ISSN:0975-9646

Secure Multimatch Packet Classification Based on SignatureTree

Pinky M S , Anna Prathibha Shobak

Department of CSE
Mangalam College of Engineering
Kottayam, Kerala, India- 686631

***Abstract*— The new network applications like network intrusion detection systems requires packet classification to report all matched rules instead of the best matched or highest priority rules. Several schemes have been proposed to find multi match packet classification, the most recent method is divide the operation of multi match packet classification from the complicated multidimensional search to several single dimensional searches, and to combine this results here we can using an asynchronous pipeline architecture based on signature tree but it does not support security. In the proposed method initially secret key must be defined to the each node by the Multicast Controller. Secret key should be maintained by the multicast controller. Assume that we have a sender, receiver, and some intermediate nodes. The sender will send the packet in an encrypted format , finally packets will reached to the receiver through an intermediate nodes and at each level the secret should be exchanged. The authorized user only can decrypt the packets. AES encryption/decryption algorithms are used for security purpose.**

***Index Terms*— AES, Multicast Controller, Packet Classification, Pipeline Architecture, Signature Tree.**

I. Introduction

Packet classification refers to finding the best matching filter containing multiple fields in a filter (also called rule) set for a given packet. These multiple fields include the source address, destination address, protocol, source port and destination port. A packet is classified based on the multiple fields extracted from its packet header. Most conventional packet classifiers find only the best matched or highest priority filter that matches the arriving packet. However new network applications like network intrusion detection systems and load balancers demanding multi match classification that is requiring all matching result instead of only the highest priority matches.

Ternary content addressable memories (TCAMs) are increasingly used for high speed packet classification. TCAMs compare packet headers against all rules in a classification database in parallel and thus provide high throughput. However commercially available TCAM is more expensive, consumes more power compared to traditional method. So here we can perform the packet classification without using ternary content addressable memory.

Fig 1 shows the packet classification diagram. Here the packet classifier can able to split the incoming packet in to several packets and it will check rules contained in the rules database.

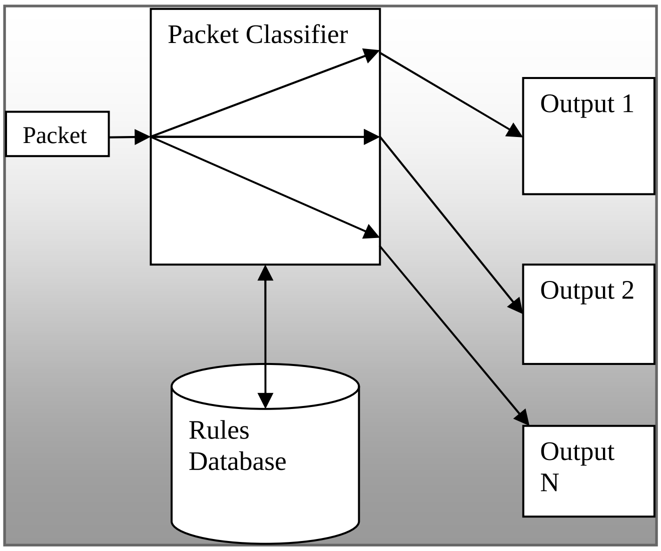

Fig.1. Packet Classification

The main objective of this paper is to provide security. In the proposed method initially secret key must be defined to the each node by the multicast controller. Every receiving node can split the contents in to specified number of packet. At the receiver side contents must be received in the encrypted format. The authorized receiver only can able to decrypt the data. Here we can use AES encryption/decryption algorithm to encrypt and decrypt the data.

The remainder of this paper is organized as follows. Section II describes related work on multi match packet classification. Section III describes about proposed work and implementation. Section IV describes experimental valuation. Section V concludes this paper.

II. Related Work

TCAM is commonly used foe high speed packet classification. In [2] two TCAM based architectures for multi match search are introduced. The first one is a renovated TCAM design that can find all or the first r matches in a packet filter set. The second architecture is a novel partitioning scheme based on filter intersection properties allowing us to use off-the-shelf TCAMs for multi match packet classification. Our classifier engine finds all matches in exactly one conventional TCAM cycle while reducing the power consumption by at least two orders of magnitude, which is far better than the existing hardware-based designs but the memory requirement, is higher than the proposed method.

Presents a scalable parallel architecture, named Para Split [3], for high-performance packet classification. We propose a rule set partitioning algorithm based on range point conversion to reduce the overall memory requirement.

Propose a novel multi field classification scheme, called P2C [4], which exploit the strength of state-of-the-art memory technologies to provide wire-speed classification performance for OC-192 and beyond, in combination with very high storage efficiency and the support of fast incremental updates.

