PAPER Special Section on New Challenge for Internet Technology and its Architecture

Collaborative Defense Mechanism Using Statistical Detection Method against DDoS Attacks*

ByungHak SONG[†a)], **Joon HEO**[†b)], *Nonmembers*, *and* **Choong Seon HONG**[†c)], *Member*

SUMMARY Distributed Denial-of-Service attack (DDoS) is one of the most outstanding menaces on the Internet. A DDoS attack generally attempts to overwhelm the victim in order to deny their services to legitimate users. A number of approaches have been proposed for defending against DDoS attacks accurately in real time. However, existing schemes have limits in terms of detection accuracy and delay if the IDRS (Intrusion Detection and Response System) deployed only at a specific location detects and responds against attacks. As in this case, it is not able to catch the characteristic of the attack which is distributed in large-scale. Moreover, the existing detection schemes have vulnerabilities to intellectual DDoS attacks which are able to avoid its detection threshold or delay its detection time. This paper suggests the effective DDoS defense system which uses the collaborative scheme among distributed IDRSs located in the vicinity of the attack source or victim network. In proposed scheme, both victim and source-end IDRS work synergistically to identify the attack and avoid false alarm rate up to great extent. Additionally, we propose the duplicate detection window scheme to detect various attacks dynamics which increase the detection threshold gradually in early stage. The proposed scheme can effectively detect and respond against these diverse DDoS attack dynamics.

key words: *IDS, DDoS attack, statistical detection, collaborative defense, detection threshold*

1. Introduction

Distributed Denial-of-Service attack (DDoS) is one of the most outstanding menaces on the Internet. A DDoS attack generally attempts to overwhelm the victim in order to deny their services to legitimate users. It can be divided into three types, TCP SYN [1], UDP, and ICMP flooding. First, TCP SYN flooding attack takes aim at the exhaustion of system resources. Zombie agents send repeatedly SYN packets spoofed with unreachable source addresses in TCP 3-way handshaking. Then the backlog queue of the victim is filled with SYNs. Eventually, it becomes a denial-of-service state as the system waits on ACKs infinitely. Next, in UDP flooding attack, zombie agents send excessive UDP packets to the victims which play a role of slaves reflecting the malicious packets to other victims. Then victims are damaged by the network traffic overload among themselves. Lastly, ICMP flooding attack abuses the vulnerability that ICMP does not support specific services or port numbers. It has the representative type that zombie agents broadcast ICMP echo request message spoofed by victim's source address to the reachable hosts. And they transmit flooding ICMP echo reply messages to the victim.

There are common characteristics of DDoS attacks traffic [2]. First, it has large volume aggregated from distributed sources to overwhelm victim. Second, it is difficult to precisely identify malformed packets from legitimate packets. Lastly, in most of the DDoS attack, zombie agents send the attack packets which have spoofed source IP address. Therefore, the detection mechanism in IDRS must catch these features of attack in early stage. Figure 1 describes the typical model of DDoS attack.

The existing defense approaches which operate apart are difficult to efficiently detect and respond against DDoS attack which has distributed type in large-scale [3]. And in order to identify accurate attack source, IDRS should be based on the detection scheme which has very low false alarm rate. Thus, it is important to cooperate among IDRSs which have high detection accuracy. According to our research, many distributed IDRSs have a good performance in a typical or specific attack traffic feature. However, various transformed attack types [4] still threaten them. Therefore, we propose an integrated mechanism which enhances the detection accuracy of collaborative IDRS and efficiently responds according to the collected information from distributed IDRSs. Besides, an approach which detects the crafty DDoS (DoS) attack that avoids the detection threshold of IDRS is suggested.

The term IDRS is used to indicate a system which has both the Intrusion Detection and Intrusion Response capa-

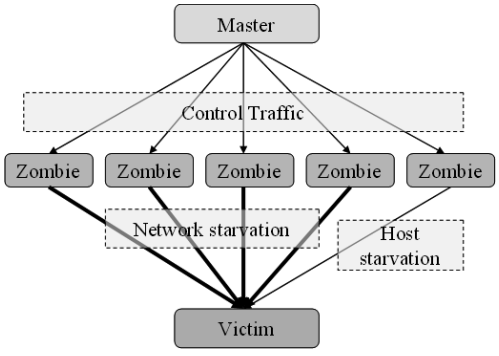


Fig. 1 Distributed denial of service model.

Manuscript received January 29, 2007.
Manuscript revised April 23, 2007.

[†]The authors are with the Department of Computer Engineering, Kyung Hee University, 1 Seocheon, Giheung, Yongin, Gyeonggi 449-701, Korea.

*This work was supported by MIC and ITRC Project. Dr. C.S. Hong is the corresponding Author.

a) E-mail: bhsong@khu.ac.kr
b) E-mail: heojoon@khu.ac.kr
c) E-mail: cshong@khu.ac.kr

DOI: 10.1093/ietcom/e90–b.10.2655

bilities. Intrusion detection means that the system is capable of detecting an intrusion. On the other hand, Intrusion response refers the actions taken to avoid this intrusion, for instance changing rule in Firewall or tracing back an attack path. Our system comprises of both Intrusion Detection and Intrusion Response modules. Our architecture uses statistical methods to detect an intrusion or attack. Whereas the bases of response mechanism are provided by dropping the malicious packets at source-end IDRS and by initiating the rate limiting Alert request from victim-end IDRS.

The remainder of the paper is organized as follows. Section 2 mentions about related work studied together with our research. In Sect. 3, statistical detection algorithms used in the proposed scheme are introduced. Section 4 addresses several attack types. Section 5 describes collaborative defense mechanism using the statistical detection method. In Sect. 6, we analyze the performance of the collaborative defense mechanism against existing schemes. Finally, Sect. 7 gives concluding remarks and future directions.

