M-019 Detection of IP spoofing by making use of routing information

Toshinori OHTSUKA† Fumitaka NAKAMURA†‡ Yuji SEKIYA†‡ Yasushi WAKAHARA†‡

1 Introduction

In the recent network society, there have been many security problems. Examples are DDoS attack, Virus, Worm and so on. To cope with these attacks, many approaches are introduced. They can be roughly divided into three groups. One is the approach of the attacker side, another is the approach of the victim side, and the other is the approach where the victim traces the attacker after attack packets are received. Needless to say, these approaches are all important to cope with the attacks. But it is considered it is the most important to detect attack packets as near the attacker as possible, so this paper focuses on the approach of the attacker side. At the attacker side, one of the most typical characteristics of these attack packets is that these source addresses are spoofed because these attackers want to hide their real location. In this paper, we propose a method for mitigating the attacks by detecting and filtering the packets whose source addresses are spoofed. The rest of this paper is organized as follows. Section2 presents an overview of the existing methods of detecting spoofed packets, and points out the problems of these methods. Section3 presents an overview of our proposed method and proves the effectiveness theoretically. In section 4, simulation results are discussed to exemplify the effectiveness. And finally, conclusions and future works are drawn in section 5.

2 Related works and Their problems

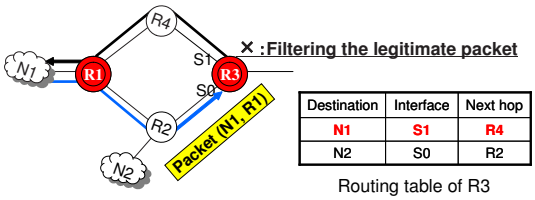
2.1 Reverse Path Forwarding (RPF)

A routing table shows a direction toward the destination of each packet. In concrete, it shows an interface through which each packet should be forwarded to a given destination. RPF uses this table in a reverse manner. Namely, if the routing table says that a packet whose destination is network N_1 is to be forwarded from interface S_1, packets received from N_1 should arrive via S_1. Unless a received packet matches this rule, the router filters the packet.

In this way, RPF assumes symmetric paths. So if it is applied to an asymmetric case, it filters legal packets wrongly(Fig.1). For such reasons, RPF is applied to only edge routers with definitely symmetric paths. That is to say, RPF tends to be used as automatic Ingress filtering[2].

2.2 Neighbor Stranger Discrimination (NSD)

NSD method[3] uses information of users ' actual flowing packets. Time is divided into 2 spoofed packet groups called Peace time and Attack time. In Peace time, there are no spoofed packets. On the contrary, in Attack time, there are spoofed packets. In Peace time, each router with NSD function collects " Neighbor information " including a list of neighbor networks and neighbor NSD routers by monitoring users ' actual flowing packets. Once an attack starts, which means it becomes attack time, Each NSD router stops collecting neighbor information and starts filtering the spoofed packets by using collected neighbor information. To be more specific, if the received packet does not come from neighbor networks or does not come via neighbor NSD routers, it is filtered as spoofed packet.



Destination	Interface	Next hop
N1	S1	R4
N2	S0	R2

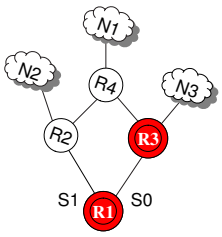
Routing table of R3

Fig. 1 Asymmetric path

NSD method has the following two defects. One is that it needs enough long peace time to get accurate neighbor information. And the other is that NSD method divides time into peace time and attack time by the existence of spoofed packets. But it is difficult to recognize the existence of spoofed packets accurately. So spoofed packets may disappear into peace time and they make neighbor information contaminated.

3 Proposed method

3.1 Efficient Filtering of IP Spoofed Packets Near the Attackers (FSN)



Source Network	Previous FSN (P-FSN)	Router interface
N1	R3	S0
	0	S1
N2	0	S1
N3	R3	S0

Fig. 2 Topology and Neighbor Link Table(NLT)

3.1.1 Brief of FSN method

Our proposed method, FSN, uses topology information to make the table for spoof detection. Each router with FSN function keeps 2 new function and information. One is a signature. When FSN router forwards a packet to next router, it marks the signature to ID field which is in the IP header of the packet. By this function, it is assured that the packet actually comes via the FSN router. The other is a Neighbor Link Table(NLT, Fig.2). This table,NLT, holds that the packets from a source network should arrive via a FSN router, called Previous FSN(P-FSN), and from an interface. If it do not arrive via any FSN router, P-FSN is set to zero. As it is seen in Fig.2, if there are equal cost multi paths, such as N_1, all cases are listed in the NLT so as not to filter legal packets. Each FSN router detects

† Graduate School of Frontier Sciences, The University of Tokyo
‡ Information Technology Center, The University of Tokyo

spoofed packets if the received packets do not match the information of the NLT. In this way, NLT is the key point in FSN method.

