ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department Of CSE, JayaShriram Group Of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

# Packet classification based on priority with shortest path algorithm

A.Vijayalalitha[1], R.Dharmaraj M.E.,(Ph.D)[2]

M.E, Department of CSE,Sri Vidya College of Engineering and Technology, Virudhunagar[1]

A/P,Dept of CSE,Sri Vidya College of Engineering and Technology, Virudhunagar [2]

**ABSTRACT**: In internet routers packet classification is one of the challenging factors, which involve multiple fields for searching relevant operation. Routers in network classifying packets based on its header fields and to determine which service they should provide. This paper describes various packet classification algorithms and proposes a new efficient packet classification algorithm using priority trie approach with shortest path algorithm. This proposed method produces a high performance by increasing searching speed and reducing number of memory access.

**Index terms:** Trie-based algorithm, Tuple space based algorithm, Cutting based algorithm**.**

## I. INTRODUCTION

In general router provides the best-effort service to all incoming packets. Advanced routers can use packet classification to support higher level functions such as QoS, access control. As an essential prior condition, packets need to be classified into multiple flows from the packet header field compared with predefined rules in rule set. The rule for packet classification consists of a set of fields such as source address, destination address and so on. Each rule in a classification table has a priority which is defined by multiple fields. In a given incoming packets are compared with worth corresponding rule fields and there may be a possibility of multiple rules can match to an incoming packet. The highest priority rule is selected among the matching rules. Most of the previous packet classification algorithms have a trade-off between the required memory size and searching speed. The searching speed is measured by the number of memory accesses since memory access is the most time consuming function in the searching procedure.

Ternary Content Addressable Memory (TCAM) has been widely used in commercial routers. It provides very good search performance [2].However TCAM consumes a lot of power and larger memory space than original memory. To reduce the power consumption and to improve the throughput by make use of large classifiers implementation in TCAM which is impractical.

The basic trie-based algorithms use a source IP prefix and destination IP prefix to build tries .A hierarchical trie(H-trie) [3] constructs the first trie using the source prefix field and each node of the trie hierarchically connects to the second trie constructed with the destination field rules with the same source field ,so that both source and destination fields are searched simultaneously. In H-trie searching for matching rules has to be continued until leaf of the trie is visited. Packet classification speed can be evaluated by the number of memory access. Hierarchical approach is very effective and providing high speed search performance, but existing hierarchical approach has two problems: back-tracking and empty internal nodes. Set-pruning [3] is used to overcome the above problem and to improve the search time of H-trie by coping all possible matching rules in the ancestor nodes are copied into the leaves. It improves the search time but it requires huge amount of memory. The grid-of-trie [4] overcomes the disadvantages of rule duplication by pre-computing best matching rules of each node and storing switch pointer of each nodes.

The HiCuts (hierarchical intelligent cuttings) [5] and HyperCuts[6] algorithms partition a multi-dimensional search space based on heuristics that exploit the structure of classifiers. The decision tree is constructed based on its depth and degree of the node. Local search decision to be made at each node is determined in a pre-processing step based on the structure of the classifier. In decision tree each leaf node includes a pre-determined small number of rules that can be searched linearly. The cutting algorithms have some issues that the search speed is highly depended on the characteristics of the classifiers and excessive pre processing time may be required. In this paper propose a new approach called Priority Trie (PT) is employed to perform match in entire rule fields in a very efficient way. The PT is constructed based on the destination prefix fields of rules.

## II.RELATED WORK

In this section, we discuss related work on trie-based algorithm and cutting based algorithm.

