Design of High Performance Packet Classification Architecture for Secure Communication Networks Using VHDL

[1]Faraaz Rana Siddiqui, [2]Somiya Pathan, [3]Sunidhi Bopte, [4]Vaishanvi Joglekar, [5] Prof. Rahil Khan

[1, 2, 3, 4]B.E Student, [5]Assistant Professor

[1]Department of Electronics and Telecommunication Engineering,

[1]Anjuman College of Engineering and Technology, Nagpur, India

[1]faraazranasiddiqui@gmail.com, [2]somiyakhan00@gmail.com, [3]sunidhibopte007@gmail.com, [4]vaishnavijoglekar25@gmail.com, [5]rahil_hkhan@yahoo.co.in

***Abstract*— Packet classification is a crucial technique for secure communication and networking. Security tools and internet services use packet classification technique which involves checking of packets against predefined rules stored in a classifier. Performance of the available software solutions of classification is not desirable and efficient for wire speed processing in high speed networks. Ternary Content Addressable Memory (TCAM), Bit-Vector (BV), field split bit vector (FSBV) and StrideBV algorithm are hardware based packet classification algorithms. In this paper, we have proposed simple and memory efficient approach for packet filtering using Xnor gate instead of using lookup tables called XnorBV approach. Packet header fields of Internet protocol (IP) addresses and protocol layer are classified using Xnor gate against predefined ruleset which also support ternary bit pattern of '1', '0' and '*' while port numbers of packet header support range match by comparing port numbers against lower bound and upper bound. Our proposed parallel pipelined architecture can sustain a high throughput of +100 Gbps and low latency. Proposed method is memory efficient than other existing techniques, also supports prefix, range and exact match without use of range to prefix conversion. Also proposed XnorBV architecture is independent of ruleset feature and supports multiple dimension classification.**

***IndexTerms*—firewall; network intrusion detection system; packet classification; quality of services.**

I. INTRODUCTION

A sequence of packets coming from the source system to a destination system is popularly label as traffic flow or packet flow and a sequence of packets from particular source to a particular destination is called a flow. A flow can be identified by using technique called packet classification which categorizes the incoming packets into different flow by inspecting values of header fields of packets within a certain time [1]. For identification and arranging packets into different flow, each incoming packet is checked against a set of rule [2], if an incoming packet is matched with any rule of a rule-set then only it is accepted otherwise rejected. After categorizing incoming packets into different classes, each flow can be processed differently to differentiate the services suggested for the user. Each application and service requested by the user requires packets of same class. Packet classification technique helps to provide respective packets to respective services efficiently using predefined rule-set. Also, various services like firewalls, Virtual private network, network security, policy-based-routing, traffic shaping and quality of services incorporated the packet classification technique to detect threats and to prevent unauthorized access to the network [3][4]. Due to these manifold advantages of packet classification technique in modern communication, packet classification has become an integrated part of all type of intrusion detection systems, firewalls, internet routers and virtual private networks[5].

Software solutions are available to perform classification of packets but they are insufficient for high speed network applications [4]. In software tools, classification is generally done by checking only port numbers or IP addresses or protocol layer. Performance of software solutions which support inspection of multiple fields is not desirable for wire speed processing. For wire-speed processing and secure networking, hardware solutions are desirable and classification of packets can be done by checking all fields of packet header. In hardware packet classification solution, multiple fields of an incoming packet are checked against each rule of a rule-set. A size of ruleset may vary from hundred to thousand rules. The challenge and difficulty for hardware implementation of packet classification system is memory requirement to store large number of rules [2]. Each rule in a classifier is stored in a decreasing order of their priority and action is taken according to their priority. Figure.1 depicted below shows a standard 5-tuple packet header having destination and source Internet Protocol (IP) address field, destination and source port number field and the protocol field [3]. For different combination of values of the fields require different matches like prefix match for destination and source Internet Protocol address field, range match for destination and source port field and exact match for protocol field.

