

國立交通大學
資訊工程學系
碩士論文

偽造來源分散式阻斷攻擊之來源端防禦方法

A Defense Scheme against Spoofed DDoS Attacks at the Source



研究生：王勝鉉

指導教授：謝續平 博士

中華民國九十三年六月

偽造來源分散式阻斷攻擊之來源端防禦方法

A Defense Scheme against Spoofed DDoS Attacks at the Source

研究生：王勝鉉

Student: Sheng-Hsuan Wang

指導教授：謝續平 博士

Advisor: Dr. Shiuh-pyng Shieh

國 立 交 通 大 學
資 訊 工 程 學 系
碩 士 論 文

A Thesis

Submitted to

Department of Computer Science and Information Engineering

College of Electrical Engineering and Computer Science

National Chiao Tung University

In Partial Fulfillment of the Requirements

For the Degree of

Master

In

Computer Science and Information Engineering

June 2004

Hsinchu Taiwan, Republic of China

中華民國九十三年六月

偽造來源分散式阻斷攻擊之來源端防禦方法

研究生：王勝鉉

指導教授：謝續平 博士

國立交通大學資訊工程學系

摘要

分散式阻斷攻擊對網路是一個嚴重的威脅，尤其是偽造來源的分散式阻斷攻擊，更是嚴重。儘管已經有許多防禦這類型攻擊的方法被提出，但是這些方法在一些應用環境下並不適用，像在 Mobile IP 的環境。因為這些方法會直接過濾掉偽造來源的封包。

我們提出一個準確偵測及有效阻止的來源端防禦方法來防止受害端遭受到偽造來源的分散式阻斷攻擊。這個方法能允許不是攻擊的偽造來源流量進入網路。因為它將網路流量做分類，並且針對不同類別的流量採用不同的處理策略。偵測攻擊的方法是根據攻擊的三個特徵來設計。第一，攻擊者會送大量封包到受害端。第二，攻擊者為了隱藏攻擊來源和在受害端難以過濾的目的，會偽造封包的來源位址。第三，分散式阻斷攻擊會造成到受害端的路徑上有嚴重的封包漏失。防止攻擊的方法是依據攻擊的行為來阻絕或限制頻寬。此外，實驗的結果證實了這個方法能有效的防止攻擊。

A Defense Scheme against Spoofed DDoS Attacks at the Source

Student: Sheng-Hsuan Wang

Advisor: Dr. Shiuh-Pyng Shieh

Department of Computer Science and Information Engineering National
Chaio Tung University

Abstract

Distributed Denial of Service (DDoS) attacks, especially spoofed DDoS attacks, are a serious threat to the Internet. In the last few years, much research has been devoted to investigate the detection and prevention of spoofed DDoS attacks. However, these approaches are impractical for some types of services, such as Mobile IP, because they filter all spoofed traffic.

We proposed a source-end spoofed DDoS defense scheme that accurately detects and effectively prevents spoofed DDoS attacks to protect servers. The scheme allows the non-attack spoofed traffic to enter the Internet because it classifies the traffic and applies different policies to distinct types. Three characteristics of spoofed DDoS attacks are applied to design the detection scheme. First, the enormous volume of attack traffic is sent to the victim. Second, source addresses of packets are forged in order to conceal origins of attacks and to filter hard at the victim. Third, there is the high packet loss rate along paths to the victim. The prevention scheme blocks or limits the allowed bandwidth of attack traffic according to its behavior. Finally, experiment results showed that the scheme can effectively prevent spoofed DDoS attacks.

誌 謝

首先要感謝的是我的指導教授謝續平博士，在這兩年中受到老師很多的照顧，老師不厭其煩的指導，傳受許多寶貴的經驗及提供珍貴的意見，讓我能完成本論文。再來，要感謝李富原學長花了許多的時間及精神和我討論，且提供許多寶貴的意見，讓我能更深入地思考問題。此外，還要感謝實驗室的同學，對於完成本論文的協助。

最後，更要感謝我的父母，在背後默默支持我，讓我能沒有顧慮的完成本論文，及感謝我的大學同學，讓我能舒解這段時間的壓力。



INDEX

CHAPTER 1. INTRODUCTION	8
1.1 REQUIREMENTS	9
1.2 DEFENSE APPROACHES	9
1.3 CONTRIBUTION	11
1.4 SYNOPSIS	11
CHAPTER 2. RELATED WORK	12
2.1 VICTIM-END APPROACHES	12
2.2 INTERMEDIATE APPROACHES	13
2.3 SOURCE-END APPROACHES	14
2.4 HYBRID APPROACHES	15
2.5 MEASUREMENT OF PACKET LOSS RATE	16
CHAPTER 3. PROPOSED SCHEME	17
3.1 ATTACK MODEL	17
3.2 OVERVIEW OF PROPOSED SCHEME	18
3.2.1 Terminology	20
3.3 DETECTION SCHEME	21
3.3.1 Source Addresses Verification	22
3.3.2 Traffic Classification	22
3.3.3 Probe Method	24
3.4 PREVENTION SCHEME	27
3.5 DISCUSSION	27
3.5.1 The overhead of the probe method	27
3.5.2 The affect of distribution of the attack	28
3.5.3 No incentive to the attacker	28
CHAPTER 4. EVALUATION	29
4.1 EXPERIMENT ENVIRONMENT	29
4.2 ATTACK SCENARIO	30
4.3 EXPERIMENT RESULTS	30
4.3.1 Number of packets of ping	31
4.3.2 Test result of the scheme	33
4.4 COMPARISON	36
CHAPTER 5. CONCLUSION AND FUTURE WORK	38

CHAPTER 6. REFERENCE..... 39

LIST OF FIGURES

Figure 3-1. The scenario of the spoofed DDoS attack 18

Figure 3-2. The detection scheme 19

Figure 3-3. The prevention scheme 20

Figure 3-4. Classification of traffic and transition of different traffic types..... 24

Figure 4-1. The environment of experiment network 29

**Figure 4-2. Frequency of packet loss rate under 100 packets of ping. The mean of
frequency is 4.63 and the standard deviation is 8.11. 31**

**Figure 4-3. Frequency of packet loss rate under 200 packets of ping. The mean of
frequency is 4.44 and the standard deviation is 8.06. 32**

**Figure 4-4. Frequency of packet loss rate under 1000 packets of ping. The mean of
frequency is 4.86 and the standard deviation is 9.27. 33**

Figure 4-5. Constant attack scenario. 34

Figure 4-6. Pulsing attack scenario. 35

Figure 4-7. Increasing attack scenario. 35

Figure 4-8. Gradual pulse attack scenario. 36

LIST OF TABLES

Table 4-1. Parameters of the experiment..... 29

Table 4-2. The comparison of approaches against spoofed DDoS attacks. 36

Chapter 1. Introduction

Distributed Denial of Service (DDoS) attacks are a serious threat to the Internet [1]. An attacker compromises several hosts, called agents, to flood packets to the same destination site, named the victim, and the traffic aggregates at the victim. The enormous volume of traffic causes the congestion and the packet loss. Resources are consumed by the attack traffic so that they are unavailable for legitimate clients. The quality of the site will decrease and it seems to be isolated.

Attackers usually spoof source addresses of packets to launch DDoS attacks. There are two purposes for spoofing. The one purpose is to conceal origins of attacks so that the victim cannot trace back to sources of attacks. Another purpose is that the victim filters packets hard because it is difficult to distinguish spoofed packets from valid packets. The challenge is due to the aggregation of the large number of traffic and the routing according to destination addresses. The victim cannot verify whether the source address carried by the packet is valid or not. Hence, it is incentive for attackers to forge source addresses. Additionally, they use addresses out of the self-network to forge packets because it is easily detected and filtered to use addresses belong to the self-network. It is notice that the spoofed packets mentioned in the thesis are packets, of which source addresses do not reside within the self-network.

However, all spoofed packets are not malicious. For instance in mobile IP, the host has one care-of address when it roams to the foreign network. The home agent uses the care-of address to forward packets to the host. The home agent will build the tunnel between himself and the foreign agent or the host and then send packets to the host through it. However, the host still uses its home address to send packets. Although the mechanism, reverse tunneling, can solve the problem, it is optional so that it is not guaranteed that all networks support the mechanism. Therefore, the traffic sent by the host should protect from being filtered as long as the traffic is not the attack.

1.1 Requirements

Some requirements for the defense scheme against DDoS attacks show as follows.

Accuracy. The false alarm of the defense scheme should be low. If the normal traffic often is mistaken for the attack traffic, there is damage to the normal traffic and there is the unnecessary overhead, such as the process of the prevention. If the attack traffic is frequently undetected, there is any interest in adopting the approach.

Congestion avoidance. The defense approach should avoid the occurrence of the congestion, which causes the decrease of performance of the Internet. The approach should effectively prevent shared resources from the exhaustion of attacks so that the server can provide services to legitimate clients.

Small damage. The defense scheme usually rate-limits or blocks all attack traffic to the victim for the purpose of the mitigation of attacks. As a result, there is collateral damage to valid clients so that attackers reach their goal. Therefore, the scheme should reduce the level of damage to legitimate traffic when it responds to attacks.

Deployment cost. The system should have the low deployment cost. The deployment cost includes the number of cooperative nodes, essential hardware requirements, the degree of modification of the Internet, and so on. The cost is one factor determining whether the system is practical or not.

1.2 Defense approaches

Many researchers proposed approaches against DDoS attacks in the recent years. These approaches are categorized to three distinct approaches: the victim-end approach, the intermediate approach and the source-end approach. This classification is based on the location at where the approach defends attacks. The victim network is the network in where the attacked server is. The source network indicates the network in where the host that initials one communication with another host is. There are usually many source networks from where

the attack origins during the DDoS attack. The intermediate network is the network, which core routers construct. In Figure 3-1, SN_1 and SN_2 are source networks, VN_1 is the victim network and CN_1 is the intermediate network. Advantages and drawbacks of approaches deployed at different positions are described as follows.

