A Survey of Secure Network Infrastructure on Different IP Traceback Mechanism for Finding the Location of Spoofers

[1] Rajratan Gawai, [2] Varsha Bejgam, [3] Madhuri Sawant , [4] Sujitkumar Patole

[1,2,3,4] Computer Engineering, Savitribai Phule Pune University,
P.G.M.C.O.E Pune, Maharashtra, India

Abstract - It is long best-known attackers might use forged source internet protocol address to conceal their real locations. To capture the SPOOFERS, a variety of information processing TRACEBACK mechanisms have been projected. However, as a result of the challenges of preparation, there has been not a widely adopted information science TRACEBACK resolution, at least at the net level. As a result, the mist on the locations of SPOOFERS has never been dissipated until currently. This paper proposes (PIT) passive ip TRACEBACK that bypasses the deployment difficulties of information processing TRACEBACK techniques. PIT investigates net control Message Protocol error messages (named path backscatter) triggered by spoofing traffic, and tracks the SPOOFERS supported public available information (e.g., topology). in this way, PIT can find the SPOOFERS without any readying requirement. This paper illustrates the causes, collection, and the applied mathematics results on path disperse, demonstrates the processes and effectiveness of PIT, and shows the captured locations of SPOOFERS through applying PIT on the path scatter information set. These results will facilitate more reveal IP spoofing, that has been studied for long however ne'er well understood. though PIT cannot work in all the spoofing attacks, it may be the most useful mechanism to trace SPOOFERS before associate degree Internet-level TRACEBACK system has been deployed in real.

***Keywords* - Computer Network Management, Computer Network Security, Denial of Service (DoS), IP TRACEBACK.**

1. Introduction

IP SPOOFING, which suggests attackers launching attacks with forged provide ip addresses, has been recognized as a significant security problem on the internet for long [1]. By mistreatment addresses that are assigned to others or not assigned at all, attackers will avoid exposing their real locations, or enhance the effect of attacking, or launch reflection based attacks. variety of infamous attacks consider field spoofing, including SYN flooding, SMURF, DNS amplification etc. A DNS amplification attack that severely.

Manuscript received Feb, 2013.

Rajratan Gawai *Computer Engineering, PUNE University/ PGMCOE (e-mail:gawairg@gamil.com). PUNE, India, 9623792135*

varsha Bejgam*, Computer Engineering, PUNE University/ PGMCOE (e-mail: varbejgam@gmail.com) PUNE, India,.9028837019*

Madhuri Sawant*, Computer Engineering, PUNE University/PGMCOE(email:sawant.madhu2000@gmail.com).PUNE, India,7709132000*

Sujitkumar Patole, *Computer Engineering, PUNE University/PGMCOE(email:sujitkumarpatole17@gmai.com).PUNE,India, 9763396801,*

degraded the service of a prime Level Domain (TLD) name server is reportable in [2]. although there has been a popular standard info that DoS attacks are launched from boot nets and spoofing is no longer essential, the report of ARBOR on NANOG 50th meeting shows spoofing is still significant in determined DoS attacks [3]. Indeed, supported the captured scatter messages from UCSD Network Telescopes, spoofing activities are still often determined [4]. To capture the origins of IP spoofing traffic is of nice importance. As long as the real locations of SPOOFERS area unit not disclosed, they will not be deterred from launching any attacks. Even simply approaching the SPOOFERS, as an example, determining the AS's or networks they reside in, attackers can be placed in a smaller area, and filters may be placed closer to the attacker before attacking traffic get collective. The last however not the least, identifying the origins of spoofing traffic can help build a reputation system for AS's, which would be useful to push the corresponding ISPs to verify IP source address.

