General Purpose Framework Designing for Network Security Test Devices Based on Multi-core Processor

Shi Guozhen , Li Fenghua, Li Li
Department of Electronic Engineering
Beijing Electronic Science and Technology Institute
Beijing 100070, China
Email: sgz@besti.edu.cn

Shi Hanzhang
School of Computer Science and Technology
Xidian University
Xi'an 710071, China

***Abstract*-In view of the present situation that network security equipments are deployed widely but their security strategies are not open to public, this paper analyzed currently used general test method for network security equipments, proposed a general purpose framework for test devices based on multi-core processor and performed a proof implementation on Tile64 processor platform. The general purpose framework includes three parts: the General network processing module and special communication protocols, master controlled dispatching module and special equipment test module. In the general purpose framework, the special test module can be loaded according to current requirement. In this basis, several problems that often exist in network security equipments test can be solved, such as security strategy leaking, batch processing for test devices and synchronous online tests for equipments of different types.**

Keywords-Testing devices, Network security, General purpose framework, Multi-core processor

I. INTRODUCTION

With the widely interconnecting of local area networks, network security has become a prominent issue in current information security. To resolve the issue, different kinds of security equipments are widely deployed such as VPN (Virtual Private Networks), IDS (Intrusion Detection Systems), fire wall and security gateway. Producibility of these devices brought another issue: how to guarantee their quality and performance? As a result, these years, studies on special test devices for network security equipments have become a study focus in and abroad.

So far, there are already several test tools for network equipments, such as Ixia&reg[1]， sigmationTF[2] and SmartBits, etc.. But these tools mainly aim at general performance test or protocol conforming test. These years, China has issued a variety of national standards on network security device testing[3][4] but test device manufacturers are still not able to completely acquire the security strategy for a certain security equipment, therefore indepth tests have to be carried out by network security supervision departments or equipment manufacturers themselves. In this connection, a general test device framework that enables users to load relevant test modules by themselves are of great importance to network security equipment test.

This paper studied general purpose framework designing for special network security test devices based on multi-core processor and performed proof implementation on TILExpress-64 development board as the hardware platform.

II. GENERAL METHODS FOR NETWORK SECURITY EQUIPMENT TEST

According to the difference of test environments, there are two ways of equipment tests: online and offline. Online test, which refers to testing the equipment when it is under normal working condition, has a higher requirement for the simultaneity and real-time performance of the test device. On the other hand, offline test is to comprehensively test the equipment and find out possible faults when the equipment is already separated from the working environment, so it is easier for the test device and test method to realize. However, since it is hard to simulate the real network environment, there would exists a gap between the test effect and the practical application. At present, general method for network security equipment test can be summarized as the following three types shown in Figure.1.

III. THE GENERAL PURPOSE FRAMEWORK DESIGNING FOR TEST DEVICES

Based on the above mentioned three types of test methods and according to unique features of different network equipment, the design for test devices may vary greatly. There are three main issues that have to be resolved in order to set up the test framework:

(1) Establish general purpose network data I/O interface. A unified regulation of network data package requires establishing the general purpose I/O interface, which is a significant issue on data sending and receiving that must be resolved.

(2) Accomplish loading and reconfiguration of different test modules.

(3) Provide adequate, optionally distributed physical network interface.

A. *The overall design for general purpose framework.*

In the basis of traditional network test device model, the design of general purpose framework of network security test device based on multi-core processor is shown in Figure.2, which includes three parts: the general network processing module and special communication protocols, master controlled dispatching module and special equipment test module.

The basic framework is composed of three parts: network interface, unified network data sending and

Published by Atlantis Press, Paris, France.

receiving module and the master controlled dispatching module. Network interface provide available external interface for the system, including user platform interface and test interface. The unified network data sending and receiving processing module, which runs in an independent core, provide each test module and the master controlled dispatching module with outward data sending, data receiving and other primary process. The master controlled dispatching module, which employs a certain core from the available core resources, loads relevant test module to perform the test. It also runs independently in a physical core, transmitting data according to the equipment analytic command.

The special device test module refers to the special test programs developed for specific network security equipments. This module has to meet some particular formation rules and requirements in order to adapt to the dynamic framework.

