4

High Performance Computing and Networking (HPCN)

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.

Highlights

The year 2005-06 has been a year of growth and expansion for HPCN both in terms of computing resource and areas of research. A substantial enhancement of C-MMACS computing platform took place through installation of an ALTIX-350 12-processor system. The two prominent research areas under HPCN: Network Security and Cryptography, provided new results in these important areas.

Inside

- ***Network Telescope for Malicious Incidents Prevalence Measurement on the Internet***
- ***Denial-of-Service Attacks: Analysis and Detection***
- ***The Web-based Secure & Automated Online Submission Package***
- ***High Performance Computing Resources***

4.1 Network Telescope for Malicious Incidents Prevalence Measurement on the Internet

Network Telescope is an emerging concept in network monitoring. It is a viable alternate to distributed network monitoring approach in which a relatively small portion of the Internet is monitored to infer the security dynamics on the rest of the Internet. Various security related phenomena that could be traced and monitored with network telescope are virus spread, automatic worm propagation, occurrence of Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks.

Network telescope is based on a key observation that during worm propagation and DoS attacks, the adversary spoofs the source address of the malicious packet with a random source address picked from a list of 232 possible IP address space. Hence, any network connected to the Internet receives unsolicited packets triggered by worms and attacks and these unsolicited packets are called backscatters.

We have developed and deployed a network telescope at C-MMACS network to capture and analyze unsolicited packets. Results for preliminary version of this tools are shown in Figure 4.1. Figure 4.1 (a) shows that total number of unsolicited packet received by our monitoring station during a period of 22 days starting from 3rd November 2005. Figure 4.1(b) gives the cause level breakup of total number of unsolicited packets received. Figure 4.1(c) gives the cumulative number of virus/worm infected machines whose IP address falls into the prefix 202.41 and located in Indian region. Finally, Figure 4.1(d) shows the transmission patterns of three virus/ worm infected machines which top-ranked in our list in terms of number of unsolicited packets received from the infected machines.

V Anil Kumar, G K Patra and R P Thangavelu

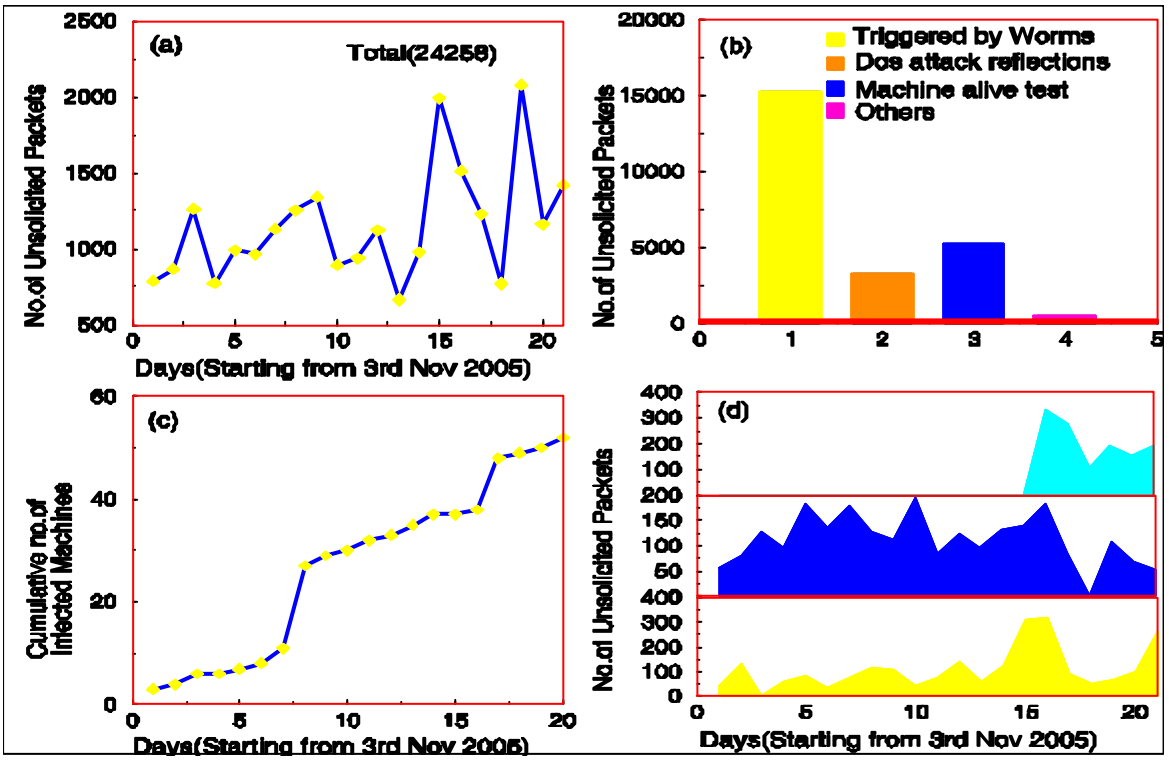

Figure 4.1 Charecterestics of unsolicited packets collected at C-MMACS.

