VHDL based Packet Classification Architecture for Firewall and Network Security

Farha Sabir
M. Tech Student
Department of Electronics & Telecommunication Engineering
Nuva College of Engineering & Technology Nagpur, Maharashtra, India

Prof. Mrs. Pooja Thakre
Head of Dept.
Department of Electronics & Telecommunication Engineering
Nuva College of Engineering & Technology Nagpur, Maharashtra, India

Abstract

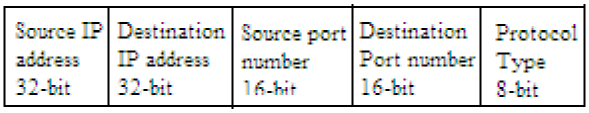
Packet Classification is a crucial function used in an internet router, firewall, network security and quality of services. Packet classification technique is very crucial since various unauthorized and malicious networks are being exposed to. For secure networking and avoiding unauthorized access, incoming packets flow based on predefined rules available in a classifier. Available software solution's performance is not efficient for wire speed processing in high speed networks. To meet the line-card requirement and wire speed processing hardware solution is more efficient and secure than software solution. For implementing hardware architecture for wire speed processing different algorithms have been proposed. This paper presents review on different algorithm and technique used to implement packet classification architecture. High performance packet classification architecture can be implemented using Field programmable gate array (FPGA) and large number of rules can be stored using on-chip memory resource of FPGA.

Keywords: Packet classification, 5-tuple, Quality of services, latency, throughput

I. Introduction

Modern packet processing system uses technique known as packet classification in place of de-multiplexing due to various advantages like high speed and ability to cross multiple layers. Various services like firewalls, Virtual Private Network (VPN), network security, policy-based-routing, traffic shaping and Quality of Services (QoS) require packet classification. This makes packet classification an integrated part of network intrusion detection system (NIDS). To access various services, it is required to figure out which rule matches with incoming packet and depending on it necessary action is taken. In other words, flows are decided by rules applied to incoming packets and each rule in a rule-set specifies a flow to which a packet may belong based on values in header fields.

Packet classification process involves inspection of multiple fields against a rule-set may be containing thousands of rules. This is one of the challenge and difficulty in the process of classification. Each rule in a classifier has a priority and action is taken according to their priority. Basic 5-tuple are present in the standard packets header which include destination and source IP address field, destination and source port number field and the protocol type field as depicted in figure.1. For different combination of values of the fields require different matches like prefix match for destination and source IP address field , range match for destination and source port field and exact match for protocol field. For better performance, packet classification system must support all the type of match.



Source IP address 32-bit	Destination IP address 32-bit	Source port number 16-bit	Destination Port number 16-bit	Protocol Type 8-bit

Fig. 1: Standard 5-tuple packet header fields

Considering the fact that packet classification system is the central part of firewalls, internet routers and various intrusion detection systems. Various packet classification algorithms have been proposed to perform packet classification; just because of special computational method most of the existing algorithms may not be suitable for hardware implementation. The main performance metrics that should be taken into an account while designing algorithms for implementing hardware packet classification system are as follow:

- Memory requirement: memory requirement for storing number of rules is limited in hardware solution. The on-chip SRAM of FPGAs can be used to store large number of rules.
- Multi match classification: packet classification algorithm should support exact match, prefix match and range match. It should also avoid the use of prefix to range match conversion which is memory inefficient.
- High speed: algorithm must meet the in-line requirement of 100/200/400 Gbps while supporting large number of rules.

- Update, modify and delete rules: Dynamic modification, updating and removing of out-dates rules is required for supporting various new applications.
- Latency: low latency application requires parallel orientation in cost of memory while in some application series orientation is feasible. It is important that algorithm should be flexible in orientation for supporting all types of application.

Above performance matrices are very crucial while designing hardware packet classification architecture to avoid degradation of performance of the architecture. However, performance of architecture depends on an algorithm used for designing it**.**

II. DETAIL STUDY ON PACKET CLASSIFICATION TECHNIQUE

From literature survey and review of related work, it is observed that researchers have designed the packet classification architecture using algorithms based on these four methods: exhaustive search, decision tree based, tuple search and decomposition based method. Decision tree based approach and decomposition based approach are desirable for hardware implementation of packet classification system. Efforts have been undertaken by researchers for designing of multi-match packet classification architecture for firewalls and all type of intrusion detection systems. Researchers put their best to implement hardware solution for packet classification.

