International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 23 Issue 9 – DECEMBER 2016.

AN UNIQUE SCHEME FOR DETECTING IP SPOOFERS USING PASSIVE IP TRACEBACK

LANKA VENNELA[#1] and VEERA RAJU RYALI[*2]

[#] *PG Scholar, Kakinada Institute Of Engineering & Technology Department of Computer Science, JNTUK,A.P, India*

[*] *Assistant Prof., Dept of CSE, Kakinada Institute of Engineering & Technology, JNTUK, A.P, INDIA*

***Abstract*— IP spoofing is a attack in which attacker launch the attack by using forged source IP address. It is long known attackers may use forged source IP address to conceal their real locations. To capture the spoofers, a number of IP traceback mechanisms have been proposed. However, due to the challenges of deployment, there has been not a widely adopted IP traceback solution, at least at the Internet level. As a result, the mist on the locations of spoofers has never been dissipated till now. Here it proposes passive IP traceback (PIT) that bypasses the deployment difficulties of IP traceback techniques. PIT investigates Internet Control Message Protocol error messages (named path backscatter) triggered by spoofing traffic, and tracks the spoofers based on public available information (e.g., topology). In this way, PIT can find the spoofers without any deployment requirement. Here it illustrates the causes, collection, and the statistical results on path backscatter, demonstrates the processes and effectiveness of PIT, and shows the captured locations of spoofers through applying PIT on the path backscatter data set. These results can help further reveal IP spoofing, which has been studied for long but never well understood.**

***Index Terms*— PIT(Passive IP Trackback), Computer network management, computer network security, denial of service (DoS), IP traceback.**

I. INTRODUCTION

IP traceback is employed to construct the trail travelled by information processing packets from supply to destination. A sensible and effective information processing traceback resolution supported path disperse messages, i.e., PIT, is planned. PIT bypasses the readying difficulties of existing information processing traceback mechanisms and really is already effective [1]. It given the limitation that path disperse messages don't seem to be generated with stable chance, PIT cannot add all the attacks, however it will add variety of spoofing activities. a minimum of it should be the most helpful traceback mechanism before Associate in Nursing AS-level traceback system has been deployed in real [2].

Through applying PIT on the trail disperse dataset, variety of locations of spoofers square measure captured and conferred. Even though this is often not a whole list, it's the 1st celebrated list revealing the locations of spoofers. PIT examines net management Message Protocol blunder messages (named means backscatter) activated by mocking movement, and tracks the spoofers in light-weight of open accessible information (e.g., topology) [3]. Along these lines, PIT will notice the spoofers with no game arrange want. This paper represent to the explanations, accumulation, and therefore the authentic results on means disperse, displays the systems and adequacy of PIT, and shows regions of spoofers through applying PIT in transit disperse information set. These outcomes will assist additional with uncovering information processing spoofing, that has been examined for long but never sure celebrated [4].

To capture the origins of IP spoofing traffic is of great importance. As long as the real locations of spoofers are not disclosed, they cannot be deterred from launching further attacks[5]. Even just approaching the spoofers, for example, determining the AS-level or networks they reside in, attackers can be located in a smaller area, and filters can be placed closer to the attacker before attacking traffic get aggregated. The last but not the least, identifying the origins of spoofing traffic can help build a reputation system for AS-level, which would be helpful to push the corresponding ISPs to verify IP source address [6].

Routers may fail to forward an IP spoofing packet due to various reasons, e.g., TTL exceeding[6]. In such cases, the routers may generate an ICMP error message (named path backscatter) and send the message to the spoofed source address. Because the routers can be close to the spoofers, the path backscatter messages may potentially disclose the locations of the spoofers. PIT exploits these path backscatter messages to find the location of the spoofers. With the locations of the spoofers known, the victim can seek help from the corresponding ISP to filter out the attacking packets, or take other counterattacks. PIT is especially useful for the victims in reflection based spoofing attacks, e.g., DNS amplification attacks. The victims can find the locations of the spoofers directly from the attacking traffic. Not all the packets reach their destinations[7].

A network device may fail to forward a packet due to various reasons. Under certain conditions, it may generate an ICMP error message, i.e., path backscatter messages. The

path backscatter messages will be sent to the source IP address indicated in the original packet. If the source address is forged, the messages will be sent to the node who actually owns the address [8]. This means the victims of reflection based attacks, and the hosts whose addresses are used by spoofers, are possibly to collect such messages.

