Phishing Text Tracking with Passive IP Traceback in Android Environment

M.Nirmala[1], Pavithra K[2],
[1]*Assistant Professor, Department of Computer Applications, Hindusthan College of Engineering and Technology, Coimbatore*
[2]*MCA Student, Department of Computer Applications, Hindusthan College of Engineering and Technology, Coimbatore*

Abstract: In order to hide their true locations while sending threatening or spam messages, attackers are known to employ forged source IP addresses, according to network security systems. A variety of IP trace back procedures have been suggested to identify the spoofers. However, there hasn't been a widely used IP trace back solution, at least not at the Internet level, due to deployment difficulties. Because of this, the mist surrounding the sites of spoofers has never cleared till now. This study suggests passive IP traceback (PIT), which avoids IP traceback solutions' implementation issues. PIT analyses path backscatter messages sent by the Internet Control Message Protocol that are caused by spoofing traffic and identifies the spoofers using publicly accessible data. PIT can locate the spoofers in this manner without the need for deployment. This study displays the procedures and efficiency of PIT and shows the collected positions of spoofers through applying PIT on the path backscatter data set. It also illustrates the causes, collection, and statistical results on path backscatter. These findings may provide more light on IP spoofing, which has long been studied but never fully comprehended. PIT may be the most effective method for tracing spoofers prior to the actual deployment of an Internet-level traceback system, despite the fact that it cannot detect all spoofing attempts. This conceptual approach outlines how passive IP traceback can be integrated into an Android environment for enhancing phishing text tracking. However, implementing such a solution would require careful consideration of technical feasibility, performance constraints, and compliance with platform-specific guidelines and regulations.

Keywords- Tracking messages, IP Spoofer, Source finder, Passive IP Trace back, Spam.

I. INTRODUCTION

IP spoofing, in which attackers launch attacks using forged source IP addresses, has been identified as a significant Internet security issue. By utilising addresses that are allocated to others or not assigned at all, attackers can avoid revealing their true locations, enhance the effectiveness of their attacks, or conduct reflection-based attacks. A number of infamous attacks, such as SYN flooding, SMURF, and DNS amplification, rely on IP hijacking. It is reported that a DNS amplification attack severely degraded the service of a top-level domain (TLD) name server. Despite the common belief that DoS attacks originate from botnets and that spoofing is no longer significant, the report of ARBOUR on the NANOG 50th meeting indicates that spoofing is still significant in observed DoS attacks. According to the backscatter messages captured by the UCSD Network Telescopes, deceptive activities are still observed frequently. It is crucial to identify the origins of IP masquerade traffic. As long as the actual locations of spoofers are not revealed, they will continue to launch attacks. Even by merely approaching the spoofers, for instance, by determining the ASes or networks in which they reside, attackers can be confined to a smaller area, and filters can be placed closer to the attacker before the attack traffic is aggregated. Last but not least, identifying the origins of deceptive traffic can aid in the development of a reputation system for ASes, which would be useful for encouraging the respective ISPs to verify IP source addresses.

II. LITERATURE SURVEY

S.M. Bellovin., 2011 [1] The TCP/IP protocol suite was developed by the Department of Defense, but it has serious security flaws. This paper describea a variety of attacks based on these flaws, including sequence number spoofing, routing attacks, source address spoofing, and authentication attacks and it presents defenses against these attacks, and conclude with broad-spectrum defenses such as encryption.

Stephen M. Specht., et al, 2004 [2] propose taxonomies to characterize the scope of DDoS attacks, the characteristics of software attack tools, and the countermeasures available. These axonomies illustrate similarities and patterns in different DDoS attacks and tools, helping to develop more generalized solutions.

Alex C. Snoeren., et al, 2001 [3] present a hash-based technique for IP trace back that generates audit trails and can trace the origin of a single IP packet. It is effective, space-efficient, and implementable in current or next-generation routing hardware. Analytic and simulation results show its effectiveness.

Geoffrey M. Voelker., et al, 2009 [4], this paper examines the prevalence of denial-of-service attacks in the Internet. It uses a new technique called "backscatter analysis" to estimate the number, duration and focus of attacks. During three week-long datasets, 12,000 attacks were observed against 5,000 distinct targets, ranging from well-known ecommerce companies to small foreign ISPs and dial-up connections. This is the only publically available data quantifying denial-of-service activity in the Internet.

