http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 8 (4): 504-512, 2009
ISSN 1812-5638

A Maekawa Set Based Marking Scheme

[1]Zaihong Zhou, [2]Dongqing Xie and [1]Bingwang Jiao
[1]School of Computer and Communications, Hunan University, Changsha, China
[2]School of Computer Science and Educational Software, Guangzhou University, Guangzhou, China

Abstract: This study describes a novel Maekawa-set-based probabilistic Marking Scheme (MMS). It aims at the disadvantages of the FMS scheme, which are the large number of false positives caused by fragment marking and the need of network topology in node exclusive-or (XOR) restore, etc. The MMS scheme is to split the edge, which is composed of the IP addresses of two neighboring routers into fragments and allocates fragment-id for each fragment. Then, it will generate a Maekawa set based on those fragment-ids. The number of subset is m and the length of subset is k for the Maekawa set. While packets pass through a router, the router will write the k fragments orderly to the IP header by m times with an optimal probability, where the fragments are split from the edge and recombined in Maekawa subset way. There is no false positive in this MMS scheme after the attack path is reconstructed theoretically. In addition, it has several other advantages, it requires fewer packets to reconstruct the attack path; computation overhead is low; it does not require the network topology support as well as is able to prevent the hijacked router from forging the markings.

Key words: DDoS attacks, traceback, fragment, packet marking, path reconstruction

INTRODUCTION

Due to the vulnerabilities that DDoS attack is easily launched and hard to defend, there are lots of such attacks occurred in the Internet. Currently, it is one of the most serious threats on Internet. There are many ways to countermeasure DDoS attack such as tracing the attack packets path and constructing the attack path back towards the attack source. However, the stateless nature of Internet routing and the IP-spoofed DDoS attack make the traceback hard.

Regarding DDoS traceback, many researchers from different countries proposed some solutions from different aspects such as logging scheme (Spatscheck and Peterson, 1999; Baba and Matsuda, 2002; Snoeren *et al*., 2001), ICMP traceback (Mankin *et al*., 2001), Pushback (Ioannidis and Bellovin, 2002; Lee, 2004), Center Track (Stone, 2000), packet marking (Savage *et al*., 2001; Song and Perrig, 2001), ingress filtering and link testing (Burch and Cheswick, 2000). Among them, packet marking is a promising scheme for traceback because it has the features of low management overhead, low network payload, low computation overhead, good security performance and the support of incremental deployment.

Savage proposed a probabilistic Fragmental Marking Scheme (FMS) (Savage *et al*., 2001). The idea is that routers mark the edge composed of local router and the next router IP addresses into the IP header with some probability while packets pass through them. Because of the space limitation in IP header, Savage utilized the way to fragment the edge. FMS firstly proposed to use the probability method to mark the packet so that it avoids to marking all packets passing through routers. It only uses the existing spare fields-ID filed in the IP header so that no extra overload has been introduced. However, the fragment scheme makes the victim end have high false positives while reconstructing the attack path. FMS scheme also used XOR after fragment. When fragments reordered, the victim end has to use a⊗b⊗b to get a back (since a⊗b⊗b = a) where a, b is in the IP header, b is provided by network topology, which is hard to obtain. Moreover, this FMS scheme does not validate the marking information so that it cannot prevent the hijacked nodes from forging the markings.

In order to solve these problems, Song and Perrig (2001) proposed advanced and Authenticated Marking Schemes (AMS) for IP traceback. AMS still utilizes the ID field in IP header to overload the marking information. The marking information is compressed by hash and XOR. But with the collision of hash function, the false positives are still high. To prevent attackers from forging the marking information, AMS adopts MAC (Message Authenticate Code) with secret key to authenticate the marking information. In this way, the distribution of the secret key is difficult. While reconstructing the attack path, it requires the network topology infrastructure in advance to attain whose IP is matched with the calculated value.

Corresponding Author: Zaihong Zhou, School of Computer and Communications, Hunan University, Changsha, 410082, China

Dean *et al.* (2002) introduce an algebraic approach to probabilistic packet marking, but it does not scale to large number of attackers. Yaar *et al.* (2005) proposed FIT scheme which uses node sampling and 1-bit distance to reduce the number of false positives and the number of packets required for attack path reconstruction and marking space. But the number of false positives is still high and the network topology is required. Law *et al.* (2005) add statistical analysis to an existing probabilistic packet-marking scheme. Goodrich combines the approach and presents a marking scheme that marks nodes instead of links into packets (Goodrich, 2008). Because, the two approaches do not use a distance field, they have issues with attack graph reconstruction and do not scale to a large number of attackers. Ogawa *et al.* (2003) proposed to mark the full path instead of the partial path into the option field in the IP header. It uses option field, thus additional overhead is introduced into the routing process. This also probably leads to packet fragmenting. Tseng *et al.* (2006) proposed to use hash function to make the fragments from the same router in FMS have the same identification based on the router's IP address and write the same identification into the TTL field in the IP header. The recombination overhead for fragments in FMS is reduced and the reconstruction for attack path is accelerated. Because of the collision in the hash function, the false positives still exist. Liu *et al.* (2003, 2005) and Li *et al.* (2007) have done some research on the marking probability. The router generates a marking probability according to the distance that a packet passed through. The number of packets required for reconstruction is heavily reduced. Ma (2005) adopted the strategy of controlling the marked packet not being rewritten and optimal probability (Ma and Tsang, 2007) to reduce the number of packets required for reconstruction. There are some other schemes to reduce the false positives. But all these schemes have not thoroughly solved the problems-large number of false positives, the requirements for network topology and without authentication for marking information - in FMS.

