INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

**ISSN: 2454-132X**
**Impact factor: 4.295**
***(Volume 5, Issue 2)***
Available online at: www.ijariit.com

# Detection of spoofing attacks in network over IP calling

*Vijay Ankamma Reddy Male*
*vijayreddy415@gmail.com*
*SRM Institute of Science and Technology, Chennai, Tamil Nadu*

*Hruthik*
*hruthiksuperstar@gmail.com*
*SRM Institute of Science and Technology, Chennai, Tamil Nadu*

*P Renuka Devi*
*renukadevi.p@ktr.srmuniv.ac.in*
*SRM Institute of Science and Technology, Chennai, Tamil Nadu*

## ABSTRACT

***Detection of call is one of the key process this generation for customers to look over and find the details and information of the caller. It is easy to identify a caller by the method of caller detection. But the calls that come from an IP based computer system through a scheme of VoIP it is difficult to find or detect a call where mostly attackers use this kind of technique. This caller detection process is also used by many banks in order to take the confirmation of the customer. This detection can be done by using a smartphone by installing an appropriate application in the mobile or by using service providers that offer caller ID spoofing. The upgrade of old hardware is very costly, and there is no mechanism available to end users where there is no storage of information and it also very difficult to locate the physical location of the attacker. The main drawback is that it is more complex when it is considered in the real world. In this article, we consider an appropriate solution named as Passive IP Trace-back to overcome the challenges in deployment in caller id detection. PIT is a kind of technique where we can find out the history of the attacker through which we can consider that a specific person is trying to attack the victim. PIT exploits the path back-scatter messages to find the location of the attacker. The scheme of PIT is used as an efficient software for computers to validate their effectiveness in the detection of spoofing attacks.***

***Keywords***— *Network, Exploits, Spoofing, PIT, VOIP, Challenges*

## 1. INTRODUCTION

Caller ID services transmit the phone number the name of a caller and related information about the caller including the number to the receiver, as caller ID intending to provide informed consent to the user before answering calls. This type of services will help the victim to find the location of the attacker who is going to steal the information because of validated phone cards or numbers. When the attacker tries to call a user through IP address then it is very difficult to find out the person, in order to trace the victim we use a technique of PIT (Passive IP Trace-back). The existing system does not provide a trustworthy, efficient and a real authentication for true locations of caller because they are vulnerable to spoofing attacks. The attacker can use false identities for spoofing or in getting the information from the caller in order to steal the information. These are used for a variety of misuses and incidents related to fraud usage of the data. When we move on to history we can find that in past decade most of the people in the United States were affected by this spoofing attacks. It has been done by the group of attackers which led to the loss of up to 15 million dollars approximately. Caller ID spoofing is also a process used for swatting, which is used to threaten the innocent and gain the information which is an attempt to pretend an emergency service with fake reporting of an incident. These are a few real-time examples that had occurred using these spoofing techniques by attackers. It had made into law because attackers have become huge in number where they try to steal money and a lot of data which should be secured from innocents. Due to this reason, the government has passed some laws to get rid of this problem.

This process of spoofing caller ID is possible because caller IDs are transmitted in plain text with no authentication mechanisms involved in it. When a call is routed between different carriers, the sender's carrier will simply accept the caller ID from the sender and is claimed by a caller's carrier. Given the lack of authenticating the caller ID between carriers, caller IDs could be truthful if: - the mobile service providers do not operate caller IDs, the telephone set-up is precise, and no stalkers could tap into the set-up to create an indiscriminate caller ID. Moreover, telephone carriers may not be able to solve the problem even if they can redesign the protocols with the latest technique. As the system used in a network, it can be a little bit complex. Caller detection can be done to find the attackers over a network when the attacker tries to steal the information in the form of packets. As in this project, we considered the computer we have to maintain secure computing. Some properties that are required for secure computing are Physical security, Prying eye protection, Anti-virus software, Access passwords, Software updates, keep secure backups. These are some of the properties which will the system not to get under the control of any attacker. Hence this is the introduction that is required to know about the past things of the project.

