International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) ISSN: 2395-5325
Volume 4, Special Issue 3 (March '2018)
Proceeding of - National Conference on Recent Trends in Information Technology and Communication,
Conference held at Velammal Engineering College,Chennai,India.

RESISTANCE ALIGNED WITH MAN IN THE MIDDLE ATTACK IN CLIENT SERVER SYSTEMS

Vijayan A,
Assistant Professor,
Department of Information Technology,
Velammal Engineering College,
Chennai,Tamilnadu,India.

V.Kanagalakshmi,
Student,
Department of Information Technology,
Velammal Engineering College,
Chennai,Tamilnadu,India.

G. Pavittra,
Student,
Department of Information Technology,
Velammal Engineering College,
Chennai,Tamilnadu,India.

S.Monisha,
Student,
Department of Information Technology,
Velammal Engineering College,
Chennai,Tamilnadu,India.

Abstract: In PC organizing, IP address mocking or IP caricaturing is the formation of Internet Protocol (IP) parcels with a manufactured source IP address, with the reason for disguising the personality of the sender or imitating another processing framework. The essential convention for sending information in the Internet arranges and numerous different systems is the Internet Protocol ("IP"). The header of every IP parcel contains the numerical source and goal address of the bundle. The source address is ordinarily the address that the parcel was sent from. By producing the header so it contains an alternate address, an aggressor can influence it to give the idea that the parcel was sent by an alternate machine. With the goal that the IP Spoofing comes into put. Cloud administrations offer better choices for viable sending of an IP trace back framework. We initially introduce novel cloud-based trace back engineering. We have proposed a novel arrangement, named Passive IP Trace back (PIT), to keep away from the difficulties in operation. To catch the sources of IP parodying movement is of extraordinary significance. For whatever length of time that the genuine areas of spoofers are not uncovered, they can't be deflected from propelling further assaults. Indeed, even simply moving toward the spoofers, for instance, deciding the ASes or systems they live in, assailants can be situated in a littler range, and channels can be put nearer to the aggressor before assaulting movement get totaled. The last yet not the slightest, distinguishing the starting points of satirizing movement can help fabricate a notoriety framework for ASes, which would be useful to push the comparing ISPs to check IP source address. The proposed arrangement guarantees that the substance asking for trace back benefit is a genuine beneficiary of the bundles to be traced.Load balancer offers many favourable circumstances over independent Load Balancing and IDS arrangements; it additionally experiences the downsides of both. It has been said that the three things most imperative to a server trough are Security (the capacity to withstand hacking), High-Availability (the capacity to withstand equipment disappointment), and low-idleness (the capacity to benefit asks for rapidly). With the present usage of secure direct, the initial two criteria, security and high accessibility, are fulfilled. Generally concerning idleness, our trials have (indeed) demonstrated that there is an exchange off amongst security and execution. While enhancing the productivity of the programming can relieve this issue to a degree, the exchange off is sure to remain, and picking the correct adjust will probably keep on being a troublesome errand for the framework manager. It is the creators' sentiment that this kind of framework could give a truly necessary extra security device; in any case, a great arrangement of streamlining work stays before it could be broadly conveyed.

Keywords:IP Traceback, Access Control, Authentication, Cloud-based Traceback

I. INTRODUCTION

Consummate exhibiting and evaluation of PC systems depend on the accessibility of vast datasets of Internet streams gained from spine joins. The information are expected to help a few research undertakings, including Internet movement investigation, displaying of topological circulation, distinguishing proof of security assaults, and approval of research comes about. Shockingly, genuine protection and security concerns debilitate the production of such datasets. From one perspective, organize streams convey greatly secret data that ought not to be discharged for security reasons. For this work, we expect that the payload is expelled from all parcels. Nonetheless, even for this situation, an enemy watching the source and goal IP locations may connect a person with the Web locales that she went to, and along these lines he may deduce private data, for example, political