### A. TRIE-BASED ALGORITHMS

Hierarchical trie (H-Trie) [3,4] first builds a source prefix trie and each prefix node of the source trie hierarchically connects to a destination prefix trie with the same source prefix field. For a given input packet the search is performed in the source prefix trie first. If there is a match with the source prefix, then the search control moves to the corresponding destination prefix trie. If there is match in the destination trie, the rule number is stored and the search is further needed then continued from the node of the source trie from where it traversed to the destination trie. The search is continued until there are no match nodes to proceed in the source trie. H-trie has some empty internal nodes which are not associated with a prefix or a rule. While searching, all the destination trie connected to every matched node of the source trie should be visited in order to determine the highest-priority rule, and this kind of search procedure is called back-tracking. The back-tracking causes the excessive number of memory accesses. The search complexity depends on the number of destination tries visited, and the memory requirement depends on the number of nodes. The H-trie includes many empty nodes in the path to prefix node (or a rule node). The empty nodes waste memory space as well as degrade the search performance by causing unnecessary memory accesses.

### B.CUTTING BASED ALGORITHMS

Cutting based algorithms [5,6] partitioning a search space into multi-dimensional space composed of each rule field based on the heuristics of rules in a given rule set, and each partitioned space is mapped to a node of a decision tree. For constructing the decision tree, HiCuts uses a local optimized decision at each node in determining the dimension (or field) of the cuts and the number of cuts to be made in the chosen dimension [5]. The criterion is to balance the storage requirement and search speed. While HiCuts algorithm only considers one field at a time in selecting the dimension of cuts, HyperCuts [6] algorithm considers multiple fields at a time. In selecting the dimension of cuts, the ratio of the number of distinct elements to the total number of possible values representing the dimension is considered. When compared with HiCuts decision tree, the decision tree of HyperCuts has smaller depth, as multiple fields are used at the same time in a single node, and thus, the search speed is improved. However,the number of entries is more in HyperCuts, due to the generation of many unnecessary entries.

### C.TUPLE SPACE BASED ALGORITHMS

In tuple space algorithm [3], each rule in the rule set is specified as a pair of prefixes. The lengths of the prefix pair in the rule is defined as tuple and denoted as (i, j), where 'i' is the length of the source prefix and 'j' is the length of the destination prefix. A packet arriving at a link is queried with all the non-empty tuple spaces by extracting 'i' bits from source IP address and 'j' bits from destination IP address.

### D.DIGITAL SIGNATURE

A digital signature is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, and that it was not altered in transit. Digital signatures are commonly used for software distribution, financial transactions and in other cases where it is important to detect forgery or tampering. Digital signatures are often used to implement electronic signatures, a broader term that refer to any electronic data that carries the intent of a signature, but not all electronic signatures use digital signatures. In some countries including the United States, India, and members of the European Union, electronic signatures have legal significance.

Digital signatures employ a type of asymmetric cryptography. For messages sent through a non-secure channel, a properly implemented digital signature gives the receiver reason to believe the message was sent by the claimed sender. Digital signatures are equivalent to traditional handwritten signatures in many respects; properly implemented digital signatures are more difficult to forge than the handwritten type. Digital signature schemes in the sense used here are cryptographically based and must be implemented properly to be effective. Digital signatures can also provide non-reputation meaning that the signer cannot successfully claim they did not sign a messge, while also claiming their private key remains secret; further some non-reputation schemes offer a time stamp for the digital signature, so that even if the private key is exposed the signature is valid nonetheless. Digitally signed messages may be anything represent as a bit string: examples include electronic mail, message sent via some other cryptographic protocol.

Digital signatures are one of the most important inventions of modern cryptography which is based on the Diffie-Hellman key exchange. The problem is how a user can sign a message such that everybody (or the intended addresses only) can verify the digital signature and the signature is good enough also for legal purposes. Digital signatures should be such that each user should be able to verify signatures of other users, but that should give him/her no information how to sign a message on behind of other users. Technically, digital signature is performed by a signing algorithm and it is verified by a verification algorithm. Digital signatures are an effective mechanism used for authentity and non-repudiation on messages. ElGamal encryption consists of three components:

- Key Generator
- Encryption algorithm
- Decryption algorithm

The ElGamal signature scheme allows that a verifier can confirm the authenticity of a message *m* sent by the signer sent to him over an insecure channel. In ElGamal encryption that a single plaintext can be encrypted to many possible an expansion size from plaintext to cipher text. Encryption under ElGamal requires two exponentiations. However, these exponentiations are independent of the message and can be computed ahead of time if need be. Decryption only requires one exponentiation. A third party can forge a signature. The signer must be careful to choose a different secret key *(k)* uniformly at random for each signature and to be certain that $k$ or even partial information about $k$ is not leaked. Otherwise, an attacker may be able to deduce the secret key *x* with reduced difficulty, perhaps enough to allow a particular attack. In particular, if two messages are sent using the same value of *k* and the same key, then an attacker can compute x directly. To more secure claimed that if any *k* is used twice in the signing, then the system of equations in uniquely determined and *x* can be recovered. So for the system to be secure, any value of *k* should never be used twice.

## III.PRIORITY BASED APPROACH

In this proposed system, classification only based on the destination prefix field in a packet. To increase the performance and reduces the number of memory access by using priority trie. Priority trie is formed, and providing priority to each rule in a predefined rule set. Highest priority rule can be checked for first prefix bit in a destination prefix match field, if match found no need to do further match then perform relevant action that means whatever action specified in corresponding rule, flow going through to that action. Otherwise next bit value being matched to trie node until reach higher priority rule in a trie or to reach a leaf of trie. In source side providing security against vulnerability using signature generated by source prefixes in packet header. Packet forwarding speed can be improved by using iterative shortest path algorithm. In iterative shortest path algorithm, find all matching paths, among these router will choose shortest cost path or minimum number of intermediate nodes or hops along the path.

An efficient priority based packet classification algorithm involves three phases. In the first phase, the router executes an iterative shortest path algorithm. In this algorithm bandwidth-delay constrained shortest paths are determined for each source and destination,(i.e) the paths with high bandwidth and lower delay will be selected and stored in the ascending order in a routing table. Then the selected paths are categorized into various groups depending on the number of paths available. For example if there are four optimum paths available for a given source and destination, then the top most two paths can be categorized into group1 and the next two paths can be categorized into group2.

The second phase involved using a signature based transmission. The signature is generated at sender which is the combination of information about priority and classification group. The priority is determined considering the following parameters:

- Importance of information carried through the data packet which is set by the sender.
- Strict delay and bandwidth requirement.
- Tolerance of packet loss.

From the above parameters a combined score is determined for signature the priority of the data packet. Then the priorities are converted into signatures of the data packets. For the conversion of priorities into signature, we use a two way merge formula. The value is digitized using binary conversion. This is the first section of signature. This digital signature is needed as the data packet has to travel among a number of hops. Then these packets along with the signatures are transmitted to the router.

In the third phase, in the router classification of prioritized packets is performed. This is done by sorting the packets into various priority groups (i.e) priorities that belongs to the specific range is classified into one group. Then the packet groups are mapped to the group of paths stored in the routing table. The packets belonging to group1 (with high priority) can be assigned to the paths of groups1 and so on. This model provides Quality of Service (QoS) for the users by providing better bandwidth and reduced delay according to user requirements. The scope of this proposed system is to improve routing performance and reduces number of access during transmission.

## IV.SYSTEM ARCHITECTURE

From figure 1 can be used to represent the architectural view of our proposed system. Once sender sends packet it consists of different information such as source address, destination address, protocol information etc. Priority rule for destination will be generated. Resultant packet passed to the router it can be classified and reaches the destination based on its flows.

### A.PRIORITY CALCULATION

Priority calculation model, each arriving packet classified based on it rules assigning from global predefined rule set present in each routers. Rules in a rule set decide whether a network allow to give permission to passes through this router or to drop a packet. Rules are assigned to packet by comparing rule prefix field to each received packets. All rules are stored in its priority position in trie. Rules are refined by adjusting its original position.