2. Related Work

We are able to classify IDRS into source-end and victim-end IDRS according to its deployed location. Figure 2 shows the location of each IDRS. In general, most of IDRSs are placed at the vicinity of edge router of victim network as it is the most suitable place for detecting the symptom of DDoS attack [5]. In other words, victim-end detector is able to identify the feature of DDoS attack with ease due to the traffic volume aggregated toward victim-end IDRS from distributed zombie agents. However, it has complicated response methods and slow response time.

IP traceback [6], the most well-known response scheme at victim-end IDRS, reconstructs its route by packets marked with probabilistic method at core routers and chases the attack source. There are famous traceback techniques, PPM (Probabilistic Packet Marking), ICMP traceback, and Hash-based traceback. It has an advantage that the source can be found. However, it is not efficient in terms of involvement and operation. First of all, it is hard to obtain sufficient routers for marking packets. And it is hard to gather enough packets for the traceback due to the overload of core routers under attacks. Furthermore, it is also hard for a receiving host to collect enough marking packets, since DDoS attacks have the distributed feature.

In contrast, source-end IDRSs [7], [8] have a good performance in terms of packet filter or rate limit. However, it is very hard to identify DDoS attack flows at the source since the traffic is not so aggregated. Therefore, it has high false alarm rate.

D-WARD [7] is one of the most famous source-end defense methods. It detects abnormal traffic based on the rate of sent and received packets and bytes and the number of allowed connections per destination host in a source-end detector. Abnormal traffic is restricted by its rate limiting method.

Several studies [9], [10] have been made on cooperative defense mechanism which has focused on the response method among the detection components. However, it is hard to identify precisely the attack source if accurate detection mechanism is not supported.

3. Statistical Detection Methods

It is difficult to distinguish malicious packets from legitimate packets because attackers use general packets for DDoS attack. And we have to consider the detection accuracy and complexity in order to detect the attack [11]. For these reasons, a statistical detection method is efficient for detecting DDoS attack. In representative statistical method, packet inter-arrival time, entropy [12], [13] and chi-square [12], [13] algorithm are used. We'll briefly discuss these terms in following section.

First, we calculate the packet inter-arrival time, T, at specific interface by using following equation. Where, $PAT[i]$ is the arrival time of a packet i.

$$T = PAT[i] - PAT[i-1], \quad PAT[0] = 0$$

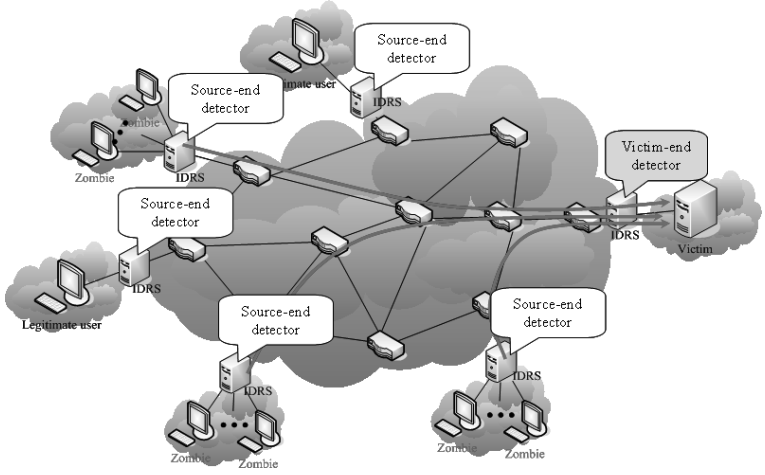


Fig. 2 Source-end and victim-end IDRS.

For a constant buffer size for instance, one buffer is composed of 100 packets, as the ingress traffic increases, the value of T will be decreased.

Second, with the help of entropy scheme, we calculate the randomness in receiving packets with respect to any property of a packet, for example, source IP address. The entropy H of a property i can be calculated as follows.

$$H = -\sum_{i=1}^{n} p_i \log_2 p_i$$

Where p_i is the probability, that ith property will be selected.

Finally, the chi-square scheme calculates the degree of dispersion of the current traffic profile from the baseline. We can determine chi-square statistic x^2, as follows:

$$x^2 = \sum_{i=1}^{B} \frac{(N_i - n_i)^2}{n_i}, \quad n_i = \frac{n}{B}, \quad n = \text{total sample size}$$

For details of the parameters N_i, B and n_i please refer [12] and [13]. We'll apply the above statistical models at different levels in our architecture to identify an attack and will be discussed in Sect. 5 in detail.

4. DDoS Attack Types

Four Attacks in Fig. 3 discussed in [4] are representative bandwidth attack dynamics which can be detectable by the proposed detection mechanism described in Sects. 5.1~5.2. First, Fig. 3(a) is the typical DDoS attack increasing suddenly to its maximum throughput, P_m. Second, Fig. 3(b) is the increasing rate attack which raises gradually the traffic volume from t_0 to t_1 in order to delay the detection time and remains constant after that. Next, in Fig. 3(c), the attack bandwidth depicts abrupt increases and decreases repeatedly. Finally, the gradual raise and rapid drop are recursively shown in the graph of Fig. 3(d). Both Fig. 3(c) and Fig. 3(d) have the attack type that can evade the detection threshold and drain victim's resources.

5. Collaborative Defense Mechanism against DDoS Attacks

We suggest the method to improve detection and response performance by using a cooperation scheme among distributed IDRSs. And each IDRS uses a proposed statistical detection scheme for reducing false negative rates. In addition, we propose an enhanced mechanism in order to detect the intelligent DDoS attack avoiding the detection threshold value of the IDRS.

Figure 4 shows the overall proposed system architecture and operation. It consists of source-end IDRS, victim-end IDRS, and aggregate server component. An IDRS has source-end and victim-end IDRS component. We can distinguish between source-end and victim IDRS by the feature of abnormal symptoms. The feature is describes in Sect. 5.1.

