Design and Implementation of High Throughput and High Speed Hypercut Packet Classification

Dr. T C.Thanuja[1] Ashwini Chougala[2] Usha S[3]
[1]Professor [2,3]M.Tech Student
[1,2,3]Department of VLSI Design and Embedded System
[1,2,3]VTU, Belgaum

Abstract— Packet classification is the critical task in networking and it is used by network processor present in router to classify the packets according to the header field values. Packet classification is the process of matching packet header values to the rule header values. The packet is processed according to the matched rule. The contribution of this paper is " Pipelined packet classification" architecture using hyper cut algorithm. This architecture is based on building the decision tree. The pipelined architecture for packet classification reduces the critical delay and gives high throughput of 3.98 Gbps.

Key words: Packet classification, high throughput, high speed, parallel and pipeline processing

I. INTRODUCTION

The usage of the internet grows for every year, because of the easy access of the internet through 'smart phones', 'note books' and 'net books'. Packets are processed through the network processor, which are responsible to convert the packets into fragments, reassembling the converted fragments, encryption and packet classification. Due to incremented line rates, pressure is creating on network processor. There are two ways to minimize the pressure. One is to insert more processing cores but it increases power consumption and clock speed, so it has created difficulty in fabrication due to physical constraint in the silicon, so there is a need to get optimized solution for relieving the pressure on network processor.

"The process of matching the incoming packets with the rules, in an network router is called Packet classification. All the packets which are matched to the same rule are processed in homogeneous manner [1]". The application of the packet classification includes' Intrusion detection',' firewalls' and 'monitoring architectures'. Due to greater evolution of internet services, the packet classification becomes difficult task. The design of any algorithm will depends on performance parameters like speed, throughput, low area etc. In this paper, different algorithms used for packet classification are also discussed with respect to performance parameters like 'time complexity', 'speed complexity', memory usage, throughput and efficiency.

The basic algorithms like 'Linear search' [2],' hierarchical trie' [3], 'set pruning trie' [4] etc are failed to meet the performance requirement. So hypercut packet classification algorithm will give the better performance like 'high speed' and 'high throughput', because of its high throughput, more packets can be processed per second, it reduces the time.

The rest of the paper is organized as follows. Section II explains packet classification using hyper cut packet classification algorithm. The hyper cut packet classification is based on decision tree structure. Section III explains the simulation results for pipelined hyper cut packet classification. Section IV explains comparison of performance parameters for parallel hyper cut packet classification[5], and pipelined hyper cut packet classification. Section V concludes the paper.

A. Evolution of Packet Classification

The world is in the midst of a greatest shift in the information and communication technology. The 'DARPA (Defense Advanced Research Projects Agency) 'internet architecture project was commenced in 1973 has produced the protocols and many historians are termed this as 'information age'. The internet users and also applications are incrementing day by day, so that it is creating greater volume of traffic for network infrastructure. As the network traffic is increasing, the search tasks performed by the routers are also increasing. The router has to process the packets and to determine its corresponding rule according to its header and also needs to provide services to the packet according to its corresponding rule.

Networks [6], were considered as constituent unit of the internet. To provide greater services, the networks were interconnected. The starting aim was to connect 'ARPHANET' with the 'ARPA packet radio network', in order to give more services on the existing 'ARPANET'. At this time there were different networks were present. But there is requirement to consider the unified system. Here the problem occurs because of combining the 'separately administrative entities' into general entities. Approximately 233 million hosts were using the internet [7]. Any device which is communicating over the internet is termed as host. The hosts may be considered as mobile phones, laptops, personal digital assistants (PDA's).

Nowadays, there were two switching techniques were widely available. One is 'packet switching' and another is 'circuit switching'. 'Packet switching' was considered as basic component of the internet. The switches were utilized to interconnect the networks and these switches are considered as 'gateways'. Networks are the building blocks of the internet. It contains the heterogeneous combination of' hosts', 'links' and 'router'. Fig 1 shows the 'architecture of the internet'.

Hosts will produce and consume the datagram's. Hosts may be mobiles, work stations and servers. Links are utilized to connect hosts to routers and from router to router. The task of the router is to switch the packets from source link to the destination link depending on the packets header value.

