Scientific Journal of Impact Factor (SJIF): 4.72

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 4, Issue 5, May -2017

IP Traceback using Deterministic Packet Marking

Shital G lungase[1], Poonam B ragmahale[2], Sadhana B chitte[3], Nikhil Karnik[4]
Asst. Professor Sushma S. Shinde[5]

[1,2,3,4,5] *Computer Engineering, Siddhant College of Engineering, Pune*

Abstract — *This paper 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). 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.*
Techniques have been developed to determine the source of large packet flows, but, to date, no system has been presented to track individual packets in an efficient, scalable fashion. We present a hash-based technique for IP traceback that generates audit trails for traffic within the network, and can trace the origin of a single IP packet delivered by the network in the recent past. We demonstrate that the system is effective, space-efficient (requiring approximately 0.5% of the link capacity per unit time in storage), and implementable in current or next-generation routing hardware. We present both analytic and simulation results showing the system's effectiveness.

Keywords- *Trace back, packet marking, IP Address, Spoofing, Security.*

I. INTRODUCTION

Denial of Service (DoS) attack attempts to generate a huge amount of traffic to the victim and thereby disrupting the service or degrading the quality of service, by depleting the resources. Distributed Denial of Service (DDoS) attack is a distributed, co-operative and large-scale attack. Attackers can launch the attack traffic from various locations of Internet, exhausting bandwidth. The processing capacity or memory of the target machine or network is drained, taking advantage of the vulnerabilities and anonymous nature of Internet. Both these attacks have been posing a major threat to the Internet for over a decade. Now-a-days these attacks are turning to be more sophisticated. DDoS attack takes place from multiple attack path from numerous zombies controlled by an attacker. According to the recent survey of Arbor networks the impact of DDoS attack is increasing every year. Even the key players such as Microsoft,Yahoo,e-bay are counted in the list of DDoS victims. The packets sent will have spoofed IP addresses [1, 2, 3] which makes it practically difficult to identify the real location of attackers. Defending an attacker with spoofed IP address is more complex and this motivates the research on IP traceback, which is a methodology to trace the true origin of spoofed IP packets.
On the internet the Distributed Denial of Service (DDoS) attack remains an open issue. The research in this field is usually categorized into detection, mitigation, and traceback. There are various detection methods in place, such as detection against mimicking attacks and information theory based detection. Based on detection, we are able to perform attack source traceback, and traceback is a critical step to eliminate cyber-attacks. IP traceback is used to construct the path travelled by IP packets from source to destination. A practical and effective IP traceback solution based on path backscatter messages, i.e., Feasible IP Traceback, is proposed. FIT bypasses the deployment difficulties of existing IP traceback mechanisms and actually is already in force. Though given the limitation that path backscatter messages are not generated with stable possibility, FIT cannot work in all the attacks, but it does work in a number of spoofing activities. This might be the most useful traceback approach before an AS-level traceback system has been deployed in real. Through applying PIT on the path backscatter dataset, a number of locations where spoofers are captured and affected the nodes and network security. Though this is not a complete list, it is the first known list disclosing the locations of spoofers. This feasible IP traceback technique examines Internet Control Message Protocol (ICMP) messages activated by mocking movement, and tracks the spoofers in light of open accessible data (e.g., topology).Along these lines, FIT can find the spoofers with no game plan need. It represent to the reasons, accumulation, and the authentic results on way backscatter, displays the systems and adequacy of FIT, and displays the origins of spoofers through applying Feasible IP traceback approach. These outcomes can assist further with uncovering IP spoofing, which has been examined for long however never surely known. In spite of the fact that FIT can't work in all the spoofing attacks, it might be the most valuable instrument to follow spoofers before an Internet-level traceback framework has been sent in genuine. To capture the origins of IP spoofing traffic on the network. The research of identifying the origin of spoofing traffic is categorized in IP traceback. To implement 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 supported by current commodity routers i.e. packet marking, 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. Since the spoofers could spread over everywhere in the corner of the world, a single ISP to deploy its own traceback system is almost meaningless.

