A New Hybrid IP Traceback Scheme

P. D. Kadam
M.B.E.S College of Engineering, Ambajogai
Maharashtra, India

B. M. Patil
M.B.E.S College of Engineering, Ambajogai
Maharashtra, India

ABSTRACT
Now days the Internet is exposed to a span of web threats, So the attack on its infrastructure poses a great challenge in its expansion. In the modern world various types of attacks are discovered on the Internet. IP spoofing is one of the major threats in the network security. Hackers use this to hide their identity or to perform an attack. IP spoofing used for many attacks like denial of service, SYN flooding and man in the middle attacks etc. It is necessary to capture or block the spoofers to defend against these attacks. Different IP trace back mechanisms are used for finding the spoofers identity. IP trace back scheme is a way used to catch the real path of web packets requiring a longer search so, a new hybrid IP trace back scheme is used with efficient packet logging aiming to have a fixed storage requirement for each router in packet logging without the need to refresh the logged tracking information and to achieve zero false positive and false negative rates in attack-path reconstruction. The hybrid IP trace back scheme compare with other related research in the aspects of storage requirement, computation, and accuracy.

Keywords
New hybrid IP trace back, CAIDA's , distributed denial of service attack ,packet logging, packet marking.

1. INTRODUCTION
Internet is a worldwide network and used in almost every field of work. Internet is growing day by day and the users using it are increasing exponentially. Security becomes an important issue, as internet is being used for the exchange of data transactions and confidential information etc. Among various attacks on internet, is focused on DoS attack. DoS attack is classified into flooding attacks and software exploit [1][2]. In flooding attack, large number of packets flooded to the victim machine. Due to highly distributed nature of DoS attacks, victim can be overwhelmed quite easily, even if individual attackers send low number of packets to the victim. Software exploit attack, attacks a host using host's vulnerabilities with few packets. Software exploit attacks include IP spoofing attack. Spoofed packets are traced via trace back scheme by augmenting the packets with partial information called as packet marking and also by storing the packet digest or signature at intermediate routers called as packet logging [2][4]. In such type of schemes, large number of packets required at victim to trace back the path. There are various problems associated with the IP trace back scheme such as the requirement of high storage on logged routers. Trace back scheme cannot avoid the false positive and false negative problem. Real source of flooding based attack can be traced using link test in which UDP service is used to generate access load to the upstream links [5]. The excess load, works against the attack packets and disturb the attack packets traffic. Through the excess load attack traffic can be traced, which passes via upstream router.

A RIHT trace back scheme that marks routers interface numbers and integrates packet logging with a hash table to deal with these logging and marking issues in IP trace back. RIHT is a hybrid IP trace back scheme having some properties like storage requirement for an arbitrary router is bounded above by the number of paths to the router, and thus every router does not need to refresh logged tracking information, achieves zero false positive and false negative rates in attack-path reconstruction, have higher efficiency in path reconstruction and can censor attack traffic. This paper is organized as follows in section 2.literature review. Section 3 introduction of RIHT. In section 4 simulation and performance analysis scenarios section 5 conclusion and future work

2. LITERATURE REVIEV
Shui Yu et al. [6] mentioned unique trace back technique for DDoS attacks, supported entropy variations between traditional and DDoS attack traffic, that is different from usually used packet marking techniques. As a basic demand once a DDoS attack has been known by the victim via detection algorithms, it initiates the pushback tracing procedure. The trace back algorithm initialy identifies its upstream routers wherever the attack flows came from, then submits the trace back requests to the connected upstream routers. This procedure continues till it reaches the discrimination limitation of DDoS attack flows. Snoeren[7] propose a system SPIE to digest the unchanged elements of a packet and used bloom filter to log the digest however this scheme needs massive space for storing and incorporates a false positive drawback within the bloom filter because of this reason, Zhang and Guan[8] propose TOPO to enhance the potency and exatness of SPIE,however TOPO still wants massive storage capability and inevitably incorporates a false positive drawback thanks to the bloom filter. The hybrid IP trace back schemes are introduced to mitigate the storage drawback of logging-based trace back schemes. Gong and Sarac [9] introduced a hybrid IP trace back scheme called Hybrid IP Trace back (HIT) combining packet marking and packet logging. HIT uses packet marking to cut back the amount of routers needed for logging. Huffman codes, Modulo/Reverse modulo Technique (MRT) [10] and MOdulo/REverse modulo (MORE) [11], these new schemes have proposed researchers to scale back the storage demand for router logging and to decrease the amount of routers needed for work. Since these schemes use interface numbers of routers for marking, they assume a router set comprising routers in an exceedingly network and need all the routers support the individual trace back schemes. Also, they use the degree of a router as a parameter in their marking schemes wherever the degree is that the variety of interfaces of the router, not as well as ports connected to native networks. Choi and Dai [12] propose a marking scheme exploitating Huffman coding to scale back the bits needed for marking on a packet. It encodes by Huffman coding in step with the traffic of every interface.Their analysis shows their scheme has higher performance once the traffic distribution for every interface is unequal. Malliga and Tamilarasi propose two traceback