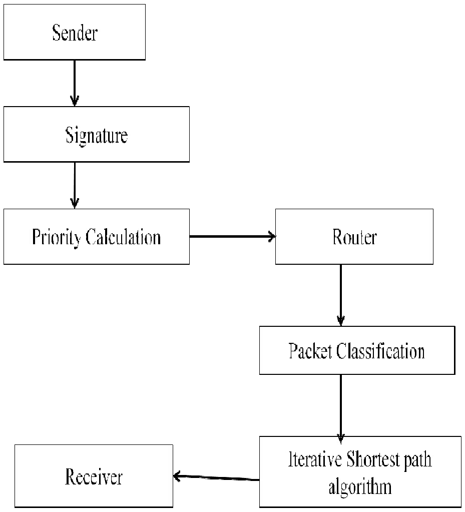

Figure 1: System Architecture

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department Of CSE, JayaShriram Group Of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

### B.SIGNATURE

Each arriving packets are treats as a normal message and to generate signature which provides more secure authentication to that's packet. Aggregate signatures are used in this model. Signatures can be applied based on its arrived basis, this will indicates tampering or any the packets have been altered or not. This signature scheme supports aggregation, given n signatures on n messages from n users and it's possible to aggregate all those signatures into a single signature whose size is constant to all users in a network.

### C.ITERATIVE SHORTEST PATH

Shortest path procedure applied between source and destination IP address is to find the path with less number of access or finding path with minimum number of intermediate nodes (routers). This algorithm applied iteratively until it reaches its destination IP address.

## V.CONCLUSION

A novel framework for packet classification is proposed in this paper. We present the priority trie algorithm including build process, search process. Compared with previous algorithm, the highest priority rule that is included in the search trie is compared first. In this way, empty nodes are completely removed and hence the required memory size and search space is improved. Hence we conclude that the priority trie for packet classification algorithm can be used effectively for providing high quality of service in networks.

### FUTURE WORK

While considering an effective classification of packet in router to be considered and priority based algorithm mainly based on rules priority from rule set. After completing that process shortest path algorithm also implemented which is used to identify the path between source and destination IP addresses.

## REFERENCES

[1]Sarang Dharmapurikar, Praveen Krishnamurthy, and David E. Taylor, "Longest Prefix Matching Using Bloom Filters", EEE/ACM Transactions on Networking,Vol. 14,No.2,April 2006.

[2]Hyesook Lim, Hyeong-gee Kim and Changhoon Yim, "IP Address Lookup for Internet Routers Using Balanced Binary Search with Prefix Vector", IEEE transaction on communication,2009.

[3]P.Gupta and N.Mckeown, Algorithm for packet classification,IEEE Network 15(2):24-32 (2001).

[4]V.Sriniasan,G.Varghese,S.Suri,M.Waldvogel,Fast and scalable layer four switching, ACM SIGCOMM, 1998.

[5]P.Gupta and N.Mckeown ,Classification using hierarchical intelligent cuttings, IEEE Micro,20(1);34-41(2000)

[6]S.Singh ,F.Baboescu ,G.Varghese and J.Wang, Packet classification using multidimensional cutting Proc.SIGCOYM,213-224(2003).

[7] Hyesook Lim, Soohyun Lee, Earl E, Swartzlander Jr, " A new hierarchical packet classification algorithm", Computer Networks,2012.

[8] Hyuntae Park, Hyejeong Hong, Sungho Kang, "An efficient IP address lookup algorithm based on a small balanced tree using entry reduction",Computer Networks,2012.

[9] Chun-Nan Lu, Ying-Dar Lin, Chan-Ying Huang, Yuan-Cheng Lai, "Session level flow classification by packet size distribution and session grouping", Advanced Information Networking and Applications, 2012.

[10] Ashley Thomas, "RAPID: Reputation based Approach for Improving Intrusion Detection Effectiveness" ,2008.

[11] Alex X. Liu, Chad R. Meiners, and Eric Torng, "TCAM Razor: A Systematic Approach Towards Minimizing Packet Classifiers in TCAMs", IEEE/ACM Transactions on Networking, vol. 18, no. 2, april 2010.

[12] Hyesook Lim,So Yeon Kim, "Tuple pruning using Bloom filters for Packet classification", EEE Computer Society, 2010.

[13] Haoyu Song, Jonathan Turner,"Fast Filter Updates for Packet Classification using TCAM",IEEE, 2006.