INTERNATIONAL JOURNAL OF ENHANCED RESEARCH IN SCIENCE TECHNOLOGY & ENGINEERING
VOL. 2 ISSUE 3, MARCH-2013 ISSN NO: 2319-7463

Chaotic Synchronization by Non-uniformly Sampled Periodic Driving to Avoid Possible Parameter Estimation

G K Patra[1], V Anil Kumar[2]
Council of Scientific and Industrial Research, Fourth Paradigm Institute
(Erstwhile CSIR Centre for Mathematical Modelling and Computer Simulations)
NAL Belur Campus, Bangalore - 560037
[1]gkpatra@cmmacs.ernet.in, [2]anil@cmmacs.ernet.in

Abstract: Discrete or computerized chaotic systems are being extensively studied for various applications in cryptography. However, the security of them is not yet convincing to be used in real applications. This paper is proposing modifications to chaotic synchronization process, which have been studies a lot as a potential replacement to LFSR's. Here we are proposing a modification to the sampling rate to avoid two forms of parameter estimation attacks. We find that the modification is very effective in protecting from these attacks.

Keywords: chaotic synchronizations, stream ciphers, parameter estimation, computerized chaos

Introduction

Parameter estimation from a given chaotic scalar time series of a nonlinear system has lots of interesting applications in physics. However, for applications such as chaotic cryptosystem, it is treated as an attack. Recently cryptosystems based on chaotic synchronization have been studied extensively as an alternate to LFSR. Chaotic synchronization is a novel phenomenon, first proposed by Pecora and Carrol [1-3] in which two different but identical chaotic systems, though very sensitive to initial conditions, can synchronize by transmitting a subset of the state space variables. In a typical multivariable chaotic system one of the time dependent variable is sent from the transmitter to the receiver, which the receiver uses to force its trajectory move towards the transmitter trajectory. By continuing this process for a large number of iterations the two systems will synchronize and follow the same trajectory there onwards. Once the systems get synchronized, the private state space variables can be used as bit sequences for use in a stream cipher cryptosystem [4]. Since the inception of this concept a large number of cryptosystems have been proposed, which differ by their communication mechanism and way of forcing [5-10]. Though these methods are very promising, many of them have fundamental drawbacks due to lack of robustness and security. The biggest challenge is to protect the time independent variables, which are also called as secret keys, from being estimated by using publicly made information. In literature, there are many parameter estimation mechanisms, which can be used to extract the secret keys from single state space variable [11-13]. Some of these methods are static or off-line and some are dynamic or on-line. The off-line attacks are more successful because they need less amount of information in comparison to the on-line attacks. There are many attempts to improve the synchronization mechanisms [8-10], to protect the cryptosystems from offline parameter estimations. But many of them have impact on the performance of the cryptosystems due to additional overheads.

In our paper we are proposing a non-performance affecting solution, which can be easily implemented as computerized chaotic synchronization. The targeted applications are secure communication in HPC Grids and also high speed secure communication over Internet. We are proposing a non-uniform sampled but periodically driving mechanism, forcing the attacker to speculate about the varying sample time. The paper is organized in the following ways. In the second section we will discuss a typical synchronization scheme and possible parameter estimation attacks on them. In the third section we will propose possible counter measures and derive its synchronization criteria. In the fourth section we will provide a numerical simulation, followed by the security analysis in the fifth section.

Non-uniformly Sampled but Periodically Driven Chaotic Systems

All most all known chaotic systems studied or known so far are uniformly sampled systems, which mean that the trajectory values are determined at equal intervals and also transmitted to the receiver at the same interval. This is done for ease in implementation both in discrete time chaotic systems and analog chaotic systems. These are easy to understand and follow the evolution of the chaotic signal with the time. Let us consider two chaotic systems which are represented by the following system of ordinary differential equations.

$$\dot{x} = f_p(x, p), \quad \dot{y} = f_p(y, p) \qquad (1)$$

Here dot (.) represents the derivative with respect to time. The system of equation with variable "x" is treated as sender and with variable "*y*" as receiver. "*p"* is the identical parameter vector, which is normally exchanged using an alternate secure method, usually

called the super key or the secret key in cryptography. These are two identical system of equations which describes the evolution of the variables x and y over time independently. For synchronization of these two systems, (*i.e* $y \rightarrow x$ as $t \rightarrow \infty$) one of the state space variable of the transmitter (say x_p) has to be determined at every time interval "*dt*" and sent to the receiver at the same interval "*dt*" in case of a discrete time chaotic system, while in an analog chaotic system the signal is continuously transmitted. In a complete replacement mode the receiver will use the received value in stead of its own value of that particular variable (say y_p). In case of feedback mode of synchronization the receiver will use the difference between its value and the received value (*i.e* y_p-x_p) as a feedback signal.

