한국시뮬레이션학회 논문지
Vol. 19, No. 4, pp. 139-149 (2010. 12)

False Alarm Rate 변화에 따른 DoS/DDoS 탐지 알고리즘의 성능 분석

장범수[1] · 이주영[2†] · 정재일[1]

Performance Analysis of DoS/DDoS Attack Detection Algorithms using Different False Alarm Rates

Beom-Soo Jang · Joo-Young Lee · Jae-Il Jung

ABSTRACT

Internet was designed for network scalability and best-effort service which makes all hosts connected to Internet to be vulnerable against attack. Many papers have been proposed about attack detection algorithms against the attack using IP spoofing and DoS/DDoS attack. Purpose of DoS/DDoS attack is achieved in short period after the attack begins. Therefore, DoS/DDoS attack should be detected as soon as possible. Attack detection algorithms using false alarm rates consist of the false negative rate and the false positive rate. Moreover, they are important metrics to evaluate the attack detections. In this paper, we analyze the performance of the attack detection algorithms using the impact of false negative rate and false positive rate variation to the normal traffic and the attack traffic by simulations. As the result of this, we find that the number of passed attack packets is in the proportion to the false negative rate and the number of passed normal packets is in the inverse proportion to the false positive rate. We also analyze the limits of attack detection due to the relation between the false negative rate and the false positive rate. Finally, we propose a solution to minimize the limits of attack detection algorithms by defining the network state using the ratio between the number of packets classified as attack packets and the number of packets classified as normal packets. We find the performance of attack detection algorithm is improved by passing the packets classified as attacks.

Key words : False negative rate, False positive rate, False alarm rate, DDoS detection

요 약

인터넷은 확장성과 최선형 라우팅 서비스를 목적으로 설계되었기 때문에 보안상에 취약점을 가진다. 이에 IP spoofing과 DoS/DDoS 공격을 탐지하기 위한 다양한 공격 탐지 방법들이 제안되었다. DoS/DDoS 공격은 공격이 시작되고 짧은 시간 내에 목적을 이루기 때문에 공격 탐지 알고리즘들은 빠른 시간 내에 정확한 탐지를 하는 것이 중요하다. 공격 탐지 알고리즘들은 미탐지율과 오탐지율로 이루어진 오경고율을 가지며 공격 탐지 알고리즘의 성능을 평가하는 중요한 요소가 된다. 본 논문에서는 공격 탐지 알고리즘의 특징을 살펴보고 그 성능을 분석하였다. 공격 탐지 알고리즘의 성능은 미탐지율과 오탐지율을 변화시켰을 시, 공격 트래픽 및 일반 트래픽에 미치는 영향을 시뮬레이션을 통해 각각 분석하였다. 이를 통해 전송되는 공격 패킷의 수는 미탐지율에 비례하며, 전송되는 일반 패킷의 수는 일정 치 이하의 미탐지율과 오탐지율에 반비례하는 것을 확인하였다. 또 공격 탐지 알고리즘의 미탐지율 변화에 따른 오탐지율의 변화를 분석하여 미탐지율과 오탐지율의 관계를 도출하고 공격 탐지 알고리즘의 한계를 분석하였다. 이러한 한계를 극복하기 위해 정확한 네트워크 상태를 판단하여 공격 탐지 알고리즘의 한계를 줄이고 성능을 개선하는 방안을 제안하였고 그 결과, 공격 탐지 알고리즘의 성능이 보다 향상됨을 확인하였다.

주요어 : 미탐지율, 오탐지율, 오경고율, DDoS 공격탐지

접수일(2010년 10월 11일), 심사일(1차 : 2010년 12월 7일), 게재 확정일(2010년 12월 13일)

[1]) 한양대학교 전자컴퓨터통신공학과
[2]) 서경대학교 전자공학과
주 저 자 : 장범수
교신저자 : 이주영
E-mail; jylee@skuniv.ac.kr

1. Introduction

Internet was originally designed for scalability and best-effort routing. Therefore, it has poor security. It makes it easy to fake the source address and difficult to find the real source of a traffic. This creates a possibility of the attack known as a denial-of-service attack[1].