For the disadvantages of the existing PPM, we propose a novel trace scheme-Maekawa-set-based Marking Scheme (MMS). The MMS scheme will divide the edge composed of two neighboring routers' IP addresses into fragments and allocate corresponding fragment-id for each fragment. Then it will create Maekawa set S on fragment-ids by Maekawa algorithm (Maekawa, 1985), $S = \{ S_i \}\ 1 \le i \le m$, $S_i = \{j | 1 \le j \le n\}$, $|S_i| = k$. When packets pass through a router, the router will write the k fragments, which are corresponding with S_i ($|S_i| = k$) into the IP header with an optimal probability q. Each edge will be written to the IP header in m times.

MAEKAWA-SET-BASED PROBABILISTIC MARKING SCHEME

Basic idea: When a packet passes through a router, the router marks the edge constituted from the current router's IP address and the next hop's IP address into the IP header of the packet with an optimal probability. In order to reconstruct the attack path at the victim end, the distance from the marked edge to the victim is marked into the IP header too. Because, the hop count from a marked edge to a victim is less than 32 hops, 5-bit space is sufficient to store the distance. Thus, the total space for storing the marking information is 69 bits. To reduce the marking space requirement, the edge is split into fragments, but the false positives will be high because of the combination of fragments. Adequate fragmental redundancy of the edge will help to solve the problem. The dependence and constraints among the marking information are created. The dependence is benefit to the reconstruction of attack paths and the constraints are to check the reordered edge whether it is correct or not. The simple method to create the dependence and constraints between marking information is to set any two fragments in to fragment-pair. Any change in fragment-pair will lead to the collision to other fragment-pair and then the reordered edge is unique. If an edge is split into r fragments, the marking times are too many, which are C_r^2 times. To reduce the number of markings, Maekawa set is used to obtain optimal marking length and the marking times.

Maekawa set: Maekawa set is an optimal algorithm to achieve mutual exclusion in a distributed system. In a distributed system with N nodes, to create a Maekawa symmetric set $S_i (1 \le i \le N)$, it must satisfy the following four conditions:

- $\forall\ i,j \in [1,N]$, $S_i \cap S_j \neq \phi$. That is, the intersection of any two-request sets is nonnull
- $\forall\ i,\ j \in [1,N]$, $i \in S_i$. That is, subset S_i always contains node i
- $\forall\ i,j \in [1,N]$, $i \neq j, |S_i| = |S_j| = \ldots = k$. That is, the size of S_i is k for any i
- $\forall\ i,j \in [1,N]$, $|\{S_i | i \in S_j, j \in [1,N]\}| = k$. That is, any node belongs to k request sets

These conditions have guaranteed the relationship between any two nodes in a distributed system is expressed and constrained in some subset. The Maekawa set applied to the problem would give us an optimal value

S_1 = {1, 2, 3, 4}
S_2= {2, 5, 8, 11}
S_3= {3, 6, 8, 13}
S_4= {4, 6, 10, 12}
S_5= {1, 5, 6, 7}
S_6= {2, 6, 9, 12}
S_7= {2, 7, 10, 13}
S_8= {1, 8, 9, 10}
S_9= {3, 7, 9, 11}
S_{10}= {3, 5, 10, 12}
S_{11}= {1, 11, 12, 13}
S_{12}= {4, 7, 8, 12}
S_{13}= {4, 5, 9, 13}

Fig. 1: Maekawa set with N = 13, m = 13, K = 4

S_1= {1, 2, 3}
S_2= {2, 4, 6}
S_3= {3, 5, 6}
S_4= {1, 4, 5}
S_5= {2, 5, 7}
S_6= {1, 6, 7}
S_7= {3, 4, 7}

Fig. 2: Maekawa set with N = 7, m = 7, K = 3

of marking length and the marking times to achieve accurate attack path reconstruction.

The fragment-ids of fragmented edge are corresponding with the node numbers N in Maekawa set. Both N = 13 and N = 7 satisfy the equation N = k (k-1) +1, there exists a corresponding S_i symmetric set. The corresponding Maekawa set created by Maekawa algorithm (Maekawa, 1985) is depicted in Fig. 1 and 2.

