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. 4, Issue 5, May 2016

Packet Classification Based Anomaly Detection in Message Transfer Protocol

Parvathy.M[1], Sheeja Agustin[2]

M. Tech Student, Marian Engineering College, Trivandrum, Kerala, India[1]

Asst. Professor, Dept. of CSE, Marian Engineering College, Trivandrum, Kerala, India[2]

ABSTRACT: The packet classification is the process of classifying packets into "flows" in an internet router. The packet classification is done with respect to the predefined rules. Many schemes are proposed for the packet classification. Some schemes are packet classification by using signature tree, packet classification by using BCAM, Packet classification by using TCAM[2] etc. The rules are defined by using the contents are present in the source part of the packet. In this paper we proposed the packet classification, data routing, and anomaly detection. The first step is in this paper is the packet monitoring and packet classification. It is based on the predefined rules. The second step is the data routing in this broadcast the all active nodes. The final step is the anomaly detection; it is the process for find out the bouncing packets. The message transfer protocol defined the proposed protocol standard on multicast routing. The socket communication is used for the message transfer protocol. The sockets are the network socket and it is an endpoint of a connection across a computer network.

KEYWORDS: Packet classification, data routing, Anomaly detection, message transfer protocol, TCAM

I. INTRODUCTION

The use of internet is spread all of world. Most of network application requires the best packet classification mechanism. According to the rule based packet classification, it returned the best matched rules. The objective of this paper is "Packet classification based anomaly detection in message transfer protocol". The rule based packet classification is used for this paper. For this purpose we define the predefined rules. The main fields of the rule set are IP address, port number, protocol type etc. The anomaly detection is proposed by data routing. In the data routing the main operation is broadcasting the data. Many types of algorithms are used for data routing .Such as static routing, dynamic routing, flood search routing, deflection routing. In this paper we used the ALERT routing algorithm for data routing.

The main contribution of this paper is show as follows

1) It model packet classification based on the predefined rules.
2) It model data routing for broadcasting the data.
3) It models an anomaly detection mechanism.

II. RELATED WORK

Many schemes have been proposed to address the problem for best match packet classification. Such as decision tree based scheme [3][4],signature tree based scheme[1][5],TCAM based scheme[2].

The decision tree based scheme is one of the best match packet classification schemes. Decision tree based packet classification algorithms focus on two aspects. The first aspect is how to select the cut dimension and the second aspect is how to decide the cut-point for dividing the address space into subspaces. There are two main methods for pick up the cut dimension: select a single cut dimension at a time and select multiple cut dimensions at a time. When choosing a single cut dimension, the height of decision tree is usually higher than that by choosing multiple cut dimensions. But the node structure size is smaller because of choosing the multiple dimensions needs to keep more information.

The signature tree based scheme is another method for the best match packet classification. Signature tree is the data structure for store strings in the encoded classifier. In the signature tree the hash table contents can be splits in to certain amount of packets. All receiving node can split the content into specified number of packet. At the receiver side the

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. 4, Issue 5, May 2016

contents will be received in encrypted formats, so that the authorized receiver only can able to decrypt the data by using AES algorithm.
TCAM [9] is the ternary content-addressable memory [6]. It is used for high speed packet classification. The power consumption of this is very high [7]. This is the main disadvantage of the TCAM

III. PROPOSED SYSTEM

The main objective of this paper is packet classification based anomaly detection in message transfer protocol. The rule based packet classification [8] is used in this paper. After this packet classification take the IP address of the sender and receiver. According to that IP address we monitor the data .then we get the matched packets. The Alert data routing algorithm is used for the routing the nodes. The main operation on the data routing is broadcasting the data.