The victim-end approach is to defend DDoS attacks at the victim-end network. It facilitates the easy detection and the high accuracy of the detection. Because all attack traffic aggregates to the victim, the approach can observe the full view of the attack so that any abnormal behavior is detected. Due to the property of the heavy aggregation, the large number of attack traffic enables the approach hard to distinguish valid packets from spoofed packets. As a result, it is very difficult to filter the traffic. Once all traffic is filtered, the attack is successful, in other words, requests of legitimate clients also are blocked.

The intermediate approach is usually deployed at core routers and detects the abnormal traffic through core routers. The accuracy of detection is lower than the victim-end approach because the phenomenon, the aggregated attack traffic and the consumption of resources, does not appear at a core router. Due to the approach needs the support of core routers, the complex coordination among different routers and networks is another disadvantage for this approach. However, the approach can effectively constrain the large volume of traffic.

The source-end approach is to detect the anomalous behavior at the source router. The prevention is the most effective because the attack traffic is blocked before it penetrates into the Internet. It can protect shared resources from the exhaustion of attacks. Compared with the whole attack traffic, a few volume of traffic passes through the source router so that the detection is difficult. However, it can differentiate the valid traffic from the attack traffic since the volume of attack is slight.

In this thesis, we proposed the defense scheme against spoofed packets at source network. The attack is stopped as close to the source as possible in order to reduce the consumption of shared resources. After different approaches are deployed extensively, the prevention of the

source-end approach is the most effective. We focused on observing the behavior of spoofed packets because the spoofed traffic makes the filtering and the traceback extremely difficult at the victim. As for the unspoofed attack traffic, it can be detected and filtered easily at the victim. Besides, we analyze the packet loss rate experienced by the server to determine whether the server incurs the DDoS attack or not.

1.3 Contribution

In this thesis, the proposed scheme detects spoofed DDoS attacks by analyzing the packet loss rate at the source network. The scheme classifies the traffic and applies different policies to distinct types of traffic. It allows the non-attack spoofed traffic to enter the Internet so that some types of services, such as Mobile IP, can operate normally.

The design of the detection scheme bases on three characteristics of spoofed DDoS attacks. First, an attacker sends the enormous volume of traffic to the victim. Second, the attacker forges source addresses of packets in order to conceal sources of attacks and to filter hard at the victim. Third, the attack causes the high packet loss rate over attack paths and at the victim. The detection scheme obtains the packet loss rate of the destination without the support of core routers so that the cost of deployment is lower. The prevention scheme blocks or limits the bandwidth of the attack traffic according to its behavior.

1.4 Synopsis

This thesis is organized as follows. The related work about DDoS defense systems against DDoS attacks and approaches to defend spoofed packets are presented in Chapter 2. In Chapter 3, the proposed scheme is studied and properties are discussed. Then, some evaluations of the effect of the proposed scheme are showed in Chapter 4. Finally, the thesis concludes with Chapter 5 and future work is presented.

Chapter 2. Related Work

There is much research to investigate the detection and prevention of DDoS attacks. According to the position of the defense, these approaches are divided into three categories, including the victim-end approach, the intermediate approach and the source-end approach. We discuss the effectiveness of three parts of approaches individually.

2.1 Victim-end approaches

The victim-end approach has high accuracy of detection, but is hard to distinguish the valid traffic and the attack traffic, even if the spoofed traffic. There have been many proposed methods to detect attacks at the victim network.

Intrusion detection systems detect attacks by DDoS attack signatures, which are stored in one database. If the behavior of traffic matches with one of these signatures, the traffic is treated as the attack traffic. The method is not suitable for new DDoS attack pattern. Another method is to build profiles of the normal traffic. If the behavior of traffic violates all profiles, the traffic is considered the attack traffic. However, the method has the high false alarm because it is difficult to collect all profile of the normal traffic. [2] and [3] are examples of intrusion detection systems.

Some approaches enhance the resistance of protocol to DDoS attacks. The fragmentation attack is that fragmented packets must be stored on the victim before the packet is reassembled. An attacker can send IP fragmented packets to consume the IP reassembly resources of the victim. In [4], the proposed mechanism allows that the victim provides the computation until the location of the client is verified. However, an attacker still sends large UDP packets to prevent handshakes from completing. In [5], some strategies are proposed to address attacks for protocols that base on UDP and need large packets. [6], [7] and [8] are also protocol security mechanisms. Nevertheless, these approaches usually offer good protection from some types of attack.

A puzzle mechanism [9], called puzzle actions, is that every client bids for resources and determines the priority in half-open queue according to the difficulty of puzzle he solves. When the queue is fully, the request with the lowest priority would be dropped. However, it enables unmodified clients to have the lower priority and it is only suitable for TCP-based protocol. [10], [11] and [12] are other examples of resource accounting.

Hop-Count Filtering [13] uses the number of hops a packet passes through to reach the destination. It applies the tree data structure to build the mapping between clients and their corresponding hop-count values. If the hop-count value computed by victim does not match the mapping table, the packet would be dropped. As a result, some services, such as Mobile IP, cannot operate.

Other examples of the victim-end approach are capability-based systems [14], and client-legitimacy-based systems [15].

2.2 Intermediate approaches

This type of approach is effective to constrain on the high volume of the traffic because it does not concentrate on only few hosts. The complexity of the coordination among core routers and networks is high so that the deployment cost is too high to widely deploy.

Filtering [16] [17] is a mechanism to prevent the attack traffic from consuming shared resources. Rate limiting is also one method to respond attacks. An aggregate-based congestion control (ACC) is proposed to control high bandwidth aggregates in [18]. The local ACC mechanism identifies aggregates and controls the throughput of aggregates. The other ACC mechanism, called pushback, enables the router to request upstream routers to rate-limit specified aggregates. The pushback messages [19] are propagated to routers in the contiguous space and all traffic on one path is limited. The pushback mechanism causes significant damage on the legitimate traffic on the path, which is the same as the traffic path.

Some approaches modify the routing to resist attacks. SOS [20] [21] constructs a secure

overlay network for privileged users to prevent DoS attacks. The unauthorized packets would be dropped during the routing process. Based on the network, the graphic turing tests [22] are exploited to defend automated DDoS attacks against web servers. Rather than privileged users, the test method checks whether the request of the connection is issued by man or not. But the network needs many secure nodes to help to filter these packets. It is necessary that one client must be modified to realize how to access the network. Moreover, the graphic test restricts the range of applications.

The traceback mechanism [23] [24] [25] [26] is studied to solve DDoS attacks. It traces origins of the attack from the victim through the facilitation of core routers. However, traceback is difficult when the volume of the attack traffic is small. The mechanism is ineffective during the attack because it is usually triggered after the attack is detected so that it is too late to avoid damage.

The protocol [27], named SAVE, provides a router with the information to verify source addresses of packets through it. It assumes that every router is associated with some source addresses. Each router sends messages carried its associated addresses to all destinations and routers along the path build the table, which records the mapping between source addresses and corresponding incoming interfaces. Therefore, the information can be used to determine spoofed packets.

2.3 Source-end approaches

The source-end approaches detect attacks as close to sources as possible. The detection at source is not high accuracy because the volume of traffic is slight. In practice, this type of approach is lack of economic incentive to deploy it. However, the prevention is the most effective because the attack traffic is stopped before it causes the harm.

Ingress filtering proposed in [28] guarantees that packets outgoing from one network have source addresses, which reside within the range of this network. Because packets

violating the principle are filtered, it is possible that the ingress filtering breaks some services, for example, Mobile IP. The reverse tunneling technology can solve this problem in [29] but it is the optional function.

MULTOPS [30] is close to attackers to detect bandwidth attacks. Its fundamental idea is that packet rates between two hosts are proportion during normal operations on the Internet. If packet rates are significant disproportion, MULTOPS considers that the traffic is an attack. However, the case that packet rates between two directions are symmetric is not always existent. For example, for the online movie, the packet rate from the server is higher than from the client. Besides, MULTOPS expects that source addresses are not spoofed by the ingress filtering. However, the assumption is not always sound presently in the Internet.

D-WARD [31] is a system, which detects and prevents DDoS attacks at source-end networks. It detects the abnormal behavior by observing the ratio of the number of packets sent to and received from one destination in an aggregate flow in an edge router. If the ratio exceeds the pre-defined threshold, the traffic is treat as an attack. Then the traffic would be rate-limited. In D-WARD, it assumes that the source network has only one router, which serves all traffic going to and coming from the Internet. Nevertheless, the network usually has several routers to balance the load in order to decrease the load of routers. In [32], advantages and challenges of source-end approaches are presented.

2.4 Hybrid approaches

There are different advantages for distinct types of approach. Hence, some hybrid approaches are proposed to obtain these benefits simultaneously.

In [33], MANAnet establishes cooperative defense nodes around the victim to stamp the packets and stamped packets can get the fair usage of resources. Reverse Firewall at source network can prevent the outgoing traffic. MANAnet lacks the incentive to widely deployment because it needs cooperative nodes and the facilitation of the IP protocol to stamp packets.

Similarity, COSSACK [34] demands to build a multicast group of nodes at victim and source networks so that it has the disadvantage of the poor scalability. The statistics method uses to detect attacks in [35], but the real-time computation cost is too high to deploy widely.

There are some principles to which DDoS defense system should adhere are presented in [36]. The Defensive Cooperative Overlay Mesh, called DefCOM, is proposed and it is the DDoS defense system adheres to those principles. The system coordinates nodes at different positions to defend attacks. However, the operation is complex and deployment cost is high.

2.5 Measurement of packet loss rate

In this thesis, we analyze the packet loss rate of the destination to detect spoofed DDoS attacks. There are some approaches to measure the packet loss rate.

The simple method to get the packet loss rate is to send packets of ping to test the destination. The sender sends some packets to the destination and receives reply packets from the destination. The packet loss rate is computed by packets, which are sent and received by the sender.

Some approaches [40] [41] [42] use the mathematical theory to estimate the packet loss rate. The advantage of these approaches is to send few packets to obtain the packet loss rate. However, they are not suited for our proposed scheme. Some of them need the support of core routers. The deployment cost is high. Some of them need the cooperation of some nodes within the destination network. Therefore, our proposed scheme cannot adopt these approaches.

