Packet Filtering Circuits for Smart Phones

Tomoaki SATO
C&C Systems Center, Hirosaki University
Hirosaki 036-8561 Japan

Phichet MOUNGNOUL
Faculty of Engineering, King Mongkut's Institute of Technology Ladkrabang
Bangkok 10520 Thailand

and

Masa-aki FUKASE
Graduate School of Science and Technology, Hirosaki University
Hirosaki 036-8561 Japan

ABSTRACT

Security measures for smart phones are important. Anti-virus software for smart phones can be used and the process consumes CPU resources. The CPUs of them are powerless CPU for an embedded system and those operations consume battery power. In this paper, the authors propose packet filtering circuits for smart phones. The packet filtering circuits are a firewall. Using the firewall is a means to protect smart phones from computer viruses and unauthorized access. In addition, they are used to control the power consumption and to reduce of detecting units for unauthorized access. The features of the circuits are to achieve those functions without reconstructing circuits. The operations of the circuits are verified by gate-level simulations.

Keywords: Packet Filtering, Firewall, Mobile Devices, Smart phones, Network Security

1. INTRODUCTION

The number of users of smart phones increases rapidly. The smart phones use iOS or Android OS based on UNIX. They enables sending and receiving of a large size file and accessing a web page that has been created for viewing on a PC. Additionally, the users input personal information such as telephone numbers and contents of a mail to them. These mean that security countermeasures of smart phone users are more important than that of PC users.

In case of Android phones, computer viruses have already been generated. We must take preventive measures against the computer viruses. Anti-virus software for Android phones can be used and the process consumes CPU resources. The CPUs of them are powerless CPU for an embedded system and those operations consume battery power. Therefore, detection capability with anti-virus software for Android phones is not enough. A firewall is used to protect computer operations from computer virus and unauthorized computer access. In general, a host-based firewall is implemented in software. The processing of the host-based firewall consumes CPU power. To use it in the smart phones is not appropriate.

On the other hand, Reconfigurable Firewall Unit [1] had been developed. Its future is that the processing doesn't need the CPU. It had been implemented in logical basis on an FPGA (Field-Programmable Gate Array) and the operations of it are very efficient. However, the circuits for firewall processing must be provided for each application of network computing. It means the combination of infinity.

In this paper, the authors propose packet filtering algorithm that can be used sustainably without having to rewrite the circuit information. The circuits for packet

filtering algorithm can be achieved with a custom design LSI. In general, FPGA circuits consume power than the circuits of custom design LSI and the operations of custom design LSI are faster than that of FPGA.

This paper is organized as follows. Section 2 presents the outlines of firewall and packet filtering circuits. Then, Section 3 describes development of the filtering circuit. In Section 4, the conclusions are made.

2. FIREWALL AND PACKET FILTERLING CIRCUITS

A. Firewall Circuits

Firewall circuits [1]-[3] are logic-based firewall and constructed with reconfigurable circuits. The example that uses reconfigurable circuits is [4]. The outline of them is shown in Figure 1. The controlled ports are for using a mobile computing, and they are at least needed. Table I is the controlled ports. Because the firewall unit is developed by FPGA, the change of ports is very easy.

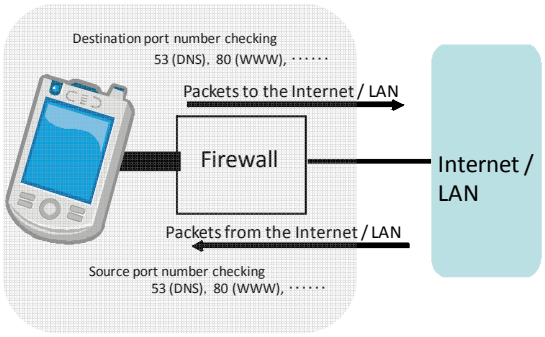


Figure 1. Firewall for H-HIPS.

TABLE I

CONTROLLED PORTS

Function	Port Number	Binary
NOP	0	0000000000000000
SMTP	25	0000000000011001
DNS	53	0000000000110101
HTTP	80	0000000001010000
POP3	110	0000000001101110
HTTPS	443	0000000110111011

Figure 2 shows synthesized circuits by using Altera Cyclone EP1C20F400C7 which is an FPGA. Maximum delay time of the circuits is 17.9 ns. The circuits can operate at 50 MHz by conventional operations. And, Minimum delay time is 12.3 ns. They can operate at 100MHz by wave-pipelined operations [5]-[7]. The gate-level simulations confirm wave-pipelined operations.

The weak points of firewall circuits are as follows.