II. RELATED WORK

The problem of computing optimal strategies to modify an attack so that it evades detection by a Bayes classifier. They formulate the problem in game-theoretic terms, where each modification made to an instance comes at a price, and successful detection and evasion have measurable utilities to the classifier and the adversary, respectively. The authors study how to detect such optimally modified instances by adapting the decision surface of the classifier, and also discuss how the adversary might react to this. The setting used in assumes an adversary with full knowledge of the classifier to be evaded. Shortly after, how evasion can be done when such information is unavailable. They formulate the adversarial classifier reverse engineering problem (ACRE) as the task of learning sufficient information about a classifier to construct attacks, instead of looking for optimal strategies. The authors use a membership oracle as implicit adversarial model: the attacker is given the opportunity to query the classifier with any chosen instance to determine whether it is labeled as malicious or not. Consequently, a reasonable objective is to find in-stances that evade detection with an affordable number of queries. A classifier is said to be ACRE learnable if there exists an algorithm that finds a minimal-cost in-stance evading detection using only polynomial many queries. Similarly, a classifier is ACRE k-learnable if the cost is not minimal but bounded by k. Among the results given, it is proved that linear classifiers with continuous features are ACRE k-learnable under linear cost functions. Therefore, these classifiers should not be used in adversarial environments. Subsequent work by generalizes these results to convex-inducing classifiers, showing that it is generally not necessary to reverse engineer the decision boundary to construct undetected instances of near-minimal cost. For the some open problems and challenges related to the classifier evasion problem. More generally, some additional works have revisited the role of machine learning in security applications, with particular emphasis on anomaly detection.

III. PROPOSED SYSTEM

In the network the Distributed Denial of Service (DDoS) attacks are launched synchronously from multiple locations and they are extremely harder to discover and stop. Identifying the true origin of the attacker along with the necessary preventive measures helps in interference additional occurrences these forms of attacks. The difficulty of tracing the source of the attack deals with the matter of IP traceback mechanism.We propose a novel solution, named Passive IP Traceback (FIT), to bypass the challenges in deployment. Routers could fail to forward an associate in nursing IP spoofing packet due to various reasons, e.g., TTL exceeding. In such cases, the routers could generate an ICMP error message (named path backscatter i.e. traceback message) and send the message to the spoofed source address. Because the routers can be close to the spoofers, the path traceback messages may potentially disclose the locations of the spoofers. FIT exploits these path backscatter messages to find the location of the spoofers. With the locations of the spoofers known, the victim will look for faciliate from the corresponding node to filter out the attacking packets, or take other counterattacks. Feasible IP Traceback is especially useful for the victims in reflection based spoofing attacks, e.g., DNS amplification attacks. The victims will notice and find the locations of the spoofers directly from the attacking traffic.

Outcome :

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.