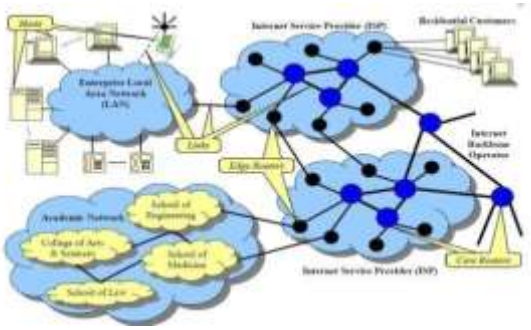

Fig. 1: 'Architecture of the internet'

At the beginning,' internet protocol suite (IP)' and 'transmission control protocol (TCP)' were used. End to end delivery of the packets will be provided by the 'internet protocol (IP)'. IP will specifies the format for attaching the information regards to source and destination and this information is attached to the packet are termed as 'packet header ' and the information present in the packet are considered as 'payload'. To uniquely identify the internet hosts, every host will be assigned with IP address. Nowadays, majority of the internet users are using IPv4 and it provides 32 bit IP addresses. Fig 2 shows the 'IP packet format'

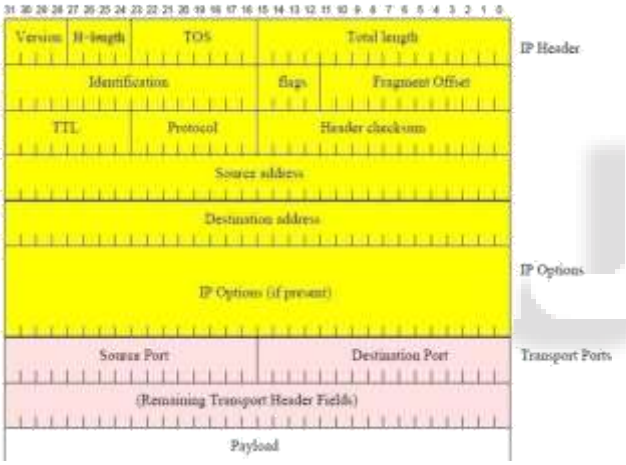

Fig. 2: Format for IP

In the IP format, it designates the type of protocol used in 'transport layer'. Instead of giving IP addresses to every host, the IP addresses are assigned to organizations in order to ensure the hosts with common initial bits. These initial bits are called as 'network addresses'. The organization is free to make the decision on the addresses which are given to individual hosts, which are connecting to it.

B. Packet Classification

The packet classification [8], is considered as an 'omnipresent' task in the network. 'Packet classification' is the task of deciding which rule(s) from the rule set, are matched to the packet, depending on its header information. If the packet is matched to 'multiple rules', the rule with highest priority is taken.

C. Filters/Rules

"The process of classifying the packets are termed as 'filters', in firewall context, it is termed as rules. These rules are used to provide various services". In this report, filter and rules [9], are used interchangeably. The classification of the packet depends on the header values. Consider the IPv4 packet having 'maximum packet width' of 65,535 bytes. "The header contains 20 bytes in which source and destination IP address have 32 bit, 'source and destination port' have 16 bit and 'protocol' have 8 bit". 'Filter database' [9], contains the number of filters. To access the filter database, the header value of the packets must be match to the filter. The header value of the packet corresponds to three well known layers of 'TCP/ IP model'. They are shown in the fig 3.

Fig. 3: Packet structure

The protocols associated with the packet consists of three layers are shown in fig 4. The 'network layer' consists Internet protocol, the transport layer consists of two protocols 'TCP' (Transmission control protocol), 'UDP' (User datagram protocol), and application layer contains several protocols like HTTP, SMTP etc.

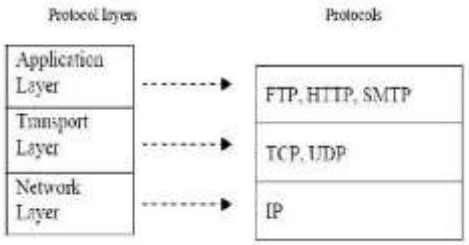

Fig. 4: Packet in network layer

For the network functions like 'routing', firewalling', and 'load balancing', packet classification is considered as 'key building block'. Every packet when passes through the network encounters the classification through the forwarding elements like 'Layer2 switches', ' layer 3 routers' as well as 'special purpose' classifiers such as ' firewall' and 'load balancer'. This is illustrated in fig 5 below.