3.1.2 Neighbor Link Table (NLT)

At the introduction, it is said that this paper focuses on the approach of attacker side. This implies that routing is controlled by IGP (Interior Gateway Protocol). In this paper, it is assumed that Link-State routing protocol, such as OSPF, is employed for IGP. The routers which speak OSPF exchange their neighbor link information each other, so all OSPF routers can keep all topology information inside an area. By using this topology information, each router can build routing table according to Dijkstra ' s algorithm. FSN routers can also establish NLT by adding a little revision to this Dijkstra ' s algorithm.

3.1.3 Characteristics and Advantage of FSN method

NSD method collects neighbor information by monitoring the actual flowing packets. On the other hand, FSN method can build the NLT by using topology information that each router already has, and which enables NLT to be established FS time. So FSN do not need to assume peace time like NSD method, as a result FSN can work not only attack time but any time. As mentioned at section 3.1.1, NLT keeps all cases at each source network. That is, FSN does not need to consider whether there are asymmetric paths, so it can be applied to not only edge routers like RPF, but also core routers.

3.1.4 Application of FSN method

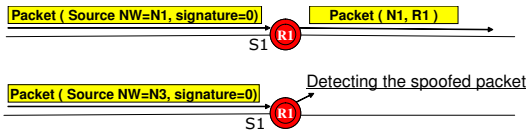


Fig. 3 Application examples of FSN method

Application examples are introduced in Fig.3. First case is that FSN router receives a packet from N_1 via interface S_1, and the packet does not go through any FSN routers. FSN router checks the NLT(Fig.2) and finds that the packet's information matches the NLT, so this packet is judged legal. On the other hand, the second case is that the packet's information does not match NLT, so this packet is judged illegal.

4 Simulation

Simulation conditions

- Topology (Generated by " BRITE[4] ")
  - BA (Barabasi Albert) model
  - The number of routers：1000
  - Location of FSN/RPF routers
    - · RPF: Selected randomly from edge routers
    - · FSN: Selected randomly from all routers
  - Ratio of FSN/RPF routers： α
  - Ratio of edge routers： γ =0.7
- The number of attackers：100
- Location pattern of FSN/RPF routers, Attackers and Victim：100
- Topology pattern：20

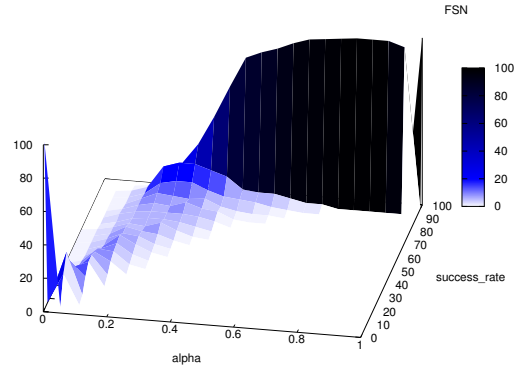


Fig. 4 Simulation results of FSN

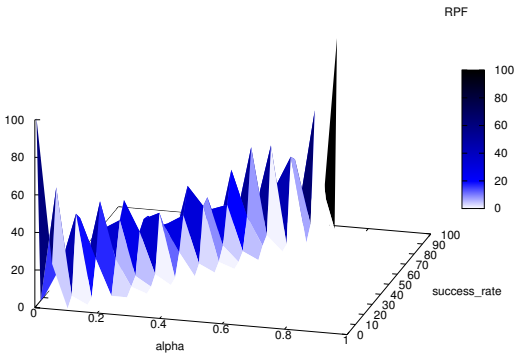


Fig. 5 Simulation results of RPF

Fig.4,5 show that probability distribution of detection success rate against FSN/RPF introduction rate α. Fig.4 shows that the detection success rate of FSN method rises rapidly as α increases. In contrast, Fig.5 shows that the detection success rate of RPF method rises only in proportion to α. So FSN method can earn higher detection success rate at the same α.

5 Conclution and future works

In this paper, We propose the effective and realistic spoof detection method, FSN. FSN method uses topology information which each router already has, so it can apply anytime and anywhere even if there are asymmetric paths. And the availability of FSN is shown by simulation.

Further works are to lay out efficient location method of FSN routers and to apply FSN method to the place where topology information cannot be obtained easily.

Reference

[1] "Configuring Unicast Reverse Path Forwarding", http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/fothersf/scfrpf.htm

[2] P. Ferguson and D. Seine, " Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing " , RFC2827, May. 2000

[3] Itani S. Aaraj, N. , Abdelahad, D. , Kayssi, A. , " Neighbor Stranger Discrimination : A New Defense Mechanism Against Internet DDOS Attacks ", the 3rd ACS/IEEE international conference on 2005 .

[4] A. Medina, A. Lakhina, I. Matta, and J. Byers, " BRITE: Universal topology generation from a user 's perspective, " Tech. Rep. BUCS-TR-2001-003, Boston University, Apr. 2001.