Marking strategy based on maekawa set: The marking edge made up of the IP addresses of router R_i and R_{i+1} is split into N fragments. The marking edge is written into m different packets according to the created Maekawa set. The marking sequence number is generated orderly and k fragments are marked every time. The order of k fragments is the same as the order of the element in subset S_i. If the edge is marked by the Maekawa set with N = 13, m = 13, k = 4, the edge is split into 13 fragments where each fragment for the first 12 fragments is composed of 5 bits, the 13th one is a 4-bit fragment. The fragment-id 1, 2…13 is allocated. Four fragments are marked into a packet each time; all fragments are marked completely in 13 times. Because, the more the marking times are, the more the number of packets required for reconstruction is. Therefore, we mark the edge according to the Maekawa set with N = 7, m = 7, k = 3 in this scheme. The edge made up of the IP addresses of router R_i and R_{i+1} is split into 7 fragments.

```
Marking Procedure at Router Ri
MARKING (q,c,k,fb)
For each packet P
Let u be a random number from [0, 1)
If  u<=q then
      j:= j mod c+1
      p.cfragno:=j
       p.cfrag:=""
       For L=1 to k
          p.cfrag:=p.cfrag+subs      (IP
           (Ri) +IP (Ri+1), S[j] [L]-1)*fb
           +1, fb)
       Endfor
   p.distance:=0
Else
   p.distance:=p.distance+1
Endif
Endfor
```

Fig. 3: Marking algorithm

where, each fragment for the first 6 fragments is composed of 9 bits, the 7th one is a 10 bit fragment. The fragment-id 1, 2…7 is allocated. The edge R_iR_{i+1} information is marked by 7 times and 3 fragments are marked into a packet each time. Let cfragno be the marking sequence number and it is generated orderly. The marking information is the combination of the fragments corresponding with the value of the elements in subset $S_{cfragno}$ and let the marking information be cfrag. For instance, when cfragno is 2, the 2, 4, 6 fragments of edge are marked into the IP header of a packet. When cfragno is 6, the 1, 6, 7 fragments of edge are marked into the IP header of a packet. In order to reorder, the cfragno and the distance are also marked into the packet. The number of bits used for 3 fragments is 28; cfragno is the range from 1 to 7, so 3 bits are required for storing it. Adding up 5- bit distance, the total number of bits used for the information is 36. In IP header, 16-bit ID, 13-bit offset, the 7-bits of 8-bit TOS can be utilized for the marking information in our scheme. The 16-bit ID is used to record the identification of fragment, but at present network, only less than 0.25% of packets are fragmented. And the MTU protocol is used to negotiate the size of transferred packets to avoid fragments. So the ID is used to mark in FMS and AMS. Because, the ID field is already used for others, the corresponding offset that is used to record the fragment sequence is of no use. The 8-bit TOS is used for the type of service required for routing, but most of routers in Internet do not support this functionality. Therefore, we can get 36-bit space to mark the information. The full procedure is described in Fig. 3.

S [][] is a Maekawa set in algorithm. Variable q is the probability for marking. Variable c is the total marking

times and its value is the number of rows of S[][]. K is the number of fragments marked every time and its value is the number of columns of S [][]. Variable fb is the number of bits of each fragment. The marking sequence number generated orderly from j (its initial value is 0) is stored into the cfragno field in IP header. Three fragments for marking are filled into the cfrag field in IP header. The distance from the marking edge to the victim is written into the distance field in IP header. The function subs (str,w,t) is to get t-bit substring from string str beginning at the w-th bit.

Attack path reconstruction based on Maekawa set: Attack path reconstruction has two major parts: one is the reordering of fragments and the other is path reconstruction. Having received the packets carrying all the attack edge information, the packets are arranged on distance and cfragno at victim. When the fragments are reordered, the fragment frag[i] is obtained from marking fragments cfrag, then the edge is reordered from fragment frag[i], $1 \le i \le 7$. There exists a dependent relationship among the marking fragments each time according to Maekawa set, so, we should get all fragments in some conditions and orders. Here, we set a two-dimensional table order[][] depicting the order of attaining all the fragments. In this table, the row represents the number of fragments and the first column represents the condition which used to deduce frag[i]. The second column represents the fragment-ID and the third column represents the position. Having attained all the fragments, the edge is generated. The edge reordered is checked by the constraints according to Maekawa set and the collision edges will be removed. For instance, an edge is split into 7 fragments and marked according to Maekawa set with N = 7, k = 3, m = 7, whose order[][] is depicted in Fig. 4.

In the 3rd column, the x of x.y represents the number of subsets and the y represents the order in subset. The edge reordered is stored in the table cons_edge, which contains three fields-distance, edge 1 and edge 2. Edge 1 is the starting node and edge 2 is the ending node. The starting node and the ending node are classified by flow direction. The fragment reordering algorithm is shown in Fig. 5.