The goal of DoS attack makes troubles for the use of shared services or resources by confusing of victim hosts or victim networks. DoS attackers can achieve their purpose in two ways. The first way is using a vulnerability of the target system. One of these attacks is the “Ping-of-death” attack. This attack crashes the target system by sending a large ICMP ping packet. When the packet is transmitted through the network, it is fragmented into multiple IP packets. These packets cause a buffer overflow at the target system when the target system received them. The second way is to send huge volume of traffics to crash the target system. These packets consume all the resources of the target system. All hosts connected to the Internet can be a target system. The first way of attacks can be solved by patching the known vulnerability. However, it is hard to prevent the second way of attacks. In this paper, we use the second way of DoS attacks[1-4].

If victim hosts or victim networks are attacked by multiple DoS attackers, it is called a distributed denial of service(DDoS). The impact of DDoS attacks is bigger than DoS attacks and the defense of the attack is more difficult. DoS/DDoS is still one of most serious attacks[1-3].

A characteristic of DoS/DDoS attack traffic is similar to that of normal traffic. DoS/DDoS attacks make victim hosts or victim networks congest by sending huge volume of traffics. However, hosts and networks can be congested by receiving large normal traffics in normal case. It is called “flash crowd”. Therefore, it is very difficult to detect DoS/DDoS attacks.

Many mechanisms have been proposed to detect DoS/DDoS such as ingress/egress filtering, router-based packet filtering(RPF), hop count filtering(HCP), path identifiers(PI) and so on[1,8,9].

Attack detection mechanisms guarantee a high security of local hosts or local networks when they has high attack detection rate. However, attack detection has error rates called as false alarm rates. False alarm rates are consisted of false negative rate and false positive rate. False negative rate is the ratio between the attack packets classified as normal packets and the total attack packets. False positive rate is the ratio between the normal packets classified as attack packets and the total normal packets. Reducing the false negative rate is very important to prevent DoS/DDoS attacks. Therefore, the false positive is an important metric to evaluate the performance of attack detection. However, attack detection has the other error rate, false positive rate. After analyzing the impacts of false negative and false positive rates on in case of normal and attack traffic, we define proper metrics to evaluate the performance of attack detection.

In this paper, we analyze impacts of false alarm rates in case of normal and attack traffics. We also analyze the limitation of attack detection. And we propose methods to decide network states as attack and normal case using the number of packets classified as attack and normal packets.

This paper is organized as follow. We first review some proposed attack detection in chapter 2. In chapter 3, we analyze the impact of false alarm rates on the performance of the attack detection and the limitation of the attack detection. We propose methods to decide network states as attack and normal case in chapter 4. Finally, we give a conclusion in chapter 5.

2. Related Works

Victim hosts or victim networks are consumed their resources by DoS/DDoS attacks that make victim congest by sending a large Vol. of traffics. DoS/DDoS attacks are more powerful combined with IP spoofing. IP spoofing is an attack that fakes the source IP address of attack packets. It makes it is harder to detect DoS/DDoS attack.

2.1 Prevention Techniques of DoS/DDoS Attack

DoS/DDoS attack prevention is the method against IP spoofing. We can prevent many extended types of

DoS/DDoS attack by detecting IP spoofing.

2.1.1 Ingress/Egress Filtering

Ingress/egress filtering is one of the methods against IP spoofing attack of incoming and outgoing packets. Ingress/egress filtering passes only allowed traffics to enter or leave the network[1,8]. The packets have unexpected source IP address will be dropped.

2.1.2 Router-based Packet Filtering

Router-base packet filtering is the method to extend ingress filtering for core networks. This allows incoming packets have expected source IP address to enter the network. If the packet has unexpected source IP address, that will be dropped.

2.1.3 Source Address Validity Enforcement Protocol

RPF is not suitable for the asymmetric and dynamic Internet routing. SAVE is proposed as a method that overcomes this drawback[1]. SAVE can provide the information of the valid IP address. SAVE transmits the information of the valid IP address to all destinations. Each router that received the SAVE message updates their valid IP address table and passes incoming packets that have a valid IP address through each interface of the router.

