© 2018 IJSRST | Volume 4 | Issue 5| Print ISSN: 2395-6011 | Online ISSN: 2395-602X
Themed Section: Scienceand Technology

Packet Classification Using Bit-Vector Algorithm In Network And Security Systems

P.AmruthaVarshini[1] ,Dr.R.Murugadoss[2]

[1]PG Scholar, Department of MCA, St.Ann's College of Engineering&Technology, Chirala, Andhra Pradesh, India

[2]Professor, Department of MCA, St.Ann's College of Engineering& Technology, Chirala ,Andhra Pradesh,India

ABSTRACT

Packet classifiers are exhaustively engaged for various network models in distinctive types of network system such as Firewalls and Router. Comprehending the actual accomplishment of endorsed packet classifiers is essential for both algorithm designers as well as clients. We employ capabilities is verification and take new authorization in the communications. All these innovations make packet classification owning good effects in attacking scenario. We develop two efficient GPGPU based parallel packet classification method to filter packets by leveraging thousands of threads. The expeditious improvement of hardware architectures and burgeoning popularity of multi core multi threaded processors decision tree based packet classification algorithms such as Hi Cuts and Hyper Cuts are grabbing considerable attention outstanding to security in satisfying miscellaneous industrial requirements for network and security systems. We propose a new packet classification to supports high scalability and fast classification results by using Bloom Filter. Bloom uses to sustain high throughput by using Longest Prefix Matching (LPM) algorithm. We propose a methodology is enables linear search based systems with jump semantics to take advantage of the superior matching performance of decision tree algorithms without the need to touch the underlying system implementation. A high speed packet classification based on Bit-Vector (BV) based architecture implemented on FPGA (Field Programmable Gate Array) is proposed stride BV is the algorithm introduced modularized to achieve better scalability than BV traditional methods. The performance of the packet classification subsystem is of paramount importance for the collective success of the network routers.

Keywords: Packet Classification; Decision Tree Algorithms, Network Security; Capabilities; Filter, TSS; Bit Vector; Hyper Cuts; Hi Cuts; Dim Cut, Intrusion Detection, High Speed Networks, Distributed Architecture, Scalability.

I. INTRODUCTION

Large security packet classification has become a key element of network security systems and Firewalls needing to classify packets speed of decision making, to accept is of utmost significance [1]. We have elucidated our erstwhile recommended Dim Cut packet classification algorithm, and compared Dim Cut with the TSS, Hi Cuts, Hyper Cuts, Woo and BV decision tree based packet classification algorithms [2]. The proposed improvements are corroborated by simulated trials [3]. Among most existing packet classification schemes the rule is often defined as a 5-tuple (SrcIP, DestIP, SrcPort, DestPort, Protocol). A lot of schemes is packet classification is proposed during the last decade [4]. Packet analysis is at the core of timely detection and typically relies on a packet filtering system. Packet filtering system drops the packets if packets match to the filter rules [5]. Packet filter system also has been applied to many

network intrusion detection systems (NIDS) as the first stage [6]. The algorithm should also support table sizes and high-speed table updates. Generally, packet classification algorithms use complex and large internal tables to magnify classification performance and the size of the tables grows exponentially with the size of the rule sets [7]. We take a different and indeed very pragmatic the boost the performance of linear search classification engines without the need to modify the implementations of the underlying matching algorithm [8]. We show that this is possible by building upon the jump ability that is present in many such classification engines [9]. The output of hardware based routers can be dramatically increased by employing pipelining techniques. Packet classification performs searching the table of filters to assign a flow identifier for the highest priority filter that matches the packet in all fields [10].

