A New Survey for Evaluation of Various Spoofing Defences

Yasoda Krishna Kuppili [#1], Venkata Ramana Adari [*2]

[#1]M.Tech Scholar, [*2] Professor & HOD
Department of Computer Science & Engineering,
Vizag Institute of Technology Engineering College,
Dakamarri, Visakhapatnam Dist, AP, India.

Abstract

This is a survey paper mainly perform analysis on evaluation of various IP spoofing defences which impart a major role in improving network security. We mainly evaluated three main defenses that filter spoofed traffic which have been proposed to date in this paper, among them two filters are designed for end-network deployment, while one filter assumes some collaboration with core routers for packet marking or filtering. Because each defense has been evaluated in a unique setting, the following important questions remain unanswered by the network users: 1) Can end to end networks effectively protect themselves or is core support necessary? 2) Which defense performs best assuming sparse deployment? 3) How to select core participants to achieve best protection with fewest deployment points? In this paper, we gave answers the above questions by: 1) formalizing the problem of spoofed traffic filtering and defining novel effectiveness measures, 2) observing each defense as selfish (it helps its participants) or altruistic (it helps everyone) and differentiating their performance goals, 3) defining optimal core deployment points for defenses that need core support, and 4) evaluating all defenses in a common and realistic setting.

Keywords:

IP spoofing, Packet Filtering, Spoofing Defense Evaluation, DDoS attacks.

1. Introduction

IP spoofing has been used in distributed denial-of-service (DDoS) attacks and intrusions since from many years. These spoofing attacks are also necessary for reflector DDoS attacks, where servers reply to spoofed requests and these replies overwhelm the victim whose address was misused, we will now formulate these attacks scenarios in two ways.

A. Spoofing Is an Open Problem Scenario

Many researchers believe that spoofing is not an open problem scenario based on the following observations: (1) the Spoofer project's research [1] that estimates that 85% of networks deploy the ingress filtering techniques and (2) prevalence of non-spoofed DDoS attacks. We now argue to the contrary which was discussed above.

In the Spoofer project research [1] many centralized network volunteers that were connected in distributed process, download software that spoofs packets to a centralized monitoring machine. From various packet losses during transmission, the authors infer the existence of ingress filtering [2] in the volunteer's individual networks, which drops outgoing traffic which carry addresses not assigned to the deploying network. Spoofer research work measurements show that around 85% of networks participating in the research project mainly deploy ingress filtering. Because the total number of participating hosts in this research on work is in the low thousands, these results cannot be readily extrapolated to the entire Internet. Further, even if

only 15% of all network users allowed spoofing, they could still generate unlimited network spoofed and reflected traffic toward any target.

Many DDoS attackers send valid application requests as input, and do not use spoofing, but a large number still do. In this paper, our analysis of backscatter traffic [3] inferred that there were several hundreds of DDoS attacks with spoofing affected per day. Another major popular trend which was currently used is use of reflectors for recursive DNS attacks [4], which mandates spoofing process.

B. Our Major Focus

Many approaches and research work have been proposed to handle IP spoofing during specific attacks that occur in networks, or to trace back the original sources of spoofed traffic. In this current study we mainly focus only on approaches that work in a generic, single-step, packet-filter manner. These three approaches associate each IP address with some parameter (e.g., a route to the filter, a secret mark, etc.) via a parameter table which we take. When a packet arrives from a source, the chosen parameter's value is inferred from that parameter table, and compared to the value in the parameter table, while doing this mismatching packets are considered as spoofed packets.

These approaches are mainly generic in nature because their goal is only to filter spoofed packets, regardless of the security threat that generated the attack. They are single-step in nature because there is no interactive communication with an alleged packet source when a suspicious packet is received. Finally, all these approaches work in a integrated packet-filter manner – where the parameter table can be viewed as a set of firewall rules that specify allowed traffic, and the default deny rule.

Till to date, nearly seven approaches have been proposed that fit for our scope. In this paper we are going to compare and use three approaches both in End-to-End Networks and router based networks. A Hop-Count Filter (HCF) [5] mainly associates a source node with a router hop count between it and the filter. A Route Based Filter (RBF) [6] mainly associates a source with the previous hop route traversed by this source's packets. An inter-domain packet filter (IDPF) [7] mainly associates a source with the set of feasible previous hops that could carry its traffic.

