean and co-variance of the Gaussian Random Variables (GRV) accurately to the third order (in terms of Taylor series expansion) for any form of nonlinearity.

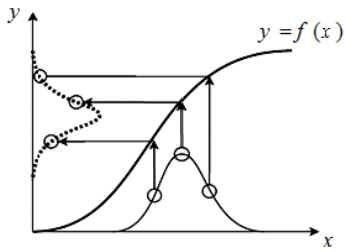

Fig. 1 The principle of the unscented transform and the propagating of sigma points through a nonlinear function

The algorithm for implementing the UKF can be summarized as follows [8]. Consider the nonlinear discrete-time system represented by

$$\begin{aligned}x_{k+1}&=f(x_k)+w_k\\ y_k&=H_k x_k+v_k\end{aligned} \tag{4}$$

$k\in N$ is discrete time and N denotes the set of natural numbers. $x_k\in R^{L\times 1}$ is the state, and $y_k\in R^{M\times 1}$ is the measurement. The nonlinear mapping $f(\cdot)$ is assumed to be continuously differentiable with respect to x_k and H_k is a measurement matrix. Moreover, $w_k\in R^{L\times 1}$ and

$v_k \in R^{M\times 1}$ are uncorrelated zero-mean Gaussian white sequences and have the following characteristics:

$$E\left[w_k w_j^T\right]=Q_k\delta_{kj},\ E\left[v_k v_j^T\right]=R_k\delta_{kj},\ E\left[w_k v_j^T\right]=0 \quad (5)$$

***Step* 1:** The L-dimensional random variable x_{k-1} with mean $\hat{x}_{k-1}$ and covariance $\hat{P}_{k-1}$ is approximated by sigma points which are computed with the following equations:

$$\begin{cases} \chi_{i,k-1}=\hat{x}_{k-1}, & i=0 \\ \chi_{i,k-1}=\hat{x}_{k-1}+\left(a\sqrt{L\hat{P}_{k-1}}\right)_i, & i=1,2,\ldots,L \\ \chi_{i,k-1}=\hat{x}_{k-1}-\left(a\sqrt{L\hat{P}_{k-1}}\right)_{i-L}, & i=L+1,\ldots,2L \end{cases} \quad (6)$$

Where $a\in R$ is a tuning parameter denoting the spread of the sigma points around $\hat{x}_{k-1}$ and $(a\sqrt{L\hat{P}_{k-1}})_i$ is the ith column of the matrix square root of $L\hat{P}_{k-1}$. The parameter is often set to a small positive value.

Step 2: *Prediction*. Each point is instantiated through the process model to yield a set of transformed samples:

$$\chi_{i,k|k-1}=f(\chi_{i,k-1}),\quad i=0,1,\ldots,2L \quad (7)$$

The predicted mean and covariance are computed as

$$\hat{x}_{k|k-1}=\sum_{i=0}^{2L} w_i\chi_{i,k|k-1} \quad (8)$$

$$\hat{P}_{k|k-1}=\sum_{i=0}^{2L}\left[w_i(\chi_{i,k|k-1}-\hat{x}_{k|k-1})(\chi_{i,k|k-1}-\hat{x}_{k|k-1})^T\right]+Q_k \quad (9)$$

where

$$\begin{cases} w_i=1-\dfrac{1}{a^2}, & i=0 \\ w_i=\dfrac{1}{2La^2}, & i=1,\ldots,2L \end{cases} \quad (10)$$

***Step* 3:** *Update*. As the measurement equation is linear, measurement update can be performed with the same equations as the classical Kalman filter.

$$\begin{aligned} \hat{y}_k &= H_k\hat{x}_{k|k-1} \\ \hat{P}_{yy} &= H_k\hat{P}_{k|k-1}H_k^T+R_k \\ \hat{P}_{xy} &= \hat{P}_{k|k-1}H_k^T \\ K &= \hat{P}_{xy}\hat{P}_{yy}^{-1} \\ \hat{x}_k &= \hat{x}_{k|k-1}+K(y_k-\hat{y}_k) \\ \hat{P}_k &= \hat{P}_{k|k-1}-K\hat{P}_{xy}^T \end{aligned} \quad (11)$$

***Step* 4:** Repeat steps 1 to 3 for the next sample.

PROPOSED COMMUNICATION SCHEME

By using a chaotic oscillator as a broadband pseudo-random signal generator and masking the message with this signal, to produce an unintelligible signal, the encrypted data can be transmitted through the unsecure communication noisy channel between wireless nodes in a smart grid. At the receiver node, by regenerating the pseudo-random signal using of synchronization and combining it with the received signal (encrypted data) through the inverse operation, the original message is recovered.

