I J C T A, 9(9), 2016, pp. 3973-3980

Passive IP Traceback (Pit): Discovery of Spoofing Locations Using Path Backscatter Analysis

S. Rajasekaran[1], A. Rengarajan[2], J. Jeejo Vetharaj[3] and R. Punidha[4]

ABSTRACT

To hide the locations of the hackers, spoofed source IP address is used. Development of IP traces back mechanisms are used to identify the true spot of the spoofers. Exact spoofers location was not identified till now, because no common IP Trace back mechanism was adopted. To overcome the difficulties of the earlier techniques, we implement Passive IP Traceback (PIT) mechanism.PIT detects path backscatter messages (ICMP messages) generated by intermediate devices in the network and traceback the spoofers using topology. We apply Pit on path backscatter data set to identify the locations of the spoofers. Also by employing the TTL field in IP packets, the geographical location details of routing device near to IP spoofers are found.

Keywords: Denial of Service, IP spoofing, Time to live, Network Security, IP traceback

1. INTRODUCTION

IP SPOOFING is a major security problem that was mainly observed in Internets for long time. SYN flooding, SMURF, DNS amplification and much more attacks rely on IP spoofing. Spoofing was not considered as a major problem when DoS attacks were launched from botnets, but spoofing is still observed in some. Spoofing activities are often observed relying on the identification of backscatter communication from UCSD Network Telescopes [1-4]. Filters are placed nearer to the attackers who are located in the minor areas, before attacking traffic gets activated. The origins of spoofing traffic are identified that builds a reputed system for ASes, which provides the corresponding ISPs to verify IP source address.

2. RELATED WORK

S. Savage *et al* [1] proposed a technique that traces unidentified packet flooding attacks through the Internet, which is moved towards to their source. The increased frequency of DoS attacks is difficult to tracing the packet with spoofed or incorrect source addresses, which is encouraged to process to the proposed work. In our approach, a sufferer can be identifying the network path(s) shifted through attack traffic that does not require interactive operational carry from ISPs. Furthermore, after the completion of attack, "post-mortem" is performed in this traceback technique. M. T. Goodrich *et al* [2] said IP traceback is obtained from the probabilistic packet marking concept. To come up to say the mechanism such as link and randomization that use the larger number of checksum codes to "link" message fragments was implemented. Data integrity verifiers can be used in checksum mechanism. It would be difficult for the attackers to generate messages, which is colliding with the legitimate messages, because the addresses of achievable router messages

[1, 2, 3] Department of Computer Science and Engineering

[4] Department of Information Technology

[1] Ph.D. Scholar, Bharath University, Chennai, Tamilnadu, India, *Email: rajasekaran009@gmail.com*

[2, 3, 4] Vel Tech Multi Tech Dr. Rangarajan Dr. Sakunthala Engineering College, Chennai, Tamilnadu, India, *Emails: rengu_rajan@yahoo.com, jeejovetharaj@gmail.com, punidha@veltechmultitech.org*

across a range are largely distributed. Our process does not include individual routers sign in for any of the setup messages. H. C. Le *et al* [3] discuss that DoS/DDoS attacks are one of the most important module of security attacks through the Internet. To trace back the real attack sources, intrinsic support from the infrastructure and current Internet protocols are not provided. IP marking, IP logging, and IETF Traceback (ITrace) are some of the traceback methods proposed. This paper proposes an enhanced ICMP Traceback with collective Path. ICMP Traceback message keeping the whole attacks, which is encoded the path information of attacks to consider for enhancement. To evaluate the increase in performance, Analytical and simulation studies are performed. Y. Xiang *et al* [4] discuses about FDPM, main goal of that mechanism is discover the real source of attacking packet through the network. An FDPM mechanism is ability to trace the source packet that is better capability of tracing system compare than other techniques. This is easily adopted in different environment. That mechanism is not only tracing the packet in network, which also give better filtering mechanism for attacking traffic packet.