The host-computer communication protocol refers to the data communication protocol between the master controlled dispatching module and the user. This protocol provides the orders and interaction methods between user and test devices.

B. The general network processing module and special communication protocols

The general network processing module has several physical network interfaces. One of them is reserved for the interaction between the test device and the user platform, and the rest of them are provided for interaction between test device and the tested equipment. The management of different interfaces is unified. The unified management program sends internal data directly according to the physical labels of different interfaces and transmits external data to relevant core for processing.

To realize the remote data communication between user and the general purpose test framework, order interaction between the two adopts the common IP protocol. User-defined command frame for communication between user platform and test device is shown in Figure.3, including identification field, sequence number, data length, command field, sub-command field and data field, etc.

Identification field: occupying 4 bytes, indicate the current frame is a test order frame (data frame) and this field can be used as the identification between devices; sequence number: occupying 4 bytes, to count the number of data packages; data length: occupying 2 bytes to indicate the valid length of the current frame; command: occupying 2 bytes, the high byte indicate the device type and the low byte indicates serial number of the device of this kind; sub-command, occupying 2 bytes, stands for the specific function of a certain device, this command is analyzed by a special device test module instead of the master controlled dispatching module; data: length uncertain, it is the data and parameters for test orders, analyzed by special device test module.

C. The general framework master controlled dispatching module

Two layers, whose structure is shown in Figure.4, are designed for the general network mastering controlled dispatching module. As the first layer, master controlled dispatching module analyses the data from the network, which is sent to the next level controlled core, and administrates all the core resource. There is only one physical core, called Xcore. The second layer is device type master controlled core, the number of which is the maximum value of device type loaded into this equipment. These cores, called #1~#N, are used to administrate some kind of devices adding and specific workflow.

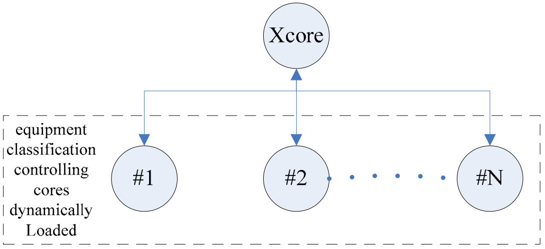
Xcore
equipment classification controlling cores dynamically Loaded
#1
#2
#N

Figure 4. Structure of scheduler module

The general framework loads a special device by following steps.

Step1. The user sends one or more command to start the device.

Step2. Device type master controlled cores are loaded.

Step 2.1 Xcore receives starting device command from the user, and checks whether this kind of devices have started. If so, goto Step3; Otherwise, checks whether this kind of device type master controlled cores remained. If the cores are remained, goto Step3; Otherwise, set “device type resources lacking” and goto Step 5.

Step 2.2 Xcore chooses one of the spare resources from #1~#N, and schedules the matching device type controlled program corresponding to the command.

Step 3. Xcore forwards the starting device command to matching device type controlled core.

Step 4. Tested devices are loaded.

Step 4.1 According to the command， device type master controlled core #x (x=1,2，⋯，N) checks whether there is enough core resources. If not, set “core resources lacking” and goto Step 4.3.

Step 4.2 Device type master controlled core #x schedules the matching program to occupy the core sources needed, and then set starting success flag, device number and the logical number of the core occupied.

Step 4.3 Device starting states arguments are sent by Xcore.

Step 5. Xcore send the results of device starting to the user.

D. The designing for special equipment test module

According to the specific features of the devices, special equipment test module is designed independently based on the framework and interface in this paper by testers or producers. There are some rules following in the general purpose framework. The special equipment test module should work on an independent core. It communicates with master controlled dispatching module in the format of pipe or message. The results of the special equipment test module testing should be sent to the communication interface rather than forwarded without passing the master controlled dispatching module. The states information should be sent to the master controlled dispatching module. Figure.5 shows the general structure of the master controlled dispatching module designing.

