International Journal of Engineering Research and Technology. ISSN 0974-3154, Volume 13, Number 10 (2020), pp. 2736-2741
 https://dx.doi.org/10.37624/IJERT/13.10.2020.2736-2741

Detection of IP Spoofing Attack

Reem K. Alqurashi, Ohoud S. Al-harthi and Sabah M Alzahrani

Computer and Information Technology College, Taif University, Taif 26571, Saudi Arabia.

ORCID: 0000-0001-8508-0430 (Sabah Alzahrani)

Abstract

With the worldwide extensive custom of the Internet, additional and additional cyber-attacks are existence achieved. Numerous of these attacks exploit IP address spoofing. This paper designates IP spoofing attacks and the projected approaches presently obtainable to perceive or avoid them. IP spoofing-based flooding attacks are a thoughtful and uncluttered security problematic on the present Internet. Another strategy is proposed to separate spoofed IP point, called IP Spoofing Area Approach (ISDA). The reason behind this method is to hold suitable bits and launch made segments of Source IP addresses under flooding ambushes and adequately compose total stream plot identification for stream-based framework interference to convey the best interference acknowledgment approach. Our examination is arranged towards making a general structure, which incorporates building stream total plans for Stream based System Interruption Recognition Framework (FNIDS), recognizing IP address spoofing level and utilizing Fluffy rationale strategy naturally to initiate the most proper stream conglomeration conspire. At last, Our proposed structure application display is assessed against DDOS inundation assaults utilizing DARPA ninety eight data. The outcomes show an observable improvement in the wake of applying the IP address spoofing discovery calculations.

Keywords - DDoS attack, IP Spoofing, HCF, OS Fingerprinting.

1. INTRODUCTION

Internet access, in today ecosphere, cannister no lengthier be measured a product nonetheless somewhat a humanoid correct [1]. Numerous dangerous facilities comparable investment, e-commerce, social media, detachment education, inaccessible operation, penetrating, and online shopping are grounded on the

Cyberspace provision. Conferring to [2], these are additional than 2.4 billion Cyberspace operators by way of 30th June 2012 . Consequently, somewhat disturbance toward this provision stays measured difficult and canister consequence in extreme monetary wounded to numerous productions. Inappropriately, Internet was not considered with safety as a main apprehension then somewhat it was considered created on scalability. These allowable numerous attackers to adventure numerous of the enterprise faintness that stay characteristic to the conventions secondhand in today Cyberspace. A predominantly stimulating faintness in the conventions secondhand in today Cyberspace dishonesties in the IP Procedure. This faintness allowable invaders toward "spoof" (deception) the foundation IP discourse and therefore stand talented toward achieve numerous bouts such by way of skyjacking meetings, packet deceiving, disavowal of provision, progressive skimming methods, and dispersed bouts. By enterprise, the IP procedure prepares not proposal slightly procedure of verification of the basis IP discourse. Consequently, an aggressor cannister direct an IP package through a "spoofed" basis IP discourse. An aggressor cannister therefore advantage after this aptitude toward continue unidentified, toward presentation beleaguered bouts, then toward avoid about safety limitations that are grounded exclusively on authenticating the bases of IP discourses [3]. There're numerous differences of bouts that exploit IP Deceiving such by way of Non-Blind Deceiving, Shade Deceiving, gentleman in The Internal, Disavowal of Provision, and Distraction Examination. There are deuce famous approaches toward avoid IP deceiving: Discourse sifting and IP security. Additional approaches address detailed suitcases comparable the Comprehensive TTL

Safety Instrument [3]. This exertion was stimulated by the “Hop-Count Filtering (HCF) " method planned. [3] [4] toward perceive IP deceiving. Their procedure stays grounded arranged the impression that though an aggressor container parody the basis IP discourse, the aggressor can't takeoff the quantity of stages a sachet negotiates toward influence the terminus. Consequently, the procedure initial studies the IP to