II. LITERATURE SURVEY

Some existing works in this areas are as follows:

A. *Efficient Packet Marking for Large-Scale IP Traceback*

Author [7] proposed a new approach to IP traceback based on the probabilistic packet marking paradigm [6]. Our approach, which we call randomize-and-link, uses large checksum cords to ”link” message fragments in a way that is highly scalable, for the checksums serve both as associative addresses and data integrity verifiers. The main advantage of these checksum cords is that they spread the addresses of possible router messages across a spectrum that is too large for the attacker to easily create messages that collide with legitimate messages. Our methods therefore scale to attack trees containing hundreds of routers and do not require that a victim know the topology of the attack tree a priori. In addition, by utilizing authenticated dictionaries in a novel way, our methods do not require routers sign any setup messages individually.

B. *Practical Network Support for IP Traceback*

This paper [8] describes a technique for tracing anonymous packet flooding attacks in the Internet back towards their source. This work is motivated by the increased frequency and sophistication of denial-of-service attacks and by the difficulty in tracing packets with incorrect, or ”spoofed”, source addresses. In this paper we describe a general purpose traceback mechanism based on probabilistic packet marking in the network. Our approach allows a victim to identify the network path(s) traversed by attack traffic without requiring interactive operational support from Internet Service Providers (ISPs) [3]. Moreover, this traceback can be performed ”post-mortem” after an attack has completed. We present an implementation of this technology that is incrementally deployable, (mostly) backwards compatible and can be efficiently implemented using conventional technology.

C. *FIT: Fast Internet Traceback*

E-crime is on the rise [9]. The costs of the damages are often on the order of several billion of dollars. Traceback mechanisms are a critical part of the defense against IP spoofing and DoS attacks. Current traceback mechanisms are inadequate to address the traceback problem Problems with the current traceback mechanisms:

- Victims have to gather thousands of packets to reconstruct a single attack path
- They do not scale to large scale attacks
- They do not support incremental deployment

D. *ICMP Traceback with Cumulative Path, An Efficient Solution for IP Traceback*

DoS/DDoS attacks constitute one of the major classes of security threats in the Internet today. The attackers usually use IP spoofing to conceal their real location. The current Internet protocols and infrastructure do not provide intrinsic support to traceback the real attack sources. The objective of IP Traceback is to determine the real attack sources, as well as the full path taken by the attack packets. Different traceback methods have been proposed, such as IP logging, IP marking and IETF ICMP Traceback (ITrace). In this paper [10], we propose an enhancement to the ICMP Traceback approach [11], called ICMP Traceback with Cumulative Path (ITrace-CP). The enhancement consists in encoding the entire attack path information in the ICMP Traceback message. Analytical and simulation studies have been performed to evaluate the performance improvements. We demonstrated that our enhanced solution provides faster construction of the attack graph, with only marginal increase in computation, storage and bandwidth.

E. *Trace IP Packets by Flexible Deterministic Packet Marking (FDPM)*

Currently a large number of the notorious Distributed Denial of Service (DDoS) attack incidents make people aware of the importance of the IP traceback technique. IP traceback is the ability to trace the IP packets to their origins. It provides a security system with the capability of identifying the true sources of the attacking IP packets. IP traceback mechanisms have been researched for years, aiming at finding the sources of IP packets quickly and precisely. In this paper, an IP traceback scheme, Flexible Deterministic Packet Marking (FDPM) [12], is proposed. It provides more flexible features to trace the IP packets and can obtain better tracing capability over other IP traceback mechanisms, such as link testing, messaging, logging, Probabilistic Packet Marking (PPM) [13] [14], and Deterministic Packet Marking (DPM) [15]. The implementation and evaluation demonstrates that the FDPM needs moderately a small number of packets to complete the traceback process and requires little computation work; therefore this scheme is powerful to trace the IP packets. It can be applied in many security systems, such as DDoS defense systems [4], Intrusion Detection Systems (IDS), forensic systems, and so on.

F. *Security problems in the TCP/IP protocol suite*

S. M. Bellovin [16] has explained The TCP/IP protocol suite, which is very widely used today, was developed under the sponsorship of the Department of Defence. Despite that, there are a number of serious security flaws inherent in the protocols, regardless of the correctness of any implementations. Here the author describe a variety of attacks based on these flaws, including sequence number spoofing, routing attacks, source address spoofing, and authentication attacks and also present defences against these attacks[6].

