4

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.

Inside

4.1 Challenge-response based Detection cum Prevention System for TCP Acknowledgement Spoofing

Transmission Control Protocol (TCP) senders are vulnerable to optimistic acknowledgements (ACKs). It is now well-known that most of the current generation operating systems seen on the Internet respond to maliciously generated optimistic ACKs. This inherent vulnerability of TCP can be exploited for multiple purposes. First, a greedy TCP receiver (e.g. web or ftp client) can exploit this vulnerability to download files faster than a genuine TCP receiver. Second, a malicious TCP receiver can exploit this vulnerability to launch flooding Denial-of-Service (DoS) attacks to edge-network. Third, an exploitation of this vulnerability in a distributed manner can result in congestion collapse on the Internet. The focus of this work is on design and experimental implementation of a detection cum prevention system to detect and mitigating attacks based on optimistic ACK spoofing. The detection system is designed to work in a Challenge Response manner in which a challenge is thrown to the TCP receiver that needs to be tested, and malicious flows are differentiated from well-behaving flows based on the nature of response from the TCP receiver.

The Challenge is derived based on the fact that well-behaving TCP receivers respond to re-ordered data packets with duplicate ACKs. As a challenge, TCP data packets are slightly re-ordered in the sender's local network at random time (random packet re-ordering). 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. Thus, non-arrival of duplicate ACKs to re-ordered data packets is a potential signature of the attack.

Figure 4.1 gives a block diagram of the deployment architecture of the detection scheme. It consists of two distinct modules, a packet re-ordering module and a network traffic monitoring module, and they can function independently, i.e. without any cooperation or assistance from the TCP end-points. The packet re-ordering module can typically run on a firewall as firewall is a middle-box through which the entire inbound and outbound traffic of a secured network is normally passed through.

The packet re-ordering module monitors

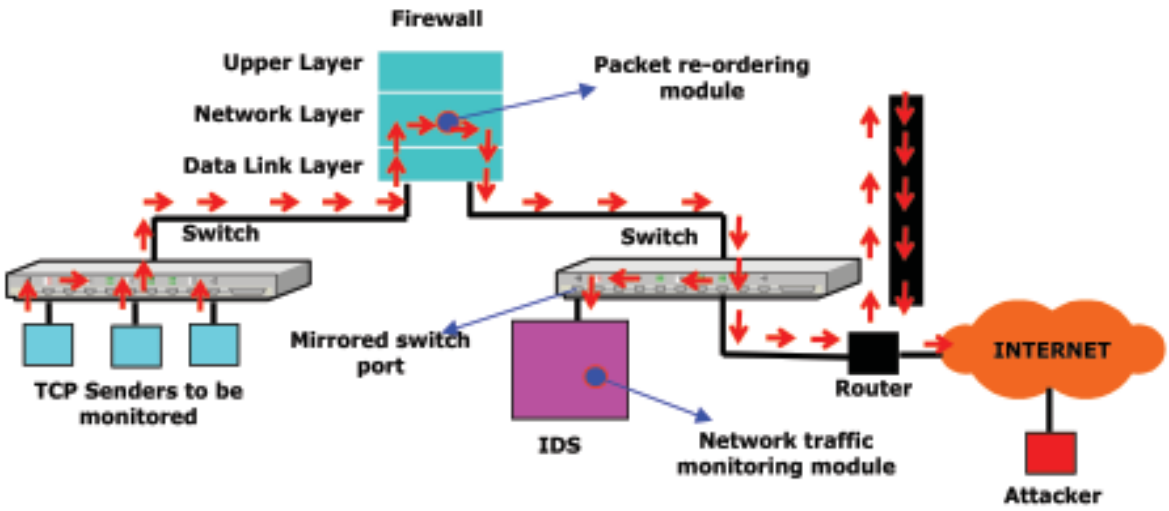

Figure 4.1 Deployment architecture of packet re-ordering based attack detection cum prevention system