## 2. RELATED LITERATURE WORKS

A Proxy-based Collaboration System to Minimize Content

 

Download Time and Energy Consumption proposed by Insun Jang, Gwangwoo Park, Dongeun Suh, Sangheon Pack, and Gy¨orgyD´an, in the year 2016 where, the author introduces a proxy-based collaboration system where Wi-Fi Direct is used for the distributed MCC formation with chunk sharing and a C-Proxy takes over the scheduling and the managing for the MCC in a centralized manner with distribution of packets. Hence, formulated the scheduling cause at the C-Proxy as a multi-objective optimization problem to reduce the download content time and the energy consumption in an MCC by selecting the optimal packet size and sharing order. Thus transformed the multi-objective optimization problem into a MINLP problem with a single-objective, and proposed a heuristic algorithm, α-LSSO, with low computational complexity. Therefore this helps in the project to deliver the information of packets.

Minimizing Content Download Time in Mobile Collaborative Community is proposed by I. Jang, D. Suh, and S. Pack in June 2014 where it is formulated as an optimization problem to reduce the content download time by selecting the optimal chunk size and sharing order. The formulated MINLP problem is relaxed into the LP problem, and a heuristic algorithm with low computational complexity is considered. Simulation solutions demonstrate that the derived heuristic algorithm reaches near-optimal performance and can lower the content download time effectively when compared with the rest of the algorithms. Considering future work, advanced MCC services with node mobility and real-time multimedia streaming and design a network structure to provide support to such MCC services.

Fairness Resource Allocation in Blind Wireless Multimedia Communications proposed by L. Zhou, M. Chen, Y. Qian, and H.H. Chen, June 2013. Which explains that it attempts to make a step ahead to understand the fairness in blind multimedia communications. Initially, we characterized the trade-off between performance and fairness by providing a higher bound of the MOS loss incurred in using -fairness scheme. Then, we divide the– fairness problem into two sub-problems that describe the need of the users and the controller and designed a bidding game for the reconciliation between the two sub-problems. We will have a belief that, in a blind environment, the fairness parameter can be selected precisely and the -fairness resource allocation can be assumed efficiently.

Collaborative Content Fetching Using MAC Layer Multicast in Wireless Mobile Networks proposed by L. Tu and C. M. Huang in the year September 2010. It explains that current smart phones are provided with multiple interfaces such as GPRS or UMTS for wireless WAN links as well as Wi-Fi and/or blue-tooth for local networking and also various properties are provided. It is also possible that a number of mobile users keep close for a period of time browse and fetch the same content from the Internet. C5 makes a lot of new contributions over prior work: (i) a small scale P2SP framework of a hybrid mobile network which considers possible concurrent mobile Internet traffic to increase the utility of WWAN links (ii) support of MAC layer multicast in the community and a new community formation procedure with the multicast rate estimation. Thus it can help to increase user experiences for mobile Internet subscribers. This paper is considered because we are using the transfer of information between to users.

Ivisher: real-time detection of caller id spoofing proposed by J. Song, H. Kim, and A. Gkelias in the year 2014. It explains about the Voice phishing (vishing) uses social engineering, based on people's trust in telephone services, to cheat people into divulging financial data or transferring money to a defrauder. In a vishing attack, a defrauder often modifies the telephone number that appears on the victim's phone to mislead the victim into believing that the phone call is coming from a reliable source since people normally judge a caller's correctness by the displayed phone number. We propose a system named iVisher for detecting a concealed incoming number in Session Initiation Protocol–based Voice-over-Internet Protocol initiated phone calls. Future works include envisioned to extend the system to detect other attacks (for example, spam messages) in VoIP networks. We will also consider how to integrate other existing systems with iVisher to reduce maintenance costs. Some drawbacks are, unfortunately, when many users encounter security warning messages, they often disregard the messages without caution. This paper provides the information in letting us know the attackers of different types which will help to overcome.