All these defenses were evaluated by their authors research work by using custom performance measures and in a customized setting, which gives comparison

If a defense does not offer good protection under any assumptions it is unrealistic in nature and should not be pursued. If no defense offers good protection in isolated deployment, the next possible strategy is to investigate an Internet-wide deployment that should help everyone. If a defense performs poorly in an optimal deployment on a small number of well-chosen networks, it is useless and should not be pursued.

2. Analysis of Defense Effectiveness

Let us assume that IProut and IPv4 be the set of globally routable and all IP addresses, respectively. During the research analysis, we mainly observe the Internet as a directed, connected graph whose nodes are routers and autonomous heterogeneous systems, and whose links are mainly determined by their available routing protocols. We consider packets sent from a source address s € IProut to destination address d € IProut, d = s, spoofing the address p € IPv4, p = s. In the research analysis, we investigate the factors that determine the portion of possible {s, d, p} combinations filtered by some defense.

2.1 Single Filter Effectiveness

Here in this single filter, we mainly assume that some spoofing defense is deployed only at a node F. For each and every source/destination pair {s; d} we define the boolean type mapping hit F (s, d), to be 1 if the path from s to d contains F, and 0 otherwise. All these approaches of interest detect spoofed packets by building a table that associates

source addresses with some parameter as summarized in Table 1. Mapping of sources to parameters is frequently many-to-one, due to aggregation of source addresses in the table or due to sharing of paths between sources those results in sharing of parameter values. Thus, in our research work F will be able to identify the spoofed packets only for some distinct variable s and p combinations, when the parameter values associated with these addresses are different. We express this similarities through the mapping diffF (s, p), which is 1 if F can detect s spoofing p, and 0 otherwise.

A packet which was sent from s to d, spoofing p, will be filtered out by a filter F iff the packet hits filter F and F can able to distinguish between s and p, that is only if both hitF (s, d)= 1 and diffF (s, p)= 1. We define the filtering function:

$$filter_F(s,d,p) = hit_F(s,d) \cdot diff_F(s,p),$$

And we also define the filter impact factor of F as the number of all possible {s, d, p} combinations from s to d and p that are filtered by F:

$$impact_F = \sum_{s \in IP_{rout}} \sum_{d \in IP_{rout}} \sum_{p \in IPv4} filter_F(s,d,p). \quad (1)$$

We can also project the impact of any filter as a composition of its strength and popularity at the source level of the node:

$$impact_F = \sum_{s \in IP_{rout}} pop_F(s) \cdot strength_F(s). \quad (2)$$

Thus, both the strength and popularity plays a very important role in defining a filter's impact factor, and interact at the single source granularity. To have a very good and very high impact, a filter need not only be popular and strong enough, but also it must be popular and strong for the same sources.

TABLE 1
Parameter Associated with a Source IP

Defense	Parameter
HCF	Hop Count.
RBF	One Previous Hop.
IDPF	Set of feasible Previous Hops

2.2 Multiple Filters Effectiveness

In order to analysis multiple filters scenario, let us now assume that a set of N filters FS = F_1 ... F_N is deployed and we investigate the collective impact of this filtering. The joint filtering function is defined as follows:

$$filter_{FS}(s,d,p) = \bigvee_{F \in FS} filter_F(s,d,p) = \bigvee_{F \in FIL(s,d)} diff_F(s,p), \quad (3)$$

Where W clearly denotes a logical or operation and the mapping of FIL(s, d) returns the set of filters traversed by traffic from s to d. Equation (3) clearly says that a packet from source s to destination d, spoofing p, will be filtered if it hits at least one filter that can distinguish between source s and spoofing p. The joint filter impact of FS is defined as follows:

$$impact_{FS} = \sum_{s \in IP_{rout}} \sum_{d \in IP_{rout}} \sum_{p \in IPv4} filter_{FS}(s,d,p), \quad (4)$$

$$= \sum_{s \in IP_{rout}} \sum_{d \in IP_{rout}} \sum_{p \in IPv4} \bigvee_{F \in FIL(s,d)} diff_F(s,p), \quad (5)$$

$$= \sum_{s \in IP_{rout}} \sum_{d \in IP_{rout}} \left| \bigcup_{F \in FIL(s,d)} \{p | diff_F(s,p) = 1\} \right|. \quad (6)$$

For some filter set X, we define the joint filter strength per source s as:

$$strength_X(s) = \left| \bigcup_{F \in X} \{p | diff_F(s,p) = 1\} \right|. \quad (7)$$

The impact factor can then be expressed as the filter strength of set FIL(s, d) per source, aggregated across all sources s and destinations d:

$$impact_{FS} = \sum_{s \in IP_{rout}} \sum_{d \in IP_{rout}} strength_{FIL(s,d)}(s). \quad (8)$$

3. Defense Performance Measures

Spoofing dimensions are mainly classified into three types. They are as follows:

1. Spoofed addresses (p),
2. Sources of spoofed traffic (s), and
3. It's Targets (d).

The main goal of any spoofing defense method is to provide protection to target nodes against spoofed and reflected traffic. We express this notion through the target protection (TP) and reflector attack protection (RAP) measures, respectively.