Chapter 3. Proposed Scheme

In this chapter, we describe details of the proposed scheme. First, the attack model is showed and the overview of the proposed scheme is presented. They introduce the environment and overall operations of the scheme. Next, we further study the detection scheme and the prevent scheme, respectively. Final, some properties are discussed.

3.1 Attack model

Let $H = \{h_i \mid 1 \leq i \leq t\}$ represent hosts. $H_s = \{h_y^s \mid 1 \leq y \leq g, 1 \leq g \leq t\}$ is the set, in which hosts provide services. $H_v = \{h_x^v \mid 1 \leq x \leq j, 1 \leq j \leq y\}$ is the set, which represents attacked server hosts, and H_v is the subset of H_s . Hosts that initial communications with H_s are represented by $H_b = \{h_p^b \mid 1 \leq p \leq k, 1 \leq k \leq t\}$. The set H_b is partitioned to four subsets: $H_r = \{h_m^r \mid 1 \leq m \leq w, 1 \leq w \leq p\}$, $H_a = \{h_o^a \mid 1 \leq o \leq z, 1 \leq z \leq p\}$, $H_n = \{h_u^n \mid 1 \leq u \leq l, 1 \leq l \leq p\}$ and $H_e = \{h_d^e \mid 1 \leq d \leq c, 1 \leq c \leq p\}$. Besides, $H_f = \{h_q^f \mid 1 \leq q \leq t', 1 \leq t' \leq o+l+d\}$ is the union set of H_a , H_n and H_e . h_m^r is the host using the real source address. h_q^f is the host using the spoofed address. The spoofed address indicates the address, which does not reside within the self-network. The host in H_a is the DDoS attack host. Although hosts in H_n and H_e use spoofed addresses, they are valid hosts. The host in H_n sends packets to H_s , not H_v . The host in H_e sends packets to H_v .

The source network is the network, where h_p^b is in, and is expressed by SN_q . The network, where h_y^s is in, is called the destination network and is expressed by DN_j . The victim network is the network, where h_x^v is in, and is expressed by VN_m . The router at SN_q is called the source router, SR_i . The routers at DN_j and VN_m are named the destination router, DR_k and the victim router, VR_s . CR_t expresses core routers. The core network, or called intermediate network, is constructed by CR_t and is expressed by CN_v .

The spoofed DDoS attack is that h_o^a floods spoofed packets to some h_v so that h_v can provide services to h_b . Figure 3-1 illustrates the scenario of the DDoS attack using spoofed

packets. h_a in SN_1 and h_a in SN_2 flood a large volume of spoofed traffic to h_v in the VN_1 . These traffic aggregates at h_v so that other traffic sent by h_r , h_n and h_e in SN_1 and SN_2 is dropped. h_v cannot serve these legitimate clients.

The proposed scheme is deployed at SR_i . It detects the traffic flooded by h_a and to protect the traffic sent by h_n from the damage. However, the scheme would mistake the traffic sent by h_e for the attack traffic.

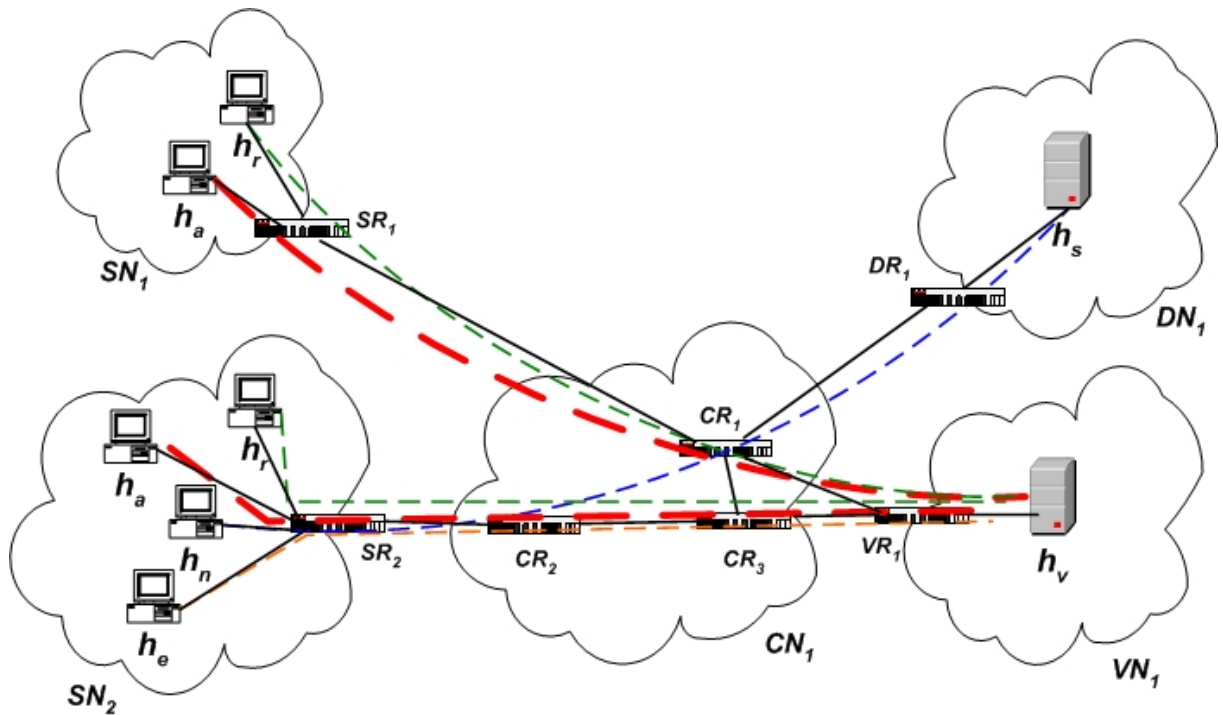


Figure 3-1. The scenario of the spoofed DDoS attack

3.2 Overview of proposed scheme

The proposed scheme is deployed at the source router, SR_i and monitors the behavior of traffic through it. The scheme includes two parts. One is the detection scheme. It is responsible for the detection of DDoS attacks. It analyses the packet loss rate of the destination and determines which type of traffic it belongs to. Then the type of traffic is passed to the other scheme. The other is the prevention scheme. It takes charge of responding to attacks to decrease the damage of them. It generates rate-limiting rules according to formulas and the type of traffic from the detection scheme.

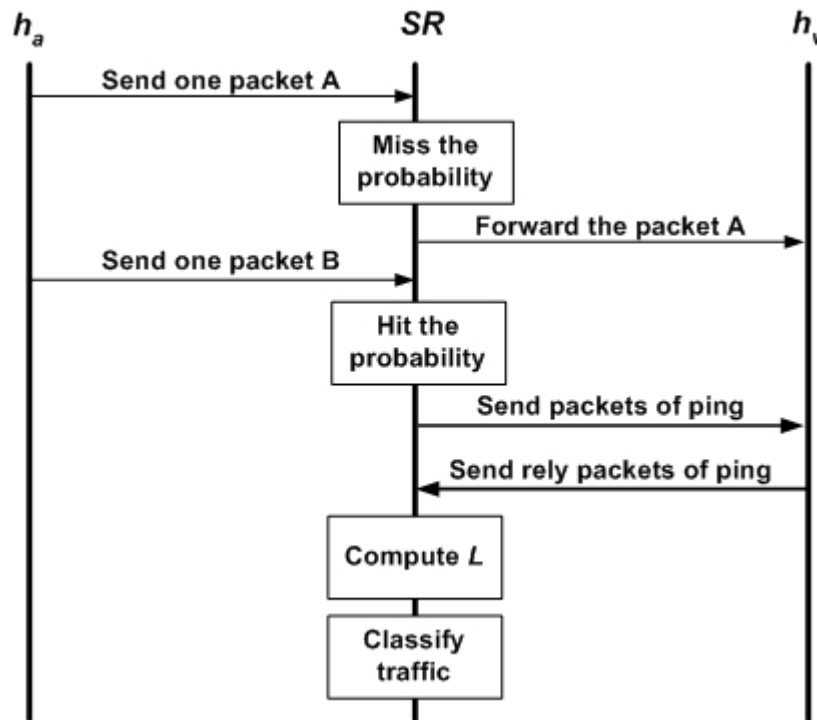


Figure 3-2. The detection scheme

Figure 3-2 shows the process of the detection scheme. It observes every packet from the source network to the Internet. When the router receives one packet from the source network, the router decides if it gets the information of the packet loss rate of the destination according to one probability. If the probability is missed, the router forwards the packet and does not get the information. If the probability is hit, the router processes the probe method, which is the process to get the packet loss rate. The router classifies the traffic based on the measured packet loss rate. Then the router passes the result of classification to the prevent scheme.

Figure 3-3 shows the process of the prevention scheme. The scheme bases on the result from the detection scheme to take the appropriate action toward the traffic. If the traffic type is the normal traffic, the scheme does not constrain the traffic. For the suspicious traffic, the traffic is rate-limited. As for the attack traffic, the scheme blocks the traffic before it enters to the Internet.