## 3. SYSTEM ANALYSIS

### 3.1 Existing system

- Existing IP trace-back approaches can be classified into five main categories: packet marking, ICMP traceback, logging on the router, link testing, overlay, and hybrid tracing.
- Packet marking methods require routers modify the header of the packet to contain the information of the router and forwarding decision.
- Different from packet marking methods, ICMP traceback generates addition ICMP messages to a collector or the destination.
- Attacking path can be reconstructed from the log on the router when the router makes a record on the packets forwarded.
- Link testing is an approach which determines the upstream of attacking traffic hop-by-hop while the attack is in progress.
- Centre-track proposes offloading the suspect traffic from edge routers to special tracking routers through an overlay network.

#### 3.1.1 Disadvantages of the existing system

- The cost to adopt a traceback mechanism in the routing system.
- Existing traceback mechanisms are either not widely supported by current commodity routers,
- The second one is the difficulty to make Internet service
- The reallocations of invaders still remain a mystery.

### 3.2 Proposed system

- We propose an innovative solution, named Passive IP Trace-back (PIT), to overcome the challenges in deployment.
- Routers may fail to forward an IP spoofing packet due to various reasons, e.g., TTL exceeding.
- In such cases, the routers may generate an ICMP error message (named path back-scatter) and send the message to the spoofed source address. This is due to the routers can be close to the attacker, the path back-scatter details may potentially reveal the locations of the attacker.
- PIT exploits these path back-scatter messages to find the location of the attacker. By knowing the physical location of the attacker, the victim can pursue help from the resultant ISP to filter out the attacking packets or take other revenge.
- PIT is especially useful for the victims in reflection based spoofing attacks, e.g., DNS amplification attacks. The victims can catch the physical location of the attacker directly from the attacking traffic history.

 

### 3.2.1 Advantages of the proposed system

- PIT messages are valuable to help understand spoofing activities.
- PIT also possible in large scale networks.
- Denial of Services (DoS), path back-scatter messages, which are sent by intermediate devices rather than the targets, have not been used in traceback.
- A practical and effective IP trace-back solution based on path back-scatter messages,

### 3.3 System architecture

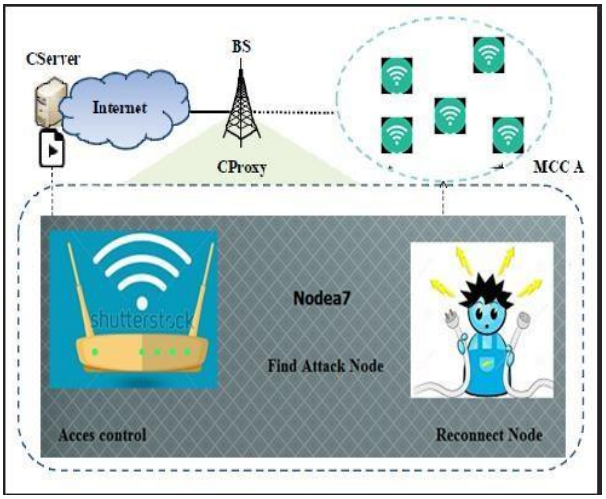


**Fig. 1: System architecture**

### 3.4 Passive IP Trace-back

The trace-back method that is used to know the physical locations of the invader which can be used in a network. PIT evades the distribution difficulties of IP trace-back technique. This considers Internal Control Message Protocol error messages triggered by spoofing traffic and track the invader based on public information that is available. PIT can be used to find invaders without any arrangement requirement. It can be used in this technique of detection of IP caller detection whereas it takes the IP address of the caller who uses a technique of VoIP and call the caller where using this PIT we can go through the previous and future records of the attacker by using MAC and IP address together where we get a confirmation that the attacker is trying to use a spoofing technique in order to grab the information from the user. With this PIT technique used in this project can be used to confirm the attacker by tracing back into previous and future records of the attacker and can the get the physical location of the attacker.

