COMPARISON OF ALGORITHMS FOR DETECTING FIREWALL POLICY ANOMALIES

[1]SHILPA KALANTRI, [2]JYOTI JOGLEKAR

[1,2]Computer Engineering Department, Shah and Anchor Kutchhi Engineering College, Mumbai, India
E-mail: [1]skalantri76@gmail.com, [2]j_jogalekar@yahoo.com

Abstract- Firewall is becoming very popular element in network security. It is widely adopted to ensure the security of private networks by filtering out unwanted traffic. Firewall rules must be defined and ordered carefully to avoid firewall policy anomalies that may cause network failure. Packet classification is the process of categorizing packets into "flows" in an Internet router. All packets belonging to the same flow obey a predefined rule and are processed by the router. A set of packet classification algorithms is proposed to automatically identify policy anomalies in packet filtering firewalls. Two fast packet classification algorithms HSM (Hierarchical Space Mapping) and RFC (Recursive Flow Classification) are implemented and analyzed on the basis of different parameters such as memory used, preprocessing time and lookup time. Further it implements space efficient policy anomaly detection using HSM algorithm for packet filtering firewalls.

Keywords- Network security, Firewall, Packet classification, Anomalies.

I. INTRODUCTION

Firewall rules contain a criterion and an action to take if any packet matches the criterion. Actions are usually to allow and to deny. The criterion of a rule consist of a protocol, source IP, source port, destination IP and destination port. A packet arriving at a firewall is tested with each rule sequentially. Whenever it matches with the criteria of a rule, the action specified in the rule is executed, and the rest of the rules are skipped. For this reason, firewall rules are order sensitive [4].

Example of Firewall rule:

<TCP, 64.233.179.104, 80, 192.168.20.*, ANY, ACCEPT>

When a packet matches with more than one rule, the first such rule is executed. Thus, if the set of packets matched by two rules are not disjoint, they will create anomalies. The process of manually defining the rules and trying to detect mistakes in the rule set by inspecting the rule base is very much error prone and time consuming [1]. The main objective of this work is to emphasize on detecting conflicts in firewall policies because an accurate detection of policy conflicts is a major concern and is very important in case of the performance of packet filtering firewall [2][3]. It improves firewall functionality by generating conflict free rule set more efficiently.

Multidimensional Packet Classification is essential to modern network security devices such as firewalls and intrusion detection systems [9]. HSM and RFC algorithms use independent parallel search on index tables. The results of the searches are combined into a final result in several phases. So these algorithms are fast in classification. Algorithms for packet classification can be categorized as [7]-

1) Hardware based: They use Ternary content addressable memories (TCAMs).

2) Software based: Trie base, Decision tree, Hash based etc.

Different classes and algorithms for packet classification are shown in table 1: [8]

Table 1: Taxonomy for packet classification algorithms [8]

No.	Class	Algorithms
1	Naïve	Linear search, Caching
2	Two dimensional	Hierarchal trie, Set Pruning Trie, Grid of Tries
3	Extended two dimensional	EGT, EGT-PC, FIS
4	Divide and conquer	BV, ABV, Cross-producting, RFC, HSM,AHSM, C-HSM
5	Decision tree	Hypercuts, D-cuts, Expcuts, Hypersplit, sBits
6	Tuple space and hash Table	TSS, HaRP, Hybrid approach to packet classification, BSOL
7	Heuristic at bit-level	DBS
8	Hardware	TCAM, BV-TCAM

II. EXPERIMENTAL DETAILS

2.1. HSM Algorithm and Example

In Hierarchical Space Mapping (HSM), packets are classified using policy lookup table by considering four parameters. Destination IP (DA), Source IP (SA), and Destination port number (DP), and Source port (SP) number. It reduces searching space by hierarchically and step by step mapping the lookup domains two-to-one.

