Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 4, April 2014, pg.898 – 903

RESEARCH ARTICLE

Enhancing Probabilistic Packet Marking by Integrating Dynamic Probability and Time to Live (TTL) Clustering

Souzan Asadollahi

Advanced informatics school (AIS), University of Technology Malaysia, Kuala Lumpur, Malaysia

Souzan.asadollahi@gmail.com

Abstract— In recent years, Denial-of-service attacks emerged as a pressing problem. Since a lot of attention has been placed on Denial-of-service defense research and a number of approaches have been proposed. One suggested solution is "IP Trace back" which is referred to as tracing malicious packets back to their origin. It categorized in several methodology. Packet Marking from this category is the subject of our study. In this paper, we focus on "Probabilistic Packet Marking (PPM)" which is inefficient in the case of Distributed Denial of Service (DDoS) attacks due to high false positive in reconstructing attack graph and also high convergence time. We adopt the dynamic probability along with Time to Live clustering method in order to reduce the rate of false positive and convergence time. We envision DDoS attack starts when network traffic is more than our default threshold. In an abstract view, we have considered dynamic probability rather than fixed, which is the root problem in most Probabilistic Packet Marking (PPM) and also to facilitate the fast reconstructing of attack graph, we exploit TTL field in two folds: one time to live and another one identification field for packets' fragments coming from same distance. Consequently, our experimental results show how our model would be efficient in comparison with some pervious methods.

Keywords— Distributed Denial of Service (DDoS); IP Trace back; Probabilistic Packet Marking; Time To Live; Traffic

I. INTRODUCTION

New attacks are emerging daily and Distributed Denial of Service D(DoS) attacks are among the most malicious where attackers prevent legitimate and authorized users access to resources [1]. Identifying D(DoS) attacks and defensing against them are one of the network security's gravest concerns to protect vital services and information. Recently, several schemes proposed to detect and/or prevent such attacks which are known as IP Trace back. IP Trace back refers to various techniques, which trace the attack flow to find the attack path. It may not be necessarily focused to find the attacker(s) because attackers mostly use forged IP addresses or source nodes. Packet Marking is one of the classified methods of IP Trace back. Packet marking techniques allows router to inscribe their IP on incoming packets either deterministically or probabilistically. By collecting and analyzing the marked packets, victim should able to reconstruct the attack path leading back to the nearest source of attack. In this literature, we have focused on this type of approach due to the Ineffectiveness to address large-scale DDoS attacks.

II. BACKGROUND OF PROBLEM

A. Probabilistic Packet Marking

In 2000, savage [2] proposed probabilistic Packet Marking which is the forerunning method from the series of IP trace back as the cornerstone of current methods. In this type of marking protocol, packets are marked based on predefined probability. It suffers some serious problems as explained in following section.

B. Some Existing Problems in Initial PPM

1) *High False Positive Ratio,* The 32 bits IP address including 16 bits ID field where the marking is stored is the common problem in many IP trace back methods because of limited rooms in IP header for storing the address of routers. Another is entrenched in the reconstruction algorithm paths, some routers may be in the same distances that caused confusion of the victims. Two steps are required for path reconstruction in PPM. One is the recovery of the 32-bit IP address of each router from several packets, another is the recovery of the whole path. In PPM, 8 packets marked by the same router need to be identified and combined to recover the IP address of that router. Since there is no hint except the distance field, it is difficult for the victim to identify which marked packets come from which router when many routers are located at the same distance from the victim. Similarly, the victim cannot identify packets that are launched from the same attack source and traverse the same path because no clues are provided in PPM, thus seriously hampering the recovery of that path.
2) *Fixed Marking Probability,* based on previous studies, it is recognized the root problem of most Probabilistic Packet Marking is the fixed probability. On the other hand, in traditional method, the best value of probability is 1/d (d is the number of hops from attacker to victim). According to [3] , dynamic probability could solve the problem of low accuracy in somehow.

III. RELATED WORKS

First, we have an overview on PPM and then move to introduce our proposed method in next section. The idea of PPM is explained previously. It is the emphasis of this research. As we mentioned before, the idea of PPM was first proposed in [2]. In this method, every packet is assigned a mark with a pre-defined probability while it passes through each router along the attack path to identify the attacker after the attack. They described a Trace back algorithm, which is add a marginal overhead to the routers in path forwarding. Moreover, they assume encoding the necessary path information in a way that peacefully co-exists with existing routers, host systems and more than 99% of today's traffic.