3. SYSTEM ANALYSIS

In existing system, to hide the real locations of the attackers, they use duplicated source IP address. We can identify the spoofers by Proposing IP traceback mechanisms [5-7]. IP traceback mechanism is secret and classified into five categories in existing system, such as ICMP traceback, packet marking, link testing, overlay, link testing, hybrid tracing and logging of the router,

1) Packet marking method keeps the router concepts, which change the packet header. That packet has information about router that will make decision to carry the packet.
2) When a router makes a record operation on the forwarded packets, attacking path will be reconstructed from the router.
3) When the attack is in progress, Link testing provides hop-by-hop upstream of attacking traffic.

Drawback of existing system,

1) Spoofing activities are often observed by identification of backscatter messages. To build the IP traceback mechanism on the internet by adopted traceback system by using routing technique.
2) Current commodity routers are supported in the existing traceback mechanism and collaboration of Internet service providers (ISPs) would also be difficult.
3) A single ISP deployment would be meaningless, since the spoofers are spread widely even at the corners of the world.
4) Author has not established Internet-scale for IP traceback system, but they have deployment of traceback mechanism does not provide much gain and has a high overhead.

In proposed system suggested the passive IP traceback, which overcomes the disputes of IP traceback mechanism. The ICMP message is a protocol which is held in IP suite. That protocol is used to indicate the error message to source from the network. The reflection of waves, particles, or signals comes back to the direction from which they came is named as Backscatter. PIT investigates the ICMP error messages stimulated by spoofing traffic and spoofer are tracked relying on public information like a topology [10, 13]

1) The target of spoofing messages generates the backscatter messages to study the path backscatter messages and DoS, which is processed by the intermediate devices but not by the targets.
2) PIT is the proposed system that has problem to deploy existing IP traceback technique. PIT works well in number of spoofing activities but not much in all attacks, though path backscatter letters are not able to generate with stable possibilities. Compared to the AS-level traceback that was deployed in real before, it might be useful in traceback technique.

3) It provides the identification of the location of the spoofers by PIT. This does not provide the entire list, but it will first disclose the known list of the spoofed location.

4. PROPOSED ARCHITECTURE

Architecture consists of four layers: context analysis, raw data collection, diary generation and event personalization. By these four layers, Smart record will be captured by critical events according to user's preference, and mechanically generates records to the user.

Node Creation

User can create a node using a particular IP address and which is stored for each particular user.

File Selection

From the system environment the text files is selected and it communicate from sender to receiver. At first the selected file will be read from system path. The content is loaded in fixed path.

Spoofer Attack

PIT is applied on the backscatter message to identify the spoofer's location. PIT is a mechanism that traces the spoofers before a traceback method by internet level; it has been established in real world. Few spoofing attacks can be work through this system.

IP Tracing

Two critical challenges are taken to construct an IP traceback method through Internet. First one, Traceback technique cost is adopted in the routing system. A presented traceback mechanism does not provide either a wide range of support from the current service or it will launch average overhead toward the routers, particularly in high-performance networks. Second, the collaboration of Internet service providers (ISPs) would be difficult [7-9].