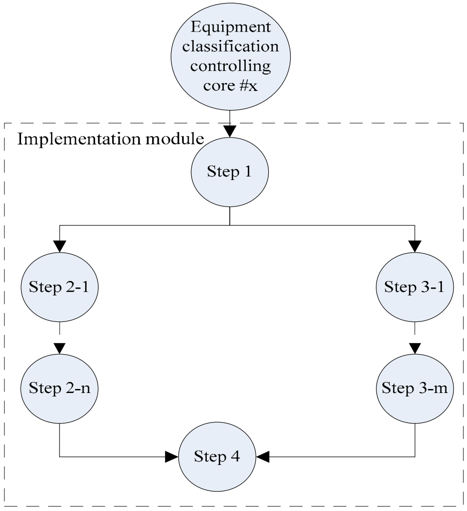

Figure 5. Architecture of special equipment testing module

IV. Realization on a Demo Test Device Based on Tile64 Processor

TILE64 is a multi-core processor launched by Tilera Corp. It is composed of 64 identical cores (called Tile), each one of which is a full-featured processor with its own L1 cache and L2 cache and is connected with other Tile cores through nonblocking switching fabrics to form a high-speed and nonblocking Mesh network [5]. TILExpress-64 developing board based on TILE64 multi-core processor provides 6 (can be extended to 12) GB interface. The board provides several significant mechanism such as IPP(Ingress Packet Processor), EPP(Egress Packet Processor), tile scheduler management, communication mode and blocking process, which can meet basic requirement of the general purpose framework[6-7].

According to the design of the TILExpress-64 developing board, 8 cores are used as operational environment for DDR, OS, IPP and EPP, etc.. The rest 56 cores resources are available. The logical 0 core are defined as Xcore. Three cores #1 - #3 (logical 1 to 3)control the device type. 52 cores(logical 4 to 55) are reserved for dispatching. This device can load 3 types of test device to perform the network device test. The design is shown in Figure.6.

2 NMAP scanning programs run in the demo device to scan different segments and tasks. 1 IDS test device is employed to completely test the IDS equipment.

V. Conclusions

In the basis of network security device test method analyzing, a General Purpose Framework Designing for Network Security Test Devices based on Multi-core processor study was proposed and was realized on the Tile64 processor. The result shows, in this framework, test modules can be loaded according to requirement. The general purpose framework resolves three issues existed in network security equipment test: users may produce special test program according to the requirement of the tested equipment, which can avoid security strategy leaking; users can load test modules of a certain type and perform batch testing processing; users can load test modules of different types so that synchronous online tests for equipments of different types can be realized.

Acknowledgement

This work is supported by the Key Program of Scientific and Technology Research of Ministry of Education (No.209156), the Beijing Natural Science Foundation (No.4102056).

References

[1] Ixia Platform Brochure [DB/OL]. http://www.ixiacom.com/pdfs/library/brochures/platform_brochure.pdf.

[2] Introduce to Sigmation TF [DB/OL]. http://www.sigmart.com.cn/product/sigmationtf/homepage_intr.php.

[3] GB/T 20281-2006. Information security technology — Technique requirements and testing and evaluation approaches for firewall products [S]. 2006.

[4] GA/T 681-2007. Information security technology — Technical requirements of gateway [S]. 2007.

[5] TILERA. TILE Architecture-Overview. pdf [Z]. 2008.

[6] TILERA.TILE MDE-System-Programmers-Guide.pdf [Z].2008.

[7] TILERA.TILExpress-64Card-Users-Guide.pdf [Z].2008.