Our architecture contains IP spoofing inspection module which can filter out the packets not from the legitimate address pool. Therefore, an attacker can not spoof his IP addresses if he wants to and can not hide the actual origin of the attack. Additionally, our architecture is strengthened by source-end IDRS which can provide useful information, for instance, ingress point of attack, to infer anything about the

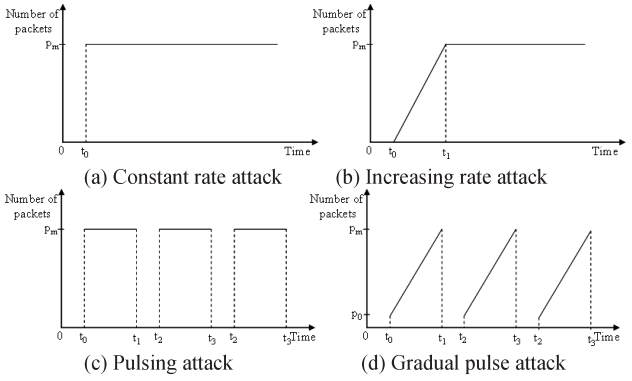


Fig. 3 Detectable attack dynamics.

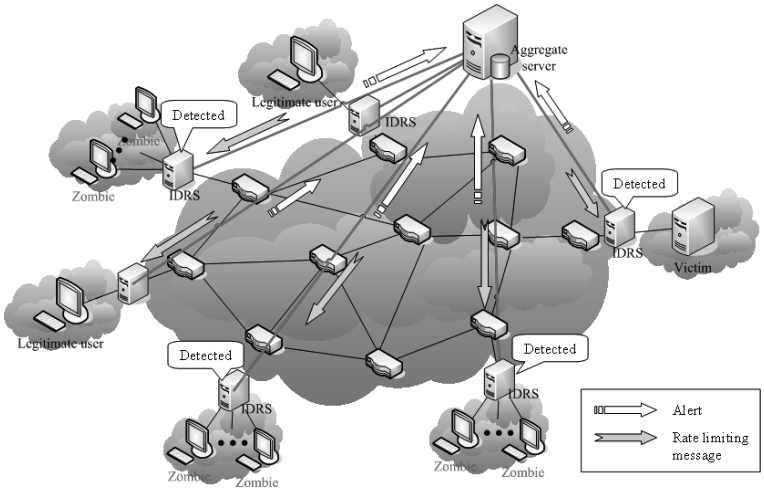


Fig. 4 Proposed system architecture.

source of the attack. Therefore, the proposed mechanism is effective in identifying the attack source(s). The other method of identifying the attack source is to use traceback techniques. However, even with most of the effective traceback techniques a victim can not find the actual source of the attack. The victim host is only able to identify the network or the address of the router closest to the attacker. In our scheme, the attack is identified by the coordination of victim-end, source-end IDRSs and Aggregate server. After getting Alert signal from the victim-end IDRS, the Aggregate server can know the injection point of the attack and the probable network of the attacker with the help of source-end IDRS.

5.1 IDRS Operation

A detection framework of IDRS is organized by two modules. One is IP spoofing inspection module and another is DDoS attack detection module.

IP spoofing inspection module is needed for source-end IDRS. This module, filters out the outgoing packets which don't include the source IP address of their own network. Therefore, zombie agents cannot use the fake source IP address of outside networks. Before getting insight of our scheme, it is better to clear two key terms used in this paper. We use the term 'sent packets' for those packets which are coming from the own network of the IDRS whereas the term 'received packets' is used to refer the packets that are coming from the other networks.

DDoS attack detection module perceives abnormal symptom by using four algorithms, packet inter-arrival time, source address entropy, chi-square, and destination address entropy. And it classifies source-end and victim-end IDRS based on these values. Figure 5 shows the overall detection procedure in IDRS.

The seven detection threshold values, $T(x)$, are calculated every observation interval by using weighted average, μ, and normal distribution values, σ. If the detecting values are closer to the average, the traffic will be considered normal else not. We determine the threshold values as follows:

$$\mu_n(x) = \alpha\mu_{n-1}(x) + (1-\alpha)\mu_{n-2}(x), \quad 0 < \alpha < 1$$

$$T(x) = \mu_n(x) \pm k\sigma(x), \quad k = 1,\ 2,\ 3\cdots$$

where $x = T,\ \dfrac{H_s(s)}{H_s(r)},\ x^2(s),\ x^2(r),\ \dfrac{H_d(s)}{H_d(r)}$

μ: average

α: weighted value

σ: standard deviation

$H_s(s)$: source address entropy of sent packets

$H_s(r)$: source address entropy of received packets

$H_d(s)$: destination address entropy of sent packets

$H_d(r)$: destination address end entropy of received packets

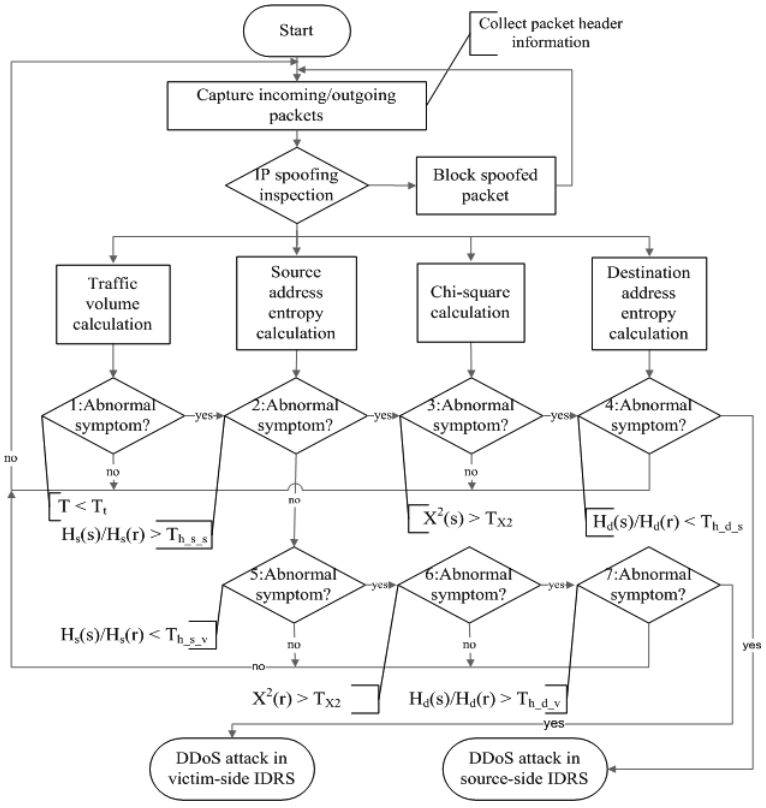


Fig. 5 Detection mechanism.