Hop Amount (HC) planning and provisions the planning in an "IP2HC" bench. When a sachet reaches, it stands associated to the HC deposited aimed at this IP. Doubt the HC standards competition, formerly the container is genuine. Then, the package is rejected. The foremost forte of HCF method dishonesties in its straightforwardness. This paper intentions on suggesting of HCF method in instruction toward improve the accurateness of HCF through counting in IP2HC bench all legalized HCs realized in the knowledge point. This alteration augments the complete accurateness associated to the innovative HCF besides its dissimilarities [4]. And OS fingerprint is the nursing of an inward packet to regulate the OS the basis is consecutively on. It is commonly rummage-sale through system managers to recognize outmoded OS inside their network.[5]

2. IP SPOOFING IN DDOS ATTACK

DDoS offensive exist frequently considered by fooling of basis IP address to camouflage its distinctiveness to prohibit informal suggestion backbone to appreciate convinced provision

accumulated to a important host. The approaches secondhand to perceive tricked IP may be commonly confidential for example moreover inactive or dynamic[6].

The Spread Repudiation of Organization (DDoS) assault dependent on flooding represents an outrageous threat to the Internet's consistent quality. In a day by day DDoS strike, endless arranging has been gathered to submit pointless bundles to hold a casualty, or its association with the System. Regardless, seeing traffic at the degree of the bundle has end up being precarious as traffic on a quick system is the aftereffect of a significant level of conglomeration of different sources. Another pattern to demonstrate solid Web traffic at stream level has risen late. NetFlow[7], first implemented in Cisco switches, is the most commonly deployed stream estimation scheme today with regard to dependent traffic inquiry. Stan [8] introduced scalable NetFlow, which can be implemented via a programming upgrade that leads to various NetFlow vulnerabilities by slowly changing the exam rate to achieve heartfulness without giving up precision. There is an array of tools for stream-based estimation evolving in view of NetFlow. Cflowd is a tool built by CAIDA for stream checking [9]. It is actually used to dissect Cisco's NetFlow [7] improved technique of trade. In[10], Flow profiling that breaks down and offers descriptions of flow information submitted by Web Convention switches was introduced. Similarly, stream level calculations are commonly used to define vulnerability or to provide awareness of a system's traffic crossing. Many NIDSs dependent on Stream will detect oddity attacks. Bro [11] is an Recognition Tool for Unixbased System Interruption (IDS). Brother screens organize traffic and identify attempts at disruption by gazing at arranging traffic as opposed to trying to show times that are considered inconvenient. Be that as it may, they flop toward provide insights around the development road traffic blend for example they record lone the aggregate quantity of road traffic spread on the purposeful relation. In any event, the stream-established investigation also own some limitations at planning rapidity plus memory prerequisites when encountering massive tricked sources throughout DOS assault. The aggressor integrates an immense amount of malevolent spoofed sources in such an attack, which could overwhelm IDS recollections and CPU data, cripple IDS to track and recognize all sources. CISCO IOS NetFlow [7] offers an method to allow the client to set the size of the base veil for the Switch Based Full feature. There are various methodologies to prevent DDoS assaults: Separate Access, Switch-based, and Case-based (Serverbased). Entrance sifting, suggested by Farguson [12], is a prohibitive device that reduces IPaddressed traffic that does not coordinate a space begin linked with the input transfer. Park and Lee [13] suggested course-setup disseminated package separation, which relies on the course data to decide if a parcel received at a switch is correct for its source / goal addresses registered, to be sifted across spoofed IP parcels. Casualty-based sifting is important for safeguarding casualties from DDoS attacks, and requires only the data found in the IP header to distinguish packages. In any case, all the networks suggest in the text so faraway miss the target toward differentiate IP address deceiving from the space in which the aggressor establish. Somewhat, sifting based approaches may reduce the anguished side effect of DDoS assaults, but some actual traffic may eventually be obstructed by them. Right now, show a strategy for spoofing the IP. Our research should concentrate on developing a general Stream Complete Administration Method (FAMA), which inevitably manufactures plots of stream conglomeration, perceives and extends the usefulness and efficiency of preventing spoofed flooding attack. We have applied a fluffy justification strategy to pick an optimal stream conglomeration program for increasing the recognition rate. The fuzzy justification module would obviously implement the most suitable stream set conspire for stream-based network disruption identification mechanism and flexible firewall, rely on the tricking point, the distinguished real highlights plus the malignancy of streams in a particular interim. Using DARPA 98 details, this use of the spoofing level recognition technique in FNIDS was assessed. The paper is constructed as follows: Section 2 essentially addressed absolute stream plan; Section 3 depicts spoofing appropriation discovery;

Region 4 depicts fuzzy chief controller to conspire in choosing stream accumulation. Segment 5 clarifies the spoofing level location technique for stream-based system interruption discovery framework engineering; Area 6 assesses the framework. Area 7 is the sides, and future job diagrams.