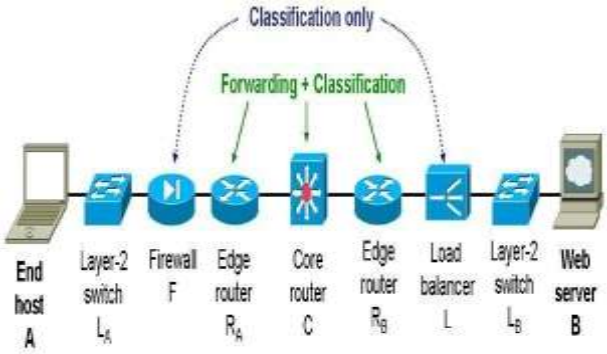

Fig. 5: the forwarding elements in the internet

A 'router' is used to classify the packet and to determine the quality of service, it should receive. A 'load balancer' is used to classify the packet to identify the 'web server'. A firewall is used to classify the packets depending on its security policies and it decides whether to accept or drop the packet".

D. Firewall

'Firewall' is a security system which is designed to block unauthorized access to the 'private network' . Firewall is placed at every point between the 'network and outside the network' and it filters the data which is coming

into the network and going out from the network. While filtering the content of header values of the packet are matched to the predefined rule base. The packet which matches to the rule base, is processed according to that rule. Nowadays, firewalls are designed to protect single pc's from the internet. Firewalls can be designed in software or hardware or combination of both. "Firewalls can be employed in packet filter ,application gateways ',' circuit-level gateways and 'proxy servers.

E. Access Control List

The 'access control lists' are the rule sets, which are assigned to the protocol or destination/ source ip addresses, which are available on the network, which have the right to access the network services. In this there are two types one is 'standard access control list' and 'extended control list'. Here classification is done based on header values of the packet such as 'source/ destination IP addresses', 'source/ destination port numbers' and 'protocol'. For every incoming packet, matching is done in order to pass or deny the packets according to a set of rules presented to it. 'Multidimensional packet classification' algorithms need greater memory usage and increased speed.

In standard access lists, only the source ip address field is used to match with the rue, this reduces the memory usage and 'classification complexity. In extended access control list, all the fields of the packet are used to match with the rule. The ACL [11], is a group of statements which are used to decide whether to accept or reject the packets. ACL consists of sequential statements. If the condition is evaluated to true, packet is allowed or denied. If any acl statements are failed to match then at the end, packet is denied automatically. The implementation of the acl is shown in below fig 6

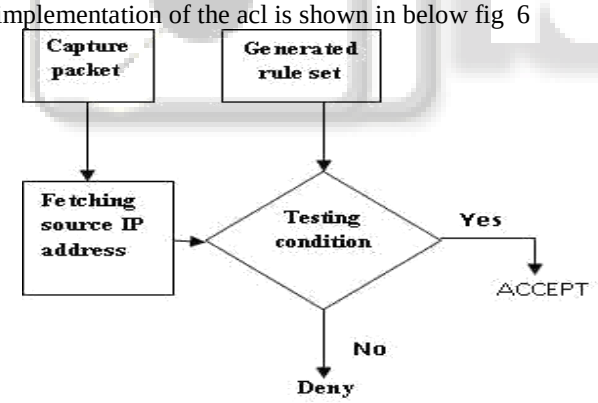

Fig. 6: The implementation of acl

The main limitations of packet classification are 'configuration hardness', 'inefficiency' and 'inflexibility'. These limitations comes from the four characteristics of 'packet classification' which are, (i) 'Complexity of classification operations' (ii) "Topology Mismatch between network administrators and forwarding mechanisms' (iii) 'Semantic Gap between entities on the packet path' (iv) 'Resource Mismatch between entities on the packet path". Due to significant improvement in the 'classification speed' of the packets, the task of packet classification is become complex. It creates 'performance' and 'scalability' bottlenecks. 'Multi field packet classification' yields the performance trade- off between memory usage and 'computational complexity'.