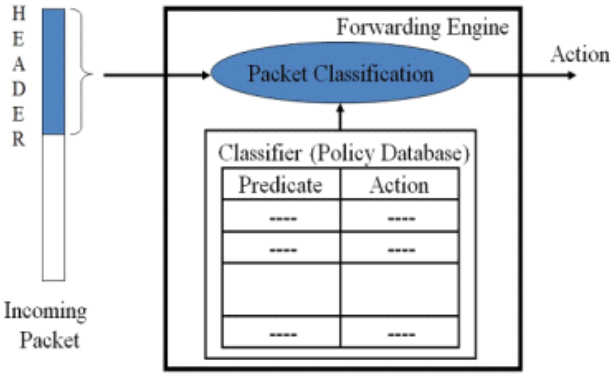

Figure 1. Packet Classification

II. RELATED WORK

A packet classifier must correlate header fields of all incoming packets against a set of rules containing the security policies. Packet classification aims at pursuing the best matching filter for a given packet header when the number of rules increases, the result is inadequate either towards search time or memory usage [10]. The commonly used and most reliable methods of classifying packet data are exhaustive search algorithms which compare packets against each and every filter in the filter set until a exact match is found [11]. It should cover the features like, support general rules which includes prefixes, range, exact values, wildcards, better data structures to rule bases, multiple matches and preprocessing [12]. Packet classification algorithms are classified according to their implementation or characteristic types. We divide algorithms into non-partitioning and partitioning types according to the accepted partitioning techniques [13]. There exist online and offline variants of such rule set modification schemes. Online rule set modification observes the matching behavior at runtime, and continuously adjusts the data structures such that highly frequented rules can be found more quickly [14]. Offline rule set modification typically aims to reduce the number of rules. This can happen either by detecting and removing redundant rules. In this case a traffic duplicator is then used to send every packet to every sensor. Each sensor performs quick check of every packet to determine if the sensor contains a rule associated with the given packet. If so, the sensor would process the packet, otherwise it would drop it [15].

III. SECURE PACKET CLASSIFICATION

The packet classification uses the capabilities marking at the network layer, and is deployed on key routers. The security of the packet classification is determined by the capabilities' feature against cyber attacks, which prevents the transmission of unauthorized data [16]. Thus the main function of packet classification is to classify the traffic produced by coordinated attacks the process of the packet classification the routers make decisions according to the actual requirements of service differentiation [17]. If the packet classification plays single defense function, the routers perform classifications of malicious and legitimate packets. Otherwise the routers need to perform additional service classification operations, according to the packets' header. For instance the Hi Cut. Presently RFC algorithm is generalization of cross-producing is the fastest classification algorithm in terms of the worst-case performance. Bitmap

compression has been used in IPv4 forwarding and IPv6 forwarding it is applied to classification to compress redundant storage in data structure [18].

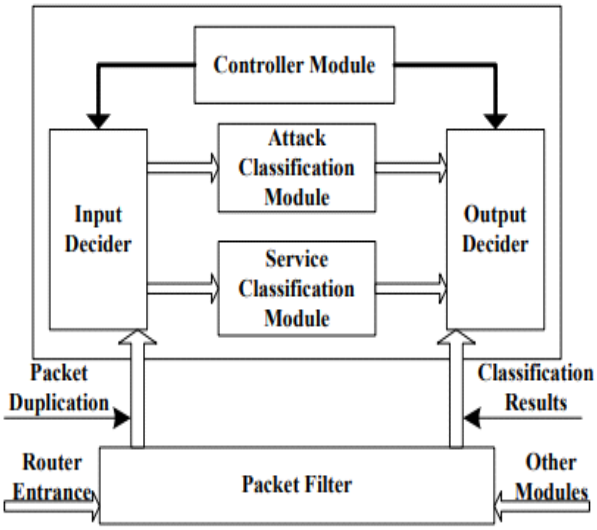

Figure 2. The Framework of PCFC

IV. CUDA PROGRAMMING MODEL

As the GPU has become increasingly more powerful and ubiquitous researchers have begun developing various non-graphics. GPUs are organized in a streaming, data parallel model in which the co-processors execute the same instructions on multiple data streams simultaneously [19]. The Compute Unified Device Architecture (CUDA) SDK to as sits developers in creating non-graphics applications that runs on GPUs. A CUDA programs typically consist of a component that runs on the CPU and a smaller but computationally intensive component called the kernel that runs in parallel on the GPU [20]. Input data for the kernel must be copied to the GPU onboard memory from host main memory through the PCIE bus prior to invoking the kernel, and output data also should be written to the GPU's memory first before copying to host's main memory. All memory used by the kernel should be pre-allocated [21]. Different to previous two memory transfer models streaming model is another way to improve the use of the threads and data Transfer. It is a pipeline of asyconizing the data transmission [22].