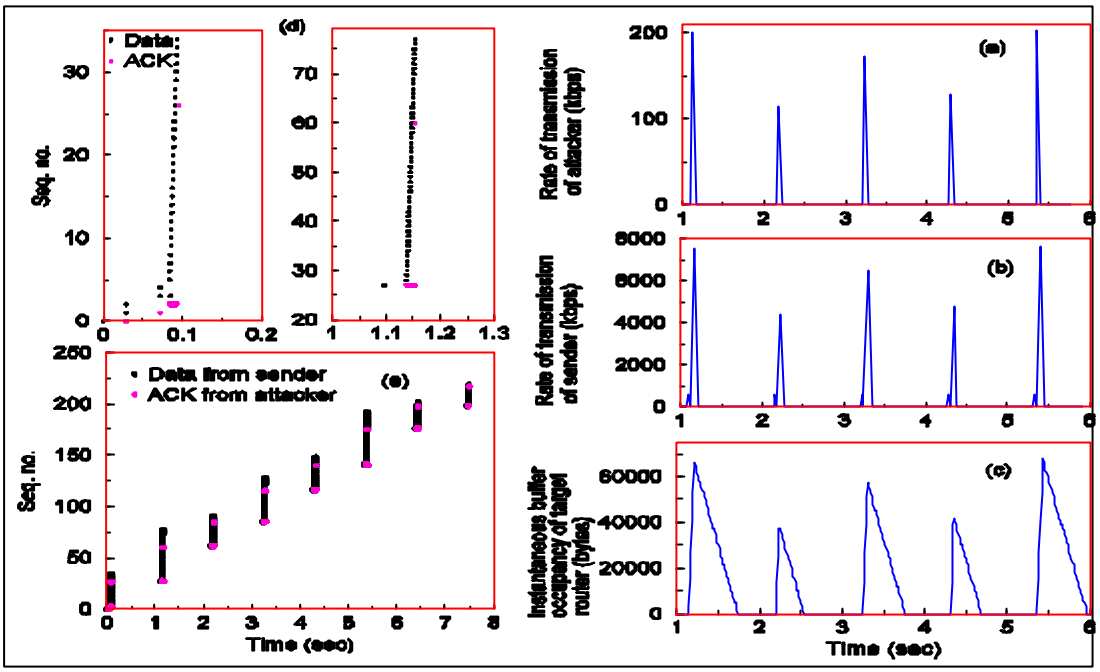

Figure 4.2 (a) Transmission pattern of the attacker, (b) Flood generated by the TCP sender, (c) Instantaneous buffer occupancy of the targeted router, (d) and (e) Time vs. Sequence number plots of the attacker and TCP sender during periodic burst attack at random intensity

4.2 Denial-of-Service Attacks: Analysis and Detection

As part of our ongoing work on analysis and detection of the new class of Denial-of-Service (DoS) attacks, which are constituted by tactically spoofing duplicate and optimistic acknowledgements (ACK), we have identified a number of tactical behaviours of a TCP receiver leading to low-rate DoS attacks. They are burst attacks, sustained attacks and pulse attacks.

Figure 4.2 shows the simulation results of one of the burst attacks, periodic bursts with random intensity. The attacker, in the form of a genuine client, first establishes a TCP connection with the server. It then spoofs several batches of ACKs with each batch having random number of spoofed ACKs and two consecutive batches having constant time gap between them. In response to this, the server ejects periodic bursts of random intensity. Depending on the burst intensity, each burst may completely fill the router buffer resulting in packet drop or partially fill the router buffer leading to high end-to-end delay.

V Anil Kumar, D Sisalem, P S Jayalekshmy

4.3 The Web-based Secure & Automated Online Submission Package

As part of our drive to improve Knowledge Management at C-MMACS the tedious process of submission of inputs to the annual report was simplified by using a "Web-based secure & Automated Online Submission Package". The first module is called "Knowledge Management Online Submission Package", designed to facilitate C-MMACS scientists to submit their technical contribution, reports, publications etc. through a browser. This facility is available through out the year, so that any researcher can use it as an information depository and refers to it whenever required. This has facility to upload files of different formats and preserve it in the server for the publication of annual report, the editor can collect the information and publish it.