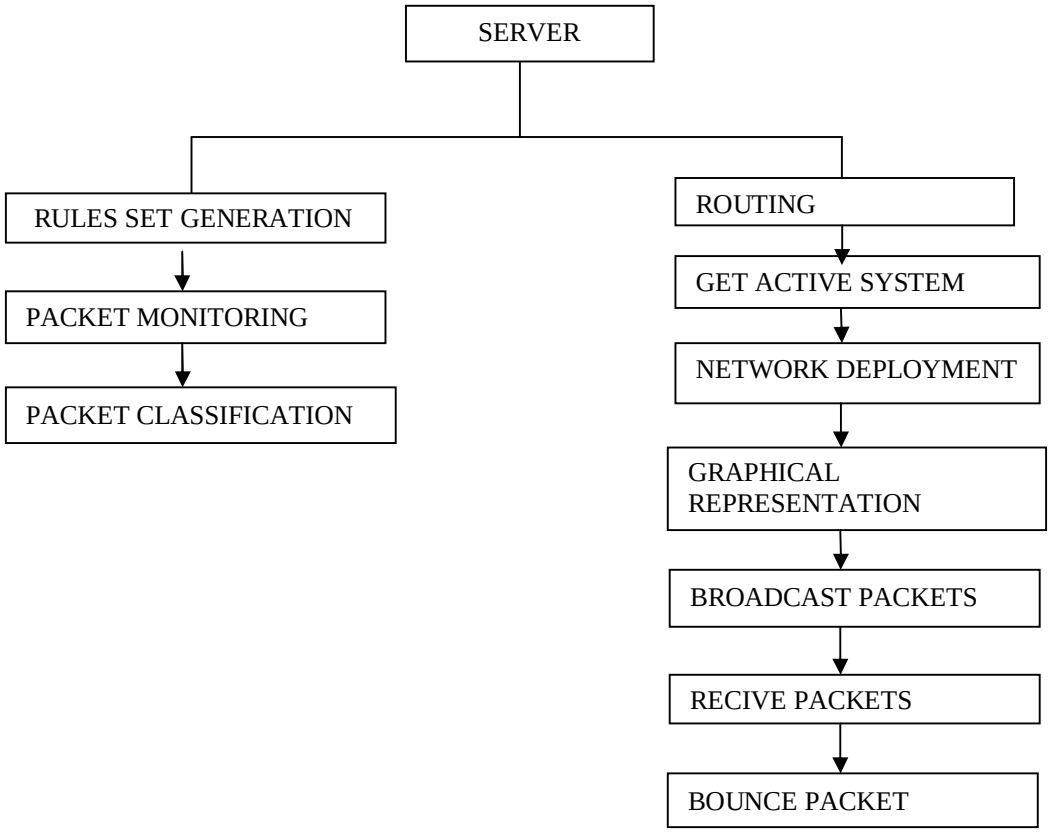

Fig 3.1.Block diagram

A. Packet Classification

The server should do two operations. One is packet classification and other is routing [10]. In packet classification, first define the rule set then monitoring the all packets. After monitoring retrieve the matched packets.

B. Routing

The alert routing algorithm is used for the data routing. First monitor the status of the system that is check whether the system is active or inactive. Then select the all active systems. Graphically represent the all active system then broadcast the packets. When the broadcasting is completed, and then checks the count of send packets, received packets and the packet loss. Finally we get the anomaly by bouncing the packets.

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. 4, Issue 5, May 2016

Anomalies are handled based on the category in which the anomaly belongs to. If the vampire is from the network, then that should be prevented from entering in to the node and from forwarding to another node. We cannot delete that packet because the packet is created by some other node in the network .If any vampire is found inside the node that should be deleted immediately and should prevent from forwarding. For avoiding the entry of anomalies from the network to any packet, all the packets should satisfy no backtracking property. The alert algorithm is explained below

IV. PSEUDO CODE

FUNCTION SECURE_FORWARD_PACKET (P)

```
1.    s ← extract_source_address(p);
2.    a ← extract_attestation(p);
3.    if (not verify_source_sig(p)) or
      (empty(a) and not is_neighbor(s)) or
      (notsaowf_verify(a))
4.    then return ;
5.    for each node in a do
6.    prevnode ← node;
7.    if (not are_neighbors (node, prevnode)) or
      (not making_progress(prevnode, node))
8.    then return ;
9.    c ← closest_next_node(s);
10.   p′ ← saowf_append(p);
11.   if is_neighbor(c)then forward(p′, c);
12.   else forward (p′,next_hop_to_non_neighbor(c));
```

V. SIMULATION RESULTS

The following tests will illustrate how the routing algorithm affects the routing of traffic. These tests will show the effectiveness of the algorithm against the system running without optimization. Since it is possible to switch nodes on and off, a number of test comparisons will be done to show how optimization can improve the routing of a network when paths are no longer valid and new routes have to be chosen.