G. *Distributed denial of service (DDOS) attacks*

Felix Lau Simon [17] has discussed about distributed denial of service attacks in the Internet. The has described attacks on Yahoo!, Amazon.com, CNN.com, and other major Web sites. A denial of service is characterized by an explicit attempt by an attacker to prevent legitimate users from using resources. An attacker may attempt to: “flood” a network and

thus reduce a legitimate user's bandwidth, prevent access to a service, or disrupt service to a specific system or a user. Some methods and techniques used in denial of service attacks, and provides the list of possible defences. The study of distributed denial of service attack can be done by using ns-2 network simulator. The algorithms are implemented in a network router to perform during an attack, and whether legitimate users can obtain desired bandwidth[8].

III. EXISTING SYSTEM

Existing IP traceback approaches can be classified into five main categories: packet marking [7] [16], ICMP traceback [11] [10], logging on the router, link testing, overlay, and hybrid tracing.

1. Packet marking methods require routers modify the header of the packet to contain the information of the router and forwarding decision.
2. Different from packet marking methods, ICMP traceback generates addition ICMP messages to a collector or the destination.
3. Attacking path can be reconstructed from log on the router when router makes a record on the packets forwarded.
4. Link testing is an approach which determines the upstream of attacking traffic hop-by-hop while the attack is in progress.
5. Center Track proposes offloading the suspect traffic from edge routers to special tracking routers through a overlay network

A. *ISSUES IN EXISTING SYSTEM*

1. Based on the captured backscatter messages from UCSD Network Telescopes, spoofing activities are still frequently observed. To build an IP traceback system on the Internet faces at least two critical challenges. The first one is the cost to adopt a traceback mechanism in the routing system. Existing traceback mechanisms are either not widely
2. Supported by current commodity routers, or will introduce considerable overhead to the routers (Internet Control Message Protocol (ICMP) generation, packet logging, especially in high-performance networks. The second one is the difficulty to make Internet service providers (ISPs) collaborate.
3. Since the spoofers could spread over every corner of the world, a single ISP to deploy its own traceback system is almost meaningless.
4. However, ISPs, which are commercial entities with competitive relationships, are generally lack of explicit economic incentive to help clients of the others to trace attacker in their managed AS-level
5. Since the deployment of traceback mechanisms is not of clear gains but apparently high overhead, to the best knowledge of authors, there has been no deployed Internet-scale IP traceback system till now.
6. Despite that there are a lot of IP traceback mechanisms proposed and a large number of spoofing activities observed, the real locations of spoofers still remain a mystery.

IV. PROPOSED SYSTEM

This paper introduces an approach to, named Passive IP Traceback (PIT), to bypass the difficulties in organization. routers may fail to forward an IP spoofing packet because of different reasons, e.g., TTL surpassing. In such cases, the switches may produce an ICMP lapse message (named way backscatter) and send the message to the caricature source address. Since the switches can be near the spoofers, the way backscatter messages might conceivably reveal the spoofers area. PIT exploits these way backscatter messages to discover the spoofers area. With the spoofers areas known, the casualty can look for assistance from the relating ISP to filters through the attackers packets, or take different counterattack. PIT is particularly valuable for the victims in reflection based spoofing attack, e.g., DNS amplification attack. The casualties can discover the spoofers areas specifically from the attacking movement.

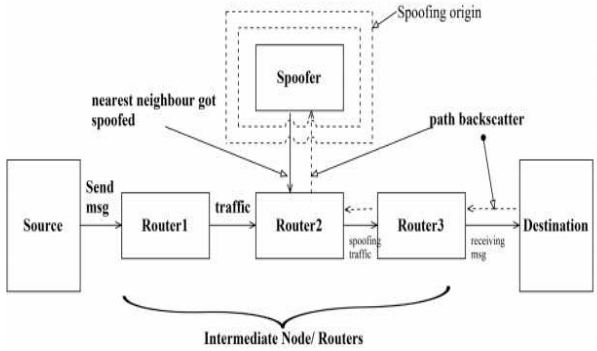

Fig.1 System Architecture

A. *Advantages of Proposed System:*

1. IP traceback is a technique to traceback to the orientation of the packets.
2. Packet marking schemes are the most effective implementation towards stopping DoS attacks by tracing to the source of attacks.
3. This is the first article recognized which investigates in deep path backscatter messages. These messages are valuable to help recognize spoofing activities. Though Moore has subjugated backscatter messages, which are generated by the targets of spoofing messages, to learn Denial of Services (DoS), path backscatter messages, which are sent by intermediate nodes rather than the targets, have not been used in traceback.

