RSS: A Reconfigurable Security System Designed on NetFPGA and Virtex5-LX110T

Kai Zhang[1], Xiaoming Ding[1], Ke Xiong[1,2], Baolong Yu[1], Shuo Dai[1]
1. Institute of Information Science, Beijing Jiaotong University, Beijing, P.R.China, 100044
2. Department of Electronic Engineering, Tsinghua University, Beijing, P.R.China, 100084
kzhang0503@gmail.com, xmding@bjtu.edu.cn, kxiong@tsinghua.edu.cn, baolong_yu@163.com

ABSTRACT
This paper designs a novel security system on NetFPGA platform and Virtex5-LX110T using embedded soft-core technology. The system consists of two subsystems. The first one is a mainly used to protection subnets, which is implemented on NetFPGA board and the second one is a network intrusion detection system (NIDS) which is implemented on Xilinx Virtex5-LX110T board. Moreover, the two subsystems are not independent and they cooperate to form the cohesive reconfigurable security system (RSS). In the proposed system, NetFPGA is used to achieve packet filtering, ARP attacks immunity and traffic monitoring with hardware, which is in fact a hardware firewall, and Virtex5 is used to analyze attacks by capturing incoming packets, then transmitting the results to NetFPGA for updating packet filtering tables. To further enhance the security, two types of remote reconfigurable design methods are introduced, by which administrators are able to reconfigure both the software and the hardware of the two subsystems via authorized devices to change the security policies. Extensive experiments show that all the functions of the designed blocks are valid and the designed security system is feasible.

Keywords
Hardware Firewall; Network Intrusion Detection System; Remote Reconfiguration; NetFPGA;

1. INTRODUCTION
With the rapid popularization of network technology, network security issues have become more and more severe. How to effectively improve network security has become an urgent problem. Network attacks, including denial of service attacks, unauthorized access, distributed attacks and SQL injection, are still rampant in networks. The dramatic rise in computer security attacks underlines the importance of security measures and forces people to reconsider a new kind of high-efficiency and more secure strategy besides traditional firewall and NIDS in network security protection to deal with the increasingly serious issues of network security.

This paper explores that how reprogrammable network hardware can help us to build network security protection system, such as reconfigurable hardware firewall and embedded NIDS that offer security, flexibility and programmability while achieving good performance and strong isolation. In this paper, we present the design and implementation of a reconfigurable security protection system on the basis of NetFPGA and soft-core technology. This system has two subsystems, in which one is implemented as a reconfigurable hardware firewall on NetFPGA for the subnet security protection and the other is run on Xilinx Virtex5-LX110T platform to implement a NIDS to detect malicious activity. In our protection system, NetFPGA is used to achieve packet filtering in hardware, immunity against ARP attacks, traffic monitoring and transmitting with hardware acceleration, and the Virtex5 board is used to read all the incoming packets, try to find malicious activity such as denial of service attacks, port scans, SQL injection and send the results of pattern matching to the Firewall immediately to help the Firewall. In order to further enhance performance, security and flexibility of our system, including both the firewall and the NIDS, we introduce two types of remote reconfigurable design method, by which administrator is able to reconfigure the two subsystems for both the software and the hardware logical circuits via any authorized devices.

The rest of this paper is organized as follows. In Section 2, we briefly introduce the related work first. Then we describe the architecture of this system as well as the implementation details such as fast packet filtering on NetFPGA platform, the embedded NIDS on Virtex5 platform, and the coordinate operation in Section 3. Section 4 presents the remote reconfiguration principles and procedures. Section 5 presents experimental results. Section 6 and Section 7 discusses future work and concludes the paper.

2. RELATED WORK
2.1 Traditional Firewall
Firewall is a useful tool for protecting networks from malicious and harmful attacks. Firewalls were first introduced in 1989 by Jeffery C. Mogul [2]. They were evolved under different changes during these 19 years. They are usually installed in primary entry point of the network with a pre-defined policy and relevant rules [3]. The administrator will define appropriate rules to protect the network against malicious attacks. It can be a valid solution for preventing most of intrusion. However, there are many limitations in traditional network firewalls.