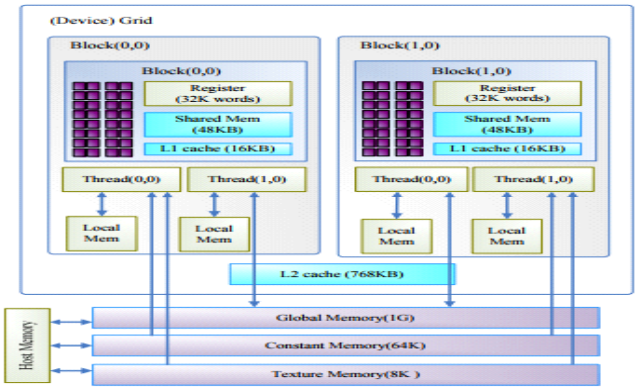

Figure 3. Memory architecture of CUDA device

V. LONGEST PREFIX MATCHING (LPM) ALGORITHM

A Bloom filter is an array of m bits for representing a set S = {x1, x2, . . . ,xn} of n elements. A software based LPM algorithm used for IP lookup. The algorithm improves the performance of a regular hash table using Bloom filters [23]. The process of packet classification is divided into some basic steps. The first step is the Longest Prefix Match (LPM) operation. Then by using perfect hash function mapping, the LPM results to the rule number in order to perform fast searching. Hence the complete Rule has to be stored in the last stepLet P.fi denote the value of field i in packet P. The packet classification process can be outlined in the following pseudocode [24].

Classify Packet(P)

1. for each field i
2. vi ← LPM(P.fi)
3. {match, {Id}} ← Hash Lookup((v1, . . . , vk))

As the algorithm depicts, we first execute LPM on each field value. Then we search the key constructed by all the longest matching prefixes in the hash table. The result of this lookup indicates if the rule matched or not and also outputs a set of matching rule IDs relating with a matching rule [25].

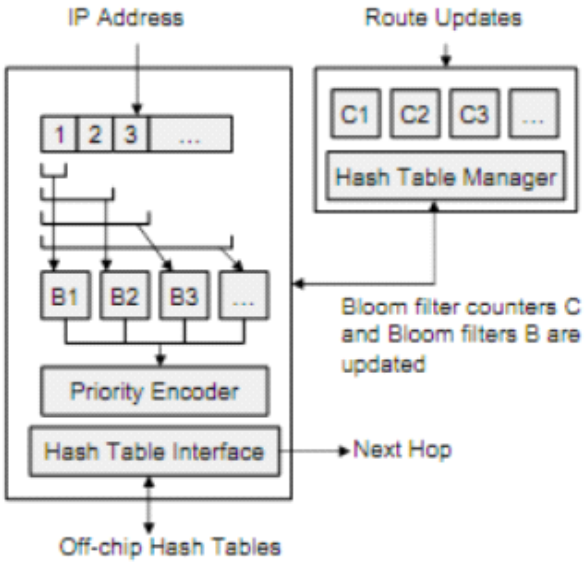

Figure 4. Longest Prefix Matching using Bloom filters

VI. BIT-VECTOR GENERATION ALGORITHM

Require: N rules each of which is represented as a W-bit ternary string: Rn = Tn, W_1Tn,W_2……Tn,0, n = 0, 1,….., N - 1 Ensure: 2k X W/k, N-bit vectors: Vi,j = Bi,j,N-1Bi,j,N-2…….Bi,j,0, i = 0; 1, . . . , W/k - 1, and j = 0, 1, . . . , 2k – 1

- Initialization: Vi,j to 00 ….. 0 ¥ i, j
- for n = 0 to N -1 do {Process Rn}
- for i= 0 to W/k -1 do
- S [2 k][k] = Permutations (R[I * k : (i + 1) * k])
- for j to 1 to 2k -1 do
- Vi,j [i * k : (i+1)* k] = S[j]
- end for
- end for
- end for

Since every individual element of the BV responsible for a single rule of entire rule set, every individual bit-level operation is independent of the rest of the bits in BV [26]. This allows partitioning the BV without effecting the operation of the BV approach. Each partition will produce a portion of the longest BV, referred to as sub-BV hereafter, which contains the matching result.