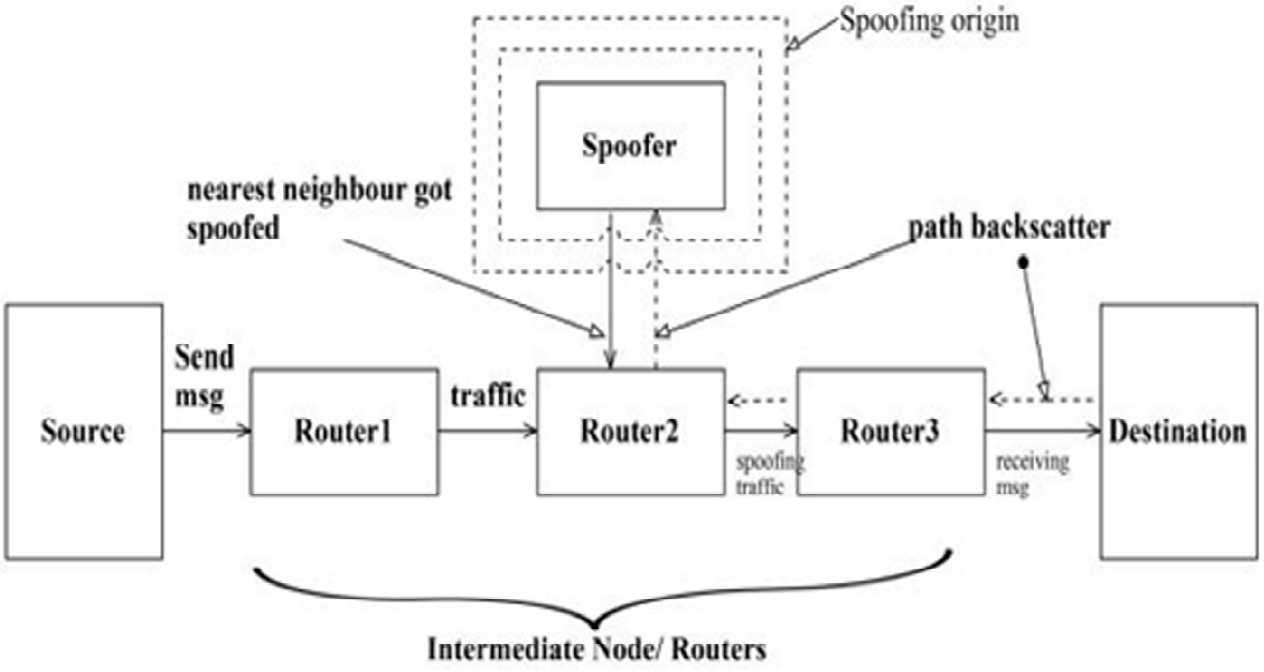

Figure 1: Architecture Diagram

5. COLLECTION OF PATH BACKSCATTER

Spoofing based attacks can be evaluated by path backscatter mechanism. It is not possible to gather path backscatter message and send it to spoofed address. This is classified into four categories such as,

1. Multiple sources, Single destination: In this kind of attack the source packet will be selected by a set of candidate address. It includes all kind of address, and this attack is known as random spoofing attack. It is to bankrupt the ability of the target. As shown in Figure 2, backscatter message had forwarded to the spoofed address randomly. Network telescope keep the spoofed address and part of the backscatter message that is capture by network telescope.

2. Single Source with Multiple Destinations: In this type of attack, each and every spoofed packet has identical source address and this is forwarded to unique destination. In this, the victim of the attack can collect the path backscatter message that is known as reflection attacks. Few packets are usually used to