sentiments, medical problems, or religious conviction. Thus, Internet streams may uncover individual interchanges among particular people, for example, email trades and talk sessions among them. Then again, those datasets may likewise help a foe to perform security assaults. For example, watching the activity of an objective system, an enemy could recognize conceivable bottlenecks to be misused for disavowal of-benefit (DoS) assaults. Therefore, a few systems were proposed to purify organize streams while protecting their utility. Early systems depended on the substitution of the genuine IP addresses with pseudo-IDs. In any case, that strategy turned out to be defenceless against various types of assaults, in light of the information of system qualities, or on the ability to infuse sham streams in the observed system. All the more as of late, a few methods have been proposed to stay away from the re-distinguishing proof of IP addresses, in light of the irritation of different fields of the streams. Be that as it may, those methods don't give any formal privacy assurance, and it has been as of late demonstrated that they are inclined to various types of assaults. Then again, understood systems proposed for smaller scale information anonymization are not specifically appropriate to arrange streams, and the approach of intervened organize follow investigation has a few weaknesses. Strategies for engineered organize stream age have been likewise proposed. Be that as it may, the utility of such datasets was addressed in the writing. In our past work, we have introduced - confusion, an obscurity system for arrange streams, which gives formal classification ensures under practical suspicions about the foe's information, while protecting the utility of discharged information. In that work, we expected a solitary arrival of the entire dataset of streams. Notwithstanding, the incremental arrival of system streams speaks to an unmistakable viable favourable position. For example, assume that an association wishes to share a month of system streams. Without the incremental discharge, it is important to hold up until the finish of the month to begin discharging the dataset. Through incremental discharges, the association could give a timelier sharing of system streams picking an every week or even an everyday plan. Also, the incremental discharge gives essential specialized points of interest. In reality, the computational expenses and the memory necessities for jumbling a vast dataset could be unequivocally diminished by dividing the dataset in littler subsets and by running the obscurity procedure freely on every subset. Concerning our past work, the first commitments of this paper comprise in: 1) the ID of classification follows; 2) a novel protection calculation to apply – obscurity to incremental arrivals of system follows; 3) a hypothetical verification of the privacy ensures gave by the guard calculations; 4) a broad trial assessment of the calculation for incremental - jumbling, did with billions of genuine streams created by the fringe switch of a business self-ruling framework. We made trials on activity decent variety, factual investigation of stream fields, and system stream examination. Our outcomes demonstrate that our system safeguards the information quality in both the single and the incremental discharge. Existing follow back instruments are either not generally bolstered by current product switches. It is exceptionally heart-breaking to influence Internet to specialist organizations (ISPs) team up. Since the spoofers are accessible at each side of the world, a solitary Internet Service Protocols to send its own follow back framework is practically futile. Notwithstanding, ISPs, which are business substances with aggressive connections, are for the most part need in the sum speculations which help customers of the others to follow assailant in oversaw ASes. Since the sending of trace back components isn't of clear picks up however evidently high overhead, to the best information of creators, there has been no conveyed Internet-scale IP trace back framework till now.

Rather than proposing another IP trace back system with enhanced following capacity, we propose a novel arrangement, named Passive IP Trace back (PIT), to sidestep the difficulties in sending. Switches may neglect to forward an IP satirizing bundle because of different reasons, e.g., TTL surpassing. In such cases, the switches may create an ICMP mistake message (named way backscatter) and send the message to the caricature source address. Since the switches can be near the spoofers, the way backscatter messages may possibly unveil the areas of the spoofers. PIT abuses these way backscatter messages to discover the area of the spoofers. With the areas of the spoofers known, the casualty can look for assistance from the relating ISP to sift through the assaulting bundles, or take different counterattacks. The casualties can discover the areas of the spoofers specifically from the assaulting movement.

II. RELATED WORKS

1. HassanAljifri in 2015. IpTrace back: A New Denial-Of-Service Deterrent. DoS assaults by flooding the objective system and its PCs with a lot of activity from one or (as on account of conveyed DoS, called DDoS) more PCs under the assailant's control. Such assaults are among the hardest to address since they are easy to actualize, hard to forestall, and hard to follow. IP trace back techniques give the casualty's system overseers with the capacity to recognize the address of the genuine wellspring of the parcels causing DoS. IP trace back is indispensable for re-establishing ordinary system usefulness as fast as could be expected under the circumstances, anticipating reoccurrences, and, at last, considering the aggressors responsible. A few endeavors are under approach to create aggressor distinguishing proof advancements on the Internet. This article takes a gander at existing DDoS IP trace back procedures and future patterns. To keep this IP address control, Kihong Park and Heejo Lee4 proposed to introduce conveyed parcel channels on self-sufficient frameworks over the Internet to stop bundles with caricature IP addresses. Another arrangement is to set up organize switches on ISP systems to guarantee that the parcels directed from the systems just contain legitimate source addresses.

