ICIC Express Letters
Part B: Applications
Volume **1**, Number **1**, September **2010**
 ISSN 2185-2766
pp. **71–76**

IMPLEMENTATION OF FPGA CARD IN CONTENT FILTERING SOLUTIONS FOR SECURING COMPUTER NETWORKS

Youngran Hong[1] and Dongsoo Kim[2,*]

[1]Research Management Office, SOMANSA Co., Ltd.
[1,2]Department of Industrial and Information Systems Engineering
Soongsil University
511 Sangdo-Dong, Dongjak-Gu, Seoul, Korea
yrhong@somansa.com
*Corresponding author: dskim@ssu.ac.kr

Received May 2010; accepted July 2010

Abstract. *The organizations in network-advanced countries confront the problem in real-time data processing because the processing capacity in IT security solutions is under 300 Mbps but network traffic is over 1 Gbps. Up to now, most IT security solutions have been implemented as software type, but they are not considered as an appropriate alternative of processing packets in the mass traffic anymore. Especially, though IT security solutions should catch all the packets on the network, they may lose some important packets related with data security for their software type. This phenomenon results in the low reliability in data security. Recently, FPGA (Field Programmable Gate Array) cards have been emerged as an alternative in this area. The FPGA, which has been used in the semiconductor manufacturing industry, is used in IT security domain due to low production costs and high performance of data processing in mass traffic. This paper presents a hardware type implementation using FPGA in the content filtering solution to treat mass packets. Also, the result of experiment in the proposed system is introduced. The results are that the performance of the processing packets of this new method is much faster than that of the software type in almost three times.*
Keywords: FPGA card, Content filtering, Mass packets, IT security

1. **Introduction.** As the speed of network has become faster than ever before, it is necessary to support the mass traffic (almost 1 Gbps) capacity for data processing in IT solution industry. Especially, because IT security solution analyzes the packets for protecting data from being leaked and avoiding security threats [8], it is important to treat packets in the mass traffic environment. In this paper, we focus on content filtering solutions in comparing the rate of losing packets between software type and hardware type solution. As a content filtering solution monitors the inbound packets through the network and blocks the malware or useless web URLs by shooting the reset packets based on the rules or the policies, it is very important not to lose packets and to analyze them correctly and timely.

Up to recently, most of the content filtering solutions have been implemented as software. Generally, it is good to develop content filtering solutions as software, because it is easy to design and implement. However, the software type has some problems in the business, nowadays. First of all, they have a limitation in their ability of processing mass packets on the fast network. They can treat packets till 300 Mbps to the maximum. If the software type is adopted on the 1 Gbps traffic devices, the packet loss rate would be over 60%. Although the content filtering solutions have to prevent the internal data from being leaked in the way of connecting with the malware, the software type does not have enough capacity to process mass packets. If the solution can protect and block

suspicious web URLs in advance, it can secure the internal server stability and reduce the IT infrastructure costs like a burden of the web firewall.

With these backgrounds, it is necessary to implement the best applications which use the various and abundant resource of software by processing mass packets in real-time. The stable hardware such as FPGA (Field Programmable Gate Array) card can be one of them. In this research, we present FPGA card adopted in a content filtering solution to overcome the problems of the software type in packet filtering. In addition, we evaluated the performance of this new method. We compared the performances of processing mass packets by using software type and FPGA card. It has been proved that the FPGA card can solve the limitations of the software type solution including packet loss problem.

2. **Related Work.** FPGA is an array technology by which an engineer can implement the circuit in the semiconductor chip. It can be designed and implemented by programming the device directly in the industrial field without requesting it to the semiconductor manufacturing companies [3]. The gate array is a kind of ASIC (Application Specific Integrated Circuit) device. Accordingly, the internal structure of the FPGA is similar to the ASIC gate array. Once the FPGA is fixed in the design, it can be produced as permanent chips loaded in the permanent electric circuits [1].