After all the fragments are reordered into edge and the table cons_edge is generated, then the attack path will be reconstructed. The results of reconstruction are stored into the table cons_path, which contains 32 fields node1~node32. The path reconstruction algorithm is shown in Fig. 6.

$$\text{Order} = \begin{bmatrix} 1\ 1\ 1.1 \\ 1\ 2\ 1.2 \\ 1\ 3\ 1.3 \\ \text{cond}\ 4\ 4.2 \\ \text{cond}\ 5\ 4.3 \\ \text{cond}\ 6\ 6.2 \\ \text{cond}\ 7\ 6.3 \end{bmatrix}$$

Fig. 4: Order table for N = 7, k = 3, m = 7

```
Reordering(c, k, fn, fb, order)
  For i: = 0 to maxd
    For each packet for p. cfragno = 1
      For j: = 1 to fn
        condexpress: = order [j] [1]
        fragno: = order [j] [2]
        setrow: = order [j ][3] .x
        setcol: = order [j] [3] .y
        search for condexpress
        frag [fragno]: = subs (p. cfrag,
        (s [setrow] [setcol] -1) *fb+1,fb)
      End for
        edge =""
      For j: = 1 to fn
        edge: = edge + frag [j]
      Endf or
      cons_edge.edge1: = subs (edge, 1, 32)
      cons_edge.edge2:= subs (edge, 33, 32)
      cons_edge.distance:=i
    Endfor
  Endfor
```

Fig. 5: Fragment reordering algorithm

```
Path reconstruction procedure at victim V
For each edge distance = 0 in cons_edge
  For i: =1 to maxd
    Cons_path.node[i]:=cons_edge.edge2
    Start: =cons_edge.edge1
    Search for cons_edge.edge2= start.and.distance=i
  Endfor
Endfor
Output each record in cons_path
```

Fig. 6: Path reconstruction algorithm

PERFORMANCE ANALYSIS

No. of packets required for reconstruction: Assume the length of the attack path is d and the probability that a packet is marked is q. Then the probability that a packet is marked by one router but not marked by any one of others is $q(1-q)^{d-1}$. Since, the marking event in each router is independent, the probability that a given packet passes through d routers and being marked is $dq(1-q)^{d-1}$. As per the well-known coupon collector problem (Feller, 1967), the expected number of trials required to select one from d equiprobable items is $d(\ln(d)+\gamma)$, where, γ represents

Euler's constant. It can be omitted while describing the expectation. Therefore, the number of packets X required for reconstructing a path with length d at victim end has the following expectation:

$$E(X) < \frac{d(\ln(d)+\gamma)}{dq(1-q)^{d-1}} = \frac{\ln(d)}{q(1-q)^{d-1}} \quad (1)$$

In this scheme, the 64-bit edge consisted of two neighboring routers' IP addresses is divided into 7 fragments. But, we adopt Maekawa optimal set to mark the edge and in fact, each edge is marked only 7 times and only 7d fragments are required for reordering. The expected number of packets required for path reconstruction with length d is as following:

$$E(X) < \frac{7d(\ln(7d)+\gamma)}{dq(1-q)^{d-1}} = \frac{7\ln(7d)}{q(1-q)^{d-1}} \quad (2)$$

In FMS scheme, the edge is divided into 8 fragments and only one fragment is marked each time. Therefore, the number of packets X required for reconstructing a path with length d at victim end has the following expectation:

$$E(X) < \frac{8d(\ln(8d)+\gamma)}{dq(1-q)^{d-1}} = \frac{8\ln(8d)}{q(1-q)^{d-1}} \quad (3)$$

From Eq. 2 and 3, we may know the number of packets required for reconstruction in this scheme is less than that in FMS. But in AMS, there are no fragments, the expectation of which the number of packets X required for reconstruction a path with length d at victim end is:

$$\frac{\ln(d)}{q(1-q)^{d-1}}$$

so, the victim requires fewer packets to reconstruct the attack path than ours. However, we can adopt the strategy of no rewriting and optimal probability to reduce the number of packets required for reconstruction.

Computation overhead for reconstruction: Computation overhead includes overhead for fragments reordering and attack path reconstruction. There exist fragments in present scheme, so the fragments are required for reordering into edge. There is no hash and XOR in our scheme; therefore, the overhead for reconstruction is mainly from the overhead of fragments reordering. FMS adopted XOR to reduce the space for storage, but the overhead of attaining raw data from the XOR for edge is much lower than the reordering, the overhead is mainly from the reordering of fragments. There is no fragment in AMS so that the overhead is mainly from the attack path reconstruction.

By the use of Maekawa set while marking, we need not consider the recombination of all the fragments with the same distance. We only need to consider two reordering of fragments 123, 45, 67 and two checks and then the unique edge is reconstructed.