3. THE DIFFERENT TYPES OF ATTACK

3.1 ICMP attack

Right now, the attacker floods tremendous measure of ICMP ECHOREQUEST parcels in an agreement using unbiased host IP address, if the enemy does not generate an IP address then the attacker shall be influenced by the fact that he will collect all the request response received. The analytical host should be affected now because the IP address has been created.

3.2 SYN-ACK attack

Typical TCP connection meets "threeway handshake" for instance target gets a SYN package from a foundation and sends rear a SYN ACK. The target will then listen to a SYNACK ACK before the relationship is set up. When sitting closely for the ACK to the SYN ACK, a limited-size affiliation line on the aim tracks associations hanging on for completion. By generating false TCP SYN packages at a rapid pace from random IP addresses, it is conceivable to top off the alliance line and refuse legitimate clients TCP administrations, such as email, log transfer or WWW.

4. APPROACHES FOR DEFENDING

Fortifications for Spread Denial of Service attack may be ordered into three classifications: defensive components, responsive systems, and sourcefollowing.

4.1 Preventive Defense

Mitigation strategies tend to strengthen a PC infrastructure or system's security level; thereby stopping the attacks from happening, or improving defense against threats. With this

designation a constructive roaming program for the server has a spot. This system consists of a few spread identical servers, besides the field of dynamic server varies across them expending a safe measurement of the meander. Only honest clients will learn the meandering time of the site and the location of new servers. When the server meanders, all connections are removed, and the honest clients can get rewards at any cost at the beginning of any meandering period until the intruder figures the complex server out again. For the most part, these schemes are costly and hard to genuinely forestall assaults.

4.2 Source Tracking

Then again the source-following plans aim to locate the stirrings of attacks, with the intention that reformatory move against attacks can be produced. The existing procedures fell into four meetings: stamping of parcels, traceback of communications, recording and interpretation of traffic. A broad variety of packet screening plans have been introduced to encrypt data within IP packages for example they are handled on the internet. Probable parcel testing (PPM), in which the switches are likely to inject data into the IP header ID field in-package, To the degree that the victim can restore the manner in which these marks are used to strike and so control the manifestations of affronting packets. Senior member et al. [13] note an arithmetic method that relies on polynomial capacities being recreated to control bundles. Belenky and nsari [10] suggest a deterministic stamping method (DPM), in which only the location of the main entrance gateway that a packet joins is embedded in the package, rather than the entire direction that the parcel goes (as found in PPM). In the Traceback Technique message [7], ICMP traceback notices are created by switches for some of the packets and sent with them. The assault route can be overcome by consolidating the ICMP parcels with their contrasts to the TTL. Of e.g. a few variables are called to determine an ICMP message's estimate, how long the transfer to the target is, how brisk the package gets at the start of the attack, and how the target needs to get it. A joint issue in these 4 systems is that recreation of the way of offensive turns out to be very volatile and costly because there are endless attackers (Properly stolen DoS assaults, for example). Additionally, once an attack has happened, these kinds of structures are meant to allow remedial step and can not be used to avoid a sustained DDoS attack.

4.3 Reactive Solution

The responsive DDoS safeguard mechanisms are designed to discern a progressive offensive and respond to it by monitoring the propagation of attack packages to relieve the disruptions of the attack. Some of the sensitive proposals suggested by Yaar et al. [12] makes use of the probability of packet screening for sifting through the packages of attack rather than attempting to locate the wellspring of these packages. This program uses a way code (called Pi) to test the bundles; the identifiable evidence area in the package is divided in a few places and every turn requires one of these tests. When the liability has learned the corresponding test to target parcels, it will sift through each such packet that comes from a similar direction. In the midst of identifying blockage, the Pushback [8] technique generates an attack fingerprint, which imposes a rate cap for contrasting incoming traffic. These data are then produced to upstream switches, and the switches help to drop these parcels, with the intention of pushing back the attack source. In the Neighbor Stranger Isolation (NSD) approach [9] neighbors and strangers are separated from the network. In case the package is from the neighbor at this point NSD will consider the packet otherwise it will reject it. Achieving the sensitive plans is based on a precise distinction between large parcels and assault parcels.