Source IP address	Destination IP address	Source port	Destination port	Protocol

Figure1: Standard 5-tuple packet header

Considering the fact that packet classification system is the central part of various security tools and applications over internet and computer systems [6]. Various packet classification methods have been proposed to perform classification of packets just because of special computational method and certain limitations most of the existing technique may not be suitable for hardware implementation. The main performance metrics that should be taken into an account while designing algorithms and architecture for implementing hardware of packet classification system are summarized below [3] [4] [7]:-

- Memory requirement: memory requirement for storing number of rules is limited in hardware solution. The on-chip static random access memory of field programmable gate arrays (FPGA) 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.
- Latency: low latency application requires parallel orientation while in some application series orientation is feasible. It is important that algorithm should be flexible in orientation for supporting all types of applications.

II. Problem In Packet Classification

Important issue of packet classification architecture is Power consumption. As throughputs of trillions of bits per second achieved by routers, power consumption becomes an increasingly critical concern. Power efficiency depends on number of rules used to classify incoming packet. This is one of aspect used for evaluation of power efficiency of packet classification system. The power consumed by the router to drive away the extremely large heat created by the router components extensively assist to the operating costs [8]. The power consumption in search engines is becoming an increasingly important evaluation parameter because each port of routers contains packet classification devices and router lookup [4].

Memory requirement is another important issue of packet classification. Nowadays, researchers aim to find out solutions for large ruleset. Method of classification and number of rules stored in classifier is related to amount of memory required. Due to limited resources available on FPGA, memory has become very important issue of hardware solution to support large number of rules [9].

Speed and pliability in specifications is another issue in packet classification devices. In packet classification process, packets are categorized based on a set of predefined rules also called as packet filters. Rules or filters define patterns that are to be matched against incoming packets for arranging packets for different flows [6] [10]. Packet filters or rules specify possible values for each field of a standard 5–tuple packet header [8] [11]. The address fields of a packet header are often used prefixes to define the addresses, although in address fields arbitrary bit masks are acceptable in a classifier or ruleset and this feature is widely used in real filter sets. Rules or Filters specify a range value for port -fields of packet header for matching incoming packets. Protocols can be in two ways either exact value or as a wildcard. Values specified by bit masks are allowed in some system for protocol field of incoming packet, even if it's not clear how convenient that feature is [8][12].

III. Proposed Work

In this work, we performed classification of each field or tuple of incoming packet using Xnor gates instead of using look-up tables called XnorBV. A XNOR gate can be used as basic comparator for comparing two bits to make the architecture simple and efficient. Using Xnor gate, the proposed design achieves good results on same operating platform with frequency of 300MHz. Each field of a packet header generates a bit vector which will be ANDing with bit vector generated by others' field to get final result. In our proposed method, we performed checking of each bit of a field against each bit of a rule stored in a ruleset. Using behavioral modeling of VHDL, our design supports ternary bit format of '1', '0' and '*' (wildcard entry). Our proposed method illustrated in figure.2, same ruleset and field value=1101 is used as that of Field split bit vector (FSBV) and StrideBV. After XNORing operation, each bit of obtained output after XNORing is ANDing to get one bit which indicates the status of a rule for incoming packet field [5]. A 5-tuple standard packet header having five fields which are source Internet Protocol (IP) address, destination Internet Protocol (IP) address, source port number, destination port number and protocol layer. We have performed the classification of IP address fields and protocol field using Xnor gate i.e. using XnorBV method. We can use XnorBV module for source Internet Protocol (IP) address (32 bits), destination Internet Protocol (IP) address (32 bits) and protocol field (8 bits). Proposed XnorBV module supports prefix and exact match for Internet Protocol (IP) addresses and protocol layer respectively.

A field of 5-tuple incoming packet is checked against N rules of a ruleset. To understand the generation of bit vector using XnorBV method with the help of circuit diagram, let the length of rule and a field of an incoming packet is k bits. Let the first rule of a ruleset is given by $R1=W_{k-1}W_{k-2}\ldots\ldots W_0$ and a field of an incoming packet is given by $F1= T_{k-1}T_{k-2}\ldots\ldots T_0$. Each bit of a rule and a field is XNORing and after completion of XNORing operation, result of k-bits is ANDing to get single bit indicating the matching or mismatching of field with a rule. Same operation is performed for each and every rules of a ruleset of size N to get N-bit vector for the particular field of a packet.