1.1 Motivation

However, to capture the origins of IP spoofing traffic on the internet is thorny. The research of identifying the origin of spoofing traffic is categorized in IP TRACEBACK. to build associate IP TRACEBACK system on the internet faces at least 2 vital challenges. the primary one is that the price to adopt a TRACEBACK mechanism in the routing system. Existing TRACEBACK mechanisms are either not wide supported by current trade goods routers(packet marking [5]), or will introduce significant overhead to the routers (Internet control Message Protocol (ICMP) generation [6], packet work [7]), particularly in superior networks. The second one is the difficulty to create internet service providers (ISPs) collaborate. Since the SPOOFERS might spread over every corner of the globe, a single ISP to deploy its own TRACEBACK system is nearly meaningless. However, ISPs, which area unit business entities with competitive relationships, are typically lack of specific economic incentive to facilitate clients of the others to trace aggressor in their managed AS's. Since the preparation of TRACEBACK mechanisms isn't of clear gains but apparently high overhead, to the best data of authors, there has been no deployed Internet-scale IP TRACEBACK system till now. As a result, despite that there are a unit a lot of IP TRACEBACK mechanisms planned and a large number of spoofing activities discovered, the important locations of SPOOFERS still remain a mystery. Given the difficulties of the IP TRACEBACK mechanisms deployment, we tend to are considering another direction :tracking the SPOOFERS while not deploying any additional mechanism. In another word, we tend to attempt to disclose the location of SPOOFERS from the traces generated by existing wide adopted functions on trade goods routers when spoofing attacks happen.

2. Our Work

Instead of producing another internet control TRACEBACK mechanism with improved pursuit capability, we tend to propose a novel answer, named Passive IP TRACEBACK (PIT), to bypass the challenges in deployment. Routers could fail to forward associate IP spoofing packet due to varied reasons, e.g., TTL exceeding. In such AS's, the routers might generate an ICMP error message (namely path backscatter) and send the message to the spoofed source address. as a result of the routers will be shut to the SPOOFERS, the path scatter messages might probably disclose the locations of the SPOOFERS Our work has the subsequent contributions:

1) This is the 1st article best-known that deeply investigates path scatter messages. These messages area unit valuable to assist perceive spoofing activities. Though Moore et al. has exploited scatter messages, which area unit generated by the targets of spoofing messages, to study Denial of Services (DoS), path scatter messages, that area unit sent by intermediate devices rather than the targets, haven't been utilized in TRACEBACK**.**

2) A sensible and effective IP TRACEBACK answer based mostly on path scatter messages, i.e., PIT, is proposed. PIT bypasses the preparation difficulties of existing IP TRACEBACK mechanisms and truly is already in force. although given the limitation that path scatter messages area unit not generated with stable risk, PIT cannot work in all the attacks, however it will work in a number of spoofing activities. At least it could be the most helpful TRACEBACK mechanism before an Autonomous System-level TRACEBACK system has been deployed in real.

3) Through applying PIT on the path scatter dataset, a range of locations of SPOOFERS are captured and presented. though this is not a complete list, it is the first best-known list disclosing the locations of SPOOFERS tendency to next describe a method for characteristic such similarities.

3. Related Work

Though PIT is used to perform ip TRACEBACK, it is very different from existing ip TRACEBACK mechanisms. PIT is inspired by a number of ip spoofing observation activities. Thus, the related work is composed by two parts. The first briefly introduces existing ip TRACEBACK mechanisms, and the second introduces the ip spoofing observation activities.

3.1. IP Traceback

A. information processing TRACEBACK IP TRACEBACK techniques square measure designed to disclose the important origin of information processing traffic or track the trail. Existing information processing TRACEBACK approaches are usually classified into 5 main categories: packet marking, ICMP TRACEBACK, logging on the router, link testing ,overlay, and hybrid tracing. Packet marking strategies need routers modify the header of the packet to contain the info of the router and forwarding call. so the receiver of the packet can then reconstruct the trail of a packet (or Associate in Nursing assaultive flow) from the received packets. There are two classes of packet marking schemes: probabilistic packet marking and settled packet marking. Packet marking methods are generally considered to be lightweight because they do not price storage resource on routers and the link bandwidth resource. However, packet marking is not a wide supported operate on routers; so, it's tough to switch packet marking TRACEBACK at intervals the network. Different from packet marking methods, ICMP TRACEBACK , generates addition ICMP messages to a collector or the destination. The ICMP messages can be used to reconstruct the assaultive path. as Associate in Nursing example, if iTrace is enabled, routers generate ICMP samples to destinations with a certain probability. The disadvantage of ICMP TRACEBACK is considerable any traffic are going to be generated to consume the already stressed metric resource.