Traditional network firewalls can be implemented in hardware or software. Traditional software firewalls are considered easier to set up and administrate, and the administrator can easily update the software upgrade package or replace it with new software to deal with new types of attack. Nevertheless, for its speed and throughput is not high enough, traditional software firewall can only fulfill the security requirements of low-bandwidth and low-flow environment [4], because bandwidth bottleneck likely causes system crashes in high-speed network environment.

Traditional hardware firewalls are often considered faster and more secure than software firewalls. Depending on the size of the private network, a hardware firewall may be responsible for filtering the network traffic of hundreds of clients [3]. However,

since the security chips and peripheral circuits are specifically designed for particular security attacks, dealing with new types of attacks needs to update the security module in software and replace the entire chip or the entire equipment. That means a lot of time and money would be wasted. Besides, this complicated work needs professional and technical personnel to deal with.

2.2 Network Intrusion Detection

A firewall is not the ultimate solution for network security. Total reliance on the firewall tool may provide a false sense of security. The firewall will not work alone (no matter how it is designed or implemented) as it is not a panacea. The firewall is simply one of many tools in a toolkit for security policy in information security. It is inconvenient for the firewall because most information about attacks of the firewall depends on the administrators.

Similarly to firewall, another buzzword has recently become very popular, NIDS. NIDS solutions are designed to monitor events in a security protection system, thus complementing the first line of defense (behind firewalls) against attacks. It tries to detect malicious activity such as denial of service attacks, port scans or even attempts to crack into computers by monitoring network traffic.

2.3 Reconfigurable Technique

The concept of reconfigurable computing has existed since the 1960s, when Gerald Estrin's landmark paper proposed the concept of a computer made of a standard processor and an array of "reconfigurable" hardware [5][6]. The main processor would control the behavior of the reconfigurable hardware. The latter would then be tailored to perform a specific task, such as image processing or pattern matching, as quickly as a dedicated piece of hardware.

The reconfigurable computers can be categorized in two classes of architectures: hybrid computer and fully FPGA based computers. Research on identifying major trends in general-purpose and special-purpose design methods showed that reconfigurable computing designs are capable of achieving up to 500 times speedup and 70% energy savings over microprocessor implementations for specific applications [7].

In information security, compared with traditional firewall, reconfigurable firewall can achieve many significant improvements in performance and security. It can be designed as a new structure. Most parts of it can be designed and implemented in hardware to improve its performance and security. Therefore, to solve the problems of traditional firewall, this paper presents a reconfigurable firewall on the basis of NetFPGA platform for the subnet security protection.

3. REMOTE RECONFIGURATION SUPPORTED HARDWARE FIREWALL

3.1 Architecture

This protection system is on the basis of NetFPGA platform and embedded soft-core technology. The hardware firewall is implemented as a reconfigurable hardware firewall on NetFPGA platform, and the other is run on Xilinx Virtex5-LX110T board to implement a NIDS to detect malicious activity and report the results of pattern matching to the hardware firewall. One of the network topology of this system is depicted in Figure.1.

On the one hand, most parts of this hardware are designed and implemented in hardware to be faster and more security. For instance, packet filtering in hardware, immunity against ARP attacks in hardware, traffic monitoring and transmitting with hardware acceleration are designed and implemented on NetFPGA to protect the subnet from network attacks. On the other hand, most parts of the NIDS are implemented in software. It receives the copied packets from the hardware firewall, and then transmits the detection results back to the firewall to help it protect the network security effectively.

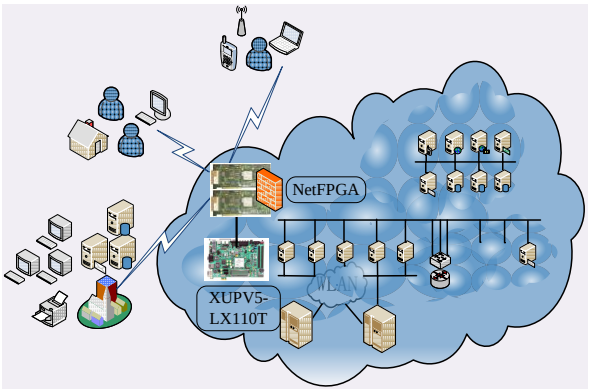

Figure 1. Architecture of the Network Topology of This Security Protection System.