## 4. IMPLEMENTATION OF THE PROPOSED SYSTEM

This section elaborates real time experiments conducted using the proposed system. The total implementation process of this paper is divided into various modules. They are:

- Network topology construction
- Path Selection
- Packet Sending
- Packet Marking and Logging
- Path Reconstruction
- Attacker
- Authentication

### 4.1 Module description

**4.1.1 Network topology construction:** A Network topology consists of the number of routers that are connected with local area networks. A router can either receive data from the neighbour router or from the local area network. An end router receives packets of information from its neighbouring network. A core router receives packets from other routers. The number of routers connected to an individual router is known as the degree of a router. This degree is calculated and stored in a table for further reference. The Upstream boundaries of each router also have to be searched and stored in the interface table.

**4.1.2 Path selection:** The path is explained to be the way in which the selected packet of information or file has to be sent from the source user to the destination user. The Upstream boundaries of each router have to be found and it is stored in the interface table. With the help of that interface table, the desired path between the designated source and destination can be created.

**4.1.3 Packet sending:** Packet sending mainly explains about the transforming of a packet of information or file from a source user to the destination user. The packet is sent along the desired path from the source network to the destination network. The destination network receives the packet of information and checks whether it has been sent along the desired path or not.

**4.1.4 Packet marking and logging:** Packet marking is the phase where it explains mainly about the efficient Packet Marking algorithm where it is applied at each and every router along the desired path. It calculates the P-mark significance and stores in the hash table. If the P- mark is not more than the capacity of the router, then it is sent to the next router. Else it refers to the hash table and again applies the same marking algorithm.

**4.1.5 Path reconstruction:** Once the Packet reaches the destination user after applying the Algorithm, hence it checks whether it has sent from the correct upstream boundaries. If any of the attacks that is done by an attacker is found, then it requests for the Path reconstruction. It is the process of finding the new path or another specific way for the same source and the destination in which an attack can be made which can be used for transferring packets of information.

**4.1.6 Attacker:** Routing attacks can manipulate the route discovery and topology generation mechanisms of routing rules. An attacker advertises routes with hop-counts higher or lower than original routes. It could be used to attract traffic to malicious nodes to the benefit of the attacker. Malicious activity may result in the adoption of data, reducing of packets and modification of packets. All such results weaken the networks ability to guarantee safe, private and reliable communication between the users. Unsecured proactive routing protocols exhibit susceptibility to packet replay and manipulation. The protection that these protocols offer is aimed at the protection of network routing services. These protocols do not protect data sent over the secured routes.

**4.1.7 Authentication:** Authentication confirms the identity of communicating nodes. In a closed network, participation is restricted to authorized nodes, and communication is encrypted to prevent third-party comprehension of the contents of network communication. Authentication is required to allow new nodes to join and be seen as legitimate by existing network members. If an incoming packet's signature is unreadable, the packet is discarded as being unauthentic. This is a point-to-point process and does not provide source authentication. To prevent replay attacks, SOLSR uses timestamped packets. If a time-stamp is seen twice by a legitimate node, the packet will

 

be discarded. Authentication provides a means by which a node may be identified as trustworthy. By using documentation to confirm that they share a trusted authority, two nodes may authenticate one- another based on their shared Trusted Authority.