In proposed scheme, the synchronization is achieved by the UKF acting as the state estimator in the presence of noise and we have enhanced the accuracy of the recovered signal by using the UKF. The block diagram of the proposed scheme for secure communication is shown in Fig. 2. This scheme does not need to know the initial condition of the chaotic signals between the receiver and the transmitter nodes. The system consists of a transmitter module (consists of a chaotic system and an encryption mechanism), a communication wireless channel, and a receiver module. In this system, the chaotic signal is generated by using the fractional Lorenz chaotic system that is described by (5) and process noise is considered in chaos states. The mechanism of encryption is based on masking modulator. The algorithm of encryption process can be described as follows:

The information signal $s(t)$ is added to the second state and then the encrypted signal $s_M(t)$ that is the sum of $s(t)$ and $x_2(t)$, passes through an AWGN wireless channel. The first state of fractional Lorenz chaotic system, $x_1(t)$, is also passed to the receiver module to synchronization. The major part of the receiver side consists of an UKF for state reconstruction and chaos masking demodulator. The fractional Lorenz chaotic states are estimated by the UKF. It should be noted that the first state of the Lorenz is used for chaotic synchronization. In the receiver, the $x_1(t)$ goes to the UKF and other states are estimated.

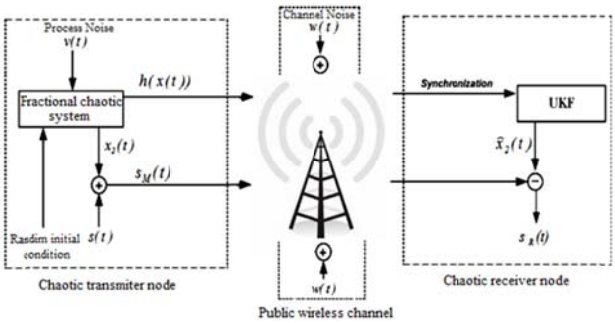

Fig. 2 Proposed chaotic secure communication scheme

SIMULATION RESULTS

The performance of synchronization method and the proposed scheme will be studied. The fractional Lorenz chaotic system is used to illustrate the effectiveness of the proposed methods. As mentioned, we have implemented the improved Adams–Bashforth–Moulton algorithm for numerical simulation in MATLAB. For the simulation problem, process noise has been added to chaotic system states and the first chaotic state is employed for synchronization. Therefore, the output measurement matrix can be represented by

$$H_k = \begin{bmatrix} 1 & 0 & 0 \end{bmatrix} \tag{12}$$

The initial conditions for this chaotic system and the UKF are as follows:

$$\begin{cases} x(0) = \begin{pmatrix} -1.0032 & 2.3545 & -0.087 \end{pmatrix}^T \\ \hat{x}(0) = \begin{pmatrix} 20 & 15 & 15 \end{pmatrix}^T \end{cases} \tag{13}$$

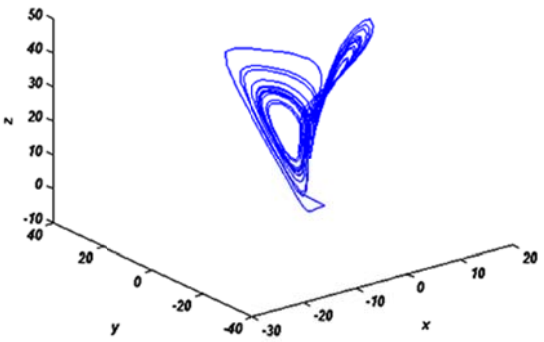

Fig. 3 Attractor of fractional Lorenz dynamical system

The characteristics of the process and channel noise used in the UKF are as follows:

$$R = 0.2, \quad Q = \begin{bmatrix} 0.18 & 0 & 0 \\ 0 & 0.18 & 0 \\ 0 & 0 & 0.18 \end{bmatrix} \tag{14}$$