5. SPOOFED IP PACKET DETECTION METHODS

5.1 Basic Principles in HCF

Designate the rudimentary philosophies of HCF. Is the authentication of the foundation IP discourse of respectively container through "hop- count" examination? the first pronounce "hopcount" calculation, and formerly contemporary a benign inform instrument that imprisonments the genuine mappings among IP discourses and hop count standards. Lastly, we recapitulate HCF in procedure of ahigh equal examination procedure [14].

5.1.1 Hop-Count Calculation

hop-count info isn't straight warehoused in the IP heading, single consumes toward calculate it grounded arranged the final TTL worth. TTL is an eight-bit field in the IP heading, formerly familiarized toward stipulate the supreme generation of respectively sachet in the Cyberspace. Respectively transitional router curtailments the TTL worth of intransit IP container via single beforehand accelerating it to the next hop. The final TTL worth after a container influences its terminus is, consequently, the preliminary TTL diminished through the numeral of transitional journeys (or basically hop-count).The encounter popular hop-count calculation remains that a terminus individual understands the final TTL worth .It would consume remained humble required completely operating systems (OSes) secondhand the similar original TTL worth, then in rehearsal, around is no agreement on the original TTL worth. Additionally, then the OS aimed at a assumed IP address might modification through time, we can't shoulder a solitary stationary original TTL worth for respectively IP address. maximum contemporary OSes use solitary a insufficient designated original TTL standards 32 ,30, 64 ,60, 255 and 128. This usual of original TTL standards protections greatest of the prevalent OSes, such by way of

Microsoft Windows, Linux, alternatives of BSD, and numerous profitable Unix system. We detect that greatest of these original TTL standards are distant separately, excluding among 32 and 30, 64 and 60, and among 60 and 32. Subsequently Cyberspace suggestions consume unprotected that insufficient Cyberspace congregations are separately via additional than 30 stages [15], [16] which is too confirmed through our personal opinion, single cannister control the original TTL worth of a container via choosing the lowest

International Journal of Engineering Research and Technology. ISSN 0974-3154, Volume 13, Number 10 (2020), pp. 2736-2741
 https://dx.doi.org/10.37624/IJERT/13.10.2020.2736-2741

original worth fashionable the usual that is greater than its final TTL. E.g., doubt the final TTL worth is 112, the original TTL worth is 128. Toward resolution obscurities cutting-edge the suitcases of {32, 30},

{32, 60}, and {60, 64}, we determination calculate a hop-count worth aimed at apiece of the conceivable original TTL standards, and receive the sachet uncertainty around stands a competition through moreover of the conceivable hop-counts [14].

```
for each packet:
  extract the final TTL T_f and the source IP address S;
  infer the initial TTL T_i;
  compute the hop-count H_c = T_i − T_f;
  index S to get the stored hop-count H_s;
  if   (H_c ≠ H_s)
       the packet is spoofed;
  else
       the packet is legitimate;
```

Figure 1: Hop-count inspection algorithm.

The problem of preventive the conceivable original TTL standards stands that containers after end systems that usage "odd" original TTL standards, might be erroneously identified by way of deceived. This might transpire unknown a operator changes OS since individual that usages a "normal" original TTL worth toward additional that usages an "odd" worth. Then our filter switches towards abandon containers solitary upon discovery of a DDoS bout, such finish organizations would agonize solitary throughout an definite DDoS bout. The education cutting-edge demonstrations that the OSes that usage "odd" original TTLs are characteristically elder OSes. We imagine such OSes to establish a actual unimportant proportion of end-hosts cutting-edge the present Cyberspace.