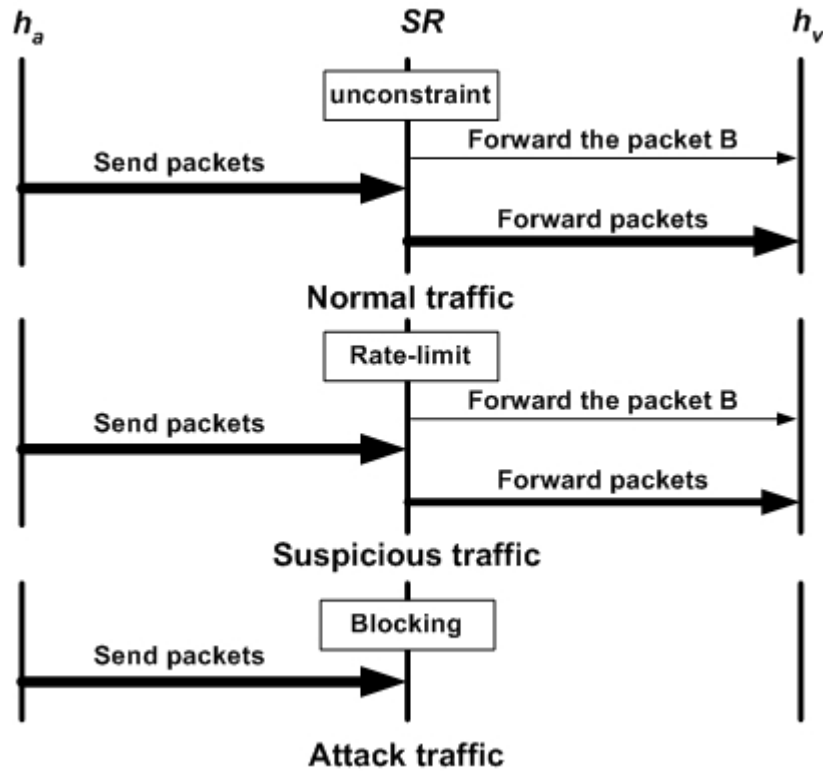


Figure 3-3. The prevention scheme

3.2.1 Terminology

Before the detail of the proposed scheme is presented, the terminology used in the scheme is defined first.

- P is the probability used by the source router to decide whether it probes the packet loss rate of the destination or not. P_0 represents the default probability.
- N_s is the number of packets of ping sent by the source router during one probe.
- N_r is the number of reply packets received from the destination during one probe.
- L is the measured packet loss rate of the destination that the source router obtained after one probe.
- L_s is the packet loss rate used as the threshold, over which the traffic is treated as the suspicious traffic by the scheme.
- L_a is the packet loss rate used as the threshold, over which the traffic is treated as the attack traffic the scheme.

- R is the sending rate allowed by the scheme. The sending rate is the total rate that all hosts in the source network send packets to some destination.

3.3 Detection Scheme

In the beginning, we introduce characteristics of DDoS attacks used by the proposed scheme. DDoS attacks cause the common result that the server cannot provide services to clients. For the purpose, an attacker floods packets to the server so that the bandwidth of the server is critically consumed. As a result, the congestion appears along the path to the server and even there is the phenomenon of the packet loss. Another reason of using a great deal of packets is that the server does not have enough time to process them. Many packets would be dropped. Consequently, sending a large number of packets is one of properties of DDoS attacks.

Attackers usually forge source addresses of packets flooded to the server. As mentioned before, they attempt to avoid that sources in the flooding traffic are revealed. It is possible for the server that it cannot distinguish the legitimate traffic from the spoofed traffic. The server is hard to filter the traffic attack. Therefore, having these incentives to spoof, most attackers launch DDoS attacks using spoofed packets. The proposed system observes the behavior of spoofed packets to prevent the occurrence of DDoS attacks.

The detection scheme determines the degree of the attack according to the packet loss rate. DDoS attacks limit or block the requests of legitimate users by exhausting resources of the server, especially the bandwidth. The phenomenon makes the packet loss rate of the server higher. Once the packet loss rate increases, the server seems to be isolated and cannot provide services to valid users. The characteristic is applied to estimate whether the server suffers the DDoS attack or not.

According to characteristics obtained by observing DDoS attacks, we present the detection scheme to detect if DDoS attacks occur or not.

3.3.1 Source Addresses Verification

The first step of the detection scheme is how to determine spoofed packets because the proposed scheme focuses on monitoring the behavior of spoofed packets. Instead of proposing the method to know if the packet is spoofed, this thesis pays attention to prevent attackers from launching DDoS attacks by spoofed packets. Hence, the protocol, called SAVE, is utilized to build the information of valid source addresses.

The protocol helps a router to realize source addresses, which are correct through it. We bases on the protocol to build the information of valid source addresses at source routers. The information records source addresses, with which packets are valid through the router. After having the information on the router, the scheme verifies whether one source address of one packet exists in the information. If the address is recorded in the information, the packet is not a spoofed packet; otherwise, it would be treated as a spoofed packet.

3.3.2 Traffic Classification

Once we know that the traffic is spoofed, we further want to understand whether it is malicious. In other words, we determine if the spoofed traffic is the DDoS traffic. However, the packet loss rate over the path from the source router to the destination is the measured value used to decide the degree of attacks.

Before discussing how to obtain the packet loss rate, we first describe the way of traffic classification because most parts of the proposed scheme relates with the classification. As for the method to get the packet loss rate, it is discussed later.

The classification of the traffic is based on the packet loss rate over the path from the source router to the destination. The purpose of the classification is to conveniently apply the different rules to distinct types of traffic. The traffic is categorized as three types, including the normal traffic, the suspicious traffic and the attack traffic. The normal traffic is the traffic, of which the behavior is usual and the packet loss rate is within the regular value. The type of traffic is allowed into the Internet and no constricted rules are applied to it. The attack traffic

indicates the DDoS attack traffic and the traffic would be blocked. Accordingly, the attack traffic would not consume shared resources of the server and the Internet so that the effect of the attack can be reduced. The suspicious traffic lies in between the normal traffic and the attack traffic. Although the behavior of this type of traffic differs from the normal behavior, it does not reach the degree of the attack. It is possible that many indeterminate factors of the network result in the burst of the packet loss rate, for instance, the change of the network topology, faults of routers and so on. Therefore, the traffic still passes through the router to the destination but the sending rate would be constrained. However, if the higher packet loss rate is due to usual faults of the network but attacks, the problem is solved by some mechanisms, such as the change of routing, rate control and so on. If the packet loss rate does not come down to the usual value and the client still persists to send packets, the traffic is treated as the attack traffic.

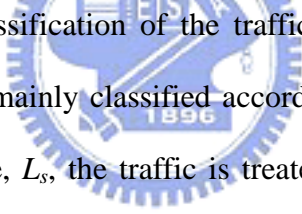


Figure 3-4 shows the classification of the traffic and the transition between different types of traffic. The traffic is mainly classified according to the packet loss rate. If the loss rate is within the normal value, L_s , the traffic is treated as the normal traffic. The traffic is decided to the attack traffic if any of the following conditions arises: 1) the packet loss rate is higher than the attack value, L_a , which is far larger than the usual value. 2) the traffic stays in suspicious traffic for the period, T_s . 3) the sending rate of packets to the destination is lower than the overhead to get the packet loss rate. The attack traffic is blocked for the penalty period, T_a . After the period, if the traffic is compliant, that is to say that the packet loss rate is lower than L_a , the traffic is changed to other types of traffic. The loss rate is between L_s and L_a , the traffic is thought the suspicious traffic. The traffic will be rate-limited according to its behavior. If the loss rate comes back to the normal value, the traffic is changed to the normal traffic.

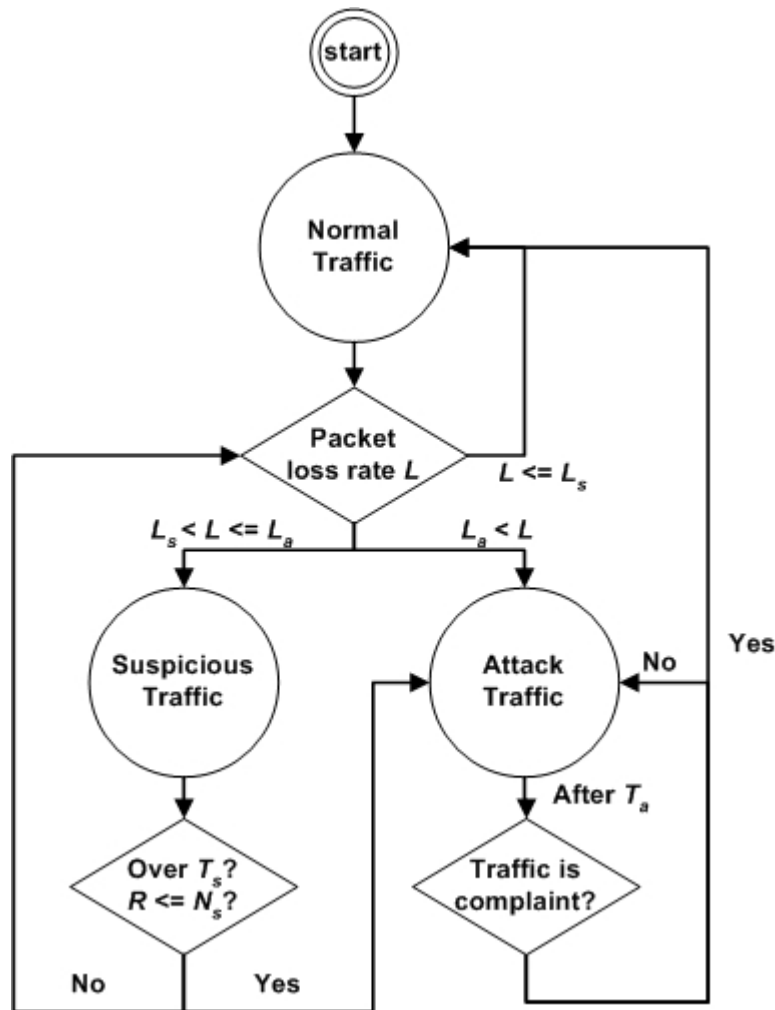


Figure 3-4. Classification of traffic and transition of different traffic types

3.3.3 Probe Method

We want to understand the packet loss rate of the destination upon receipt one spoofed packet.

Definition 1: A probe. The process to obtain the packet loss rate is called a probe. The probe is to send some packets from the source router to the destination for the knowledge of the packet loss rate along the path.

The probe method should meet two requirements including the realization of the packet loss rate and the unnecessary support of core routers.