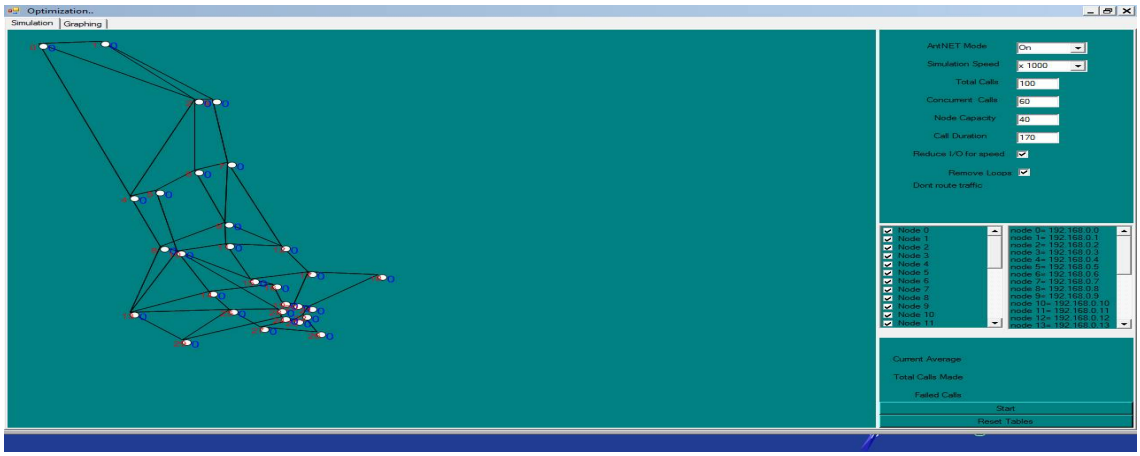

Fig 5.1Data routing

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. 4, Issue 5, May 2016

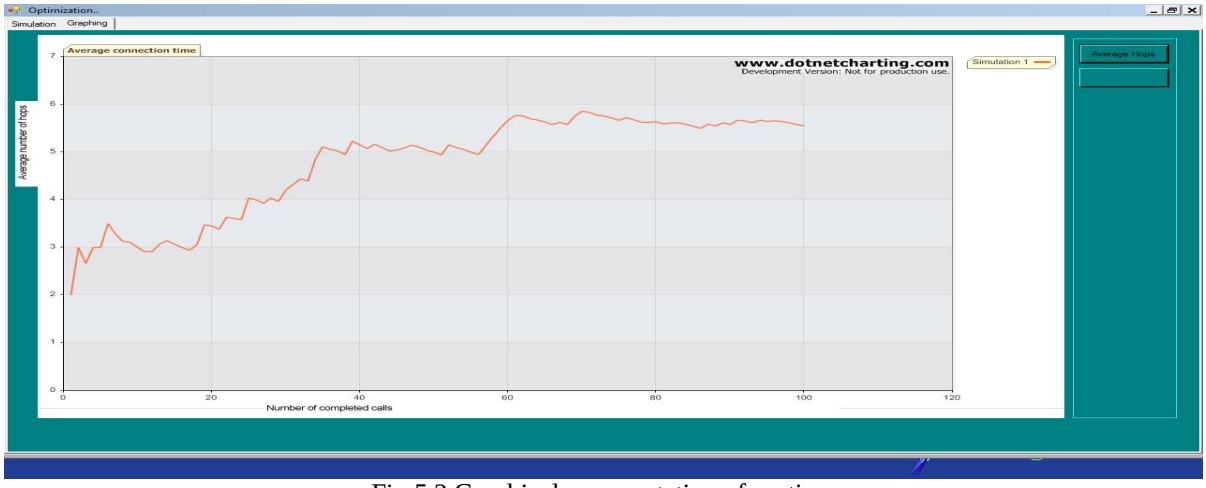

Fig 5.2 Graphical representation of routing

These tests have been run with the following parameters:

- Simulation speed -1,000 tick p/s
- Total calls to make – 100
- Maximum concurrent calls – 60
- Node capacity – 40
- Call duration - 170 (the length (in ticks) of a call)
- Reduce I/O - bypasses the network visualization to increase simulation speed
- Return on connection - returns the node immediately to source after connection

From this simulation, it is clear that even by the first 100 calls completed; optimization has reduced the average number of hops by approximately 1.5 nodes. This is made more apparent by the end of the simulation where the best paths are made more biased as a choice, and are re-enforced as the optimal route, resulting in improving network performance by almost 3.5 hops. To view the algorithm from a different perspective, the following graph depicts the system running with the algorithm off and then activated on the 2,000th call. This can be identified by a label, and follows with a decline of average hops by almost 2