In Fig. 3, the attractor of the fractional Lorenz system that is described by (5), using the aforementioned parameters can be seen. The following results are obtained for chaotic synchronization of the fractional-order Lorenz system, using UKF methods. The simulations show that UKF is capable of achieving synchronization for the system and the synchronization is done with very low error and high speed. The mean squared error (MSE) for the three states using UKF (Table 1). The MSE in state estimation is

$$MSE = \frac{1}{N}\sum_{i=0}^{N}\left(x_k(i) - \hat{x}_k(i)\right)^2, \quad k = 1,2,3 \tag{15}$$

where $x_k(i)$ and $\hat{x}_k(i)$ are the k th state variable and its estimate at instant of i respectively. For comparison purpose, we run the simulation using the extended Kalman filter (EKF). As it can be observed in Table 1, the UKF method has more accuracy than EKF. Then the UKF performance shows clear superior results. The UKF outperform all results and proffer possibility to use synchronization under noisy channels for our proposed communication application.

Table 1: MSE (0-50 sec) for three state variables

	Synchronization method	
	EKF	UKF
x	0.7730	0.5862
y	6.3926	3.4060
z	2.4991	1.0989

In Fig. 4, the data that is encrypted by masking modulation can be seen in the case of using fractional Lorenz system in time domain. In this case, the data is masked by the first state for encryption. This makes the signal complicated and secure that we cannot understand the content of the message. It is obvious that the analog data is completely hidden in the frequency content of the chaotic state and filtering techniques cannot recover the information which is modulated by masking modulation. Fig. 5 presents the original sinusoid data and the recovered data that are simulated in the same coordinate. We can see that the recovered data is nearly the same as the original data. As indicated in Fig. 5 after 1.071 seconds, the data is recovered and converged nearly to the original data. By using our proposed secure chaotic communication scheme in the presence of channel noise and processing noise, the data can be precisely recovered in the receiver node of a WSN-based smart grid. The noise performance of this system is related to the use of the UKF for state synchronization. For evaluating the performance of the proposed system in a digital case, a pulse input is also used. Fig. 6 shows the digital data encrypted with masking modulation. Fig. 7 shows the original digital data and the recovered digital data in the same coordination. As indicated after 1.099 seconds the digital data is recovered and converged to the original digital data.

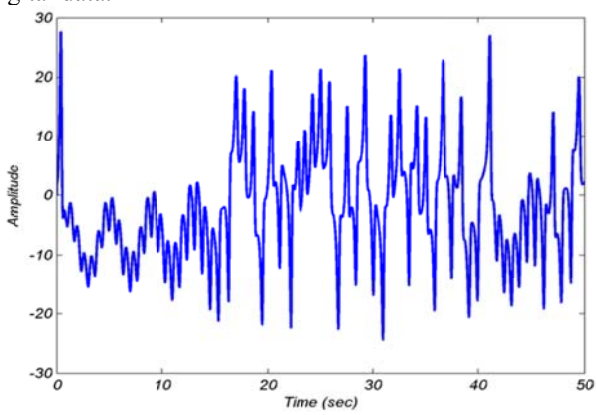

Fig. 4 Analog data encrypted with chaos masking modulation.

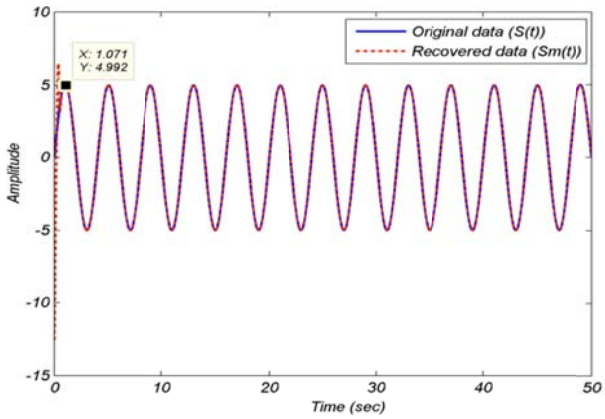

Fig. 5 Original sinusoid data and the recovered data.