5.1.1 Source-End IDRS

When attacks happen, the packet inter-arrival time, T, of the total packets decreases. Therefore, when T is smaller than its threshold, T_t, we can suspect a DDoS attack. As a number of zombie agents increases source address entropy, $H_s(s)$, of packets sent through source-end IDRS increases and its destination address entropy, $H_s(r)$, of packets received by the IDRS decreases. Therefore, the rate of source address entropy, $H_s(s)/\ H_s(r)$, of sent and received packets suddenly rises. On the other hand, the ratio $H_d(s)/\ H_d(r)$ is rapidly reduced due to its opposite property. Based on these parameters, we can decide suspicious packets as DDoS attack when the rate of source address entropy exceeds its threshold value, T_{Hs}, and the rate of destination address is smaller than its threshold value, T_{Hd}. Moreover, when attacks occur, chi-square, $X^2(s)$, of sent packets from the IDRS abruptly gets bigger because zombie agents in attack source networks send an amount of packets which include more distributed source IP addresses than its previous statistics. Hence, the inspected packets are regarded as suspicious packets when the calculated chi-square exceeds its threshold value, T_{x2}.

When all four detection parameters compared with their threshold values simultaneously exceed, source-end IDRS is able to conclude the DDoS attack. As a result, it sends an alert message to aggregate server.

Packet inter-arrival time

$$T < T_t$$

T: traffic volume

T_t: threshold of traffic volume (1)

Rate of source address entropy

$$\frac{H_s(s)}{H_s(r)} > T_{H_s}$$

$H_s(s)$: source address entropy of sent packets

$H_s(r)$: source address entropy of received packets

T_{H_s}: threshold of source address entropy (2)

Chi-square

$$x^2(s) > T_{x^2}$$

$x^2(s)$: chi-square of sent packets

T_{x^2}: threshold of chi-square (3)

Rate of destination address entropy

$$\frac{H_d(s)}{H_d(r)} < T_{H_d}$$

$H_d(s)$: destination address entropy of sent packets

$H_d(r)$: destination address entropy of received packets

T_{H_d}: threshold of destination address entropy (4)

5.1.2 Victim-End IDRS

On the victim side the *sent* packets from source-end IDRS will be treated as *received* packets therefore, the values of source address entropy, chi-square, and destination address entropy have opposite meanings as compared to source-end IDRS. Consequently, when the values of $H_s(s)/H_s(r)$ is smaller than the legitimate threshold range and the value of $H_d(s)/H_d(r)$ is bigger than the threshold, the traffic will be considered as the attacking traffic. Same as source-end IDRS, after detecting the DDoS attack the alert message is also sent to the aggregate server. Along with identification of attack, the Alert message also contains the address of the victim-end IDRS based on which the Aggregate server can distinguish between source end and victim-end IDRS. Figure 5 shows the victim and source-end IDRS operation in detail.

5.2 Aggregate Server Operation

Aggregate server gathers the alert messages detected at source-end and victim-end IDRS. Based on received messages the aggregate server takes a decision whether the attack happens or not. It makes a comparison among the alert messages from source-end and victim-end IDRS because the detection accuracy of victim-end IDRS is higher than that of source-end IDRS. On receiving Alert message, the aggregate server sends rate limiting messages to the source-end IDRSs. And it restricts the traffic bandwidth which exceeds its normal threshold range in attack source network. Additionally, it analyzes the alert information and calculates its statistics of port number, protocol type, flag, and so on. It also provides the specific attack information to the network operator of source-end and victim-end IDRS. The operation of aggregate sever is depicted in Fig. 6.

5.3 Intelligent DDoS Attack Detection Method

Figure 7 shows increasing-threshold attack. The attack traffic is able to grow the detection threshold gracefully without any exposure for a long time. In the end, it paralyzes the services of ISP (Internet Service Provider) by its network starvation. Therefore, it is a threat for the ISPs which have to provide continuously stable services.

Increasing-threshold attack has the feature that it slowly increases source address entropy and decreases packet inter-arrival time and destination address entropy. The chi-square used in short-term detection interval is hard to detect abnormal symptom if the distribution of source IP addresses rise at a slow rate because it compares inspecting sample packets with its previous expected value. Consequently, packet inter-arrival time, source address entropy, and destination address entropy of each detection threshold value calculated in the short-term detection interval and used for detecting various features of increasing-threshold attack. Generally, NMS (Network Management System)

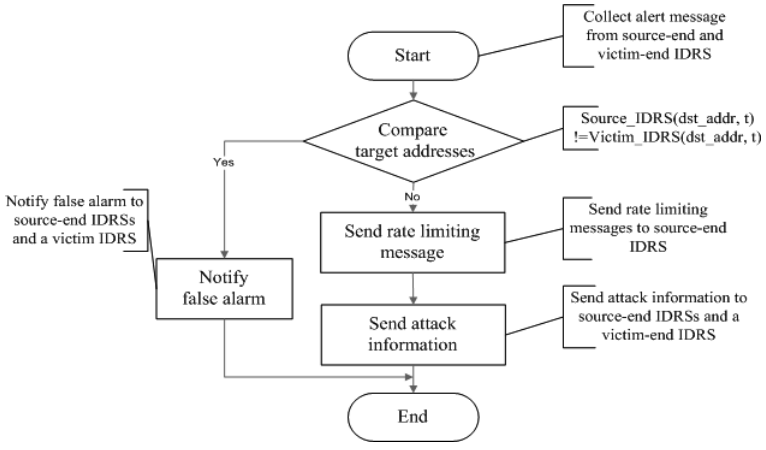


Fig. 6 Aggregate server operation.