These methods of synchronization have inherent flaws, when applied to secure communication. The observed public time series from the dynamical system contains information about the number as well as the form of the functions governing the evolution of the system variables and the parameters [11-13]. We will discuss about few successful parameter estimation strategies, in the section dealing with the security analysis. The root cause of this successful parameter estimation methodology lies in the information which is made public by transmitting the state space variable. By presenting a diluted information to the attacker (to the public), while at the same time preserving the information content for a genuine receiver, we can avoid the parameter estimation attacks. We are proposing a scheme by which the attacker will have a distorted time series, while the receiver can still have a non-distorted time series.

The publicly available time series can be diluted by adopting non-uniformly sampled but uniformly driven mechanism. This means that communication between the sender and receiver happens at uniform duration of "*dt*" like a normal synchronization, while the value which is sent is sampled at a different but pre-defined time, in the interval "*dt*" (but not at time "*dt*"). This is explained pictorially in Figure 1 using a simple sinusoidal time series as an example. To achieve synchronization the receiver should precisely know the sampled time, to regenerate the correct time series. For this purpose the sampled time should be a function of the secret keys. As the attacker does not have the secret keys, he cannot find the sampled time. So the attacker has no other option than assuming this as a uniformly sampled time series and tries to estimate the parameters from it. The time step "*dt*" plays an important role in all most all the parameter estimation mechanisms, hence synchronization achieved using this mechanism are expected to be safe against those attacks.

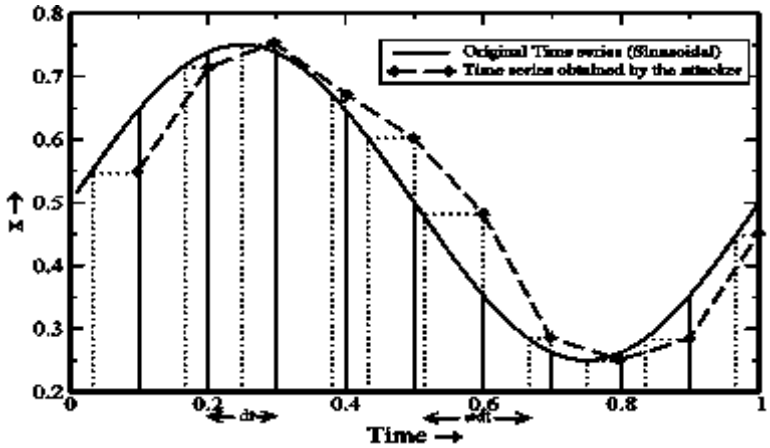

Figure 1. A pictorial presentation of uniformly sampled (solid lines) and non-uniformly sampled (doted lines) time series, communicated at the same time interval.

Let us now see how the modified systems look like. The transmitter and the receiver have the exclusive knowledge of knowing the non-uniform time steps. So the new system at the n^{th} iteration is given by the following equations.

$$\frac{dx}{dt_n} = f_p(x,p), \quad \frac{dy}{dt_n} = f_p(y,p), \quad dt_n = dt + h_n - h_{n-1}, \quad h_n = g(p, x_p, h_{n-1}, h_{n-2}, dt) \ \text{for } n > 2 \quad (2)$$

Here "*g*" is the function to calculate the new sampling time h_n in the time duration "*dt*" and "dt_n" is the varying time step. The evolution of the x and y variables can be easily implemented on a discrete time system with the knowledge of p (the identical parameters), h_0 and h_1 (the two initial time steps), which together form the new super key. The function "*g"* can be public, but as p, h_{n-1} and h_{n-2} are secrets, finding h_n for attacker will not be possible. Using h value of previous two iterations, introduce more confusion and improves the security level. The variability in terms of step size, with respect to different initial condition comes because of the presence of the public variable, x_p in the function. Interestingly, derivative with respect to a varying time-step does not have any mathematical interpretation and can not be implemented in analog chaotic systems. But computerized chaos, as it is a discrete chaotic system, where the evolution with time is numerically calculated using the current time step; it becomes feasible to implement such a concept. The idea of this proposal is to make applications, such as secure high speed grid computing, high speed data communication over Internet, to take advantage of the chaotic communication system, which were discarded because of various security threats.

