Design and Implementation of High Performance IPSec Applications with Multi-core Processors

Yizhen Liu[1], Daxiong Xu[1], Wuying Song[2], Zhixin Mu[2]
[1] *College of Electronics and Engineering,*
Beijing University of Posts and Communications, Beijing, 100876, China
[2] *Laboratory of Network Security System, QQTechnology, Beijing, 100037, China*
liu_yizhen@163.com, dxxu@bupt.edu.cn
wysong@qqtechnology.com, zxmu@qqtechnology.com

Abstract

The rapid increasing Internet services need high performance, scalable and flexible network security devices. IPSec is a set of protocols to ensure transmission of packets in IP network. Multi-core processors are targeted to a wide range of applications with complex packet processing and high throughput requirements. Although there are several designs of IPSec system with heterogeneous hardware platforms, practical ultra-speed network security systems remain elementary. The disparity arises because IP network security algorithms with theoretically considerable computational cost and packet processing have unacceptably memory access latency. This paper discusses the design and implementation of IPSec applications at 17Gbps using next generation programmable multi-core processor RMI XLR732. We focus on IP Security software architecture suitable for high speed network, and present consideration of traffic load balance and hardware framework. The improved software architecture is implemented on the dual multi-core processor hardware, and actual packet data is used to assess performance.

1. Introduction

The fast expansion of internet services speeds up the development of a wide variety of novel networking systems and technologies. Security of Internet protocol network is one of the most important aspects of the future network technologies. In particular, web-based services, e-commerce, multimedia and new extensive network services need IP network security systems to secure those transactions and communications are safe and reliable. Furthermore, the infrastructure and architecture of IP network security systems are required to improve performance and to accommodate growth in network traffic.

IP network security concerns have caused the wide use of secure communication protocols, such as DES, AES, and SSL. These protocols support network services to achieve authentication, encryption, integrity and protection [1]. IPSec is a set of protocols developed by the IETF to support secure exchange of packets at the IP network.

RMI XLR732 is the next generation multi-core processor, which enables fast deployment of intelligent network services by providing flexible programming and high performance. It is suitable to a wide variety of applications at complex packet processing. The XLR732 processor supports a broad range of speed from 2.5Gbps to 20Gbps.

Although ultra-speed IPSec system appears to be practical, the evaluations so far have only used network simulators, such as ns-2 [2]. Because network traffic simulations do not account for all operations performed by most security algorithms and practical memory access, it is difficult to assess the real performance of the design of IPSec applications. Therefore, to obtain a better creditable measurement of IP security algorithms performing, they must be implemented a hardware prototype and measured.

This paper describes the design and implementation of maximal 17 gigabits IPSec system using next generation programmable multi-core processor RMI XLR732. We present design framework, system architecture, and report measurements. In particular, we demonstrate performance improved by distributed scheme and trade-off in software framework. We show an IPSec system can exploit dual multi-core processors, and make suggestions about hardware features that can significantly improve algorithms performance of encryption and authentication.

The rest of the paper is organized as follows. Section 2 presents the related works on hardware design of network security system. Section 3 describers an overview of the programmable multi-core processor RMI XLR732 and fundamental features. Section 4 discusses the

978-0-7695-3480-0/08 $25.00 © 2008 IEEE
DOI 10.1109/FITME.2008.88

implementation of ultra-speed gigabit IPSec system, and some considerations, such as load balance, software architecture. Section 5 introduces hardware experiment and measurement result. Finally, Section 6 presents summary and conclusions.

2. Related work

Many researchers have developed a large cryptography and authentication applications through a wide variety of software and hardware techniques. There are several works using enhanced instruction to add general purpose processors [3], [4], [5], improve them to computer cryptographic and authentic algorithms faster. On the other hand, some specific hardware platforms and processors are available from commercial vendors such as Cisco [6], Broadcom[7], SafeNet [8]. The IPSec applications used at network processors [9] can perform most security algorithms, but the performance remains lower level.

3. Multi-core processors

In this section, we describer a brief overview of the programmable multi-core processor RMI XLR732. Especially, we introduce advanced MIPS64-based core, security acceleration engine and on-chip fast message network.

Several types of multi-core processor exist. These processors are based on a growing mix of semi-programmable ASICs and network processors [10]. Many platforms have created a hardware and software environment that is increasingly complex, expensive and difficult to scale. Although they are different hardware designs, most architectures use some combinational technologies of parallelism, pipelining and special coprocessors to achieve high speed data packet processing.