### 4.2 Data Flow Diagram

#### 4.2.1 Normal Mode

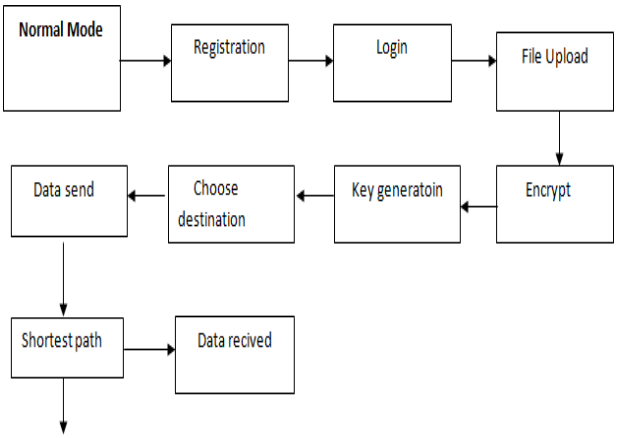


**Fig. 2: Normal Mode**

#### 4.2.2 Attack mode

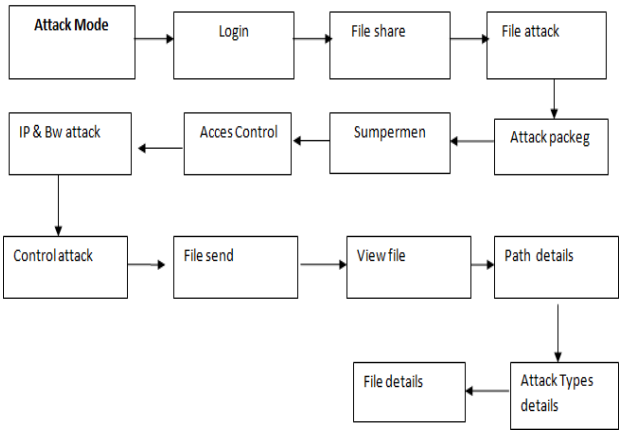


**Fig. 3: Attack mode**

## 5. RESULTS

### 5.1 Registration

The Initial process in order to go into and work with the project. It includes various details like username, password, email id, mobile number. After entering the details we have to submit where these details are stored in SQL.

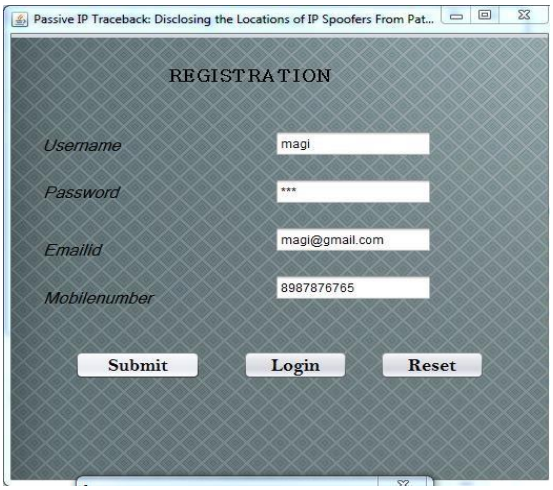


**Fig. 4: Registration**

Secondly, after entering the registration details, we should enter the IP address and Mac address manually. After entering details manually submit then and they will be stored.

### 5.2 Login

The user can log in with the details that happened while the registration process. Thereby becoming an authenticating user.

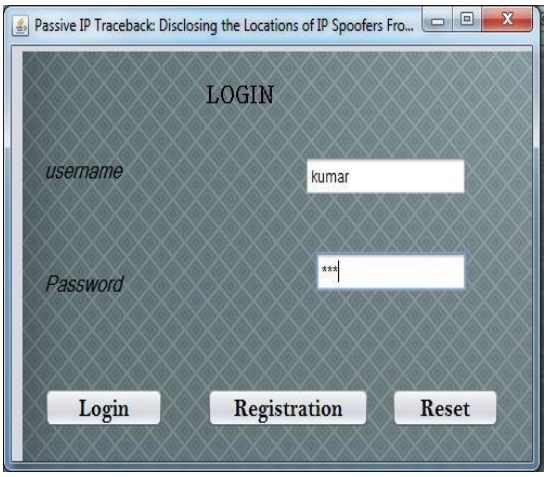


**Fig. 5: Login**

### 5.3 Sending a file

A file of information should be selected for sending it to the end-user. Thereby encrypting takes where asymmetric is generated and then by clicking the send option the file is sent to the receiver.