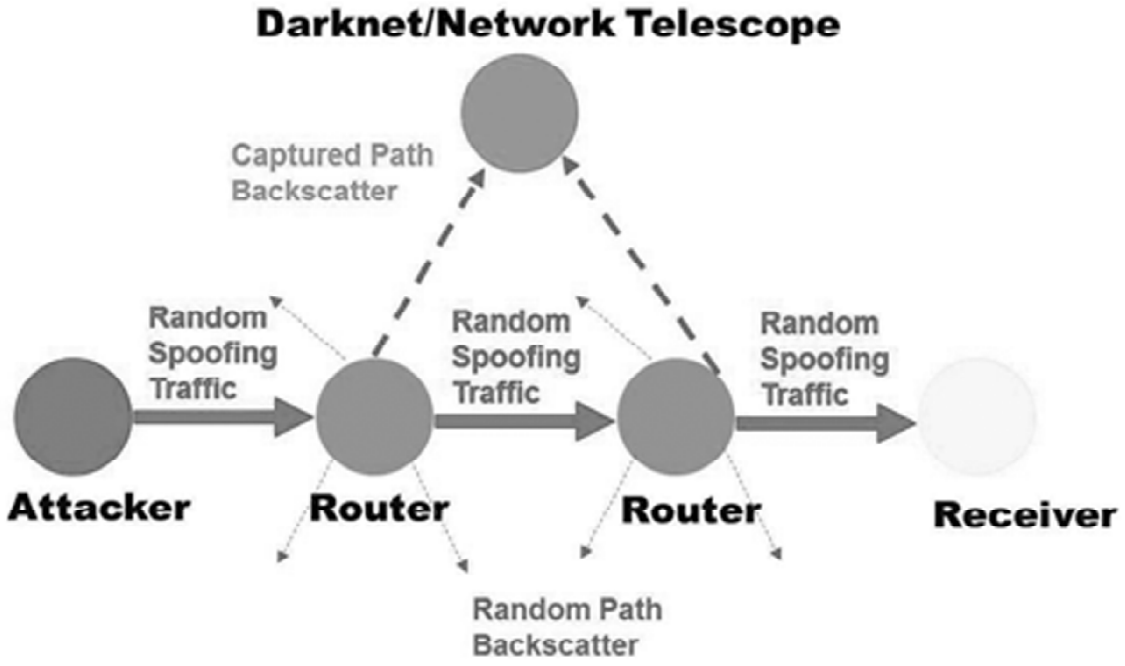

Figure 2: Path backscatter for Darknet captures in random spoofing attacks

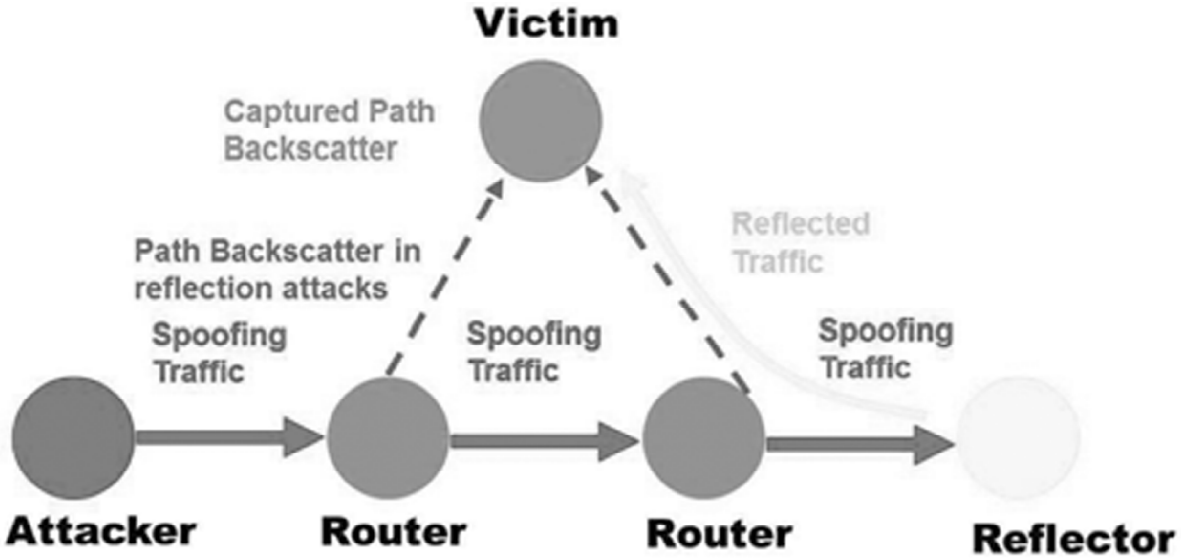

Figure 3: Path backscatter attacks for victim nodes in reflection

barrage observation threats. As in Figure 3, the victim can capture every path backscatter message by reflection attacks because each and every spoofing packet has set the victim address, with that backscatter message will be forwarded to victim. Backscatter message could trace the victims the checking the message when it get forward to origin destination IP address [9].

3. Multiple Sources with Destinations: These types of threats are usually being the combination of above two categories of attacks. Packets are sent from multiple sources to multiple destinations and it will establish the session between multiple sources to multiple destination.

4. Single Source, Single Destination: In this type of attack, spoofed packet will be send from single source address to single destination address. It is usually done to steal or break a session between two communication parties. The spoofed origin will receive all the path backscatter messages. It can be tracked the attacker by path backscatter in efficient manner.

6. ALGORITHM

1) Find the shortest path from source node to destination nod.
2) The message can be send from source to destination through many intermediate nodes i.e. routers(r).
3) There may be spoofer origin available between the paths.
4) If suppose any intermediate node has being spoofed by spoofer node, then the destination node will send the path backscatter message to all intermediate node indicating that spoofing has occurred somewhere in the network.
5) Then each node in the network will send the acknowledgement for that path backscatter message. The node which fails to give back acknowledgement that will be assumed as spoofer node.