Therefore, the benefit of organizing HCF must overshadow the danger of repudiating facility toward persons endhosts throughout attack [14].

5.1.2 Taking Legitimate Hop-Count Values

To preserve a precise IP2HC planning bench, we necessity detention lawful hop-count mappings and genuine variations in hop-count, though prevention slightly effort to gradually contaminate the planning bench. We can complete this concluded TCP joining formation. The IP2HC planning bench must be rationalized solitary via packets going to TCP acquaintances in the government [17]. The three-way TCP handclasp for joining arrangement necessitates the active-open gathering toward refer an ACK (the previous package in the three-way handclasp) to recognize the inactive gathering's original arrangement quantity. The sleepwalker (flooding basis) that directs the SYN package by a deceived IP discourse determination not accept the target's SYN/ACK packet and consequently can't comprehensive the three-way handshake. By means of packets after recognized TCP contacts safeguards that an attackers can't gradually contaminate a bench by spoofing basis IP discourses.

Though our pollution-proof instrument delivers protection, it might stand also luxurious toward examine besides inform the IP2HC planning bench through respectively afresh recognized TCP joining, meanwhile our inform connotation is arranged the dangerous track of TCP dispensation. We deliver a user-configurable limitation toward regulate the incidence of informs. Memorandum that the pollution-proof instrument the whole thing to imprisonment genuine vicissitudes in hop-count as glowing by way of hopcount standards of novel IP discourses[14].

5.1.3 Inspection and Validation Algorithm

Review and Authentication Procedure Presumptuous that a precise IP2HC mapping table is contemporary, Figuer1 plans the HCF process secondhand to classify spoofed packets.

Table 1. Diversity of Traceroute

Type	Sample Number
.com sites	11
.edu sites	4
.org sites	2
.net sites	12
foreign sites	18

The examination algorithm excerpts the basis IP address and the final TTL worth as of apiece IP package. The procedure concludes the original TTL worth besides withdraws the final TTL worth since it toward get the hop-count. The basis IP discourse assists by way of the catalogue hooked on the bench to recover the accurate hop-count aimed at this IP discourse. Uncertainty the calculated hop-count competitions the deposited hop-count, the package consumes remained "authenticated"; then, the package stands classified by way of deceived. Memorandum that a deceived IP discourse might transpire toward take the similar hop-count by way of the single since a sleepwalker toward the target. Cutting-edge this circumstance, HCF will not remain talented toward recognize the deceived pack [14].

5.2 OS Fingerprint

OS fingerprint is the nursing of an inward packet to regulate the OS the basis is consecutively on. It is commonly rummage-sale via system managers to recognize outmoded OS inside their network, discover and reinforcement susceptible OS and to recognize malevolent customer. OS fingerprint discovery cannister remain moreover sedentary or energetic [19] . It receipts the benefit that dissimilar OS apparatuses dissimilar TCP/IP heap apiece consuming its exclusive autograph [18] [19].

International Journal of Engineering Research and Technology. ISSN 0974-3154, Volume 13, Number 10 (2020), pp. 2736-2741
 https://dx.doi.org/10.37624/IJERT/13.10.2020.2736-2741

5.2.1 OS fingerprint features

In resonant obtainable an OS fingerprint arranged an IP pack, the benefit that dissimilar OS consume their excellent worth mergers aimed at TCP/IP heading ground remains browbeaten. Amongst the IP heading ground characteristic that are frequently examined are: preliminary Time to Living (TTL) worth, opening magnitude, IP DF (Don't Portion) selection and IP ToS (Category of Provision) selection. These arenas determination remain removed after the IP heading of the received TCP SYN or SYN + ACK section [18].