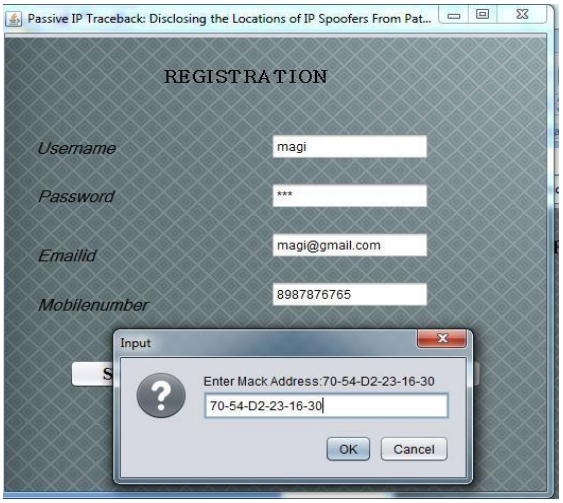


**Fig. 6 (a): Sending a file**

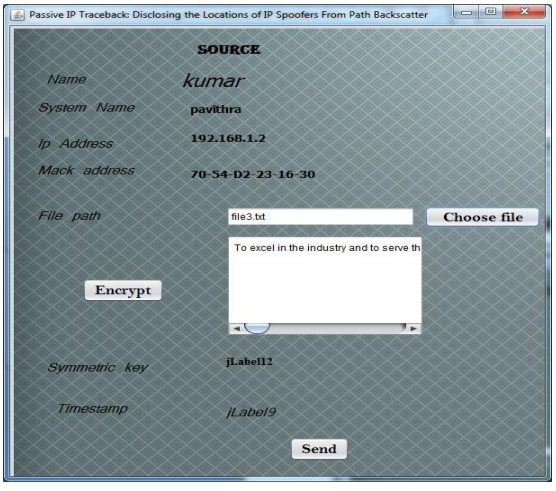


**Fig. 6 (b): Sending a file**

 

### 5.4 Encrypting the file

It is a process of changing the original data into a set of alphabets chosen randomly. This is done because to provide security to the data that needs to transform from the sender to the receiver.

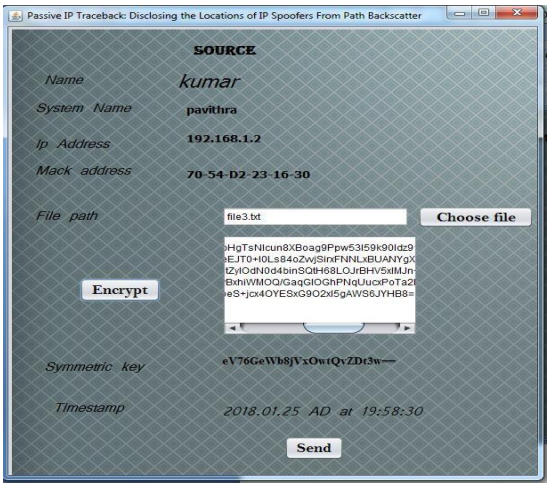


**Fig. 7: Encrypting the file**

### 5.5 Data sent to the user

By choosing the receiver and sending the information of data it chooses the shortest path across all the nodes and finally the data is sent by the user to the receiver.

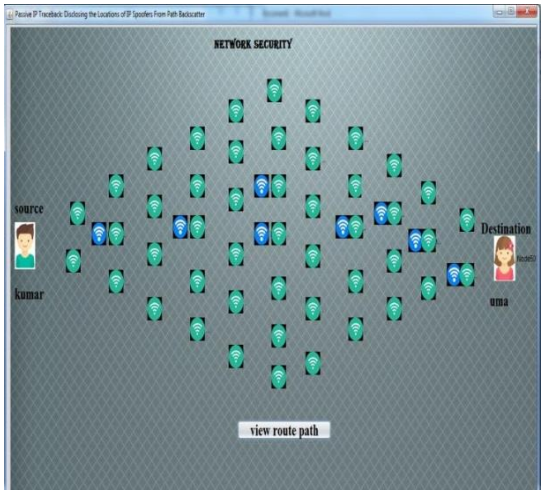


**Fig. 8: Data sent to the user**

**Case 2:**

### 5.6 Attacking a file

Here is where the attacker is involved where IP address is given by the attacker which will change its location continuously by using the VPN method. This is called IP attack+


**Fig. 9: Attacking a file**

### 5.7 Node has been attacked

Here we have to enter all the details like choosing the node choosing the packet and thus the node will be attacked.

