

High-throughput ASIC design for e-mail and web intrusion detection

Ming-Jen Chen¹, Yi-Mao Hsiao^{2a)}, Hui-Kai Su³,
and Yuan-Sun Chu¹

¹ Institute of Electrical Engineering, National Chung Cheng University,
168 University Road, Minshiung, Chia-Yi, Taiwan 62102

² Design Automation Technology Division, Information and Communications
Research Lab. (ICL), Industrial Technology Research Institute (ITRI),
Hsin-Chu, Taiwan 31040

³ Dept. of Electrical Engineering, National Formosa University, Yunlin, Taiwan
a) YMHsiao@itri.org.tw

Abstract: The malicious attacks adversely affect every user over the Internet. This paper proposes an application-specific integrated circuit (ASIC) design with parallel exact matching (PEM) architecture to accelerate the Snort intrusion detection system (IDS). The PEM is half mesh architecture to compare the Snort rules in parallel. The ASIC named snort rule accelerator (SRA) focuses on the TCP protocol to detect the attacks of e-mail and web applications. As shown in post-layout simulation, the ASIC operated at 435 MHz to perform the needs of high speed with 13.9 Gbps system throughputs. So that it resolves the complexity of information security limitation to manage data received from the 10 Gbps core network.

Keywords: IDS, Snort, ASIC

Classification: Integrated circuits

References

- [1] H. Song, T. Sproull, M. Attig and J. Lockwood: Proc. Inter. Con. on Field Programmable Logic and Applications (2005). DOI:10.1109/FPL.2005.1515770
- [2] C.-C. Wang, C.-J. Cheng, T.-F. Chen and J.-S. Wang: IEEE J. Solid-State Circuits **44** (2009) 1571. DOI:10.1109/JSSC.2009.2017009
- [3] C.-H. Lin and S.-C. Chang: IEEE Trans. Very Large Scale Integr. (VLSI) Syst. **19** (2011) 33. DOI:10.1109/TVLSI.2009.2028346
- [4] C.-H. Lin, C.-H. Liu, S.-C. Chang and W.-K. Hon: Proc. IEEE INFOCOM (2012). DOI:10.1109/INFOCOM.2012.6195575
- [5] T.-H. Lee and N.-L. Huang: IEEE/ACM Trans. Netw. **21** (2013) 1104. DOI:10.1109/TNET.2012.2224881

1 Introduction

Viruses and malicious software are spread quickly, increasing usage of users over the Internet. The network security becomes more and more essential, about person-

al information service. The IDS monitors network activities for malicious activities and subsequently report to the network administrator. When the network speed is slow, the security detection is suitable for software. However, the current network line speed exceeds the CPU speed. The detection of malicious software over the Internet in real-time is difficult. An effective solution is an accelerator hardware design.

Many designs are proposed to implement a parallel and pipelined pattern-matching engine for IDS. They use Snort rules or the ClamAV virus database. Bloom filters are hash-based architecture with efficient probability. Song divided the filter into active and passive filters [1]. The high usage content is placed into the active filter as first level, and the suspicious packets are sent to the second level to perform pattern matching. The virus detection operation may be reduced as a string matching problem. The content addressable memory (CAM) was used for snort rule matching. However, the system throughput is reduced if a particular amount of rules exist. The CAM-based architecture usually costs more and consumes more power. Wang proposed a TCAM-based virus detection processor for mobile devices [2]. A dual-port TCAM design reduces the power consumption and achieves a high performance system. A finite state machine correctly implements high-speed matching with the snort rule and virus signature. Lin proposed a memory-efficient pattern-matching algorithm with FSM hardware design to reduce the memory requirement of Snort rule sets for inspecting packet contents against thousands of predefined malicious or suspicious patterns [3]. Furthermore, he proposed another memory-efficient architecture using perfect hashing to condense state transition tables without hash collisions [4]. The implemented architecture is on graphic processing units and tested using attack patterns from Snort system and input packets are from DEFCON. Lee proposed a pattern-matching architecture consisting of a stateful pre-filter and an AC-based verification engine that achieves a significant improvement in both throughput performance and memory usage for IDS [5].