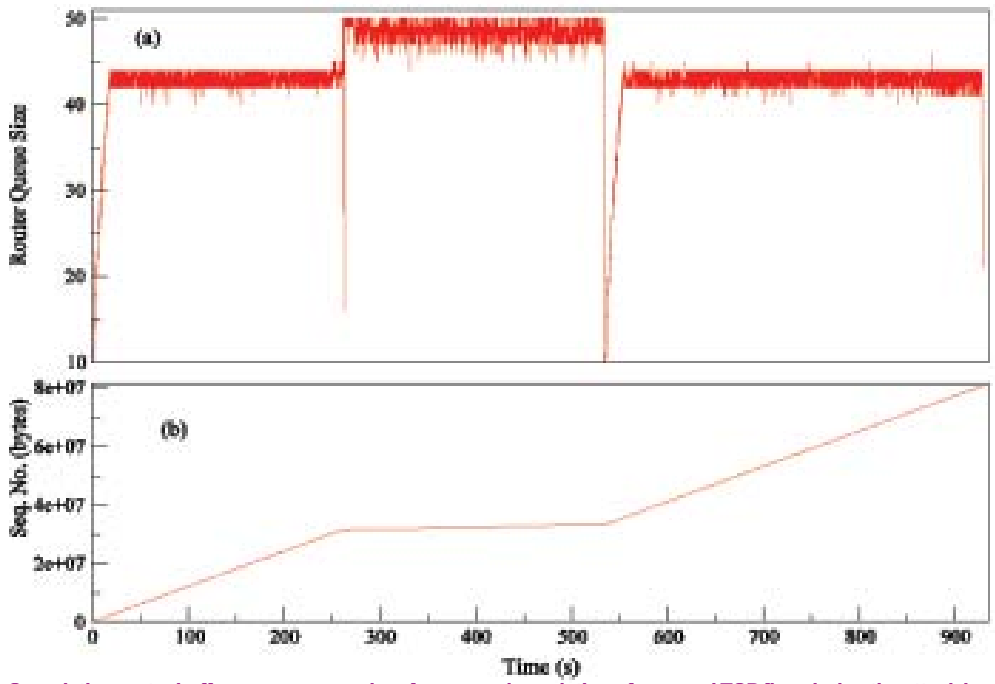

Figure 4.2: Cumulative router buffer occupancy and performance degradation of a normal TCP flow during the attack in absence of the detection system.

outbound TCP flows and injects random re-ordering to data packets of TCP flows.

The network traffic monitoring module can typically run on an Intrusion Detection System (IDS). This module monitors the data packets of the outbound TCP flows, records various state information of the flow including the sequence number of the re-ordered packets, and detects the attacks by monitoring inbound ACKs.

We present a scenario where one normal and one attack flows are passing through a bottleneck link when the detection system is OFF. Figure 4.2 (a) the cumulative router buffer occupancy and Figure 4.2 (b) sequence no. vs. time of the normal flow. At time t=0, the normal flow is started; B (t=260) second, the attack flow is started at which is stopped at about t=540 seconds. The normal flow alone has occupancy of about 42-44 packets in the router buffer space of maximum 50 packets.

However, once the attack flow is started, it suppresses the normal flow and takes up the entire router buffer space. Further, the normal flow is able to take back its buffer share only after the attack flow is terminated. The ability of the attack flow to suppress the normal flow is further evident in Figure 2(b). Initially the normal flow showed a steady growth, and this sustained performance got almost flattened as soon as the attack flow was started. Further, the normal flow starts to regain its performance only after the attack flow is terminated.

Next, Figure 4.3 shows a scenario similar to that in Figure 4.2, except that here the detection system is turned ON. As in the previous case, a normal flow is started at time t=0, which takes about 42-44 packets in the router buffer space (Fig. 4.3(a)). At around t=300 second an attack flow is started, which completely fills the router buffer (50 packets). However, since the detection system is active, it detects the attack flow and terminates it by fabricating and sending an RST packet to the TCP sender. Upon termination of the attack flow, the normal flow takes back its router buffer share. Many attack flows are started one after the other (e.g. at t=400 seconds, t=480 seconds, t=560 seconds etc.). In each case, the attack is terminated shortly after it is initiated.