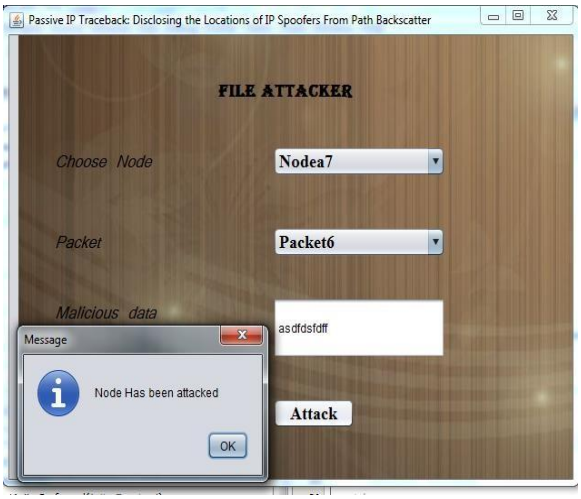


**Fig. 10: Node has been attacked**

## 6. BACKGROUND

Three categories of telephone carriers are in service Public Switched Telephone Network (PSTN), cellular networks, and Voice over Internet Protocol (VoIP) providers. In all these telephone networks, creating a phone call typically involves two types of channels: an end-to-end control channel for signaling, and an end-to-end voice channel for transmitting voice data. In accumulation, all telephone carriers support caller ID which works as follows. When a caller dials a number, the carrier first authenticates the caller, and then generates or looks up the associated caller ID. Finally, the caller ID is forwarded to the sender, possibly from one carrier to another. In the following, we discuss the popular caller ID standards used within each type of carrier and between different carriers with the goal of understanding the feasibility of introducing spoofed caller IDs.

## 7. CONCLUSION

In this article, we investigated caller ID spoofing attacks and identified that it is the network interconnection protocols that make caller ID spoofing possible. There is no evidence that telephone carriers will change their networks to support caller ID verification. Thus, we seek an end-to-end solution to detect a spoofed caller ID. Although the end-to-end delay for completing a verification takes a few seconds, such delay can be hidden when a verification is performed in parallel to the voice call. Moreover, PIT technique is used in order to use the traceback mechanism where we can trace-back into the previous and future records of the spoofer by using MAC and IP address. Hence this software helps the customer to find the spoofers that are trying to attack in order to grab the information for many purposes like stealing money fraud detections etc. Thus PIT is used as a traceback technique in order to detect the caller ID spoofing attacks

## 8. REFERENCES

[1] Hossen Mustafa, Member, IEEE, Wenyuan Xu, Member, IEEE Ahmad-Reza Sadeghi, Member, IEEE and Steffen Schulz. Year: 2014.

[2] B.Schneier, Caller ID Spoofing, http://www.schneier .com/blog/archives/2006/03/caller_id_spoof.html.

[3] ABCNews, Caller ID Scam Solicits Personal Info, Money. abcnews.go.com/GMA/Consumer/story?id=3305916, 2007.

 

[4] D. Cuellar, Pranksters Terrorize Delco Family in "swatting" Call. WPVI-TV, Philadelphia, PA, 2010.
[5] Rep. Elliot L. Engel, Rep. Engel Anti-Spoofing Bill Passes House, http://engel.house.gov/latest-news1/rep-engel-antispoofing-bill-passes-house.
[6] U. Congress, Truth in Caller ID Act of 2009, www.gpo.gov.
[7] X-Lite, www.counterpath.com/x-lite.html.
[8] Caller ID Faker, Caller ID Faker-Fake a Call! www.calleridfaker.com.
[9] TrustID, Automated Caller Authentication, www.trustid.com.
[10] D. Livengood, J. Lin, and C. Vaishnav, Public Switched Telephone Networks: A Network Analysis of Emerging Networks, ocw.mit.edu, 2006.
[11] Bell Communication Research, Bellcore Technical Specification,www.morehouse.org/hin/blckcrwl/telcom/callerid.txt, 1984
[12] Qualcomm White paper Ericson.Year:2014.
[13] J. Song, H. Kim and A. Gkelias. Year: 2014.
[14] J. H. Chang Year: 2012
[15] Narongsak Sukma, Roongroj ChokngamWong, Year: 2012

 