SYSTEM ARCHITECTURE

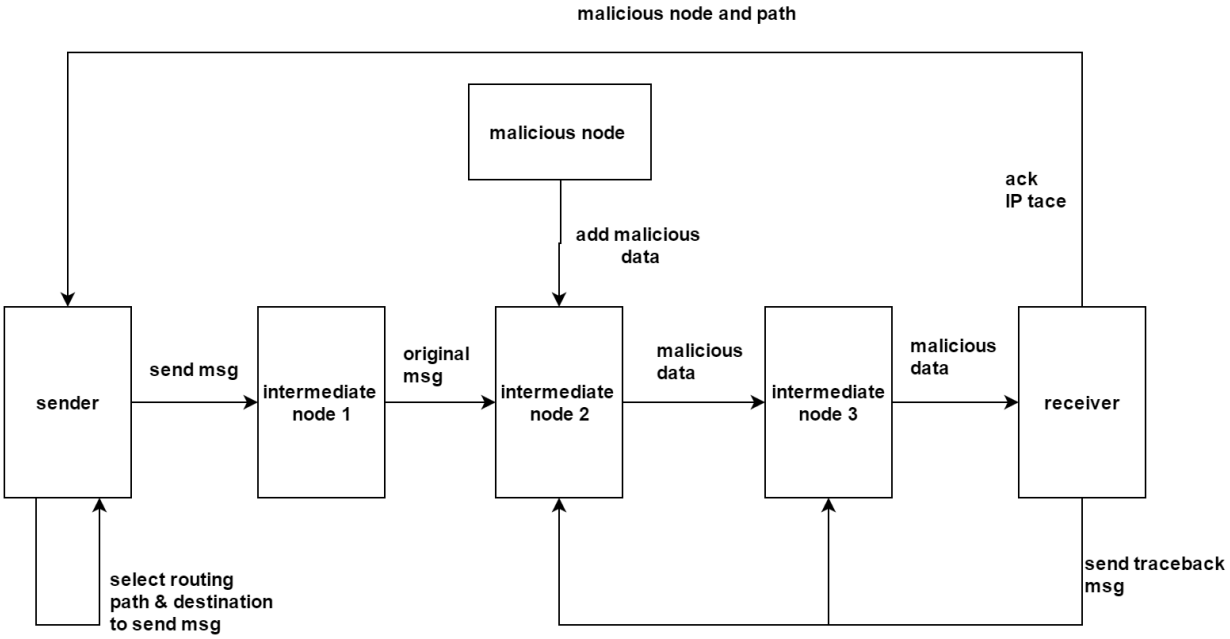


Fig.1 System Architecture

.

V. IMPLEMENTATION DETAILS

Source node:
At first the source node will select the routing path to send destination node which is in same network. As we are working in static network, the source node can choose the routing path for message to be sent to destination.

Intermediate nodes:
The message can be send from SIP to DIP through many intermediate nodes IIP that may called as routers (R).

Intermediate nodes:
The attacker/ hacker A will alters message transmitting from one node to another node in the N. there is TTL assigned on each node i.e. fixed time at each required to receive and forward the data received at node. When A will alter the message, that message will be spoofed the node at that moment where the source message is in the network for transmitting at particular intermediate node.

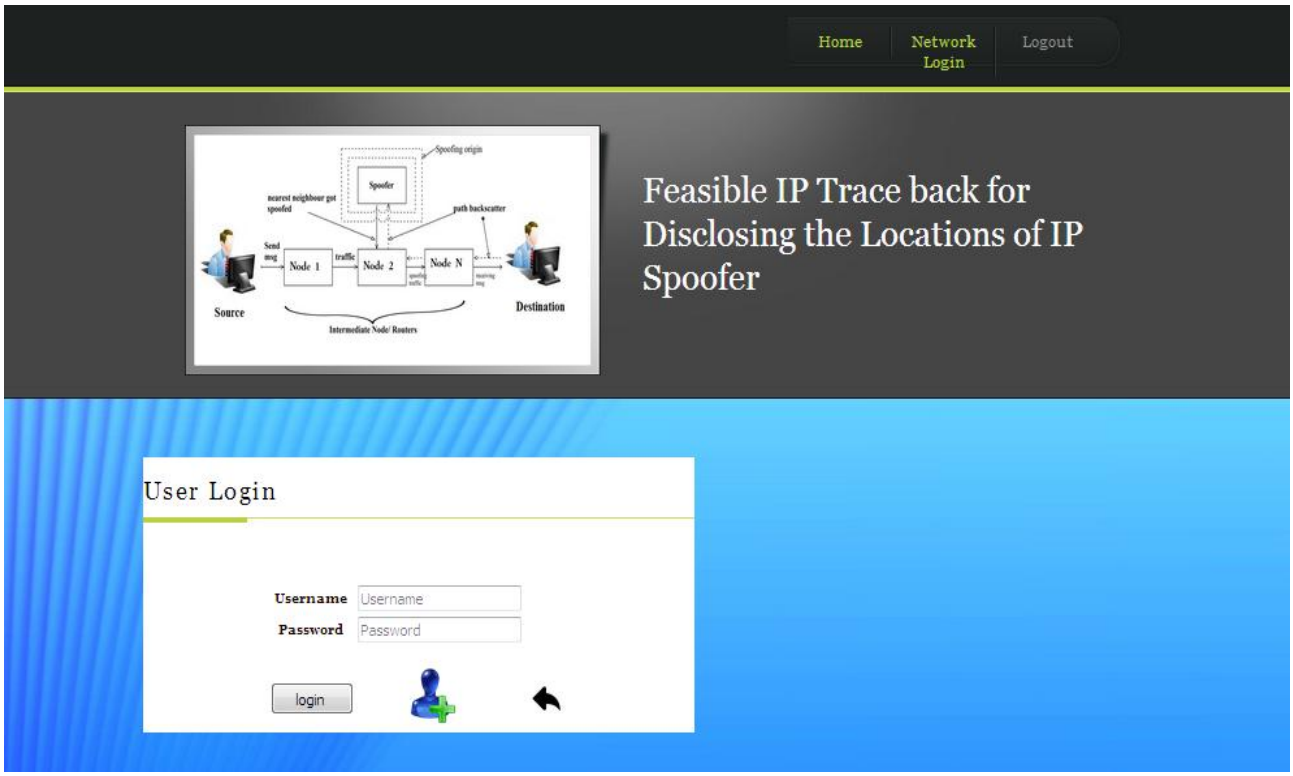
Destination Node:
Upon message delivered at destination, the destination will send the trace back message Tm to the entire intermediate nodes i.e. to the path from where the data has been received at destination through R. The destination node gets notify from system that the message received at his side is malicious or not if A has done any changes in message at particular IIP then, it will get IP address of that node indicating that node has been malicious node which has been transmitted the malicious data to all the further intermediate node in the path.