The ping tool is one of solutions, which meet requirements of the probe method. The tool is to send the ICMP echo request packet to the destination and to wait for the ICMP echo reply packet from the destination. If the sender can receive the reply packet, the path and the

server are normal. We assume the destination must reply the ICMP echo request for the usage of the ping. When the scheme decides to probe the destination, it sends N_s packets of ping to the destination and calculates the number of reply packets, N_r . The measured packet loss rate L is computed by received reply packets divided by total sending packets. The scheme exploits the measured loss rate to infer the status of the path and the destination.

Definition 2: Packet loss rate. The packet loss rate is the measure value obtained through one probe. If N_s is the number of packets of ping sent to the destination and N_r is the number of reply packets. The measured packet loss rate L is $L = \frac{N_s - N_r}{N_s} * 100$.

When the router receives one spoofed packet going out from the source network, the scheme decides to probe the status of the destination based on one probability, P , instead of every spoofed packet. The reason is to reduce the overhead of the probe and to avoid causing the DDoS attack. In order to know the packet loss rate, the scheme must pay the extra overhead, N_s packets of ping sent by the probe method in one probe. The overhead is expensive if one probe is processed for every spoofed packet. Hence, the scheme takes the probability method to do the decision to enforce one probe. It is possible for the attacker to exploit the flaw to enable the router to launch the DDoS attack. The problem is discussed later.

The probability, P , is adjusted to the status of the destination and is not the constant value. If P is larger, the overhead becomes significant high; on the other hand, the detection time increases and the effective of the prevention decreases if P is smaller. The condition of the network and the destination varies over the time, so the probability should be changeable according to different situations. In the proposed scheme, P has different values under distinct types of traffic. That is to say, the probability bases on the packet loss rate to tune. The following formula is the adjustment formula for the probability, P :

$$P = \begin{cases} P_0 & L \leq L_s \\ P_0 + (N_s^{-1} - P_0) * \left(\frac{L - L_s}{L_a - L_s} \right) & L_s < L \leq L_a \\ 0 & L_a < L \end{cases}$$

When the traffic is the normal traffic, the scheme keeps a stationary probe rate to investigate the packet loss rate. However, when the behavior of traffic is suspicious, it means the possibility that the traffic is the attack traffic increases with the deterioration of packet loss rate. The scheme takes the active action to prevent the occurrence of the attack. It increases the frequency of probes to know the running status of the destination and to early respond to the attack. Therefore, the probability enlarges with the raisement of the packet loss rate. The degree of increasement of the probability is proportional to the degree of deterioration of the packet loss rate. For the attack traffic, the scheme does not enforce the probe during the period of penalty. After the period, the scheme probes the destination to understand the packet loss rate. If the loss rate is complaint, the traffic is changed to other types of traffic; otherwise, the scheme continues to punish for the traffic.

It is necessary that the distinct probe probability for every destination is maintained by the scheme because every destination has different packet loss rates. However, the scheme does not record probabilities of all destinations. Hosts in a source network usually connect some servers during the some period so total number of records only meets the requirement to avoid replacing excessively. Each record comprises the destination address and the corresponding probe probability. The replacement strategy is to randomly choose the entry with the smallest probability to replace. The record set $T = \{E_1, E_2, \dots, E_n\}$ where E_i is the entry of the table and $1 \leq i \leq n$ where n is the max number of records. The entry $E_i = (D_i, P_i)$ where D_i and P_i is the destination address and the corresponding probe probability, respectively. $T' = \{E_1', E_2', \dots, E_m'\}$ where E_j' is the record with the smallest probability, $1 \leq j \leq m$ and $1 \leq m \leq n$. When the replacement is needed, the scheme randomly picks one in T' .

3.4 Prevention Scheme

The purpose of the prevention scheme is to block the malicious traffic and to protect the valid traffic. The prevention scheme takes the appropriate policy against the DDoS attack according to the result of the detection scheme. Through the detection scheme, the traffic is classified as the normal traffic, the suspicious traffic and the attack traffic. In the prevention scheme, types of traffic and packet loss rate are used to define the prevention policies. The prevention formula is the following:

$$R_{t+1} = \begin{cases} \infty & L \leq L_s \\ R_t * (1 - L) & L_s < L \leq L_a \\ 0 & L_a < L \end{cases}$$

For the normal traffic, the prevent scheme does not constrain the sending rate, in other words, senders can use the entire bandwidth which they acquire. When the traffic is unusual, the scheme limits the sending rate of traffic or blocks the traffic. The bandwidth of suspicious traffic is limited and the degree of rate-limit is proportional to the packet loss rate. However, the attack traffic is blocked for the period of penalty, T_a .

3.5 Discussion

There are some properties that are discussed. They have relations with the overhead, the effectiveness of the scheme.

3.5.1 The overhead of the probe method

Theorem 1: The overhead of the probe method. Under a probe sends N_s packets of ping to obtain the packet loss rate of the destination based on the probability P , the overhead of probe method is $P * N_s$.

The probe method in the detection scheme provides the way that the source router can get the information of packet loss rate of the destination without the support of core routers. However, some extra overhead must be paid in order to achieve the objective. The overhead

consumes the bandwidth of the destination and even causes the attack. Besides, the source router sends the packets of ping to increase the overhead of it. Therefore, reducing the overhead is important for the proposed scheme. The principle to decide P and N_s is that P and N_s should be as small as possible.

3.5.2 The affect of distribution of the attack

The scheme is effective no matter origins of the attack are from the single source network or several source networks. Because the attacker needs to send a large number of packets to the destination in order to overwhelm resources of the destination. When the attacker is in the single source network, the attack is easily detected although the scheme decide to probe the destination according the probability, P . The attacker launches the DDoS attack from many different source networks in order to reduce the volume of the attack traffic for every source network to evade the detection. This case shows many proposed schemes try the probability, P , simultaneously so that the possibility that the attack is detected increases. Therefore, the attack is detected whether origins of the attack is distributed or not.

3.5.3 No incentive to the attacker

In the proposed scheme, we send packets of ping to the destination for the purpose of the knowledge of packet loss rate. We endeavor to reduce the overhead so that attackers have no way to exploit the scheme to launch DDoS attacks. Even though the propose scheme becomes the attack tool of attackers unfortunately, the effect of the attack is restricted. The difficulty of filtering at the victim is that the victim is hard to differentiate the spoofed packets from valid spoofed packets. Once the attacker uses the proposed scheme, packets sent by the source router carry the real source address so that the advantage of spoofing is disappeared. Hence, the proposed scheme is unworthy for attackers.

Chapter 4. Evaluation

We implemented the proposed scheme in order to verify the effectiveness of the scheme. Several attack programs are developed to test the proposed scheme against them.

4.1 Experiment environment

The proposed scheme is implemented in a FreeBSD software router. Figure 4-1 shows the environment of the experiment. The test network environment comprises a router host, which is simulated by software routing, an attack machine, which generates the attack traffic, and a victim machine.



Figure 4-1. The environment of experiment network

The left host is the attack host and adjusts the sending rate according to different attack scenarios. The proposed scheme is deployed in the middle host. The libpcap library is used to capture traffic and analyze packets in the detection component. In the prevention component, the allowed bandwidth is maintained by using the IPFW tool [37]. The tool creates one pipe and the bandwidth of the pipe represents the allowed bandwidth to the destination. The functionality of the rate limiting can be achieved by configuring the size of the pipe. Table 4-1 presents configurations and parameters in the experiment.

<u>Attacker host</u>	<u>Scheme parameters</u>
Attack packet: SYN packet	$L_s = 30\%$
IP range: 192.168.2.0/24	$L_a = 60\%$
Maximum sending rate = 500KBps	$N_s = 100$
<u>Victim host</u>	$P = 10^{-4}$
Bandwidth = 200KBps	$T_s = 20 \text{ sec}$
IP range: 192.168.3.0/24	$T_a = 20 \text{ sec}$

Table 4-1. Parameters of the experiment

4.2 Attack scenario

Similar to D-WARD [31], four attack scenarios are developed in the experiment. The purpose is to test the ability of the detection scheme and the prevention scheme under different attacks. These scenarios are constant rate attack, pulsing attack, increasing rate attack and gradual pulse attack. The parameters of each attack scenario describe as follows:

- **Constant rate attack**

The sending rate is constant and fixed during the period of the attack. The rate of traffic achieves the maximum rate immediately and fixed until the attack is stopped.

- **Pulsing attack**

The cycle of the attack includes two parts: the active period and the inactive period.

The sending rate is the maximum rate in the active period. On the contrary, the sending rate is zero in the inactive period. The attack rate oscillates between the maximum rate and zero.

- **Increasing rate attack**

The sending rate is proportional to increase with the time. After the rate achieves the maximum rate, the sending rate is maintained until the attack is terminated.

- **Gradual pulse attack**

In the beginning, the sending rate increases with the time. When the rate achieves the maximum rate, the sending rate is keep for one period. After the period, the rate gradually decreases to zero.

4.3 Experiment Results

There are two experiments. One is to decide how many packets of ping sent for one probe. In this experiment, various numbers of packets are analyzed and three parameters of the scheme are determined, including number of packets (N_s), threshold of the suspicious traffic (L_s) and threshold of the attack traffic (L_a). The other is the effectiveness of the

proposed scheme. The experiment shows the ability of the scheme under various attack scenarios.

4.3.1 Number of packets of ping

The first experiment is to determine the number of packets of ping, N_s , during one probe and to define values of L_s and L_a . In order to get the precise packet loss rate, it is expected to send many packets to measure the actual packet loss rate experienced by the destination. When the volume of sending packets is larger, the measured packet loss rate is close to the real packet loss rate. However, the overhead, including the consumption of bandwidth and the effort of the router, is proportional to the number of sending packets. Besides, the volume of sending packets affects the detection time. The numbers of packets of ping increases the detection time so that the effectiveness to response attacks decreases. Therefore, we expect that the number of packets is lower and the accuracy does not drop off critically.