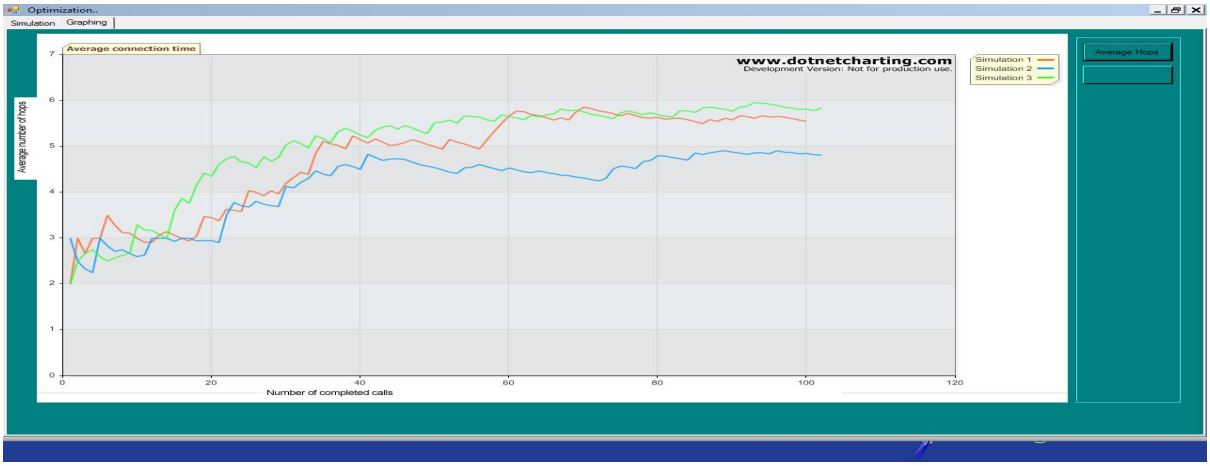

Fig 5.3 Performance analysis

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. 4, Issue 5, May 2016

VI. CONCLUSION AND FUTURE WORK

In this paper, we model the multimatch packet classification and the data routing. The data routing is done by the Alert algorithm. The anomalies are calculated by bouncing the packets. By using the routing protocol the anomaly detection is makes fast.

REFERENCES

1. Yang Xu, Member, IEEE, Zhaobo Liu, Zhuoyuan Zhang, and H. Jonathan Chao, Fellow, " High- Throughput and Memory-Efficient Multimatch Packet Classification Based on Distributed and Pipelined Hash Tables", IEEE/ACM Transactions On Networking, Vol. 22, No. 3, June 2014 .
2. M. Faezipour and M. Nourani, "Wire-speed TCAM-based architectures for multimatch packet classification," IEEE Trans. Comput., vol. 58, no. 1, pp. 5–17, Jan. 2010.
3. P.Guptaand N.McKeown, "Classifying packets with hierarchical intelligent cuttings," IEEE Micro, vol. 20, no. 1, pp. 34–41, Jan.–Feb. 2000.
4. S.Singh, F.Baboescu, G.Varghese, and J.Wang, "Packet classification using multi dimensional cutting, "in Proc. SIGCOMM, New York, NY, USA, 2003, pp. 213–224
5. Pinky M S "Secure Multimatch Packet Classification Based on Signature Tree" etal/IJCSIT ,Vol.6(2),2013
6. M. Faezipour and M. Nourani, "Cam01–1: a customized TCAM architecture for multi-match packet classification," in Proc. IEEE GLOBECOM, Dec. 2006, pp. 1–5.
7. F. Yu, R. H. Katz, and T. V. Lakshman, "Efficient multimatch packet classification and look up with TCAM,"IEEE Micro,vol.25,no.1,pp. 50–59, Jan. 2005.
8. P. Gupta and N. McKeown, "Algorithms for packet classification," IEEE Netw., vol. 15, no. 2, pp. 24–32, Mar.–Apr. 2001.
9. D. Pao, Y. K. Li, and P. Zhou, "An encoding scheme for TCAMbased packet classification," in Proc. 8th ICACT, Feb. 2006, vol. 1, pp. 470–475.
10. M. Degermark, A. Brodnik, S. Carlsson, and S. Pink, "Small forwarding tables for fast routing lookups, "Comput. Commun. Rev., vol. 27, pp. 3–14, Oct. 1997

BIOGRAPHY

Parvathy.M is a M.Tech Student in the Computer Science department, Marian Engineering College, Kerala University.
Sheeja Agustin is an Asst.Professor, in computer science department, Marian Engineering College, Trivandrum, Kerala, India