A Probabilistic Packet Marking with non-preemptive with compensation was a new novel which proposed by Tseng et al.[4]. The main goals of them were modification on PPM, which ensures equal probabilities in between probability of receiving marked packets and original. However the disadvantages of this method caused marked packets from distant routers remarked by downstream routers. This leads to loss of information sent from distant routers and increases the number of packets required to reconstruct the path. Meanwhile, previous research showed that (p=1/*d*) , where *d* is the distance between victim and attacker, is ideal probability marking. However, it is not ideally achievable, as the value for *d* is not always fixed for known victims.

Unlike the pervious schemes in PPM, Tseng.Y et al. [6] suggested an improvement on original PPM to reduce the computing overhead stemming from combine fragments. They calculated the unique ID and initialize TTL with it. This ID must be the same for 8 fragments. As a result of that false positive is reduced dramatically and also it improves the response time to DDoS attack. Before every IDPPM- enabled router, takes an action to mark a packet. It has to calculate this ID and inscribe it into TTL field of own fragments by equation 1:

$$TTL= f_2 (IP_i) \bmod 256 . \qquad (1)$$

Where i is the number of router and f_2 is the arbitrary hash function. This amount should be between 30 and 255 in order to guarantee that victim receives marked packets. If the amount is smaller than 30, then it should be set to (TTL+30) at the victim's side. After receiving all fragments, it can verify and examine the values: f_2 (IP $_i$) mod 256 equals to some of the TTL and distance field value (numbers of routers on the attack path) . If two values are not equal, then compare (TTL+distance – 30) with (f_2 (IP $_i$) mod 256) .If both equations are not true, then false positive occurs and the packets have to be dropped .We exploit this advantage for our proposed method to distinguish the incoming fragments originating from the routers which are in the same distance.

The main idea behind [3] is that they set all the probability of routers to 1/25, which is the best value in traditional method. At any time packet passes through the router, it will observe the value of the flag tag, firstly. If flag=0 , it recognizes that the packet has not been marked before so decides whether to mark the packet with probability of 1/25 or not . If packet has been marked then the probability should change to p=1. It should be remarked that probability should be kept on 1/25. While flag=1, it means that this packet has been marked previously and just increase the distance field by one. Furthermore, when the p=1 it is ensured that IP address of the current router will be marked by other unoccupied incoming packets. Due to ineffectiveness of this method against DDoS attacks, we have adopted it with IDPPM .The pseudo code and results will be presented in following sections.

IV. OUR PROPOSED ALGORITHM

In this section, we present our new integrated algorithm which is efficient in reducing false positive ratio and convergence time. First, we explain the marking mechanism and pseudo code of the algorithm and then analyze the experimental results.

A. *Marking algorithm*

Based on pervious researches [3][4][5], fixed marking probability is the main problem of PPM. Different methods were introduced to fix this issue but unfortunately none of them could succeed to resolve the issue completely. According to [3], dynamic probability could somehow solve the problem of low accuracy. But it still needs improvement in other aspects.

In simple terms, our aim is to design an approach, which would remarkably reduce the false positive rate in multi-source attacks using dynamic probability. We assume that not all incoming packed are marked probability. Instead, we consider routers to be marked either with p=1 or p=1/d .We also employed dijkestra algorithm [7] which is placed in router in order to route packets as a routing algorithm. So in this case we do not need to know the attack path's length in advance because the algorithm will calculate the length from current router to the attacker automatically. The flag according to [3] demonstrates whether this packet has been marked before or not. If it has been marked before then the marking probability will be changed to 1, this helps the prevention of being overwritten by downstream routers otherwise it should be marked with p=1/d. (note that d is the distance of router from victim) [9]. Also, marking format in IP header is shown as Fig1.