In this paper, we propose SRA with parallel rule matching to accelerate the Snort system. Focused on the TCP protocol, the SRA detects the attacks of e-mail and web applications. The ASIC performed 13.9 Gbps system throughputs to manage the requirements of high speed and high accuracy for IDS.

2 The snort system and the rules

By combining the benefits of signature, protocol and anomaly-based inspection, Snort is the most widely deployed IDS technology worldwide. In a snort rule to describe the grammar of exact position content, the parameters are offset and the depth indicates the address of content at the TCP payload and the size of content. Most of the misuse behavior is by treating a hole or a specific port so that the signature is in an exact position in the early stage. There is no exact position of misuses exists in the packet payload. The relative position manages this limitation. The parameters are the “distance” and “within” in Snort grammar, which describes the beginning of the last byte of content from the range between the bytes. The range without an exact position and the flexible length causes difficulty in the hardware design for Snort.

Web pages and e-mail are the most widely used applications on the Internet. Based on TCP protocol in transport layer, they use HTTP and SMTP protocols in application layer. The total number of rules is 4,020 and 85% are with TCP protocol in the Snort rules. In our analysis, the Snort rules with version 2.8.6 about e-mail and web intrusion detection are to deal with content (message) matching in packet level. The matching results of each packet are independent. Additionally, the state information of multiple TCP flows is maintained by original Snort software module. If a packet matches TCP state and belongs to web and e-mail applications, the packet is filtered by SRA ASIC. The performance of the stateless matching mechanism is improved for web and e-mail packets. The Snort system contains four progresses: sniffer, preprocessor, detection engine and alert logging. The SRA plays the role of detection engine to accelerate Snort system and then the system determines whether the packet is passed or dropped.

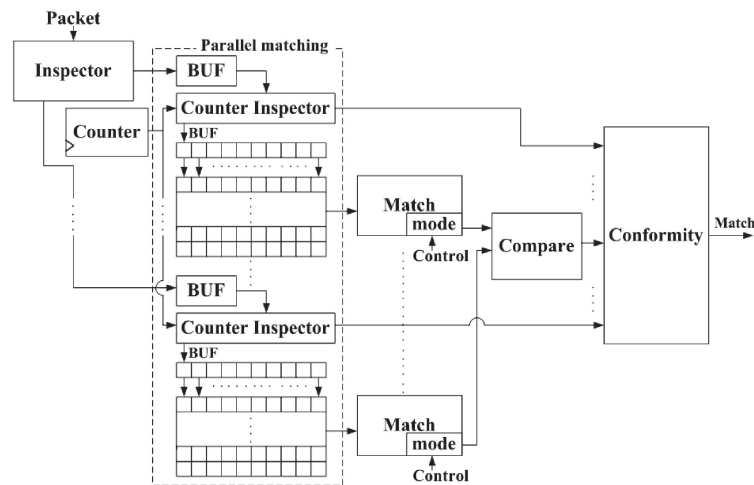
3 System architecture

The SRA is proposed with stateless parallel-matching scheme to perform high throughput packet filter as an accelerator of detection engine for the Snort system. Because the snort rules describe the position or range of the content, our proposed system is based on the rule without assessing the whole packet of the TCP payload. The data as the input of SRA are the TCP payload and port number. The hardware architecture of SRA is composed of five major modules, including the *inspector*, *counter*, *parallel matching*, *conformity*, and *compare* modules, as shown in Fig. 1(A). The core module is the *parallel matching* module, and the others are assistant modules. The *inspector* filters the packets, except for web page and e-mail packets with the port numbers 25 and 80. The *parallel matching* module compares the payload in the content range during the counter time. When an entry is matched, the SRA is in an idle state and sends a *compare_end* signal to the *conformity* module. The *conformity* module integrates all signals and determines whether an abnormal payload is presented. We design half mesh architecture in the *parallel matching* module as shown in Fig. 1(B). The *location recorder* module stores the position information. Each block is composed of several attack rules, and every rule is composed of several contents. Although the length of the content is not consistent, the *parallel matching* module can manage various lengths using byte to byte in the content range.