2.2 Detection Techniques of DoS/DDoS Attack

DoS/DDoS attack detection algorithms are proposed to detect actual DoS/DDoS attacks. The goal of DoS/DDoS attack detection is to detect DoS/DDoS attacks as soon as possible to minimize the impact of the attack for local hosts or local networks.

2.2.1 MULTOPS

MULTOPS assumes that the packet ratio between incoming and outgoing packet rates is disproportional[1]. It is possible to detect DoS/DDoS attack by monitoring both packet rates.

2.2.2 SYN Detection/Batch Detection

SYN detection and batch detection are proposed to detect SYN floods[1]. SYN detection detects attacks using the ratio of SYN, FIN and RST packets. And batch detection detects using TCP and UDP traffic volumes.

2.2.3 Spectral Analysis

Normal TCP traffic can be control by flow control mechanism of TCP protocol. However, attack traffics are not controlled by flow control mechanism. Spectral analysis detects DoS/DDoS attacks using this characteristic of attack traffics[1].

2.2.4 Kolmogorov Complexity based Detection Algorithm

Transmitted attack packets by the source of DoS/DDoS attack are similar with each others. However, normal packets have a different traffic type. Therefore, the traffic is not highly correlated. Based on this assumption, Kolmogorove is a proposed scheme to detect attacks[1].

2.2.5 Time Series Analysis

Time series analysis also uses the correlation between attack traffics. After extracting the key variables, this detection scheme monitors them[1]. For example, the number of ICMP ping packets is the key variable for ping-of-death attack. The host that generates the ICMP ping packets highly correlated with the key variable that is regarded as attacker.

3. Analysis of the Attack Detection Performance and Limits

3.1 Simulation Environment

We evaluate the performance of the attack detection using different false alarms. We can get the simulation results using Qualnet(4.0) simulation tool. In this simulation, the network state is classified as attack and normal state. Attack state means the network state which is being attacked and normal state means the network state without attacks. The performance of the attack detection is changed by false alarms. Therefore, we count passed attack packets and passed normal packets with different false alarms to measure the attack detection

Table 1. Characteristics of traffics

(i) A characteristic of the attack traffic

Protocol	UDP
Packet Size	32 bytes
Duration	24s
Bytes	76,800,000
Packets	2,400,000

(ii) A characteristic of the normal traffic

Application	CBR
Protocol	UDP
Packet Size	512 bytes
Duration	24s
Bytes	2,457,600
Packets	4,800

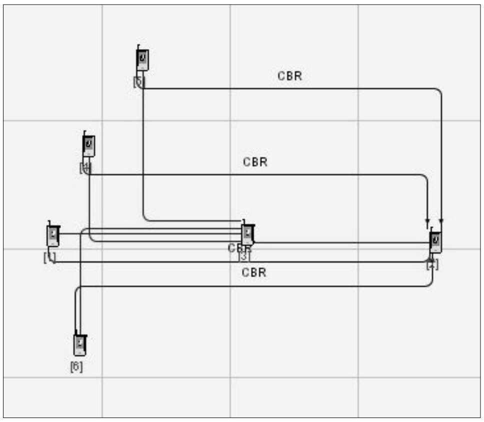


Fig. 1. Topology of simulation

performance. Intrusion detection system is placed at the edge router and the characteristics of the attack traffic and the normal traffic are as follow.

The attack traffic uses an UDP protocol to transmit attack packets. The UDP protocol is a connectionless protocol. Therefore the target network can be congested easily by UDP traffics. The congested router has a little queue size to receive incoming packets. In this case, small sized packets can be queued in the router queue with the higher priority than the other traffic. Because 32-byte attack packets smaller than that of normal packets, it can be queued to congest router during attack. Target network can be attacked continuously in this case.