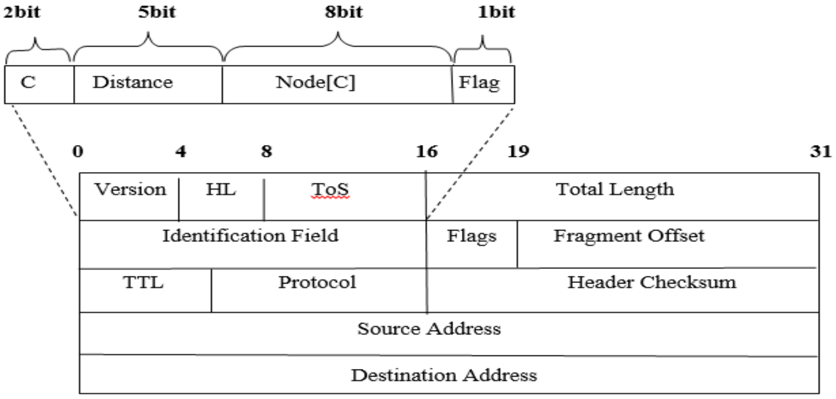

Fig. 1 The structure of marking algorithm in IP header

Below are the details of IP header in our enhanced algorithm:

C: Which part of IP address is being received?

Distance: How far current node from victim

Node[C]: denotes Cth segment of Routers IP

In marking mechanism in spite of exploiting dynamic probability, we used another method to reduce the false positive rate. Because of the problem in addressing DDoS attacks and also adding authentication function, we suggest TTL coding which is discussed in[6]. So, in case of receiving packets from the same distance we will consider TTL value which should be the same in all incoming fragments. The pseudo code of the scheme explained in following.

Marking Algorithm

```
 Let x be a random number [0…1)
 IP[c]={ip[0] , ip [1] , ip [2] , ip [3]}

If x < p & w.flag=0 then

   Write router's address into w.start
    TTL=$f_2$ (IP)mod 256

            If TTL<30 then TTL ←TTL+30
                w.flag=1 & p=1/d

                w.start=c++(mod4)
                 Node[c] ← IP[c ]

              else
                 If w.flag=1 then
                 P=1
   endif
     d++
 end if
```

B. Reconstruction procedure:

The Second part of our method is to detect and reconstruct the attack path by collecting marked packets. So, in this step we have to reassemble these fragments to map the attack path. All incoming packets are clustered according to their distances.[8] Also, Packets with same distances goes to the appreciate cluster based on their TTL.

Reconstruction Algorithm

```
 Let Node.tb1 be a table of (node , distance , TTL)
  For each packet w from attacker
       Z:=look up w.node in node tb1
 If Z<> null then
           Insert tuble(w.node ,1) in node tb1
 If TTL(w.node)mod 256 = TTL+d or ttl+d-
 30

    then
 Sort node tb1 by distance and by TTL value Extract
path ( Ri ….R j) from ordered node fields in node
tb1
```

V. EVALUATION AND EXPERIMENTAL RESULT

Fig .2 presents the comparison of the other methods similar to our scheme. The experimental topology includes one victim and number of attackers along the attacking path. All examined algorithms are compared by measuring the respective average reconstruction time under different distances. Moreover, we benchmarked false positive ratio of these algorithms under different number of attackers. As shown in Fig.3, false positive ratio increased gradually when number of attacker increases. Also, we have to emphasize the false positive happened when packet fragments are placed in a wrong cluster therefore our proposed reconstruction algorithm is not to recover the router's address properly.