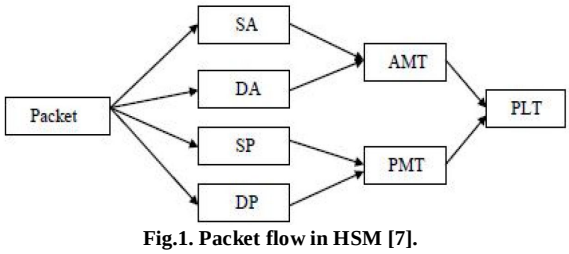

Fig.1. Packet flow in HSM [7].

First, it maps the IP address spaces (SA, DA) and the port number spaces (SP, DP) into non overlapped segments by considering the network address and port number ranges used in the policy table, and reduces the original four-dimension space to a two-dimension space by looking up the two tables, AMT (Address Mapping Table) and PMT (Port Mapping Table). These tables are transformed to the one-dimension policy lookup table (PLT). Step by step flow of packet in HSM is shown in Fig. 1 [7]. Policy Lookup Table gives information about conflicting rules. Procedure for Generation of Policy Lookup Table is as follows.

1. IP Address Fragmentation

Both source and destination address spaces are fragmented by considering the ranges appeared in the policy table. After completing this for every policy in the policy table, an address sequence number (ASN) is assigned in the ascending order, starting from 0. Bitmap is assigned to each source address sequence no (SASN) and destination address sequence no. (DASN) as shown in HSM example.

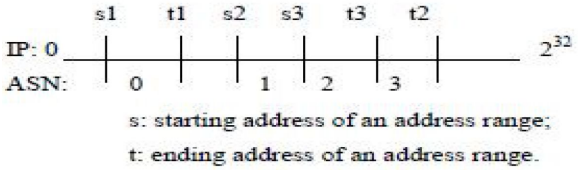

Fig.2. IP Address Segmentation [10].

2. Port number Fragmentation

Port number fragmentation is done and PSN is assigned in same manner as IP address fragmentation in first step. BM is assigned to each source port sequence no. (SPSN) and destination port sequence no. (DPSN).

3. Generation of AMT

A bitmap is assigned for each ASN indicating which policies in the policy table contain this ASN. Each policy in the policy table has one bit in bitmap. For example if there are 3 policies in the policy table and policy 1 and 2 are covered by SA#0 then a BM of 110 will be set to SA#0. Each entry of AMT is given an Address Group Number (AGN) according to the order of its appearance along with a BM tagged to it. The BM is formed by an AND operation of SA and DA BMs. Different AGN has different BM [10].

4. Generation of PMT

PMT generation is identical to AMT. Port Group Number (PGN) is assigned to each entry of PMT and has a BM tagged to it. The BM is formed by an AND operation of SP and DP BMs.

5. Generation of PLT

PLT is generated from AMT and PMT. AND operation is performed on BMs of AGN and PGN and then policy numbers are picked up from no. of 1's in the result. Each entry of PLT is filled with those policy numbers. It gives the information about conflicted rules [6].

Example of HSM that shows stepwise complete operation of HSM for table 2 is shown in fig. 8.

2.2. RFC Algorithm and Example

In RFC, the packet classification is done by mapping *S* bits in the packet header to *T* bits of class ID (where T << S). The mapping is performed recursively; at each stage the algorithm performs a reduction, mapping one set of values to a smaller set.

The RFC algorithm has P phases, each phase consisting of a set of parallel memory lookups. Each lookup is a reduction in the sense that the value returned by the memory lookup is shorter than the index of the memory access.

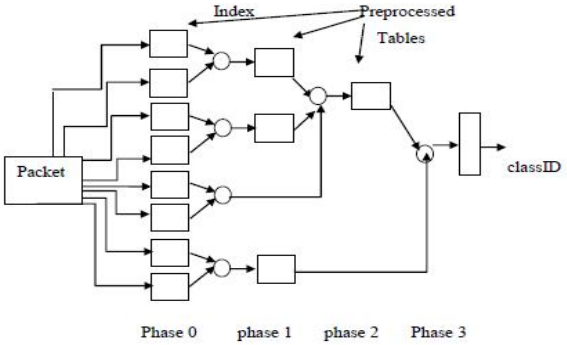

Fig.3. Packet flow in RFC [11].