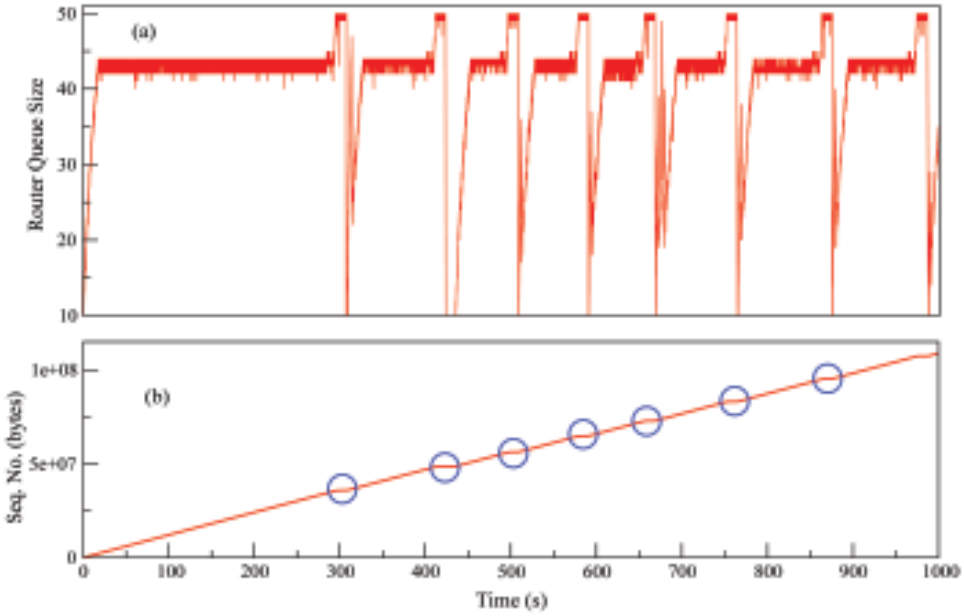

Figure 4.3: Demonstration of the performance of the attack detection cum mitigation system

Figure 4.3(b) shows sequence number vs. time of the normal flow in presence of the attack flows. The circled regions show the sequence spaces of the normal flow when the attack flows are active. Some of these regions are enlarged and placed next to the corresponding circles to highlight the short duration performance degradation experienced by the normal flow. In the above experiment, we have set the threshold for suspicious flow to 20. That means a flow will be tested 20 times before the detection system conclude that it is malicious. Setting a lower suspicious threshold will eventually detect the attack and rescue the normal flow in shorter time.

V Anil Kumar, G K Patra and R P Thangavelu

4.2 Chaotic Synchronization based Secure Communication Mechanisms

The interesting relationship between chaos and cryptography due to the properties such as ergodicity, sensitivity to initial conditions, deterministic dynamics and structural complexity has shown promises for a new class of secure communication mechanisms. The technique of chaotic synchronization is the heart of this new class of systems. Synchronization of two lightly interacting identical chaotic systems can be used to generate large key streams for stream ciphers. Many variants of cryptosystems based on chaotic synchronization have been proposed and some of them are fundamentally flawed due to lack of sufficient security and robustness. In our work we have analyzed two variants of chaotic synchronization one of which is based on alternately switched bi-directionally coupling and other based on negative feed-back of super-positioned signals.

Let us consider a typical synchronization scheme, where the two chaotic systems are represented by the following system of ordinary differential equations:

$$\frac{dx}{dt} = f(x, p)$$
$$\frac{dy}{dt} = f(y, p) \qquad (1)$$

Here x and y are the non-identical state vectors, of the two systems and p is the identical parameter vector. The above set of equations represents two identical chaotic systems. The most popular interaction scheme is the unidirectional coupling, which can be realized either by complete replacement or by using

feedback signals. Both the schemes guarantee synchronization if the Conditional Lyapunov Exponents of the error system $e_i = x_i - y_i$ are negative. For the analysis we have considered a feedback synchronization scheme.

The transmitter and the receiver generate data using two independent but identical systems and time independent variable P, is exchanged between the parties using an alternate method of key exchange. The only difference between the two communicators, are the time dependent variables x and y. For synchronization, one of the state variables from the transmitter is sent to the receiver continuously and the error in that variable is used as a feedback.

By continuing this interaction, both the system synchronizes after a finite number of iterations. This drive/response form of synchronization suffers from very low degree of security, because of its vulnerability to parameter estimation from the public information.