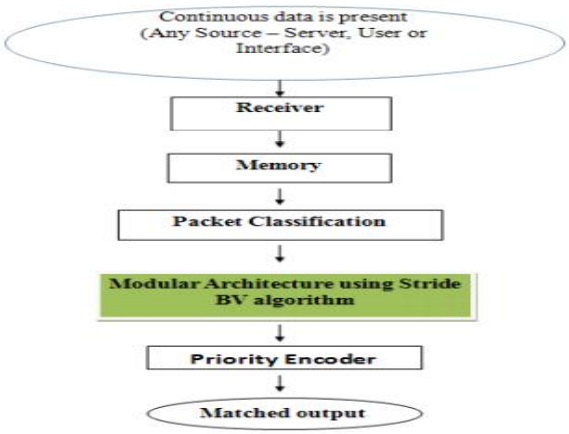

Figure 5. Flow diagram of modular BV model

VII. EXPERIMENTAL RESULTS

The worst case scenario is provided for tests and tests have been conducted multiple times to calculate the average. The both Dim Cut and Hyper Cut act better with respect to time consumption and Dim Cut is faster than the others during the progress of rule classification process. While, the memory amount for proposed system using bloom filter and LPM depends on hash key and value. The following graphs show that, the total memory amount required for storing rules in proposed system is less than that of existing system. Rule-based sensor contains only a part of the rule set and is fed with the whole dump file. In order to select the packets that corresponds to the sensor ports. The X-axis is the number of packet processed by Snort and the Y-axis is the corresponding processing time. The doted red curve corresponds to the centralized architecture. It shows a linear curve which is a normal behavior. The others curves correspond to maximum and the minimum of the rule based scenario.

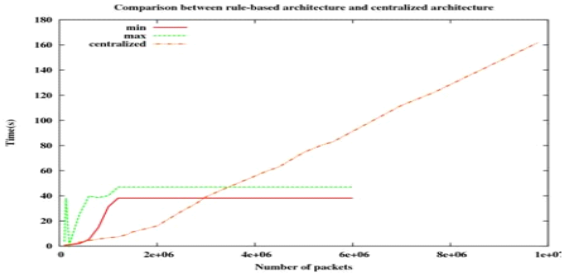

Figure 6.comparison rule-based architecture and centralized architecture

VIII. CONCLUSION AND FUTURE WORK

Packet classification of various algorithms has been studied. Stride BV is algorithm used here for packet classification. This algorithm explains the classification which is done in terms of Stride which is rule set independent compared to past methods of packet classification. Packet classification algorithms which is a critical attribute in Firewalls routers network security and quality of service. The PCFC aims at the infrastructure of the packet classification at core routers, combines capabilities and other intelligent marking technologies, and can support dual-stack structure of IPv4 and IPv6 well. In the future, we will apply GPU-based packet filter system to other network security systems, such as Botnet detection system and network intrusion detection system, to improve the performance. Also, we focus on improving the proposed methods to provide a real-time giga bit network and fast network telescope packet analysis applications. To construct such classification, it uses LPM and Bloom filter. Throughout the extensive analysis using Class bench databases performed between previous decision-tree algorithms that uses boundary cutting algorithm and bloom filter. Memory requirement for the proposed system is less than that of existing system. Proposed algorithm enables both the highest priority match and the multipath packet classification.

IX. REFERENCES

[1]. D.E.Taylor,"Survey and taxonomy of packet classification techniques," ACM Computing Surveys,vol.37,iss.3,pp.238-275,Sep.2005,doi:10.1145/1108956.1108958

[2]. P.Gupta & N.McKeown,"Packet Classification Using Hierarchical Intelligent Cuttings",in Proceedings of IEEE Symp.High Performance Interconnects (HotI),7,1999.

[3]. B.Vamanan,G.Voskuilen&T.N.Vijaykumar,"Effi Cuts: optimizing packet classification for memory and throughput",in Proceedings of the ACM SIGCOMM 2010 conference on SIGCOMM,New Delhi,India,2010

[4]. D.E.T aylor,Survey and taxonomy of packet classification techniques,ACM Comput.Surv.37(3) (2005) 238-275.

[5]. A.Nottingham and B.I rwin,Parallel packet classification using GPU co-processors,SAICSIT Conf.ACM,(2010),pp.231-24.

[6]. M.Roesch,Snort - L ightweight intrusion detection for networks,in Proc.the 13th USENIX Conference on System Administration,(1999),pp.229-238.

[7]. Thilan Ganegedara,Weirong Jiang,and Viktor K.Prasanna,"A Scalable and Modular Architecture for High-Performance Packet Classification," IEEE Trans on parallel and distributed systems,vol.25,no.5,pp.1135-1144,MAY 2014.