To support range match for port numbers, we compared the field value against lower bound and upper bound value. Figure.3 shows the range module to perform range match for port numbers. For range match we have to define two values i.e. lower bound and upper bound as shown in figure.3. We defined ruleset set containing lower and upper bound and assume field value = 1000. In this work, field value is to compare against lower bound, if field value is greater or equal to lower bound then it gives '1' otherwise '0' similarly if a field value is lower than or equal to upper bound then it gives '1' otherwise '0'. Bit values obtained after comparing field value against lower bound and upper bound are ANDing to get one bit which indicates that field value is lying in the range of lower bound and upper bound. Range search module can support source port number and destination port number each of 16 bits. Our method supports prefix match for IP addresses, range match for port numbers and exact match for protocol field. Our architecture is independent of ruleset feature and supports multiple dimension classification.

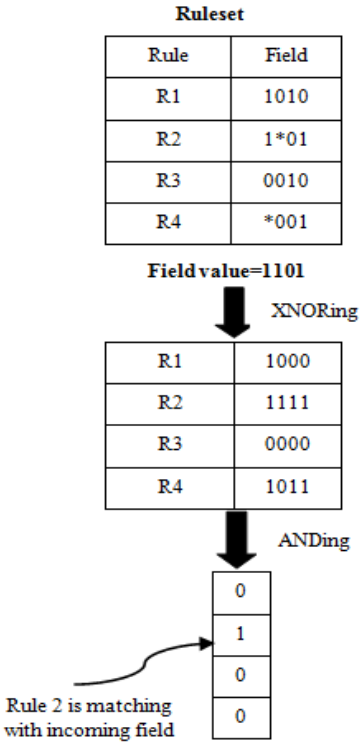

Figure2: Proposed XnorBV Algorithm

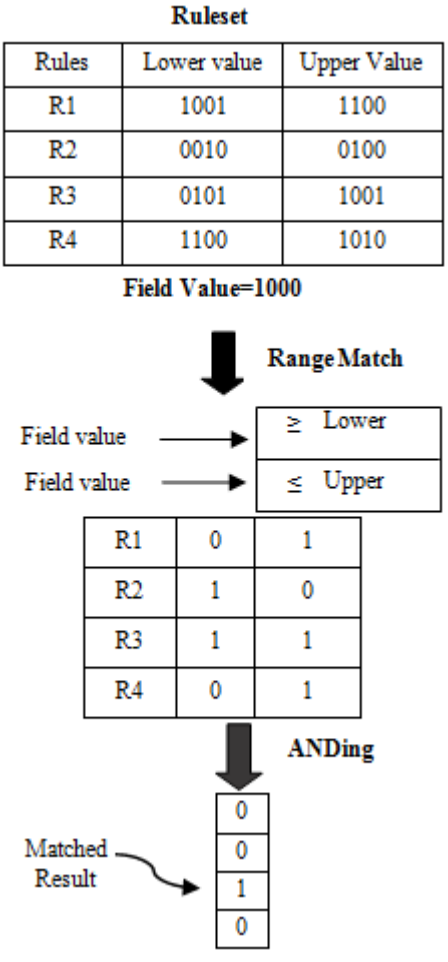

Figure3: Range Search Module for Range Match

IV. CONCLUSION

Proposed method XnorBV architecture using Xilinx ISE 13.1 suite selecting Virtex 6 XC6VLX760 as target device is memory efficient requires 15 byte/rule less than any other existing technique of packet classification. Architecture supports prefix, exact and range match without use of range to prefix conversion and is independent of ruleset feature. Power efficiency is also improved with power increment in addition of one rule. Proposed architecture can sustain high throughput of +100 Gbps at low latency which is desirable for low latency applications.