- When changing of the firewall composition, it is necessary to synthesize the circuits again.
- The circuits need an FPGA.

Therefore, they cannot use in custom-designed LSI.

B. Filtering Circuits

To improve the weak points of firewall circuits, filtering circuits are proposed. The processing procedure of packet filtering algorithm is shown figure 3 and as follows.

- When the smart phone has made a communication request to a server computer, the source port number

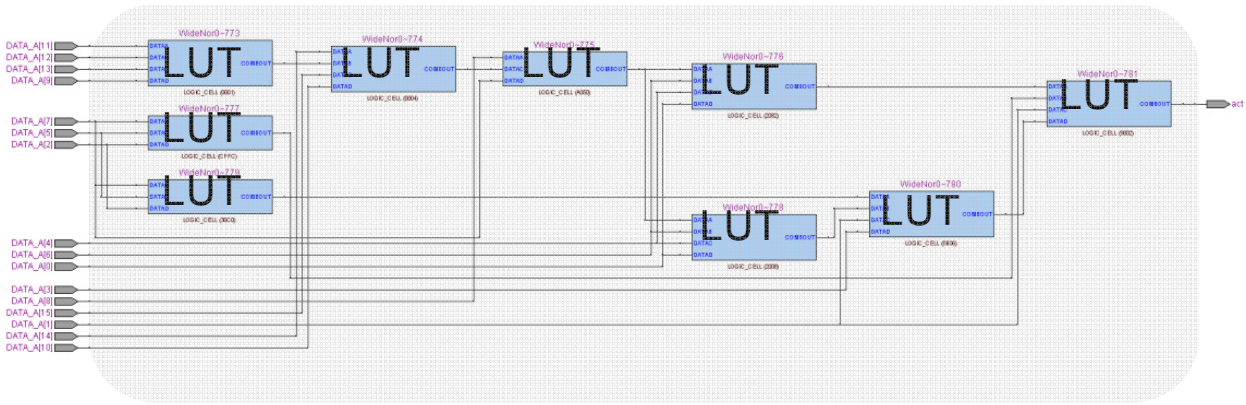


Figure 2. Firewall Unit.