For one-dimensional packet classification, Ternary Content Addressable Memory (TCAM) is the desirable hardware solution because of its simple management and speed. To check all fields at a time and at high speed, TCAM based search engine is used. For multi-dimensional packet classification using TCAM, Yeim-Kuan Chang and Cheng-Chien Su have proposed an efficient range-encoding Scheme for Packet Classification using Gray code [3]. Experimental result’s shows the proposed binary reflected gray code-based (BRGC) encoding scheme requires less TCAM storage than parallel packet classification encoding (PPCE) scheme. The BRGC based encoding scheme is proposed for range values of source and destination port number but it is also used for source and destination address field of packets having prefix addresses. Problems like limited scalability and the range to prefix blowout for large number of rule-set have solved using BRGC based encoding scheme.

Lu Sun, Hoang Le, Viktor K. Prasanna have proposed optimizing decomposition-based packet classification on FPGA [4]. Decomposition-based IP classification algorithms consist of two phase: in first phase, independent searches are performed on each field of packets, while in second phase: results from the first phase are combined. Due to limited resources and limited on-chip memory on FPGAs, the second phase of the decomposition based algorithms become challenging. To solve this problem, they have proposed a systolic-array-based architecture which efficiently combines the results of the first phase in the second phase. The proposed architecture on set intersection and compact representation of matching rules yields better performance in second phase of the algorithm. The design is more efficient, feasible and attractive in logic resources, in handling large rulesets and in area than any other decomposition based algorithm. The proposed architecture has implemented on Xilinx Virtex-6 XC6VLX760 with -2 speed grade as a target in Verilog using Xilinx ISE 12.4 tool. The implemented design achieves high throughput of 107 Gbps while supporting rules upto 64K of minimum packet size of 80 bytes**.**

Weirong Jiang and Victor K. Prasanna have introduced Field-Split Parallel Bit Vector (FSBV) based architecture [2]. The FSBV architecture is suitable for Snort rule and it is a novel SRAM-based architecture which exploited the use of BlockRAMs of current FPGA. It supports multi match packet classification and also handles the negation and value list problem. The architecture is memory efficient because range to prefix conversion is not used for range values. Proposed architecture used TCAM algorithm for source and destination address fields, CAM algorithm for protocol field and Bit Vector (BV) algorithm for source and destination port fields. The FSBV architecture achieved clock frequency of 167 MHz and processed two packets every clock cycle with the use of dual-port RAMs on a Xilinx Virtex-5 XCVFX200T device. Using SRAM-based architecture and low memory requirement, one fourth power reduction can be achieved over BV-TCAM.

Researchers have developed various software solutions for packet classification, but hardware solutions yield high performance and supports dynamic updates. Yun R Qu, Shijie Zhou, and Viktor K. Prasanna have proposed a high performance 2-dimensional pipelined architecture for packet classification on FPGA which supports dynamic updates of rules [6]. The proposed architecture consists of self-reconfigurable processing elements. A modular processing element (PE) can handle range match as well as prefix match and does not need range to prefix conversion. Multiple modular processing elements (PEs) are used in the architecture to construct a 2-dimensional architecture for handling large number of rules. Striding and clustering technique is used in the implemented architecture to vary size of sub-field and number of rules. The architecture can perform packet classification of s-bit subfield against a set of n rules using striding and clustering technique. A set of algorithm supports modification, deletion and insertion operations on the proposed architecture. Dynamic updatable of rules on hardware is possible without deteriorating the pipeline performance. The architecture is scalable with respect to large input length. The Proposed architecture maintains very high clock frequency of 324 MHz and can achieve throughput of 190 Gbps with 1K 15-tuple rule-set on Virtex-6 XC6VLX760 FFG1760-2 FPGA device.

A scalable and modular architecture for high performance packet classification have been proposed by Thilan Ganegedara, Weirong Jiang, and Viktor K. Prasanna [1]. They have proposed a novel modular Bit-Vector based architecture on field programmable logic array (FPGA) using StrideBV algorithm. Range integration search in the architecture avoids the use of range-to-prefix conversion and supports all type of match. The architecture is scalable on hardware and pipelined priority encoder is used for extracting highest priority match. Proposed serial and parallel versions of StrideBV based architecture are ruleset-feature independent solution. Their solution is flexible in orientation depending on an application and latency requirement. Proposed architecture is memory efficient, achieves 100+ Gbps throughput while supporting upto 28K rules using only on-chip resources on a state-of-the-art Xilinx Virtex-7 2000T FPGA device and evaluates the performance of both serial and parallel version of strideBV using post place-and-route results.