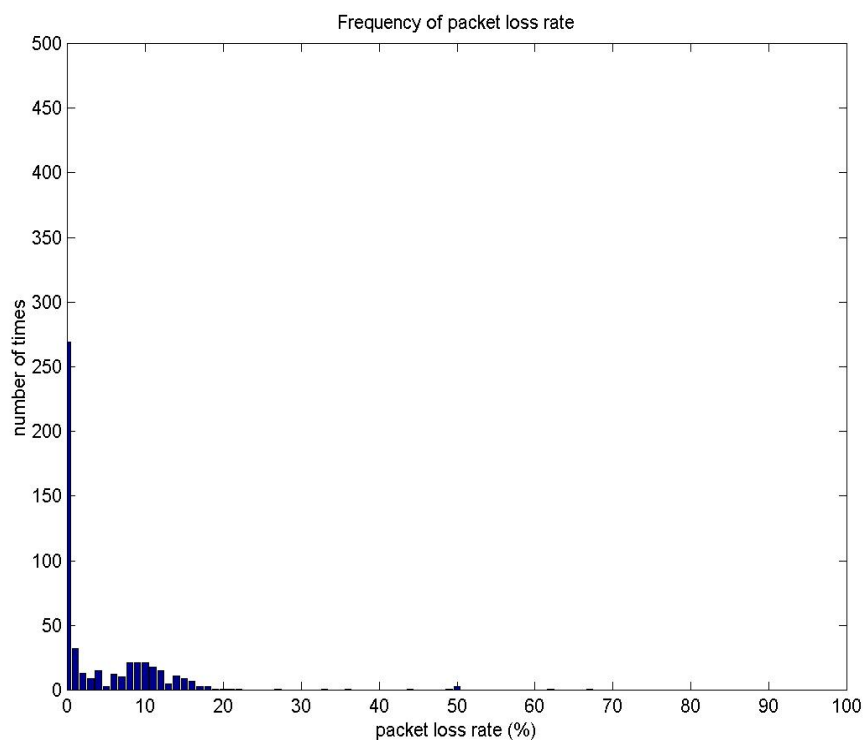


Figure 4-2. Frequency of packet loss rate under 100 packets of ping. The mean of frequency is 4.63 and the standard deviation is 8.11.

In the experiment, we adopt hosts in Burch and Cheswick's Internet map [38] [39] as our

test destinations. They both traceroute many hosts in the Internet from a single source, then collect all traceroute data. We treat the single source as the source router and choose hosts in the map as destinations. We first select hosts, which will reply requests of the ping. In this thesis, we choose the ping tool as an instrument, which gets the information of packet loss rate. For the usage of the ping, we must guarantee that the host will reply requests. After replying hosts is determined, we randomly choose 500 hosts as the test set. We ping each host in the test set using 100, 200 and 1000 packets of ping, respectively.

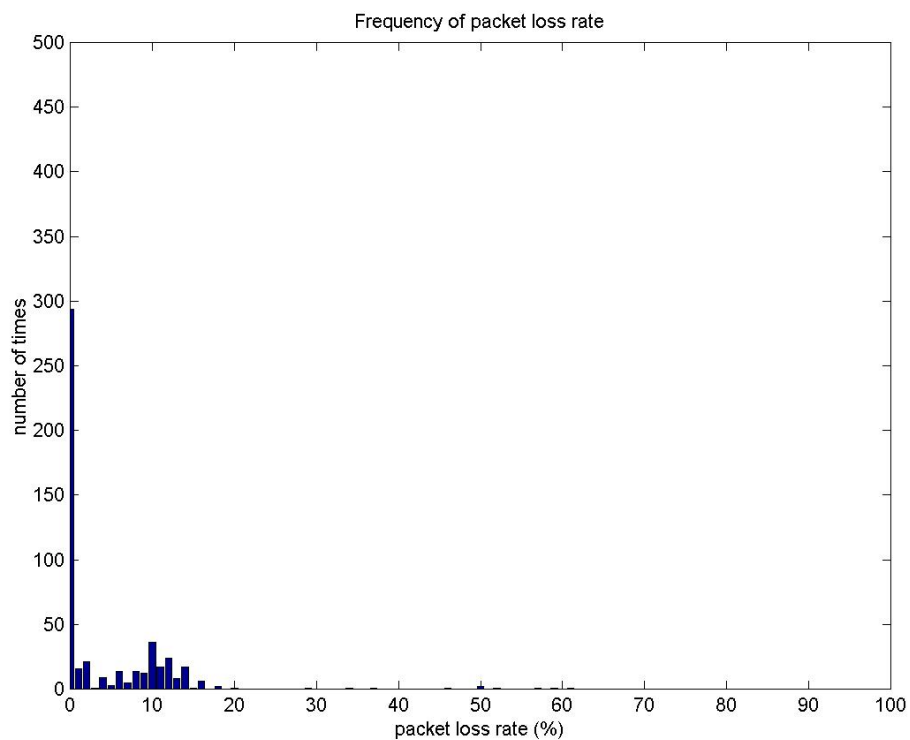


Figure 4-3. Frequency of packet loss rate under 200 packets of ping. The mean of frequency is 4.44 and the standard deviation is 8.06.

Results of the experiment are showed from Figure 4-2 to Figure 4-4. We infer that the packet rate loss is low without the occurrence of attacks. The mean value and the standard deviation of each figure are used to measure the degree of differences among various configurations. The mean value is from 4 to 5 and the standard deviation is from 8 to 9 in these figures. The level of differences is small. The most part of the packet loss rate is zero. The packet loss rate of the percentage of 90% is lower than 20%. We conclude that the packet

loss rate obtained by using 100 packets is similar to that obtained by using 1000 packets. The packet loss rate is low during normal operations. Therefore, we set parameters of the following experiment by results and observations of this experiment. We define that N_s is 100, L_s is 30% and L_a is 60%.

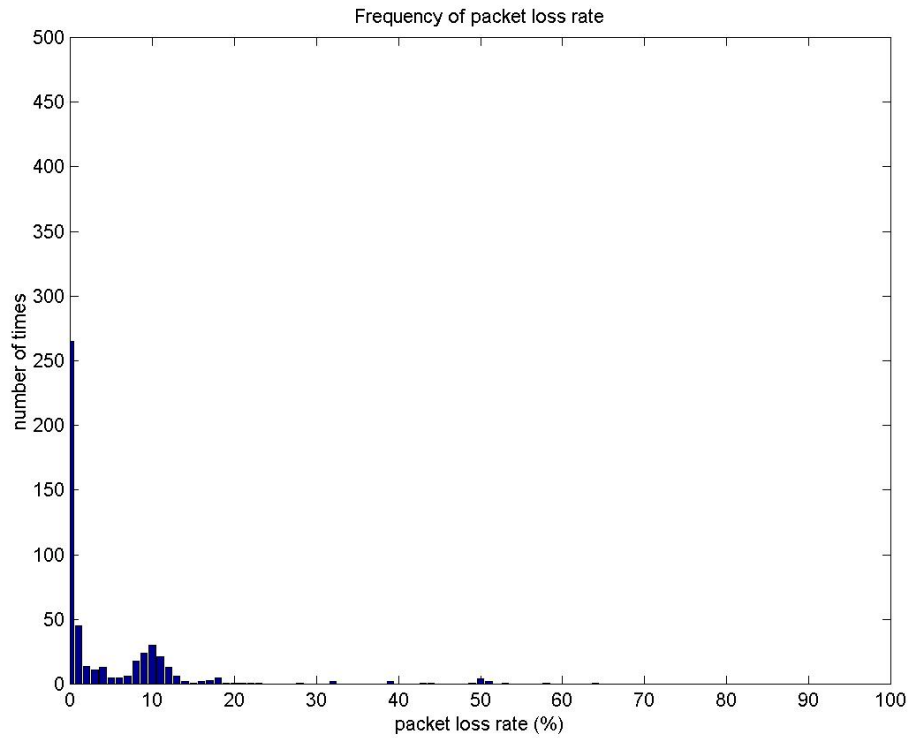


Figure 4-4. Frequency of packet loss rate under 1000 packets of ping. The mean of frequency is 4.86 and the standard deviation is 9.27.

4.3.2 Test result of the scheme

The purpose of the experiment is to test the ability of the scheme. We build four attack scenarios and observe the power of the detection scheme and the prevention scheme under these four scenarios. The maximum sending rate of the attacker is 500KBps. The bandwidth of the victim is 200KBps and the whole bandwidth is offered to the attacker. Other parameters are presented in Table 4-1. Besides, we reconstruct the implementation of detection scheme of D-WARD to compare with the proposed scheme. The purpose of the comparison is the accuracy of the detection. The modification is that the traffic is blocked when the detection scheme of D-WARD detects an attack.

Test results shows from Figure 4-5 to Figure 4-8. It infers that the proposed scheme can accurately detect four attacks and effectively prevent them. It notices that the probability, P , affects the length of the detection time so that attackers cannot predict the time when the scheme probes the status of the victim. In Figure 4-6, three lengths of time, when the attack is detected, are different because of the factor of the probability. There is the same condition in Figure 4-7 and Figure 4-8. Besides, in constant attack scenario and pulsing attack scenario, the accuracy of the proposed scheme is similar to that of D-WARD. In increasing attack scenario and gradual pulsing attack scenario, the accuracy of the proposed scheme is higher than that of D-WARD.