Moreover, when the attack is against the data live of the victim, the inflated traffic will create the attack a lot of serious. ICMP generation can be performed by the processor, however vital overhead will be introduced to the processor. Attacking path is also reconstructed from go browsing the router when router makes a record on the packets forwarded . Bloom filter is employed to cut back the amount of bits to store a packet. yet, to realize a low enough collision probability in current high-speed networks, the storage cost is still overlarge for product routers. Link testing is Associate in Nursing approach that determines the upstream of assaultive traffic hop-by-hop whereas the attack is ongoing. A controlled flooding mechanism supported activity UDP Charge request flooding iteratively on the victim stock-still tree to see the consequences on assaultive traffic is planned in . Because of the massive scale of the online, this approach is hard to perform at the net level. YAO et al.: revealing THE LOCATIONS OF information processing SPOOFERS 473 Center Track proposes offloading the suspect traffic from edge routers to special following routers through a overlay network. although such a mechanism can scale back the requirement over strung routers, the management of the tunnels and the overlay network are going to be considerably increase the network management overhead. proposes building Associate in Nursing AS-level overlay to trace SPOOFERS. it's found if a whole lot of AS's will be a part of the overlay network, the SPOOFERS is accurately placed. However, the challenge in observe is however to make the AS's collaborate. The intra-domain version of this work will avoid this downside, however it's necessary to update routers to adopt modification on OSPF. The on top of mechanisms is combined to attain higher tracing capability and/or scale back the value. There ar variety of hybrid mechanisms use each packet marking and logging . although the overhead on routers is reduced, they need the routers to support each mechanisms; thus the barrier to adopt them is over adopting one mechanism. Though there are an oversized variety of promising TRACEBACK mechanisms, there's still a protracted thanks to get the planned mechanisms wide deployed, particularly at the net level. Currently, there is still lack of a ready mechanism to trace the SPOOFERS.

3.2. IP Spoofing Observation

Network telescope [4] may be a basic technique for passive observation of spoofing activities on the internet. Network telescope captures non-solicited messages, which area unit in the main generated by victim attacked by traffic with source prefix set in the scope closely-held by the telescope. Then, it can be determined a part of nodes which area unit attacked by spoofing traffic. Currently, the largest scale telescope is the CAIDA UCSD telescope, which owns 1/256 of all the ip addresses and is in the main used to observe DDoS activities and worms. Moore el at. conferred a method namely “back-scatter analysis” that uses the feature of DoS attacks based mostly on traces collected by the network telescope. though ICMP error messages area unit mentioned in the paper, it does not additional investigate these messages to trace SPOOFERS. CAIDA provides publicly accessible information. The main analysis and experimental work of this article area unit performed on the information provided by CAIDA The MIT SPOOFER Project tries to disclose which networks area unit able to launch spoofing based mostly attacks. Volunteer participants install a shopper that tests the spoofing ability of their hosts and networks. The statistic result shows 6700 ASs out of 30205 do not filter spoofing. A recent report from Arbor network based mostly on additional than 5000 attacks shows an intriguing result [3]. unreasonable per IP traffic of 4Gbps is determined in 100% attacks, and significant rate of TCP connections area unit launched from just a few validated hosts. though this is not direct evidence of spoofing, it suggests spoofing could be used in such attacks.

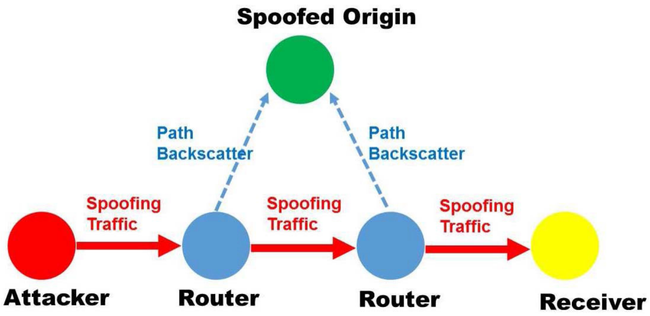

Fig. 1. The scenario of path backscatter generation and collection

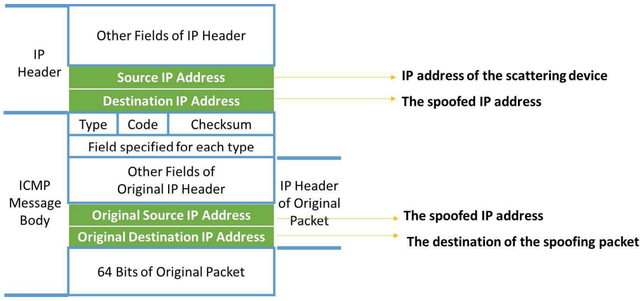
Other Fields of IP Header
IP Header
Source IP Address
Destination IP Address
Type
Code
Checksum
Field specified for each type
ICMP Message Body
Other Fields of Original IP Header
IP Header of Original Packet
Original Source IP Address
Original Destination IP Address
64 Bits of Original Packet
IP address of the scattering device
The spoofed IP address
The spoofed IP address
The destination of the spoofing packet

