Minimizing Range Rules for Packet Filtering Using a Double Mask Representation

Ahmad Abboud, Abdelkader Lahmadi, Michaël Rusinowitch, Miguel Couceiro, Adel Bouhoula

Minimizing Range Rules for Packet Filtering Using a Double Mask Representation

Ahmad Abboud, Abdelkader Lahmadi, Michael Rusinowitch, Miguel Couceiro, Adel Bouhoula

Université de Lorraine, CNRS, Inria, Loria F-54000 Nancy, France

NUMERYX TECHNOLOGIES, France.

Overview

In this work, we introduce a novel representation of packet filtering rules, so called *double masks* [1], where the first mask is used as an inclusion prefix and the second one for exclusion. An efficient algorithm is developed to compute a set of double masks for a given range.

Background and Motivation

Problem Statement

- Large number of hosts affects the size of routing tables.
- Size of blacklists keeps increasing due the increase of number of attacks on the Internet.
- Effective filtering to handle the rapidly increasing and the dynamic nature of network traffic.

Overview of double-mask representation

$$\overbrace{11000000.10101000.01100100.01}^{mask1=26}\ \overbrace{10}^{mask2=2}\ 0000 \quad 192.168.100.96/26/2$$

Example 1 Range [1,14] needs a set of 6 standard prefixes to be represented. However this range can be represented using only two double masks prefixes as shown below :

$$[1,14] = \begin{cases} 0001 \\ 001* \\ 01** \\ 10** \\ 110* \\ 1110 \end{cases} \quad \begin{matrix} \text{simple masks} \\ \\ \\ \\ \\ \\ \end{matrix} \quad \begin{matrix} \text{double masks} \\ \\ \\ \begin{cases} 0000/0/4 \\ 1111/0/4 \end{cases} \\ \\ \\ \end{matrix}$$

Example 2 Range $[1,15]$ is of form $[1,2^4-1]$ and needs 4 simple masks $\{0001, 001*, 01**, 1***\}$ but only one double mask: 0000/0/4.

Benefits of Double Mask

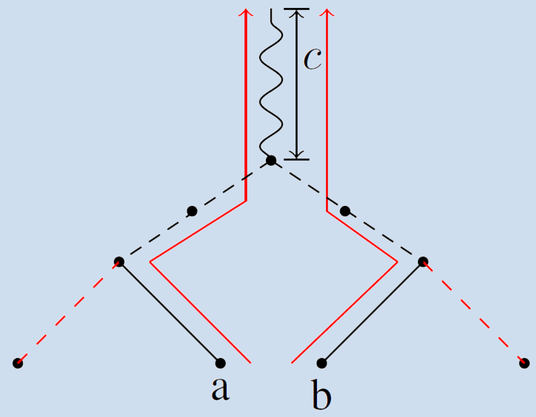
- Reduces the number of entries and therefore packet classification, rules lookup times and memory usage.
- Adds flexibility and efficiency in the deployment of security policies, since the generated rules are easier to manage.
- Makes configurations simpler since we can accept and exclude IPs within the same rule.

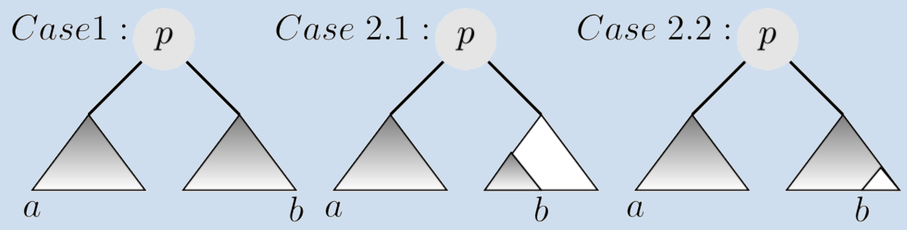
Acknowledgements

This work is supported by a CIFRE convention between the ANRT (National Association of Research and Technology) and the company NUMERYX Technologies.

