Vindictive IP Trackback: Revealing the Area of IP Spoofers with Efficient Tracking

Jaeerahmad Indikar[1] Irfan Bagawan[2]
[1]Assistant Professor & PG Coordinator [2]PG Student
[1,2]Department of Computer Science Engineering
[1,2]SIET, Vijayapur, India

Abstract— In IP spoofing attack, malicious node disguise their real location from victim nodes using fake IP (Internet Protocol) address, which is a major disadvantage in present internet architecture. This crime in the internet is controlled by deploying the technology named as Internet Protocol (IP) trackback technique. This project primarily focuses on IP spoofing attack, which is among one of the Denial of Service (DoS) attack. IP spoofing attack is one among the challenging issue in the internet. This trackback technique proposes a novel features to track the origin of spoofers with best tracking performance than existing techniques, as an enhancement to existing trackback techniques. Analysis of simulation results and implementation of real time system, illustrates that this IP trackback needs to add very small amount of packets, which would load the routers moderately to accomplish the objective of tracking to detect the spoofers in a vast internet. The enhanced system IP trackback mechanism achieves the objective of accomplishing best possible results on trackback although when router is loaded at its maximum. DDoS defence motivates this trackback technique.

Key words: Internet Protocol (IP), DDoS

I. INTRODUCTION

This paper is based on, defending IP spoofing attacks and to trackback the origin of malicious nodes (spoofers), which has been a prolonged major challenging issue in the network security. IP spoofers utilize counterfeited IP address to hide their original location from victim nodes and network administrators. These counterfeited IP addresses are the addresses yet to be allocated or private addresses. This IP spoofing attack is among one of the attack in Denial of Service (DoS) attacks. Dos attacks include attacks such as flooding of SYN flags, Smurf attack, and Domain Name Server (DNS) amplification. In present internet architecture, to trap the real location IP spoofers is major problem. Implementation of filters across these attackers is not possible till their original location is not determined. Instead just dragging the spoofers closer, determining the autonomous system or network in which the spoofers launch their attacks, filters can be implemented nearby the spoofers. As by minimizing the area of detecting the spoofers, the normal traffic and affected traffic can be separated with deployment of filters across the area of spoofers or across autonomous system of the spoofers. Detecting the origin of IP spoofing packets, which would help to develop a best possible system for an autonomous system (AS), as the source of that address can be identified by forcing internet Service Providers (ISP).

II. LITERATURE SURVEY

The main objective of the project is to track the spoofers, by applying the IP trackback mechanism on the affected packet. According to the definition in computer networking, IP address spoofing is generation of Internet Protocol (IP) packets with counterfeited IP address, with purpose of hiding the real location of attackers.

A. Related Work: Practical network support for IP trackback [3] – Packet Marking.

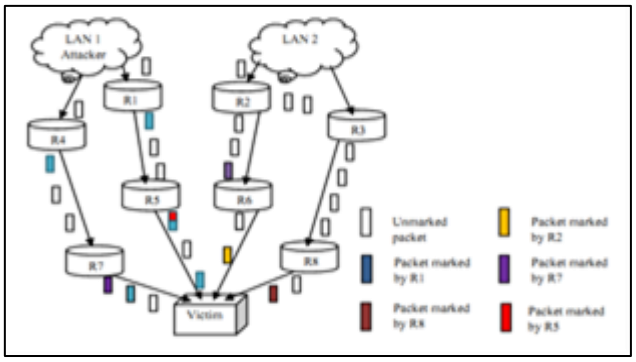

Fig. 1: IP trackback using packet marking.

This system, illustrates a technique for attacks including transmission a huge amount of traffic to block the resources of the victim. Motivation for this work is increase in DoS attacks and attacks pursuing hiding of their real address or can be said IP spoofing attack. This work, demonstrates the defensive mechanism utilizing probabilistic packet marking technique.

B. Hash-based IP trackback

The current architecture of internet includes flaws which let the attacker to hide their original identity. Although without any manipulation of IP packet origin, NAT network address translator forwarding the packets and various encryption techniques may change the original identity of packet's origin. This technique overcomes the difficulties of existing techniques, by implementing the system to trace the origin responsible for flooding of packets to a victim, by tracking the individual packet in the path. In this technique, the "Hash-based" trackback mechanism generates test results for the packets in the network and traces the source using a single packet, which was generated recently in the network.