Fig. 2. The format of path backscatter messages

4. Path Backscatter

A. Overview

Not all the packets reach their destinations. A network device might fail to forward a packet due to numerous reasons. Under bound conditions, it might generate associate degree ICMP error message, i.e., path scatter messages. the trail scatter messages are going to be sent to the supply IP address indicated within the original packet. If the supply address is solid, the messages will be sent to the node WHO truly owns the address. This means the victims of reflection primarily based attacks, and the hosts whose addresses area unit utilized by SPOOFERS, area unit probably to collect such messages. This state of affairs is illustrated in Fig. 1. As specific by RFC792 , the format of the path backscatter messages, is illustrated in Fig. 2. each message contains the source address of the reflective device, and the ip header of the original packet. Thus, from every path backscatter, we have a tendency to will get 1) the ip address of the reflecting device which is on the path from the aggressor to the destination of the spoofing packet; 2) the ip address of the original destination of the spoofing packet. The original IP header conjointly contains alternative valuable data, e.g., the remaining TTL of the spoofing packet. Note that as a result of some network devices might perform address rewrite (e.g., NAT), the original supply address and the destination address might be different.

TABLE I
PATH BACKSCATTER CLASSES

Type	Class
Time Exceeded	TIMXCEED_INTRANS
Destination Unreachable	UNREACH_FILTER_PROHIB, UNREACH_NET_PROHIB, UNREACH_HOST_PROHIB, UNREACH_HOST, UNREACH_NET, UNREACH_NEEDFRAG
Source Quench	SOURCEQUENCH
Redirect	REDIRECT_HOST, REDIRECT_NET
Parameter Problem	PARAMPROB

B. Classes and Causes of Path Backscatter

Classes and Causes of Path backscatter Path backscatter messages can be triggered for various reasons. based on RFC792, there can be totally 5 types of path backscatter messages, as listed in the following sections. There are variety of codes associated with each kind. The combination of kind and code specifies the cause that the router decides to send the ICMP message. we name the combination of type and code by class. we use the names defined in [32] to denote the classes of path backscatter messages. In the path backscatter dataset from CAIDA [4], totally 23 classes of path backscatter messages are found, 11 of them are listed in Table I. Messages belonging to the other 12 types are very rare. we do not find all the possible classes. We try to explain the causes of the classes of path backscatter messages listed in Table I based on analyzing the dataset.

Especially, we try to make out the reasons that they are generated near the SPOOFERS. However, although we have tried our best to explore the possible reasons, considering the sophistication of attacks and the complexity of networks, we do not claim we found all the (or even the main) reasons for the generation of the messages. It should be noted that in general a majority of path backscatter messages are generated near the victim. However, considering the huge number of spoofing messages, if only a small ratio of them trigger path backscatter messages close to the SPOOFER, the total path backscatter dataset will be valuable. Even for the path backscatter messages generated far away from the SPOOFERS, their generation locations are at least closer to the SPOOFERS than the victims. Thus, they can be used in the first step of TRACEBACK.

1) Time Exceeded: TIMXCEED_INTRANS messages are triggered by packets with zero TTL value. Such messages are the most common path backscatter messages. Though the attackers can set the initial TTL value to be large enough to avoid triggering such messages, they may intentionally send packets with small initial TTL values, which trigger routers on the path to generate TTL exceeding messages to consume the processor resource of the router. Generally such attacks target the routers instead of hosts. we also find the attack against a host and the attack against the nearby routers of the target host may be combined.

We think the attacker may want to degrade the forwarding performance of the routers near the target host, and then less aggregated spoofing traffic are require to prevent legitimate traffic from reaching the host. Besides, to determine the correct initial TTL value to make sure the TTL exceeding events happen on the targeted router, the attacking hosts should perform some traces. The traces using real address can be cloaked with a number of traces using forged addresses to avoid tracking. this could be the reason that we found a number of TIMXCEED_INTRANS messages from cascading routers in the dataset.

