Design of System on Chip for Generating SYN Flood Attack to Test the Performance of the Security System

Shaila R Ghanti
Dept of Electronics, Goa University,
Goa, India

G.M.Naik
Dept of Electronics, Goa University,
Goa, India

ABSTRACT
DDoS attack is generated by the attacker on the server, so that the genuine clients will not have access to the services provided by server. To protect servers from such attacks, large variety of security systems are available. The best security system can be selected by comparing the performance of these systems. There is a need to generate attacks at very high speed to test the performance of security system. This manuscript presents the design of FPGA based reconfigurable hardware System-on-Chip (SoC), that can generate the SYN flood attacks at high speed in real time. The SoC SYN flood attack is implemented using the soft core NIOS II processor, Triple_Speed Ethernet, etc. The manuscript also compares the attacks generated using such hardware based SoC SYN flood attacker with the SYN flood attacks generated using purely software based tool hping3. It is found that the attacks generated using FPGA based system is much faster than software based tool.

The same hardware design can be used to generate many different types of attacks such as spoofed, non-spoofed, layer 3 , layer 4 attacks like TCP flood attack, UDP attack, ICMP flood attack, TCP SYN-ACK attack, TCP FIN-ACK attack, etc. Such attacks are essential to benchmark the security systems. The proposed technique can be used as industry standard to benchmark the performance of the security systems.

General Terms
Security, syn flood attack, fpga.

Keywords
FPGA, NIOS II processor, Packet generation, SYN flood attack, Triple-Speed Ethernet etc

1. INTRODUCTION
Today we all are heavily dependent on the services available on the Internet for day to day activities like E-mail, browsing, money transactions, etc. According to Neustar annual report [1] over 90 percent of respondents see DDoS attacks as the bigger threat compared to the previous year. SYN flood attack is a type of DDoS attack generated on the Internet, by which the access to the service is denied. Hence it is very important to protect servers from such attacks. As the number of attacks and type of attacks gets larger on Internet, the new methods of detection and prevention of attacks also increased proportionately. If these detection and prevention methods are to be deployed to secure the servers, then there is a need to select the best security systems based on its performance. In order to test the performance of the security system, there is a need to generate continuously different types of attacks at a very fast rate so that benchmarking of security systems can be done.

Although software tools like Hping3 [2] are available that can generate such attacks but the speed at which these tools can generate attack is slow.

Today lot of work is done to improve the performance of security systems by using hardware design so that they process data at a very high speed. But however authors have not come across any attack tools designed using hardware systems. Hence our important contribution of developing hardware tool that generates SYN flood attack is important. As hardware based systems can generate these attack packets at a very fast rate. Also, there is a need to reconfigure based on based on the type of attack. Therefore Field Programmable Gate Arrays (FPGA) [3] can be used to generate different types of attacks, that provides all the advantages of using hardware and also provide the flexibility of software such as re-configurability.

Hence, in this paper we design and implement a FPGA based System on Chip (SoC) that generates SYN flood attack at very high speed and in real time. It is used for benchmarking of the security system. The attacks generated using the hardware based SoC SYN flood attacker is compared with the SYN flood attacks generated using purely software based tool called hping3.

2. BACKGROUND
Internet provides many services using TCP client server technology and the most common is web based applications. The client communicates to the server by first setting up the TCP connection using three way handshakes. The TCP connection using three way handshakes is set up first by sending SYN packet to the Server [4]. The Server replies with SYN-ACK and the client will respond with ACK as shown in below figure1

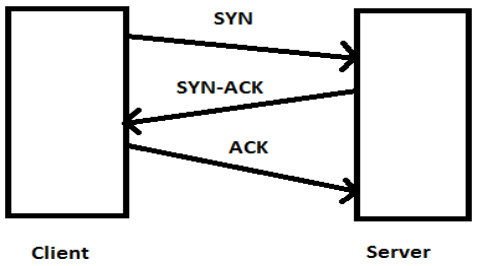

Figure1: TCP three way handshake

During SYN flood attack the attacker sends large number of spoofed SYN packets to the server. The server replies with the SYN-ACK by setting the half-open connections on the server. As the attacker is using spoofed source IP address the server will never receive corresponding ACK. The server keeps on waiting for the ACK till the TCP connection delay expires. During this time the large number of half-open connections is

set up on the server, which consumes all server resources. Hence during SYN flood attack if the genuine user requests for TCP connection, the service is denied to the genuine clients. Such servers need to be secured from SYN flood attacks using the best protection/prevention System.