REFERENCES

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

[2] T. Ganegedara and V. Prasanna, ''StrideBV: 400G+ Single Chip Packet Classification,'' *in Proc. IEEE Conf. HPSR*, 2012, pp. 1-6.

[3] Mahmood Ahmadi, S. Arash Ostadzadeh, and Stephan Wong; "An Analysis of Rule-Set Databases in Packet Classification," in *18th Annual Workshop on Circuits, Systems and Signal Processing (ProRISC 2007), 29-30 November 2007, Veldhoven, The Netherlands.*

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

[5] Ausaf Umar Khan, Yogesh Suryawanshi, Dr. Manish Chawhan, Sandeep Kakde, "Design and Implementation of High performance Architecture for Packet Classification," in *International Conference on Advances in Computer Engineering and Applications,* IMS Engineering College, Ghaziabad, India, page 598-602, IEEE.

[6] Aladdin Abdulhassan and Mahmood Ahmadi, "Parallel Many Fields Packet Classification Technique using R-Tree ," in *Annual Conference on New Trends in Information & Communications Technology Applications-(NTICT'2017),* 7-9 March 2017.

[7] Safaa O.Al-Mamory and Wesam S.Bhaya; "Taxonomy of Packet Classification algorithms," in *Journal of Babylon University/Pure and Applied.*

[8] Balasaheb S. Agarkar and Uday V. Kulkarni, Ph.D., "A Novel Technique for Fast Parallel Packet Classification," in *International Journal of Computer Applications (0975 – 8887)* Volume 76–No.4, August_2013.

[9] Andreas Fiessler, Sven Hager and Björn Scheuermann, "Flexible Line Speed Network Packet Classification Using Hybrid On-chip Matching Circuits," in *IEEE 18th International Conference on High Performance Switching and Routing (HPSR),* 18-21 June 2017.

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

[11] G. Jedhe, A. Ramamoorthy, and K. Varghese, ''A Scalable High Throughput Firewall in FPGA,'' in *Proc. 16th Int'l Symp. FCCM.* Apr. 2008, pp. 43-52.

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

[13] M. Faezipour and M. Nourani, ''Wire-Speed TCAM-Based Architectures for Multimatch Packet Classification,'' in *IEEE Transactions on Computers,* vol. 58, no. 1, pp. 5-17, Jan. 2009.

[14] D.E. Taylor, ''Survey and Taxonomy of Packet Classification Techniques,'' in *ACM Computing Survey*, vol. 37, no. 3, pp. 238-275, Sept. 2005.

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

[16] W. Jiang and V. K. Prasanna, "Field-split Parallel Architecture for High Performance Multi match Packet Classification using FPGAs," *in Proc. of the21st Annual Symp. on Parallelism in Algorithms andArch. (SPAA)*, 2009, pp. 188–196.

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

[18] C.R. Meiners, A.X. Liu, and E. Torng, "*Hardware Based Packet Classification for High Speed Internet Routers,*" Berlin, Germany: Springer-Verlag, 2010.

[19] Cheng-Liang Hsieh and Ning Weng, "Many-Field Packet Classification for Software-Defined Networking Switches," *in @ACM 2016 , ANCS '16,* March 17-18, 2016, Santa Clara, CA, USA.

[20] H. Song and J.W. Lockwood, ''Efficient Packet Classification for Network Intrusion Detection Using FPGA,'' *in Proc. ACM/SIGDA. 13th Int'l Symp. FPGA*, 2005, pp. 238-245

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

[22] D. Taylor and J. Turner, ''Scalable Packet Classification Using Distributed Crossproducing of Field Labels,'' in *Proc. 24th Annu. Joint IEEE INFOCOM,* Mar.2005, vol.1, pp.269-280

[23] C.A. Zerbini and J.M. Finochietto, ''Performance Evaluation of Packet Classification on FPGA-Based TCAM Emulation Architectures,'' in *Proc. IEEE GLOBECOM,* 2012, pp. 2766-2771.

[24] Weirong Jiang and Viktor K. Prasanna, "Large-Scale Wire-Speed Packet Classification on FPGAs," in *ACM*, 2009.