2) Destination Unreachable: UNREACH_FILTER_ PROHIB, UNREACH_NET_PROHIB and UNREACH_HOST_PROHIB messages are mainly triggered by filtering mechanisms deployed between the spoofing origin and the victim, e.g., Access control List (ACL). A result of the mit SPOOFER project shows 80th filters are deployed one ip hop from the source, and over 95th of blocked packets are filtered at the source AS.

Thus, such messages may be from the gateways near the SPOOFERS. It ought to be noted that at least part of the spoofing traffic from the SPOOFERS has been filtered. Considering the filtering granularity may be coarse, the remaining spoofing messages will still reach the victims. Thus, TRACEBACK in such a situation continues to be valuable. UNREACH_HOST and UNREACH_NET messages are generated if there is no route to the destination. Such messages are mostly triggered by attacking traffic launched against a private or unallocated address prefix. Whenever a SPOOFER sends packets to a private address, if the SPOOFER is attached to a public network or the victim address is not in the same private network of the SPOOFER, such ICMP messages will be generated when the spoofing packets arrive at the DFZ (Default-free Zone). we find a large number of such messages whose original destination is a private address. Such messages may be triggered by attacks against hosts behind NAT or in VPN.

UNREACH_NEEDFRAG messages are generated if the size of the attacking packets are larger than the MTU of a hop on the path, but the Don’t Fragment flag is set. Such messages may be generated due to attacks against the routers. Besides, we think such messages can be triggered occasionally. Attackers use large packet to consume the bandwidth of the target. due to forged addresses are used, the attackers cannot get the ICMP message and are unaware of that the attacking packets are dropped on path.

3) source Quench: SOURCEQUENCH messages are generated when the router has no buffer to queue the original packet. It can be resulted from the aggregated attacking traffic is too large to be forwarded by the router. in general such messages are generated near the victim. However, if there are a large number of attackers in the same network/AS, it is possible to trigger such messages on the gateways near the attackers.

4) Redirect: REDIRECT_HOST and REDIRECT_NET messages are generated if the spoofing origin has two or more gateways and a gateway, G1, finds the spoofing packet should be sent to another gateway, G2, as this is the shortest path. As multi-homed networks become common, such messages may be generated with higher probability. because this message is generated by gateways near the spoofing origin, it is particularly helpful to find the location of the origin. As specified in RFC792, G1 should check the address of the packet and G2 are in the same network. However, the dataset is collected by a network telescope, and apparently any G2 and the address of a network telescope must not in the same network. it may be due to miss configuration of implementations inconsistent with the standard.

5) Parameter Problem: PARAMPROB messages are generated if the router finds a problem with the header parameters in the original packet. Such messages are rare in the dataset. Possibly they are triggered by malformed attacking packets or just some type of attack.

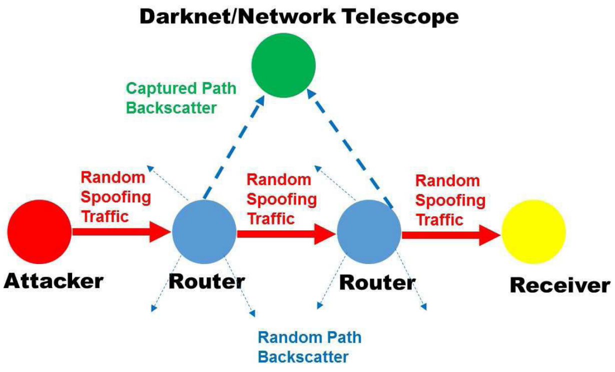

Fig. 3. Network telescope captures path backscatter in *random spoofing* attacks.

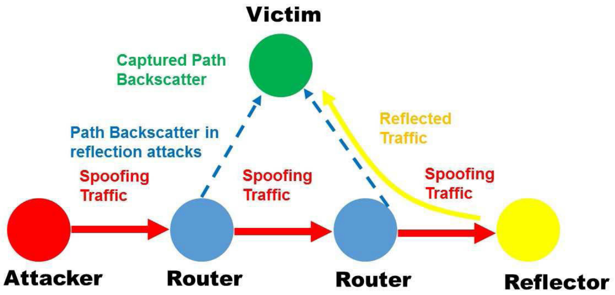

Fig. 4. The victim captures path backscatter in *reflection attacks.*

.