C. Testing of each link traversed by malicious packet

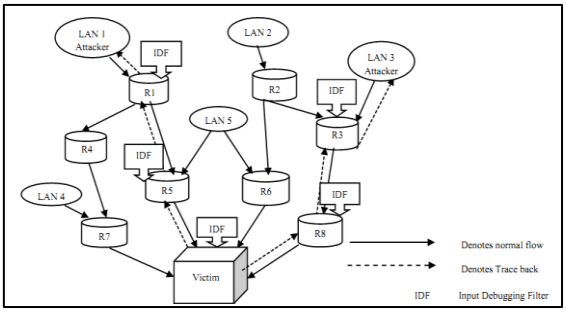

Fig -2: Testing of links.

Link Testing can be illustrated in the figure 2.1.4 above, which traces the origin of a packet towards upstream links, with the assumption of attack is in progress. Hence this type of technique would be not suitable to trace the origin of spoofers, when the attacker is aware of this mechanism. This technique includes two types of testing, "Input debugging" and "Control flooding". Input Debugging scheme involves, the attacker has to be recognized by the victim, through implementation of pattern of attacks.

III. RESULTS & ANALYSIS

This paper analyzes the simulation result of the IP trackback mechanism used in this project in detail. MIT is developed from scratch of existing track backtechniques, utilizing their applications and methodologies. But the variation in this technique is the possibility of generation of path backscatter messages. This section includes, effectiveness of the technique, results based on implementation of trackback technique on the dataset of path backscatter.

A. Evaluation of MIT.

Due to generation of huge amount of path backscatter messages, without any specific possibility. Because of this difficulty, this mechanism cannot be analyzed like other existing mechanisms, such as packet marking, packet logging etc. To locate the spoofers in with greater possibility, it tries to ignore uncertainties like path backscatter message generation with huge amount. To accomplish this objective, it tries to make out some assumptions based on attacks and message generation:

1) Attackers are randomly distributed.
2) Spoofers choose random victims for conducting attacks.
3) Path backscatter message is triggered by the random router node, between attacker and victim.

B. Possibility of precisely locating the spoofer based on "Loop-Free" assumption.

According to this assumption, attackers can be located on the basis of three situations from path backscatter messages:

1) There is only one attacker.
2) Attacker is not the destination node.
3) Reflector node (router) is attacker.

On the basis of first condition, which states network node with single node ratio is equated to this situation. To determine this possibility, power law is included,

$$f_d \propto d^{\mathcal{O}}$$

where f_d is the frequency of degree d, and $\mathcal{O}$ is the out degree exponent. Transform it to

$$f_d = \lambda d^{\mathcal{O}} + b_d$$

where λ and b_d are two constants. Then, $f_1 = \lambda + b_d$.

On the basis of second situation, the possibility is just (N-1)/N. By second condition, the possibility is equalized to 1/(1+len(path(attacker, destination node))). The accuracy of locating the attacker based on the above three conditions gives:

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

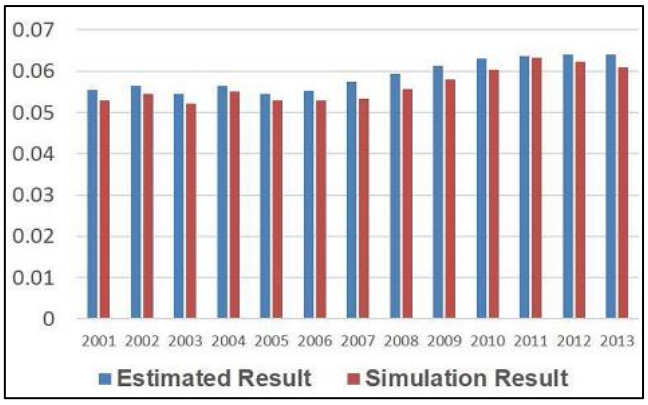

Fig. 3: Estimated result and simulation result on precisely locating the spoofers based on loop free assumption.

C. Simulation of ad hoc wireless nodes in NS2

This section illustrates the simulation of IP spoofing attack and tracking these attackers utilizing the proposed algorithms. The figure 8.2.0 below illustrates the deployment of 40 nodes in wireless ad hoc network, where after the implementation of MIT after the spoofing attack, a spoofer is located in the minimal set indicated by maroon color, as shown below in figure 8.2.2. When the spoofer is located in a minimal set, spoofer is indicated by the red color and victim node is indicated by the blue color as illustrated in figure 4.