3.2 Key Blocks Design

Our main focus in this section is on describing the implementation of packet filtering in hardware on subnet protection subsystem, embedded NIDS, and the coordinate operation with the two subsystems.

3.2.1 A Cohesive Firewall/IDS System

The two subsystems are not only independent with each other. On the contrary, the whole security protection system is a cohesive system. The reconfigurable hardware firewall uses Logic Element to deal with packet filtering in hardware, immunity from ARP attacks in hardware and traffic monitoring with hardware acceleration. At the same time, the firewall copies all of the packets to the other subsystem, NIDS. While the NIDS are running to receive the copied packets from the hardware firewall, run the BMP pattern matching, and then transmit the detection results back to the firewall.

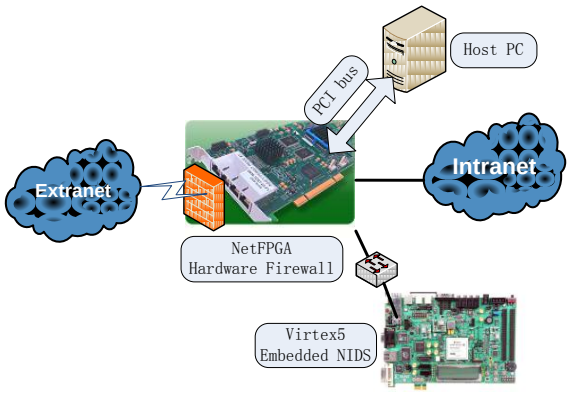

Figure 4. the Coordinate Operation of the System

3.2.2 *Fast packet filtering in hardware*

We selected NetFPGA as the subnet security protection subsystem platform because it offers fast way to develop custom network systems that run at line-rate, and to create re-usable designs to share with others [8]. It provides an easy way to move our implementations directly on hardware by taking advantage of reprogrammable FPGA circuits enabling prototype implements that can handle high speed data processing and transmission (4*1Gbps). We can also avoid time consuming and expensive process of designing new physical hardware components.

Our hardware firewall is focused on the data path implementation of the packet filtering modules for fast packet filtering. To implement it, we have redesigned the Output Port Lookup module of the reference router, designed a new program and panel to control the data exchanging via PCI bus and cooperate with the hardware system. Figure 2 shows the layout of the modules with the addition of the packet filtering in hardware and removing modules and hardware firewall's control panel on the CentOS system.

The "preprocess_new" module is a new preprocess block with controlling the packets analysis of the next components. The "src ip parser and filtering" module is a new processing block with indentifying packets containing untrusted source IP addresses, while the "port parser and filtering" module is another one with indentifying vulnerability ports. After indentifying, the "remove filtered packets" module is designed to remove packets according to the results of the two filtering modules Most of the network attacks are from IP packets.

In addition to checking for the source IP address and destination port of all packets in hardware, indentifying packets involves inspecting two other header fields (refer to Table 1). Besides, to parse the source IP addresses or ports from the packets, the parse control of src_ip_parse and ports_parse must be inserted to the preprocess_control module. For the design of the source ip addresses and ports filtering list, untrusted_ip_Addr_table and vulnerability_port_table are designed in the registers bank to cooperate with packets filtering modules based source IP Address and port.