III. Our proposed work

StrideBV is the one of the efficient decomposition based packet classification technique which supports hardware implementation. StrideBV algorithm achieves low latency and sustains high throughput than any other existing technique. However, it is not memory efficient technique for large number of rules which is the major drawback of this technique. Because of all the above reasons, in this paper we presented our proposed method which classify a packets using XNOR gate. Our proposed method is memory efficient and can achieve low latency for same number of rules than StrideBV.

In our work we use 512 rules of ternary string format having values in '1', '0' and '-'. In strideBV, lookup table indicates status of rules. A look-up table is stored in a memory having depth (height) of 2^k and entry (width) in each row is equal to number of rules (N). An incoming stride extracts N-bit vector from the corresponding memory location. An N-bit vector from corresponding memory location contains matching result of rules with incoming stride. The memory required in this method is generally depends on number of rules and stride size. The priority encoder is used to select incoming stride for highest priority rule. The register transfer level view of priority encoder is depicted below in fig. 2.

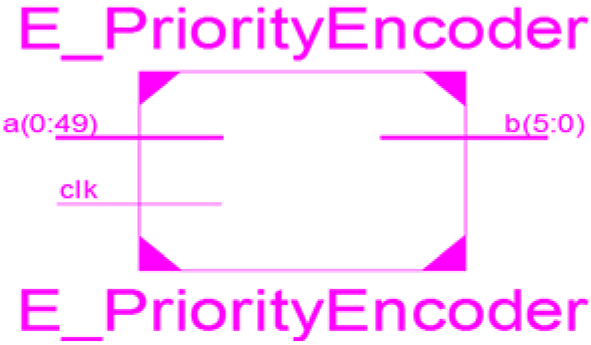


Fig. 2: RTL View of Priority Encoder

In proposed work, we use basic XNOR gate for matching incoming packets against a set of rule and produce bit vector of same size as that of rule and then ANDed all bits of match result and produce one bit for each rule. Each bit after ANDing operation gives status of incoming packet against each rule of the rule-set. For selecting highest priority rule from the rule-set, priority encoder is used. Technology schematic view of proposed work is shown in fig. 3. For same number of rules our proposed method of packet classification is memory efficient because each rule in our proposed work require only 32 bit whereas in strideBV each rule requires 2^32 bit for lookup table.

We have designed and optimized the proposed method in VHDL using Xilinx ISE 13.1 tool. We select Spartan6 as a family and 6slx4tqg144-3 as target device for performing synthesis and optimizing the design using Xilinx tool. Simulation results are shown in next section to check the functionality of designed module of packet classification.

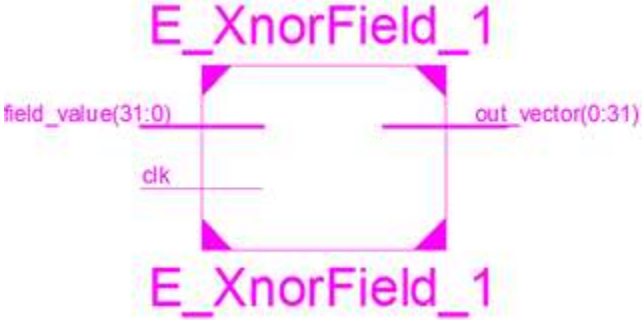


Fig. 3: RTL View of Xnor Based Packet Classification

Simulation Result

Fig. 4 shows simulation result of priority encoder for input of 32-bit and output will be the highest match. Here, MSB has highest priority whereas LSB has lowest priority. It means rules should be arranged in descending order of their priority.

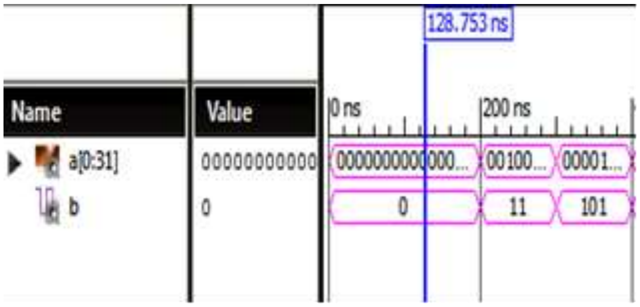


Fig. 4: Simulation Result of Priority Encoder

Fig. 5 shows simulation result of Xnor based packet classification where input packet is of 32-bit and output is a vector which indicates match and mismatch of rule against predefined ruleset. From simulation results it is cleared that we get output in one clock cycle. Pipelining stages are not used in this design to get less latency and also lookup table is not used to minimize the memory cost.