For finding the router nearest to the spoofer, we employ the concept of TTL. The TTL value is set by the sender of a packet, and is reduced (by 1) at every router on path to the destination. Hence we can conclude that the router with the largest TTL value will be the one closet to the sender. With the help of different IP location trackers and databases available, the geographical location of this router can be obtained **[14]**.

7. PERFORMANCE EVALUATION

PIT is a different traceback mechanism from other existing techniques. The backscatter path message does not have fixed probability. A chart between Reflector AS number and Original Destination AS number is shown in figure 4. It is obvious from the figure that the generation of path backscatter messages shows much diversity between the two ASes. It also indicates that the victim probably has large number of attacks from various internet points **[15]**.

The locations of reflector IP addresses all over the world are depicted in Figure 5. They are all capable to produce ICMP error messages.

Different classes of messages and tuples with their contribution ratio are displayed in Figure 6. Among all, TIMXCEED_INTRANS and UNREACH_HOST enclose more messages and IP tuples. Stub messages indicate the path backscatter messages from stub source AS. The original destination is not the stub source AS.

Comparison of Cumulative Distribution Function with top reflector of the original destination IP is exhibited in Figure 7(a). Figure 7(b) shows the attacks on less number of addresses from various corners.

The result offers that the number of attackers is potentially large. The possibility of original destinations to be reflectors is far less.