II. HYPER CUT PACKET CLASSIFICATION

"The hypercut packet classification algorithm' is a decision tree based packet classification algorithm". it was designed by Singh et al. It was designed for mainly 'multidimensional packet classification'. Demand on increased line speed due to growing of internet usage, there is requirement of high speed and optimized algorithm like 'hypercut packet classification algorithm' to meet the increased line speed.

A packet is a 'formatted unit of data' which is carried by 'packet switched network'. When the data is formatted to packet, the bandwidth associated with the communication channel reduces". Packet mainly consists of three parts. They are 'packet header', 'payload' and 'trailer', which is shown in fig 7. The maximum size possible for the packet is 64535 bytes, and minimum size is 20 bytes. The size of header and trailer for IPv4 are fixed and which are 20 bytes and 32 bits respectively. The size of payload varies from 0 bytes to 64,511 bytes. The fig 8 shows the 'format of packet'.

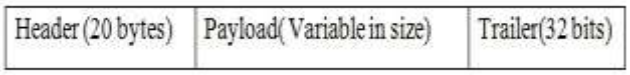

Fig. 7: 'format of packet'

1) Header: Header is a portion of the 'IP' packet, and it contains the destination address information. The header of the packet has five fields which are "source IP address (size 32 bit), Destination IP address (size 32 bit), source port number (16 bit), destination port number(16 bit),protocol(size 8 bit)", and also it contains packet number and synchronization bits.
2) Payload: It contains the actual data that is transmitted between the two nodes, and it is variable in size from 0 bytes to 64,511 bytes.
3) Trailer: It is used to inform to destination device about the completion of transmission of the packet.

A. Packet Classification:

'Packet classification' is the task of deciding which rule(s) from the rule set, are matched to the packet depending on its header information. If packet is matched to multiple rules, then the rule with highest priority is taken. Packet classification is required to sort the packets depending on the services they require such as mail service, facebook service, you tube and it also deny the unsecured data.'Packet classification' [11], is shown in fig 8, here incoming packet is given to the forwarding engine. The forwarding engine contains the rule sets and every incoming packet is matched to the rule sets which are present in 'forwarding engine' and according to the matched rule, packet classification can be carried.

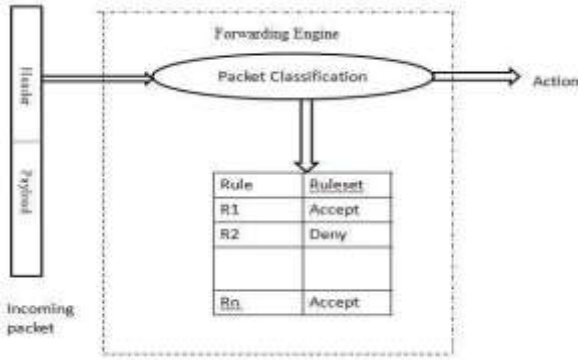

Fig. 8: Packet classification engine

B. The Architecture of Pipelined Packet Classification Using Hyper Cut Algorithm

The architecture of pipelined packet is shown in fig 9. Here the incoming packets are stored in the packet buffers A and B. The "memory" of the packet classification architecture contains the tree structure. The rulesets are present in memory. The tree structure is used to match the incoming packets to the rules present in memory. The architecture of pipelined packet classification contains eight packet classification engines. The incoming packets from the buffer A are given to the packet classification engines 11,12,13 and 14. The incoming packets from packet buffer B are given to the packet classification engines 21,22,23 and 24.Here the incoming packets from packet buffer A and B are given simultaneously to the packet classification engines, so that eight packet classification engines are working simultaneously, processing two packets at a time. Here the packet classification engines 11,12,13 and 14 are produce the packet classification engines output as match, nomatch and rule id signals for the packet buffer A. The packet classification engines 21,22,23 and 24 are produce the packet classification engines output as match, nomatch and rule id signals for the packet buffer B. The two sorter blocks are used to output the two matching rules simultaneously. If the incoming packet is matched to more than one rule, then the rule with highest priority is taken as matched rule.