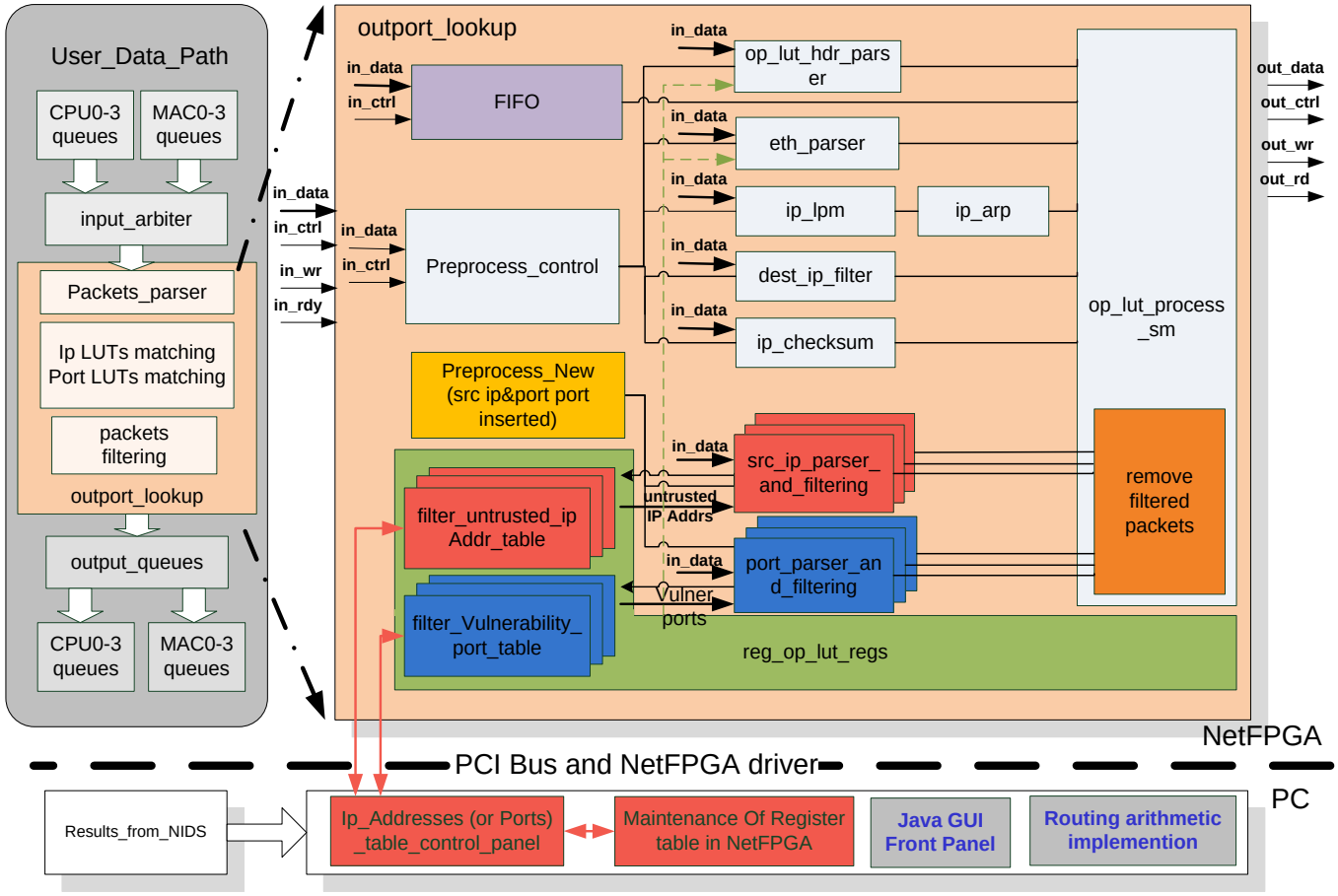

Figure 2. Modules layout of the fast packet filtering in hardware and control panel of the hardware firewall

Table 1. NetFPGA word alignment for network packets. Fields shaded in green and orange are inspected for packet filtering [9].

	User Data Path (in_data) Register Bits			
Words	63:48	47:32	31:16	15:0
1	eth dst add			eth sa hi
2	eth sa lo		type	ver,ihl,tos
3	total length	id	flags,fof	tll,proto
4	checksum	src ip		dst ip hi
5	dsp ip lo	src_port	dst port	len
6	TCP/UDP cksum	DATA		
7	DATA			
...				

After the two modules of packet filtering and the remove filtered packets module design finished, we add the definition of wire connections of the three new modules to other modules and filtering lists. Finally, we design a new control panel and program on the CentOS system to receive the results from NIDS and control the filtering lists of the hardware.