Dawn Xiaodong Song., et al, 2001 [5] present two new schemes, the Advanced Marking Scheme and the Authenticated Marking Scheme, which allow the victim to trace back the approximate origin of spoofed IP packets. These techniques feature low network and router overhead and support incremental deployment. They have higher precision and lower false positive rate than previous work, and the Authenticated Marking Scheme provides efficient authentication of routers' markings.

Qian Cui., et al, 2017 [6] have monitored 19,066 phishing attacks over a period of ten months and found that over 90% of these attacks were actually replicas or variations of other attacks in the database. This provides several opportunities and insights for the fight against phishing: quickly and efficiently detecting replicas is an effective prevention tool, current prevention techniques are ineffective and need to be overhauled, and a new perspective into the modus operandi of attackers suggests that a small group of attackers could be behind a large part of the current attacks. Taking down this group could potentially have a large impact on the phishing attacks observed today.

N.Srilakshmi., et al, 2013 [7], IP traceback is a major challenge to the security of the Internet, with many techniques proposed. Source IP spoofing attacks are critical issues, and there has been active research on IP traceback technologies. However, the traceback from an end victim host to an end spoofing host has never yet been achieved due to insufficient probes installed on each routing path. Recently, a number of technologies have been developed to detect and prevent DDoS traffic, but it is difficult to distinguish normal traffic from DDoS traffic due to network features.

K.Munivara Prasad., et al, 2012 [8] proposed an information-theoretic frame work to model the flooding attack of DDoS against ITM monitors. A novel traceback method for DDoS using Honeypots is proposed to trace the attack sources and punish the perpetrators. This method is more efficient than commonly used packet marking techniques.

Bhavani Yerram., et al, 2010 [9] Denial-of-service (DoS) attacks pose an increasing threat to today's Internet. One major difficulty to defend against Distributed Denial-of-service attack is that attackers often use fake, or spoofed IP addresses as the IP source address. Probabilistic packet marking algorithm (PPM), allows the victim to trace back the appropriate origin of spoofed IP source address to disguise the true origin. In this paper we propose a technique that efficiently encodes the packets than the Savage probabilistic packet marking algorithm and reconstruction of the attack graph. This enhances the reliability of the probabilistic packet marking algorithm.

Minho Sung., et al, 2003 [10] present a novel technique that can effectively filter out the majority of Distributed Denial of Service (DDoS) traffic, improving the overall throughput of legitimate traffic. The proposed scheme leverages on and generalizes the IP traceback schemes to obtain the information concerning whether a network edge is on the attacking path of an attacker ("infected") or not ("clean"). By preferentially filtering out packets that are inscribed with the marks of "infected" edges, the proposed technique removes most of the DDoS traffic while affecting legitimate traffic only slightly. Simulation results based on real-world network topologies all demonstrate that the proposed technique can improve the throughput of legitimate traffic by three to seven times during DDoS attacks.

III.SYSTEM ANALYSIS AND SPECIFICATION

EXISTING SYSTEM

The five primary types of IP trackback techniques used in the current system are packet marking, ICMP trackback, router logging, link testing, overlay, and hybrid tracing. Current commodity routers either do not support existing trace back technologies well or will add a significant amount of overhead to router production, especially in high-performance networks. The distributed Meta management system is used. The disadvantages are data should be carefully maintained and not efficient if there exist heavy interaction between branches.

PROPOSED SYSTEM

In the proposed system, users and applications utilize passive IP trace back (PIT), which circumvents the deployment issues associated with IP trace back methods. PIT analyses Internet Control Message Protocol path backscatter messages caused by impersonating traffic and identifies the spoofers using publicly accessible data. We propose the Passive IP Traceback (PIT) method, which monitors spoofers using path backscatter messages and publicly available data. According to network security systems, in order to conceal their true locations when transmitting threatening or spam messages, attackers are known to forge source IP addresses. The techniques are very efficient even if there exists heavy interaction between branches and the data can be stored normally and efficiently.

SYSTEM SPECIFICATIONS

HARDWARE SPECIFICATION

PROCESSOR	:Intel Core i5
RAM	:8GB
HARD DISK DRIVE	:1TB

SOFTWARE SPECIFICATION

Back End	:SQLITE
Operating System	:Windows 07
IDE	:Eclipse, Android Studio
Documentation	:Microsoft Word

IP spoofing is a technique used by attackers to manipulate the source IP address of network packets. In normal network communication, the source IP address indicates the origin of the packet, allowing the recipient to send a response back to the correct location. However, with IP spoofing, the attacker forges or "spoofs" the source IP address to make it appear as if the packet is coming from a different source than its actual origin. The primary goal of IP spoofing is to deceive or hide the true location of the attacker.