Whenever we try to evaluate these measures, we will first assume that the remaining two dimensions—{s, p} where s is source and p spoofed address in case of target protection and {s, d} in case of reflector attack protection are distributed uniformly at random in the IPv4 space. We mainly do this because we cannot directly predict which addresses may be initially spoofed and toward which targeted nodes. The observed distribution of Internet attackers is always not uniform, with attackers maximum showing strong preference toward a few network nodes that are poorly secured in nature [8], [9]. Our research measures express very good protection offered to any victim in this scenario. Further, we also evaluate how lucrative attack locations are after a defense is deployed via the attacker impairment (AI) measure.

3.1 Target Protection Measure

TP measure for any node x defines the number of {s, p} combinations that will be filtered en route to destination x.

$$TP(x) = \sum_{s \in IP_{rout}} \sum_{p \in IPv4} filter(s, x, p) = \sum_{s \in IP_{rout}} strength_{FIL(s,x)}(s).$$

TP(x) mainly depends on the number of filters hit by traffic from various sources to x, and the filter strengths. For many defenses in real time , TP measure for filter-deploying networks will be more higher than for normal legacy networks because all spoofed traffic sent to a filter-deploying network hits at least one filter.

3.2 Reflector Attack Protection Measure

RAP measure for node x defines the number of {s; d} paths on which packets spoofing x will be filtered out

$$RAP(x) = \sum_{s \in IP_{rout}} \sum_{d \in IP_{rout}} filter(s, d, x) = \sum_{s \in IP_{rout}} \sum_{d \in IP_{rout}} \bigvee_{F \in FIL(s,d)} diff_F(s, x).$$

RAP(x) mainly depends on the path coverage (FIL(s, d)) and the filters' ability to detect spoofing of the address x.We will show that isolated defenses and collaborative defenses that are deployed randomly and sparsely cannot provide good protection against reflector attacks, because they do not have sufficient path coverage.

3.3 Attacker Impairment Measure

AI measure for node x defines the number of {d, p} combinations in spoofed traffic generated by x that will be filtered. It expresses the impairment of node x's spoofing ability, if it were recruited as a bot.

$$AI(x) = \sum_{d \in IP_{rout}} \sum_{p \in IPv4} filter(x, d, p) = \sum_{d \in IP_{rout}} \sum_{p \in IPv4} \bigvee_{F \in FIL(x,d)} diff_F(x, p).$$

AI(x) will be high if x's traffic crosses a large number of filters that can distinguish x from many addresses. Nodes that reside in vicinity of filters should be less lucrative for attackers since there is a good chance that many of their routes cross a filter. We will call a node very impaired if AI >= 0.95 and moderately impaired if 0.95 >AI(x) >= 0.9.

TABLE 2
Elementary Cost Components

Category	Variable	Component Description	Cost
Per-packet	l	Table lookup and comparison with some packet value	8 ns
	m_d	Insert a deterministic mark into packet	8 ns
	m_c	Insert a cryptographic mark into packet	1 μs
	v_c	Verify a cryptographic mark	250 ns
Storage	N_{AS}	Number of ASes in the Internet	30 K
	N_T	Number of (adequately aggregated) entries in the parameter table	200 K
	N_l	Number of links at an AS	280
	N_p	Number of prefixes in an AS	5
	N_{ASh}	Number of AS hops from source to destination	4

4. Defense Evaluation Results

We first present results for each defense separately, and then aggregate them into a single table at the end of this section.

4.1 Hop-Count Filtering (HCF)

HCF associates each of its sources with the router hop count between it and the filter (F). Hop counts are inferred from the TTLs in packets belonging to established TCP connections. Since we mainly reproduce Internet topology at the AS-level, we mimic router-level hop counts by associating a random hop count chosen from [1], [2], [3], [4] inclusively, with each AS-AS link. This strategy produces Gaussian hop-count distribution, observed in the real Internet [5], and end-to-end hop counts lie within observed limits.

