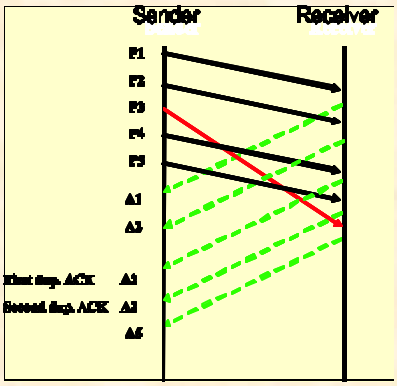
4

High Performance Computing and Networking (HPCN)

Highlights

The research activities on network security and communication have now developed into a comprehensive programme with a several well-defined research tasks.

The year 2006-07 saw a number of important works on network security and secure communication. Alongside, the C-MMACS High-performance computing platform has further evolved in terms of scope.



Inside

- ***Acknowledgement Spoofing Denial-of-Service Attacks: Analysis and Detection***
- ***New Mutual Chaotic Synchronization for secure Communication***
- ***High Performance Computing Resources***

Acknowledgement Spoofing Denial-of-Service Attacks: Analysis and Detection

TCP (Transmission Control Protocol) acknowledgement (ACK) spoofing has become a topic of concern as it can be effectively exploited to launch flooding Denial-of-Service (DoS) attacks to edge networks. Such attacks, if launched, can tactically exploit standard implementation of TCP senders as flood sources and cause DoS scenarios by flooding the Internet access link of the edge-network. Ongoing work at C-MMACS has conducted an in-depth analysis of the feasibility as well as the potential negative impact of such attacks The Figure given below illustrates a scenario where a popular and widely deployed Operating System is exploited as flood source for launching ACK spoofing DoS attack.

Apart from conducting an in-depth analysis of the attack scenario, significant progress has been made towards detecting the attacks scenario through network traffic monitoring. A technique called random packet re-ordering is implemented at IDS (Intrusion Detection System) level and its suitability for the attack detection is being studied in details.

As per section 3.2 of RFC (Request For Comments) 2581 “A TCP receiver SHOULD send an immediate duplicate ACK when an out-of-order segment arrives”. These duplicate ACKs can allow the TCP sender to infer packet loss and then trigger the fast-retransmit algorithm. Packets are said to be re-ordered if a packet with a lower sequence number arrives at the receiver after one or more packets with higher sequence numbers arrive at the receiver.