To overcome these vulnerabilities, we proposed a new concept of switched bi-directionally coupled synchronization scheme, where we follow the same drive/response scheme, but the communicating parties alternatively act as transmitter and receiver. This introduces a mechanism of mutual interaction and learning from each other.

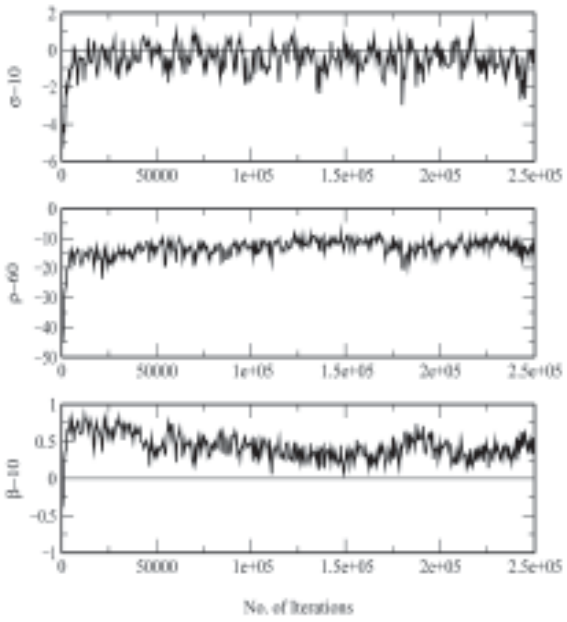

Figure 4.4 Difference in the parameter values of the transmitter and the attacker for synchronization point based modification to the feedback signal.

The synchronization criteria have been deduced from the eigen values of the Jacobian matrix generated from the error system. For a three variable Lorenz system by using alternate bi-directionally coupled system the eigen values are as follows

$$\lambda_1 = -\beta$$
$$\lambda_2 = \frac{-(\sigma+1+k_1)}{2} + \frac{1}{2}\sqrt{(\sigma+k_1-1)^2 + 4\sigma(\rho-<x_3>)} \qquad (2)$$
$$\lambda_3 = \frac{-(\sigma+1+k_1)}{2} - \frac{1}{2}\sqrt{(\sigma+k_1-1)^2 + 4\sigma(\rho-<x_3>)}$$

For a typical Lorenz system with s=10, b=8/3 and r=60 the value of the coupling constant k_1 for x_1/y_1 coupling should be more than 42. We discuss the on-line attack, which are based on the formulation of differential equations governing evolution of parameters. A typical online attack is based on a least square approach, where the identical system z (an attacker) has additional evolutions equation derived by minimizing $G=(z-x)^2$.

By following the trajectory for the variables as well as the parameters, it was found that the attacker will be able to synchronize with the communicating parties as in the case of unidirectional coupling. But the advantage with the proposed method is that, as the communication is bi-directional; both parties know when they have synchronized.

This gives the option to use a modified signal as feedback after the synchronization is achieved. For example after the synchronization is achieved instead of exchanging x_1 and y_1 in alternate steps one can exchange $(x_1+L(x_2,x_3))$ and $(y_1+L(y_2,y_3))$, where L can be a predefined function. Figure 4.4 shows the difference in the parameter