1) *PROBLEM STATEMENT*

The Distributed Denial of Service (DDoS) attacks are launched synchronously from multiple locations and they are extremely harder to detect and stop. Identifying the true origin of the attacker along with the necessary preventive measures helps in blocking further occurrences these types of attacks. The issue of tracing the source of the attack deals with the problem of IP traceback.

2) *GOALS AND OBJECTIVES*

1. Designing the IP traceback techniques to disclose the real origin of IP traffic or track the path.
2. A practical and effective IP traceback solution based on path backscatter messages.
3. Passive IP traceback (PIT) that bypasses the deployment

difficulties of IP traceback techniques.

4. Packet marking methods to modify the header of the packet to contain the information of the router and forwarding decision.

3) METHODOLOGY

1. Find the shortest path from source (s) node to destination (d) node.
2. The message can be send from r to d through many intermediate nodes i.e. routers (r).
3. There may any spoofers origin available in between the path

Assume, that 'sp' is the spoofers node in the network. There are two assumptions for locating such spoofing origin while routing the packets in the network.

a) Loop-Free Assumption: This assumption states there is no loop in the paths. This assumption always holds unless misconfiguration or the routing has not converged.

b) Valley-Free Assumption: This assumption states there should be no valley in the some node level network paths. Though the increased complexity of node relationship has reduced the universality of this assumption, it is still the most common model of intermediate network level routing.

1) If suppose any intermediate node has being spoofed by spoofers node then the destination node will send the path backscatter message to all intermediate node indicating that spoofing has occurred at somewhere in the network.

2) Then each node in network will send the acknowledgment for that path backscatter message. The node which fails to give back acknowledgment that will be assumed as spoofers node.

B. MATHEMATICAL MODEL

Let S is the Whole System Consists:

S= {V, E, P, G}.

Where,

- V is the set of all the network nodes.
- E is the set of all the links between the nodes in the network.
- P is path function which defines the path between the two nodes.
- Let G is a graph.

Suppose, G (V, E) from each path backscatter, the node u, which generates the packet and the original destination v, Where u and v are two nodes in the network. i.e. u ∈ V and v ∈ V of the spoofing packet can be got. We denote the location of the spoofers, i.e., the nearest router or the origin by s, Where, s ∈ V.

1) PROCEDURE

1. For each path backscatter message, at first we check whether it belongs to the classes i.e. dataset or source list. If yes, the reflector should be near the attacker.
2. We simply use the source AS of the message as the position of the spoofers. If the message does not belong to the types, it is mapped into an AS tuple.
3. We conclude whether the AS tuple can accurately locate the source AS of the attacker based on our proposed mechanisms. Then if the AS tuple can exactly locate the source AS of the message, the source AS of the spoofers is just this AS.
4. Then we also use the source AS-level as the location of the spoofer.

We assume some Probability for Accurate Locating on Loop-Free for spoofer based on the Loop-free assumption, to accurately locate the attacker from a path backscatter message (v, s),

There are three conditions:

1) LF-C1: the degree of the attacker sis 1;
2) LF-C2: v is not s;
3) LF-C3: u is s.

Based on the Assumption I, the probability of LF − C1 is equal to the ratio of the network nodes whose degree is 1. To estimate our assumptions of probability, we introduce the power law of degree distribution from,

$$f_d \alpha d^o \qquad (1)$$

Where f_d is the frequency of degree d, and O is the out degree exponent.

Transform it to $f_d = \lambda d^o + b_d$, (2)

Where λ and b_d are two constants. Then,

$$f_1 = \lambda + b_d \qquad (3)$$

Based on the Assumption II, the possibility of LF − C2 is basically (N − 1)/N.

Based on the Assumption III, the probability of LF −C3 is equal to 1/(1+len(path(u, v)).