III. RESEARCH METHODOLOGY

IP Spoofing technique can be employed for various purposes

- Enhancing Attack Effectiveness
- Avoiding Detection
- Reflection-Based Attacks
- Impersonation

IP spoofing is indeed a significant security concern on the Internet. Attackers utilize forged source IP addresses to hide their true locations and enhance the effectiveness of their attacks. It enhances the effectiveness of attacks and enable reflection-based attacks. Various IP spoofing attacks are SYN flooding, SMURF, and DNS amplification. Emphasize the importance of identifying the origins of IP masquerade traffic to effectively combat spoofing attacks. The actual locations of the spoofers need to be identified so that the launching of next possible attacks can be stopped.

Various attacks that commonly uses IP spoofing are

SYN Flooding: A SYN flooding attack sends a flood of TCP connection requests with spoofed source IP addresses to a target server, but the responses never reach valid destinations, leading to a backlog of half-open connections and denial of service.

SMURF: Attack sends ICMP echo request packets to IP broadcast addresses, spoofing the source IP address to be the victim's, causing multiple hosts to respond simultaneously, leading to a denial-of-service condition.

DNS amplification: The attacker sends DNS queries with spoofed source IP addresses to open DNS resolvers, which are larger in size than the original queries. This can cause a significant impact on the victim's network bandwidth and potentially lead to a service disruption.

Botnets: Botnets use IP spoofing techniques to hide the source IP addresses of their C&C communications and malicious traffic, making it difficult to trace the true origin of an attack.

Phishing Attacks: Phishing attacks use spoofed IP addresses to deceive the recipient into believing the communication is legitimate, increasing the likelihood of successful attempts.

Security measures such as ingress and egress filtering are essential to protect against IP spoofing.

Need for Identifying the Origins of Spoofers

- Identifying the origins of IP masquerade traffic is essential for Internet security, as it helps to prevent deceptive traffic.
- Identifying the origins of spoofers or attackers allows security teams to focus their efforts on specific geographic areas, networks, or ASes associated with the attackers, reducing the impact of attacks and protecting potential targets.
- Accurate identification of origins of deceptive traffic enables more efficient incident response, allowing security teams to collaborate with relevant entities to investigate and take appropriate actions against attackers, minimizing potential damage.
- Revealing the origins of deceptive traffic helps to establish a reputation system for ASes and networks, encouraging ISPs and network operators to implement stronger security measures and take responsibility for their networks' activities. This can improve overall network security.
- Identifying the origins of deceptive traffic can help security professionals develop better countermeasures, update security policies, and enhance detection mechanisms to stay ahead of evolving threats, strengthen network defenses, and prevent future attacks.
- Researchers can gain insights into the techniques, motivations, and strategies of attackers by investigating and analyzing spoofing incidents, which can help develop improved security solutions and protocols to mitigate spoofing attacks.

Passive IP Traceback (PIT)

The algorithm applied in this work is Passive IT Traceback (PIT). Passive IP Traceback (PIT) is a method for identifying the source or origin of IP masquerade attacks without requiring the active participation or cooperation of network elements along the attack path. PIT uses passive analysis of network traffic to trace back intruders, as opposed to traditional active IP traceback methods that involve modifying network infrastructure or embedding additional information in packets. Passive IP Traceback (PIT) has the following characteristics and procedures to be followed which is depicted in Figure 1: PIT Flowchart.

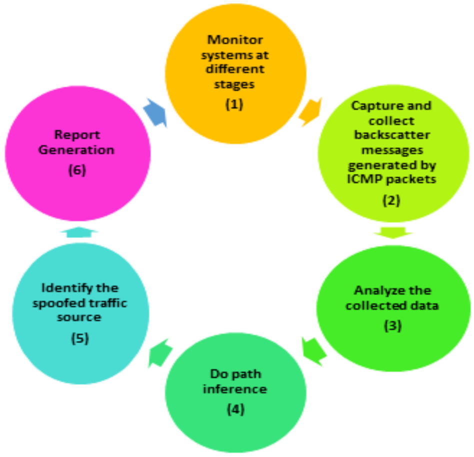

Monitor systems at different stages
(1)
Capture and collect backscatter messages generated by ICMP packets
(2)
Analyze the collected data
(3)
Do path inference
(4)
Identify the spoofed traffic source
(5)
Report Generation
(6)