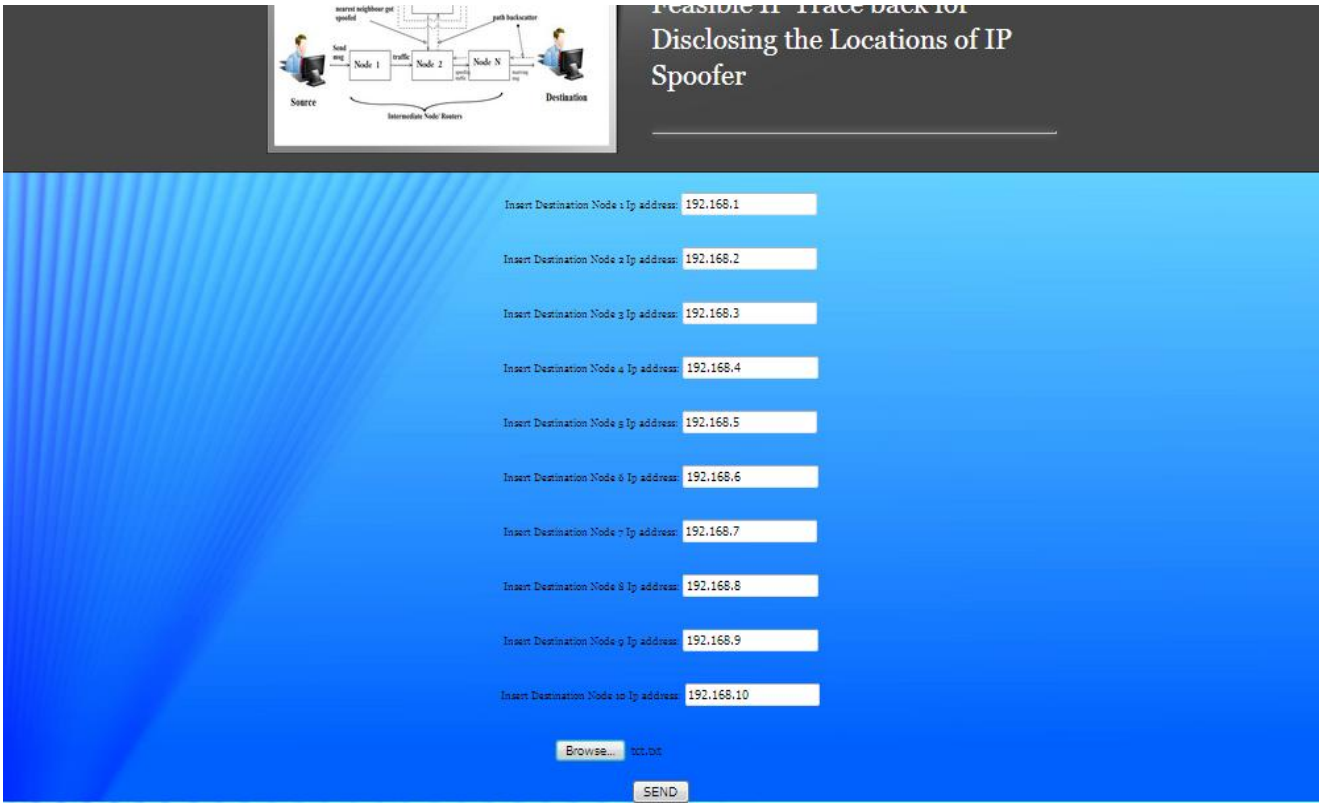
VI. Relevant mathematics associated with the Project