Because s and u are random chosen, the expectation of len (path (u,v)) is the effective diameter of the network δ_{ef}. i.e,

$$\delta_{ef} = 1 + len(path((u,v)) \qquad (4)$$

Based on our three assumptions, these conditions are mutually independent. Thus, the expectation of the probability of accurate locating the attacker is

$$E(P_{LF-accurate)} = \frac{N-1}{N} * \frac{\lambda + b_d}{1+\delta_{ef}} \qquad (5)$$

This form gives some insight on the probability of accurate locating of spoofer. If the power-law becomes stronger, λ will get larger and δ_{ef} will get smaller. Then the probability of accurate locating will be larger.

We proposed Passive IP Traceback (PIT) which tracks spoofers based on path backscatter messages and public available information. We specified how to apply PIT when the topology and routing are both known, or the routing is unknown, or neither of them are known. We presented two effective algorithms to apply PIT in large scale networks and proofed their correctness. We demonstrated the effectiveness of PIT based on deduction and simulation. We showed the captured locations of spoofers through applying PIT on the path backscatter dataset.

2) APPLICATIONS

1) IP traceback is a method to traceback to the source of the packets.

2) Packet marking schemes are the most successful implementation towards preventing DoS attacks by tracing to

the source of attacks.

V. RESULTS AND IMPLEMENTATION

The NS2 tool is used to study the performance of our scheme in detecting IP spoofers by using PIT (passive IP Traceback) can be evaluated through graph. We employ the IEEE 802.11 [17] MAC with a channel data rate of 11 Mb/s. We make comparative analysis with existing and proposed system, which is represented in the stimulation graphs. We choose the important evaluation metrics: End to End delay, cumulative fraction, throughput and Number of bytes received.

Fig2. End -To –End Delay

Red line show proposed system and green line is for existing system. Figure 2 shows the end to end delay for both existing and proposed system. Delay after applying PIT is less in proposed system as compared to existing system.

Figure 3. Shows overall performance of the proposed system.

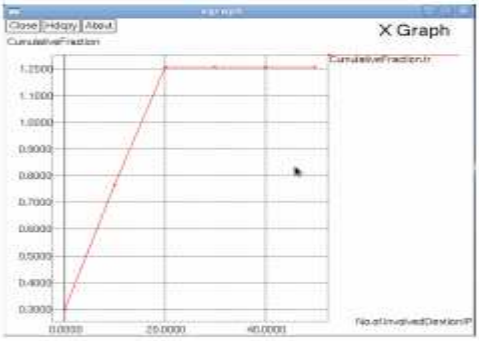

Fig3. Cumulative Fraction

Figure 4. Throughput

Fig.4 represents throughput for existing and proposed system. Throughput is more in proposed system than in existing system

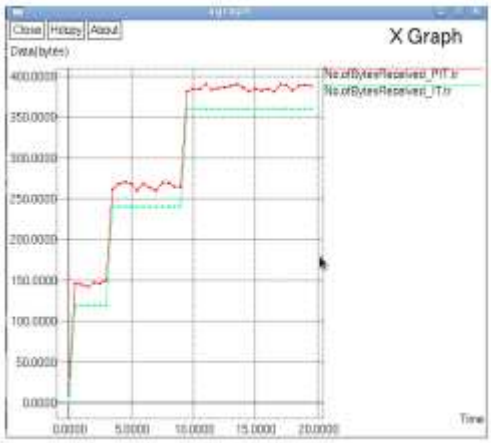

Fig 5. Number Of Bytes Received

Figure.5 shows number of bytes received in proposed system is more than the existing system. In above graph the Number of bytes received is more in proposed system this is achieved by PIT (Passive IP Traceback) .

VI. CONCLUSION

In this paper, we have presented a new technique, backscatter analysis, for estimating denial-of-service attack activity in the Internet. Using this technique, we have observed widespread DoS attacks in the Internet, distributed among many different domains and ISPs. The size and length of the attacks we observe are heavy tailed, with a small number of long attacks constituting a significant fraction of the overall attack volume. Moreover, we see a surprising number of attacks directed at a few foreign countries, at home machines, and towards particular Internet services. We try to dissipate the mist on the actual locations of spoofers based on investigating the path backscatter messages. In this, we proposed Passive IP Traceback (PIT) which tracks spoofers based on path backscatter messages and public available information. We illustrate causes, collection, and statistical results on path backscatter. We specified how to apply PIT when the topology and routing are both known, or the routing is unknown, or neither of them are known. We presented two effective algorithms to apply PIT in large scale networks and proofed their correctness. We proved that, the effectiveness of PIT based on deduction and simulation. We showed the captured locations of spoofers through applying PIT on the path backscatter dataset. In future work we can extend this to include more power full cryptographic technique.