Today's FPGAs have evolved far beyond the basic capabilities presented in their predecessors, and they incorporate hard (ASIC type) blocks of commonly used functionality such as RAM, clock management and DSP. Following are the basic components of an FPGA [6]. Configurable Logic Block (CLBs) is the basic logic unit in an FPGA. Interconnect is the second basic component. While the CLB provides the logic capability, flexible interconnect routing routes the signals between CLBs and to and from I/Os. Select I/O (IOBs) is the third basic component. I/O in FPGAs is grouped in banks, which are independently able to support different I/O standards. The forth component is Memory. Embedded Block RAM memory is available in FPGAs. The fifth is Complete Clock Management. Digital clock management is provided by most FPGAs in the industry.

Due to their programmable nature, FPGAs are an ideal fit for many industries: aerospace & defense, automotive, broadcast, consumer, industrial/scientific/medical, storage & server, wireless communications and wired communications and so on [6]. This paper focuses on the storage & server industry, especially the data processing solutions for the Network Attached Storage (NAS), Storage Area Network (SAN), servers and storage appliances [5]. The FPGA is being adopted in order to achieve the high performance and low costs in the storage & server part.

Looking into Figure 1, we can understand how to achieve the high performance and how to reduce the costs by implementing the FPGA in the content filtering solution. The software type content filtering solution is dependent on the servers and the programming languages in the processing packets and in logging data I/O. However, once it is implemented in the FPGA card, the packet processing problems such as hang-data and I/O data packet loss can be solved, for it can guarantee processing mass packet stably up to the implemented chip-typed capacity as a processing packet form [2].

Content filtering is a technique whereby contents are blocked or allowed based on the results of content analysis, rather than the source or other criteria. It is widely used to filter e-mails and web accesses on the Internet [3]. In this paper, we focus on the web access part. Content filtering solutions are usually used to prevent computer users from viewing inappropriate web sites or contents in organizations such as offices and schools, or they can be used as a pre-emptive security measure to prevent access to known malware hosts. Filtering rules are typically set by a central IT department and may be implemented via software on individual computers or at a central point on the network such as a proxy server or an Internet router. Depending on the sophistication of the system used, it may be possible for different computer users to have different levels of the Internet access [9].