The algorithm operates as follows:

1) In the first phase, *F* fields of the packet header are split up into multiple chunks that are used to index into multiple memories in parallel. Figure 4 shows an example of how the fields of a packet may be split across each memory. Each of the parallel lookups gives an output value that we will call eqID. The contents of each memory are chosen so that the result of the lookup is narrower than the index.

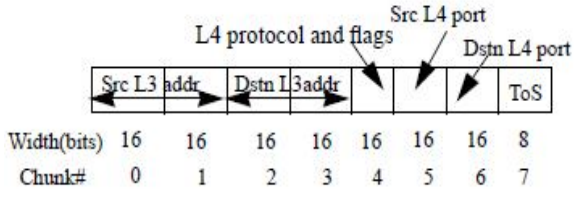

Fig.4. Example splitting packet headers into chunks [11].

2) In subsequent phases, the index into each memory is formed by combining the results of the lookups from earlier phases.

For example, the results from the lookups may be concatenated.

3) In the final phase, we will get one result from the lookup. This value corresponds to the class ID of the packet [11]. From this final Class bitmap (CBM), we will get the information about matching rules.

Example of RFC that shows complete operation of RFC for table 3 is shown in fig. 9.

III. RESULTS AND DISCUSSION

The purpose of this performance evaluation is to compare two fast packet classification algorithms HSM and RFC which can be used for detecting conflicts in firewall rules. For this comparison, results of HSM and RFC are taken on different data sets of different sizes and further evaluated by considering the lookup time, complexity of pre-processing time and the resulting storage requirements. Following are the results.

3.1. Memory Occupied/Used

Table 4: Comparison of Memory Occupied

File name (No. Of rules)	Memory used for HSM	Memory used for RFC
acl1-1k (1000)	103580	124296
acl1-5k (5000)	860820	1032984
acl1-10k (10000)	1066428	1279713

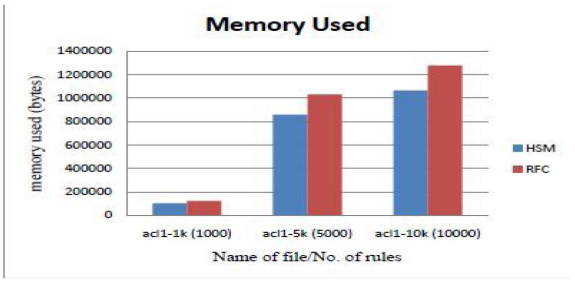

Fig.5. Memory used by HSM and RFC

Table 4 and fig. 5 shows the comparison between HSM and RFC on memory occupied. HSM is superior to RFC in space complexity.

3.2. Lookup Time

From table 5 and fig. 6, it is concluded that the Lookup time required for HSM is more than that of RFC.

Table 5: Comparison of Lookup Time

File name (No. Of rules)	Lookup Time for HSM	Lookup Time for RFC
acl1-1k (1000)	51	31
acl1-5k (5000)	145	125
acl1-10k (10000)	285	249

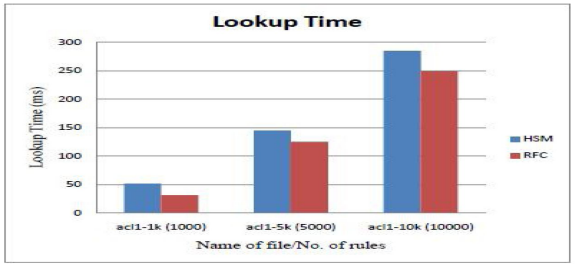

Fig.6. Lookup Time required for HSM and RFC

3.3. Pre-processing Time

Table 6 and fig. 7 illustrates that pre-processing time required for HSM is longer than RFC.