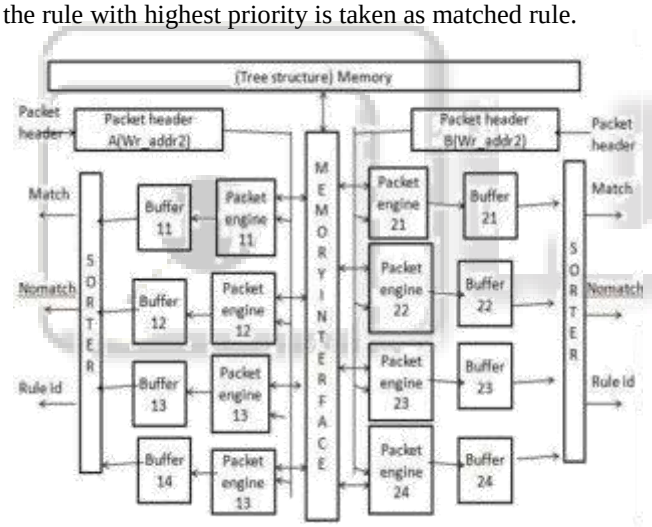

Fig. 9: The architecture for pipelined hyper cut packet classification

The rule set header values are shown in the table 1. This ruleset contains seven rules. These ruleset is used for authentication of the packets. In the table S.IP denotes source IP address of rule header, D.IP denotes destination IP address of rule header, S.P denotes source port number of rule header, D.P denotes destination port number of rule header, Protocol denotes the protocol field of rule header

RuleID	S. IP	D. IP	S. Port	D. Port	Protocol	Action
R_1	0000	0101	30-80	0-65535	UDP	ACT_1
R_2	111*	1***	0-2000	10-10	UDP	ACT_2
R_3	1***	101*	60-80	0-65535	TCP	ACT_3
R_4	101*	0***	0-65535	960-990	TCP	ACT_4
R_5	00**	101*	0-65535	800-811	TCP	ACT_5
R_6	000*	0111	30-80	0-65535	UDP	ACT_6
R_7	000*	0110	30-80	0-65535	UDP	ACT_7