A. Basic following Mechanism

Whenever a path backscatter message whose source is router r (named reflector) and the original destination is captured, the most direct inference is that the packet from offender to should bypass r . we use a very simple mechanism in spoofing origin following. The network is abstracted as a graph G(V, E), where V is the set of all the network nodes and E is the set of all the links. A network node can be a router or an AS, depending on the tracking scenario. From each path backscatter message, the node r, r ∈ V that generates the packet and therefore the original destination od, od ∈ V of the spoofing packet can be got. Denote the location of the SPOOFER, i.e., the nearest router or the origin AS, by a, a ∈ V. We make use of path information to help track the location of the SPOOFER. Use path(v, u) to denote the sequence of nodes on one of the path from v to u, and use P AT H (v, u) to denote the set of all the paths from v to u. Use φ(r, od) to denote the set of nodes from each of which a packet to od can bypass r,i.e., φ(r, od) = r ∈ path(v, od), path(v, od) ∈ P AT H (v, od). φ(r, od) actually determines the minimal set which must contain the SPOOFER. we name the result set of φ(r, od) by suspect set. As illustrated in Fig. 5, if all the paths are loop-free, the suspect set determined by the path backscatter message is . If the topology and routes of the network are known, this mechanism can be used to effectively confirm the suspect set. for instance, an ISP can make this model to locate SPOOFERS in its managed network. However, for many AS's, the one who performs tracing does not know the routing choices of the other networks, which are personal data. Moreover, the topologies of most of the AS's are unknown to the public. within the following sections, we discuss a way to track while not routing data in section IV-B, and how to trace with neither topology nor routing information in section IV-C.

B. Trailing Without Routing Data

It is possible to induce the topology of the network in some TRACEBACK scenarios. for instance, the router-level topology can be got from trace route, and also the AS-level topology can be inferred from the BGP data and supplementary means. Besides, variety of AS's create public their topologies [34]. However, the routes of a network are continually treated as business secret and are non-public. in this section, we discuss how to perform PIT if topology is known but the detailed routing is unknown. It should be noted that if the routing has not constraint, packets from any node v ∈ V to od will bypass any intermediate node r. Then the following is senseless. as luck would have it, it is not the case in real networks. we build use of two assumptions on the routing respectively:

1) Loop-Free Assumption: This assumption states there is no loop in the methods. This assumption forever holds unless miss configuration or the routing has not converged.
2) Valley-Free Assumption: This assumption states there should be no natural depression in the AS level ways [35]. Though the increased quality of AS relationship has reduced the catholicity of this assumption, it is still the foremost common model of AS level routing. In the following subsections, we discuss how to perform PIT based on each of the belief severally.

C. Collection of Path Backscatter Messages

Though path backscatter can happen in any spoofing based attacks, it is not always possible to collect the path backscatter messages, as they are sent to the spoofed addresses. We classify spoofing primarily based attacks into four classes, and discuss whether path backscatter messages can be collected in each category of attacks.

1) Multiple Sources, Single Destination: In such attacks,

the source address of spoofing packets is chosen from a set of candidate addresses. particularly, this set contains all the addresses. Such attacks are named random spoofing. Random spoofing is typically used to deplete the resource of the target, e.g., SYN flooding. Network Telescopes (or dark nets) can be used to capture path backscatter messages in random spoofing attacks. As illustrated in Fig. 3, in random spoofing attacks, the path backscatter messages are sent to the randomly spoofed addresses. because the addresses owned by network telescopes can be used in random spoofing attacks, the network telescopes are possibly able to capture part of the path backscatter messages. Potentially, volunteers can make use of packet capturing tools to collect non-solicited messages, and then they can help in TRACEBACK rather than completely relying on the network telescopes. However, this topic is beyond the scope of this work.

V. PIT: T Wrenching Supported Path Backscatter

We name the IP TRACEBACK solution based on exploiting path backscatter messages by Passive scientific discipline TRACEBACK (PIT). PIT is actually composed by a set of mechanisms. The basic mechanism, which is predicated on topology and routing information, is illustrated in section IV-A. However, generally the routing information is tough to realize. The mechanisms work in case the routing information in unknown are specified in section IV-B. In terribly special AS's, it is possible to trace the SPOOFER without topology and routing information. The mechanism for these AS's is discussed in section IV-C.