Normalized strength of a hop-count filter is: $\text{strength}_F = \sum_{P \in IProut} \text{Hop}(p)/|IProut|^2$, where Hop (p) is the number of all sources whose hop count differs from p's hop count. Because the node distances on Internet-like graphs, that exhibit power-law distribution of node degrees, follow the Gaussian distribution [11], the strength of HCF filters should be fairly constant and high.

HCF was proposed as a selfish defense. Fig. 2a shows the TP and RAP measures in isolated deployment. The TP measure is consistently high, because of high filter strength, making HCF an ideal selfish defense. The RAP measure, on the other hand, is low since a single filter does not achieve sufficient path coverage to lower its danger from reflector attacks.

HCF can be transformed into an altruistic defense by applying the same filtering approach to the transit traffic. TP and RAP measures for altruistic deployment are shown in Figs. 2b and 2c, respectively. TP and RAP measures are very high for optimal deployment and the top 50 HCF filters offer 95 percent protection to everyone. Filters' TP measure is high in sparse deployment offering good deployment incentive, but their RAP measure remains low until sufficient path coverage is achieved. The vertex cover deployment for HCF offers a slightly higher protection (one-three percent) than the optimal deployment, but with many more deployment points. Around four percent of IPs is very impaired with regard to hosting attackers, and 71 percent are moderately impaired. Thus, HCF makes around 3/4 of IP addresses unattractive for hosting attackers.

The cost of hop-count filtering consists of per-packet lookup (<8 ns) and 1.2 MB of storage to record hop count for all source prefixes, assuming that we need 5 B to record the prefix and 1 B for hop-count value. A probing attacker can learn the correct TTL value for a given source address, and a given destination [5]. Thus, HCF is vulnerable to the probe-fix attack. An attacker located on the path of

the traffic can replay all packets to their original destination— replaying them to another destination may result in a wrong hop count if the real source takes a different path than replayed traffic. Therefore, HCF is also vulnerable to the replay-fix attack.

4.2 Route-Based Filtering

RBF associates each source with the previous hop its traffic crosses to reach the filter. It was proposed as an altruistic defense and its authors recommended a vertex cover deployment [6]. Normalized strength of an RBF filter is $\text{strength}_F = \sum_{P \in IProut} pH(p)/|IProut|^2$, where PH(p) is the number of sources whose previous hop at F differs from p's previous hop. ASes with more neighbors should have a higher filtering strength because they have a higher diversity of potential previous hop values.

We show the RBF performance in selfish deployment in Fig. 3a. Unlike HCF, only a small number of filters have a high TP measure in isolated deployment. This is because the AS connectivity follows a power-law distribution so a few ASes are well connected and make strong RBF filters. As expected, RAP measure in isolated deployment is low because of low path coverage.

TP and RAP measures for altruistic deployment are shown in Figs. 3b and 3c, respectively. Protection of all nodes is similar to that of HCF, and 50 optimal filters result in 93 percent TP and RAP measure. Again, the VC deployment offers a slightly higher protection (2-5 percent) but requires around 60 times more deployment points. Filters' TP measure is lower than the same measure for the HCF defense, but it is still higher than an average node's protection in isolated deployment, creating good deployment incentive. The RAP measure is the same for filters and for all nodes. Around 22 percent of IPs is very impaired with regard to attacker placement, and 52 percent are moderately impaired. RBF has the highest impact on limiting possible attacker locations out of the defenses we evaluated.

RBF has the same per-packet cost and a slightly larger storage cost, when compared to HCF. The storage cost is larger because an AS may have up to several thousand links; so, two bytes are needed instead of one to store the parameter value. An attacker that shares the path between the source and the filter can spoof this source's traffic to all destinations the source reaches via this path. He can also replay the traffic he captures to the same destinations but this attack is unlikely since spoofing is easier for attackers than replay. RBF is thus vulnerable to the path-all, replay-all, and replay-fix attacks.

RBF's parameter table values change when a change in end-to-end routing leads to a previous hop change for some sources. Thus, frequency of false positives at an RBF filter is at most as high as for HCF filters, but likely smaller since many end-to-end routing changes may not result in peering change at large ASes that act as RBF filters. An attacker cannot influence the previous hop of spoofed packets with regard to filter thus false negatives due to guessing are zero.

4.3 Interdomain Packet Filtering

IDPF associates each source with a set of feasible neighbors (previous hops). A neighbor N is feasible for source x if N advertises a route to x to this filter. In [7], Duan et al. assume that route advertising rules are based on relation-ships between ASes [10]. IDPF was proposed as an altruistic defense with a recommended vertex cover deployment [7].