A normal traffic is CBR applications. CBR applications also use an UDP protocol. Nowadays, the usage of multimedia services such as VoD and VoIP increase. Moreover, most of these applications use an UDP protocol that is more simple and faster than TCP protocol. Multimedia services transmit multimedia streaming data packets frequently. Therefore the multimedia data traffic is similar to the CBR traffic.

Multimedia services are sensitive in delay, jitter, packet loss rate and so on. For this reason, DoS/DDoS attacks have a large impact on multimedia services. Therefore, we can analyze the impact of DoS/DDoS attacks on the multimedia service with this simulation environment.

Fig. 1 shows the topology of the simulation environment. Node 1 is a malicious node and node 2 is a victim node. Node 1 generates the attack traffic heading to node 2 during simulation. A node 3 is an intrusion detection system that detects attack packets with false alarms. 4～6 Nodes are normal nodes. They generate normal traffic heading to node 2. All nodes are connected by 10Mbps links. We simulate during 30 sec. An attack and normal nodes generate traffic from 1 sec to 25 sec. After finishing the simulation, we count the attack packets and normal packets passed from node 3 to node 2 to analyze the performance of the attack detection. We simulate with different false alarms when false negative rate is 5, 10, 30 and 70 respectively and false positive rate si 10, 30, 70 and 90 respectively.

3.2 Performance Analysis of the Attack Detection in Attack Network State

Fig. 2 shows attack traffic packets that passed IDS with different false alarms.

Each graph is a result of simulation with different false positive rate. In Fig. 2, they have same the number of passed attack packets when the IDS has same false negative rate although it has different false positive rates. When the IDS has 5% false negative rate, 5% attack packets are passed and when the IDS has 10% false negative rate, 10% attack packets are passed. If the IDS has 30% and 70% false negative rates, 30% and 70% attack packets are passed. We can find out passed attack packet ratio is same with the false negative rate. Therefore we can define that passed attack packets are affected only false negative rate. DoS/DDoS attacks make victim host or victim network cannot use network services by generating huge volumed attack traffic enough to congest victim hosts or victim networks, so that consume their resources. If the attack traffic is not enough to congest victim hosts or victim networks, attacker cannot achieve their goal. Therefore, reducing attack traffic volume can increase the strength of victim host or victim network's security. In other words, we can say that getting reduce the false negative rate, more getting increase the security of the IDS.

Fig. 3 shows the normal packets variation passes the IDS with different false alarms in attack. Each line means each result of simulation with different false negative rates. Almost normal packets cannot pass the IDS when the false negative rate is bigger than 10% that is not related with the false positive rate. However, in the case of false negative rate is less or equal with 10%, normal packets can be forwarded to victim and the ratio of passed normal packets is different according to different false positive rates.

When the false positive rate is 90%, the ratio of passed normal packets is 10%. If the IDS has lower false positive rate, the passed normal packets increase. When the false negative rate of the IDS has a value under the specific rate, the normal traffic is not affected by the attack traffic and the false positive rate has the relation of an inverse proportion with the ratio of passed normal traffic. Therefore, we can say that the false positive rate affects only the ratio of passed normal traffic. If the ratio of passed normal traffic has high value, users use good quality network services. In other words, quality of service(QoS) is affected by the false positive rate.

3.3 Performance Analysis of the Attack Detection in Normal Network State

We assume the normal network state is the network state without any incoming attack packets. So that, false negative rate is no more important in normal network state. Therefore, false negative rate do not affect to the performance of attack detection in normal network state.