[8]. T.V.Lakshman and D.Stiliadis,"High-Speed Policy-Based Packet Forwarding Using Efficient Multi-Dimensional Range Matching,SIGCOMM Comput.Commun.Rev.,vol.28,no.4,pp.203-214,Oct,1998.

[9]. 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.

[10]. W.Eatherton,G.Varghese,and Z.Dittia,"Tree Bitmap: Hardware/ Software IP Lookups with Incremental Updates,SIGCOMM Comput.Commun.Rev.,vol.34,no.2,pp.97-122,Apr.2004.

[11]. H.Lim,N.Lee,G.Jin,J.Lee,Y.Choi,and C.Yim,Boundary Cutting for Packet Classification,vol.22,no.2,pp.443-456,April 2014)

[12]. N.Kothari and S.E.Pawar,Packet Classification based on Boundary Cutting analysis by using Bloom Filters,ISSN: 2321-8169,Volume 3,Issue 7,July 2015.

[13]. Wooguil Pak and Young-June Choi,High Performance and High Scalable Packet

Classification Algorithm for Network Security Systems,IEEE Transactions on Dependable and Secure Computing,2015.

[14]. LU Zhi-Jun,ZHENG Jing,HUANG Hao.A Distributed Real-Time Intrusion Detection System for High-Speed Network.Journal of Computer Research and Development,2004,41(4):667-673.

[15]. Tarek Abbes,Alakesh Haloi,Michaël Rusinowitch.High Performance Intrusion Detection using Traffic Classification.Proceedings of the IEEE International Conference on Advances in Intelligent Systems (AISTA2004),Luxembourg ,Nov 2004.

[16]. T.Abbes,A.Bouhoula,and M.Rusinowitch.A traffic classification algorithm for intrusion detection.In AINA Workshops (1),pages 188-193,2007.

[17]. O.Erdem,H.Le,V.K.Prasanna.Hierarchical Hybrid Search Structure for High Performance Packet Classification.In Proceedings of IEEE INFOCOM,Mar.2012.

[18]. Chen Bing,Pan Yuke,Ding Qiulin.A Heuristic Lookup Partition Algorithm for Packet Classification.Journal of Electronics & Information Technology,2009,31(7) pp.1594-1599.

[19]. A.Nottingham and B.Irw in,GPU packet classification using OpenCL: a co nsideration of viable classification methods.In Proc.SAICSIT Conf.ACM.,(2010),pp.160- 169.

[20]. M.LCharalambous,P.Trancoso and A.Stamatakis,Initial Experiences Porting a Bioinformatics Application to a G raphics Processor,In Proc.the 10th Panhellenic Conference on Informatics,2005,pp.415-425.

[21]. J.D.Owens,D.Luebke,N.Govindaraju,M.Harris,J. Krüger,A.E.Lefohn and T.Purcell,A Survey of General-Purpose Computation on Graphics Hardware,Computer Graphics Forum,26 (2007),pp.80-113.

[22]. C.L.Hung and G.J.Hua,Local Alignment Tool Based on Hadoop Framework and GPU Architecture,Biomed Research International,2014 (2014),Article ID 541490.

[23]. S.Dharmapurikar,H.Song,J.Turner,J.Lockwood,-Fast packet classification using Bloom filters,in: Proc.of ANCS,2006,pp.61-70.

[24]. A.G.Alagu Priya and H.Lim,-Hierarchical packet classification using a Bloom filter and rule-priority tries,Comput.Commun.,vol.33,no.10,pp.1215-1226,Jun.2010.

[25]. H.A.J.Sistani,S.P.Amin,and H.Acharya,-Packet classification algorithm based on geometric tree by using Recursive Dimensional Cutting (DimCut),vol.2,no.8,pp.31-39,August2013.

About Authors:

P.AMRUTHA VARSHINI is currently pursuing her MCA in MCA Department, St.Ann's College Of Engineering and Technology,Chirala, A.P. She received her Bachelor of science from ANU.

Dr.R.MURUGADOSS,MCA., M.E(CSE), Ph.D(CSE),MCSI,MISTE., is currently working Technology as a Professor in MCA Department ,St.Ann's College of Engineering & Technology College, CHIRALA-523187.

His research includes networking and data mining.