3.2.3 Embedded NIDS

We implement a Network Intrusion Detection System (NDIS) upon XUPV5-LX110T board. Its general content as shown both in figure 3 and below:

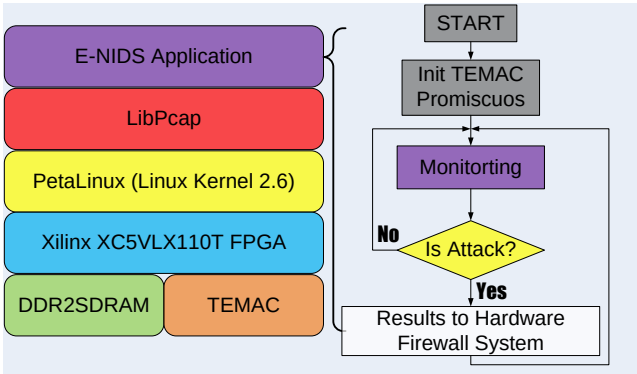

Figure 3. General Layout of Embedded NIDS

1. PetaLinux on XUPV5-LX110T board.
2. LibPcap library migration.
3. TEMAC driver with Promiscuous Option.
4. MII 10BaseT Half Duplex Mode supported in Linux Kernel 2.6.
5. Pattern Matching Algorithm with hardware acceleration.

The Embedded NIDS captures packets on the firewall, analyzed their content field in BMP pattern matching algorithm with hardware acceleration. After these two steps, NIDS gets the result of these packets under detection whether they are harmful or not, and then tells the firewall to deal with the result.

4. REMOTE RECONFIGURATION

As mentioned earlier, most parts of this system are implemented in hardware to enhance its performance and security. Indeed, for security protection system, the hardware one can be much more secure and faster than the software one. But the flexibility of the hardware one is much lower. Once new security threats outbreak, to further keep the performance, security and flexibility of our system, the hardware and software systems should be updated as soon as possible by our remote reconfiguration mechanism.

To implement the remote reconfiguration, we give top priority on security issues. Two-Way Authentication protocol is added to ensure the security of the remote reconfiguration. Only the authentication passed, the remote reconfiguration can be started via any authorized devices (such as computers and phones). Fig.5 shows the remote reconfiguration for the two subsystems.

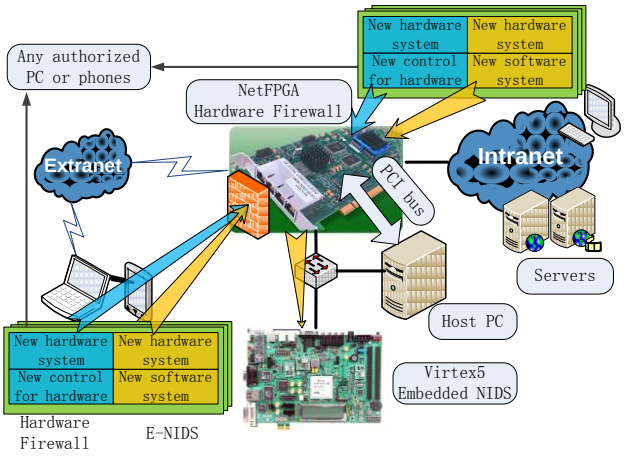

Figure 5. Remote Reconfiguration Design for the Subsystems

For the two subsystems, the device of translating the configure files and the download controlling are quite different. There is no flash chip to reserve the configure data of NetFPGA, so the configure file of NetFPGA in remote devices can be transmitted and translated on the host PC, then downloaded to NetFPGA under the controlling of the Host PC. While for the NIDS, the new configure files can be transmitted to the NIDS and then these configure files must be translated to data flow that can be downloaded to the flash chip directly by the NIDS itself. Besides, the downloading of the data flow is also under the controlling of itself.

5. TEST and ANALYSIS

The basic functionality is tested by running the denial of service and SQL injection on a PC in extranet to attack the two servers in the intranet that is under the protection of our security protection system. In the two servers, we have built our own Web Service with PHP and XML for test. In practice, 97.3% of the packets are detected in the embedded NIDS. 100% packets of the detected attacks can be filtered. The detected results from the NIDS appear in the maintenance of the filtering tables in hardware. At the same time, all the packets form the untrusted IP addresses or to the vulnerability ports have been filtered effectively.

In order to verify the correctness of the remote reconfiguration mechanism, we design a few new hardware circuits and new software systems for each subsystem. The experiments show that our remote reconfiguration mechanism is valid.

6. FUTURE WORK

As referred earlier, it is inconvenient because most information about attacks of our hardware firewall depend on the extra Network Intrusion Detection System (NIDS). If an embedded NIDS with hardware acceleration can be added into NetFPGA and coprocess with our hardware firewall subsystem, the performance and security will be greatly improved.