3. RELATED WORK

The performance of IPS used to protect the server against the DDoS threat is evaluated by generating different attacks using the hping3 tool [6]. The study uses FPGA based network packet generator using VHDL [7] code that generates different packets used for testing at different layers. A packet generator is implemented on NETFPGA [8] allows Internet packet to be transmitted at a very fast rate.

4. PROPOSED METHOD FOR DESIGN AND IMPLEMENTATION OF SOC SYN FLOOD ATTACK GENERATOR AT HIGH SPEED

4.1 Design and Implementation of FPGA based SoC SYN flood attack generator

The hardware system is built using the NIOS II Processor, Triple Speed Ethernet Mega Core [9], Transmit SGDMA, Receive SGDMA, JTAG UART component, and On-chip memory as shown in figure2

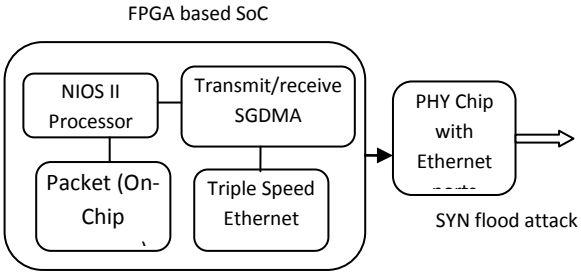

Figure2: Block diagram of FPGA based SYN flood attack generator

NIOS II is a soft core IP Processor provided by Altera and can be added to FPGA and is used to run an application program. Triple-speed Ethernet Mega Core is a configurable IP core that complies with the IEEE 802.3 standard. It is used so that media access controller feature is used in this system that supports 10/100/1000 mbps. The two SGDMA controllers are used to transmit and receive functions of the core [10]. The program code, data as well as descriptors for the SGDMA controllers are stored in on-chip memory. JTAG UART is used to provide communication support interface to PC to processor on the FPGA. Altera's DE4 board is used to implement the SYN flood attack generator on Stratix IV GX EP4SGX230KF40C2 FPGA.

Quartus II 11.1 QSYS software is used to build the hardware system[10]. Adding the components NIOS II Processor, Triple-speed Ethernet Mega Core, Transmit SGDMA, Receive SGDMA, JTAG UART component, and On-chip memory components and making necessary connections, the hardware system is created as shown in below figure 3. Besides the above components the Phase Locked Loop (PLL) module is used to generate clocks with different frequencies to make the triple-speed Ethernet system work properly. Then QSYS tool is used to generate VHDL code for the SYN flood attack generator.

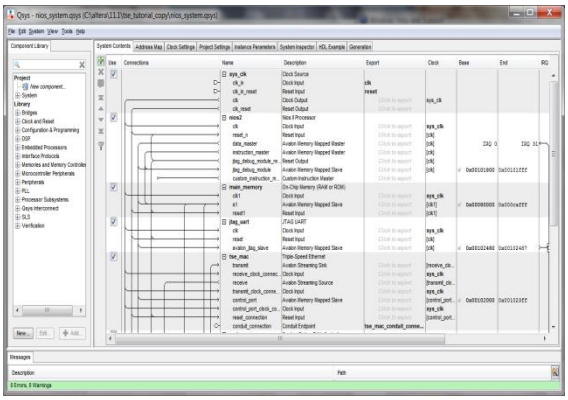

Figure3:QSYS components

Quartus11.1 is used to integrate the modules by adding the necessary pin assignments for the DE4 board. Then compile the whole project in Quartus. The soft core is downloaded onto FPGA. NIOS II version11.1 software is used to run application program that generates packet headers. An application program is created to initialize the triple speed Ethernet IP core to read and write transfers, and also to open and set interrupts for SGDMA device. The Ethernet header, IP header and TCP header are created as shown in figure4 to generate the SYN packets [11][12].