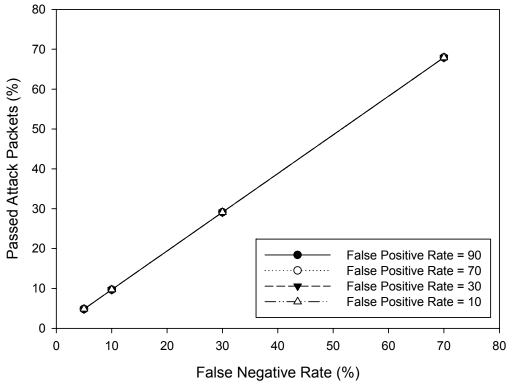


Fig. 2. Passed attack packets in attack network state

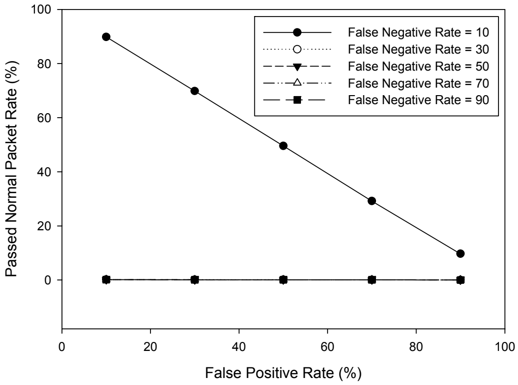


Fig. 3. Passed normal packets in attack network state

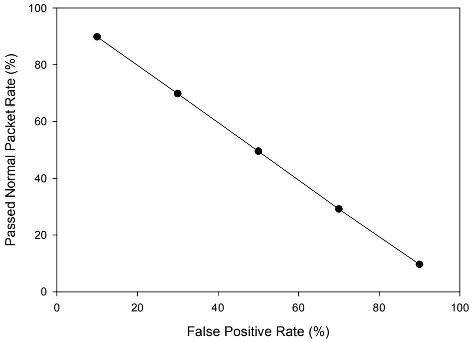


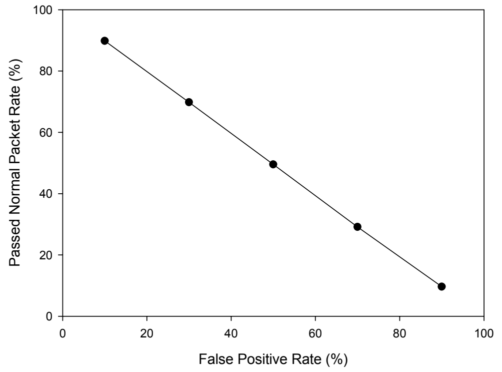
Fig. 4. Passed normal packets in normal network state

However, the false positive rate affect to normal packets in normal case. Fig. 4 shows the ratio of passed normal packets with different false positive rates.

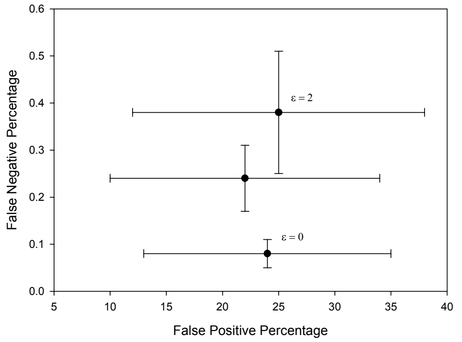
In the normal network state the ratio of passed normal packets is different according to the false positive rate. Therefore the quality of services used by users is affected by the false positive rate. The lower the false positive rate, the more normal packets are passed. In general, the period of the normal network state is longer than that of the attack network state. If the network keeps the normal state so long period, the number of the normal packets affected by false positive rate is greater than that of affected by attack packets. In this case, reducing false positive rate is important as much as reducing false negative rate.

3.4 The Relation between the False Negative and the False Positive Rate

In previous chapter, we already analyze that the performance of attack detection is affected by false alarms. False negative rate affects to the security of the IDS and the false positive rate affects to the QoS of the network services. If the false negative rate decreases, the security of the IDS increase. Moreover, the false positive rate decrease, the QoS of the network services increases. Therefore, the attack detection shows ideal performance when the false alarms closed to 0%.