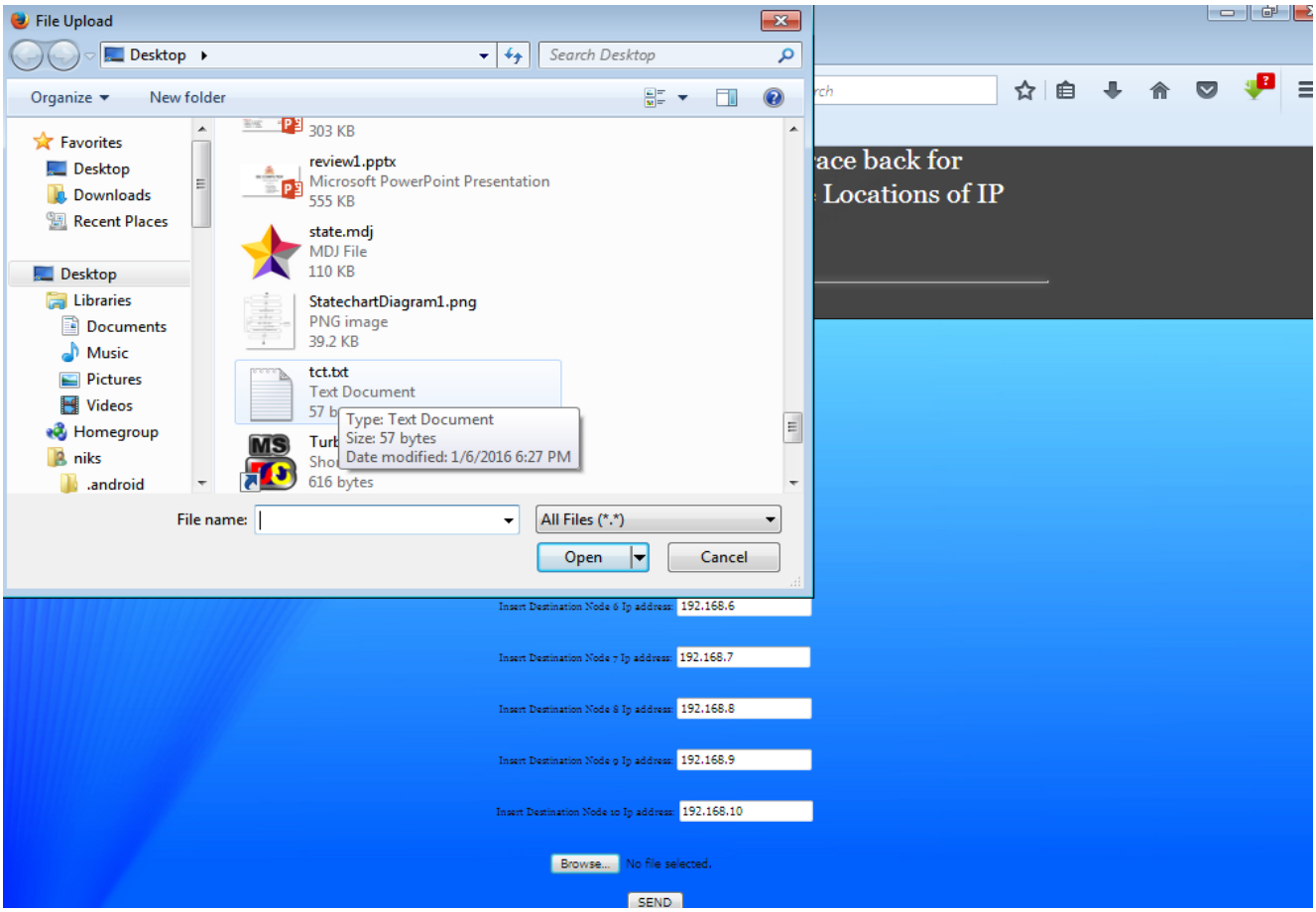
Let S is the Whole System Consists:
S= V, E, P, G.
Where,
1. V is the set of all the network nodes.
2. E is the set of all the links between the nodes in the network.
3. P is path function which defines the path between the two nodes.
4. Let G is a graph.
Suppose, G (V, E) from each path backscatter, the node u, which generates the packet