schemes, particularly MRT [10] and MORE [11]. MRT uses a 32-bit marking field, MORE uses a 16-bit marking field and separates a log table into elements. however there square measures the subsequent two issues within the MRT and MORE's schemes. First, once logged in, if the marking field of the packet remains 0 on the adjacent downstream router, it will be known as a logged router for the packet whereas tracing back. Then it will fail to search out the origin. Second, since the digests in an exceedingly log table may need a collision, it causes the false positive drawback throughtout the path reconstruction. The storage demand is proportional to the amount of logged packets. sadly,wthin the flooding-based attack, a large quantity of attack packets can go surfing identicle router. Thus, it demands a high storage demands on the logged router. Moreover, while reconstructing a path, a logged router for a packet must search the digests within the log table using exhaustive search so as to search out the old marking field. The complete search is not economical once the log table is massive,thanks to the higher than issues within the Huffman codes, MRT and MORE schemes, we propose a traceback scheme that marks routers' interface numbers and integrates packet logging with a hash table (RIHT). RIHT contains a lower storage demand and higher exactness and potency than Huffman codes and MRT.

3. INTRODUCTION OF RIHT

Like MRT and MORE, RIHT marks interface numbers of routers on packets thus on trace the trail of packets. Since the marking field on every packet is restricted, our packet-marking scheme may have to log the marking field into a hash table and store the table index on the packet. We tend to repeat this marking/logging method till the packet reaches its destination. After that, we are able to reverse such method to trace back to the origin of attack packets. To perform such task there may be some steps to perform.

Despite the very fact that current hybrid IP traceback schemes are ready to track single packet attacks which RIHT has reduced the storage demand to associate extent that a router does not ought to refresh its tracing logs, packet fragmentation and packet drop problems will still fail their path reconstruction.

3.1 Network Topology and Preliminaries

A Network Topology may consist of the number f routers that are connected with local area networks. Thus, a router can either receive data from the nearer router or from the local area network. A border router receives packets from its local network. A core router receives packets from other routers. The number of routers connected to a single router is called as the degree of a router. For example, serves as a border router when it receives packets from Host. However, it becomes a core router when receiving packets from .The assumptions of our scheme are as follows.

- A router creates an interface table and numbers the upstream Interfaces.
- A router knows whether a packet comes from a router or a local network.
- Such a trace back scheme is viable on every router.
- The traffic route and network topology may be changed, but not often. This is shown in following Fig 1.

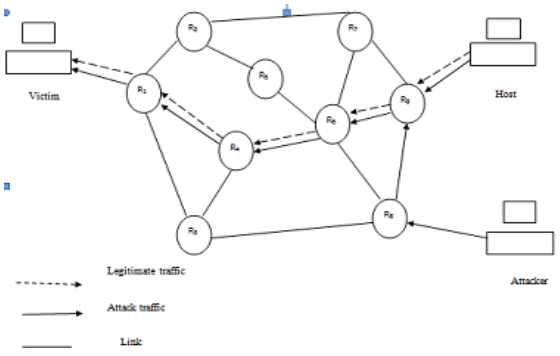

Fig 1: Network Topology

If we use the identification field to mark a packet, it can lead to identification number collision in the reassembling process.