This online submission also has another facility of "Online Registration System" for recognizing CSIR scientist as a Ph.D guides of Tezpur University, Osmania University and Cochin University of science and technology, students from various institution also

can register as Ph.D students to carryout their research in the above mentioned Universities, under CSIR University Interface.

These modules are developed using JAVA, JSP, HTML and JavaScript. The "Knowledge Management Online Submission Package" has to be authenticated by using a login name and password which will be created by the administrator, but for "Online Registration System" every user will have to be authenticated using a login name and password, which is created by themselves during the process of registration.

R P Thangavelu, N Prabhu, R Kavita, C Jayalakshmi, Suchanda Ray, Prashant Behara

4.3 High Performance Computing Resources

C-MMACS High Performance Computing was further strengthened after the procurement of two numbers of 24 processors, SGI Altix 3700 server after a detailed technical evaluation based on benchmarking of the possible systems by running LMD GCM and GFDL MOM4. The system is based on Intel Itanium 2 processors and each system is configured with 96 GB of Global memory and software components like Intel Fortran and C++ compilers and MPI libraries.

The 24 processor Origin 3000 server was upgraded to Origin 3900 server by replacing the older 24 processors with 32 numbers of MIPS R16000@1 GHz, 16 MB cache processors. This has enhanced the computing power of the major work horse of the C-MMACS HPC. In addition upgradation of Altix350 servers were done by adding 20 Itanium 2 processors, out of which 16 forms a different system. With this C-MMACS HPC have 112 high performance processors delivering a total computing power more than 550 G flops.

All the high performance servers are maintained with very high uptime efficiency and are efficiently used not only by C-MMACS scientists, but also by other CSIR laboratories. The major applications run on these servers are GFDL MOM, LMD GCM, MM5/ WRF and ABAQUS. In addition commercial application/utilities like Matlab, NISA, GAMIT/GLOBK, IDL, CFD-ACE are extensively used on these servers for designing, processing and visualization.

Storage Area Network

A high performance Storage Area Network (SAN) to cater the ever growing need of data storage is being procured after a detailed technical evaluation of various possible solutions. TP9700 storage solution from SGI is short listed which will provide a three tier solution of about 6 TB of on-line, 20 TB of near-line and 100 TB of off-line storage (archival). This has automatic Data Migration Facility and automatic backup facility. This will provide consolidation and virtualization of the newly procured storage and the already available FC storage. As a result of this all the HPC servers will access the storage as a local file system, which will eliminate the computational time delay arising because of I/O waiting due to Network File Systems (NFS). The SAN is likely to be ready by the end of June 2006.

Other Hardware and Software Enhancements

To improve network services like mail, Webmail, firewall, gateway etc. Intel Pentium based 2U rack servers are procured and are being configured. This is expected to be ready by the end of June 2006. In addition to the HPC servers, to cater the needs of less compute intensive jobs, two numbers of Intel Xeon based servers, one for Linux based applications and other for windows based applications has been procured and installed. The windows server can be access through remote desktop from any PC running both windows and Linux. This has enabled users to access windows applications like Corel Draw, MS-Office from their desktops. This has considerably decreased the financial burden of purchasing individual licensed software for each user.

Software is an integral part of the High

PerformanceComputing. Timely upgradation is essential to keep in pace with the growing requirement. Many new software are purchased and many are upgraded to its newer versions. A complete list of the hardware and software available at C-MMACS can be obtained from the website http://www.cmmacs.ernet.in.

Other Technical services

In addition to providing HPC service for the C-MMACS scientific community, the Computer Communication and Convergence (C3) group also provided various other technical services. This includes supporting students from various institutions of the country to carryout their project work at C-MMACS, and also providing computing facility for Ph.D. scholars from different universities. Computational facilities were provided for various courses and workshops organized at C-MMACS. Further, scientists and researchers from other CSIR and premier institutions use our facility through secure remote login. Technical consultancy is provided to different Government/ CSIR establishment for designing and evaluation of their computing platform. These institutions include INCOIS Hyderabad, DMC Karnataka, SERC Chennai etc.

Last year HPC group was actively involved in restoring the campus wide network from a major cyber attack. Systems affected by various viruses had launched Denial of Service attacks by overloading the campus wide routers and effectively bringing down the total network. The campus network was restored by first analyzing the network at packet level, finding the cause as well as the source and disinfecting them. The analysis showed that almost 50-60% of the systems were infected by some or other kind of viruses. The three campuses were isolated from each other from infection by setting proper need based Access Control List (ACL) at the campus routers.

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