5.2.2 OS fingerprint methods

OS fingerprint extremely be contingent on whether it's energetic or inactive. Vigorous fingerprint includes distribution a particularly manufactured investigation packet towards the accurate source while indolent acquires the heading topographies from received packets [19]. Communal dynamic fingerprint apparatuses contain SinFP, Xprobe and Nmap whereas inactive fingerprinting apparatuses contains p0f (Inactive OS Fingerprint), OSF (inactive OS fingerprint aimed at iptables) besides Ettercap. we deliberate p0f and Nmap. Nmap is a prevalent energetic network planning instrument. It delivers skimming mouth through distribution up to fifteen investigations which are completed up of ICMP , TCP and UDP to sweeping and local harbors of the board host. The heading grounds of the comebacks remain investigated toward recognize theOS its consecutively arranged. This is accomplished through corresponding the experimental answer toward its deposited OS catalogue [19]. P0f stands a inactive fingerprint method that remained initially printed in two thousand through Michal Zalewski [19]. It meanings through investigating the TCP/IP pack heading parklands toward control the inaccessible host OS. It fingerprint the introducing SYN pack of a inaccessible host joining toward the attendant and the SYN + ACK answer since the attendant. It submits after Vigorous OS uncovering apparatuses by way of it doesn't direct investigation packets to the inaccessible host [18].

6 CONCLUSION AND FUTURE WORK

This paper has studied dissimilar approaches secondhand toward substantiate the correct basis of an inward pack toward perceive IP deceiving throughout DDoS bout. We anticipated together energetic and inactive host-based OS fingerprint that confirms the correct basis of an inbound pack through recognizing its OS. In future work, the idea is to mechanize the procedure for improved presentation and circumvent humanoid interference. And We proposed another method we partake accessible a hop-count-based filter arrangement that distinguishes besides castoffs deceived IP packs toward marmalade organization possessions. Our arrangement reviews the hop-count of external packets toward authenticate their legality. By means of solitary, a reasonable quantity of stowage, HCF concepts a correct IP2HC planning board through IP discourse accumulation besides hop-count gathering. A pollution-proof instrument prepares and apprises entrances cuttingedge the planning board. Through avoidance, HCF breaks in the knowledge government, monitoring nonstandard IP2HC planning performances deprived of removal slightly packet. When spoofed DDoS traffic is perceived, HCF changes to the filter government and castoffs greatest of the spoofed packets. Through examining genuine network. IP

Spoofing Detection Approach (ISDA) to coordinate Identification Architecture for Interruption has been suggested right now. Exploratory findings tested by DARPA 98 reveal that the discovery of caricature stage enhances the appearance of Flow-based NIDS under satirized flood attacks. It is not only used for exploration of stream-based network disruption, but is also used for other barrier systems, for example: ISDA will hold persuasive parts to the limit and eject parts from satirizing flooding attacks that would effectively gain heads or firewall (on-line) to protect noxious sources and boost the operation of the entire expectation process.