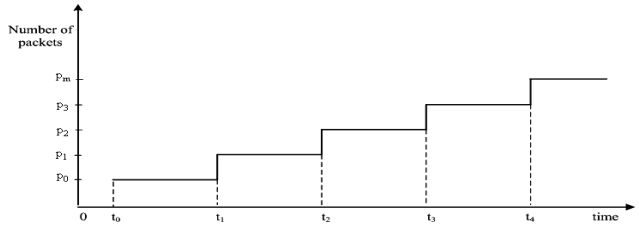


Fig. 7 Increasing-threshold attack.

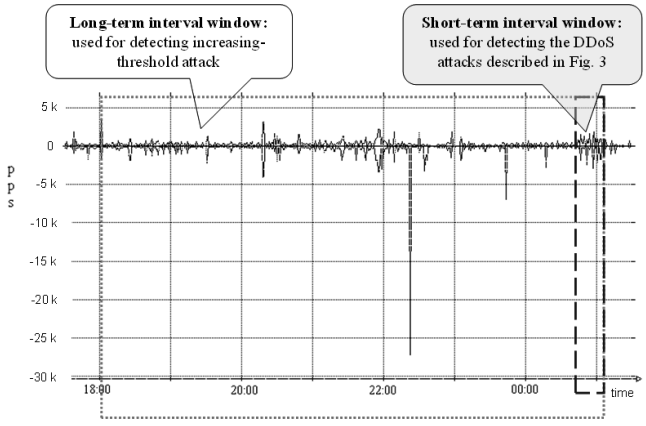


Fig. 8 Duplicate detection window method.

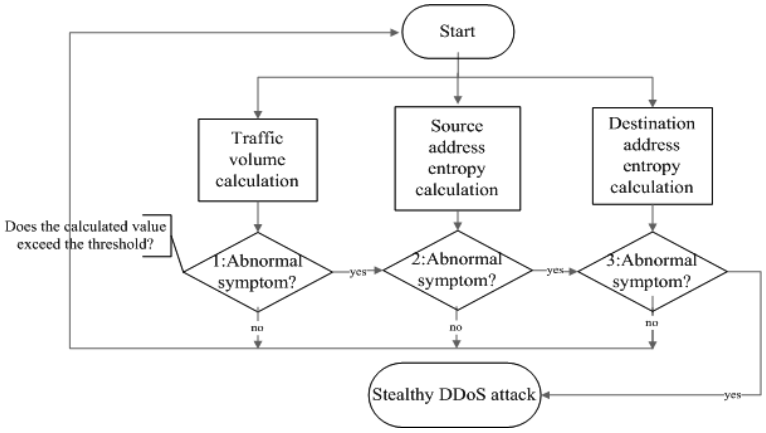


Fig. 9 Flowchart of increasing-threshold attack detection mechanism.

has the static threshold value to detect bandwidth attacks threatening its system. However, it doesn't have proper response time. Duplicate detection window method provides the bases of detecting increasing-threshold attack in early stages. Traffic pattern showed in Fig. 8 is the actual data of approximately 8 hours gathered from KOREN (KOrea REsearch Network). Values on positive y-axis show the outgoing packets from campus network to KOREN. While the values on negative y-axis show the incoming packets from KOREN to campus network. It shows the relative scale of short-term and long-term interval window which is used in duplicate detection window method. The window sizes can be changed according to the conditions of the network. Increasing-threshold attack detection mechanism

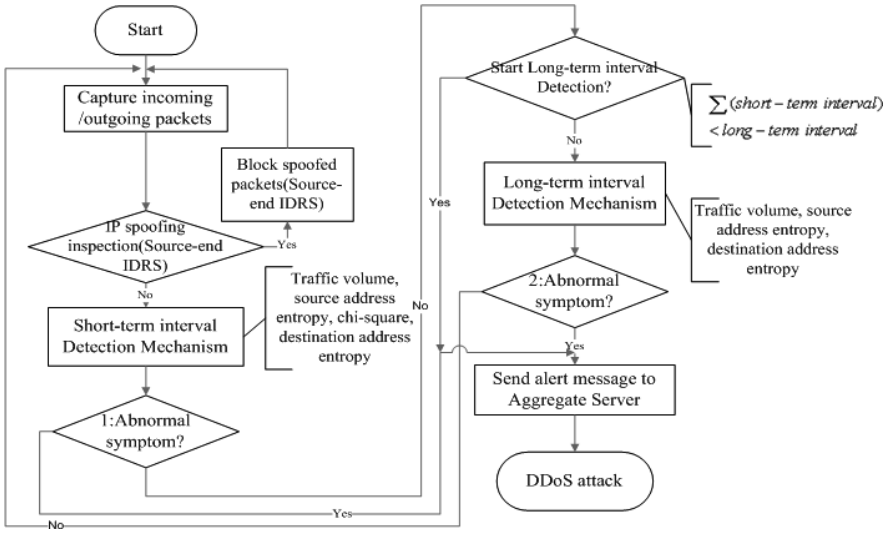


Fig. 10 Overall detection mechanism.

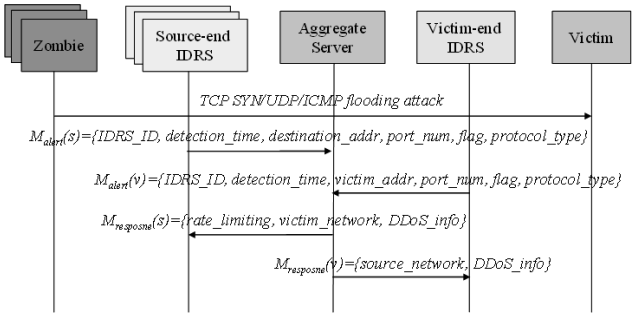


Fig. 11 Collaborative defense system.