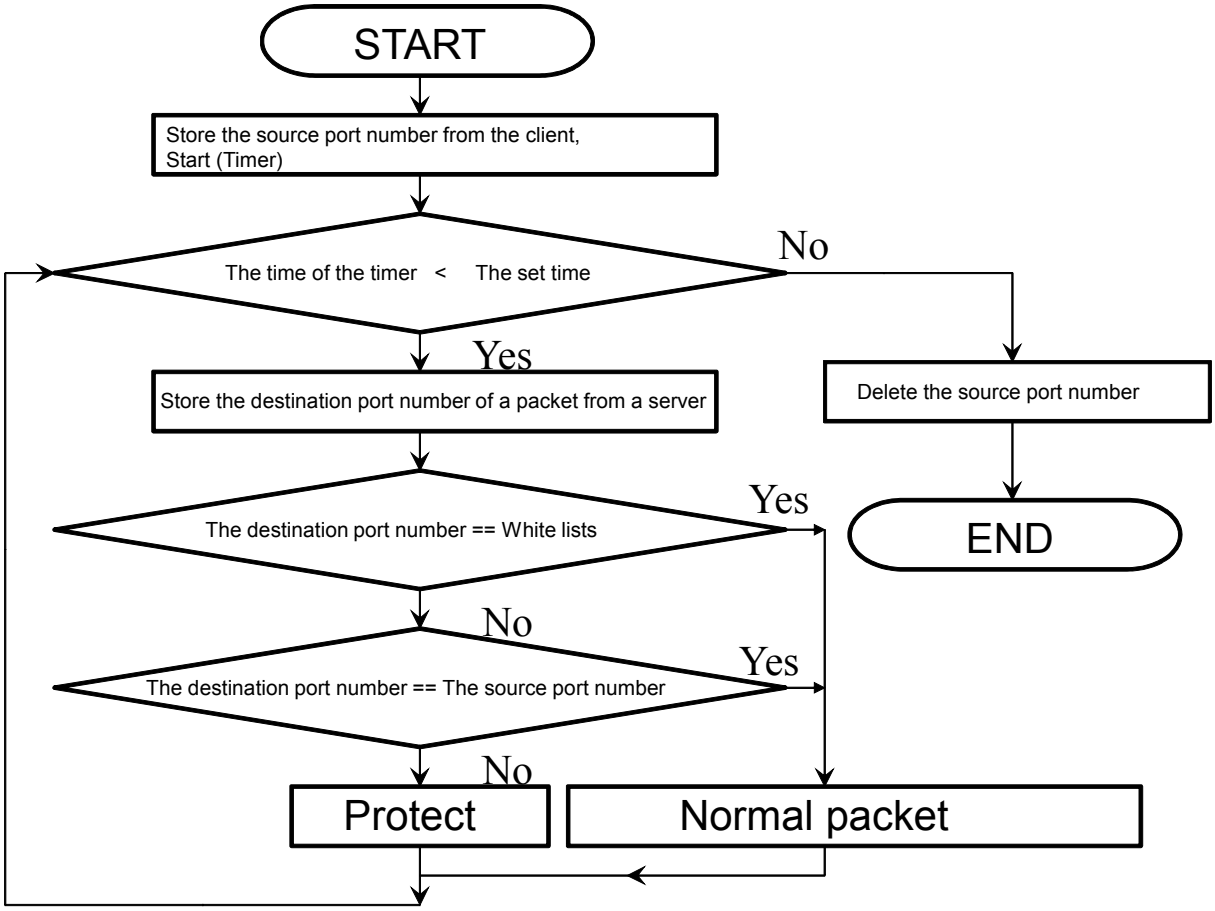


Figure 3. Packet Filtering Algorithm

of the TCP header of the packet is stored.

- The time of the packet is record.
- When the smart phone receive a packet, the destination port number of the packet is stored.
- The source port number is matched against the destination port number.

If the source port number and the destination port number are matched, it is judged that the packet to the smart phone is normal communications. Excluding a normal packet is discarded. In addition, when a certain period of time has elapsed from the recorded time, some packets are discarded.

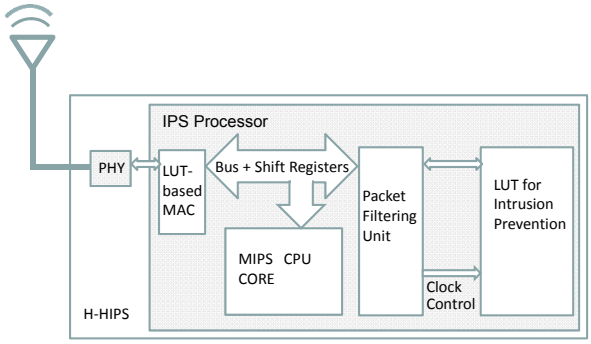


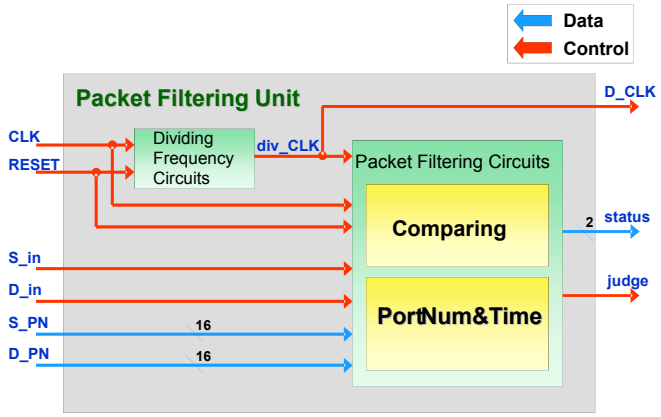
Figure 4. H-HIPS with Packet Filtering Unit.

On the other hand, the authors have developed H-HIPS (Hardware- and Host-based Intrusion Prevention System) [8]. H-HIPS is shown in Figure 4. The target of the system

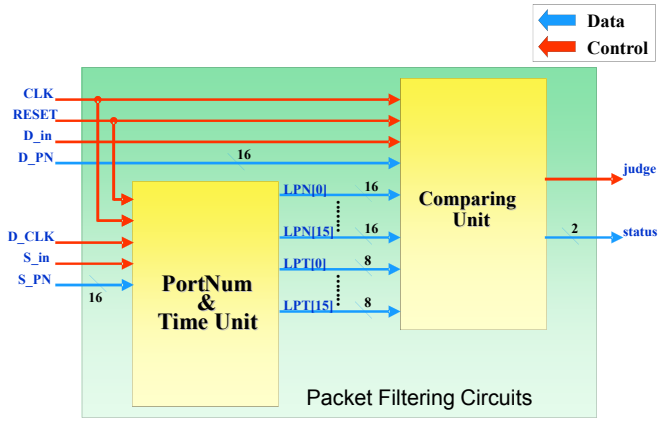
is smart phones and mobile PCs. It has been implemented on an FPGA, and its detection units have been achieved by logic circuits that can be reconfiguration. The system needs a firewall function. The firewall function is indispensable for not only the function of firewall but also the reduction of power consumption and detection units. The packet filtering circuits on the FPGA can be applied to H-HIPS for these reasons.