Propose an all-match based complete redundancy removal algorithm [9]. This is the first algorithm that attempts to solve first-match problems from an all-match perspective. We formally prove that our redundancy removal algorithm guarantees no redundant rules in resulting packet classifiers. Layering algorithms [7] are based on approximations for specific variants of interval-graph coloring. We evaluate these algorithms by performing extensive comparative analysis on real-life classification databases.

The range expansion can reduce TCAM utilization because it introduces a large number of redundant TCAM entries. This redundancy can be mitigated by making use of extra bits, available in each TCAM entry. Here this paper present a scheme for constructing efficient representations of range rules [6], based on the simple observation that sets of disjoint ranges may be encoded much more efficiently than sets of overlapping ranges. Since the ranges in real-world classification databases are none disjoint, the algorithms we present split ranges between multiple layers each of which consists of mutually disjoint ranges. Each layer is then coded independently and assigned its own set of extra bits.

The interval expansion problem of TCAMs can be addressed by removing redundant rules in packet classifiers. This equivalent transformation can significantly reduce the number of TCAM entries needed by a packet classifier. Propose an all match based complete redundancy removal algorithm [8]. This is the first algorithm that attempts to solve first-match problems from an all match perspective. One major drawback of TCAMs is their high power consumption. Although Smart PC, the state-of-the-art technique was proposed to reduce power consumption by constructing a pre classifier to activate TCAM blocks selectively, its bottom –up approach restricts its ability of grouping rules in to disjoint TCAM blocks. So we can propose a top-down approach [15] for two-stage TCAM based packet classification.

Packet classification is an enabling technology for next generation network services and often a performance bottleneck in high-performance routers. The performance and capacity of many classification algorithms and devices, including TCAMs, depend upon properties of filter sets and query patterns. Despite the pressing need, no standard performance evaluation tools or filter sets are publicly available. To overcome this problem, we present Class Bench [14], a suite of tools for bench marking packet classification algorithms and devices.

We know that several schemes have been proposed recently to address the multi match packet classification problem, most of them require either huge memory or expensive ternary content addressable memory to store the intermediate data structure, or they suffer from steep performance degradation under certain types of classifiers. To overcome this we can decompose the operation of multi match packet classification from the complicated multidimensional search to several single dimensional searches [1], and present pipeline architecture to combine the single dimensional search result.

III. Proposed Approach

The proposed pipeline architecture has very strong robustness. In the proposed method initially secret key must be defined to the each node by the multicast controller. Secret key should be maintained by the multicast controller. Before any data transmission between the nodes, key must be exchanged. If key matches the data can be transferred. If key does not match data should not be transferred and node should be blacklisted. In the four types of signaling message first secret key should be sent and only if the secret key matches data transmission occurs. Four types of signaling messages are follows.

1) In the Join message secret key must be send from the receiver to the source and used for multicast tree establishment and multicast state refreshment.
2) In the group message secret key must be send from the source to the receiver and used as the response for join message.
3) If both the secret key matches Select message which is used to reselect.
4) In the leave message secret key must be sent from the receiver to the source for the multicast termination.

We can propose the multi match packet classification as a concatenated multi string matching problem, which can be solved by traversing a flat signature tree. To speed up the traversal of the signature tree, here we can divide the edges in to different hash tables in both vertical and horizontal directions. These hash tables are then connected together by using pipeline architecture. They work in parallel when packet classification operations are performed. A perfect hash table construction is also presented, which guarantees that each hash table lookup can be finished in exactly one memory access. Because of the large degree of parallelism and elaborately designed edge partition scheme. The proposed method is able to achieve secure, high packet classification speed with a very low storage requirement.

A. *Fast join and Leave*

The receiver who want to enjoy the multicast service and the receiver who ovens during the multicast session could receive the multicast as soon as possible. Besides the router should immediately stop sending packet to the receiver who want to leave the multicast group. For security purpose we have used AES encryption/decryption algorithm.

B. Minimize the Signaling Cost

To construct and maintain the multicast tree, the signaling messages are necessary. However the signaling message exchange should be simple and the cost should be as low as possible.

C. Efficient Packet Transmission And Reception

Packets have PM destination addresses. The routers that only act for a specific group are responsible for creating packet copies with modified destination addresses. Besides the SDSC should be transmitted through the SPT from the source to the receiver. At the receiver side the contents will be received in encrypted format, authorized receiver only can decrypt the data.

D. Signature Tree

In the signature tree the hash table contents can be splits in to certain amount of packets. Every receiving node can split the content into specified number of packet. At the receiver side the contents will be received in encrypted formats, authorized receiver only can able to decrypt the data by using AES algorithm.

IV. Performance Evaluation

The performance and scalability of the proposed system evaluate only with respect to the security mechanisms.

Fig. 2. Shows the security level. The security level of our proposed method is higher than existing method. Here at each node the packet are divided in to several packets and finally we can combine these packets in to one by using pipelined architecture [1] To improve the security of this packets, here we can use AES encryption/decryption algorithm.