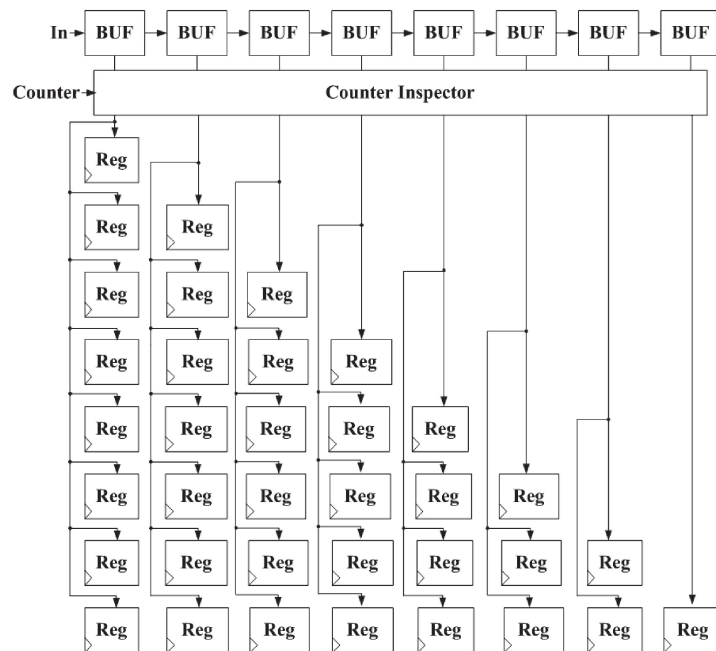
The *parallel matching* is the crucial part of SRA system, which performs the packet payload comparison with the stored Snort rules. The system updates and deletes the content of Snort rules constantly. In the content block design, each location has its own tag. To change the signature, the SRA use the location tag number with desired content data. A time controller stores the last range of content before sending the data to the next component. Payload data are still received if the counter value is under the last range. The two time controllers store the range of shared content and independent content. Because the hardware is unable to record the content of each data, the hardware only blocks content in the same storage, which is the earliest and latest end of the range.

Although false positives originate from the surface, there are no absolute locations observed in a real case. We increased the scope in the system to prevent

effects on the correctness. In every matching operation, a content signal passes the results from the mode module for comparison. The *parallel matching* scheme is designed in four modes to the content blocks. Basically, the system is designed with two storage blocks architecture to store the content. Then, we use two methods to enlarge the storage efficiency as shown in Fig. 2(B) so that there are four modes. Each match module receives a signal that is compared to the end. In the same type of attack, there are exhibit absolute and relative characteristics of the Snort rules. The absolute key is independent to reduce the comparison of duplicate content. The match conformity is the storage of rule files. Each content has its own counter register, the inner controller controls the length of the content. The number with input data can change the length of the content. When the content is compared with the Snort rules, the data are sent to the *compare* module. After the comparison, the signal with a match or a pass is sent to the Snort system.



(A) The system architecture.



(B) The parallel matching with the half mesh architecture.

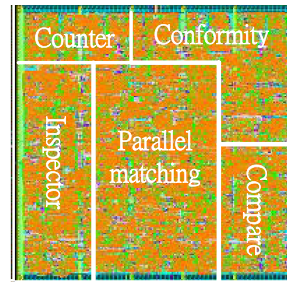
Fig. 1. The system architecture of SRA and the parallel matching architecture

4 VLSI implementation and performance analysis

We implement the SRA as an ASIC to accelerate the Snort rule matching. The matching result was determined by the timing control parameter so that the ASIC does not assess the whole packet. The power dissipation of the ASIC for rule matching is reduced. The design is conducted with the Verilog hardware description language and synthesized by Synopsys using the TSMC 90 nm CMOS single-poly nine metals standard cell library. Fig. 2(A) shows the layout of ASIC. As the post-layout simulation result indicates, the speed is 435 MHz, the chip area is $2.15 \times 2.12 \text{ mm}^2$ and the power consumption is 79.3 mW.