Synchronization Criteria and Numerical Simulations

Let us study a three variable Lorenz model as an example.

$$\dot{x}_1 = \sigma(x_2 - x_1), \quad \dot{x}_2 = (\rho - x_3)x_1 - x_2' \quad \dot{x}_3 = x_1 x_2 - \beta x_3 \qquad (3)$$

Equation 3 shows a sender system, with σ, ρ and β are secret keys and x_1, x_2 and x_3 are the time dependent variables. Replacing x with y we will obtain the receiver system. The dots (.) represent the derivative with respect to "dt", for a uniform sampling system, while derivative with respect to "dt_n" for a non-uniform sampling system. In both the case the transfer of one of the sampled variable

(say x_1) will be transmitted to the receiver at uniform interval "dt". In the complete replacement mode the receiver uses x_1 in place of y_1, while in case of feedback mode the receiver feeds back k_1 (y_1-x_1) to the y_1 equation. Here k_1 represents the feedback constant. Now, we will discuss the synchronization criteria for a successful synchronization for both complete replacement and feed back scheme. For a complete replacement scheme one can define a Lyapunov function L equal to $e_2^2 + e_3^2$. It can be seen that L≥0 for all values of x_i and y_i. It is also easy to show that [10] $\dot{L} = -e_2^2 - \beta e_3^2$. Here $\dot{L}$ represents the change in L with respect to the varying time step dt_n. For a successful synchronization $\dot{L}$ should be always less than 0. So if β is positive then the Lyapunov function would keep decreasing asymptotically till both the system synchronizes. For a feedback synchronization scheme the stability criteria can be derived from the coefficient matrix of the error system e_i given by Equation 4, for one way diagonal coupling (coupling coefficients of k_1, k_2 and k_3 for the y_1, y_2 and y_3 equations of the receiver respectively)[14][15].

$$\dot{e}_1 = -(\sigma + k_1)e_1 + \sigma e_2, \ \dot{e}_2 = (\rho - x_3)e_1 - (1 + k_2)e_2 - y_1 e_3, \quad \dot{e}_3 = x_2 e_1 + y_1 e_2 - (\beta + k_3)e_3 \qquad (4)$$

For guaranteed synchronization starting at any initial value ($x_i(0)$,$y_i(0)$), $e_i(t) \to 0$ as $t \to \infty$, the coupling coefficients k_1, k_2 and k_3 should satisfy the condition [14]

$$(\sigma + k_1)(1 + k_2)(\beta + k_3) - \frac{\beta^2(\sigma + \rho)^2}{16(\beta - 1)} N > 0 \qquad (5)$$

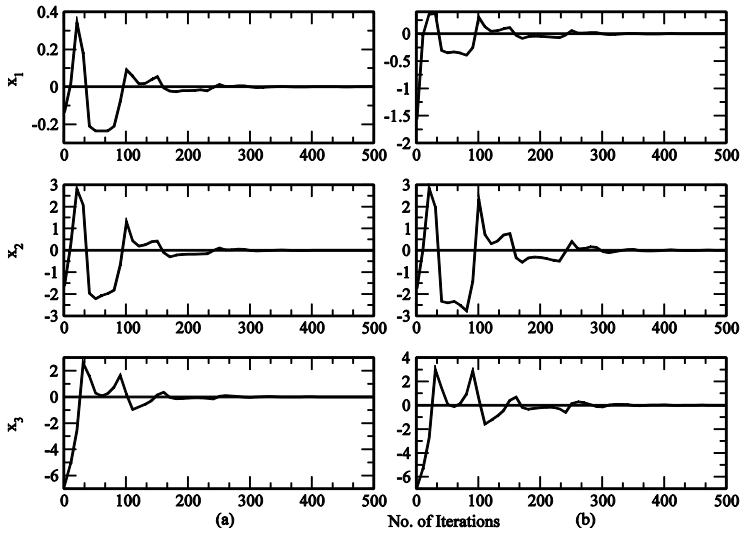

Figure 2. Difference in the time varying variables for a non-uniformly sampled but periodically driven synchronization system (a) complete replacement (b) feedback. Convergence to zero indicates successful synchronization.