To ensure whether there is a feasible solution to add a NIDS into NetFPGA, many intensive studies have been done, including check the resources of the NetFPGA board and account the device utilization for our reconfigurable hardware firewall. The studies concluded that adding an embedded NIDS in our network security subsystem is feasible.

There are two IBM PowerPC hard-core in the FPGA chip which is on NetFPGA (Xilinx Virtex 2 Pro50). In addition to that embedded PowerPCs, there is a 64M Byte two second-generation Double Date Rate (DDR2) SDRAM and two 18 Mb SRAMs [10]. We can use these resources to build an embedded system to run the NIDS.

If this work can be done, the architecture of the new network security protection system will consists of hard-core processors and reconfigurable logic elements. Most of the Logic Element will be used by the reconfigurable hardware firewall to deal with packet filtering in hardware, immunity against ARP attacks in hardware, traffic monitoring with hardware acceleration and coping all of the packets to the other part. Meanwhile the hard-core processors and the remains of the logic elements and storage chips will be used to build an embedded system to implement the NIDS. Most parts of the NIDS are implemented in software, receive the copied packets from the hardware firewall, and then transmit the detection results back to the firewall.

There are many great advantages in this architecture, such as better performance, much more security and flexibility, more optimized hardware and software co-processing. Moreover, because all the data transmission is on-chip transmission, the performance and reliability will be improved greatly

7. CONCLUSION

The reconfigurable security protection system is a complete solution for system security. In the implementation, packet filtering in hardware, immunity against ARP attacks in hardware, flow monitoring and transmitting with hardware acceleration, BMP pattern matching modules with hardware acceleration enhance the performance and security of this protection system. Moreover, the performance and reliability can be further enhanced greatly by remote reconfiguration. The Administrator can update the two subsystems via any authorized devices whenever to deal with the known and unknown security threats.

Extensive experiments show that all the functions of the designed blocks are valid and the designed system is feasible. However, our work is just preliminary, for the reliability of the system, security in the remote reconfiguration still need to be improved.

8. REFERENCES

[1] Mogul and C. Jeffery. 1989. Simple and Flexible Datagram Access Controls for Unix-based Gateways. In *USENIX Conference Proceedings*, 203-221.

[2] H. Salehi, H. Shirazi and R.A. Moghadam. 2009. Increasing overall network security by integrating Signature-Based NIDS with Packet Filtering Firewall. *IEEE International Joint Conference on Artificial Intelligence* (Dec. 2009), 357 - 362.

[3] D. Laturnas and R. Bolton. 2005. Dynamic Silicon Firewall. In *Electrical and Computer Engineering* (May 2005), 304-307

[4] G. Estrin. 2002. Reconfigurable computer origins: the UCLA fixed-plus-variable (F+V) structure computer. *IEEE Annals of the History of Computing*. Volume 24, Issue 4 (Oct. 2002), 3–9. DOI= http://dx.doi.org/10.1109/MAHC.2002.1114865

[5] G. Estrin. 1960. Organization of Computer Systems—The Fixed Plus Variable Structure Computer," *Proc. Western Joint Computer Conf., Western Joint Computer Conference*, New York, 33–40

[6] T.J. Todman, G.A. Constantinides, S.J.E. Wilton, O. Mencer, W. Luk and P.Y.K. Cheung. 2005. Reconfigurable Computing: Architectures and Design Methods, *IEE Proceedings: Computer & Digital Techniques* (March 2005), Vol. 152, No. 2, 193–208.

[7] G.A. Covington, G. Gibb, J. Naous, J.W. Lockwood and N. McKeown. 2009. Encouraging Reusable Network Hardware Design", In *IEEE International Conference on Microelectronic Systems Education* (Sep. 2009), 29-32

[8] M. Ciesla and V. Sivaraman. 2009. URL Extraction on the NetFPGA Reference Router. Developers Workshop (Aug. 2009), 39-44

[9] G. Gibb, J.W. Lockwood, J. Naous, P. Hartke and N. McKeown. 2007. NetFPGA – An Open Platform for Teaching How to Build Gigabit-rate Network Switches and Routers, In *IEEE International Conference on Microelectronic Systems Education* (Jun. 2007), 160-161