3. DEVELOPMENT AND VERIFICATIONS OF CIRCUITS

To verify packet filtering algorithm, the authors implement packet filtering algorithm to an FPGA. The FPGA is Cyclone of Altera. The hardware structure is shown in Figure 5.



(a)



(b)

Figure 5. The Hardware Structure of Packet Filtering Unit. (a) Packet Filtering Unit. (b) Packet Filtering Circuits.

The circuits of packet filtering algorithm are simulated by gate-level simulations. The simulations are shown in Figure 6. As a result, the operations of 100MHz are confirmed. Because it is easy to verify the actual behavior, we chose the FPGA. The circuits don't have a peculiar function to an FPGA.

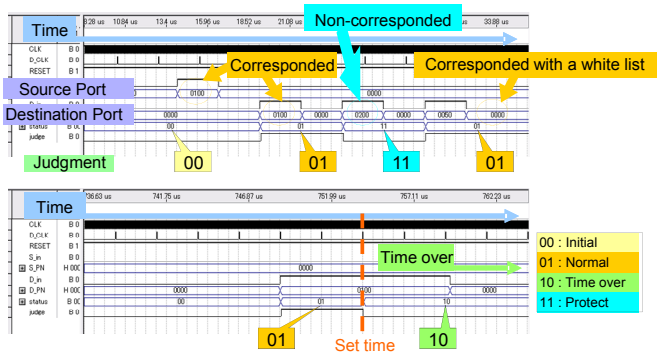


Figure 6. Simulation Results

4. CONCLUDING REMARKS

In this paper, the authors proposed packet filtering algorithm for smart phones. Then, the algorithm was implemented to an FPGA and operations of the algorithm were confirmed by gate-level simulations. According to the results, 100 MHz operations were shown. Future works are an evaluation by the measurement of the FPGA and a verification of the packet level.

ACKNOWLEDGMENT

This work has been supported in part by Grant-in-Aid for Young Scientists (B) (23700068) from Japan Society for the Promotion of Science (JSPS), Japan.

REFERENCES

[1] Tomoaki Sato, Phichet Moungnoul, and Masa-aki Fukase, "Delay Time Analysis of Reconfigurable Firewall Unit," Proc. of the 4th International Multi-Conference on

Engineering and Technological Innovation, Vol. II, pp. 109-114, 2011.
[2]Tomoaki Sato, Syuya Imaruoka, and Masa-aki Fukase, “ReconFigureurable Firewall Unit by Wave-Pipelined Operations,” proc. of ISPACS 2008, pp. 449-452, 2009.
[3] Tomoaki Sato, Kei Ito, Keisuke Saito, Phichet Moungnoul and Masa-aki Fukase, "Development of a shift register for Firewall Circuits by Wave-Pipelined Operations," Proc. of 2010 International Workshop on Information Communication Technology, pp. w4c-1-1-w4c-1-4, 2010.
[4] David V. Schuehler and John W. Lockwood, “TCP Splitter: A TCP/IP Flow Monitor in Reconfigureurable Hardware,” IEEE Micro, Vol. 23, No. 1, pp. 54-59, 2003.
[5] L. Cotton, “Maximum rate pipelining systems,” Procs. AFIPS Spring Joint Computer Conference, pp. 581-586, 1969.
[6] F. Klass and M. J. Flynn, “COMPARATIVE STUDIES OF PIPELINED CIRCUITS,” Stanford University Technical Report, No. CSL-TR-93-579, July 1993.
[7] W. P. Burleson, M. Ciesielski, F. Klass, and W. Liu, “Wave-Pipelining: A Tutorial and Research Survey,” IEEE Trans. on Very Large Scale Integration (VLSI) Systems, Vol. 6, No. 3, pp. 464-474, Sept. 1998.
[8] Tomoaki Sato, Syuya Imaruoka, and Masa-aki Fukase, "Hardware-Based IPS for Embedded Systems," Proc. of WMSCI 2009, Proc. of WMSCI 2009 ol. III, pp. 74-79, 2009.
[9] Keisuke Sito, Shuya Imaruoka, Tomoaki Sato, and Masa-aki Fukase, “Evaluation of Packet Filtering Unit,” Proc. of FIT 2009, Vol. 8, No. 4, pp. 129-130, 2009.