Table 6: Comparison of Pre-processing Time

File name (No. Of rules)	Pre-processing Time for HSM	Pre-processing Time for RFC
acl1-1k (1000)	151	119
acl1-5k (5000)	488	318
acl1-10k (10000)	2142	1925

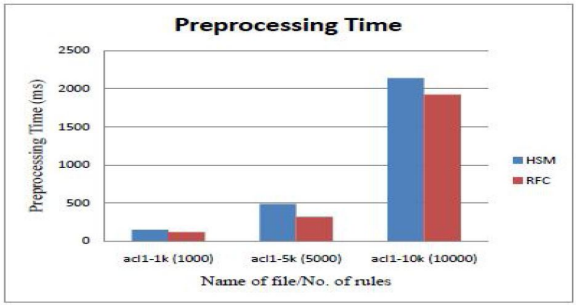

Fig.7. Pre-processing Time for HSM and RFC

CONCLUSIONS

The HSM and RFC algorithms are implemented for packet classification and analyzed on the basis of memory requirement, time taken for classification, that is pre-processing time and lookup time. I found the following results.

1. Space complexity of HSM is better as compared to RFC.
2. The pre-processing time required for RFC is less than that of HSM.
3. Lookup time of HSM is longer than RFC.

It also focuses on systematic detection of anomalies in rules for packet filtering firewall using HSM algorithm. HSM algorithm is used in proposed system to facilitate space efficient anomaly detection

REFERENCES

[1] Hongxin Hu, Student Member, IEEE, Gail-Joon Ahn, Senior Member, IEEE, and Ketan Kulkarni "Detecting and Resolving Firewall Policy Anomalies", IEEE Transactions on dependable and secure computing, vol. 9, no. 3, MAY/JUNE 2012.

[2] L. Yuan, H. Chen, J. Mai, C. Chuah, Z. Su, P. Mohapatra, and C. Davis, "Fireman: A toolkit for firewall modeling and analysis," Proc. IEEE Symposium on Security and privacy, p. 15, 2006.

[3] Amjad Gawanmeh1 and Sofi`ene Tahar, "A Novel Algorithm for Detecting Conflicts in Firewall Rules", 25th IEEE Canadian Conference2, 2012.

[4] Muhammad Abedin, Syeda Nessa, Latifur Khan, and Bhavani Thuraisingham "Detection and Resolution of Anomalies in Firewall Policy Rules", Data and Applications security, vol 4127, pp 15-29, 2006.

[5] Ehab Al-Shaer, Hazem Hamed, Raouf Boutaba, and Masum Hasan, "Conflict classification and Analysis of Distributed Firewall Policies", IEEE Journal on Selected Areas in Communications, vol. 23 , October 2005.

[6] Abhishek K. Chawan, Shashikant S. Mahajan, "Solving Firewall Policy Anomalies Using Generic Algorithm",

International Journal of Engineering Trends and Technology (IJETT) , vol. 20 no. 4, Feb 2015.

[7] Mrudul Dixit, Anuja Kale, Madhavi Narote and B.V.Barbadekar, "Fast Packet Classification Algorithms", International Journal of Computer Theory and Engineering, vol. 4, no. 6, December 2012.

[8] Safaa O. Al-Mamory , Wesam S. Bhaya , Anees M. Hadi, "Taxonomy of Packet Classification Algorithms" Journal of Babylon University, Pure and Applied Sciences vol. 21, no. 7, 2013.

[9] Pankaj Gupta and Nick McKeown, Stanford University, "Algorithms for Packet Classification", IEEE Network , March/April 2001.

[10] Bo Xu Research Institute of Information Technology (RIIT), Tsinghua University Dongyi Jiang Juniper Networks, "HSM: A Fast Packet Classification Algorithm", Proc.19th IEEE International Conference on Advanced Information Networking and Applications, 2005.

[11] Pankaj Gupta and Nick McKeown, "Packet Classification on Multiple Fields", *Proc. conference on Applications, technologies, architectures, and protocols for computer communication* , pp.147-160, 1999.