3.2 Marking and Logging Scheme

Packet Marking is that the part, wherever the economical Packet Marking algorithm is applied at every router on the outlined path. It calculates the P_{mark} value and stores within the hash table. If the P_{mark} is not overflow than the capability of the router, then it is sent to the upnext router. Otherwise it refers the hash table and once more applies the algorithm. once a border router receives a packet from its native network, it sets the packet's marking field as zero and forwards the packet to the upnext core router. As shown in following algorithm.

Input: P, UI_i

Begin

1. $Mark_{new}$ = P.mark *($D(R_i)$ + 1) + UI_i +1
2. If $mark_{new}$ is overflow then
3. Index = h =H(P.mark)
4. Probe =0
5. While not(HT[index] is empty or HT[index] is equal to (P.mark),UI_i))
6. Probe++
7. Index = (h + c_1 * probe + c_2 * $probe^2$) % m
8. Endwhile
9. If HT[index] is empty then
10. HT[index].mark = P.mark
11. HT[index].UI =UI_i
12. Endif
13. $Mark_{new}$ = index * ($D(R_i)$ +1)
14. Endif
15. P.mark = $mark_{new}$
16. Forword the packet to the next router
17. End

3.3 Path Reconstruction

Reconstruction is that the method of obtaining back and packet casuation them one by one by denial of service.This helps in construction of improper packets and conjointly helps in avoiding more loss of packets.

Once the Packet has reached the destination once applying the Algorithm, there it checks whether or not it sent from the proper upstream interfaces. If any of the attack is found, it request for the Path Reconstruction. Path Reconstruction is that the method of finding the new path for an equivalent supply and also the destination during which no attack are often created. A victim is under attack sends to the upstream router a reconstruction request, which has the attack packet's marking field.once a router receives a reconstruction request,

it tries to search out the attack packet's upstream router. If packet came from associate upstream router on the upstream interface, the requested router then restores the marking field to its premarking status. it implies that either the attack packet's marking field and its upstream interface variety are logged on the requested router, or the requested router itself is the source router. As shown in following algorithm.

Begin

1. $UI_i = mark_{req} \% (D(R_i) + 1) - 1$
2. If $UI_i = -1$ then
3. Index = $mark_{req} / (D(R_i) + 1)$
4. If not index = 0 then
5. $UI_i = HT[index].UI$
6. $Mark_{old} = HT[index].mark$
7. Send reconstruction request with $mark_{old}$ to upstream router by UI_i
8. Else
9. This router is the nearest border router to the attacker
10. Endif
11. Else
12. $Mark_{old} = mark_{req} / (D(R_i) + 1)$
13. Send reconstruction request with $mark_{old}$ to upstream router by UI_i
14. Endif

End

3.4 RIHT Extension

In our traceback scheme, every router solely has to understand its upstream router that complies with our scheme. Then, the two routers can use a tunnel for direct communication between them. It means that if the adjacent router does not support our trace back, we will not receive any regeneration and can need to question futur one (more than one-hop away) [13].

On the opposite hand, if an attack packet reaches a NAT server before any routers that support our traceback scheme, we will solely trace its supply to the NAT server. That to mention, we can only realize the attack's LAN, which, is sufficient to locate the origin of an attack. Also, the modification of a router's port numbers may lower the accuracy of scheme. During this case, extend path reconstruction scheme into a two-layer approach to urge around this problem.

First every ISP has to run our traceback scheme individually one by one. Since each ISP is cognizant of the port-number modification, they will precisely establish an incoming and outgoing border routers which a packet goes through.

Second, the victim site has to run scheme to question a traceback server in an AS so as to reconstruct an attack path. With this extension of our scheme, we will guarantee the high accuracy of this approach.

4. SIMULATION AND PERFORMANCE ANALYSIS

4.1 Simulation

The simulation scenario of this hybrid trace back scheme as shown in following results.A network topology may consist of the number of routers that are connected with local area networks. Thus, a router can either receive data from the nearer router or from the local area network. A border router receives packets from its local network. A core router receives packets from other routers. The no.of routers connected to a single router is called as the degree of a router. This is calculated and stored in a table. The Upstream interfaces of each router also have to be found and stored in the interface table. Enter the number of routers for example eight and click next by Clicking the next button the following topology will display which is shown in Fig 2.