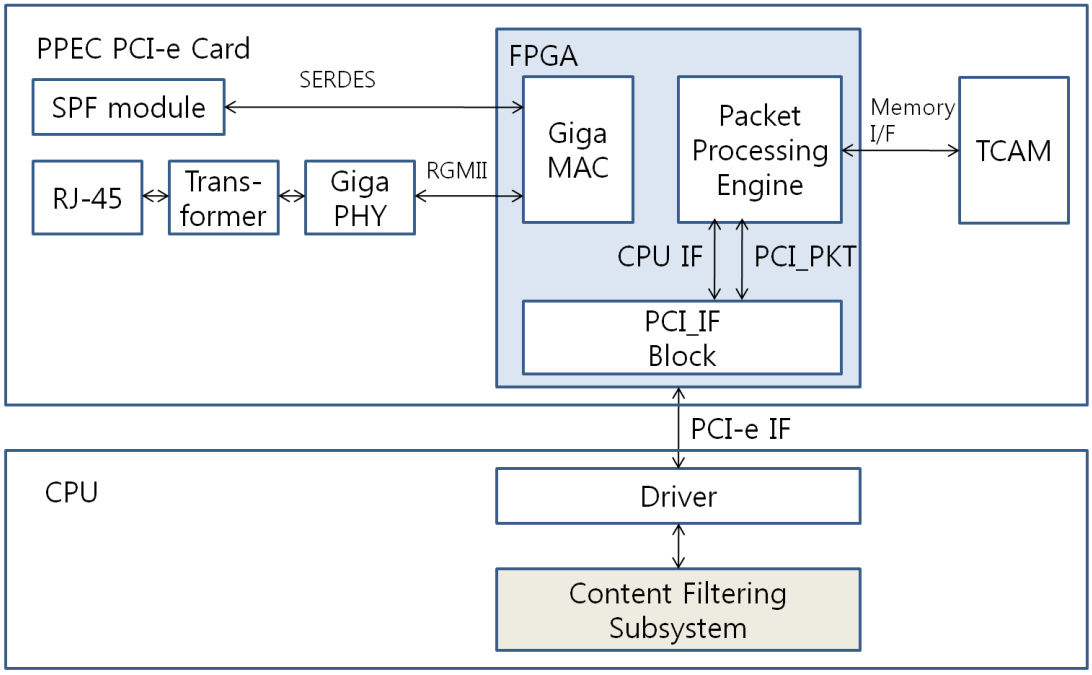

FIGURE 1. Block diagram of FPGA in content filtering solution

Common content filtering methods include the following techniques. Attachment method blocks certain types of files (e.g. executable programs). Bayesian, char-set, content encoding, heuristic method is a filtering based on heuristic scoring of the content according to multiple criteria and it depends on the contextual technology. HTML anomalies, language, mail header method is a filtering based solely on the analysis of e-mail headers, but it is less effective due to the ease of message header forgery. Mailing list method is used to detect mailing list messages and file them in appropriate folders. Phrases method is a filtering based on detecting phrases in the content text. Proximity method is a filtering based on detecting words or phrases when used in proximity, but it has high rate of false positive errors. Regular expression method is a filtering based on rules written as regular expressions. URL method is a filtering based on the URL and suitable for blocking websites or sections of websites. Most content filtering solutions combines of these techniques [1].

Among the common content filtering methods, most of the software type solutions are based on the URL based filtering method, and they are used in the B2B markets. These solutions monitor the internal employees' web access in the network level. Therefore, it is classified as a network security system.

3. **Architecture and Implementation of FPGA Card.** This section presents the architecture of the FPGA card and content filtering solution implemented based on the FPGA card.

The FPGA card contains some functions of software type security solutions as a hardware chip-type solution and it is loaded onto the server as shown in Figure 1. We can see the interaction between a PCI-e Card (a kind of FPGA card) and a CPU. This has been designed in order to increase the availability of the CPU. It is noteworthy to adopt Giga MAC to deal with the Packet Processing Engine. The driver in the CPU is used for the high performance with the purpose of reducing the burden in general CPU. In the case that the high performance driver is used for processing mass packets in software type, the software engine is stopped because of the hang packets in the CPU [4].

Figure 2 shows the logical diagram designed as IS 2320/2321 in the FPGA card, Port and Channel. In the IS 2320/2321, the number of ports of a card is 2(0, 1), while that

of the channel is 1(0, 0). We can design the same logic diagram according to the IS 2420/2421, which has 1 port (0, 0) and two channels (0, 1) for the duplex configuration [4,7].

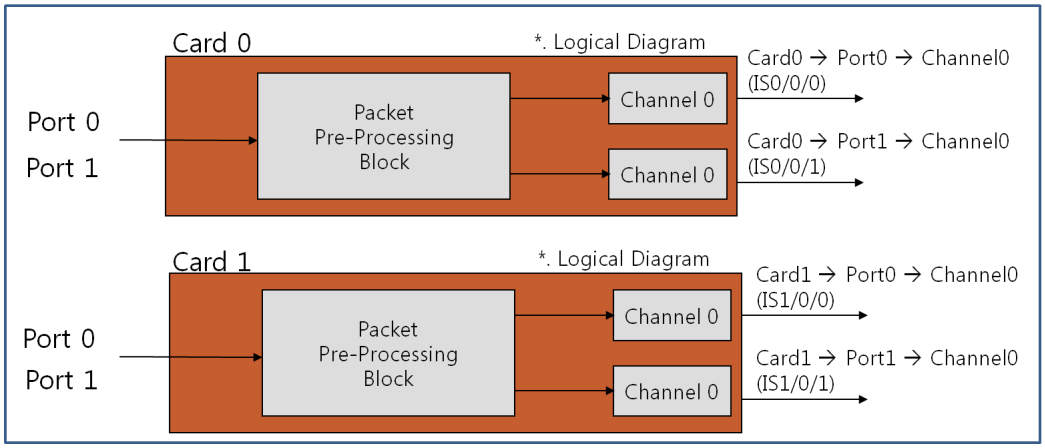

FIGURE 2. Logical diagram in FPGA for processing packets in IS 2320/2321

Figure 3 shows how the FPGA card processes the mass packets. In the software type solution, all the input packets are transferred to the content filtering engine on the HOST computer by the general Network Interface Card (NIC). It triggers the full-buffering and results in the packets dropped. Consequently, the resource is being consumed for handling packets in O/S. However, in the FPGA card, the input packets are processed in the card in advance, and the selected meaningful packets are transferred to the engine. It is a DMA (Direct Memory Access) method, and therefore it can process packets in real-time instead of handling packets in O/S [9].