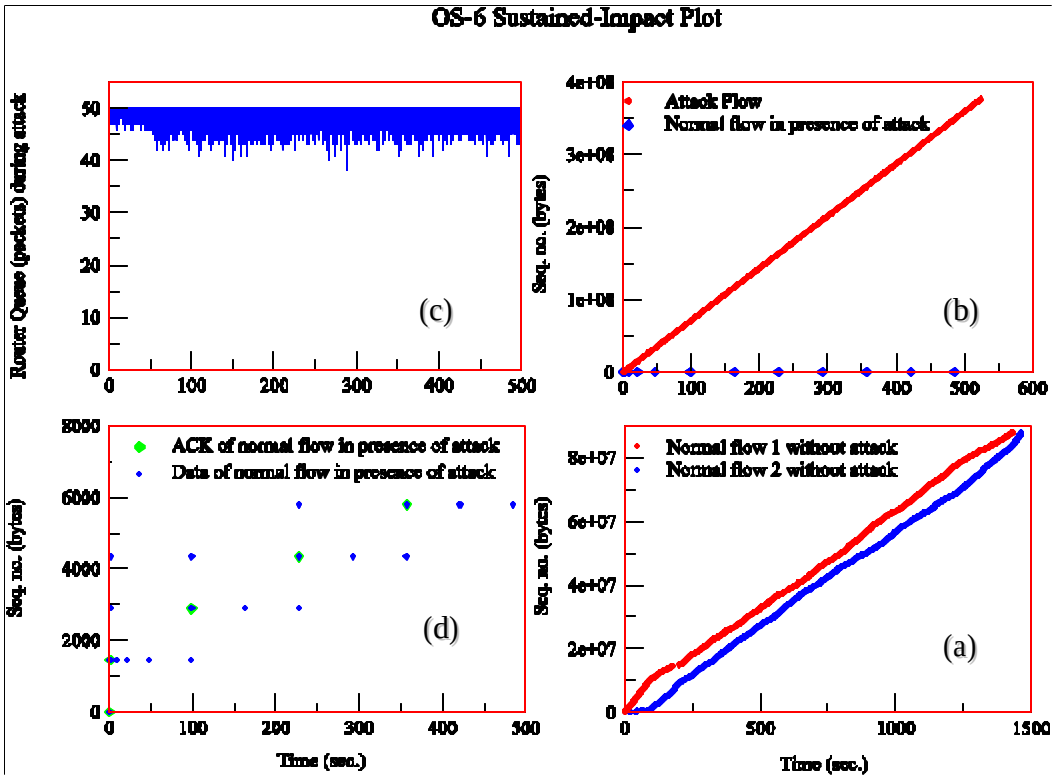


Figure 1: ACK spoofing attack real implementation and impact quantification. Plot (a): time vs. sequence plots of two normal TCP flows in absence of attack; plot (b): the impact of the attack on one of the normal flows when the other normal flow is replaced with an attack flow; plot (c): instantaneous buffer occupancy of the router while it is being subjected to the attack; plot (d): an enlarged view of the time vs. sequence plot of the normal flow in presence of the attack.

For example, if a packet with lower sequence number reaches the receiver after two higher sequence numbers, it is called a two-packet reordering. The normal response of a genuine TCP receiver to re-ordered data packets is shown in Figure 2. Here, P1, P2, P3 etc. are the data packets and A1, A2 etc are the corresponding ACKs. P4 and P5 are the re-ordered packets as they reached the receiver before P3, and both P4 and P5 generated duplicate ACKs, A2 (first A2 is the original ACK and the second and third A2 are the duplicate ACKs).

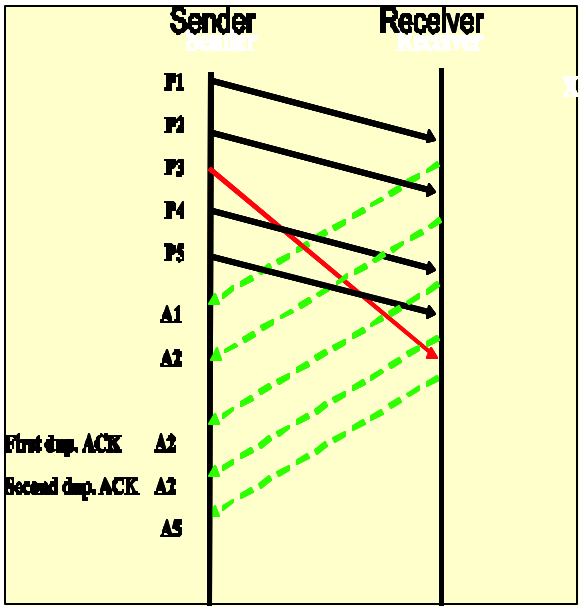


Figure 2: Response of a genuine TCP receiver to re-ordered packets

The fact that well-behaving TCP receivers respond to re-ordered data packets with duplicate ACKs can be translated into an effective signature for attack detection. If TCP data packets are captured and slightly re-ordered in the sender's local network at random time (random packet reordering), only a genuine TCP receiver, which generates ACKs after receiving the data packets, will be able to respond with duplicate ACKs. On the other hand, a malicious receiver (attacker), which spoofs ACKs without actually seeing the data packets, cannot correctly react to the re-ordered packets.

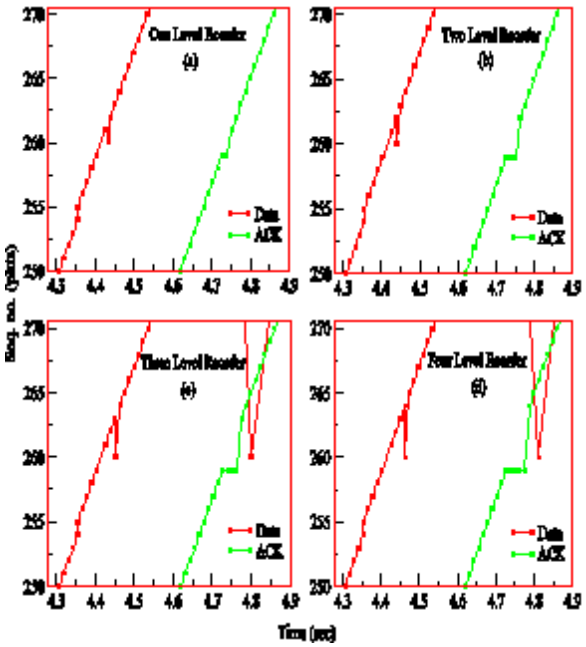


Figure 3: Simulation of packet re-ordering technique (a), (b), (c) and (d) respectively show the time vs. sequence number plot of TCP flows with one, two three and four packet re-ordering