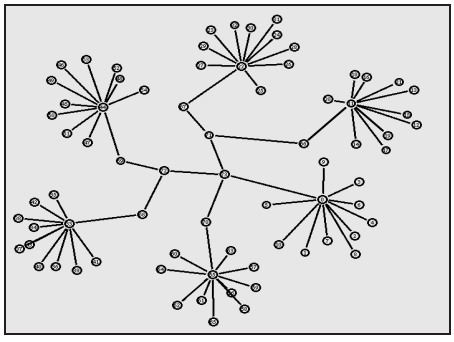


Fig. 12 NS-2 network topology.

which uses the duplicate detection window method is represented in Fig. 9.

Figure 10 shows the flowchart of the overall detection mechanism which includes the intelligent DDoS attack detection component. The SDM (Short-term interval detection mechanism) module which uses four detection algorithms, T, H_s, x^2, and H_d, detects four DDoS attack dynamics shown in Fig. 11. Then, it sends an alert message if abnormal traffic is detected. If attacks are not detected in the SDM module, LDM (Long-term interval detection mechanism) module inspects the transformed attacks shown in Fig. 7 during its extended time by calculating T, H_s, and H_d. Similarly, when the LDM module alarms, it transmits alert message and limits the bandwidth of its attack source network.

6. Performance Evaluation

6.1 Simulation Environment

We analyze the performance of the proposed detection and response mechanism by using NS-2 (Network Simulator 2) on Linux redhat 9.0 and to Stacheldraht v4 [14] which is one of the well known tools for attack tests. The simulated network topology is composed like Fig. 12 and each link is connected by 100 Mbps. There are five edge routers of attack source network and each edge router is linked with legitimate and attack node. In the source-end edge router, the generated legitimate traffic is about 200 Kbps and the maximum network bandwidth is about 2,000 Kbps under DDoS attack. And in victim network, normal traffic is about 1,000 Kbps and maximum abnormal traffic is about 10 Mbps. The graph of Fig. 13 shows the normal and abnormal traffic bandwidth of the attack source and victim network.

6.2 Performance Evaluation Metrics

We have three factors, detection delay, detection rate, and false negative rate, for estimation of the detection performance [15]. The detection delay, T_d, is calculated by the time gap between T_a and T_s. T_a is the time that alarm is raised and T_s is the time that DDoS attack is started. The earlier IDRS detects, the lower T_d is gained.

$T_d = T_a - T_s$

T_d: detection delay

T_a: time alarm is raised

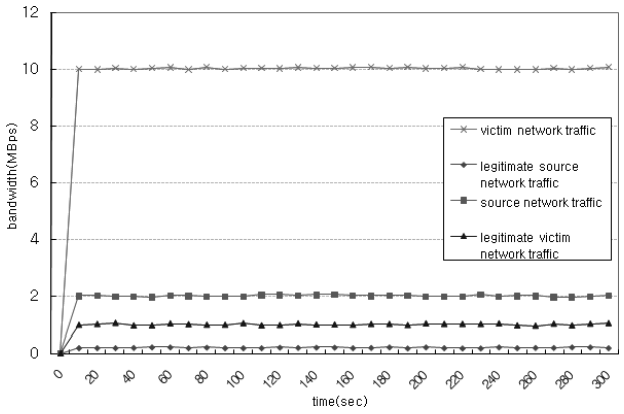


Fig. 13 Attack and legitimate traffic bandwidth.

T_s: time DDoS attack is started

Detection rate, R_d, means the number of detected attack packets, N_d, divided by the total number of attack packets, N_a. Therefore, the more accurate IDRS detects, the higher R_d is calculated.

$$R_d = \frac{N_d}{N_a}$$

R_d: detection rate

N_d: number of detected attacks

N_a: total number of attacks

False negative rate, R_f, is the number of false negative packets, N_f, divided by the total number of attack packets, N_a. So the more legitimate packets which are detected as DDoS attack, the higher R_f is gained.

$$R_f = \frac{N_f}{N_a}$$

R_f: false negative rate

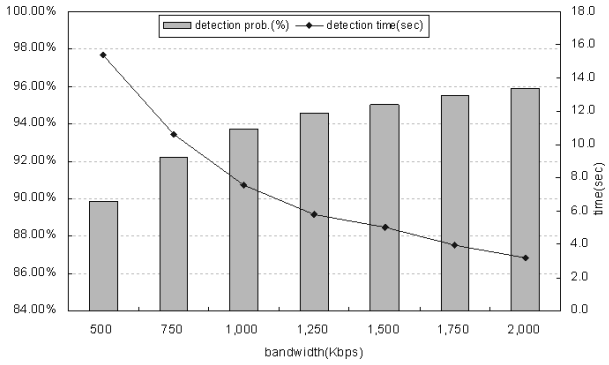
N_f: number of false negative packets

N_a: total number of attacks

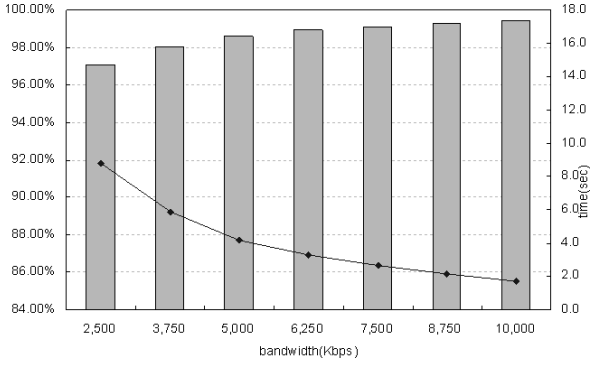
6.3 Simulation Result

Figure 14 depicts the simulated result of the detection time and rate in source-end and victim-end IDRS. In both IDRSs, as the attack bandwidth grows, attack detection rate increases and detection delay decreases. The more aggregate traffic is generated hugely, the more accurately and early an IDRS can catch the symptoms of DDoS attack. In this experiment, there is little difference of the detection rate between source-end and victim-end IDRS and it is 3.5~7.3% due to the number of zombie agents. We expect that the gap of detection rate will grow if the number of the agents increases.