Assume, the number of distinct routers at distance d is $|M_d|$, the set of fragments (to be reordered) with a distance d and fragment-id f is $\psi_{d,f}$, $1<=f<=2$. Considering the number of fragments which are selected from $\psi_{d,f}$ and meet condition c is $\sigma_c|\psi_{d,f}|$, the number of reordering to be checked is Γ, then the total number of reordering for all the fragments and all the distances is

$$|\Gamma| = \sum_{0<=d<=\max d} |M_{d-1}| \times \prod_{1<=f<=2} \sigma_c |\Psi_{d,f}| \quad (4)$$

All the packets are indexed on distance and cfragno fields in the IP header and the items with same distance, cfragno and cfrag are removed, this leads to further reduction of the number of fragment reordered.

But, in FMS, the victim cannot distinguish which fragments are from which router. In order to reconstruct the attack path, the victim should consider all possible combinations in set $\Psi_{d,f}$ ($1<=f<=8$). Therefore, the total number of reordering to be checked for all the distance is

$$|\Gamma| = \sum_{0<=d<=\max d} |M_{d-1}| \times \prod_{1<=f<=8} |\Psi_{d,f}| \quad (5)$$

Apparently, the total number of fragment reordered in this scheme is less than that in FMS.

In AMS, there is no fragment, but it uses hash and XOR to compress the edge. It needs network topology to reconstruct the attack path. The hash value of each router IP in level d ($0 \le d \le$ maxd) must XOR the hash value of all routers IP in next level and then the result of XOR will be compared with all received packets. So, the overhead for reconstruction is:

$$|\Gamma| = \sum_{0<=d<=\max d} |M_{d-1}| \times |\Psi_d| \quad (6)$$

False positives for reconstruction: FMS adopts fragmental strategy to compress the marking information. Although, each router has a unique IP address and the edge constituted from neighboring router IP address is also unique, the edge fragments are probably identical; this results in that the reordering edge is not unique. Some non-existent attack paths would be reconstructed. For instance, the edge constituted from 152.63. 17.201 and 152.63.25.189 and the edge constituted from 152.63. 17.205 and 152.63. 24.209, having fragmented, the 16 fragments aregenerated, which are 152,63, 17,201, 152,63, 25,189 and

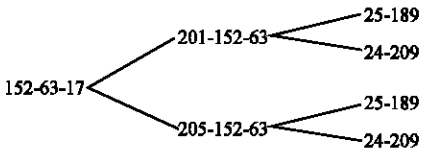

Fig. 7: Fragment reordering

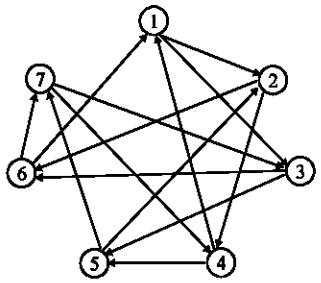

Fig. 8: Circular locking for N = 7

152,63, 17,205, 152,63 and 24,209. The reconstructed attack path is shown as Fig. 7. The rate of false positives is 100%.

However, the marking strategy is based on the Maekawa set in present scheme. The goal of the Maekawa set is that uses optimal messages to make resources be accessed mutual exclusively in a distributed system. It is based on the fact that, if node i locks all members of S_i, no other node can capture all its members. Therefore, when it invokes mutual exclusion, node i tries to lock all members of S_i. The circular locking among mutual exclusion request is achieved. As for a 7-node Maekawa set, the circular locking is depicted as Fig. 8.

Every node is linked to every other node in Fig. 8, thus different combinations are generated. Changing any link will make that link conflict with the other links and hence any uncorrected combination is removed. Thus, when the Maekawa set is applied to our scheme, it will guarantee the reordered edge to be unique, so the false positives from reordering are 0 theoretically. Furthermore, we adopt the redundant marking to check the reordered edge. Only when the reordered edge is matched with the relative information in redundant marking information, the reordered edge is considered as an attack edge. The compress based on hash and the authentication method based on MAC are not adopted so that there is no false positive from hash collision. However, the expectation of false positives in FMS is $(1-(1-1/2^{32})^{\alpha})2^{32}$, α is the number of valid reordered edges. In AMS, 8-bit hash function is used to compress the 32-bit IP address. While there are many routers with the same distance to the victim, 8-bit hash function is not enough to avoid collision and the false positives will be high too. Assume, the number of distinct routers at distance d is $|M_d|$, the set of distinct edges and with a distance d is Ψ_d, t_y is the number of router's children in M_d, the expectation of t_y is $t_y|\Psi_d|/2^{11}$, the expectation of all routers in M_d is $(1-(1-1/2^{11})^{|M_d|})2^{11}$.

No need routers topology support: In FMS, the edge is divided into fragments. When the victim reconstructs the attack path, the victim cannot distinguish which fragments are from which router. In order to reconstruct the attack path, the victim needs to recombine all fragments with same distance. But not all recombined edge is in attack path. To determine the attack path, the support of routers topology is needed. In AMS, what routers will mark to the IP header is the XOR-ed value of the hashed IP addresses, which is corresponding with an edge. Since, hash function is a one-way function, the IP address cannot be calculated back from the hash value. The routers topology is needed to reconstruct the attack path. If the XOR-ed value of the hashed IP addresses is matched with the marking information in received packets, the edge will be considered as an attack edge. The rest reconstruction is deduced similarly. In present scheme, there exists dependence among the marking information. According to the dependence, the attack edge can be reconstructed. The marking information has no hash and XOR; therefore, a node can get the matched children node easily without the support of routers topology.