Figure 1: PIT Flowchart

- Monitor the systems from Various Locations.
- Capture and gather backscatter messages produced by ICMP packets in response to spoofed traffic.
- Analyze the gathered data:
  - ❖ Extract IP addresses, timestamps, and metadata from backscatter communications.
  - ❖ Store the data for analysis purposes.
- Perform path deduction:
  - ❖ Determine the order in which backscatter messages were received by analyzing their timestamps.
  - ❖ Determine the IP addresses or network segments shared by multiple backscatter messages from various monitoring points.
  - ❖ Reconstruct the approximate network path followed by the spoofed traffic.
- Fake source identification of traffic:
  - ❖ Analyze the inferred paths and determine the most probable sources of spoofed traffic.
  - ❖ Correlate the backscatter communications to more precisely pinpoint the sources.
- Analysis and report generation:
  - ❖ Analyze the identified sources for commonalities, trends, or patterns.
  - ❖ Generate reports or alerts to inform incident response teams or other relevant parties.
  - ❖ Utilize the results to inform targeted mitigation measures or investigations.

IV. EXPERIMENTAL SETUP

The experimental process is carried out using Android studio and consists of the following operations to be performed. If the user is a new user who intends to utilize the service, he must first register by giving the required information. The user must log into the programme after completing the sign-up procedure successfully by entering their username and exact password. If the login is successful, the user will be taken to the main page; otherwise, they will remain on the login page. The user must provide the exact username and password that they supplied at registration is shown in Figure 2 : User Registration Page

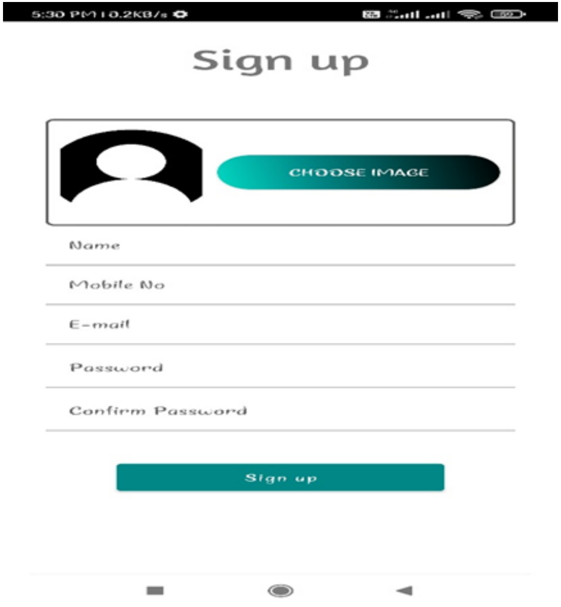


Figure 2 : User Registration Page

Many of the intrusions described above succeed only because the target host uses the IP source address for authentication, and assumes it to be genuine. Unfortunately, there are sufficiently many ways to spoof this address that such techniques are all but worthless. Put another way, source address authentication is the equivalent of a file cabinet secured with an S100 lock; it may reduce the temptation level for more-or-less honest passers-by, but will do little or nothing to deter anyone even slightly serious about gaining entry. The login entry process of credentials are depicted in Figure 3 : Login Authentication.

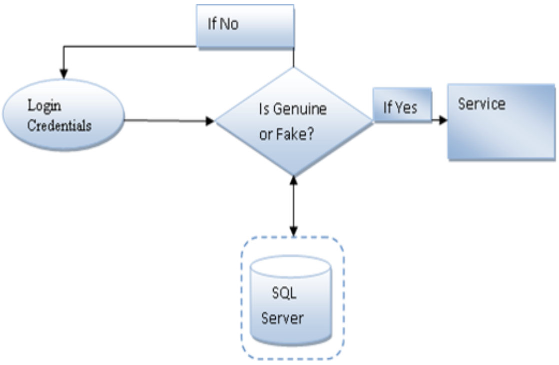


Figure 3 : Login Authentication

Customers who intend to utilise the service must first register by giving the required information. The consumer must provide their consumer ID and PIN number to get into the application when the process has been successfully completed. In order to go to the main page after successful login, the administrator must enter the identical username and password that were given at the time of registration. Otherwise, the user will be left on the login page is shown in the Figure 4 : User Process and its corresponding screenshot is shown in Figure 5 : Admin and User Signup