Table 2: Rule Table for HSM

Rule	SA Range	DA Range	SP Range	DP Range	Action
0	0.0.0.0~128.0.0.0	0.0.0.0~64.0.0.0	64~256	128~256	Deny
1	64.0.0.0~255.255.255.255	0.0.0.0~32.0.0.0	128~65535	128~65535	Permit
2	32.0.0.0~64.0.0.0	0.0.0.0~255.255.255.255	0~65535	0~65535	Deny

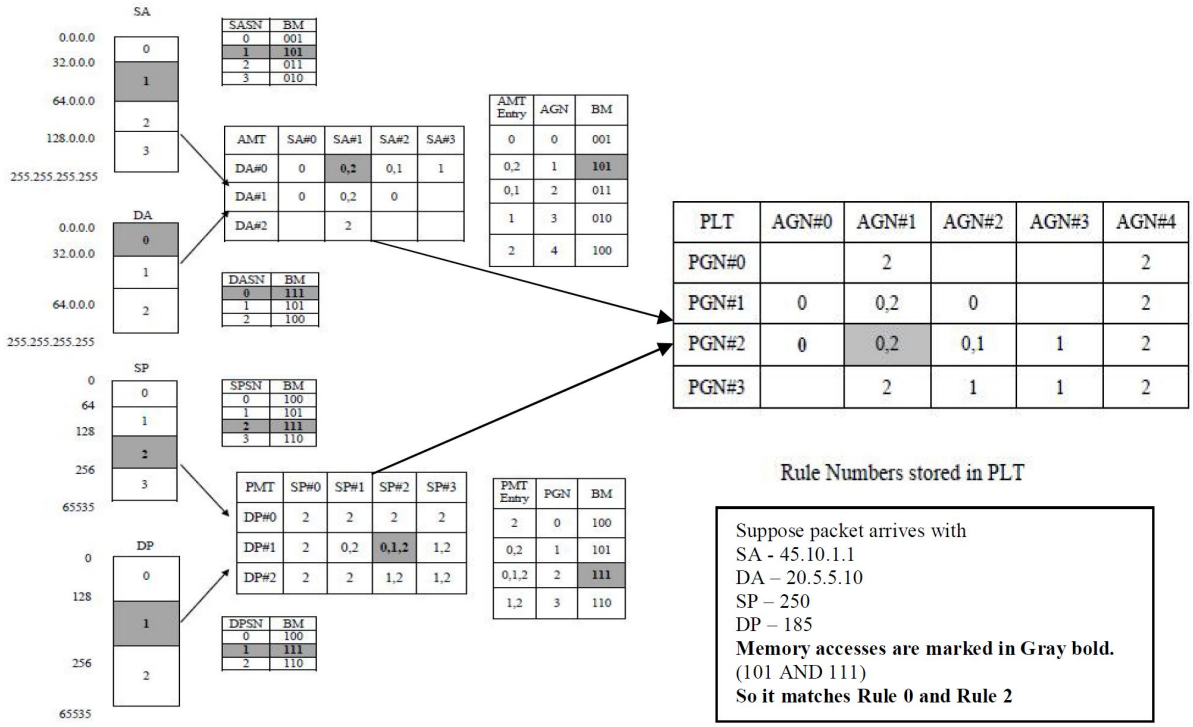

Fig.8. Contents of HSM tables for the example classifier of Table 2. The accesses made by example packet have been shown in gray color.

Table 3: Example Chunk Table for RFC

Rule	Chunk#0 Destination address (32 bits)	Chunk#1 Source address (32 bits)	Chunk#2 Destination port (8 bits)	Chunk#3 Protocol (8 bits)
0	151.161.190.69	151.161.85.1	*	*
1	151.161.5.0	151.161.300.155	80 (www)	TCP
2	151.161.5.0	151.161.300.155	Range 20-21	TCP
3	151.161.5.0	151.161.300.155	80 (www)	UDP
4	151.161.198.3	151.161.200.10	>1023	UDP
5	151.161.198.3	151.161.35.0	>1023	UDP