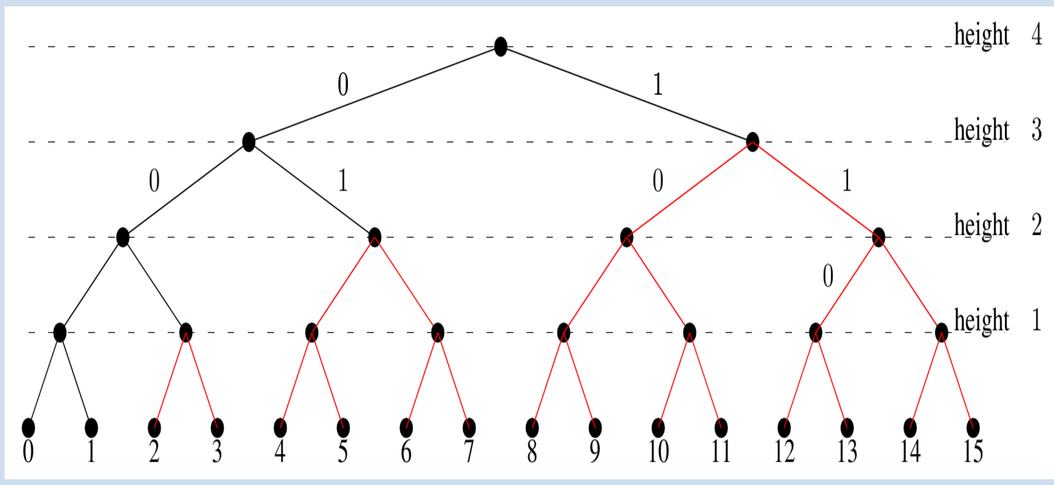
Double Mask Computation

The algorithm computes the set of masks for $[a,b]$ in a bottom up way, starting from the two nodes $bin_w(a)$ and $bin_w(b)$. Then, when reaching node c, the set of computed masks at the siblings of c (i.e., $c0$ and $c1$) are combined and the algorithm stops.



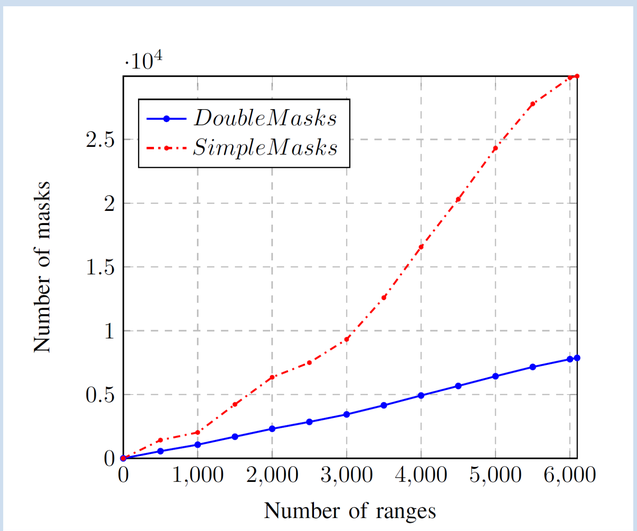


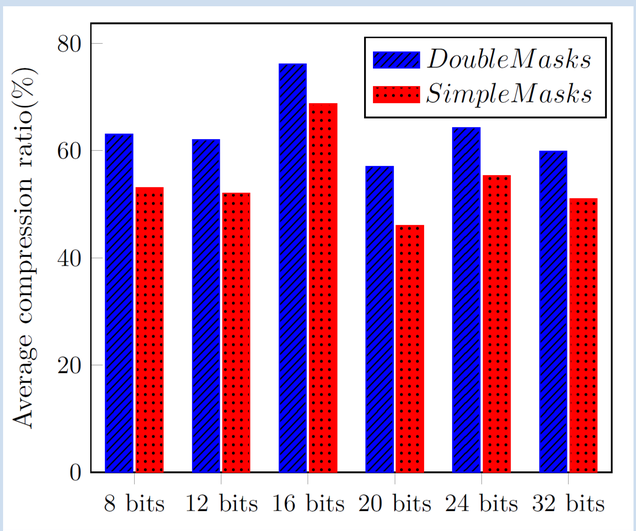
- The algorithm is linear in $|bin_w(a)| + |bin_w(b)|$, where $|x|$ is the length of the binary representation of a and b.
- Each range needs at most $2w-4$ masks to be represented.
- Can also be applied to port ranges and for reducing range expansions in TCAM.
- Can be applied after or in combination with known redundancy removal techniques [2] in order to further reduce the number of entries in filtering rule tables.



Experimental Results

- Over 6000 ranges computed from more than 1.5 millions IPs generated in a synthetic way.
- The total number of generated simple masks is 29958.
- We are able to reduce this number by 74% (i.e. 7872 masks).





- Double Mask representation performs better than Simple Mask with a difference of at least 10% while increasing the number of Bits.

References

[1] ADEL Bouhoula and NIZAR Ben Neji. Double-masked IP filter. Patent, 04 2015.

[2] A. X. Liu, E. Torng, and C. R. Meiners. Firewall compressor: An algorithm for minimizing firewall policies. In *IEEE INFOCOM 2008 - The 27th Conference on Computer Communications*, pages 176–180, April 2008.