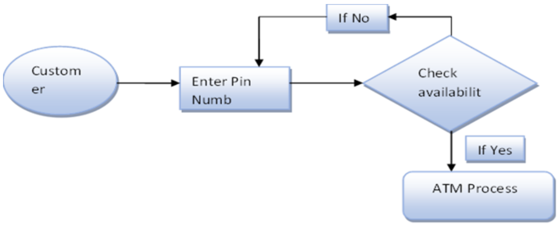


Figure 4 : User Process

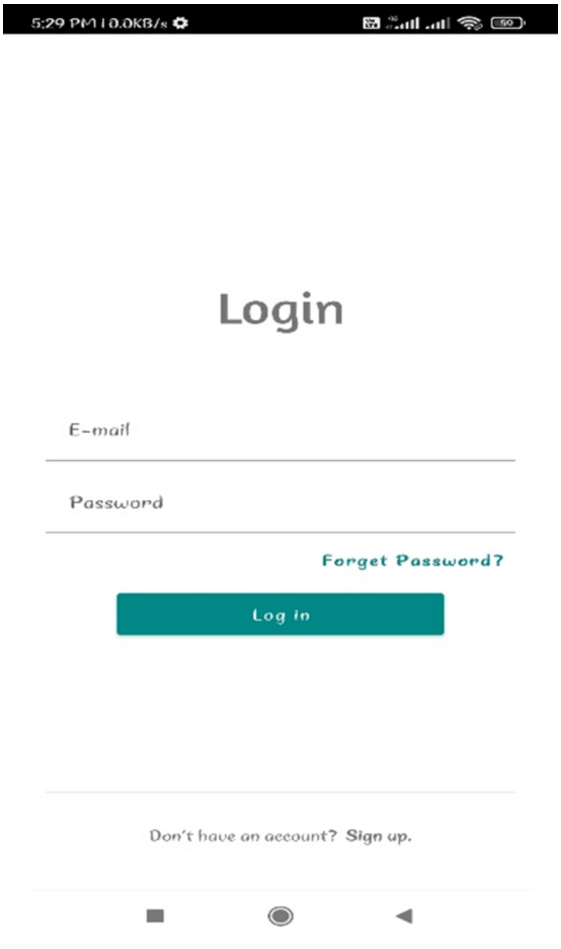


Figure 5 : Admin and User Signup

In accordance with this module, an IP spoofer is able to locate their data from that storage place and obtain it from the IP address. Internet Protocol (IP) spoofing is a type of malicious attack where the threat actor hides the true source of IP packets to make it difficult to know where they came from. The attacker creates packets, changing the source IP address to impersonate a different computer system, disguise the sender's identity or both. With IP spoofing, intruder sends message to a computer system with an IP address indicating message is coming from a different IP address than its actually coming from. If intent is to gain unauthorized access, then Spoof IP address will be that of a system the target considers a trusted host is depicted in the Figure 6 : IP Spoofer Process.

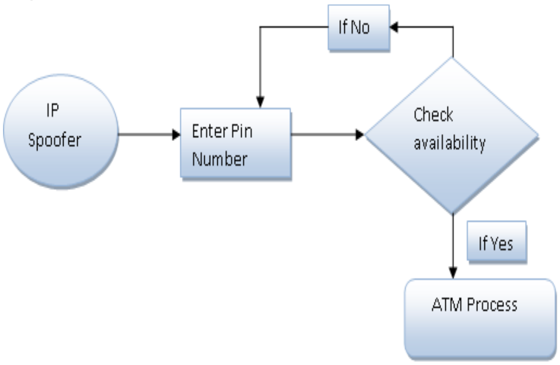


Figure 6 : IP Spoofer Process

The administrator homepage is shown in can locate data from that storage location and acquire customer information in accordance with this module. Verify the sender's email or phone number to make sure it comes from the correct place. Watch out for emails with a domain name that has been slightly altered or misspelt but otherwise appears to be from a reputable business or organisation. As an administrator, you can protect incoming mail against phishing and harmful software (malware). You can also choose what action to take based on the type of threat detected. The operations are depicted in the Figure 7 : Admin Process and the admin home page with spam, fake detection , malware detection and source finder details are depicted in Figure 8 : Admin Home