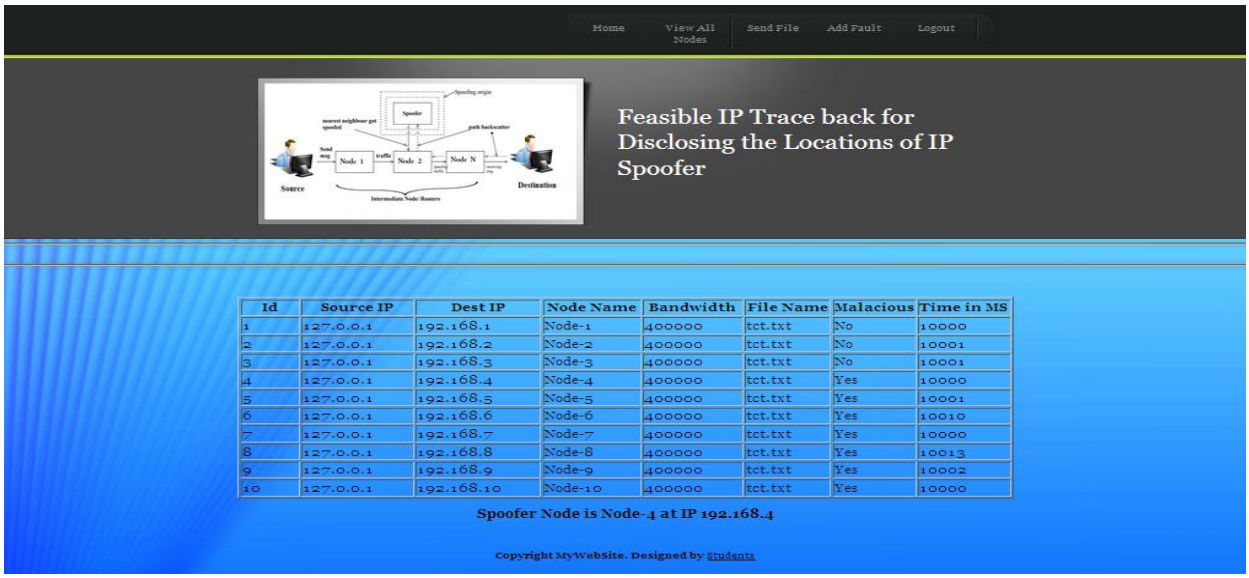
and the original destination v, Where u and v are two nodes in the network.i.e. uV
and v V of the spoofing packet can be got.
It denote the location of the spoofer, i.e., the nearest router or the origin by s, Where,
sV.