In addition, for a given N, the Maekawa set generated is not unique. Based on the feature, we may change the Maekawa set non-periodically to prevent a compromised router from forging marking information.

EXPERIMENTAL RESULTS

To test the feasibility of present scheme in real circumstances, we conduct an experiment on simulation attacks and reconstruction by using a real traceroute dataset-20060109_paths from Lucent Bell Labs. The traceroute dataset contains 328847 distinct traceroute paths from a single source 65.198.68.33 to different destinations widely distributed over the entire Internet. There are 42789 complete paths among them. In all the tests, we use the single source of the traceroute 65.198.68.33 as the victim and we randomly select a given number of destinations in the dataset as attackers. We simulate the process that a router marks a packet and the victim reconstructs the attack path. This scheme is a Maekawa set based Marking scheme, so it is called as MMS. To reduce the number of packets required for reconstruction, the following strategies are adopted: (1) changing the randomly marking in FMS into orderly marking in this scheme. Let MMSR denote the MMS with randomly marking and MMSO denote MMS with orderly marking as shown in Fig. 9, (2) no rewriting to the marking information. Let MMSOU denote the MMS with orderly marking and no rewriting, (3) marking the packet with an optimal probability. Let MMSp denote MMS with

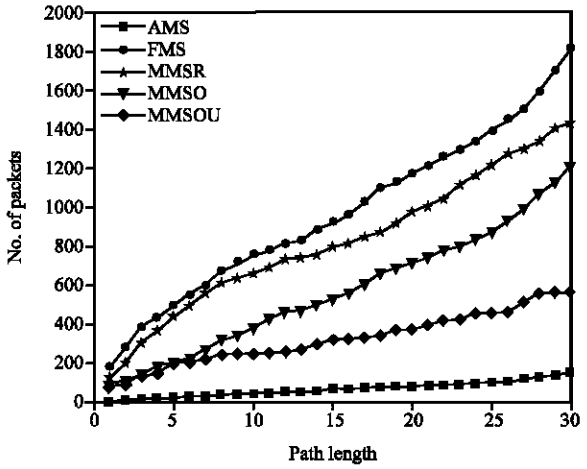

Fig. 9: No. of packets required for reconstruction for MMS, FMS, AMS with q = 4%

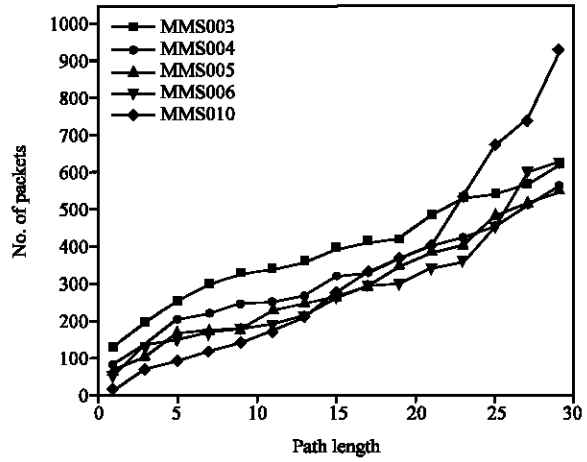

Fig. 10: No. of packets required for reconstruction for MMS with varying probability

different probability p where p is the marking probability. For instance, MMS003 is the MMS marking scheme with probability 0.03. The number of packets required for reconstruction is compared among the MMS with randomly marking, MMS with orderly marking, MMS with orderly marking and no rewriting, FMS and AMS with a fixed probability q = 0.04. The results are shown as Fig. 9. Each data point is averaged over 30 independent tests with an attacker at a certain distance from the victim. The number of packets required for reconstruction in MMS with orderly marking and no rewriting with varying probability is also tested. Figure 10 shows the simulation result. From Fig. 10, we can see when the probability is the range from 0.04 to 0.05; the number of packets required for reconstruction is least in MMS with orderly marking and no rewriting. Figure 11 and 12 show the overhead for