Here $N = \max\{1 + k_2, \beta + k_3\}$. If we consider only coupling at the y_1 equation (k_1>0, k_2=k_3=0), we get the following synchronization condition from Eq. 6.

$$k_1 > \frac{\beta^2(\sigma + \rho)^2}{16(\beta - 1)} - \sigma, \quad k_2 > \frac{\beta^2(\sigma + \rho)^2}{16\sigma(\beta - 1)} - 1 \quad \text{and} \quad k_3 > \frac{\beta^3(\sigma + \rho)^2}{16\sigma(\beta - 1)} - \beta \qquad (6)$$

These are only sufficient conditions for synchronization. In fact numerical simulations show that some of the coupling constants which do not satisfy the above conditions also make the coupled systems reach synchronization. We will now compare the proposed mechanism with the existing by means of numerical simulations. Let the secret keys be σ=10, β=2.667 and ρ=29.75 and the random initial conditions. Using the 4th order Runge-Kutta procedure the trajectories are determined. Figure 2 shows the successful synchronization (a) complete replacement (b) feed-back mode for a non-uniformly sampled but periodically driven system.

Security Analysis

It is well known that a great deal of information about a chaotic system is contained in the time series of its variables. Parameter estimation using this time series is considered to be a threat to chaotic communication systems. Parameter estimation techniques can be broadly classified into on-line or dynamic [11][12] and off-line or static [13] strategies.

The off-line attacks normally involve parameter estimation using time series analysis methods. The publicly available time series is exploited to estimate the secret parameters. There have been many attempts to estimate the parameters form publicly available information by direct methods. These include guessing the parameter values and finding out some norm of difference with the actual sample. Logically, keeping the time step secret, one can understand that these attacks will not be successful, as it is essential to have the knowledge of the time step for estimating the parameters from the available time series. We will explain this by using a typical time series analysis method, which needs only a small portion of the public data to estimate the parameters [13]. We will use the Lorenz system in Equation (3) to show and establish the concept using numerical results. The procedure is as follows. First the variables of the Lorenz system are transformed to a new set of variables P, Q, R and S, related to each other in differential terms as shown below [13].

$$P = x_1,\ Q = \dot{x}_1,\ R = \ddot{x}_1,\ S = \dddot{x}_1 \qquad (9)$$

The number of dots (.) indicates the order of the derivative with respect to time. The singularity is avoided by not considering data near the zero. The values of *P*, *Q*, *R* and *S* can be determined by finding the first three derivatives of the available time series. If the data is sampled at sufficiently high rate, large order derivatives can be determined accurately by expanding the Taylor series (expanded up to $(m+1)^{th}$ term) as shown below [10].

$$T = x(t_0 + r) = x(t_0) + \sum_{m=1}^{M} \frac{r^m}{m!} \frac{d^m}{dt^m} x(t_0) \qquad (10)$$

Here *r* is the step size. Considering *n* number of consecutive points with reference $x(t_0)$, one can write Equation 10 in a matrix form as T=AF, where, A is a known coefficient matrix of size $(m \times n)$ and F is the unknown column matrix with the derivatives up to order m, as elements of it. F can be solved by using any generalized inverse procedure. Once the first three derivatives are known, using the relations in Equation 9, the values of the parameters σ, ρ and β can be estimated accurately[13].