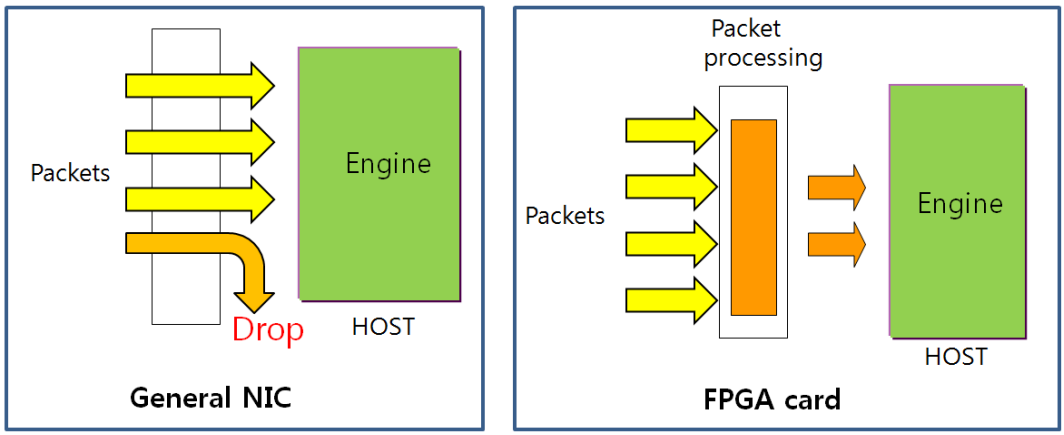

FIGURE 3. Comparison of NIC and FPGA card packet processing method

4. **Performance Evaluation.** In order to evaluate the performance of the proposed method, we established a test environment. SQL server is used for logging the database. The specification of the used system is Xeon Quad 2 GHz × 2, 4 GB RAM, 150 GB 5400 rpm HDD. Under this environment, the packets have been pumped and input to the FPGA card. The packet input ranges 100 Mbps ∼ 1 Gbps.

Figure 4 shows the flow of the packet processing through the FPGA Card [4]. The FPGA card is covering all the packet processing procedures from the TCP filtering to the content type filtering. It is necessary to make only the content filtering engine being a FPGA card, for there are irregular patterns or newly generated URL should be updated frequently in the content filtering solutions.

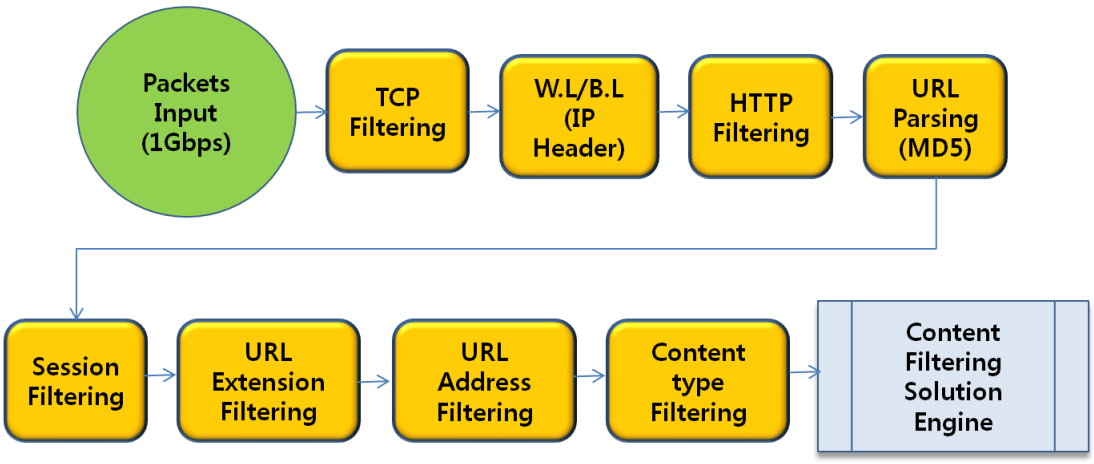

FIGURE 4. Flow of packet filtering processed by FPGA

Figure 5 shows the results of the performance evaluation. The FPGA card proposed in this paper does not show any packet loss whereas general NIC starts its packet loss from 300 Mbps. Also, our method shows low CPU usage rate compared with the general NIC. The results of this experiment show that the FPGA card can be used as an alternative for solving the packet loss problem in mass traffic network.