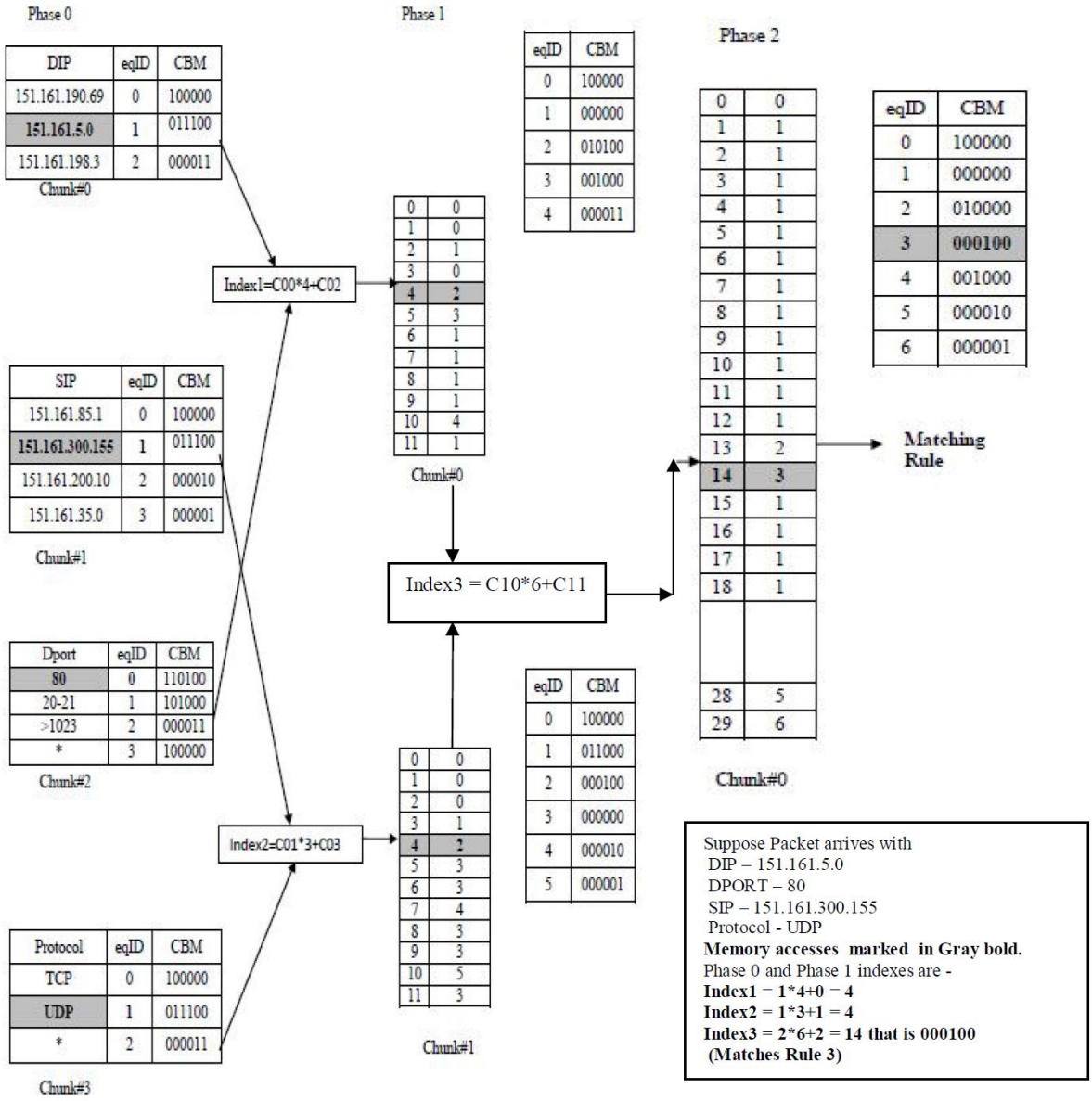

Fig.9. Contents of RFC tables for the example classifier of Table 3. The accesses made by example packet have been shown in gray color.

★★★