2. Minho Sung and Jun Xuin 2014. IpTraceback-Based Intelligent Packet Filtering: A Novel Technique For Defending Against Internet DdosAttacks.The proposed plot influences on and sums up the IP trace back plans to get the data concerning whether a system edge is on the assaulting way of an assailant ("tainted") or not ("spotless"). We watch that, while an aggressor will have every one of the edges on its way set apart as "contaminated," edges on the way of a real customer will for the most part be "perfect." By specially sifting through parcels that are engraved with the signs of "tainted" edges, the proposed plot expels a large portion of the DDoS movement while influencing true blue activity just somewhat. Appropriated Denial of Service (DDoS) is a standout amongst the most troublesome security issues to address. While many existing methods (e.g., IP trace back)

concentrate on following the area of the aggressors afterward, little is done to moderate the impact of an assault while it is seething on. In this paper, we exhibit a novel system that can viably sift through the dominant part of DDoS activity, accordingly enhancing the general throughput of the genuine movement. DDoS programming, for example, TFN (Tribe Flood Network) is then introduced on them. These hosts will later be charged by the foe to at the same time send a huge volume of movement to a casualty host or system. The casualty is overpowered by so much activity that it can give practically no support of its honest to goodness customers.

3. Yang Xiang, Member, Wanlei Zhou and MinyiGuoin 2013. Flexible Deterministic Packet Marking: An IpTraceback System to Find the Real Source of Attacks**.** Web Protocol (IP) trace back is the empowering innovation to control Internet wrongdoing. In this paper, we introduce a novel and reasonable IP trace back framework called Flexible Deterministic Packet Marking (FDPM) which gives a guard framework the capacity to discover the genuine wellsprings of assaulting parcels that navigate through the system. While various other trace back plans exist, FDPM gives creative highlights to follow the wellspring of IP bundles and can acquire preferred following ability over others. Specifically, FDPM receives an adaptable check length methodology to make it good to various system conditions; it additionally adaptively changes its stamping rate as per the heap of the taking part switch by an adaptable stream based stamping plan. Assessments on both recreation and genuine framework usage exhibit that FDPM requires a reasonably modest number of parcels to finish the trace back procedure; add minimal extra load to switches and can follow countless in one trace back process with low false positive rates. The implicit over-burden anticipation component makes this framework equipped for accomplishing an agreeable trace back result notwithstanding when the switch is vigorously stacked. The inspiration of this trace back framework is from DDoS safeguard. It has been utilized to follow DDoS assaultingparcels as well as improve sifting assaulting movement. It has a wide cluster of uses for other security frameworks.

4. Terence K.T. Law, John C.S. Lui and David K.Y. Yau in 2012. You Can Run, But You Can't Hide: An Effective Statistical Methodology To Trace Back Ddos Attackers**.** Our work depends on a probabilistic checking calculation in which an assault chart can be developed by a casualty site. We broaden the fundamental idea with the end goal that one can rapidly and proficiently derive the power of the "neighbourhood activity" created at every switch in the assault diagram in light of the volume of got checked bundles at the casualty site. Given the forces of these nearby movement rates, we can rank the neighbourhood activity and recognize the system areas producing the vast majority of the assault activity. We display our trace back and assailant ID calculations. There is right now an earnest requirement for viable arrangements against dispersed refusal of-benefit (DDoS) assaults coordinated at some outstanding Web locales. Due to expanded modernity and seriousness of these assaults, the framework overseer of a casualty site needs to rapidly and precisely distinguish the likely assailants and kill the assault movement. We likewise give a hypothetical structure to decide the base stable time tmin, which is the base time expected to precisely decide the areas of assailants and neighbourhood activity rates of taking part switches in the assault diagram. Entensive trials are completed to show that one can precisely decide the base stable time tmin and, in the meantime, decide the area of assailants under different edge parameters, organize measurements, assault movement appropriations, on/off examples, and system activity conditions.