However, there are some limitations of this study in applying the results to the real network service environment. First of all, the test environment depends on the simple content filtering engine. If the packet processing engine can be implemented more complicatedly, for example, if it supports not only dealing with the URL method but also Heuristic or Proximity method, the usage rates in CPU and memory would be increased.

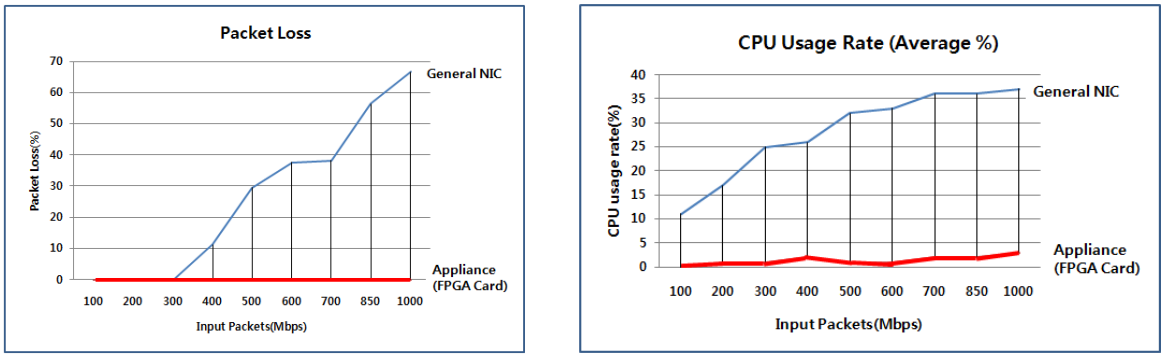

FIGURE 5. Result of performance evaluation

5. **Conclusions.** We implemented the FPGA card for improving the performance of processing packets on the mass traffic network like 1 Gbps. As the results of performance evaluation showed, we conclude that the FPGA card should be blended into the content filtering solutions to overcome the limitations of software type security solutions. We believe that it is meaningful to propose an alternative such as the FPGA card based hardware-centric implementation method in order to solve the mass traffic problems in the ubiquitous networked society.

The range of the implementation in this experience was limited to the filtering engine for processing packets in the content filtering solutions. In the future, this kind of FPGA implementation is expected to be adopted in the other IT security parts such as email filtering and DB access control area in order to make the packet and data processing speed higher and more efficient.

REFERENCES

[1] *http://www.xilinx.com/.*
[2] J. Luo, J. B. Bernstein, J. A. Tuchman, H. Huang, K.-J. Chung and A. L. Wilson, A high performance radiation-hard field programmable analog array, *Proc. of the 5th International Symposium on Quality Electronic Design*, pp.522-527, 2004.
[3] *http://en.wikipedia.org/wiki/Field-programmable_gate_array.*
[4] I. Choi, Development of network based content security & data leakage prevention solution in BcN network, *IITA*, pp.33-45, 2008.
[5] K. Sridharan and P. R. Kumar, *Robotic Exploration and Landmark Determination: Hardware-efficient Algorithms and FPGA Implementations*, Springer, 2008.
[6] P. P. Chu, *FPGA Prototyping by Verilog Examples: Xilinx Spartan-3 Version*, Wiley-Interscience, 2008.
[7] C. Maxfield, *FPGAs: Instant Access*, Newnes, 2008.
[8] J. Ye, B. Fang, Y. Zhang and Z. Tian, A quantitative method for evaluating the security threats of grid system to tasks, *International Journal of Innovative Computing, Information and Control*, vol.5, no.4, pp.1125-1136, 2009.
[9] D. Shin and H. Yang, Design and implementation of an intrusion detection system based on outflow traffic analysis, *Journal of Korea Contents Association*, vol.9, no.4, pp.131-141, 2004.