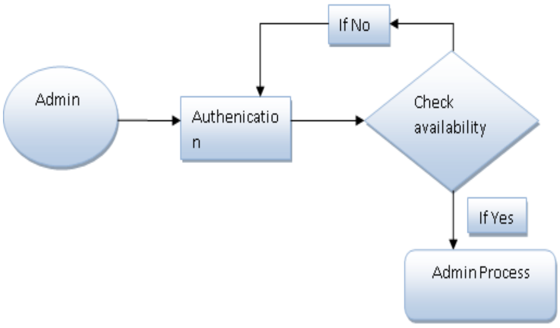


Figure 7 : Admin Process

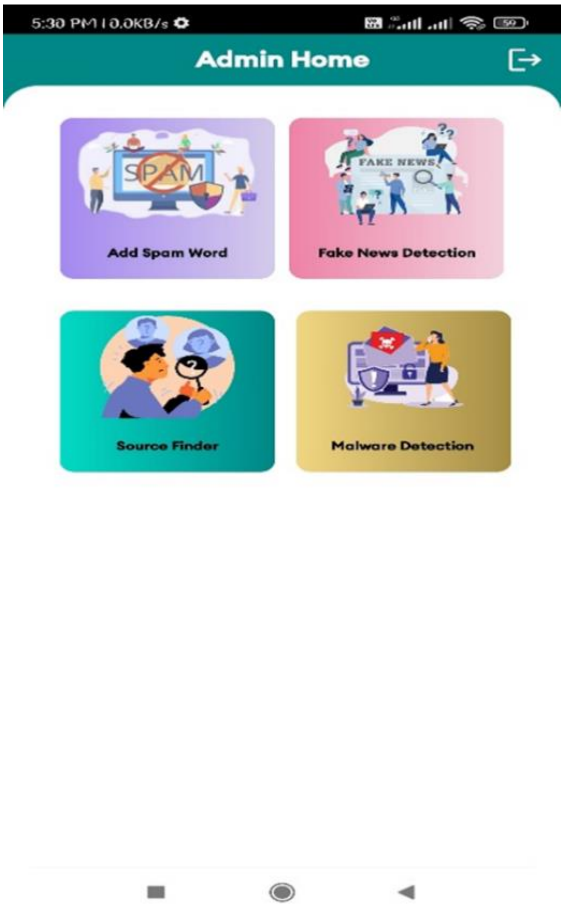
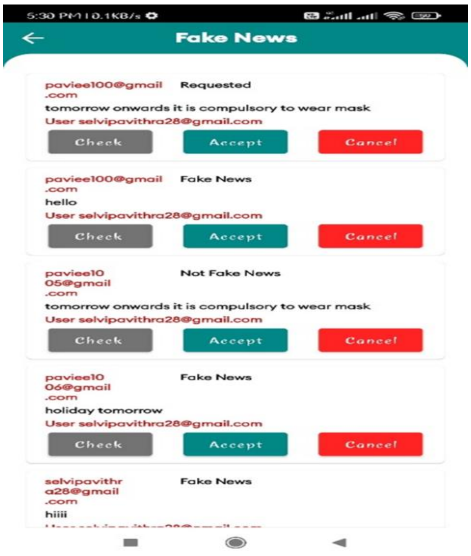


Figure 8 : Admin Home

PIT is utilised to perform IP trace back; it differs greatly from extant IP trace back mechanisms. PIT is influenced by various IP deception observation activities. Thus, the relevant product consists of two sections. The first section provides an overview of existing IP trace back mechanisms, while the second describes IP deception observation activities. IP Trace back is a DDoS detection technique that is used to trace the path of an IP packet back to its source in order to determine the true identity of the perpetrator and the path characteristics. IP monitoring serves primarily to identify an IP address whenever a device connects to a network or another device. A network or remote device that receives a connection request and lacks this information would be unable to communicate with the connecting device. IP monitoring serves primarily to identify an IP address whenever a device connects to a network or another device. A network or remote device that receives a connection request and lacks this information would be unable to communicate with the connecting device. The identification of fake news and spam messages are depicted in the Figure 9 : Fake News Detection and Figure 10 : Spam Messages



paviee100@gmail.com Requested
tomorrow onwards it is compulsory to wear mask
User selvipavithra28@gmail.com