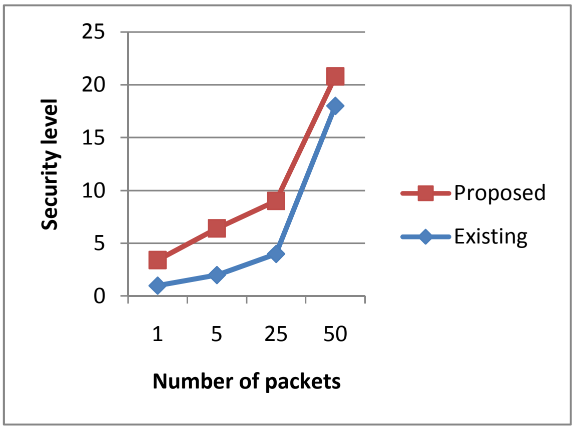

Fig. 2. Security level Vs Number of packets

V. Conclusion

In this paper we can produce a secure multi match packet classification model. In a signature tree, at each node the receiving packet can be split in to several packets. Initially secret key must be defined to the each node by the multicast controller. Secret key should be maintained by the multicast controller. At the receiver side the data will be received in encrypted format, authorized receiver can only able to decrypt the packets. Here single dimensional searches are performed in parallel when the receiving packet arrived and we can combine these results by using pipeline architecture. We can use hash table to store the data in each partition. This paper proposes an AES encryption/decryption algorithm to encrypt and decrypt the data.

Acknowledgment

The first author would like to thanks all those people, who guided and supported and also likes to thank colleagues for their discussions and suggestions.

References

[1] Yang Yang Xu, Zhaobo zhang and H.Jonathanchao, “High-Throughpput and Memory-Efficient Multimatch Packet Classification Based on Disributed and Pipelined Hash Tables”,*IEEE Trans.on networking*,vol.22, no.3,june 2014.

[2] Miad Faezipour, Mehrdad Nourani, “Wire-speed TCAM-based architectures for multimatch packet classification,” *IEEE Trans. On computers*,vol.58,no.1,pp.5-17,Jan. 2009.

[3] Jeffrey Fong ,Xiang Wang ,Yaxuan Qi and Weirong Jiang, “ParaSplit: A scalable architectures on FPGA for terabit packet classification” ,2012 *IEEE* 20th annual symposium on high performance interconnects.

[4] Jan van Lunteren and Ton Engbersen, “Fast and Scalable Packet Classification,” *IEEE Journal on communications*,vol.21,no.4,pp. 560-571, May 2003.

[5] F. Yu, R. H. Katz, and T. V. Lakshman, “Efficient multimatch packet classification and lookup with TCAM,” *IEEE Micro*, vol. 25, no. 1, pp.50–59, Jan. 2005.

[6] A. Bremler-Barr, D.Hay, and D.Hendler, “Layered interval codes for TCAM-based classification,” *Proc. IEEEINFOCOM*, pp. 1305-1313, Apr.2009.

[7] M. Faezipour and M. Nourani, “Cam01-1: a customized TCAM architecture for multi-match packet classification,” in *Proc. IEEE GLOBECOM*, pp. 1-5, Dec. 2006.

[8] A. Liu, C. Meiners, and Y. Zhou, “All-match based complete redundancy removal for packet classifiers in TCAMs,” in *Proc. 27th IEEE INFOCOM*, pp. 111-115, Apr.2008.

[9] Haoyu Song and S. Turner, “ABC: Adaptive binary cuttings for multidimensional packet classification,” *IEEE Trans.on networking*,vol.21,no.1,feb. 2013.

[10] R. McGeer and P. Yalagandula, “Minimizing rulesets for TCAM implementation,” *Proc IEEE INFOCOM*, pp. 1314-1322, Apr.2009.

[11] X. Sun, S. K. Sahni, and Y. Q. Zhao, “ Packet classification consumng small amount of memory,” *IEEE/ACM Trans. Netw*., vol. 13,no.5, pp. 1135-1145, Oct.2005.

[12] I. Papaefstathiou and V. Papaefstathiou, “Memory-efficient 5D packet classification at 40 Gbps,” in *Proc. 26th IEEE INFOCOM*, May 2007, pp. 1370-1378.

[13] Y. K. Chang, C. I. Lee, and C. C. Su, “Multi-field range encoding for packet classification in TCAM,” *Proc. IEEE INFOCOM*, pp. 196-200, Apr. 2011.

[14] D. E. Taylor and J. S. Turner, “Classbench: a packet classification benchmark,” *IEEE/ACM Trans. Netw*., vol. 15,no. 3, pp. 499-511, Jun 2007.

[15] Zhao Ruan, Xianfeng Li, Wenjun Li, “An Energy-efficient TCAM-based Packet Classification with Decision-tree Mapping” 2013 *IEEE.*