Normalized strength of the IDPF filter is: $\text{strength}_F = \sum_{P \in IProut} NF(p)/|IProut|^2$,, where NF(p) is the number of source IPs whose previous hop does not exist in the feasible neighbor set of p. Well-connected nodes are good candidates for strong filters because of the diversity of their neighbors and the prevalence of peer relationships that limit the size of the feasible neighbor set. Like in the case of RBF, because AS degrees follow the power-law distribution we expect the number of strong IDPF filters to be low. This is confirmed by the IDPF performance in selfish deployment in Fig. 4a. The protection of filters is very low both for the

TP and for the RAP measure.In optimal deployment, 50 filters provide 80 percent TP measure for all nodes (Fig. 4b) and 72 percent RAP measure (Fig. 4c). The VC deployment improves TP measure to levels comparable with RBF. Due to large memory requirements we could not compute the RAP measure for VC. IDPF makes 20 percent of attacker locations very impaired, and 35 percent moderately impaired.

5. Conclusion

In this paper, we mainly performed evaluation of various Spoofing defences like HCF, IDPF (End-to-End Network based) and RBF (Router based) are used for controlling of IP spoofing, imparting a major role in improving network security. With the growth of network scale, now a day's network administrators dissipate large amounts of time and costs to manage network addresses (IP/MACs), so network access control and IP, ARP management also studied. But still now a day IP address is hacked, these schemes doesn't provide full controlling over IP spoofing to improve maximum network security. So it is required to propose new techniques which specially focus on IP-MAC address binding to control IP spoofing as MAC address is unique throughout the world.

6. References

[1] Advanced Network Architecture Group, ANA Spoofer Project, http://spoofer.csail.mit.edu/, 2009.

[2] P. Ferguson and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks Which Employ IP Source Address Spoofing," IETF RFC 2267, 1998.

[3] D. Moore, C. Shannon, D.J. Brown, G.M. Voelker, and S. Savage, "Inferring Internet Denial-of-Service Activity," ACM Trans. Computer Systems, vol. 24, no. 2, pp. 115-139, May 2006.

[4] D. Kawamoto, "DNS Recursion Leads to Nastier DoS Attacks," ZDNet.co.uk, Mar. 2006.

[5] C. Jin, H. Wang, and K.G. Shin, "Hop-Count Filtering: An Effective Defense against Spoofed DDoS Traffic," Proc. 10th ACM Conf. Computer and Comm. Security, 2003.

[6] K. Park and H. Lee, "On the Effectiveness of Route-Based Packet Filtering for Distributed DoS Attack Prevention in Power-Law Internets," Proc. ACM SIGCOMM, 2001.

[7] Z. Duan, X. Yuan, and J. Chandrasekhar, "Constructing Inter-Domain Packet Filters to Control IP Spoofing Based on BGP Updates," Proc. IEEE INFOCOM, 2006.

[8] M. Collins, T.J. Shimeall, S. Faber, J. Janies, R. Weaver, and M. De Shon, "Predicting Future Botnet Addresses with Uncleanliness," Proc. Internet Measurement Conf. (IMC), 2007.

[9] V. Yegneswaran, P. Barford, and S. Jha, "Global Intrusion Detection in the DOMINO Overlay System," Proc. Network and Distributed System Security Symp. (NDSS), 2004.

[10] F. Wang and L. Gao, "On Inferring and Characterizing Internet Routing Policies," Proc. Internet Measurement Conf., Oct. 2003.

[11] S.N. Dorogovtsev and J.F.F. Mendes, Evolution of Networks: From Biological Nets to the Internet and WWW. Oxford Univ. Press, 2003.

7. About the Authors

Yasoda Krishna Kuppili is a student of the Department of Computer Science & Engineering of Vizag Institute of Technology, Visakhapatnam. Presently he is pursuing his M.Tech from this college. His area of interest includes Data Ware Housing and Mining, Networks.

Venkata Ramana Adari is a Professor and HOD in the Department of Computer Science & Engineering of Vizag Institute of Technology, Visakhapatnam. He is having more than 20 years of experience in teaching and industry. He is a SUN CERTIFIED JAVA Professional from Sun Micro Systems, USA.His area of interests include Software Engineering, Web mining and Object Oriented Programming. He has published several national and international research papers. He worked in Centurion University, Orissa and in some other reputed colleges in Visakhapatnam also.