5. Conclusion

We attempt to dissipate the mist on the locations of SPOOFERS based on investigation the path backscatter messages. In this article, we projected Passive ip TRACEBACK (PIT) which tracks SPOOFERS based on path backscatter messages and public available data. we illustrate causes, collection, and statistical results on path backscatter. we specified how to apply PIT once the topology and routing are both known, or the routing is unknown, or neither of them are known. We given two effective algorithms to apply PIT in large scale networks and proofed their correctness. we demonstrated the effectiveness of PIT primarily based on deduction and simulation. We showed the captured locations of SPOOFERS through applying PIT on the path backscatter dataset. These results can help further reveal ip spoofing, that has been studied for long but never well understood.

References

[1] S. M. Bellovin, “Security problems in the TCP/IP protocol suite,”ACM SIGCOMM Comput. Commun. Rev., vol. 19, no. 2, pp. 32–48,Apr. 1989.

[2] ICANN Security and Stability Advisory Committee, “Distributed denial of service (DDOS) attacks,” SSAC, Tech. Rep. SSAC Advisory SAC008,Mar. 2006.

[3] C. Labovitz, “Bots, DDoS and ground truth,” presented at the 50th NANOG, Oct. 2010.

[4] *The UCSD Network Telescope*. [Online]. Available:http://www.caida.org/projects/network_telescope/

[5] S. Savage, D. Wetherall, A. Karlin, and T. Anderson, “Practical network support for IP TRACEBACK,” in Proc. Conf. Appl., Technol., Archit.,Protocols Comput. Commun. (SIGCOMM), 2000, pp. 295–306.

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

[7] A.C. Snoeren *et al.*, “Hash-based IP TRACEBACK,” *SIGCOMM Comput. Commun. Rev.*, vol. 31, no. 4, pp. 3–14, Aug. 2001.

[8] D. Moore, C. Shannon, D. J. Brown, G. M. Voelker, and S. Savage,“Inferring internet denial-of-service activity,” *ACM Trans. Comput. Syst.*, vol. 24, no. 2, pp. 115–139, May 2006. [Online]. Available: http://doi.acm.org/10.1145/1132026.1132027.

[9] M. T. Goodrich, “Efficient packet marking for large-scale IP TRACEBACK,”in Proc. 9th ACM Conf. Comput. Commun. Secur. (CCS), 2002, pp. 117–126.

[10] D. X. Song and A. Perrig, “Advanced and authenticated marking schemes for IP TRACEBACK,” in Proc. IEEE 20th Annu. Joint Conf. IEEE *Comput. Commun. Soc. (INFOCOM)*, vol. 2. Apr. 2001, pp. 878–886.

[11] A.Yaar, A. Perrig, and D. Song, “FIT: Fast internet TRACEBACK,” in *Proc.* IEEE 24th Annu. Joint Conf. IEEE Comput. Commun. Soc. (INFOCOM), vol. 2. Mar. 2005, pp. 1395–1406.

[12] J. Liu, Z.-J. Lee, and Y.-C. Chung, “Dynamic probabilistic packet marking for efficient IP TRACEBACK,” *Comput. Netw.*, vol. 51, no. 3,pp. 866–882, 2007.

[13] K. Park and H. Lee, “On the effectiveness of probabilistic packet marking for IP TRACEBACK under denial of service attack,” in *Proc. IEEE* 20th Annu. Joint Conf. IEEE Comput. Commun. Soc. (INFOCOM),vol. 1. Apr. 2001, pp. 338–347.

[14] M. Adler, “Trade-offs in probabilistic packet marking for IP TRACEBACK,” *J. ACM*, vol. 52, no. 2, pp. 217–244, Mar. 2005.

[15] A. Belenky and N. Ansari, “IP TRACEBACK with deterministic packet marking,” *IEEE Commun. Lett.*, vol. 7, no. 4, pp. 162–164, Apr. 2003.

[16] Y. Xiang, W. Zhou, and M. Guo, “Flexible deterministic packet marking:

An IP TRACEBACK system to find the real source of attacks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 20, no. 4, pp. 567–580, Apr. 2009.

[17] R. P. Laufer *et al.*, "Towards stateless single-packet IP TRACEBACK," in *Proc. 32nd IEEE Conf. Local Comput. Netw. (LCN)*, Oct. 2007 I pp. 548–555. [Online]. Available: http://dx.doi.org/10.1109/ LCN.2007.160

[18] M. D. D. Moreira, R. P. Laufer, N. C. Fernandes, and O. C. M. B. Duarte, "A stateless TRACEBACK technique for the origin of attacks from a single packet," in *Proc. IEEE Int Conf.Commun. (ICC)*, Jun. 2011, pp. 1–6.