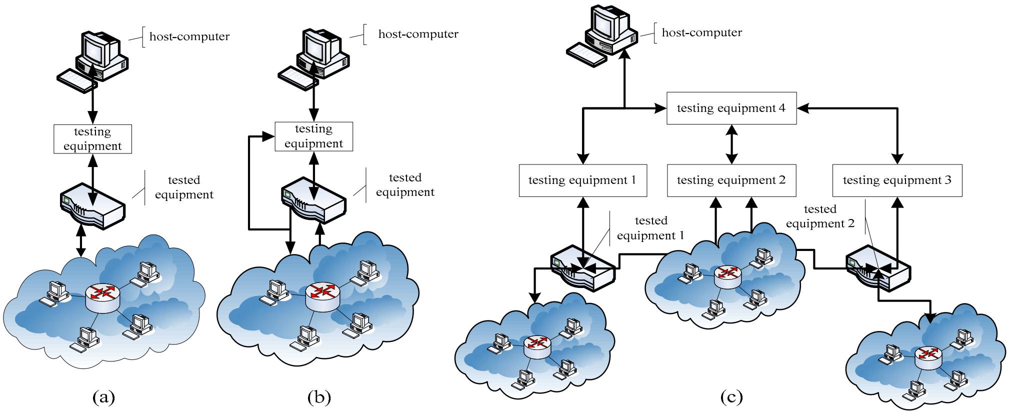

Figure 1. Network security equipment testing method

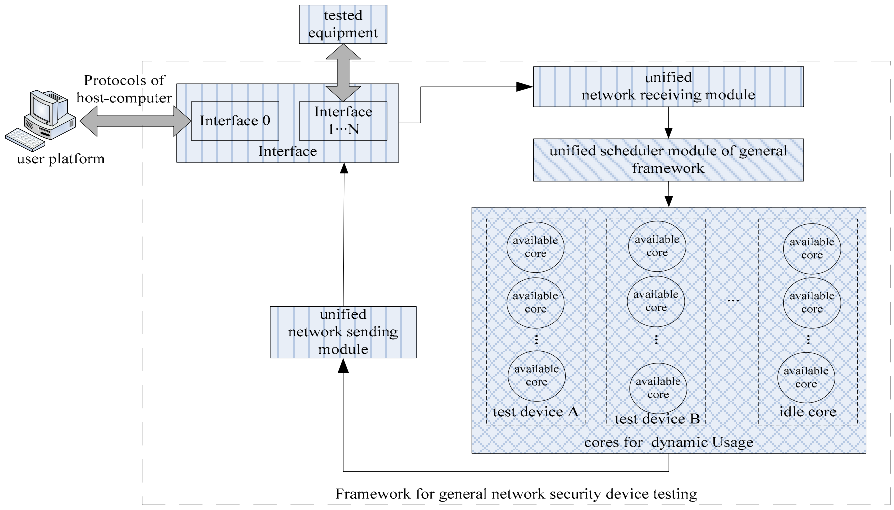

Figure 2. The overall design for general purpose framework

identifying field	sequence number	data length	command	sub command	data
4bytes	4bytes	2bytes	2bytes	2bytes	MaxLen-14 bytes

Figure 3. Structure of protocol

Published by Atlantis Press, Paris, France.

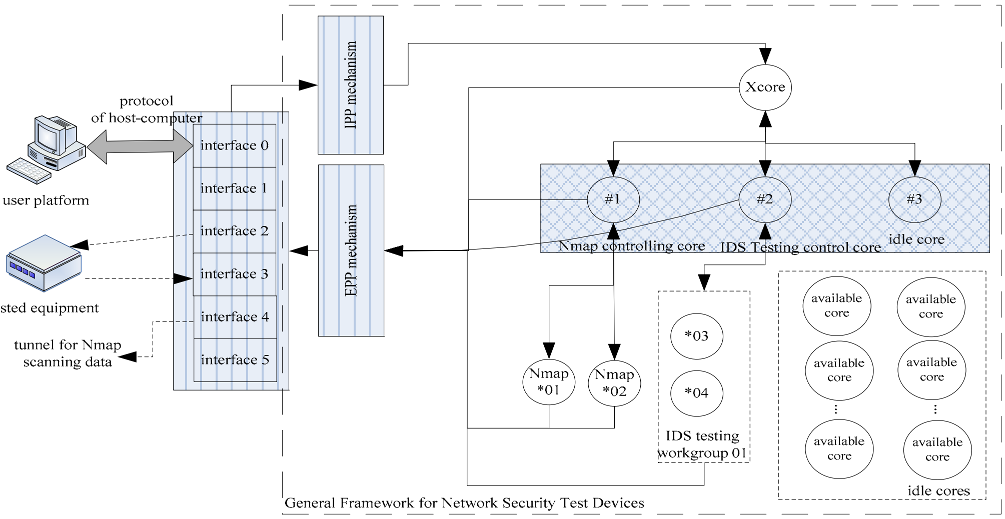

Figure 6. Architecture of demo test equipment based on Tile64 processor

Published by Atlantis Press, Paris, France.