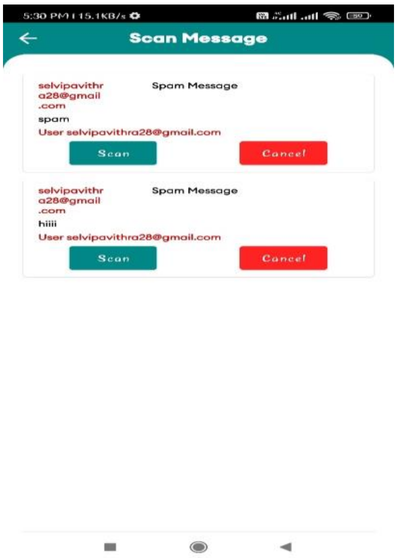
paviee100@gmail.com Fake News
hello
User selvipavithra28@gmail.com

paviee1005@gmail.com Not Fake News
tomorrow onwards it is compulsory to wear mask
User selvipavithra28@gmail.com

paviee1006@gmail.com Fake News
holiday tomorrow
User selvipavithra28@gmail.com

selvipavithra28@gmail.com Fake News
hiiii

Figure 9 : Fake News Detection

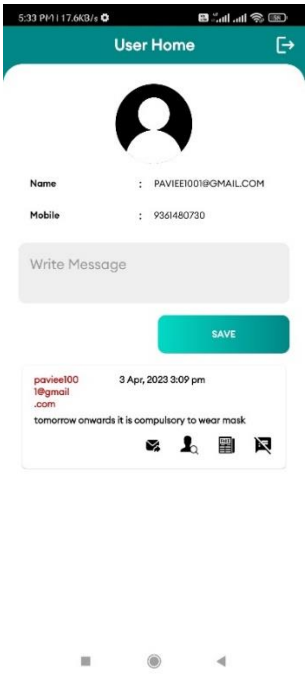


selvipavithra28@gmail.com Spam Message
spam
User selvipavithra28@gmail.com

selvipavithra28@gmail.com Spam Message
hiiii
User selvipavithra28@gmail.com

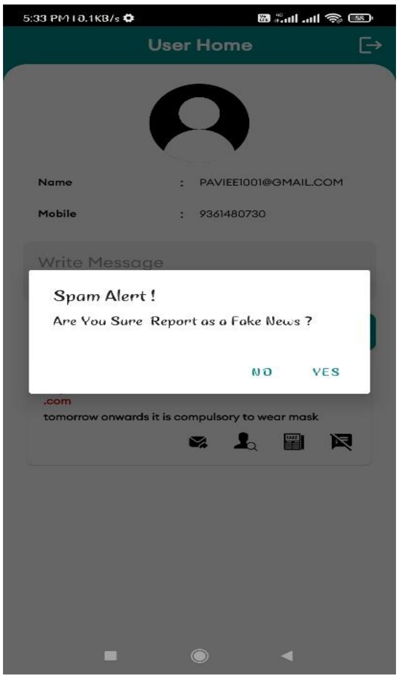
Figure 10 : Spam Messages

IP monitoring serves primarily to identify an IP address whenever a device connects to a network or another device. A network or remote device that receives a connection request and lacks this information would be unable to communicate with the connecting device. The user home page and the spam alert message to ensure that the message transformed is a spam alert is displayed in the Figure 11 : User Message Page and Figure 12 : Reporting as Fake News. The source finder from the origination of fake message is transformed is ip spoofed by Figure 8 : Spam Messages the algorithm and it is depicted in **Error! Reference source not found.**.

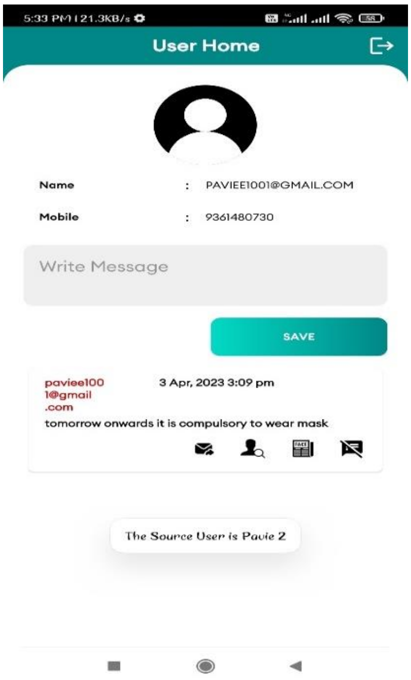


Name : PAVIEE1001@GMAIL.COM
Mobile : 9361480730
Write Message
paviee1001@gmail.com 3 Apr, 2023 3:09 pm
tomorrow onwards it is compulsory to wear mask