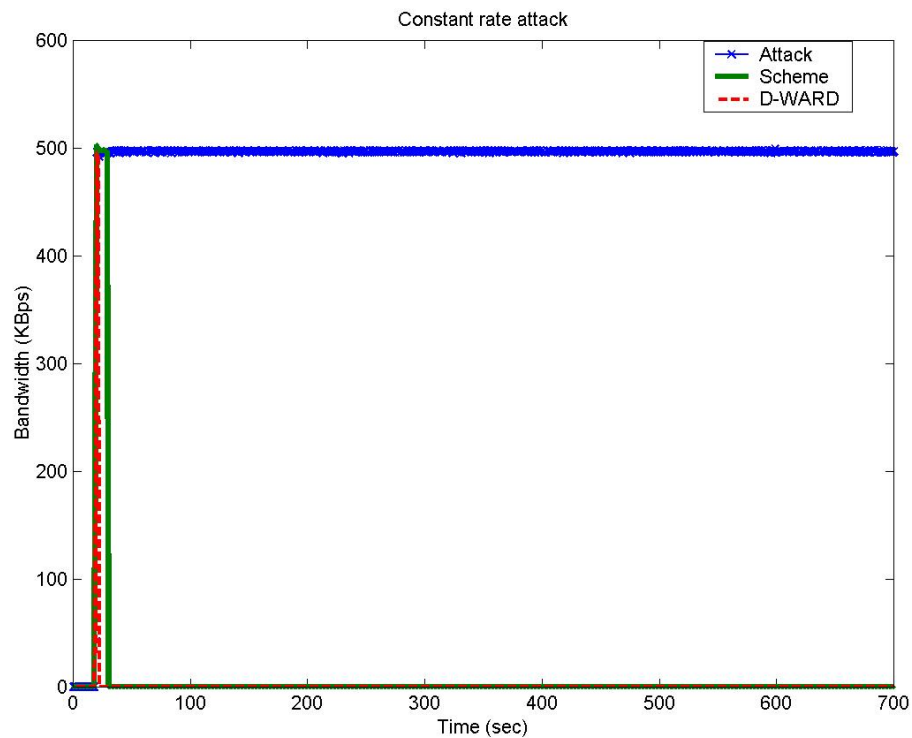


Figure 4-5. Constant attack scenario.

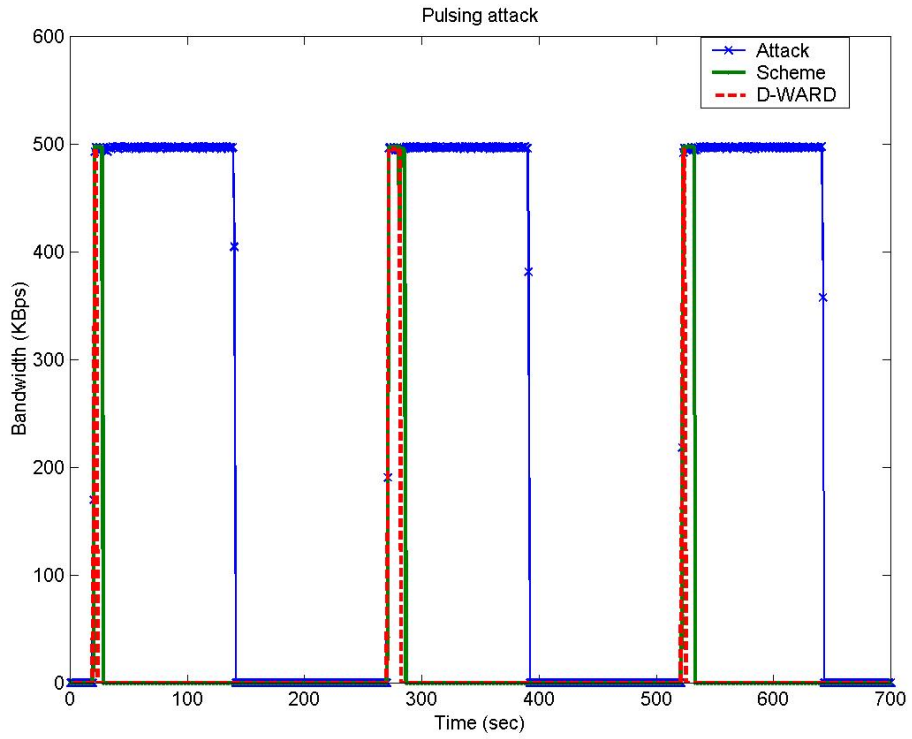


Figure 4-6. Pulsing attack scenario.

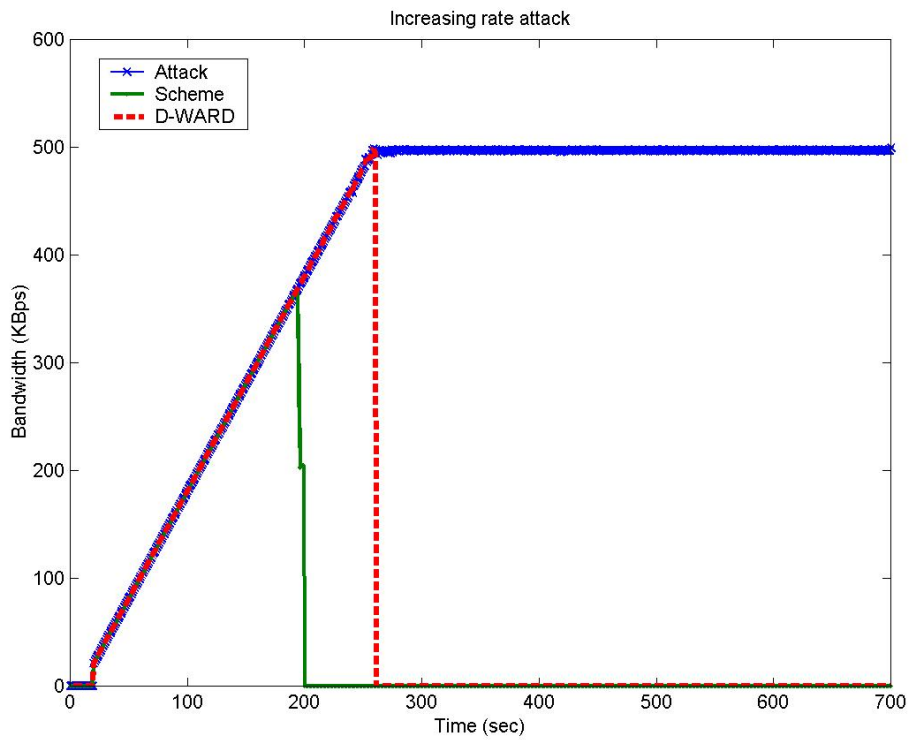


Figure 4-7. Increasing attack scenario.

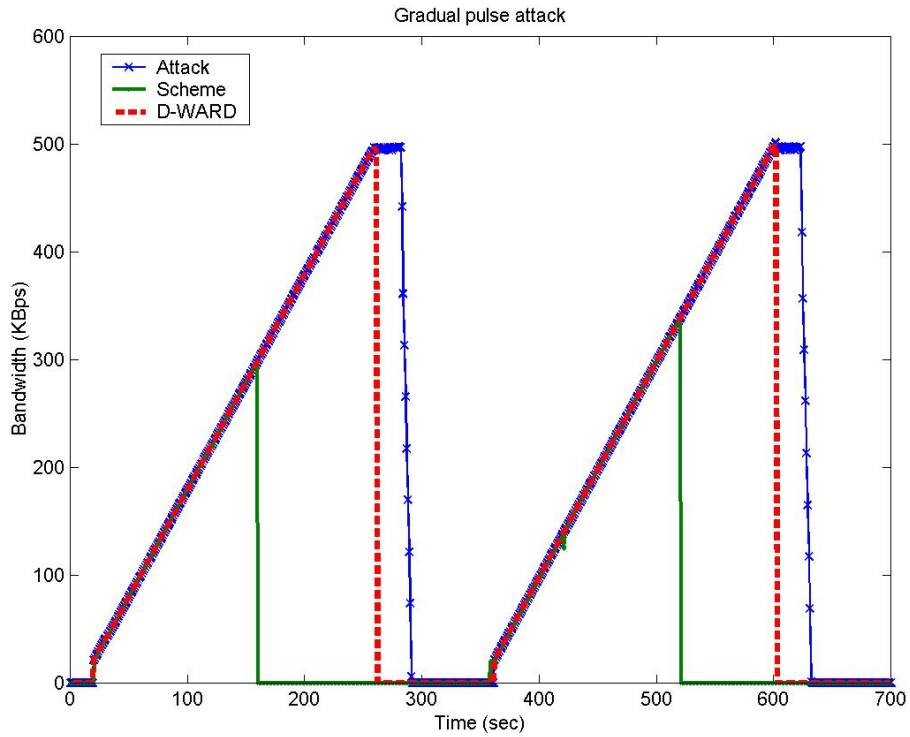


Figure 4-8. Gradual pulse attack scenario.

4.4 Comparison

We compared several approaches against spoofed DDoS attacks, include hop-count filter, SAVE, ingress filtering, D-WARD and our proposed scheme. The comparison bases on the requirements as mentioned above. Table 4-2 shows results of the comparison and the explanations for results are as follows.

	Accuracy	Congestion Avoidance	Damage	Deployment Cost
Proposed Scheme	High	Yes	Small	Low
D-WARD	Low	Yes	Small	High
Ingress Filtering	Low	Yes	Large	Low
SAVE	Low	Yes	Large	High
Hop-count Filter	Low	No	Large	Low

Table 4-2. The comparison of approaches against spoofed DDoS attacks.

Accuracy. The D-WARD defines one upper bound of UDP connections to detect the

spoofed UDP attacks. If the number of UDP connections to one destination breaches the bound, the D-WARD considers that the spoofed attack occurs. The accuracy is not precise if the number of UDP connections is more than the upper bound. The result of experiment showed that the accuracy of D-WARD is lower than our proposed scheme. The hop-count filter, SAVE and ingress filtering have high false positive because the non-attack spoofed traffic is considered as the attack. Our proposed scheme bases on the status of the destination so that the accuracy is higher.

Congestion avoidance. The hop-count filter cannot avoid the congestion because it is deployed at the victim network. The congestion arises along paths to the victim. The ingress filtering filters all spoofed packets so that the spoofed traffic is not allowed to enter the Internet. Our proposed scheme and other approaches cause the slight congestion before they detect attacks. However, the effective prevention scheme can amend the problem.

Small damage. The hop-count, SAVE and ingress filtering filter all spoofed packets so that the legitimate spoofed traffic cannot operate normally. These approaches do serious damage to the non-attack spoofed traffic. Our proposed scheme and D-WARD enforce different policies to distinct types of traffic so that they can protect the legitimate traffic.