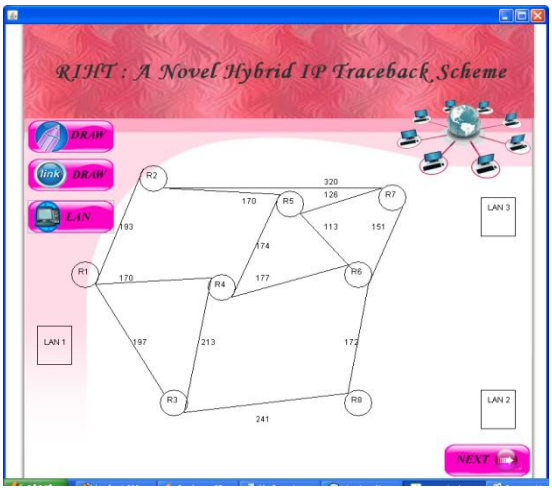

Fig 2: A Supposed router network.

Then, select the source and destination LAN and click path Enter the source IP and Port number and select any text file from your folder and click send .The next window shows that by Clicking Frame (Only the needed path will be constructed),it shows the message box that packet received with attack shown in fig 3 , then click Request for reconstructing the path so as to avoid attacked router or attacked path

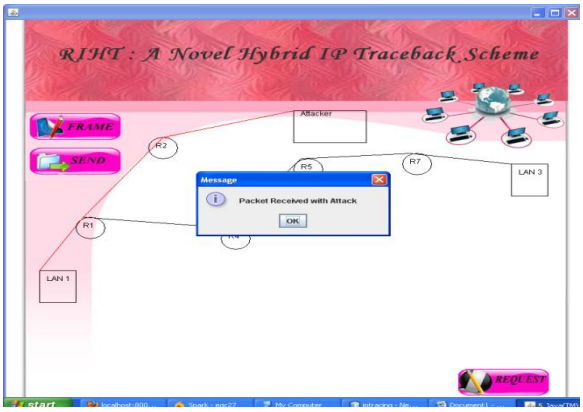

Fig 3: Simulation start

By Clicking on Frame (New path is constructed). Packet is received successfully. Click View it will shows the new path reconstruction which is shown in Fig 4,hence packet sent to destination successfully by avoiding attack.

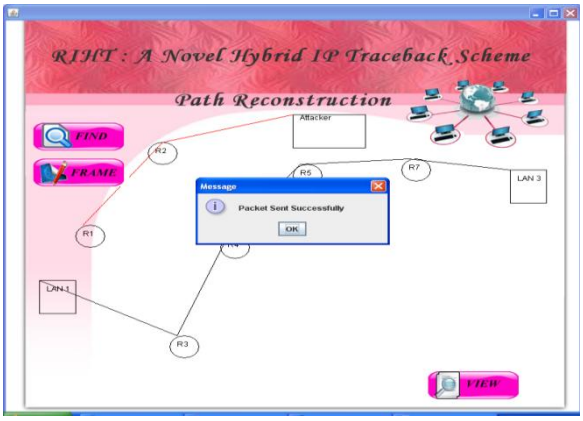

Fig 4: New path construction

4.2 Performance Analysis

In this section we compare computing time of IP traceback scheme with MRT and MORE.As RIHT uses Hash table for logging,we compare these techniques using Murmur hash function

Initialy empty hash table is initiated with 32 bit marking field,as our scheme uses 32 bit marking field.Marking field refer to path of router.Eevery marking field is repeated k times as input and then overall computing time is calculated.

MurmurHash2 is taken to compute the computing time of logging schemes as shown in fig 5.It shows that computing time of proposed IP traceback scheme is shorter That is it is faster than MRT and MORE . Here for the computing time of path reconstruction MRT and MORE needs that router searches its own log table using request finding its previously stored marking field.

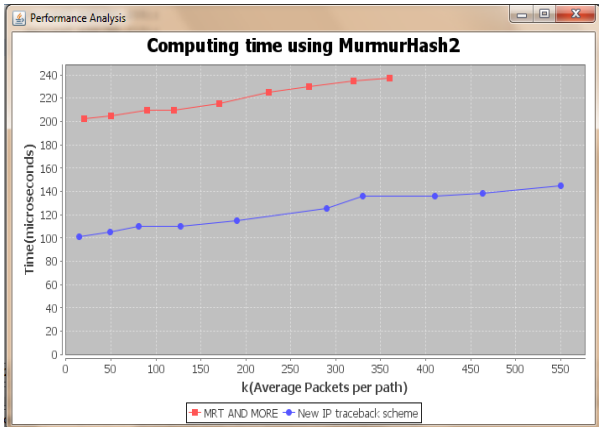

Fig 5: Graph of performance analysis

whereas proposed IP traceback scheme need to get index stored on the request packet's marking field hence her no need to spend time on search,hence path reconsruction is faster than that of MRT and MORE.