Figure 3 shows the time vs. sequence number plot of data and ACK packets of well-behaving TCP flows with different levels of packet re-ordering. As shown in Figure 3, a one packet re-ordering, resulted in one duplicate ACK (out of the two ACKs for the same sequence number, the first is the original ACK and the second is the duplicate ACK). Similarly, two, three and four level re-ordering triggered two three and four duplicate ACKs. However, it is important to note that three or more packet re-ordering will trigger a spurious re-transmission of the delayed packet, and this can cause performance degradation to TCP flows.

V Anil Kumar, P S Jayalakshmy, G K Patra and R P Thangavelu

4.2 New Mutual Chaotic Synchronization for Secure Communication

Two interacting (non-linear) identical chaotic systems with different initial conditions can synchronize by transmission of only a subset of the state space information. Most of the chaotic synchronization processes are based on master-slave model, where the slave learns from the master for sufficiently large period of time and synchronize. The fundamental weakness of the master-slave based synchronization is that the initial conditions chosen by the master, drives the process of synchronization. One can, by observing the evolution process of the master's publicly available state space variables, pose a serious threat to the security of the system. The attacking strategies are normally based on parameter estimation through a time series analysis of publicly available information. We have proposed a new approach of synchronization which follows learn-learn model where both transmitter/receiver alternatively transmit the values of the same time space variable to each other and synchronize. We will assume that the transmitter and the receiver generate data using two independent but identical differential equations, say the Lorenz equation, which exhibits chaos for specific values of the time independent parameters. We also assume that only the genuine receiver has the parameters already, which is exchanged using an different method. The transmitter and receiver differ only in their time dependent variables because of different random initial conditions.

We introduce the concept of dynamic learning, also called switched mutual chaos synchronization, where the two systems try to synchronize with each other at alternate time steps so that at n^{th} step we get.

$$\frac{dx_1}{dt} = s\ (x_2 - c), \qquad \frac{dy_1}{dt} = s\ (y_2 - c)$$
$$\frac{dx_2}{dt} = (r\ - x_3)c - x_2, \quad \frac{dy_2}{dt} = (r\ - y_3)c - y_2 \qquad (1)$$
$$\frac{dx_3}{dt} = cx_2 - b\ x_3, \qquad \frac{dy_3}{dt} = cy_2 - b\ y_3$$
$$c = \begin{cases} y_1 & for \quad n \equiv 0 \,(\mathrm{mod}\, 2) \\ x_1 & otherwise \end{cases}$$

Using the 4^{th} Order Runge-Kutta procedure the Lorenz equations can be solved for given initial conditions. We can define a Lyapunov function $L = (y_2 - x_2)^2 + (y_3 - x_3)^2\ [\geq 0]$ to see that synchronization can be achieved if β is positive $(dL/dt \leq 0)$.

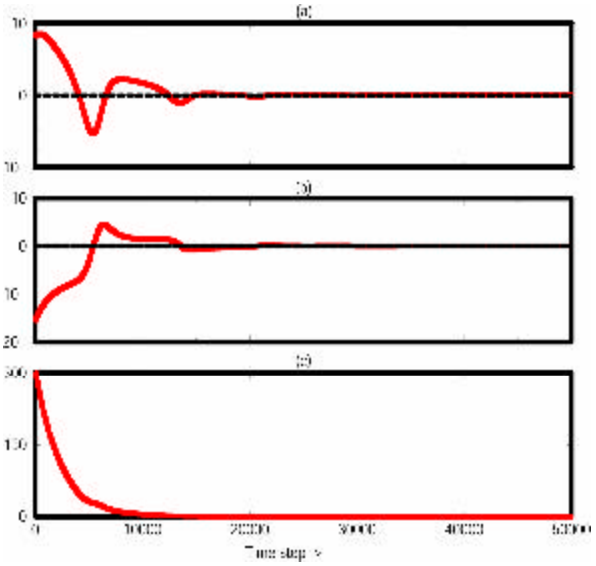


Figure: 4.4 (a) y_2-x_2 with every time step (b) y_3-x_3 with every time step and (c) The monotonic decrease of L with every time step.