Now we will verify the analysis with a numerical experiment. Let us use a Lorenz system with σ=10, β=2.667 and ρ=29.75 with the initial condition (1.874, 2.056, 19.142). Figure.3 shows the three time series generated by the time dependent variables for uniform sampling (original) and non-uniform sampling (observed). Let us consider the x_1 time series for estimation of the parameters for different uniform and non-uniform sampling frequencies. The non-uniform sampling time is calculated using the following function

$$h_n = \left| f \bmod\left((\sigma h_{n-1} + \rho h_{n-2} + \beta x_1), dt\right)\right| \ for\ n > 2\ with\ given\ h_0\ and\ h_1 \qquad (11)$$

Here *fmod* is a C language implementation to obtain the floating point reminder. Table 1 shows the estimated values. We can see that for the uniformly sampled system the parameters are estimated with sufficient accuracy. For a non-uniformly sampled periodically driven system the parameter estimation mechanism does not work as expected. It is observed that in some cases the analysis estimates values which are unstable (β negative).

On-line parameter estimation is a dynamic mechanism, where a receiver, even with un-identical parameters, can synchronize to a sender using some additional differential equations, with a damping term, describing the evolution of the parameters. These methods are useful in a large numbers of non-cryptographic applications. Even in cryptographic applications, where a small amount of information needs to be transmitted, these methods are not treated as attacks, as the estimation processes are quite slow.

However, this method can be a threat to applications, such as High Performance Secure Grid and High Speed Internet, where huge amount of information needs to be exchanged. This is because the sender sends the value of one of its state space variable continuously to the receiver even after synchronization to avoid any de-synchronization at a future time, due to truncation errors, especially in discreet chaotic systems. Many efforts have been made to design synchronization based parameter estimation methods, because of its importance in many fields of physics [1-2]. However a majority of them fail to estimate all the parameters at the same time. A recent method [11] based on least square minimization problem has been very effective to estimate all the parameters.

Let the attacker system be represented by the following equation.

$$\dot{z} = f_q(z,q) \qquad (12)$$

The function f_q have the same functional form as f_p but with different parameter values. The aim of the attacker is to design a strategy that drives the measured synchronization error as shown in equation 13 and minimize the distance between the transmitter and itself.

$$G(q) = \min[(s(z) - s(x))^2] \qquad (13)$$

Here *s(x)* and *s(z)* are observable scalar time series of the two systems. The minimization equation leads to the following differential equations which governs the evolution of parameters [].

$$\dot{q}_j = \frac{\partial G}{\partial q_j} = -2\varepsilon_j (z_i - x_i)\frac{\partial z_i}{\partial q_j} \quad and \quad \frac{d}{dt}\left(\frac{\partial z_i}{\partial q_j}\right) = \sum_{k=1}^{3}\frac{\partial f_{q_i}}{\partial z_k}\frac{\partial z_k}{\partial q_j} + \frac{\partial f_{q_i}}{\partial q_j} - K^T\sum_{k=1}^{3}\frac{\partial z_k}{\partial q_j} \qquad (14)$$

Here *i*=1 to *n* and *j*=1 to *m*, where *m* is the number of parameters and *n* is the number of equations in the chaotic system. K is the gain vector and the positive term ε_j (called learning rates) in Equation 14 is introduced to control the stability.