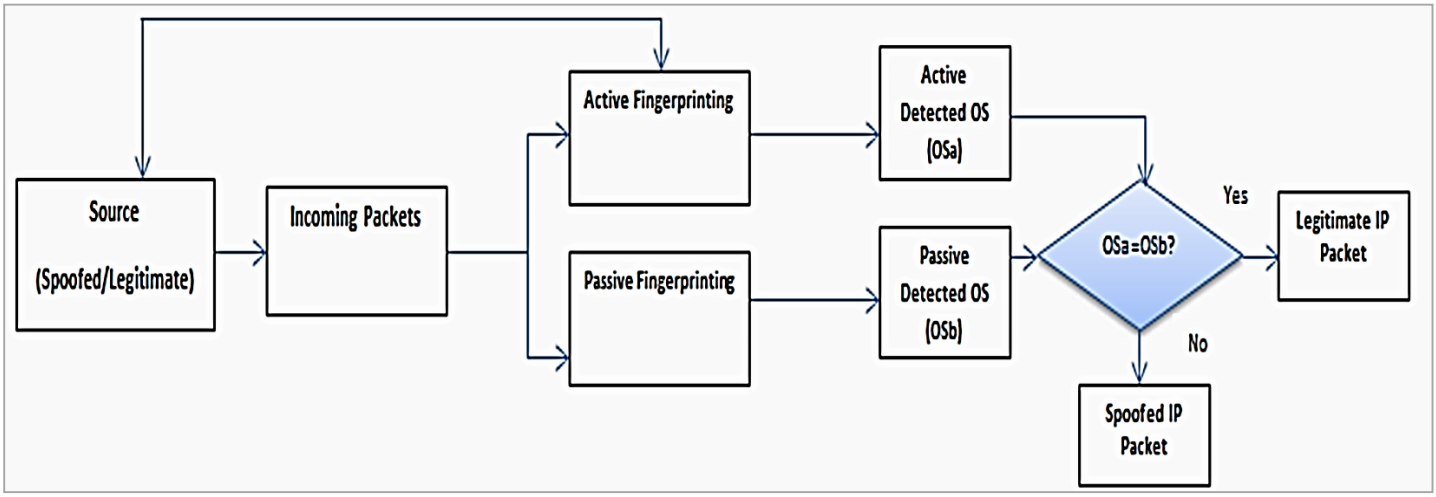

Figure 2. IP Spoofing Detection Block

REFERENCE

[1] D. Kravets, "UN report declares internet access a human right," *accessed April,* vol. 28, p. 2012, 2011.

[2] I. Stats, "Internet world stats," *Internet World Stats,* p. 17, 2012.

[3] A. G. Mukaddam, "IP spoofing detection using Hop Count and Round Trip Time profiling," 2012.

[4] A. Mukaddam and I. H. Elhajj, "Round trip time to improve hop count filtering," in *2012 Symposium on Broadband Networks and Fast Internet (RELABIRA)*, 2012, pp. 6672: IEEE.

[5] A. Mukaddam, I. Elhajj, A. Kayssi, and A. Chehab, "IP spoofing detection using modified hop count," in *2014 IEEE 28th International Conference on Advanced Information Networking and Applications*, 2014, pp. 512-516: IEEE.

[6] O. A. Osanaiye, "Short Paper: IP spoofing detection for preventing DDoS attack in Cloud Computing," in *2015 18th International Conference on Intelligence in Next Generation Networks*, 2015, pp. 139141: IEEE.

[7] A. Belenky and N. Ansari, "IP traceback with deterministic packet marking," *IEEE communications letters,* vol. 7, no. 4, pp. 162-164, 2003.

[8] A. Yaar, A. Perrig, and D. Song, "Pi: A path identification mechanism to defend against DDoS attacks," in *2003 Symposium on Security and Privacy, 2003.*, 2003, pp. 93-107: IEEE.

[9] D. Dean, M. Franklin, and A. Stubblefield, "An algebraic approach to IP traceback," *ACM Transactions on Information and System Security (TISSEC),* vol. 5, no. 2, pp. 119-137, 2002.

[10] D. Plonka, "FlowScan: A Network Traffic Flow Reporting and Visualization Tool," in *LISA*, 2000, pp. 305-317.

[11] N. Aaaraj, S. Itani, and D. Abdelahad, "Neighbor stranger discrimination (NSD)-A new defense mechanism against DDoS attacks," in *in Proceedings of the 3rd FEA Student Conference*, 2004: Citeseer.

[12] P. Ferguson and D. Senie, "rfc2827: network ingress filtering: defeating denial of service attacks which employ ip source address spoofing," ed: RFC Editor, 2000.

[13] K. Park and H. Lee, "A Proactive Approach to Distributed DoË Attack Prevention using Route-Based Packet Filtering," 2000.

[14] H. Wang, C. Jin, and K. G. Shin, "Defense against spoofed IP traffic using hop-count filtering," *IEEE/ACM Transactions on networking,* vol. 15, no. 1, pp. 40-53, 2007 .

[15] B. Cheswick, H. Burch, and S. Branigan, "Mapping and visualizing the Internet ",in *USENIX Annual Technical Conference, General Track*, 2000, pp. 1-12: Citeseer.

[16] K. Claffy, "Traci e. Monk, and Dani el McRobb. Internet tomography. N at u re Web M flatters," ed, 1999 .

[17] K. R. Fall and W. R. Stevens, *TCP/IP illustrated, volume 1: The protocols*. addison-Wesley, 2011.

[18] O. A. Osanaiye, "Short Paper: IP spoofing detection for preventing DDoS attack in Cloud Computing," in *2015 18th International Conference on Intelligence in Next Generation Networks*, 2015, pp. 139-141: IEEE.

[19] J. M .Allen, "OS and Application Fingerprinting Techniques," *SANS Institute InfoSec Reading Room,* 2007