5. Basheer Al-Duwairi, and ManimaranGovindarasu in 2011. Novel Hybrid Schemes Employingm Packet Marking and Logging forIpTraceback.Conventional traceback plans give satirize parcels traceback ability either by expanding the bundles with incomplete way data (i.e., parcel stamping) or by putting away bundle condensations or marks at middle of the road switches (i.e., parcel logging). Such methodologies require either an expansive number of assault bundles to be gathered by the casualty to construe the ways (parcel checking) or a lot of assets to be saved at middle of the road switches (bundle logging). We embrace a half and half traceback approach in which parcel checking and bundle logging are coordinated in a novel way, in order to accomplish the best of the two universes, that is, to accomplish few assault bundles to direct the traceback procedure and a little measure of assets to be allotted at moderate switches for bundle logging purposes. In light of this idea, two novel traceback plans are displayed. We assess the viability of the proposed plans against different execution measurements through a blend of logical and reproduction thinks about. Our investigations demonstrate that the proposed plans offer an exceptional decrease in the quantity of parcels required to lead the traceback procedure and a sensible sparing in the capacity prerequisite. These assaults deny standard Internet administrations from being gotten to by authentic clients either by blocking administration totally or by irritating it with the end goal that clients wind up noticeably not inspired by the administration any longer (for instance, causing noteworthy deferral in getting to an aircraft reservation site). In such assaults, the primary target is to overwhelm the casualty while covering assailant's personality. The present Internet has seen a few occurrences that affirm the overwhelming impact of such assaults.

6. Abraham Yaar, Adrian Perrig,and Dawn Song in 2015. Stackpi: New Packet Marking and Filtering Mechanisms forDdosandIp Spoofing Defense. We propose the StackPi denoting, another bundle checking plan in light of Pi, and new sifting instruments. The StackPi checking plan comprises of two new stamping techniques that considerably enhance Pi's incremental organization execution: Stack-based stamping and compose ahead checking. Our plan totally kills the impact of a couple of heritage switches on a way, and performs 2– 4 times superior to anything the first Pi plot in a scanty organization of Pi-empowered switches. For the separating system, we determine an ideal limit technique for sifting with the Pi checking. We likewise build up another channel, the PiIP channel, which can be utilized to distinguish Internet convention (IP) satirizing assaults with only a solitary assault parcel. The StackPi checking enhancements, Stack-based and compose ahead stamping, take out the stamping gaps created by heritage switches and incorporate the markings from single

inheritance switches instantly following Pi-empowered switches in a way. Likewise present a novel channel which depends on the Pi, IP tuple of every parcel, making it far more outlandish that an aggressor will effectively sidestep the channel. An assailant sends TCP SYN parcels as though to start a TCP association with its casualty. These SYN bundles contain satirize source IP addresses, which make the casualty squander assets that are dispensed to half-open TCP associations which will never be finished by the assailant. Which utilize a lot of movement to impair a casualty server, are the concentration of this article? In any case, source IP address satirizing is likewise utilized as a part of numerous different assaults.

7. Shui Yu, Wanlei Zhou, Robin Doss, and WeijiaJia, in 2014. Traceback Of Ddos Attacks Using Entropy Variations.We propose a novel traceback strategy for DDoS assaults that depends on entropy varieties amongst ordinary and DDoS assault activity, which is in a general sense not the same as usually utilized parcel checking systems. In contrast with the current DDoS traceback strategies, the proposed technique has various points of interest—it is Memory non intensive, proficiently versatile, vigorous against bundle contamination, and free of assault activity designs. The aftereffects of broad test and recreation examines are exhibited to show the adequacy and effectiveness of the proposed strategy. Our examinations demonstrate that exact traceback is conceivable inside 20 seconds (around) in a huge scale assault connect with a huge number of zombies. Strategy manages the parcel flooding sort of assaults splendidly. In any case, for the assaults with modest number assault parcel rates, e.g., if the assault quality is under seven times of the quality of no assault streams, at that point the present metric can't segregate it. We can identify the assault with the data that we have gathered so far utilizing customary strategies. Two noteworthy techniques for IP traceback, the probabilistic parcel stamping and the deterministic bundle checking both of these procedures expect switches to infuse marks into singular bundles. The PPM procedure can just work in a neighbourhood scope of the Internet (ISP arrange), where the protector has the expert to oversee.