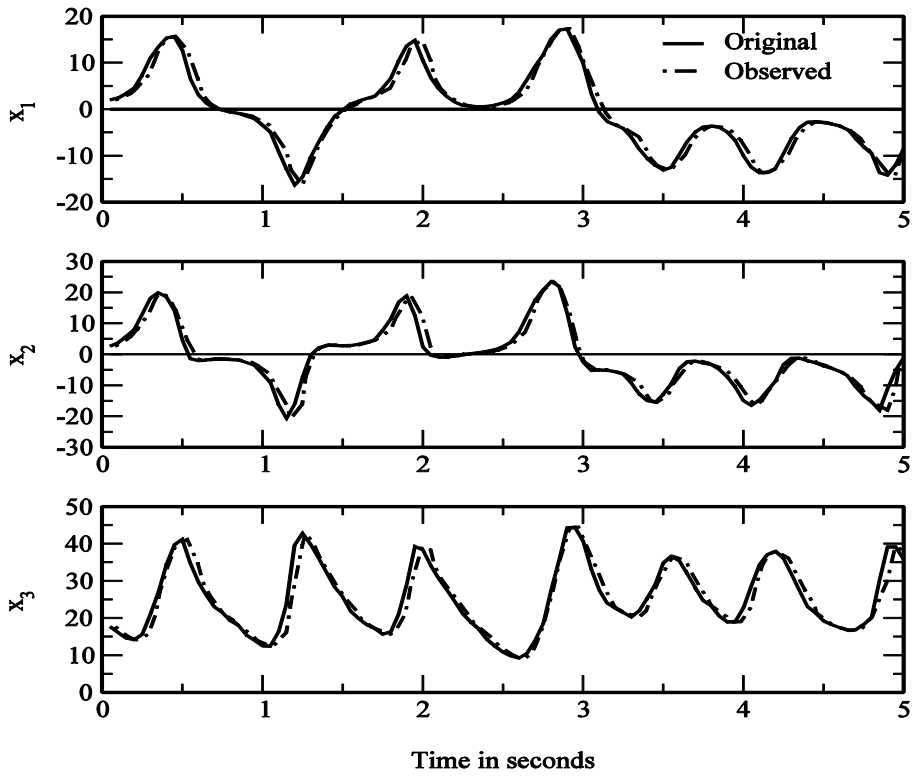

Figure 3. Original and observed time series due to the non-uniformly sampling but periodic driving for all the three variables.

Table 1.
Estimated parameter values for both uniformly and non-uniformly sampled systems for different sampling frequencies and ranges. f_r, f_{r0} and f_{r1} are $1/h_n$, $1/h_0$ and $1/h_1$ respectively in KHz.

f_r	f_{r0}	f_{r1}	σ	ρ	β
Uniform Sampling					
4	4	4	10.0058281111205	29.8836728847202455	2.67317775354497
3	3	3	9.99721469577266	29.7222519484211408	2.66708560686265
2	2	2	9.99929881429367	29.7117939283402198	2.66934192090557
1	1	1	10.0000714308363	29.7483203294389907	2.66687027349984
Non-uniform Sampling					
≥ 5	6	7	2186.60449167345	1.65749826422010326	4251.8435336239
≥ 4	5	6	3812.30569273375	-2.4131955051967579	383.613070904581
≥3	4	5	9871.98349723808	-0.0194610231823175	-6066.66217849213
≥2	3	4	3259.60391718308	-4.6309028564060017	-501.474104070536
≥1	2	3	142.722989604708	2.69533033365465277	1010.17916666023

We will verify the process of parameter estimation with a numerical experiment. Let us consider a Lorenz system with σ=10, β=2.667 and ρ=29.75 and initial conditions (1.874, 2.056,19.142) for the sender and (2.125,-6.138,34,672) for the receiver. The variable x2 is made public. The attacker starts with an initial parameter values of σ=7.0, β=1.56 and ρ=17.0 and random initial values for the time dependent variables. Figure 4 shows the relative error in the three parameters with the time for a uniform sampling system using equation 14. It can be seen that all the three parameters can be estimated accurately within finite time. A data transfer which needs more time than the learning time, (i.e time required for the attacker to synchronize with the attacker) is susceptible to this attack. Estimating the exact learning time is a difficult task as these values will vary for different initial conditions and learning rates, selected by the attacker. So deciding which size data transfer is safe is difficult. Let us try to understand the results of the parameter estimation method on a non-uniform but periodically driven chaotic system. Figure 5 shows the relative error of the three parameters with respect to time. We can see that the three parameters estimated are different from the parameter values of the genuine communicators. In this particular case of the numerical example the attacker estimates σ=18.190, β=0.477 and ρ=10.293.

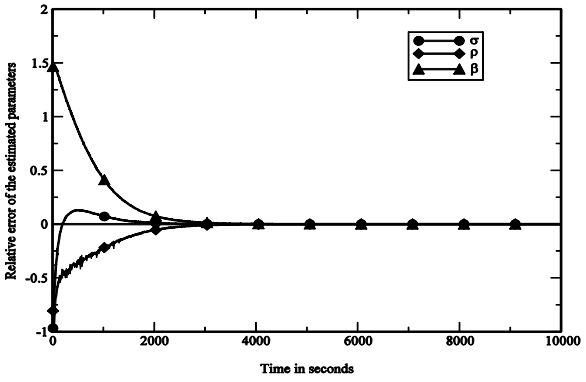

Figure 4. Relative error of the parameters with respect with time. The convergence to zero indicates successful attack