5. CONCLUSION

A new hybrid IP traceback scheme is used for efficient packet logging aiming to have a fixed storage requirement packet logging without the need to refresh the logged tracking information. Also, this scheme has zero false positive and false negative rates in an attack-path reconstruction and have the properties that can also deploy a marking field as a packet identity to filter malicious traffic and secure against DoS/DDoS attacks.,with high accuracy, a low storage requirement, and fast computation, RIHT can serve as an efficient and secure scheme for hybrid IP traceback.

6. REFERENCES

[1] A. Hussain, J. Heidemann, and C. Papadopoulos, "A Frame-work for Classifying Denial of Service Attacks," Proc. ACM SIGCOMM '03,Aug. 2003

[2] B.Al-Duwariand M.Govindarasu,"Novel hybrid schemes employing packet marking and logging for IP traceback," IEEE Trans. Parallel Distributed Syst. , vol. 17, no. 5, pp. 403–418, May 2006.

[3] A. C. Snoeren, C. Partridge, L. A. Sanchez, C. E. Jones, F. Tchak-ountio, B. Schwartz, S. T. Kent, and W. T. Strayer, "Single-packet IP traceback," IEEE/ACM Trans. Networking, vol. 10, no. 6, pp. 721–734, Dec. 2002. traceback," Proceedings of ACM SIGCOMM 2001, pp.3–14, 2001.

[4] C. Gong and K. Sarac, "A more practical approach for single-packet IP traceback using packet logging and marking," IEEE Trans. Parallel Distributed Syst. , vol. 19, no. 10, pp. 1310–1324, Oct. 2008.

[5] Glenn Carl and George Kesidis, Richard R. Brooks and Suresh Rai." Denial-of-Service Attack - Detection Techniques", IEEE Internet Computing, pp: 82-89, January • February 2006

[6] Shui Yu, Wanlei Zhou, Robin Doss and Weijia Jia, "Traceback of DDoS Attacks UsingEntropy Variations" in proc *IEEE* transactions on parallel and distributed systems, vol. 22, no. 3, march 2011.

[7] A. C. Snoeren, C. Partridge, L. A. Sanchez, C. E. Jones, F. Tchakountio, B. Schwartz, S. T. Kent, and W. T. Strayer,"Single- packet IP traceback," IEEE/ACM Trans. Networking, vol. 10, no. 6, pp. 721–734, Dec. 2002.

[8] L. Zhang and Y. Guan, "TOPO: A topology-aware single packet attack traceback scheme," in Proc. IEEE In. Conf. Security Privacy Communication Networks (SecureComm 2006), Baltimore, MD, Aug. 2006, pp. 1–10.

[9] C. Gong and K. Sarac, "A more practical approach for single-packet IP traceback using packet logging and marking," IEEE Trans. Parallel Distributed Syst., vol. 19, no. 10, pp.1310–1324, Oct. 2008.

[10] S. Malliga and A. Tamilarasi, "A proposal for new marking scheme with its performance evaluation for IP traceback,"WSEAS Trans. Computer Res., vol. 3, no. 4, pp. 259–272, Apr. 2008.

[11] S. Malliga and A. Tamilarasi, "A hybrid scheme using packet marking and logging for IP traceback," Int. J. Internet Protocol Technol., vol. 5, no. 1/2, pp. 81–91, Apr.2010.

[12] K. H. Choi and H. K. Dai, "A marking scheme using Huffman codes for IP traceback," in *Proc.7th Int. Symp. Parallel Architectures, Algorithms Networks (SPAN'04)*, Hong Kong, China, May 2004, pp.421–428.

[13] T. Korkmaz, C. Gong, K. Sarac, and S. G. Dykes, "Single packet IP traceback in AS-level partial deployment scenario," *Int. J. Security Networks*, vol. 2, no. 1/2, pp. 95–108, 2007.