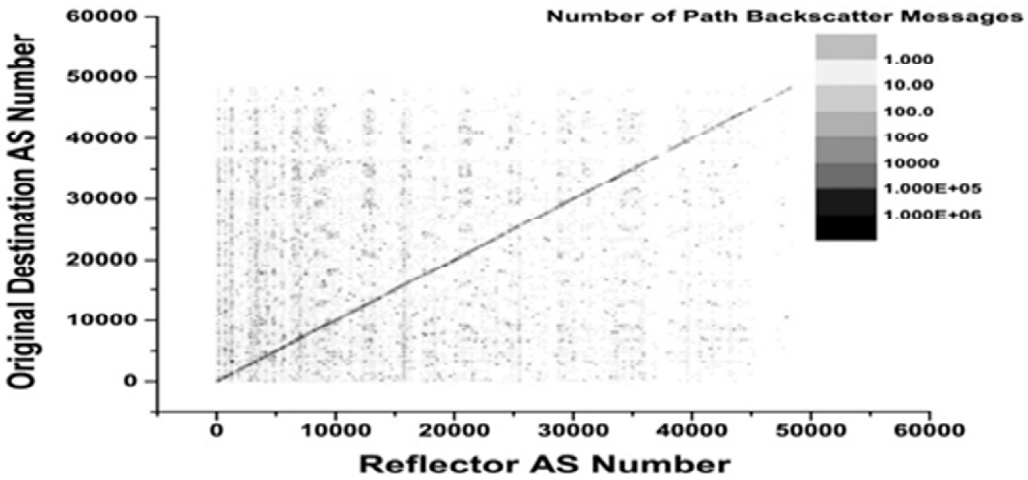

Figure 4: Path backscatter AS tuples

Figure 5: The geolocations of reflectors

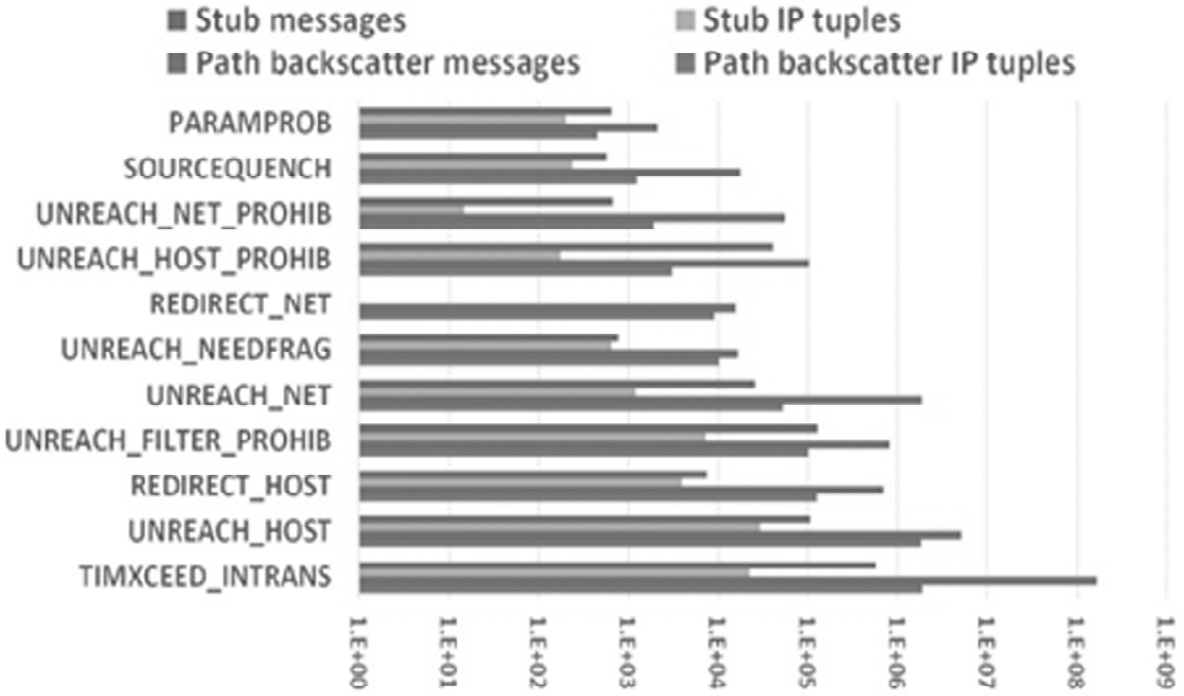

Figure 6: Classes and their proportions

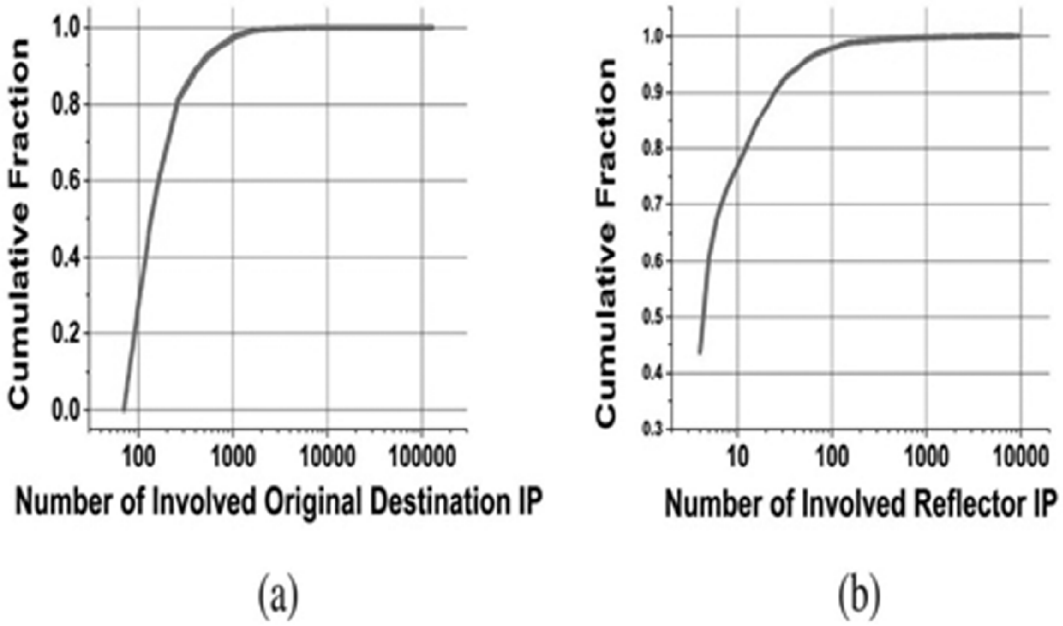

Figure 7: (i) The top original destination IP. (ii) The top reflector IP

8. CONCLUSION

In this paper, we identify the Spoofer location by introducing Passive IP Trackback through the path backscatter. With this implementation, the topology and routing, either both should be known or unknown or none of them is known. The correctness was proved by applying the PIT in large scale networks with two effective algorithms. In simulation results, we have demonstrated the effectiveness of the PIT. Further this result helps us to reveal IP spoofing.