(i) New /24s seen per day at attacked server, without map reduction



(ii) False negative vs False positive rate

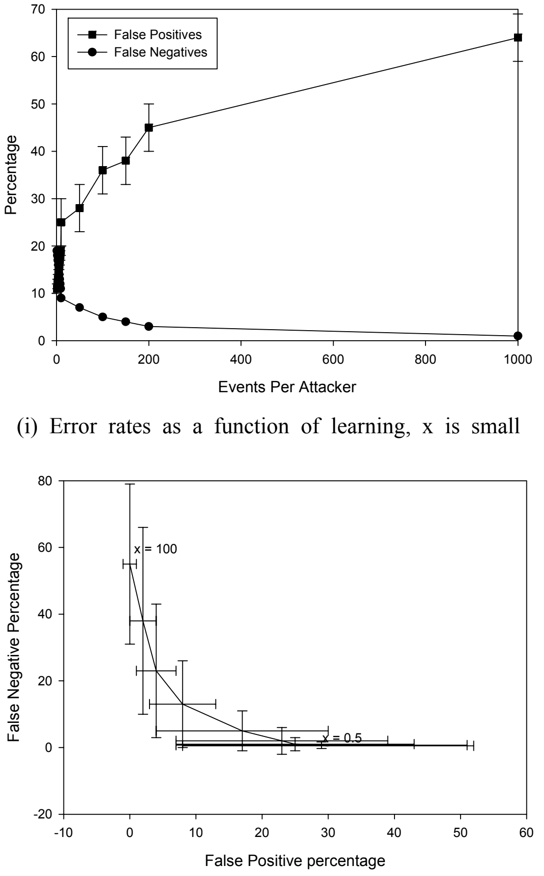
Fig. 5. The Performance Results of HCF

However, It causes an increase of false negative rate for the IDS which can process a wide range attack detection to detect the attack of new type. The number of incoming packets increases by enlarging the network bandwidth. It is hard to monitor all incoming packets. In addition, the characteristic of DoS/DDoS attack traffic is similar to that of a normal traffic. Therefore, it is difficult to improve the false negative rate and the possibility of normal traffic classified as an attack traffic increase due to the decrease of false negative rate. The false negative rate is getting lower, the false positive rate is getting higher. These situations are shown in the performance results of proposed attack detection[7].

Fig. 5 shows the performance analysis of hop counts filtering(HCF). Fig. 5-(i) shows the count of new incoming packet's source address when the HCF has a different training period in normal case. When the HCF has trained over 13 days, the count of new incoming packet source addresses decreases dramatically. In attack network state, the count of new incoming packet's source address increase rapidly. Therefore, when the HCF has a low count of new incoming packet's source addresses, it is easy to detect attack traffic. The long training period makes the HCF get lower false negative rate. Fig. 5-(ii) shows false alarms with different ε when the HCF has trained over 13 days. ε is the adaptive error rate and the HCF can get low false negative rate when the ε is small. When the ε decrease from 1 to 0, false negative rate also decrease from 0.25% to less than 0.1%. However, false positive rate increase to close 25% at that time.

Fig. 6 shows an analysis of the relation between false negative rate and false positive rate of path identifiers (PI). Fig. 6-(i) shows false negative and false positive rates of PI after training on both attack traffic and normal traffic.

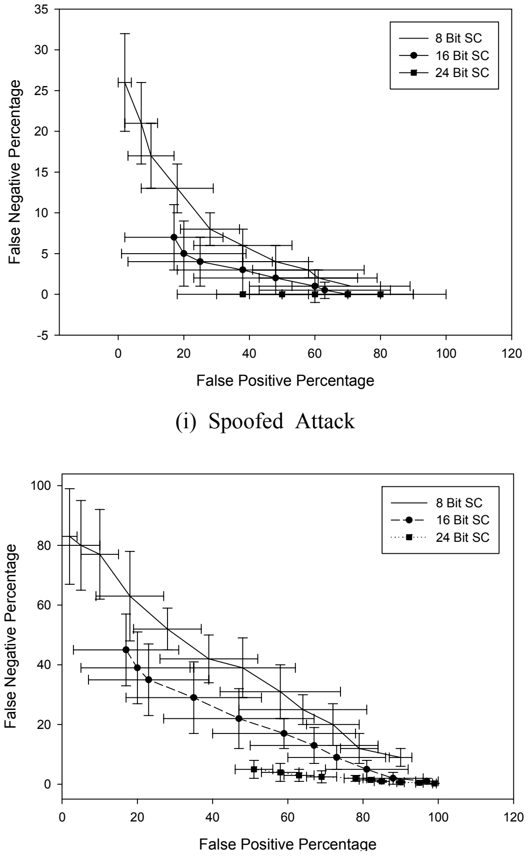
If attackers send packets during PI is training, then PI received 1,000 packets per the computer of attacker. To compensate for collision, PI has a strategy for rejec-