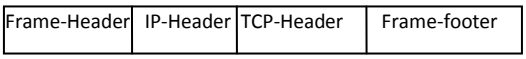

Figure4: Frame details

Hardware System creates the packets with the SYN=1 and sends the packet through the triple-speed Ethernet on to the network. Thus the SYN flood attack is generated.

4.2 Testing the SoC SYN flood attack generator

The experimental set up is as shown in below figure5. Xampp web server is downloaded and installed on windows 7 system [13].

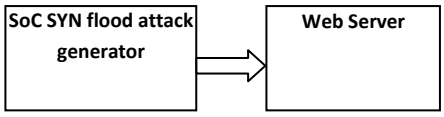

Figure5: Experimental set up to test the effect of SoC SYN flood attack generator

The SYN flood attack is generated using the above designed SoC SYN flood attack generator, and the netstat command is used to check the half open connections set up on the server. It is found that half open connections are set up on the server. This indicates the SYN flood attack is generated.

4.3 Comparison of software based SYN flood attack generator with FPGA based SoC SYN flood attack generator

First, Generate SYN flood attack using hping3 tool. As shown in figure 6, one machine is used to generate SYN flood attack using hping3, the command is: Hping3 –c 897 –S –p 80 172.22.1.16. Another machine is used to capture the packets generated on the network using Wireshark [5].

Next Generate the SYN flood attack using FPGA based SoC attack generator. The SoC SYN flood attack generator is connected instead of machine to another machine and the attack is generated as shown in figure 6. Then Wireshark is used to capture the attack packets on another computer.

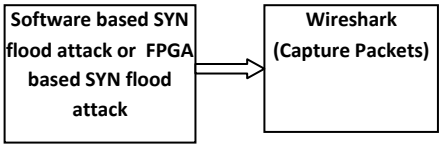

Figure 6: Experimental set up to generate attack using software tool and SoC SYN flood attack.

These captured packets were analyzed and results are discussed in section-V of the manuscript.

5. RESULTS

The FPGA based SoC SYN flood attack generator is successfully implemented on DE4 board and the resource utilization is only 5%, the details are as shown in below table1

Table 1: FPGA Utilization

1	Logic utilization	5 %
2	Total registers	6900
3	Total pins	9 / 888 (1 %)
4	Total block memory bits	2,689,972 / 14,625,792 (18 %)
5	DSP block 18-bit elements	4 / 1,288 (< 1 %)
6	Total PLLs	2 / 8 (25 %)

Figure 7 below shows the screen shot of wireshark tool that has captured SYN flood attack packets generated on the network using hping3 tool. Similarly we have captured the SYN flood attack packets generated by FPGA based SoC SYN flood attack generator.

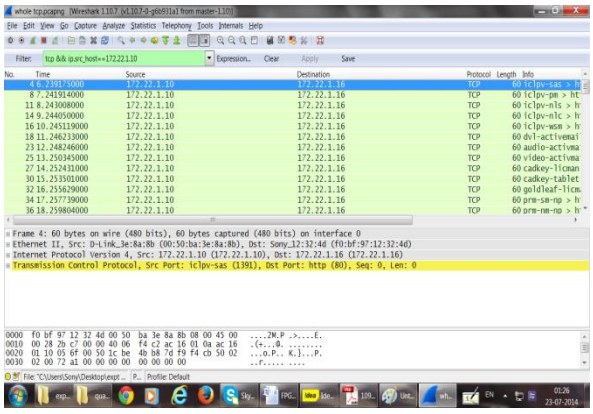

Figure 7: Packets captured by wireshark

After analyzing the attack packets generated both using hardware based SoC SYN flood attack generator and the software based hping3 tool the results are as shown in the below table 2

Table 2: Comparison of SYN Packets received due to software tool hping3 and FPGA based SoC SYN flood attack System.