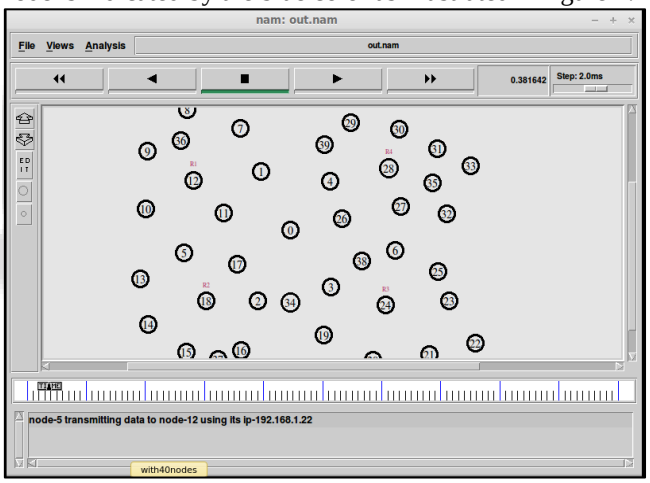

Fig. 4: This figure illustrates, the deployment of nodes in NS2

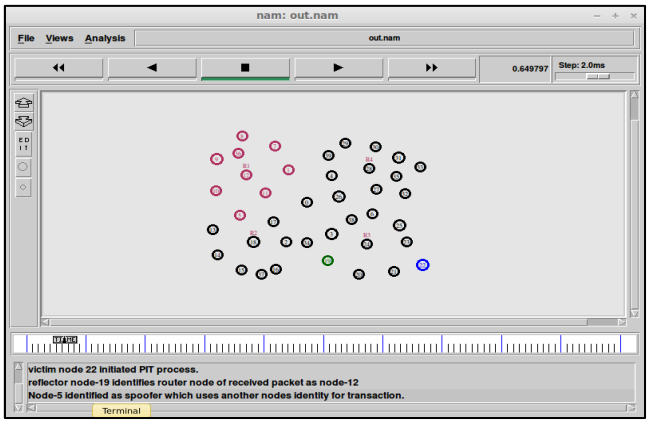

Fig. 5: It illustrates, the malicious set pursuing attacker, destination and victim node.

IV. CONCLUSION

This paper utilizes the concept of, generation of ICMP or path backscatter messages, once there is error in transmission. These messages are used in this project to track back the IP spoofers to their origin, by path reconstruction. This project illustrates detailed study on path backscatter messages. By using this technique in trapping attackers, many IP spoofing attacks has been observed across the track in the large environment of network. Using the prototype in this project, a huge quantity of attacks has been analysed, whereas it was difficult to perform this in some complex situations. This project illustrates the simulated results, by which can be observed that, a huge amount of attackers can be tracked based on the algorithms of the two assumptions. As the two assumptions are valley free and loop free. This illustrates the tracking of attackers, by determining minimal suspect set. As the spoofers are tracked in a minimal region, like in an autonomous system. Hence filters can be deployed across the autonomous systems to filter the normal traffic from malicious traffic. It overcomes the difficulties of implementation of any special purpose devices for tracking the spoofers.

It utilizes low computational power across network elements, which would not degrade the performance of network components. The enhancement in this project includes, the computational power required by victim node and time required in path reconstruction is reduced by the use of negative acknowledgment. This project also illustrates tracking the attackers, when the topological and routing details are not available and available. It is also demonstrated, the implementation of the mechanism on the dataset of path backscatter. But this project could not fully overcome the difficulties of huge generation of path backscatter messages.

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] R. Stone, "CenterTrack:An IP overlay network for tracking DoS floods" in Proc 9th USENIX Secur symp.,vol. 9.2000, pp, 199-212
[3] S. Savage, D. Wetherall, A. Karlin, and T. Anderson, "Practical network support for IP trackback," in proc. Conf. Appl., Technol., Archit., Protocols Comput. Commun. {SIGCOMM}, 2000, PP. 295-306.
[4] 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. IEE Cmput. Commun. Soc. (INFOCOM), vol. 1. Apr. 2001, pp. 338-347.
[5] L. Gao, "On inferring autonomous system relationships in the internet," IEEE/ACM Trans. Network., vol. 9, no. 6, pp.733-745, Dec 2001.
[6] C Sneron et al., "Hash-based IP trackback," SIGCOMM Comput. Commun Rev.,vol. 31, no. 4,pp.3-14, Aug.2001.
[7] M. T. Goodrich, "Efficient packet marking for large-scale IP trackback," in Proc, 9th ACM Conf. Comput. Commun. Secur. (CCS), 2002, pp. 117-126.
[8] H. C. J. Lee, V, L. L.Thing, Y.Xu and M. Ma, "ICMP trackback with cumulative path,an efficient solution for IP trackback,"in Information and Communications Security. Berlin Germany : Springer-Verlag,2003,pp. 124-135.