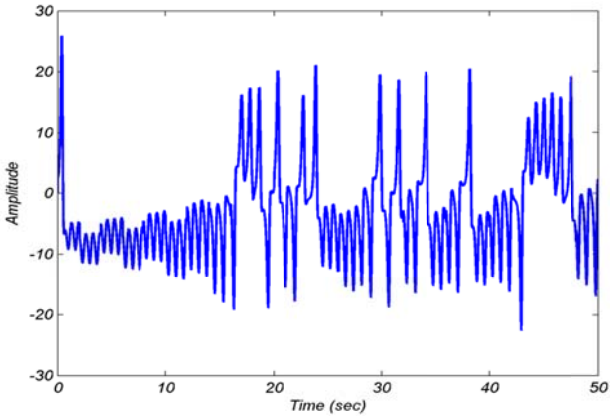

Fig. 6 Digital data encrypted with chaos masking modulation.

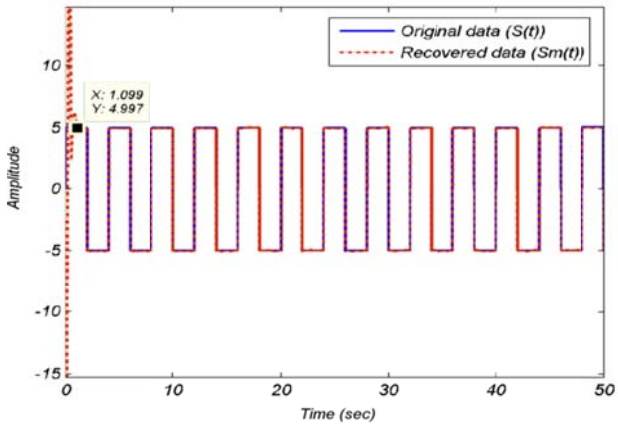

Fig. 7 Original digital data and the recovered data

CONCLUSION

This paper showed the synchronization of noisy fractional-order Lorenz chaotic system using the UKF. We have implemented the improved Adams–Bashforth–Moulton algorithm for numerical simulation of fractional-order Lorenz system in MATLAB. The synchronization of the state variables has been done with high accuracy and high speed. The UKF method has been compared with the EKF method to show the improvement of synchronization act and its growth in the performance in regard to accuracy in decreasing state variable estimation error. The secret keys can be selected as $(q_1, q_2, q_3, \sigma, \rho, \beta)$, and they are independent of each other. So the key space of the proposed method is large enough in theory to resist all kinds of brute-force attacks in theory. Fractional-order chaos encryption algorithm is sensitive to secret keys, that is, only a small change of the key will generate a completely different decryption result and cannot get the correct original data. Due to the facts that the dynamics of fractional derivatives are more complex than integer order system, and fractional derivative orders can be used as secret keys as well, we conclude that it is a good choice to apply fractional order chaotic signal into secure communication in WSN-based smart grid.

REFERENCES

[1] Gungor, Vehbi C., et al. 2011, "Smart grid technologies: communication technologies and standards." *Industrial informatics, IEEE transactions on 7.4*, 529-539.

[2] V. C. Gungor, B. Lu, G. P. Hancke, 2010, "Smart Grid Technologies: Communication Technologies and Standards", *IEEE on Trans. Ind. Electron*, vol. 57, no. 10, 3557-3564.

[3] Padmavathi, Dr G., and Mrs Shanmugapriya. 2009, "A survey of attacks, security mechanisms and challenges in wireless sensor networks" *(IJCSIS) International Journal of Computer Science and Information Security*, Vol. 4, No. 1 & 2.

[4] Akyildiz, Ian F., Xudong Wang, and Weilin Wang, 2005, "Wireless mesh networks: a survey." *Computer networks 47.4*, 445-487.

[5] J. Benoit, 2011, "An Introduction to Cryptography as Applied to the Smart Grid," Cooper Power Systems.

[6] Fang, Qian, Ying Liu, and Xiaoqun Zhao, 2008, "A chaos-based secure cluster protocol for wireless sensor networks." *Kybernetika 44.4*, 522-533.

[7] Kiani, K. Fallahi, N. Pariz, H. Leung, 2009, "A chaotic secure communication scheme using fractional chaotic systems based on an extended fractional Kalman filter", *Communications in Nonlinear Science and Numerical Simulation*, 863-879.

[8] S. J. Julier and J. K. Uhlmann, 2004, "Unscented filtering and nonlinear estimation," *Proc. IEEE*, vol. 92, no. 3, 401–422.