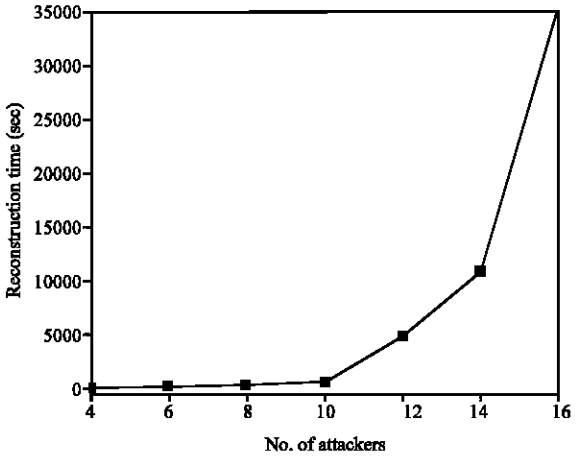

Fig. 11: Computation overhead for FMS

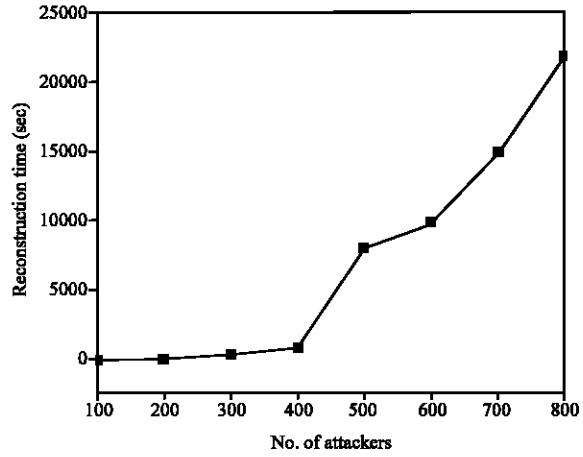

Fig. 12: Computation overhead for MMS

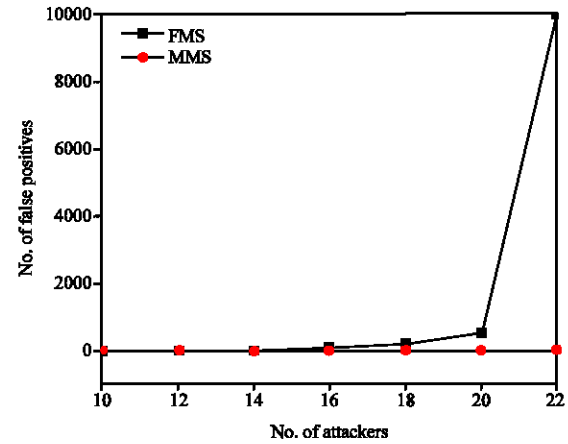

Fig. 13: False positives for FMS and MMS

reconstruction in FMS and MMS. FMS cannot work in large scale DDoS attack. Though there are hundreds of

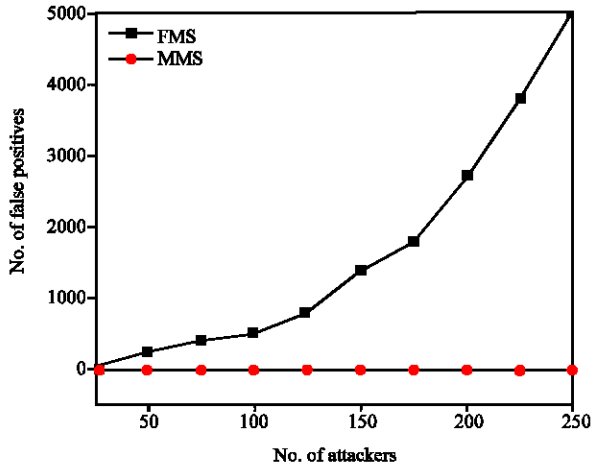

Fig. 14: False positives for AMS and MMS

thousands of attackers, MMS works well. Figure 13 compares MMS with FMS in false positives. There are only 20 attackers, the false positives are sharply arising in FMS, but the false positives are 0 in MMS. This result is obtained from the ideal network environment. Figure 14 compares the MMS with AMS in false positives under DDoS.

CONCLUSION

In order to solve the problem about large number of false positives, no authentication on marking information and the need for network topology in FMS, a novel probabilistic marking scheme (MMS) is proposed. MMS splits the edge into fragments making up of two neighboring routers' IP addresses, by using Maekawa set, the k fragments are marked into the unmarked packet's IP header with an optimal probability for several times. The Maekawa set makes the marking information and the marking times optimal. Not only the overhead for the reordering of fragments is heavily reduced, but also the marking information can be checked. The false positive of fragments reordering is 0 in theory and in ideal network environment. MMS does not need the support of the network topology, which makes the scheme more practical. The Maekawa set can be changed non-periodically to prevent a compromised router from forging marking information to achieve advanced authentication simply. Although MMS is proposed on the basis of the FMS, it can apply to all PPM scheme with fragment strategy.

ACKNOWLEDGMENTS

The authors thank Jian Zhou for insightful technical discussion. This research is supported by National Natural Science Foundation of China under grant No. 60673156 and by National High Technology Research and Development Program of China (863 Program).

REFERENCES

Baba, T. and S. Matsuda, 2002. Tracing network attacks to their sources. IEEE Internet Comput., 6: 20-26.