To reduce the chip area, we focused on the parallel matching module that is 64% of the ASIC. First, we reduced the rules directly or shortened the length of the content. However, reducing the rules affects the false positive ability. Second, we modified the blocks of the parallel matching module, as shown in Fig. 2(B). Every block has its own assistant module so that the large chip area is happened. If the storage content of every block increases twofold, the assistant module reduced by 50% of area. Two methods are used to increase the storage efficiency of hardware architecture. In the first method, we enlarge the storage element to increase the area of every block by 26%; however, a 50% reduction of usage in SRA occurred, as shown in Var.2 of Fig. 2(B). The other method is by adding two storage elements of content to increase the area of every block by 51%, as shown in Var.3 of Fig. 2(B). Based on the comparison of Var.2 and Var.3, the area increasing ratio is small when the storage element is enlarged directly. The Var.2 is chosen for area reduction by enlarging the storage element, finally. The capacity of the content is 60 with two blocks, as shown in Var.4 of Fig. 2(B). As the post-layout simulation indicates, The SRA ASIC operates at 435 MHz to 513 MHz and the minimal chip area of Var.1 to Var.4 is $1.94 \times 1.96 \text{ mm}^2$.

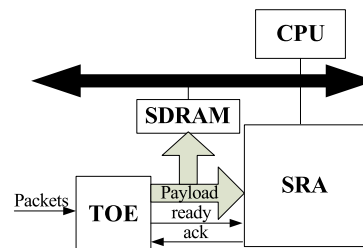
We design the SRA with 32 bits system so that the throughput of ASIC is 13.9 Gbps. With the state of the art in VLSI technology, the TCP/IP offload engine (TOE) has been proposed with 10 Gbps throughput. The DDR3-1600 and DDR3-1866 SDRAM are with 12.8 and 14.9 Gbps throughput. To model system throughput, the system design is evaluated as shown in Fig. 2(C). The Snort rules databases are loaded from memory to contents of SRA initially. The packet from the network is received by network interface card (NIC) of TOE and then the payload of packet is send to SRA through GMII interface. The SDRAM memory plays the role of packet buffer between TOE and SRA. The dual port memory achieves pipeline operations with packet receiving and rule pattern matching. Therefore, the SRA ASIC can deal with the throughput requirement of traffic from the network. And the database access from memory is also with high throughput. Table I shows the comparison of our system with those of related designs. Our proposed SRA system performs the highest system throughput for the pattern matching of the application rules. The key module of the SRA is the register with 3.3 K Snort rules. And the others are the bloom filter, TCAM and FSM. The proposed SRA system exhibits not only a low false positive characteristic without off-chip memory support but also achieves highest system throughput.



(A) The layout of SRA ASIC.

SRA block	Var.1	Var.2	Var.3	Var.4
Block Content	10	20	10	30
	10	20	10	30
	10	20	10	30
	10	20	10	30
Block Area	2164 cell	2726 cell	3267 cell	3375 cell
64 block content	1.28K	2.56K	2.56K	3.84K

(B) The comparison of chip area.



(C) The evaluation of system.

Fig. 2. The layout of SRA ASIC and the comparison of chip area

Table I. Comparison results with others works

Design	Song [1]	Wang [2]	Lin [3]	Proposed
Key module	Bloom Filter	TCAM	FSM	Half mesh
Application rules	2.6 K Snort rules	30 K ClamAV	2.2 K Snort rules	3.3 K Snort rules
Throughput (Gbps)	10	3	4	13.9
False positive	High	-	Normal	Low

5 Conclusion

The Snort IDS is widely used for personal computers or servers. Several studies focused on Snort; however, real ASIC implementation is limited. In this paper, we have proposed a parallel matching architecture and implemented the system as an ASIC to accelerate the Snort IDS. The SRA ASIC performs parallel matching for the Snort rule. With the counter design, the system compares the content range bytes with the whole payload. Web pages and e-mail are protected in the SRA system. We compared four types of design to reduce the chip area. As the post-layout simulation result indicates, the ASIC operated at 435 MHz and the system achieved throughput of 13.9 Gbps. Therefore, the SRA accelerates the Snort system to manage the requirements of high speed and high accuracy features for 10 Gbps core network traffic.