Table 1: The rulesets containing seven rules

The flow chart for the tree structure is shown in fig 10 as

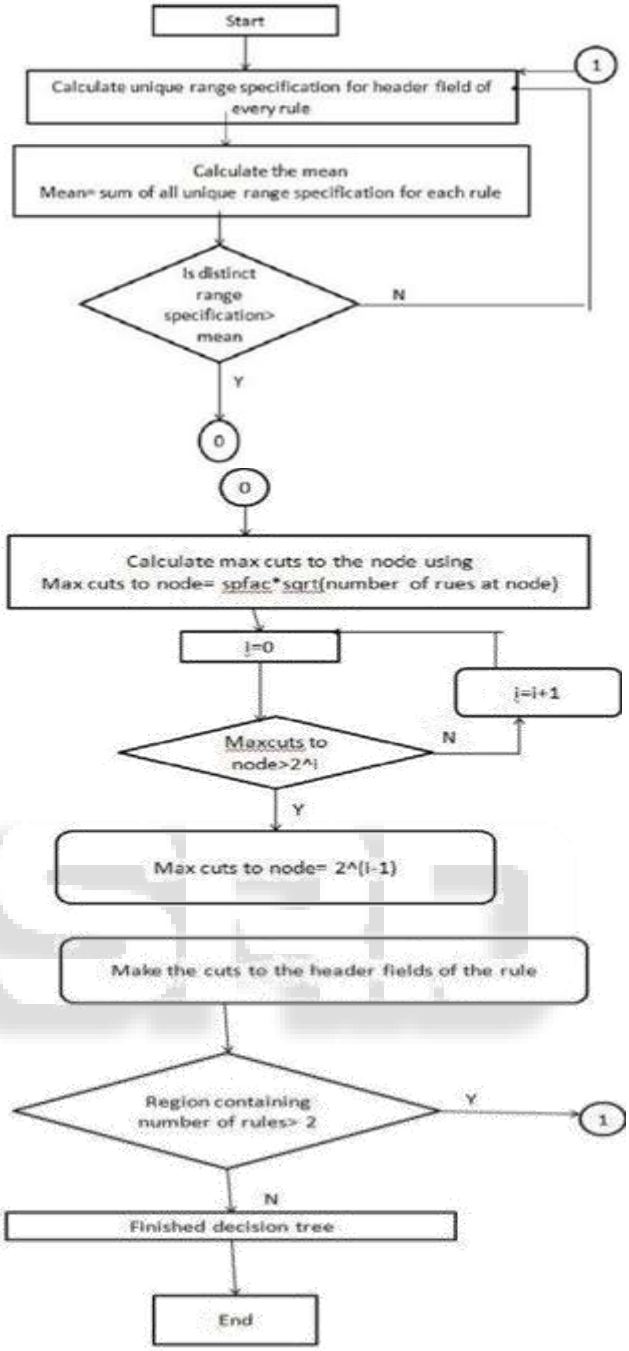

Fig. 10: The flowchart for building the decision tree

The steps for building the decision tree is shown in the flowchart. The tree structure for the rulesets shown in table ar1e constructed according to the flowchart shown in fig 4. From the table 1 , it is observed as the distinct range specification for source IP address has 6, destination IP address has 6, source port number has 4, destination port number has 4 and protocol field has 2. The mean is obtained as (6+6+4+4+2)/5=4.4. The distinct range specification for source and destination IP address field has range specification as 6, it is more than 4.4, so it is considered for cutting.

The number of cuts performed to the fields are obtained using this equation as max number of cuts to the field<= spfac* sqrt(number of rules), here the value of spfac is 3, because if the spfac value is less than two then maximum two regions are created and the memory used to

store all the rules is less,but the time needed to traverse the entire memory is more . If the spfac value is more than two then number of regions created more, but the time needed to traverse the tree is less. Max cuts to the field is<= 3*sqrt(7)= 7.9, which should be the power of two. So maximum four cuts can be performed to the header fields. After cutting, the tree structure is obtained as shown in fig 11.

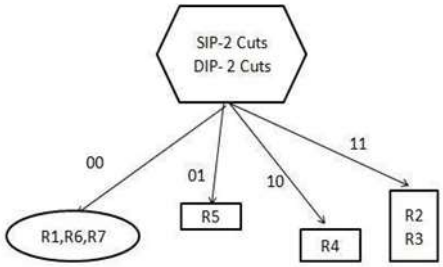

Fig. 11: The tree structure obtained after cutting the root node

The region having more than two rule is considered for cutting. Here the first region of the tree contains three rules, which is more than two so it is considered for cutting. Next three rule header fields of R1,R6 and R7 are considered for cutting. The distinct range specification for source IP address has 2, destination IP address has 3, Source port number has 1, destination port number has 1 and protocol number has 1. The mean is calculated as (3+2+1+1+1)/5=1.6, the distinct range specification for source and destination field is greater than mean, so these two fields are considered for cutting.

The number of cuts performed to the fields are obtained using this equation as Max cuts to the field is<= 3*sqrt(3)= 5.9, which should be the power of two. So maximum four cuts can be performed to the header fields. After cutting, the tree structure is obtained as shown in fig 12 as

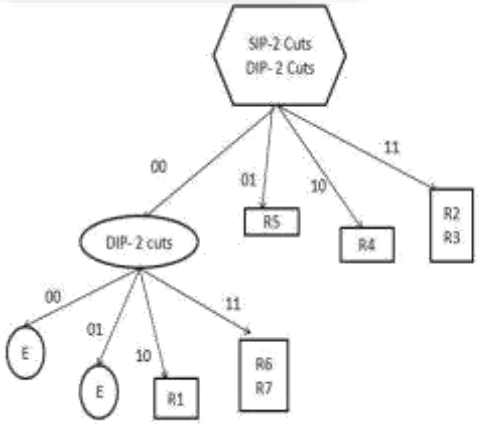

Fig. 12: The finished tree structure

The regions obtained after cutting the internal node are shown in the fig 13. Here all the regions contains less than two rules. Now the cutting process is complete. Procedure for matching the incoming packets to the tree structure is shown as first the MSB bits of both source and destination IP address fields are considered to traverse the tree next the two MSB bits of destination IP addresses are considered for traversing. The regions for traversing is shown in Table 2 as

Region	Rules	Region	Rules
44(0111)		34(1111)	R2
43(0110)		33(1110)	R2
42(0101)	R5	32(1101)	R2,R3
41(0100)		31(1100)	R2
14(0011)	R6,R7	24(1011)	R4
13(0010)	R1	23(1010)	R4
12(0001)		22(1001)	R4
11(0000)		21(1000)	R4

Table 2 The regions for rules

The matching of incoming packets to the rule id's takes 16 clock cycles. In the first 4 cycles the four incoming packets are stored in memory. In 5th cycle, the incoming packets for the buffer B are enabled. In next 3 clock cycles three incoming packets are stored in memory. In 9th clock cycle, the process of storing in the buffer is finished. In 10th clock cycle, the selection of buffer location to read the incoming packets are takes place. It takes 7 clock cycles to process the packets and produce the result.