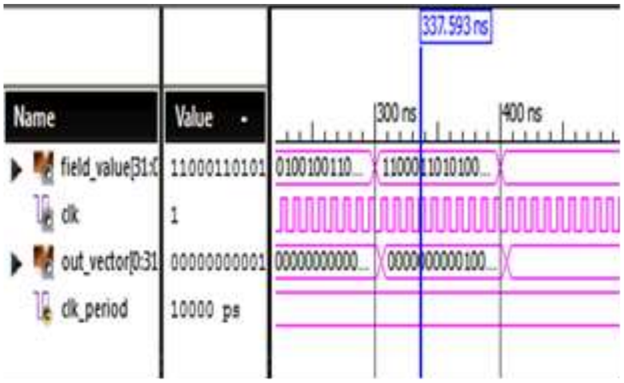


Fig. 5: Simulation Result of Packet Classification

IV. CONCLUSION

Our proposed method of packet classification is latency and memory efficient as compared to strideBV algorithm. Latency achieved in proposed work is one clock cycle which is better as compared to strideBV for same rule-set. Memory required to represent one rule in the proposed work is less which has overcome the major bottleneck of hardware solution. In future we can implement the packet classification architecture for complete packet header field.

REFERENCES

[1] Thilan Ganegedara, Weirong Jiang, and Viktor K. Prasanna, Fellow, IEEE; "A Scalable and Modular Architecture for High-Performance Packet Classification"; IEEE Transactions on Parallel And Distributed Systems, Vol. 25, No. 5, May 2014; 1045-9219 _ 2013 IEEE, Pp.1135-1144)

[2] J W. Jiang and V. K. Prasanna, "Field-split Parallel Architecture for High Performance Multi match Packet Classification using FPGAs," in Proc. of the 21st Annual Symp. on Parallelism in Algorithms and Arch. (SPAA), 2009, pp. 188–196.

[3] Yeim-Kuan Chang and Cheng-Chien Su, "Efficient TCAN Encoding Scheme Packet Classification using Gray Code," in IEEE GLOBECOM 2007 proceedings @2007 IEEE.

[4] Lu Sun, Hoang Le, Viktor K. Prasanna; "Optimizing Decomposition-based Packet Classification Implementation on FPGAs"; 2011 International Conference on Reconfigurable Computing and FPGAs; 978-0-7695-4551-6/11 $26.00 © 2011 IEEE; pp. 170-175

[5] Andrea Sanny, Thilan Ganegedara, Viktor K. Prasanna; "A Comparison of Ruleset Feature Independent Packet Classification Engines on FPGA; 2013 IEEE 27th International Symposium on Parallel & Distributed Processing Workshops and PhD Forum", 978-0-7695-4979-8/13 $26.00 © 2013 IEEE

[6] Yun R. Qu, Shijie Zhou, and Viktor K. Prasanna; "High- performance architecture for dynamically updatable packet classification on FPGA," Architecture for Networking and communication systems (ANCS), 2013 ACM/IEEE Symposium on @ 2013 IEEE, pp. 125-136

[7] Pankaj Gupta and Nick Mckneown; "Algorithms for packet classification" in IEEE magazine, March/April 2001 pp. 24-32

[8] Hung-Yi Chang, Chia-Tai Chan, Pi-Chung Wang, Chun-Liang Lee; "A Scalable Hardware Solution for Packet Classification," in ICCS @2004 IEEE.

[9] Mahmood Ahmadi, S. Arash Ostadzadeh, and Stephan Wong; "An Analysis of Rule-Set Databases in Packet Classification,"

[10] Nekoo Rafiei Karkvandi, Hassan Asgharian, Amir Kusedghi, Ahmad Akbari, "Hardware Network packet Classifier for High Speed Intrusion Systems" ;International Journal of Engineering and Technology; Volume 4 No.3, March, 2014.

[11] Safaa O.Al-Mamory and Wesam S.Bhaya; "Taxonomy of Packet Classification algorithms", Journal of Babylon University/Pure and Applied Science/No.(7)/Vol.(21):201.