System Design of Network Data classification Based on Deep Packet Inspection

Qi Lu¹, Jiadong Lin¹, Zhou Su¹ and Fei Liu¹*

¹ Radar NCO School, Air Force Early Warning Academy, Wuhan, Hubei, 430345, China

*Corresponding author’s e-mail: kjjjxyzgc@163.com

Abstract. With the rapid development of the Internet, as an important method of network security protection, network data classification has become the focus of high-tech research. In order to efficiently process massive network data, filter irrelevant data packets, and resist malicious attacks, so as to ensure the safety and stability of network operating, based on the research of deep packet inspection (DPI) technology, a kind of network data classification system has been presented. This system is based on the architecture of field-programmable gate array (FPGA) and ternary content addressable memory (TCAM). Tests show that the system can meet actual requirements of network data classification.

1. Introduction

From 1969 to 2020, after half a century of rapid development, new Internet application services emerged, such as online shopping, online food delivery, travel booking, Internet financial management, online payment, online live broadcast, online car-hailing and online education. The Internet has become an indispensable part of human society. According to "The 45th China Statistical Report on Internet Development Status" released by the China Internet Network Information Centre (abbreviated as CNNIC) in April 2020, as of March 2020, the number of Internet users in my country reached 904 million [1]. From January to December 2019, mobile Internet access traffic consumption reached 122.0GB, a year-on-year increase of 71.6%. However, the openness of the Internet allows any device that conforms to the Internet network specifications to be allowed to access the Internet, which brings unprecedented challenges to network data security and management. This article introduces the design and implementation of a high-speed network data classification system, through which the system can complete the in-depth identification of high-speed network packets and provide a basis for data classification, thereby alleviating the processing pressure of back-end equipment, improving processing efficiency, and improving the network status. Monitoring and management provide guarantees to ensure network security.

2. Hardware platform design of the system

In view of the substantial increase in the transmission rate of the backbone network, a more efficient interconnection technology that not only meets the current network conditions but also faces the future development is required. The architecture of high-speed network signal deep processing platform should be scalable, high-density, and easy-to-build. The performance can realize the rapid upgrade of the overall system platform, and timely adapt to the changes of real physical conditions, so as to ensure that the in-depth processing efficiency can be maintained for a certain period of time even in the case of high load efficiency.
This paper designs a network data classification system based on DPI technology for the traceability of food safety. When processing data packets, it is necessary to filter not only data packets that meet the corresponding 5-tuple conditions, that is, source IP address, destination IP address, source port, destination port, protocol number, but also data packets that meet the corresponding application layer information (such as food type, production time). The design of the data classification system adopts the FPGA+TCAM architecture. The functions of the system should include signal collection and acquisition, signal processing, signal storage, etc., and due to the large number of users of the food safety traceability system, the designed classification system should be able to meet the requirements of high speed and large capacity network signal access and processing needs. Based on the above functions and requirements, this hardware system is divided into five modules: high-speed network signal access module, core processing module, data cache module, hardware matching module, and online management module. Figure 1 shows the overall design of the system.

2.1. High-speed network signal access module
The access module receives the optical signal of the external network channel, converts it into an electrical signal, and restores it to the original frame data after synchronization and descrambling. In order to ensure the requirements of high-speed processing, the output rate of this module must reach the 1Gbps-level and limit the packet loss rate as much as possible.

The optical network receiving module is the source of the system to analyse and process signals, and its compatibility, stability, and bit error rate will have a significant impact on the processing results. The current single-wave mainstream transmission rate of optical fibre backbone networks is at least 10Gbps, so the designed system platform should be able to meet the access of network signals at a rate of 10Gbps. Considering that SFP+ can guarantee 10Gbps communication capacity and meet forward and backward compatibility, and achieve low-cost and high-density integration of hardware modules, it is currently considered an ideal solution for 10G transmission optical transceivers. Therefore, the system optical module adopts the standard SFP+ receiving module, which can not only receive high-speed signals smoothly, but also adapt to new technologies in the future. The system design uses 4 integrated interfaces to transmit and receive network data of multiple services, and the access rate is up to 40Gbps.

2.2. Core processing module
The core processing module is the main control part of the entire system, interacts with the cache module and the hardware matching module for data information, connects to the intelligent management module and monitors the execution process of the system. It completes the in-depth processing and analysis work, including the extraction of IP packets after the original frame data is accessed, high-speed stream caching, key information matching operations, load balancing forwarding and output according to rules, monitoring information collection, and other important systemic functions.

According to the functional requirements of the high-speed network signal deep processing system, when selecting the processing core, designer must first meet the requirements of digital signal access...
at a rate of 10Gbps; secondly, for high-speed signal synchronization, descrambling, IP packet extraction, and other technologies, the logic computing capability becomes the main factor limiting performance; moreover, in the face of the rapid development of the Internet, the technology of processing network information is also deepening and improving, which requires the processing core to support easy modification and arbitrary programming at the software level.