III. SIMULATION RESULTS FOR PIPELINE PACKET CLASSIFICATION ARCHITECTURE

The simulation results for the pipeline packet classification architecture is shown in the fig 13 and fig 14.. Here 13 clock cycles are needed to write, read and to process the incoming packets. The first 4 clock cycles to write 4 incoming packets to the buffer B as shown in fig 9, one clock cycle is to start writing operation for buffer A, 3 clock cycles are needed to write the 3 incoming packets to buffer A, one clock cycle is to start read operation for packet classification, next four clock cycles are needed to process the seven incoming packets as shown in fig 13.

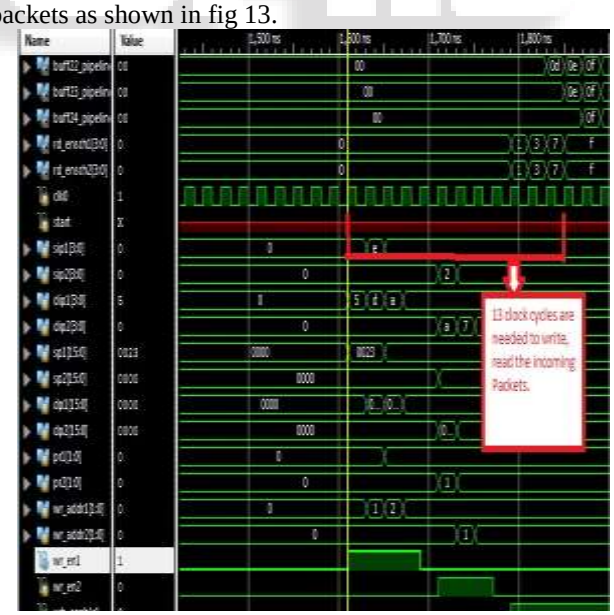

Fig. 13: The simulation results for write,read operation in pipelined packet classification architecture

The four clock cyces are needed to produce the packet classification output for seven incoming packets as shown in fig 14 . The critical delay for this packet classification is 13 clock cycles where as critical delay for parallel packet classification is 15 clock cycles.The performance parameter are compared with respect to the

parallel packet classification[5] using hyper cut algorithm is given in table2.

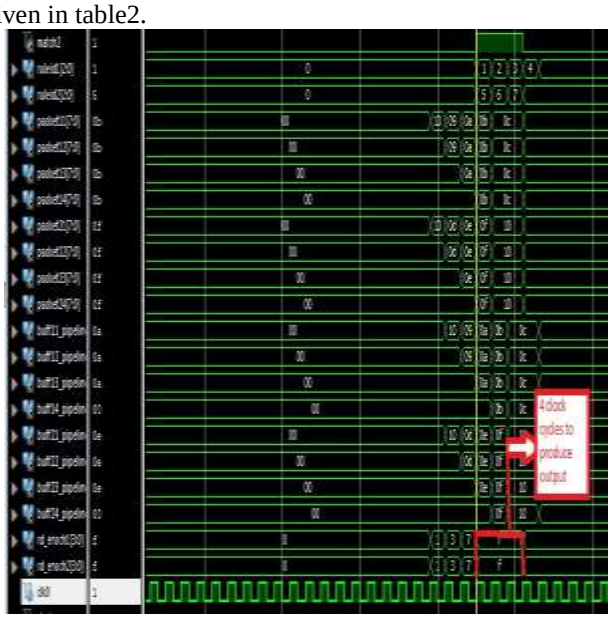

Fig. 14: The simulation results for write operation in pipelined packet classification architecture

IV. COMPARISON OF PERFORMANCE PARAMETERS

The performance parameters like frequency of operation, throughput, minimum clock period, the critical path delay and number of slice registers are compared in the table 3. The frequency of operation for parallel packet classification[5], is less as compared to parallel and pipelined packet classification architecture. The throughput for parallel and pipelined architecture is high compared to parallel packet classification architecture. The critical path delay in parallel and pipelines packet classification is reduced as compared to parallel packet classification.