Table 1 shows false negative rate of each IDRS. As attack bandwidth increases, false negative rate decreases. The rate of victim-end IDRS is 13.8~28.8% of source-end IDRS. The gap between source-end and victim-end IDRS will be



(a) Attack source network.



(b) Attack source network.

Fig. 14 Detection time and rate.

Table 1 False negative rate.

Source-end (Kbps)	*Victim-end (Kbps)*	*Source-end R_f (%)*	*Victim-end R_f (%)*
500	2500	10.2	2.9
750	3750	7.8	2.0
1000`	5000	6.3	1.4
1250	6250	5.4	1.1
1500	7500	5.0	0.9
1750	8750	4.5	0.7
2000	10000	4.1	0.6

Table 2 Defence delay and accuracy.

Source-end (Kbps)	*Victim-end (Kbps)*	*Defense delay (sec)*	*Defense accuracy (%)*
500	2500	15.8	97.1
750	3750	10.8	98.0
1000	5000	7.8	98.6
1250	6250	6.0	98.9
1500	7500	5.2	99.1
1750	8750	4.2	99.3
2000	10000	3.4	99.4

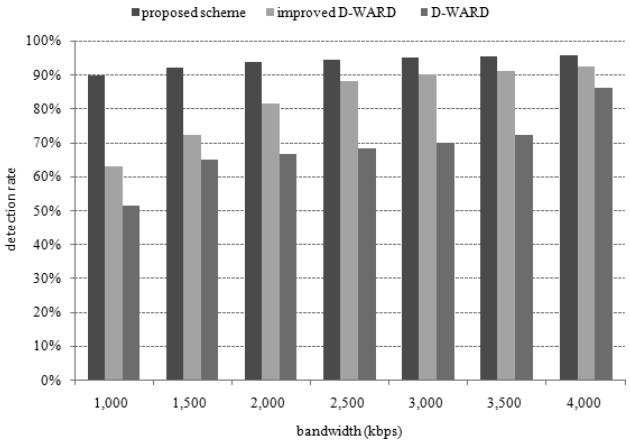


Fig. 15 Comparison of detection rates.

Table 3 Comparison of DDoS attack defense methods.

		Proposed scheme	*D-WARD*	*IP Traceback (PPM)*
ISP involvement		Middle	Low	High
Delay	Detection delay	Middle	Middle-Low	Depends on its detection algorithm
	Response delay	Low	Low	Middle-High
Accuracy	Detection accuracy	High	Middle	Depends on its detection algorithm
	Response accuracy	High	Middle	Middle
False negative rate		Low	Middle	Depends on its detection algorithm
Memory		Middle	Middle-Low	Middle-High
Complexity		Middle	Middle-Low	Middle-High

wide as the number of zombie agents increases.

The defense delay and accuracy of the proposed scheme are shown in Table 2. The defense accuracy represents the degree of how veracious IDRS can find the attack source. The defense accuracy has a good performance for its delay since the proposed IDRS chases the source with the accuracy of victim-end IDRS.

Figure 15 shows the comparison results of the proposed scheme with D-WARD and improved D-WARD. The gap in detection rate between proposed and D-WARD is 9.7~38.3%. And the gap of detection rate between proposed and improved D-WARD scheme is 3.3~26.7%.

Table 3 compares the proposed mechanism with D-WARD and traceback schemes and presents the relative measurement with them. The three defense methods have their advantages and disadvantages. One of the well known response method IP traceback is dependent on the accuracy of its underlying IDS system. Moreover, traceback accuracy depends upon the algorithm in use, whether we are using packet marking, messaging or hashing algorithm. Therefore, the evaluation of traceback techniques is out of the scope as most of the characteristic of traceback techniques are not common to our architecture. However, here we compare our scheme to the most well acclaimed traceback technique i.e. PPM (probabilistic packet marking). On the other hand D-WARD is only the source-end IDRS therefore we will compare the source-end IDRS part of our scheme with D-WARD.

ISP Involvement: D-WARD is installed just at the edge router whereas PPM requires that all routers in core network support the marking scheme. Therefore, the involvement level of D-WARD and PPM is Low and High respectively. On the other hand, the proposed scheme is the middle level because it needs the cooperation among edge routers.

Our test bed works in a single administrative domain and for the sake of simplicity, the working mechanism of proposed scheme is discussed for this scenario only. Inter-administrative domain IDRS implementation is not possible right now as it will require BLA (Business Level Agreement) and SLA (Service Level Agreement). And finding a unified solution for inter-domain IDRS is another issue itself. Most of the technically sound IDRS techniques might not be applicable in multiple administrative domains without having any mutual and legal collaboration.

However, if such agreement is present, hierarchical deployment of proposed scheme is required. One or multiple Aggregate servers could reside in each administrative domain and would be responsible for managing internal resource demands, resources and security aspects as well as setting up bilateral agreement with neighboring domains. On DDoS attack, the origin of an attack can be found with the collaboration of participating Aggregation Servers and the steps described in earlier sections will be applied recursively on each domain. It is not possible for us to show this whole procedure in limited space. The basic working has already been explained and will remain same for Inter-domain intrusion detection system.

Detection Delay: The D-WARD detection procedure which operates in source network is simpler than the proposed scheme. Therefore, the detection delay of the proposed scheme is higher than D-WARD. Whereas, in case of PPM, it depends upon the underlying IDS.

Accuracy: The accuracy of detection and response is the highest and its false negative rate is the lowest among other defense methods as victim and source-end IDRSs work synergistically to detect the attack.