In current network applications, mainstream processing cores usually adopt 3 solutions: 1) application solutions based on Application Specific Integrated Circuit (ASIC); 2) application solutions based on Network Processor (NP) network processor; 3) application solutions based on FPGA. Including general-purpose processors (GPP), Table 1 compares four processing devices.

| Contrast content                  | ASIC | NP  | FPGA | GPP |
|-----------------------------------|------|-----|------|-----|
| Development cycle                 | shorter | Short | Short | Long |
| Development environment           | Richer | Rich | Rich | Single |
| Flexibility                       | Better | General | Best | Poor |
| Processing speed                  | Fast | Slow | Fast | Faster |
| Scalability                       | General | Good | Good | Poor |
| Logic processing capability       | Poor | General | Good | General |

Broadly speaking, Field Programmable Gate Array is also a special integrated chip in the ASIC series. As a semi-custom circuit, compared with ASIC fixed circuits, its flexibility, scalability, and repeatable programming have given FPGA a very broad application prospect. At present, it has been widely used in many fields such as communication, network, aerospace, and computing application. In fact, FPGA also has the advantages of short development cycle, convenient test and verification, manufacturers' comprehensive development environment, and diverse programming forms.

FPGAs represented by the Stratix series of Altera products have integrated ultra-high-performance, high-speed transceiver modules for high-speed applications, namely high-speed Transceiver. Its full-duplex transmission and reception rates have reached 14.1Gbps and 28.05Gbps in the 5SGX and 5SGT series respectively. Fully meet the access requirements of four channels of 10Gbps high-speed digital signals.

2.3. Data cache module

The integrity of the data has a great influence on the accuracy of the matching function. In a high-speed fibre optic backbone network, data is transmitted in packets, and some data packets are also decomposed into data frames before transmission. Therefore, in order to reorganize the packet data and ensure its data integrity, the data needs to be cached. Considering the stability of the system, the maximum access rate reached 40Gbps when receiving 4 channels of 10Gbps signals, so the capacity of the high-speed data cache is at least 5Gb which equal to 40Gb divided by 8, and the bandwidth also needs at least 40Gbps.

At present, the commonly used cache technology solutions include high-speed Cache, Flash, DDR, solid-state hard disk (SSD) and so on. The double-rate synchronous dynamic random access memory series (Double SDRAM, DDR) has obvious advantages in terms of speed, capacity, and volume. Therefore, the network data classification system uses DDR3 as the IP packet buffer structure. Under normal circumstances, the bit width of DDR3 is 64-bit, it adopts double read and write mode, the single chip capacity is 4Gb, combined with FPGA input and output structure specifications, when the frequency does not exceed 533MHz, it can meet the highest bandwidth requirement of 68.224Gbps, which is equal to 533MHz times 64bit times 2 and is greater than 40Gbps; the design uses two DDR3 as the cache module, and the total amount reaches 8Gb which is greater than 5Gb. Theoretically, this design meets the cache requirement of the 40Gbps network signal.
2.4. Hardware matching module

After completing the data packet recovery and parsing, the quintuple information is sent to the hardware matching module for matching operation. The matching database is stored in the core device TCAM of the matching module, and only the data to be matched is sent to the matching unit. The matching module will automatically search for matching entries and return the best matching result to the core processing module. The core processing module classifies the data packet according to the matching result, and determines whether the data packet is passed, discarded or further analysed according to the classification result. Since the matching rule data in TCAM will be lost after power off, and in order not to occupy too much storage resources of the core processing unit, a FLASH module is added to the system design, so that the system does not need to be operated after power on work directly, simplifying the configuration work.

The high-speed network deep processing platform uses Netlogic Company’s TCAM as the key word matching search module. Suppose it is mainly for IPv4/IPv6 quintuple matching, and 144-bit is used as the information extraction bit width. Considering the extreme situation, that is, there are 15 million packets in 10Gbps information, then the 8-channel POS (Packet over SDH) signal uses the network search engine for quintuple matching. The bandwidth is 17.28Gbps which is equal to 144 times 8 times 15Mbps. The TCAM transmission bus interface used by the system adopts the working mode of parallel dual search, the bit width reaches 80-bit, the maximum working frequency can reach 300MHz, and its matching bandwidth is actually 48Gbps which is equal to 2 times 80 times 300MHz. Therefore, based on the requirements for system scalability, operational stability and reliability, the theoretical calculation value of redundant design far exceeds the target demand.

3. Software design of system

Data from the external network enters this hardware port through the high-speed network signal access unit. First, the system analyses the data packet in the core processing module to extract the five-tuple information. The acquired quintuple information is sent to the hardware matching unit for matching, and according to the feedback of the hardware matching unit, it is known whether the data packet hits the information in the matching database, so as to determine whether the data packet needs further analysis. Then, for data packets that do not need further analysis, pass them directly or discard them; for data packets that need further analysis, perform deep analysis in the core processing unit to obtain the type of food in the package and the production time information. The package that meets the limited conditions for the food type and production time can be made to pass through the core processing unit and enter the intranet, otherwise it will be discarded.