The number of slice registers required for parallel and pipelined architecture is more compared to parallel packet classification architecture. It shows that the speed, throughput and frequency of operation are more in parallel and pipeline packet classification, but the area is increased in parallel and pipelined architecture because of insertion of buffers.

Parameter	Parallel packet classification	Parallel and pipelined packet classification
Frequency(Mhz)	251.825	474.15
Throughput(Gbps)	2.12	3.98
Min clock period(ns)	3.971	2.109
Critical path delay(no of clock cycles)	15	11
No of slice registers	124	164

Table 3: The comparison of performance parameters

V. CONCLUSION AND FUTURE SCOPE

There are various algorithms for packet classification based on performance parameters like time complexity, space complexity etc. available in the literature. In all algorithms, there is an enhanced research on reducing area, increasing speed and throughput. In this thesis, the proposed parallel and pipelined design made an attempt to enhance the performance and to reduce the critical path delay at the cost of little increase in area and propagation delay.

There is the need of modification in the way that the rule is stored in the leaf node of decision tree and to fetch the information needed to match the incoming packets to the rule. There are some modifications, like node merging; pushing common rule upset and rule overlap are possible in order to reduce the memory consumption.
Further work is needed to increase the performance and reduce the area and power. It is also possible to design modified hypercut algorithm using node merging, pushing common rule upset and rule overlap to reduce the number of memory accesses and to reduce the memory storage of rule sets. This can be considered as future work.

REFERENCES

[1] Dixit, M.Barbadekar, B.V. and Barbadian, A.B."Packet classification algorithms IEEE International Symposium on Industrial Electronics", 2009. ISIE 2009.,seoul, IEEE, 2009, pp1407 – 1412.
[2] Sahni,S. Kun Suk Kim and Haibin Lu "Data Structures For One-Dimensional Packet Classification Using Most-Specific-Rule Matching". I-SPAN '02. Proceedings. International Symposium on Parallel Architectures, Algorithms and Networks, 2002, Makati City, Metro Manila,pp 1 – 12
[3] Gupta,P. and McKeown, N,"Algorithms for packet classification", Network, IEEE (Volume:15 , Issue: 2),2001,pp 24 – 32.
[4] Yeim-Kuan,Chang and Hsin-Mao Chen "Set Pruning Segment Trees for Packet Classification", 2011 IEEE International Conference on Advanced Information Networking and Applications (AINA),2011,singapur,pp 688 – 694
[5] Alan Kennedy and Xiaojun Wang "Ultra-High Throughput Low-Power Packet Classification", IEEE Transactions on (Volume:22 , Issue: 2) Very Large Scale Integration (VLSI) Systems,pp 286 – 299.
[6] David D. Clark "The Design Philosophy of the DARPA Internet Protocols", Originally published in Proc. SIGCOMM '88, Computer Communication Review Vol. 18, No. 4, August 1988, pp. 106–114.
[7] Hui-Chih,Wang and Her-Sen Doong" Validation in Internet Survey Research": Reviews and Future Suggestions, International Conference on System Sciences, 2007. HICSS 2007. 40th Annual Hawaii ,Waikoloa, HI,2007, pp 243
[8] Taylor,D.E. and Turner, J.S. " ClassBench: A Packet Classification Benchmark", IEEE/ACM Transactions on (Volume:15 , Issue: 3), Networking, pp 499 – 511.
[9] Andrei Broder and Michael Mitzenmache, "Network Applications of Bloom Filters: A Survey", internet Mathematics Vol. 1, No. 4: pp 485-509
[10] Chandra Kopparapu- text book on "Load Balancing Servers, Firewalls, and Caches", 2 nd edition 2001.
[11] Sharat Kaushik , Anita Tomar, Poonam "Access Control List Implementation in a Private Network" International Journal of Information & Computation Technology. ISSN 0974-2239 Volume 4, Number 14 (2014), pp. 1361-1366.