8. Long Cheng, Dinil Mon Divakaran, Wee Yong Lim, Vrizlynn L. L in 2013. Opportunistic Piggyback Marking forIp Traceback**.** Traceback message content encoding and conveyance works in MBT, and productively accomplishes sped up and vigorous traceback message conveyance by abusing piggyback stamping openings. In view of the proposed OPM plot, we at that point display the adaptable checking based traceback system, which is a novel plan worldview for IP traceback and has a few ideal highlights for reasonable sending of IP traceback. Through numerical examination and exhaustive recreation assessments, we exhibit that our plan adequately diminishes the traceback fulfilment postponement and switch handling overhead, and builds the message conveyance proportion contrasted and other benchmark approaches. The principle thought is to misuse free ride open doors for sped up and vigorous conveyance of traceback message pieces to end hosts. Introduced an adaptable stamping based traceback (FMBT) system, which meets a few ideal destinations that past individual traceback plans neglected to fulfill all the while. Clearly applying parcel level denoting all the time on all movement streams is superfluous and it endures the versatility issue which over-burdens switches by denoting each passing bundle. There is a major disengaging between the length of a traceback message and the stamping space accessible in IP header.

9. Vrizlynn L. L. Thing, Morris Sloman and NarankerDulay in 2012. Locating Network Domain Entry and Exit point/path for DDoS Attack Traffic. A strategy to decide passage and leave focuses or ways of DDoS assault movement streams into and out of system spaces is proposed. We watch substantial source addresses seen by switches from inspected activity under non-assault conditions. Under assault conditions, we distinguish course oddities by figuring out which switches have been utilized for obscure source addresses, to build the assault ways. We consider organization issues and show comes about because of reproductions to demonstrate the possibility of our plan. We at that point actualize our Traceback component in C++ and more practical investigations are led. Our traceback system assembles reserves of substantial source addresses (white rundown age) for switches at circulated WL storing gadgets, plays out the development of the assault chart inside a regulatory area, and gives an expansion to bury space support to recognize the system point closest to the assault source. SPB (Strategic Points Based) can accomplish the traceback objective while lessening the work load and overhead. The overheads of creating and putting away even a 28 byte hash can be somewhat high so IP Logging isn't done in many systems. Where the aggressors utilize satirize source delivers to shroud their personality and area.

III. SYSTEM DESIGN

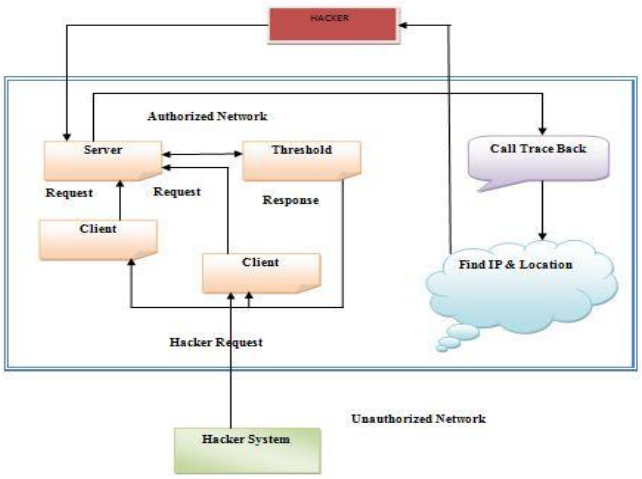

Figure 1. Architecture Diagram

IV. OUR CONTRIBUTION

A. Clients Registration

In the enlistment stage, the client points of interest Client's name, IP-address, Port and a key string (secret word) is asked from the client at the season of enrollment for the protected site. The key string can be a mix of letters in order and numbers to give more secure condition. This string is linked with haphazardly created string in the server. After Client-

Server enrollment convention has finished, the server will have the accompanying data in its memory, IP-address Port, Client's Name, Public Key of enlisted Client's and limit esteem.

B. File sending using threshold value

We characterize a limit an incentive for every association. Each time a parcel is sending on an association its limit esteem is included. Sender can be either host or system based, as all cooperation is ordinarily performed over a system association. One of the Packet or document is to be chosen for the change procedure. The bundle is sent along the characterized way from the source LAN to goal LAN .The goal LAN gets the parcel and checks whether that it has been sent along the characterized way or not utilizing edge esteems.

C. Hacker zone - unauthorized network

The hub which is available in the distinctive system or individual framework getting to the information in the bogus name of a hub which is available in the switch arrange is called as programmers. The limit esteem isn't dispensed to the programmer framework. Checking Access module deals with the information sending through the system utilizing the limit esteem. It gets to the database to check the approval for legitimate and uncalled for client. It likewise screens the programmers on the off chance that anyone getting to the information, which does not have a place with the system.

