

## HIGH PERFORMANCE COMPUTING & NETWORKING

Mathematical modelling and computer simulation in the fields of ocean, atmosphere, earth science and engineering involve computational tasks which can only be provided by High Performance Computing(HPC). The need for computational power, measured in terms of Giga Floating Point Operations per Seconds (FLOPS), grows exponentially with every bit of increase in the complexity of problem. C-MMACS today has one of the best computing facilities in the country. In addition HPC group is also involved in research in the field of Cryptography and Network Security.

### *Inside*

- *Chaotic Synchronization by Non-uniformly Sampled Periodic Driving to Avoid Possible Parameter Estimation*
- *High Performance Computing Resources*



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

Almost all chaotic systems studied or known so far are uniformly sampled systems, which means that the trajectory values are determined at equal intervals and also transmitted to the receiver at the same interval. This is done for ease of 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 time. In this work two chaotic systems are considered which are represented by the following system of ordinary differential equations.

Here dot ( $\dot{\cdot}$ ) represents the derivative with respect to time. The system of equations 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 describe the evolution of the variables x and y over time independently. In order to synchronize 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.

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. 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 diluted

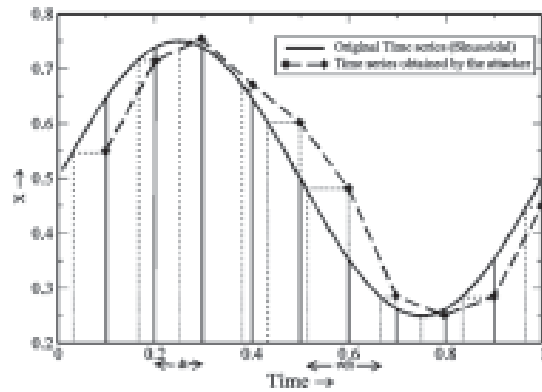


Figure 4.1 A pictorial presentation of uniformly sampled (solid lines) and non-uniformly sampled (dotted lines) time series, communicated at the same time interval.

information to the attacker (to the public), while at the same time preserving the information content for a genuine receiver, one can avoid parameter estimation attacks. In theory a new scheme is proposed by which the attacker will have a distorted time series, while the receiver can still have a non-distorted time series.

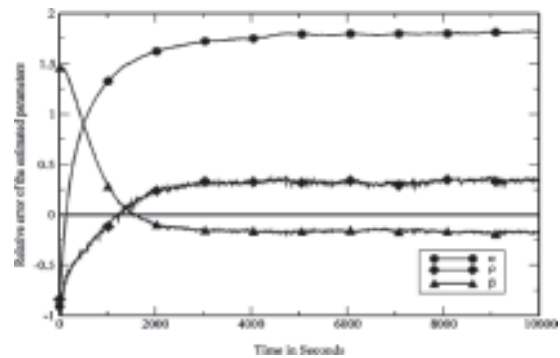


Figure 4.2 Relative error of the parameters with respect to time for a non-uniformly sampled but periodically driven system. Non-convergence to zero indicates unsuccessful attack

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 the receiver happens at uniform duration of " $dt$ " like a normal synchronization, while the value which is sent is sampled at a different but predefined time, in the interval " $dt$ " (but not at time " $dt$ "). This is explained pictorially in Figure 4.1 using a simple sinusoidal time series as an example. The transmitter and the receiver have the exclusive knowledge of knowing the non-uniform time steps.



Figure 4.2 shows the results of parameter estimation attacks based on the least square minimization methods. The non-convergence of the error to zero indicates an unsuccessful attack.

*G K Patra*

## 4.2 High Performance Computing Resources

The Altix 4700 system with 200 Itanium2 processing cores (9140M, 1.66GHz, 18 MB cache), 400 GB of shared memory, 3.6 TB of RAID storage became the major computing platform for modelling and simulation in 2008-09. The system was ranked 10th in the top supercomputers of India list published in November 2008. The performance was measured by a High Performance LINPACK benchmark and it delivered a sustained performance of 1.18 TFlop (1.33 TFlop peak). It is also the largest shared memory system in India.

The Altix 3700 BX2 (2 x 24 processors), Altix 350 (2 x 16 processors) and the Origin 3900 (32 processors) provide an excellent support for smaller jobs, which needs lesser numbers of processors. The jobs are submitted through PBS Pro workload management software for efficient use of the processors and systems. The Origin 3900 system acts as both a compute server as well as a Network File Server (NFS), providing the users home area over network.

### Network Facilities

C-MMACS is connected to the other two campuses of NAL (Kodihalli and Belur) through 10Gbps backbone network. This allows both data and voice transfer between the three major campuses. This enables the scientists from NAL to use the C-MMACS HPC facility from their desktops. Internet is made available through a 512Kbps link to ERNET and a 15 Mbps link from the NAL Kodihalli Campus.

## High Performance Storage

The high performance computing platform is well supported by a high performance Storage Area Network (SAN). It is a virtualized 3-tiered storage solution with 6 TB online (FC), 20TB of near-line (SATA) and 200TB offline (SL500 tape library with 6 numbers of LTO-3 drives) storage. The SAN provides transparent access to data on all the HPC system through shared file systems and hierarchical storage management. This is used as an archival system, while high I/O intensive jobs are run in the local high speed scratch area of the individual servers for better performance.

## Software Enhancements

Continuous upgrade of software is essential to keep in pace with the hardware enhancements. All the software currently in use are updated regularly. The heavily used software are NISA, Hyperworks, Fluent, ANSYS, ABAQUS, CFD-ACE+, IDL, GAMIT/GLOBK, Matlab, Mathematica, Tecplot, S-Plus etc. A current list of hardware and software in the computing environment can be accessed from the C-MMACS website <http://www.cmmacs.ernet.in>. The systems are used extensively for running complex models in the field of Ocean and atmosphere, such as MOM4, LMD GCM, MM5, WRF etc.

## Other Technical Services

Technical support was provided to a large number of users from C-MMACS & NAL. In addition, several students from academic institutions across the country have availed the computing services as part of their academic work at C-MMACS. Technical advice / consultancy were provided to various institutions within CSIR and outside CSIR.

*R P Thangavelu, V Anilkumar, G K Patra, N Prabhu*