In addition, the data cache module meets the needs of processing high-speed and large-capacity data; the online management unit includes a matching host computer, which can update and read back matching conditions such as matching database, food type, production time, etc. online, which greatly enhances the human-computer interaction capability of the hardware system.

Due to the large number of Internet users, timely resolution of emerging threats is a necessary capability for a fully functional data classification system. The system is designed with a matching host computer program, which can update the matching rules, which greatly enhances the flexibility and scalability of the system.

4. System platform test

System testing is mainly carried out from three aspects: network signal access processing and data packet analysis. Based on Altera's dedicated development environment Quartus-II software, VHDL is used as the basic hardware description language, and Quartus-II integrated built-in debugging tool SignalTap is used to analyse the data in real time to verify the feasibility of the network data classification system.
4.1. Test signal generation
The software tester used to test the signal source can arbitrarily set the data in the package. The content of the set data packet is shown in Figure 2. The data packet contains 5-tuple information, type information, and time information.

| Source IP address | Destination IP address | Protocol | Source port | Destination port |
|-------------------|------------------------|----------|-------------|-----------------|
| ac 06 3d 81 56 46 9e 92 b6 10 34 a7 | 00 00 45 00 | 80 | 01 48 1a 82 40 00 80 86 06 07 99 0a 01 01 09 b7 0e |
| 00 00 20 | 14 a8 d4 2f 1f 98 b6 e1 9c fe 4a 83 76 c1 50 18 | 80 | 00 30 | 02 59 58 00 00 47 45 54 20 2f 44 61 74 61 43 | 00 00 30 | 02 59 58 00 00 47 45 54 20 2f 44 61 74 61 43 |
| 00 00 40 | 69 65 6e 74 2e 43 4e 33 39 4f 33 31 33 46 6f | 00 00 40 | 69 65 6e 74 2e 43 4e 33 39 4f 33 31 33 46 6f |
| 00 00 50 | 72 49 46 53 2e 73 76 63 6f 44 61 74 61 44 65 61 | 00 00 50 | 72 49 46 53 2e 73 76 63 6f 44 61 74 61 44 65 61 |
| 00 00 60 | 6c 2f 46 31 2f 32 30 31 36 30 34 31 35 30 30 30 | 00 00 60 | 6c 2f 46 31 2f 32 30 31 36 30 34 31 35 30 30 30 |
| 00 00 70 | 36 30 32 37 34 30 30 34 30 37 37 34 32 30 36 | 00 00 70 | 36 30 32 37 34 30 30 34 30 37 37 34 32 30 36 |
| 00 00 80 | 39 31 31 32 33 34 35 36 37 38 39 33 2f 6e 6e 6e | 00 00 80 | 39 31 31 32 33 34 35 36 37 38 39 33 2f 6e 6e 6e |
| 00 00 90 | 20 48 54 50 50 2f 31 2e 31 0d 0a 43 61 63 68 65 | 00 00 90 | 20 48 54 50 50 2f 31 2e 31 0d 0a 43 61 63 68 65 |

Figure 2. Packet format

4.2. Network signal access test
Call the PHY (physics) IP core and MAC IP core of the high-speed network signal inside the FPGA. After the IP core is configured, the signal processing can be completed and the data packet can be directly obtained. Use SignalTap to capture the header, and the result is shown in Figure 3.

Figure 3. Packet capture

4.3. Parsing test of data packet
In the parsing process of the data packet, the packet structure is mainly decomposed to obtain five element group information, type information, and time information. Use SignalTap to observe the analysis results, as shown in Figure 4.
5. Conclusion
This paper designs a network data classification system platform based on deep packet inspection technology, which uses FPGA+TCAM architecture. Through in-depth processing, the system can filter and filter data packets. Compared with the system designed in the article [2], this design combines the advantages of the two, optimizes the hardware structure, and improves the system access rate and data packet processing depth. Judging from the test results, this system can achieve high-speed signal access, not only can use the traditional 5-tuple matching method to complete the filtering of the data packet, but also can use the internal information of the data packet to perform in-depth screening to achieve the design The basic requirements. In the future, the software and hardware of the system will be further optimized to adapt it to a more complex network environment.

References
[1] CNNIC, 2020. The 45th China Statistical Report on Internet Development Status. http://www.cnnic.net.cn/hlwzjy/hlwzxbg/hlwzjy/201908/P020190830356787490958.pdf.
[2] Chen S.W., Huang W.W., Cao J.Y., 2014)A Deep Packet Inspection Engine Hardware Design Based on FPGA. Measurement & Control Technology, 33:100-102.
[3] Chen N., Li Z., 2007)A New Technology of Firewall - Deep Packet Inspection. Journal of Chongqing University of Science and Technology (Natural Sciences Edition), 9(3):69-71.
[4] Lu J.Q., Huang Z.P., Liu C.W., Liu D.S., Chen S., 2016)Design and implementation of flow distribution system on FPGA and TCAM. Microcomputer & its Application, 35(15):65-68.
[5] Liu Y.H., Gao X.L., Zhu M.C., Su P.H., 2019)Research on Classification Method of Network Data Based on Data Feature Learning. Netinfo Security, 10:50-56.