D. Call Trackback

Call trackback outline which is fueled by knowledge alongside the plan of assault classifier. The yield produced by the classifier creates a dynamic rundown of assaults, which are then lined in the proposed backscatter engineering worked with arrange security to comprehend different approach of conduct and examples of the assailant. The system overseer gathers all such pertinent data over the system itself permitting the inbound system association from the assailant to do as such. The framework makes a TTL structure to keep the likelihood of powerless and antagonistic circumstance over the system even before the assault occasion is performed by the assailant.

E. To find hacker location

Bundle sifting is one guard against IP caricaturing assaults. The portal to a system for the most part performs entrance separating an edge esteem, which is hindering of bundles from outside the system with a source address inside the system. This keeps an outside aggressor parodying the address of an inward machine. In a perfect world the portal would likewise perform departure separating on active bundles, which is obstructing of parcels from inside the system with a source address that isn't inside. This keeps an aggressor inside the system performing sifting from propelling IP caricaturing assaults against outer machines.

V. ALGORITHM

IP traceback is a name given to any strategy for dependably deciding the starting point of a parcel on the Internet. Because of the putting stock in nature of the IP convention, the source IP address of a parcel isn't verifiedThus, the source address in an IP parcel can be adulterated (IP address caricaturing) taking into account disavowal of-benefit assaults (DoS) or one-way assaults (where the reaction from the casualty have is so notable that arrival bundles require not be gotten to proceed with the attack [clarification needed]).

The issue of finding the wellspring of a parcel is known as the IP traceback issue. IP traceback is a basic capacity for recognizing wellsprings of assaults and establishing assurance measures for the Internet.Most existing ways to deal with this issue have been customized toward DoS assault recognition. Such arrangements require high quantities of parcels to unite on the assault path(s). To XOR every hub framing an edge in the way with each other. Hub a supplements its IP address into the parcel and sends it to b.After being recognized at b, b XORs its address with the address of a. This new information element is called an edge id and lessens the required state for edge examining considerably.

Their next approach is to additionally take this edge id and part it into k littler sections. At that point, arbitrarily select a section and encode it, alongside the part balance with the goal that the right comparing piece is chosen from a downstream switch for preparing. At the point when enough parcels are gotten, the casualty can recreate the greater part of the edges the arrangement of bundles navigated (even within the sight of numerous aggressors)

Field	Type	Comment
c_name	varchar(15) NULL	
c_ip	varchar(15) NULL	
c_pwd	varchar(50) NULL	

Figure 1. Client table

Field	Type	Comment
file_name	varchar(100) NULL	
share_with	varchar(50) NULL	
full_name	varchar(500) NULL	
threshold_value	varchar(10) NULL	

Figure 2. File list

Field	Type
hack_ip	varchar(15) NULL
hack_info	varchar(50000) NULL

Figure 3. Hacker

VI. CONCLUSION

In this task, we tended to the testing research issue of system stream jumbling. We have recognized the dangers postured by the incremental arrival of system streams. In view of our past research, we have proposed a novel calculation to implement – jumbling to incremental discharges, and we have formally demonstrated the classification ensures gave by the new calculation. We have tentatively assessed our strategy with an extensive arrangement of genuine Cisco Net Flows accumulated inside an imperative Tier-II self-governing framework. Results demonstrated that our system saves the utility of system streams for various system investigation assignments.

VII. FUTURE WORK

Future research bearings incorporate the expansion of our formal model and safeguard method to various enemy models. Specifically, we go for tending to the case in which a foe has outside information about the transient correspondence example of particular has and may utilize this learning to reidentifyIP addresses in the watched history of jumbled streams.

VIII.REFERENCES

[1]. H. Aljifri, "IP traceback: a new denial-of-service deterrent?" IEEE Security and Privacy, vol. 1, no. 3, pp. 24–31, 2003.

[2]. M. Sung and J. Xu, "IP traceback-based intelligent packet filtering: a novel technique for defending against Internet DDoS attacks," IEEE Trans. on Parallel and Distributed Systems, vol. 14, no. 9, pp. 861–872, 2003.

[3]. Y. Xiang, W. Zhou, and M. Guo, "Flexible Deterministic Packet Marking: An IP Traceback System to Find the Real Source of Attacks," IEEE Trans. on Parallel and Distributed Systems, vol. 20, no. 4, pp. 567–580, 2009.