Figure 11 : User Message Page



Name : PAVIEE1001@GMAIL.COM
Mobile : 9361480730
Write Message
Spam Alert !
Are You Sure Report as a Fake News ?
.com
tomorrow onwards it is compulsory to wear mask



Name : PAVIEE1001@GMAIL.COM
Mobile : 9361480730
Write Message
paviee1001@gmail.com 3 Apr, 2023 3:09 pm
tomorrow onwards it is compulsory to wear mask
The Source User is Pavie 2

Figure 12 : Reporting as Fake News Figure 13 : Finding the Source User

V. SCOPE FOR FUTURE ENHANCEMENT

Passive IP Trace Back (PIT) is a system that monitors spoofers using path backscatter messages and publicly accessible data. We provide examples of path backscatter's causes, collection, and statistical findings. When the topology and routing are both known, when the routing is unknown, and when neither of them are known, we described how to apply PIT. We demonstrated two efficient PIT implementation techniques and demonstrated the correctness of each. We used simulation and deduction to show the PIT's effectiveness. By using PIT on the path backscatter dataset, we were able to display the spoofer's collected locations. These findings may provide more light on IP spoofing, which has long been studied but never fully comprehended.

VI. CONCLUSION

Based on an examination of the path backscatter messages, we attempt to clear the mist surrounding the locations of the spoofers. We suggested Passive IP Traceback (PIT) in this post, which keeps track of spoofers via path backscatter messages and publicly available data. We provide examples of path backscatter's causes, collection, and statistical findings. When the topology and routing are both known, when the routing is unknown, and when neither of them are known, we described how to apply PIT. We provided two efficient PIT application techniques and demonstrated the correctness of both. We used simulation and deduction to show the PIT's effectiveness. By using PIT on the path backscatter dataset, we were able to display the spoofers' collected locations. These findings may provide more light on IP spoofing, which has long been studied but never fully comprehended.

REFERENCE

[1] S.M. Bellovin, “Security Problems in the TCP/IP Protocol Suite”, Reprinted from Computer Communication Review, (Vol. 19, No. 2, pp. 32-48, April 1989).

[2] Stephen M. Specht, Ruby B. Lee, “Distributed Denial of Service: Taxonomies of Attacks, Tools, and Countermeasures, September 15-17, 2004

[3] Alex C. Snoeren, Craig Partridge, Luis A. Sanchez, Christine E. Jones, Fabrice Tchakountio, Stephen T. Kent, and W. Timothy Strayer, “Hash-Based IP Traceback”, SIGCOMM’01, August 27-31, 2001

[4] David Moore, Geoffrey M. Voelker and Stefan Savage, “Inferring Internet Denial-of-Service Activity”, 2000

[5] Dawn Xiaodong Song and Adrian Perrig, “Advanced and Authenticated Marking Schemes for IP Traceback”, IEEE INFOCOM 2001

[6] Qian Cui, Gregor V. Bochmann, “Tracking Phishing Attacks Over Time“, the 26th World Wide Web Conference (WWW2017), (April 2017).

[7] N.Srilakshmi, K.Rani, “An Improved IP Traceback Mechanism For Network Security”,: International Journal of Research in Engineering and Technology, (Volume: 02 Issue: 08 | Aug-2013)

[8] K.Munivara Prasad, A.Rama Mohan Reddy, V Jyothsna, “IP Traceback for Flooding attacks on Internet Threat Monitors (ITM) Using Honeypots”, International Journal of Network Security & Its Applications (IJNSA), (Vol.4, No.1, January 2012)

[9] Bhavani Yerram, Reddy P.Niranjan, “An Efficient IP Traceback Through Packet Marking Algorithm”, International Journal of Network Security & Its Applications (IJNSA), (Vol.2, No.3, July 2010)

[10] Minho Sung and Jun Xu, “IP Traceback-Based Intelligent Packet Filtering: A Novel Technique for Defending against Internet DDoS Attacks”, Ieee Transactions on Parallel And Distributed Systems, (vol. 14, no. 9, September 2003)