REFERENCES

[1] S. M. Bellovin, “Security problems in the TCP/IP protocol suite,” ACM SIGCOMM Comput. Commun. Rev., vol. 19, no. 2, pp. 32–48, Apr. 1989.

[2] ICANN Security and Stability Advisory Committee, “Distributed denial of service (DDOS) attacks,” SSAC, Tech. Rep. SSAC Advisory SAC008, Mar. 2006.

[3] C. Labovitz, “Bots, DDoS and ground truth,” presented at the 50th NANOG, Oct. 2010.

[4] S. Savage, D. Wetherall, A. Karlin, and T. Anderson, “Practical network support for IP traceback,” in Proc. Conf. Appl., Technol., Archit. Protocols Comput. Commun. (SIGCOMM), 2000, pp. 295–306.

[5] S. Bellovin. ICMP Traceback Messages. [Online]. Available: http://tools.ietf.org/html/draft-ietf-itrace-04, accessed Feb. 2003.

[6] A. C. Snoeren et al., "Hash-based IP traceback," SIGCOMM Comput. Commun. Rev., vol. 31, no. 4, pp. 3–14, Aug. 2001. D. Moore, C. Shannon, D. J. Brown, G. M. Voelker, and S. Savage,"Inferring internet denial-of-service activity," ACM Trans. Comput. Syst., vol. 24, no. 2, pp. 115–139, May 2006. [Online]. Available: http://doi.acm.org/10.1145/1132026.113202
[7] M. T. Goodrich, "Efficient packet marking for large-scale IP traceback," in Proc. 9th ACM Conf. Comput. Commun. Secure (CCS), 2002, pp. 117–126.
[8] D. X. Song and A. Perrig, "Advanced and authenticated marking schemes for IP traceback," in Proc. IEEE 20th Annu. Joint Conf. IEEE Comput. Commun. Soc. (INFOCOM), vol. 2. Apr. 2001, pp. 878–886.
[9] K. Park and H. Lee, "On the effectiveness of probabilistic packet marking for IP traceback under denial of service attack," in Proc. IEEE 20th Annu. Joint Conf. IEEE Comput. Commun. Soc. (INFOCOM), vol. 1. Apr. 2001, pp. 338–347.
[10] M. Adler, "Trade-offs in probabilistic packet marking for IP traceback," J. ACM, vol. 52, no. 2, pp. 217–244, Mar. 2005.
[11] A. Belenky and N. Ansari, "IP traceback with deterministic packet marking," IEEE Commun. Lett., vol. 7, no. 4, pp. 162–164, Apr. 2003.
[12] Y. Xiang, W. Zhou, and M. Guo, "Flexible deterministic packet marking: An IP traceback system to find the real source of attacks," IEEE Trans. Parallel Distrib. Syst., vol. 20, no. 4, pp. 567–580, Apr. 2009.
[13] R. P. Laufer et al., "Towards stateless single-packet IP traceback," in Proc. 32nd IEEE Conf. Local Comput. Netw. (LCN), Oct. 2007, pp. 548–555. [Online]. Available: http://dx.doi.org/10.1109/ LCN.2007.160
[14] 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. Conf. Commun. (ICC), Jun. 2011, pp. 1–6.
[15] 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 Int. Conf. Comput. Commun. Netw., Oct. 2001, pp. 159–165.
[16] 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.
[17] H. Burch and B. Cheswick, "Tracing anonymous packets to their approximate source," in Proc. LISA, 2000, pp. 319–327.
[18] R. Stone, "CenterTrack: An IP overlay network for tracking DoS floods," in Proc. 9th USENIX Secur. Symp., vol. 9. 2000, pp. 199–212.

LANKA VENNELA is a student of Kakinada Institute Of Engineering & Technology affiliated to JNTUK, Kakinada pursuing M.Tech (Computer Science). Her Area of interest includes NETWORKING and its objectives in all current trends and techniques in Computer Science.

VEERA RAJU RYALI M.TECH is Working as M.Tech Assistant Professor, Department of Computer Science & Engineering of Kakinada Institute Of Engineering & Technology affiliated to JNTUK, Kakinada, A.P, India.