[4]. T. Law, J. Lui, and D. Yau, "You can run, but you can't hide: an effective statistical methodology to trace back DDoS attackers," IEEE Trans. Parallel Distrib. Syst., vol. 16, no. 9, pp. 799–813, 2005.

[5]. B. Al-Duwairi and M. Govindarasu, "Novel hybrid schemes employing packet marking and logging for IP traceback," IEEE Trans. on Parallel and Distributed Systems, vol. 17, no. 5, pp. 403–418, 2006.

[6]. A. Yaar, A. Perrig, and D. Song, "StackPi: New Packet Marking and Filtering Mechanisms for DDoS and IP Spoofing Defense," IEEE Journal on Selected Areas in Communications, vol. 24, no. 10, pp. 1853– 1863, 2006.

[7]. S. Yu, W. Zhou, R. Doss, and W. Jia, "Traceback of ddos attacks using entropy variations," IEEE Trans. on Parallel and Distributed Systems, vol. 22, no. 3, pp. 412–425, March 2011.

[8]. L. Cheng, D. M. Divakaran, W. Y. Lim, and V. L. L. Thing, "Opportunistic Piggyback Marking for IP Traceback," IEEE Transactions on Information Forensics and Security, vol. 11, no. 2, pp. 273–288, 2016.

[9]. V. Thing, M. Sloman, and N. Dulay, "Locating network domain entry and exit point/path for DDoS attack traffic," IEEE Trans. on Network and Service Management, vol. 6, no. 3, pp. 163–174, 2009.

[10]. C. Gong and K. Sarac, "A More Practical Approach for Single-Packet IP Traceback using Packet Logging and Marking," IEEE Trans. on Parallel and Distributed Systems, vol. 19, no. 10, pp. 1310–1324, 2008.

[11]. S. Alarifi and D. Wolthusen, Mitigation of cloudinternal denial of service attacks, in Service Oriented System Engineering (SOSE), 2014 IEEE 8th International Symposium on, Oxford, UK, 2014, pp. 478–483.

[12]. F. Barbhuiya, S. Biswas, N. Hubballi, and S. Nandi, A host based des approach for detecting arp spoofing, in Computational Intelligence in Cyber Security (CICS), 2011 IEEE Symposium on, Paris, France, 2011, pp. 114– 121.

[13]. D. Bruschi, A. Ornaghi, and E. Rosti, S-arp: A secure address resolution protocol, in Computer Security Applications Conference, 2003. Proceedings. 19th Annual, IEEE, 2003, pp. 66–74.

[14]. S. Y. Nam, D. Kim, and J. Kim, Enhanced arp: Preventing arp poisoning-based man-in-the-middle attacks, Communications Letters, IEEE, vol. 14, no. 2, pp. 187–189, 2010.

[15]. P. Pandey, Prevention of arp spoofing: A probe packet based technique, in Advance Computing Conference (IACC), 2013 IEEE 3rd International, Ghaziabad, India, 2013, pp. 147–153.

[16]. N. Hubballi, S. Biswas, S. Roopa, R. Ratti, and S. Nandi, Lan attack detection using discrete event systems, ISA Transactions, vol. 50, no. 1, pp. 119–130, 2011.

[17]. H. Neminath, S. Biswas, S. Roopa, R. Ratti, S. Nandi, F. Barbhuiya, A. Sur, and V. Ramachandran, A des approach to intrusion detection system for arp spoofing attacks, in Control & Automation (MED), 2010 18th Mediterranean Conference on, Marrakech, Morocco, 2010, pp. 695–700.

[18]. S. Y. Nam, S. Djuraev, and M. Park, Collaborative approach to mitigating arp poisoning-based man-inthemiddle attacks, Computer Networks, vol. 57, no. 18, pp. 3866–3884, 2013.

[19]. W. Lootah, W. Enck, and P. McDaniel, Tarp: Ticket-based address resolution protocol, Computer Networks, vol. 51, no. 15, pp. 4322–4337, 2007.

[20]. M. V. Tripunitara and P. Dutta, A middleware approach to asynchronous and backward compatible detection and prevention of arp cache poisoning, in Computer Security Applications Conference, 1999. (ACSAC99) Proceedings. 15th Annual, Phoenix, UK, 1999, pp. 303–309.