	SYN attack generated by hping3 tool (Software tool)	SYN attack generated by FPGA based SoC(Hardware tool)
Avg bytes/sec	47.335	4986.157
Avg bit/sec	**378**	**40000**

It is found that the average number of bits generated per second using the SOC SYN flood attack generator is **40,000**. The average number of bits generated per second using hping3 tool is **378.** The results prove that the SoC SYN flood attack generator is capable of generating attack much faster than the hping3

6. CONCLUSION

A good security system can be selected based on benchmarking of the security system. To benchmark the security system there is a need to generate attacks at a very high speed. Hence hardware tool described above which can generate SYN flood attack at very high speed in real time is appropriate for testing the high performance servers. In the present study the hardware based SoC SYN flood attack tool is successfully implemented on DE4 FPGA board. The testing of SoC SYN flood attack was done on the xampp web server. It is observed that the server gets attacked as all the resources of server are used in setting up of half–open connections. The results show that the FPGA based SoC SYN flood attack generator has very high performance as compared to software based tool hping3. The same hardware design can be used to generate attacks such as spoofed, non-spoofed, layer 3, layer 4 attacks, like TCP floods attacks, TCP random flag flooding, ICMP echo flood, UDP attack, TCP SYN-ACK attack, TCP FIN-ACK attack etc.

The basic hardware design can be modified to work as ethical hacking tool, as a network monitoring tool, router, firewall, Intrusion Detection System, Network Address Translation etc.

7. ACKNOWLEDGEMENT

This work is supported by UGC minor research Project

8. REFERENCES

[1] Neustar Annual DDoS Attacks and Impact Report "THE DANGER DEEPENS" 2014 http://www.neustar.biz/resources/whitepapers/ddos-protection/2014-annual-ddos-attacks-and-impact-report.pdf

[2] "Download Hping3 source code" . http://www.hping.org/download.html

[3] "Introduction to FPGA Technology: Top 5 Benefits" http://www.ni.com/white-paper/6984/en/, Publish Date: Apr 16, 2012 | 52 Ratings | **3.69** out of 5

[4] Andrew S. Tanenbaum, "Computer Networks", 4th edition

[5] "Learn" "Enhance" "download Wireshark" . http://www.wireshark.org/

[6] Prof Bill Buchanan, Flavien Flandrin, Richard Macfarlane, Dr Jamie Graves, Edinburgh Napier

University, 10 Colinton Road, Edinburgh, EH10 5DT, "A Methodology to Evaluate Rate-Based Intrusion Prevention System against Distributed Denial-of-Service (DDoS)"

[7] Venkata Yellapragada, Venkat Gaddam, shripal Pandey a project report on "Network Packet generators" April 17, 2009

[8] G. Adam Covington, Glen Gibb, John W. Lockwood, Nick McKeown, " A Packet Generator on the NetFPGA Platform" http://yuba.stanford.edu/netfpga/documents/NetFPGA-FCCM-2009-Packet_Generator.pdf

[9] "Triple-Speed Ethernet Megacore Function user Guide" www.altera.com/literature/ug/ug_**ethernet**.**pdf** Document last updated for Altera Complete Design Suite version:13.0 Document publication date: May 2013

[10] Using Triple-Speed Ethernet on DE4 Boards. ftp://ftp.altera.com/up/pub/Altera_Material/12.0/Tutorials/DE4/using_triple_speed_ethernet.pdf

[11] Jami Aditya and Priyanka Priyadarsini, "Application of Ethernet over powerline Communication" Department of Electronics and Communication Engineering National Institute of Technology, Rourkela May, 2013. http://ethesis.nitrkl.ac.in/4695/http://generalengineering.sjsu.edu/docs/pdf/mse_prj_rpts/spring2009/Network%20Packet%20Generator_By_Pandya_etal_EMD.pdf

[12] "The TCP/IP Guide–A TCP/IP Reference you can understand" http://www.tcpipguide.com/free/index.htm

[13] "Free Software download" Xampp webserver http://download.cnet.com/BitNami-for-XAMPP/3001-2070_4-75924895.html?hlndr=1