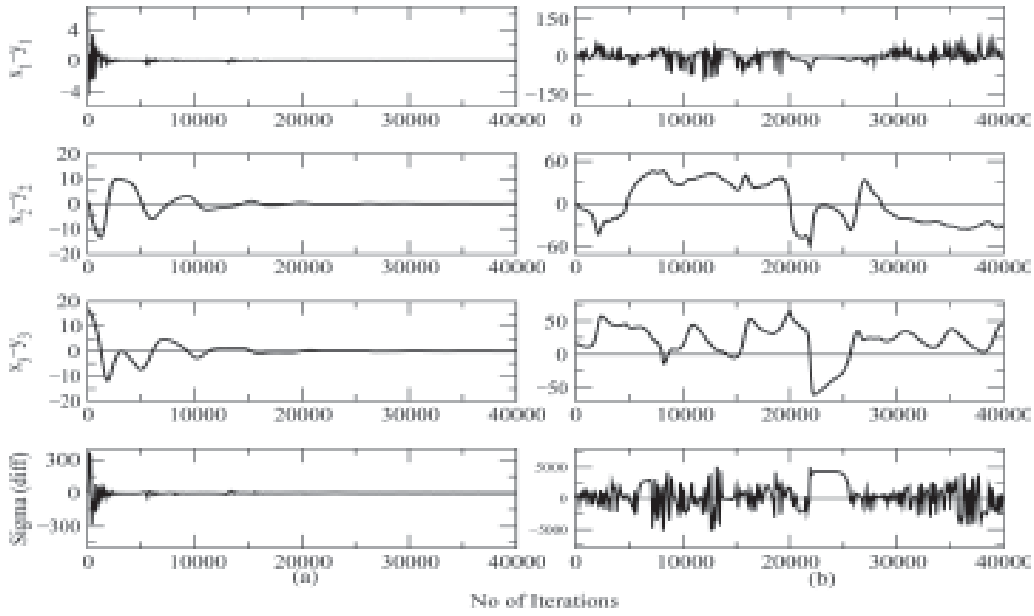

Figure 4.5 Differences in all the three state space variables as well as one of the parameter values of the attacker and the transmitter (a) for a normal one variable feedback synchronization (b) for the proposed super-positioned feedback synchronization.

values of the transmitter and the attracter for synchronization point based modification to the feedback signal, which shows that the attacker is not able to synchronize with the genuine communicators.

positioned feedback and analyzed the security. This modification was expected to provide better security as the information made public is diluted by the superposition mechanism, which is an irreversible process.

We analyzed the synchronization process and derived the synchronization criteria from the Jacobian of the error matrix. We found that synchronization can be achieved for feedback strength more than 13.6 for x_1 coupling. Figure 4.5 shows the result of online security analysis based on the least square approach. The result suggests that synchronization by using super-positioned feedback is protected against on-line parameter estimation methods.

G K Patra, V Anil Kumar and R P Thangavelu

4.3 High Performance Computing Resources

The Altix 3700 BX2 (2 x 24 processors), Altix 350 (2 x 16 processors) and the Origin 3900 (32 processors) servers were the major resources of the high performance computing facility during the year 2007-08. Due to the poor performance of A/C plant for HPC, some of the servers had to be kept off in the initial part of the year which in turn affected the uptime efficiency.

In a move to provide a more computing power to meet the modelling and simulation requirements of scientists from C-MMACS and NAL, an Altix 4700 system with 200 Itanium 2 processor cores (9140M, 1.66 GHz, 18 MB cache), 400 GB of shared memory, 3.6 TB of RAID storage has been procured. The Altix 4700 with SuSE Linux Enterprise Server 10 operating system, Intel Compilers and cluster tools provides a powerful combination for excellent performance on compute and memory intensive applications. This server is expected to be the largest shared memory system in India.

Storage Virtualisation Solution

The high performance storage area network (SAN) based 3-tiered storage virtualisation

was further augmented by upgrading the SL 500 tape library with additional tape drives and tape slots and is presently configured with 6 nos. of LTO-3 drives and 500 tapes (200 TB). The DMF facility has been scaled up, to support 500 TB of storage virtualisation. The SAN implementation has enhanced the productivity by providing transparent access to data across all HPC systems through shared file system and hierarchical storage management.

Networking Resources

The backbone network connecting C-MMACS to NAL campuses at Kodihalli and Belur was upgraded to 10 Gbps by deploying Cisco 3750E switches with 10 Gbps uplinks. In addition, new access switches have been installed for better desktop connectivity. Internet services were provided through the 512 Kbps link to ERNET and as well as the 10 Mbps link to VSNL from NAL Kodihalli campus.

Other Hardware & Software Enhancements

About 45 numbers of HP desktop computers based on Pentium dual core processor, 2 GB memory, 19" TFT monitor were installed as a replacement to old desktops. Most of these new desktops run on Linux operating system while few of them run on Windows XP operating system. Major application software available on the C-MMACS computing environment include MOM4, LMD GCM, MM5, WRF, 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.

In order to meet the cooling requirements of the Altix 4700 server, the A/C plant for the HPC data centre was revamped by replacing the old A/C units with new packaged A/C units providing a total capacity of 33 TR.

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 including CSIR HQ, IICT, INCOIS, and NIMHANS on computing and networking.

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