Unlike the traditional ASIC and network processor, we used the XLR732 processor for IPSec applications and all measurements. Figure 1 shows the architecture of the XLR732 multi-core processor. The XLR732 consists of eight general-purpose MIPS64-based cores [11] and a set of auxiliary on-chip hardware logic units such as security acceleration engine, network accelerator and high speed distributed interconnects. The XLR732 processor includes flexible and maximal 24Gbps network interfaces, PCI-X, and configurable SRAM and DRAM memory controllers.

The XLR732 processor is based on a set of next generation multi-cores which have 32 threads in eight identical 4-way multithreaded cores. Each core includes four tightly integrated hardware threads. In contrast with single-core processor, this multi-issue architecture is well adapted to future increasingly network security processing systems. Each core contains a 32-KB, Level-1, 8-way set-associative data cache. As with the instruction cache, the high degree of set associatively reduces cache-conflict misses.

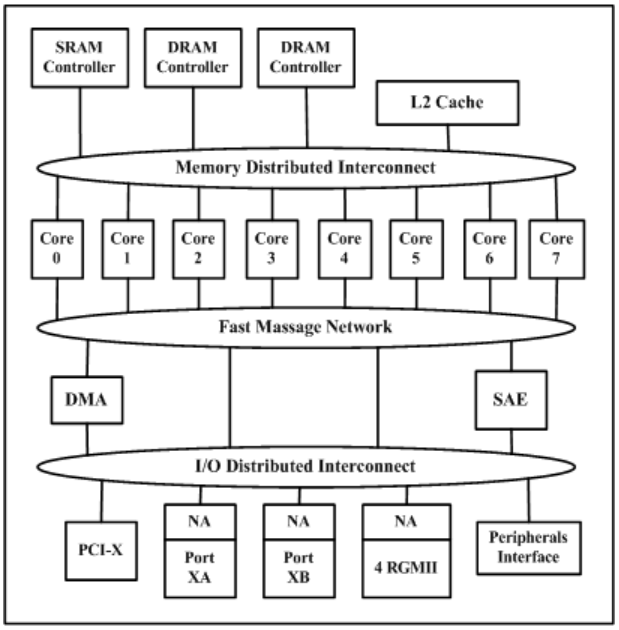

Figure 1 XLR732 architecture

Furthermore, the XLR732 Processor integrates a high performance security acceleration engine (SAE) that enable speed up to high performance cryptographic processing with standard security protocols such as IPSec and SSL. To provide greater flexibility for security implementations, the SAE includes four parallel crypto cores and one RSA core. These cores can be operated independently. Figure 2 shows that the SAE supports not only DES, 3DES, AES and ARC4 cryptography, but also SHA, MD5 authentication, CRC checksum and RSA exponential key generation. Each of the crypto cores can encrypt or authenticate and decrypt a packet.

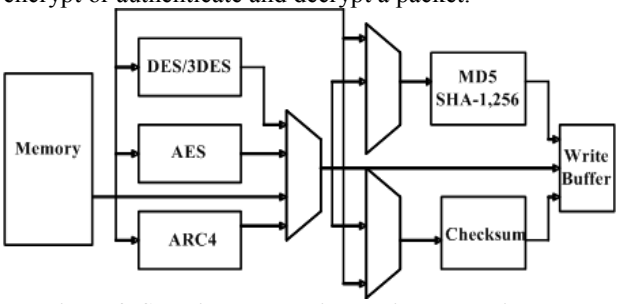

Figure 2 Security acceleration engine block diagram

Besides security acceleration engine, fast Messaging Network (FMN) is another fundamental mechanism in the XRL732 processor. The FMN is a high-performance, low-latency messaging network that connects key system elements. It connects the eight cores, network accelerators, DMA Engine and DMA for Security Accelerator. Network interfaces and software communicate about packets via messages sent on the

FMN. The FMN ensures fairness among its stations by using a credit-based, round-robin scheme for placing messages onto the message network. This scheme guarantees that messages arrive quickly at their destination and ensures that cores and threads are not starved from access to the FMN.

4. Implementation of IPSec applications

In this section, we discuss three most important factors of implementation for IPSec applications. These factors are load balance consideration for high-speed network, improved IPSec software architecture and hardware experimental platform design.