Deployment cost. The SAVE needs core routers to install it so that the cost of deployment is higher. The D-WARD needs the cooperation of routers of the source network; otherwise, the attack traffic is dispersed to these routers so that the attack cannot be detected. The cost of deployment of our proposed scheme and other approaches is lower because they do not need the support of other nodes and the modification of the Internet.

Chapter 5. Conclusion and Future Work

There are many proposed approaches against DDoS attacks. They attempt to address these problems, include the overhead of the scheme, the accuracy of the detection, the effectiveness of the prevention and the deployment cost. However, there is no approach, which can solve these problems simultaneously. Although hybrid approaches endeavor to achieve the goal, the cost of the deployment is the greatest challenge.

In this thesis, the proposed scheme can accurately detect various types of attacks and effectively respond to attacks. The detection scheme detects attacks by analyzing the packet loss rate. It exploits these characteristics for DDoS attacks, including the enormous volume of traffic, spoofed packets and the occurrence of packet loss. The prevention scheme rate-limits or blocks the traffic according to the behavior of the traffic. Besides, the proposed scheme can still provide operations of the spoofed traffic, except the traffic to the victim, during attacks.

The greatest difficult is the overhead of the probe. In order to get the information of packet loss rate, we send some packets of ping to measure it. However, these packets will consume the bandwidth and the operation of the source router. In the future, the end-to-end measurement is expected to solve this problem although there are some challenges, which must be overcome presently. It can use few packets to estimate the packet loss rate based on mathematical theories.

Chapter 6. Reference

- [1] D. Moore, G. M. Voelker, and S. Savage, “Inferring Internet Denial-of-Service Activity,” in *Proceedings of the 10th USENIX Security Symposium*, pp. 9–22, August 2001.
- [2] Sourcefire, INC., *Snort: The Open Source Network Intrusion Detection System*. <http://www.snort.org>.
- [3] Cisco, *NetRanger Overview*. <http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/csids1/>
- [4] W. A. Simpson, “IKE/ISAKMP Considered Harmful,” *USENIX;login.*, vol. 24, pp. 48–58, December 1999.
- [5] C. Kaufman, R. Perlman, and B. Sommerfeld, “DoS protection for UDP-based protocols,” in *Proceedings of ACM Computer and Communication Security*, pp. 2–7, October 2003.
- [6] T. Aura, P. Nikander, and J. Leiwo, “DOS-Resistant Authentication with Client Puzzles,” *Lecture Notes in Computer Science*, vol. 2133, pp. 170–177, 2001.
- [7] J. Leiwo, P. Nikander, and T. Aura., “Towards network denial of service resistant protocols,” in *Proceedings of 15th International Information Security Conference*, August 2000.
- [8] G. R. Malan, D. Watson, F. Jahanian, and P. Howell, “Transport and Application Protocol Scrubbing,” in *Proceedings of IEEE INFOCOMM 2000*, vol. 3, pp. 1381–1390, March 2000.
- [9] X. Wang, Reiter, and M.K., “Defending against denial-of-service attacks with puzzle auctions,” in *Proceedings of IEEE Symposium on Security and Privacy*, pp. 78–92, May 2003.
- [10] A. Garg and A. L. N. Reddy, “Mitigation of DoS attacks through QoS regulation,” in *Proceedings of Tenth IEEE International Workshop on Quality of Service*, pp. 35–44, May 2002.

- [11] A. Juels and J. Brainard, "Client puzzles: A cryptographic countermeasure against connection depletion attacks," in *Proceedings of In Network and Distributed System Security Symposium*, pp. 151–165, March 1999.
- [12] F. Lau, S. H. Rubin, M. H. Smith, and L. Trajovic, "Distributed Denial of Service Attacks," *IEEE International Conference on Systems, Man, and Cybernetics*, vol. 3, pp. 2275–2280, October 2000.
- [13] C. Jin, H. Wang, and K. G. Shin, "Hop-count filtering: an effective defense against spoofed DDoS traffic," in *Proceedings of ACM Computer and Communication Security*, pp. 30–41, October 2003.
- [14] J. S. Shapiro and N. Hardy, "EROS: A Principle-Driven Operating System from the Ground Up," *IEEE Software*, vol. 19, pp. 26–33, January-February 2002.
- [15] R. Thomas, B. Mark, T. Johnson, and J. Croall, "NetBouncer: Clientlegitimacy-based High-performance DDoS Filtering," in *Proceedings of DARPA Information Survivability Conference and Exposition*, vol. 1, pp. 14–25, April 2003.
- [16] K. Park and H. Lee, "On the Effectiveness of Router-Based Packet Filtering for Distributed DoS attack and Prevention in Power-Law Internets," in *Proceedings of ACM SIGCOMM*, pp. 15–26, August 2001.
- [17] M. Sung and J. Xu, "IP Traceback-based Intelligent Packet Filtering: A Novel Technique for Defending Against Internet DDoS Attacks," in *Proceedings of IEEE Transactions on Parallel and Distributed Systems*, vol. 14, pp. 861–872, September 2003.
- [18] R. Mahajan, S. M. Bellovin, S. Floyd, J. Ioannidis, V. Paxson, and S. Shenker, "Controlling high bandwidth aggregates in the network," *ACM SIGCOMM Computer Communication Review*, vol. 32, no. 3, pp. 62–73, July 2002.
- [19] J. Ioannidis and S. M. Bellovin, "Implementing Pushback: Router-Based Defense Against DDoS Attacks," in *Proceedings of Network and Distributed System Security Symposium*, February 2002.

- [20] A. D. Keromytis, V. Misra, and D. Rubenstein, "SOS: Secure Overlay Services," in *Proceedings of ACM SIGCOMM*, pp. 61–72, August 2002.
- [21] A. D. Keromytis, V. Misra, and D. Rubenstein, "Using Overlays to Improve Network Security," in *Proceedings of SPIE ITCOM Conference on Scalability and Traffic Control in IP Networks II*, vol. 4868, pp. 245–254, July 2002.
- [22] W. G. Morein, A. Stavrou, D. L. Cook, A. D. Keromytis, V. Misra, and D. Rubenstein, "Using graphic turing tests to counter automated DDoS attacks against web servers," in *Proceedings of ACM Computer and Communication Security*, pp. 8–19, October 2003.
- [23] R. Stone, "CenterTrack: An IP Overlay Network for Tracking DoS Floods," in *Proceedings of 9th USENIX Security Symposium*, pp. 199–212, August 2000.
- [24] K. Park and H. Lee, "On the effectiveness of probabilistic packet marking for IP traceback under denial of service attack," in *Proceedings of IEEE INFOCOM 2001*, vol. 1, pp. 338–347, April 2001.
- [25] S. Savage, D. Wetherall, A. R. Karlin, and T. Anderson, "Practical Network Support for IP Traceback," in *Proceedings of ACM SIGCOMM*, pp. 295–306, August 2000.
- [26] H. Burch and B. Cheswick, "Tracing Anonymous Packets to Their Approximate Source," in *Proceedings of 2000 USENIX LISA Conference*, pp. 319–327, December 2000.
- [27] J. Li, J. Mirkovic, M. Wang, P. Reiher, and L. Zhang, "SAVE: source address validity enforcement protocol," in *Proceedings of IEEE INFOCOM 2002*, vol. 3, pp. 1557–1566, June 2002.
- [28] P. Ferguson and D. Senie, *Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing*. RFC 2827, May 2000.
- [29] G. Montenegro, *Reverse Tunneling for Mobile IP*. RFC 2344, May 1998.
- [30] T. M. Gil and M. Poletto, "MULTOPS: a data-structure for bandwidth attack detection," in *Proceedings of the 10th USENIX Security Symposium*, pp. 23–38, August 2001.
- [31] J. Mirkovic, G. Prier, and P. L. Reiher, "Attacking DDoS at the source," in *Proceedings*

- of 10th IEEE International Conference on Network Protocols, pp. 312–321, November 2002.
- [32] J. Mirkovic, G. Prier, and P. L. Reiher, “Source-End DDoS Defense,” in *Proceedings of IEEE Network Computing and Applications*, pp. 171–178, April 2003.
- [33] Cs3. Inc., *MANAnet DDoS White Papers*. <http://www.cs3-inc.com/mananet.html>.
- [34] C. Papadopoulos, R. Lindell, J. Mehringer, A. Hussain, and R. Govidan, “COSSACK: coordinated suppression of simultaneous attacks,” in *Proceedings of DISCEX III*, pp. 2–13, April 2003.
- [35] L. Feinstein, D. Schnackenberg, R. Balupari, and D. Kindred, “Statistical Approaches to DDoS Attack Detection and Response,” in *Proceedings of DARPA Information Survivability Conference and Exposition*, vol. 1, pp. 303–314, April 2003.
- [36] M. Robinson, J. Mirkovic, M. Schnaider, S. Michel, and P. Reiher, “Challenges and Principles of DDoS Defense.” submitted to SIGCOMM 2003.
- [37] The FreeBSD Project, *IPFW*. <http://www.freebsd.org>.
- [38] H. Burch and B. Cheswick, “Mapping the Internet,” *IEEE Computer*, vol. 32 (4), pp. 97–98, April 1999.
- [39] H. Burch and B. Cheswick, “Tracing Anonymous Packets to Their Approximate Source,” in *Proceedings of the USENIX Large Installation Systems Administration Conference*, pp. 319–327, December 2000.
- [40] R. Cascares, N. Duffield, J. Horowitz, and D. Towsley, “Multicast-based inference of network-internal loss characteristics,” in *Proceedings of IEEE Transactions on Information Theory*, vol. 45, pp. 462–2480, November 1999.
- [41] K. Ishibashi, M. Aida, and S. ichi Kuribayashi, “Estimating packet loss-rate by using delay information and combined with change-of-measure framework,” in *Proceedings of Global Telecommunications Conference*, vol. 7, pp. 3878–3882, December 2003.
- [42] N. Duffield, F. Lo Presti, V. Paxson, and D. Towsley, “Inferring link loss using striped

unicast probes,” in *Proceedings of IEEE INFOCOM 2001*, vol. 2, pp. 915–923, April 2001.