Memory Usage and Complexity: The memory usage and complexity is higher than D-WARD due to the cooperation overhead among the distributed IDRSs. But it is lower than PPM in which all of the core routers mark the suspicious packets.

7. Conclusion

Obviously, we need the defense method which cooperates among dispersed IDRSs for the reason that the independent and isolated detection scheme is difficult to defend efficiently against DDoS attack which has a distributed feature. And in order to detect the DDoS attack which is hard to classify into anonymous and legitimate packets under DDoS attack, statistical detection method is necessary. Therefore,

this paper presented the problem of the existing defense techniques and the solution brought the detection scheme into focus.

Our scheme uses packet inter-arrival time, source address entropy, chi-square, and destination address entropy to accurately detect the DDoS attack. Furthermore, in proposed mechanism, both victim and source-end IDRS work synergistically to identify the attack and avoid false alarm rate up to great degree. On the other hand, related schemes are based on only source-end or victim-end IDRS. Along with all above reasons, with the help of IP spoofing inspection module we are able to reduce spoofed IP attacks. Due to all above factors, we can say that the proposed scheme has an edge over other proposed schemes.

For future work, the number of aggregate sever can be more than one when the proposed scheme is applied to the large-scale network. So, we will consider the defense scheme which shares the information among aggregate servers.

References

[1] Computer Emergency Response Team, CERT Advisory CA-1996-21 TCP SYN Flooding Attacks. http://www.cert.org/advisories/CA-1996-21.html, Sept. 1996.
[2] D. Moore, G.M. Voelker, and S. Savage, "Inferring Internet denial-of-service activity," Proc. Usenix Security Symposium, pp.9–22, Usenix Assoc., 2001.
[3] J. Mirkovic, M. Robinson, and P. Reiher, "Alliance formation for DDoS defense," Proc. 2003 Workshop on New Security Paradigms, pp.11–18, 2003.
[4] J. Mirkovic and P. Reiher, "A taxonomy of DDoS attack and DDoS defense mechanisms," ACM SIGCOMM Computer Communication Review, vol.34, no.2, pp.39–53, April 2004.
[5] M. Ratul, M. Steven, F. Sally, I. John, P. Vern, and S. Scott, "Controlling high bandwidth aggregates in the network," ACM SIGCOMM Computer Communication Review, vol.32, no.3, pp.62–73, July 2002.
[6] A. Belenky and N. Ansari, "On IP traceback," IEEE Commun. Mag., vol.41, no.7, pp.142–153, July 2003.
[7] J. Mirkovic and P. Reiher, "D-WARD: A source-end defense against flooding denial-of-service attacks," IEEE Trans. Dependable and Secure Computing, vol.2, no.3, pp.216–232, Sept. 2005.
[8] T.M. Gil and M. Poletto, "MULTOPS: A data-structure for bandwidth attack detection," Proc. 10th Usenix Security Symposium, pp.23–38, Aug. 2001.
[9] J. Mirkovic, M. Robinson, and P. Reiher, "Alliance formation for DDoS defense," New Security Paradigms Workshop, pp.11–18, Aug. 2003.
[10] C. Papadopoulos, R. Lindell, J. Mehringer, A. Hussain, and R. Govindan, "Cossack: Coordinated suppression of simultaneous attacks," DARPA Information Survivability Conference and Exposition, pp.2–13, April 2003.
[11] G. Carl, G. Kesidis, R.R. Brooks, and S. Rai, "Denial-of-service attack-detection techniques," IEEE Internet Comput., vol.10, no.1, pp.82–89, Jan./Feb. 2006.
[12] L. Feinstein, D. Schnackenberg, R. Balupari, and D. Kindred, "Statistical approaches to DDoS attack detection and response," DARPA Information Survivability Conference and Exposition (DISCEX 2003), pp.303–314, April 2003.
[13] C.E. Shannon and W. Weaver, The Mathematical Theory of Communication, University of Illinois Press, 1963.
[14] The "stacheldraht" distributed denial of service attack tool, http://staff.washington.edu/dittrich/misc/stacheldraht.analysis
[15] Y. Chen and K. Hwang, "Collaborative change detection of DDoS attacks on community and ISP networks," International Symposium on Collaborative Technologies and Systems (CTS'06), pp.401–410, 2006.
[16] J. Kang, Z. Zhang, and J.-B. Ju, "Protect e-commerce against DDoS attacks with improved D-WARD detection system," 2005 IEEE International Conference on e-Technology, e-Commerce and e-Service (EEE'05), pp.100–105, 2005.

ByungHak Song received the B.S. and M.S. degrees in Department of Computer Engineering from Kyung Hee University, South Korea, in 2005 and 2007. Currently he is an engineer in Department of New Tec. Development from PLANTYNET Co., Ltd., South Korea. His research interest includes Network Security, Network Management, IPv6, and Broadband Network.

Joon Heo received the B.S. and M.S. degrees in Department of Computer Engineering from Kyung Hee University, South Korea, in 2002 and 2004. Currently he is researching in Networking Laboratory and pursuing his Ph.D. in Computer Engineering at Kyung Hee University, South Korea. His research interest includes Security in Wireless Mobile Ad Hoc and Sensor Networks, Secure routing, Key management in Wireless Sensor Networks.

Choong Seon Hong received his B.S. and M.S. degrees in electronics engineering from Kyung Hee University, Seoul, Korea, in 1983, 1985, respectively. In 1988 he joined KT, where he worked on Broadband Networks as a member of the technical staff. From Sept. 1993, he joined Keio University, Japan. He received the Ph.D. degree at Keio University in March 1997. He had worked for the Telecommunications Network Lab, KT as a senior member of technical staff and as a director of the networking research team until August 1999. Since September 1999, he has worked as a professor of the School of Electronics and Information, Kyung Hee University. His research interests include Ad hoc Networks, Network Security and Network Management. He is a Member of IEEE, IPSJ, KISS, KIPS, and KICS.