Burch, H. and B. Cheswick, 2000. Tracing anonymous packets to their approximate source. Proceedings of the 14th Systems Administration Conference (USENIX LISA 2000), Dec. 3-8, New Orleans, Louisiana, USA., pp: 319-327.

Dean, D., M. Franklin and A. Stubblefield, 2002. An algebraic approach to IP traceback. ACM Trans. Inform. Syst. Secur., 5: 119-137.

Feller, W., 1967. An Introduction to Probability Theory and its Applications. 3rd Edn., Wiley, New York, ISBN: 9787115147295.

Goodrich, M.T., 2008. Probabilistic packet marking for large-scale IP traceback. IEEE/ACM Trans. Network., 16: 15-24.

Ioannidis, J. and S.M. Bellovin, 2002. Implementing pushback: Router-based defense against DDoS attacks. Proceedings of the 9th Symposium Network and Distributed System Security (NDSS '2002), Feb. 6-8, San Diego, California, USA., pp: 1-12.

Law, T.K.T., J.C.S. Lui and D.K.Y. Yau, 2005. You can run, but you can't hide: An effective statistical methodology to trace back DDoS attackers. IEEE Trans. Parallel Distributed Syst., 16: 799-813.

Lee, H.W., 2004. Advanced packet marking mechanism with pushback for IP traceback. Proceedings of the 2nd International Conference on Applied Cryptography and Network Security, Jun. 8-11, Yellow Mountain, China, pp: 426-438.

Li, D.Q., P.R. Su, D.M. Wei and D.G. Feng, 2007. Router numbering based adaptive packet marking. J. Software, 18: 2652-2661.

Liu, J., Z.J. Lee and Y.C. Chung, 2003. Efficient dynamic probabilistic packet marking for IP traceback. Proceedings of the 11th IEEE International Conference on Network, Nov. 4-7, Atlanta, Georgia, USA., pp: 475-480.

Liu, W., H.X. Duan, J.P. Wu and X. Li, 2005. Improved marking model ERPPM tracing back to DDoS attacker. Proceedings of the 3rd International Conference on Information Technology and Applications, Jul. 4-7, IEEE Computer Society Press, pp: 759-762.

Ma, M., 2005. Tabu marking scheme for IP traceback. Proceedings of the 19th IEEE International Parallel and Distributed Processing Symposium, Apr. 3-8, Denver, Colorado, USA., pp: 292-300.

Ma, M. and D.H.K. Tsang, 2007. Finding optimal marking probability to reduce convergence time. Proceedings of the 2nd International Conference on Communications and Networking, Aug. 22-24, Shanghai, China, pp: 192-196.

Maekawa, M., 1985. An algorithm for mutual exclusion in decentralized systems. ACM Trans. Comput. Syst., 3: 145-159.

Mankin, A., D. Massey and C.L. Wu, 2001. On design and evaluation of intention-driven ICMP traceback. Proceedings of IEEE International Conference on Computer Communications and Networks, Oct. 15-17, Scottsdale, Arizona USA., pp: 159-165.

Ogawa, T., F. Nakamura and Y. Wakahara, 2003. Branch label based probabilistic packet marking for IP traceback. Proceedings of the 11th IEEE International Conference on Networks, Sept. 28-Oct. 1, Sydney, Australia, pp: 467-474.

Savage, S., D. Wetherall and A. Karlin, 2001. Practical network support for IP traceback. IEEE/ACM Trans. Network., 9: 226-237.

Snoeren, A.C., C. Partridge and L.A. Sanchez, 2001. Hash-based IP traceback. Proceedings of the ACM SIGCOMM 2001 Conference on Applications, Technologies, Architectures and Protocols for Computer Communication, Aug. 27-31, San Diego, California, USA., pp: 3-14.

Song, D.X.D. and A. Perrig, 2001. Advanced and authenticated marking schemes for IP traceback. Proceedings of the 20th Annual Joint Conference on IEEE Computer and Communications Societies, Apr. 22-26, Anchorage, Alaska, USA., pp: 878-886.

Spatscheck, O. and L.L. Peterson, 1999. Defending against denial of service attacks in scout. Proceedings of the 3rd Symposium on Operating System Design and Implementation, Feb. 22-25, New Orleans, LA, pp: 59-72.

Stone, R., 2000. Centertrack: An IP overlay network for tracking DoS floods. Proceedings of the 9th USENIX Security Symposium, Aug. 14-17, Denver, Colorado, USA., pp: 107-118.

Tseng, Y.K., Y.Y. Lu and J.Y. Huang, 2006. ID-based PPM for IP traceback. Proceedings of the 1st International Conference on Innovative Computing, Information and Control, Aug. 30-Sept. 1, Beijing, China, pp: 262-265.

Yaar, A., A. Perrig and D. Song, 2005. FIT: Fast internet traceback. Proceedings of the 24th Annual Joint Conference of the IEEE Computer and Communications Societies, Mar. 13-17, Miami, Florida, USA., pp: 1395-1406.