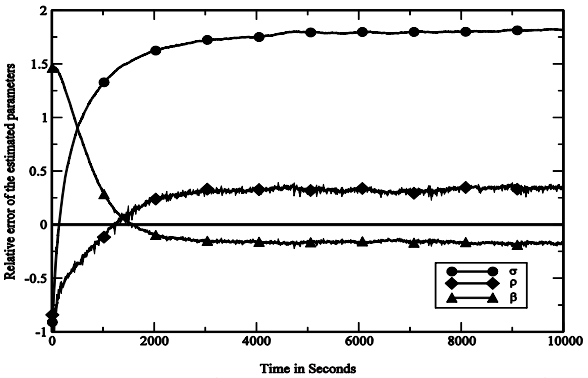

Figure 5. Relative error of the parameters with respect to time for a non-uniformly sampled but periodically driven system. Non-convergence to zero indicated unsuccessful attack

Conclusion

Computerized chaotic system can be made more secure by the proposed modification of dynamic sampling rates rather than static sampling rates. The proposed modification is only a way of implementation. However, there could be different way this dynamism can be brought in. We have found from our simulations that it could be very effective and can be made more complex for an attacker, by keeping the complexity of the genuine participants to minimal. The attacks which have been considered here are the once which are already know and extensively discussed in literature. Hence, more analysis needs to be carried out to ascertain the security level of the chaotic crypto systems.

References

[1]. L. M. Pecora, T. L. Carroll, "Synchronization in chaotic systems", Phys. Rev. Lett. 64 (8), pp. 821-824, 1990.
[2]. L. M. Pecora, T. L. Carroll, "Driving systems with chaotic signals", Phys. Rev. A 44(4), pp. 2374-2383, 1991.
[3]. T. L. Carroll, L. M. Pecora, "Synchronizing chaotic circuits", IEEE Trans. Circ. Syst. 38 (4), pp. 453-456, 1991.
[4]. H. Zhou and X. Ling, "Generating chaotic secure sequences with desired statistical properties and high security", Int. J. Bifurc. Chaos 7, pp. 205-213, 1997.

[5]. Ronge He and P. G. Vaidya, "Implementation of chaotic cryptography with chaotic synchronization", Phys. Rev. E 57, pp. 1532-1535, 1998.
[6]. R Brown and N F Rulkov, "Synchronization of chaotic systems: Transverse stability of trajectories in invariant manifolds", Chaos 7(3), pp. 395-413, 1997.
[7]. T. Yang, "A survey of chaotic secure communication systems", Int. J. Comput. Cognition 2, pp. 81-130, 2004.
[8]. G K Patra, T R Ramamohan, V Anil Kumar, R P Thangavelu, "Improvement in Security Level of First Generation Chaotic Communication System by Mutual Synchronization", Proceedings ADCOM 2006, IEEE Press, pp. 195-198, 2006 .
[9]. G K Patra, V Anil Kumar, R P Thangavelu, "Secure Chaotic Synchronization Using Negative Feedback of Super-positioned Signals", ICISS 2007, LNCS 4812, pp. 193-207, 2007.
[10]. P. G. Vaidya, "Monitoring and speeding up chaotic synchronization", Chaos, Solitons and Fractals 17(2), pp. 433-439, 2003.
[11]. R Konnur, "Estimation of all parameters of a model from discrete scalar time series measurement", Physics Letters A 346, pp. 275-280, 2005.
[12]. A Maybhate and R E Amritkar, "Use of synchronization and adaptive control in parameter estimation from a time series", Phys. Rev. E 59, pp. 284, 1999.
[13]. P. G. Vaidya, S Angadi, "Decoding chaotic cryptography without access to the super key", Chaos, Solitons and Fractals, pp. 379-386, 2003.
[14]. D. Li, J. Lu and X Wu, "Linearly coupled synchronization of unified chaotic systems and the Lorenz systems", Chaos, Solitons and Fractals 23, pp. 79-85, 2005.
[15]. J Park, "Stability criterion for synchronization of linearly coupled unified chaotic systems", Chaos, Solitons and Fractals 23, pp. 1319-1325, 2005.