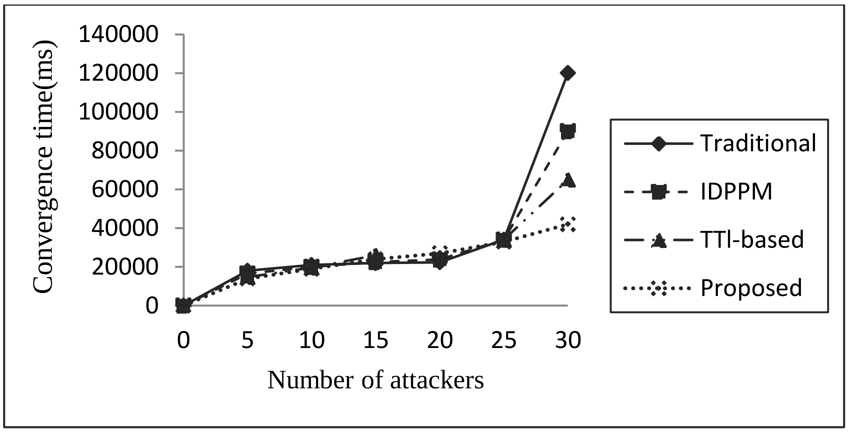

Fig. 2 Convergence Time Ratio

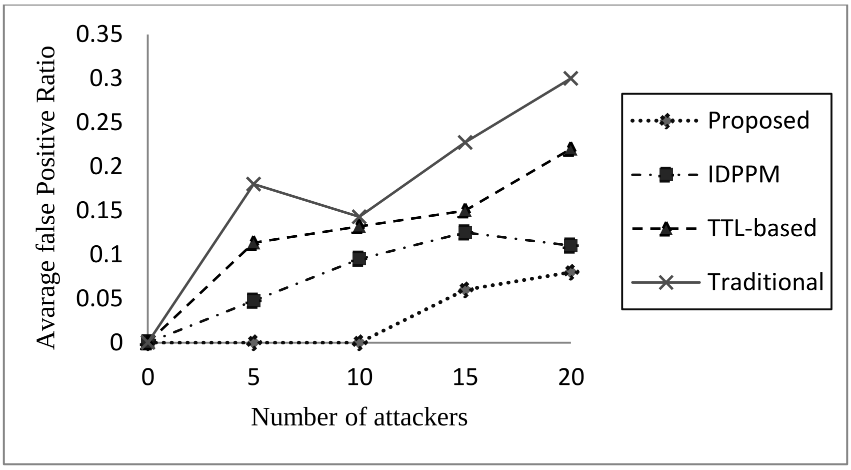

Fig. 3 Avarage False Positive Ratio

VI. CONCLUSION

In this paper we contributed to the design and implementation of efficient and optimized Packet Making Algorithm. As mentioned previously, probabilistic packet marking (PPM) has a high false positive ratio and also does not perform well in the event of DDoS attacks. To overcome the limitations of PPM that we have mentioned, we used dynamic marking probability in order to reduce the convergence time and rate of false positive. In this method, we utilized two type of marking p=1/d where d is a length of path traversed by packet and p=1. Indeed, we have successfully exploited TTL in two ways: coding the TTL placed in a TTL field to identify the same fragments and recognize the time to live (TTL) of packets. Hence, two algorithms were implemented and coded to produce experimental results where the outcome was achieved by comparing the traditional algorithm’s result against the improved algorithm’s result. Of course, this algorithm is not perfect and needs further improvement.

REFFRENCES

[1] U .Tupakula and V. Varadharajan (2010). Analysis of Trace back Techniques. [Online] . Available: http://crpit.com/confpapers/CRPITV54Tupakula.pdf.

[2] Savage .D.Belenky, A.Wetherall, A.Karlin and Anderson. “Network support for IP trace back”. IEEE/ACM Transnet working, 2001. Vol 9, pp. 226–237

[3] F.bo, G.Fan and D. Mingling. “Dynamic Probabilistic Packet Marking Based On PPM”. *Web mining and Web-based Application. WMWA '09. Second Pacific-Asia Conference on.2009*.p. 289 – 292.

[4] Y.Tseng, H.Chen and S.Wen. “Probabilistic Packet Marking With Non-Preemptive Compensation”. *IEEE COMMUNICATIONS LETT. VOL 8, PP. 359 – 361*.June. 2004.

[5] Y. Tseng, Y.Lu, J. Huang, W. Hsieh, B.Chang, Y.Chen and Sh.Chen. “ID-Based PPM for IP Trace back”. *ICICIC '06. First International Conference on..2006.* p. 264-265

[6] V. Paruchuri, A.Durresi and S. Chellappan. “TTL based Packet Marking for IP Trace back”. *Global Telecommunications Conference. IEEE GLOBECOM 2008. P. 2552-2556*

[7] M.Yan (2010). Dijkstra Algorithm. [Online]. Available: http://math.mit.edu/~rothvoss/18.304.3PM/Presentations/1-Melissa.pdf

[8] C. Vaiyapuri and R. Mohandas. “IP Trace Back Scheme for Packet Marking and Packet Logging Using RIHT”. IJCSMC, Vol. 2.pp. 429 – 432.