4.1. Load balance consideration

We often use distributed and parallel processing mechanism for complex data packet operation at high speed network. Therefore, distribution of 20Gbps traffic and load-balance on each thread become the main issue for IP security system architecture. We consider three stages to achieve distribute massive packets into many threads. So, each core or thread can handle proper traffic, and can not cause traffic block and packet drop. Firstly, master XLR732 (see Figure 4) divides all packets received by 10Gbps interface into two 5Gbps traffic. Then, one half is transmitted to slave XLR732 and another half is handled by itself. Secondly, each multi-core processor distributes data packets to multiple threads. Finally，the slave processor XLR732 aggregate all traffic and transmit result packets to network interface.

Data packet received from network interfaces are exchanged in a SPI4.2 switch, and transmitted to master processor XLR732. The network accelerator of multi-core processor extracts the classic five fixed fields (protocol, source IP, source port, destination IP, and source port) from packet header and executes 7-bit CRC hash algorithm to compute hash value. The hash Polynomial is given by: $CRC7 = x^7 + x^4$.

After three stage of distribution, we achieve load balance on two 32-threads processors. The CRC7 hash algorithm ensures packets that belong to each flow will be send to corresponding threads. Consequently, data from each user or host will be encrypted or decrypted together, which ensure the integrality of data.

4.2. Design of IPSec software architecture

IPSec is a set of IP network layer protocols that guarantees exchange and communications safely. IPSec includes two different protocols, Encapsulation Security Payload (ESP) and Authentication Header (AH) [1]. While ESP encrypts and authenticates the payload field of a packet, AH authenticates all field of a packet, and operate Transport and Tunnel modes.

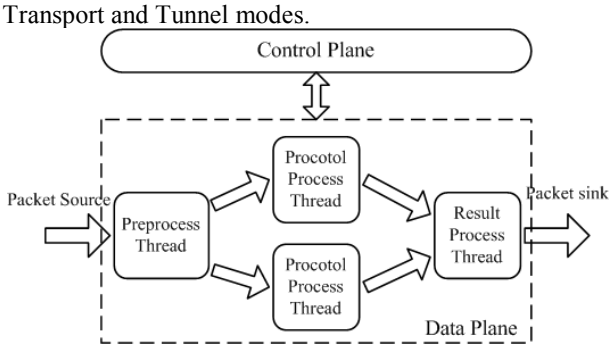

Figure 3 Micorblock of IPSec software pipeline

We consider three phases software pipeline implemented using 4 threads per core (see Figure 3). Firstly, the preprocessing thread Performs policy lookup and security association database lookup (SADB) to determine cipher, digest, and keys for security engine operation. Secondly, two protocol processing threads add headers and trailers according to policy for this packet. For example, protocol encapsulation for 3DES encrypted ESP tunnel mode to a 64 bytes packet would entail adding 20 bytes IP header, 8 bytes ESP headers, 8 byte increase value, 2 bytes pad and 12 bytes digest, thus adding 50 bytes to the packet. Then, it sends message to SAE for encryption decryption and hash. Finally, the fourth thread handles SAE result, compare Authentication result to one in packet and strip IPSec protocol headers.

4.3. Hardware experimental platform

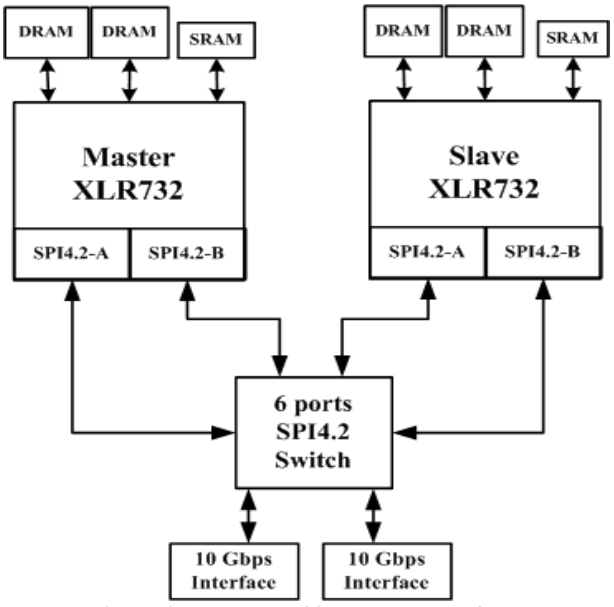

Figure 4 Dual XLR732 hardware platform

Figure 4 shows the architecture for our 20Gbps IPSec application hardware platform. This hardware platform consists of two RMI XLR732 multi-core processors, a 6-ports SPI4.2 switch, memory systems and two 10Gbps network interfaces. Network interfaces enable to measure at maximal 20Gbps wire speed in real network environment.