ACKNOWLEDGEMENT

Authors deliver their graduate to SERB (Young Scientist Scheme, No. SP/FTP/ETA-51/2013) Govt. of India for Financial Assistance and The author would like to deliver their graduate to Bharath University, Chennai, India for their support during this research work

REFERENCES

[1] S. Savage, D. Wetherall, A. Karlin, and T. Anderson, "Practical network support for ip traceback," in ACM SIGCOMM Computer Communication Review, vol. 30, pp. 295-306, ACM, 2000.

[2] M. T. Goodrich, "Efficient packet marking for large-scale ip traceback," in Proceedings of the 9th ACM Conference on Computer and Communications Security, pp. 117-126, ACM, 2002.

[3] H. C. Lee, V. L. Thing, Y. Xu, and M. Ma, "Icmp traceback with cumulative path, an efficient solution for ip traceback," in Information and Communications Security, pp. 124–135, Springer, 2003.

[4] Y. Xiang, W. Zhou, and M. Guo, "Flexible deterministic packet marking: An ip traceback system to find the real source of attacks," Parallel and Distributed Systems, IEEE Transactions on, vol. 20, no. 4, pp. 567-580, 2009.

[5] A. Yaar, A. Perrig, and D. Song, "Fit: fast internet traceback," in INFOCOM 2005, 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE 2, pp. 1395–1406, IEEE, 2005.

[6] J. Liu, Z.J. Lee, and Y.C. Chung, "Dynamic probabilistic packet marking for efficient IP traceback," Computer Network, vol. 51, no. 3, pp. 866–882, 2007.

[7] Y. Xiang, W. Zhou, and M. Guo, "Flexible deterministic packet marking: An IP traceback system to find the real source of attacks," IEEE Transaction on Parallel Distribution System, vol. 20, no. 4, pp. 567–580, Apr. 2009.

[8] K. Park and H. Lee, "On the effectiveness of probabilistic packet marking for IP traceback under denial of service attack," in Proc. IEEE 20th Conference on IEEE Computer Communication Society (INFOCOM), vol. 1, Apr. 2001, pp. 338-347.

[9] R. P. Laufer et al., “Towards stateless single-packet IP traceback,” in Proceeding, 32nd IEEE Conf. Local Computer Network (LCN), Oct. 2007, pp. 548-555.

[10] H. C. J. Lee, V. L. L. Thing, Y. Xu, and M. Ma, “ICMP traceback with cumulative path, an efficient solution for IP traceback,” in Information and Communications Security. Berlin, Germany: Springer-Verlag, 2003, pp. 124-135.

[11] M. Adler, “Trade-offs in probabilistic packet marking for IP traceback,” J. ACM, vol. 52, no. 2, pp. 217-244, Mar. 2005.

[12] A. Belenky and N. Ansari, “IP traceback with deterministic packet marking,” IEEE Communication Letter, vol. 7, no. 4, pp. 162-164, Apr. 2003.

[13] A. Mankin, D. Massey, C.-L. Wu, S. F. Wu, and L. Zhang, “On design and evaluation of ‘intention-driven’ ICMP traceback,” in Proc. 10th International Conference Computer Communication Network, Oct. 2001, pp. 159–165

[14] Dr. A. Rengarajan, S. Rajasekaran, P. Kumaran, “Incorporation of Security Features in Agonistic Protocol in the Web Search”, Middle-East Journal of Scientific Research (MEJSR), ISSN: 1990-9233, Volume 23, Issue 9, 2015 and Page No: 2051-2059.

[15] M. D. D. Moreira, R. P. Laufer, N. C. Fernandes, and O. C. M. B. Duarte, “A stateless traceback technique for identifying the origin of attacks from a single packet,” in Proc. IEEE Int. Conference on Communication (ICC), Jun. 2011, pp. 1-6.