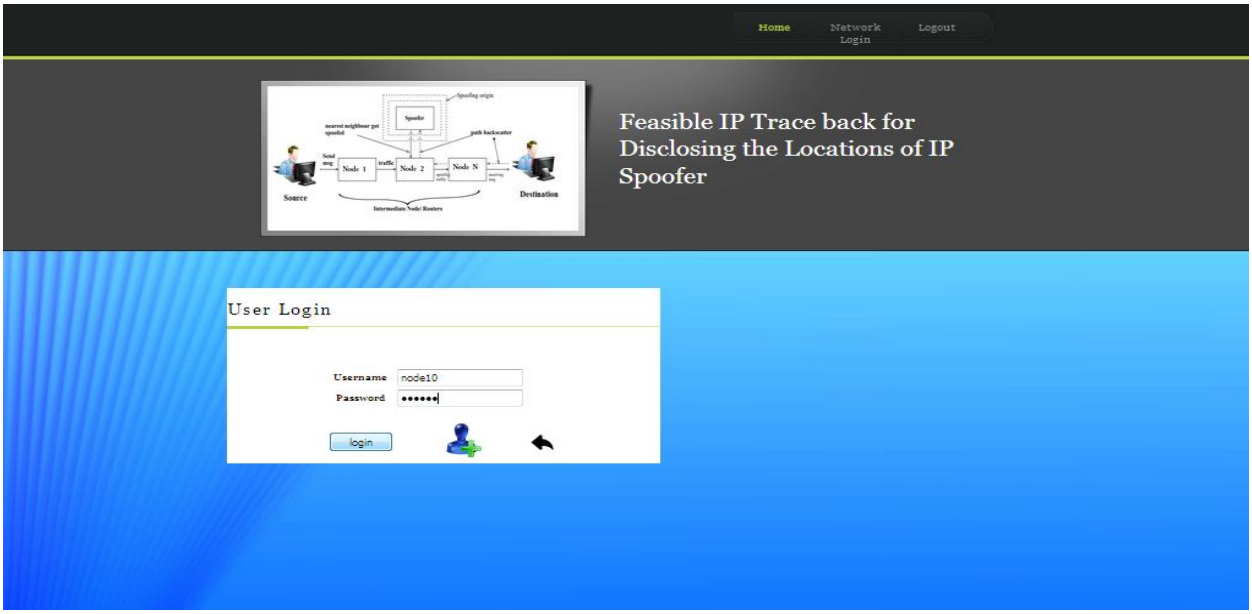
V. Snapshots

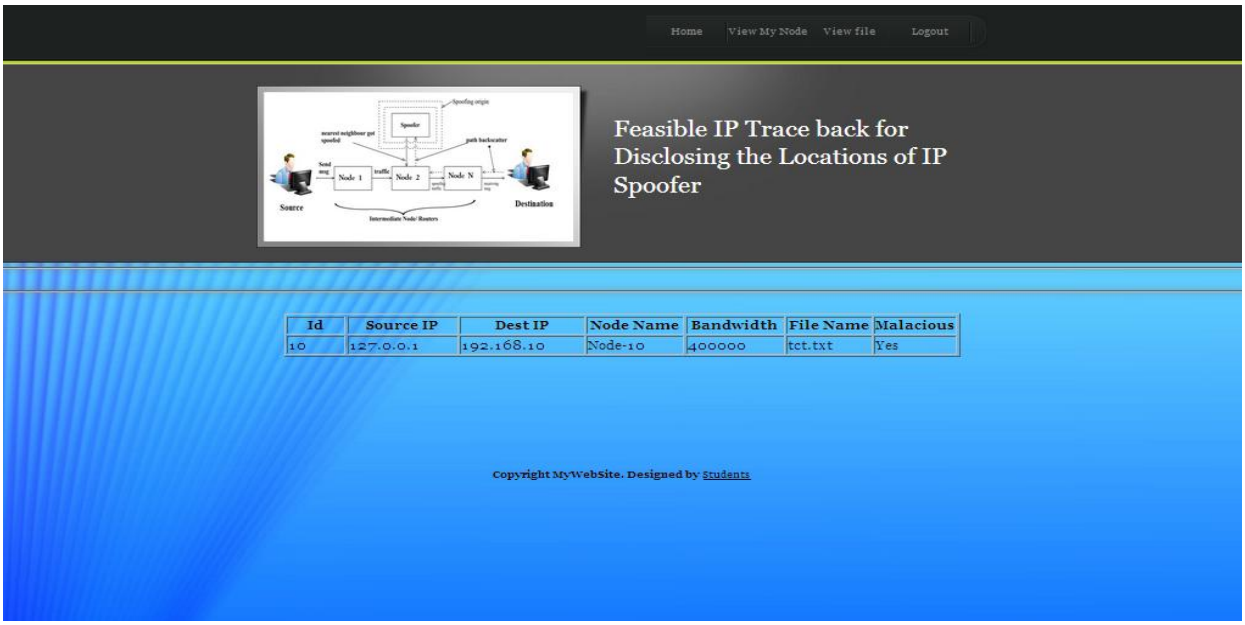












VI. Conclusion

Using a new technique, Traceback analysis, for estimating denial-of-service attack activity in the Internet. Using this technique, It observed attacks in the Internet, distributed among many different domains and ISPs. 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, we can find out the locations of spoofers.

VII. References

1) uang Yao, Jun Bi, Senior Member, IEEE, and Athanasios V. Vasilakos, Senior Member, IEEE, Passive IP Traceback: Disclosing the Locations of IP Spoofers From Path Backscatter, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 10, NO. 3, MARCH 2015.

2) S. M. Bellovin, Security problems in the TCP/IP protocol suite, ACM SIGCOMM Comput. Commun. Rev., vol. 19, no. 2, pp. 3248, Apr. 1989.

3) ICANN Security and Stability Advisory Committee, Distributed denial of service (DDOS) attacks, SSAC, Tech. Rep. SSAC Advisory SAC008, Mar. 2006.

4) C. Labovitz, Bots, DDoS and ground truth, presented at the 50th NANOG, Oct.2010.

5)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. 295306.

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

7) A. C. Snoeren et al., Hash-based IP traceback, SIGCOMM Comput. Commun. Rev., vol. 31, no. 4, pp. 314, Aug. 2001

8) S. Yu, S. Guo, and I. Stojmenovic, Fool me if you can: Mimicking attacks and anti-attacks in cyberspace, IEEE Trans. Computers, vol. 64, no. 1, pp. 139151,2005.