Table 1 shows the memory configuration of hardware platform. We use 1GB DDR2 Dram per channel at 400MHz, 8MB QDR SRAM per channel at 250MHz and 32MB flash for each XLR732. The clock frequency of XLR732 processor is 1.0GHz.

Table 1 Memory configuration for each XLR732

Memory type	Size
QDR SRAM	8MB
DRAM	2GB
Flash	32MB

5. Hardware experiment

This section reports measurements of our implementation on dual XLR732 processor hardware platform. We concentrated on the highest incoming packet rate that can be supported.

To measure the highest incoming packet rate, we used a worst-case incoming method. Because packet processing time is proportional to number of incoming packets rather than there size, we used 64 bytes small packet for the experiment. In addition, we arrange that packets behavior is worst case, such as random 5-tuple value and mixed payload to lead most cache misses.

5.1. Result

Table 2 shows the results for the worst-case processing rate measurement. None of the rates is close to hardware line speed of 20Gbps. However, ARC4 and MD5 processing achieve almost the same maximal rate. The reason is that most overhead comes from memory accesses and same complex computation.

Table 2 Rate measurements at worst–case

Number of threads per processor		16
Encryption Algorithm	3DES	12.4 Gbps
	AES128	10.6 Gbps
	ARC4	17.0 Gbps
Authentication Algorithm	MD5	16.9 Gbps
	SHA256	14.1 Gbps
	HMAC_MD5	12.7 Gbps

We analyzed the potential packet processing rate if cache overhead could not exist. With no cache misses, the encryption and transmission of a single packet in 3DES algorithm takes about 76 cycles.

6. Conclusion

This paper describers the design of high performance IPSec software architecture and a general framework for implementation on the next generation multi-core multi-threaded processor. We present hardware design and software pipeline architecture for the multi-core processor. We also focus on the 20 Gbps traffic load balance on dual multi-core processors.

Based on our experimental data, we conclude that the improved software architecture and optimal hardware platform can guarantee IPSec algorithms at 17Gbps. Measurements show that the main performance bottleneck for IPSec algorithms arises not only from complicated encryption and authentication computing process but also from memory latency and traffic distribution cost. Hereby, a smooth load balance method and fast memory cache mechanism can improve performance. Finally, we conclude that with an available hardware, the improved IPSce software architecture and load balance method are better suited to ultra-speed network because they are efficient and have scalable properties.

Acknowledgement

The authors would like to acknowledge Dong Liu and Lingge Sun for useful discussions related to this work.

References

[1] W. Stallings, *Cryptography and Network Security: Principles and Practice*. Prentice Hall, 1998.

[2] "The network simulator ns2," http://www.isi.edu/nsnam/ns/.

[3] J. Burke, J. McDonald, and T. Austin, "Architectural support for fast symmetrickey cryptography," in *Proc. Intl. Conf. Architectural Support for Programming Languages and Operating Systems (ASPLOS)*, pp. 178–189, Nov. 2000.

[4] R. B. Lee, Z. Shi, and X. Yang, "Efficient permutations for fast software cryptography," *IEEE Micro*, vol. 21, pp. 56–69, Dec. 2001.

[5] *SmartMIPS*. (http://www.mips.com).

[6] "Cisco ASA 5500 Series Adaptive Security Appliances," http://www.cisco.com/en/US/products/ps6120/index.html.

[7] *Security Processor Solutions*. Broadcom Inc. http://www.broadc-om.com/products/Enterprise-Networking/Security-Processor-Solutions.

[8] *Safenet EmbeddedIP*. Safenet Inc. http://www.safenet-inc.com.

[9] Minho Han, Kiyonny Kim, Jongsoo Jang, "The design of IPSec Application for IXDP2851," in *Proc. of ICACT'06*, pp. 309-313, 2006.

[10] D. Comer, *Network Systems Design using Network Processors*, IXP2400 version. Prentice Hall, 2005.

[11] "XLR Processor Family Programming Reference Manual" RMI Corpration, December 2006.