As a numerical example we consider a typical case with different initial conditions for transmitter and receiver. The parameters are (σ=10.0, β=2.667 and ρ=28.0). The transmitter and the receiver calculate their trajectories using the Lorenz equations and exchange x_1/y_1 at every alternate time step.

Figure 4.4 (a-b) shows the difference in other variables with time, which shows that the two systems have synchronized. With different initial conditions the synchronization time may vary slightly. Figure 4.4c shows the Lyapunov function decreasing monotonically with time. The advantage of this method is that both Alice and Bob know when the synchronization has taken place. This allows them to use all the time variables for masking of the signal.

We did a time series analysis on the available public signal for both original (P) and proposed method (Q, R, S). The estimated parameter values are given in Table 4.1, which shows successful estimation of P and S. S is the region in the proposed system after the synchronization has happened. This is understandable as after synchronization the two systems behave like the same system.

Table 4.1 Values of the parameters in Lorenz Equation used for different methods.

	s	r	b
P	9.99928	27.99351	2.66608
Q	1086.31431	2.64449	13822.49115
R	57870.148204	5.71277	34782.64162
S	10.02297	27.68638	2.68628

The security of region S can be taken care of, due to the advantage of the method that both the communication parties know when their systems have synchronized. The moment they know the systems have synchronized, they can either stop exchanging the values or frequently communicate and change the parameters of the equation to prevent an attacker from obtaining the super-key. Further they can fool the attacker by sending confusing signals.

G K Patra, T R Ramamohan, V Anil Kumar and R P Thangavelu

4.3 High Performance Computing Resources

The Origin 3900, Altix 350 and the Altix 3700 BX2 servers together with 112 processors and a total computing power of 550 Giga flops continued to be the main stay of the high performance computing facility. These servers were maintained with more than 99% uptime efficiency during the year 2006-07 while the network infrastructure was maintained with 100% uptime efficiency. Apart from C-MMACS users, the major beneficiaries of this computing facility were scientists from NAL, Bangalore and NCL, Pune.

Storage Virtualisation Solution

A significant improvement in the data storage and retrieval at C-MMACS was achieved with the installation and commissioning of a high performance storage area network (SAN) based 3-tiered storage virtualisation solution in July 2006. This facility with an online storage of 6 TB using 4 Gbps fibre channel RAID technology, near line storage of 20 TB on SATA disks, offline storage of 40 TB on tape library along with the SGI data migration facility and clustered XFS file system provides transparent access to data from systems across the network.

Other Hardware & Software Enhancements

The radio link through ERNET was upgraded to 512 Kbps and a new router was installed with security enhancements through extended ACL at router level. Users are provided Internet access through this link and as well as the 10 Mbps link to VSNL from NAL Kodihalli campus. Few desktop workstations with Windows / Linux operating system, a HP C8000 workstation with HP-UX operating system, a HP 8150DN laser printer (A3 size) and a HP

5550DN colour laser printer (A3 size) were added to the computing environment.

S-Plus software was procured and installed for statistical data analysis and data mining applications. Application software such as ABAQUS, CFD-ACE+, IDL, GAMIT/GLOBK, Intel compilers, TotalView debugger, and PBSpro workload management software have been upgraded. A current list of hardware and software in the computing environment can be accessed from the C-MMACS website http://www.cmmacs.ernet.in.

In order to ensure non-stop availability of computing resources to users, DSP technology based 2 x 100 KVA parallel redundant UPS systems were procured, installed and commissioned.

Other Technical Services

Computing services were provided to the hands-on sessions of the Intensive course on Inverse Modelling and Tutorial workshop on Atmospheric Inverse Modelling that were conducted in June and November 2006 respectively. Technical advise / consultancy was provided to various institutions including IICT, NGRI, NCL, IITM, INCOIS, NIMHANS and CLRI on computing and networking. Further, a large number of students from various academic institutions have benefited from the computing services of C-MMACS.

R P Thangavelu, V Anilkumar, G K Patra, N Prabhu and Seenappa