(i) Error rates as a function of learning, x is small

(ii) Error rates as x is varied

Fig. 6. The Performance Results of PI



(i) Spoofed Attack

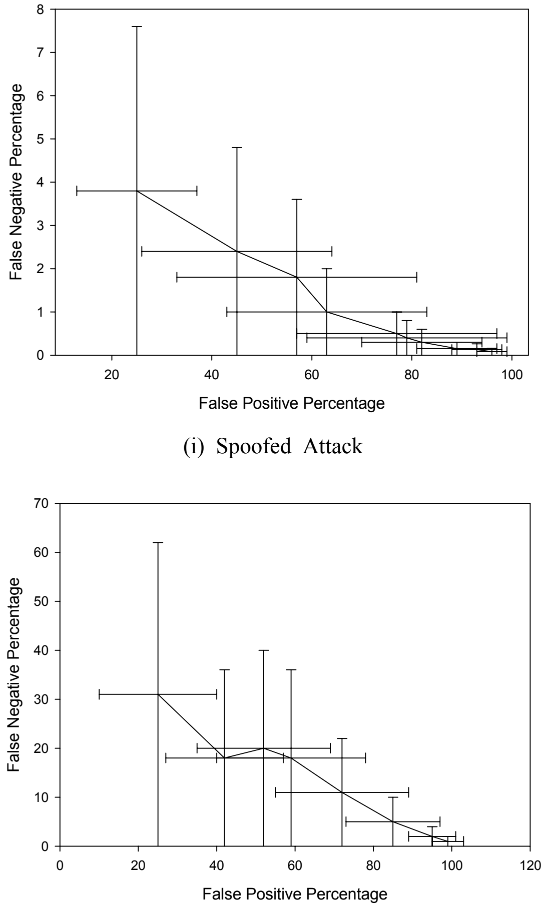
(ii) Non-spoofed Attack

Fig. 7. The Performance Results of SC

ting packets. In this strategy, a packet will be dropped if it bears a mark for which at least x% of the traffic during learning was attacker traffic. Therefore false negative rate decrease when the x decreases. Fig. 6-(ii) shows results for varying x between 95% and 100%. When the x is 100%, false positive rate becomes 0% according to the PI strategy. As this graph shows, false positive rate increase when false negative rate is decreased.

The performance of static cluster(SC) for 8-bit, 16-bit and 24-bit clustering is shown in Fig. 7. Fig. 7-(i) shows the performance against the spoofed attack and Fig. 7-(ii) shows the performance against the non-spoofed attack. In Fig. 7-(i), all of the graphs show high false positive rate when the false negative rate is low. If the false positive rate is higher than 60%, the false negative rate is closed to 0%. In other words, the performance of SC using more bits for clustering is better than that of using bits for clustering. The false negative rate of SC using more bits for clustering is lower when false positive rates are same. The characteristic of the performance against the non-spoofed attack is similar with that of the spoofed attack.

The performance of network-aware clusters(NAC) is shown in Fig. 8. The performance of NAC is similar to 16-bit SC. Fig. 8-(i) shows the performance against spoofed attack and Fig. 8-(ii) shows the performance against the non-spoofed attack. In Fig. 8-(i), when the false negative rate is less than 4%, the false positive rate is closed to 25%. However, when the false negative rate decrease to almost 0% the false positive rate increase to more than 80%. We can find out the similar characteris-



(i) Spoofed Attack

(ii) Non-spoofed Attack

Fig. 8. The Performance Results of NAC

tic in Fig. 8-(ii). False positive rate increase from 25% to more than 90% during the false negative rate decrease from about 30% to almost 0%.

3.5 The Limitations of Attack Detection

Detecting attack traffics and saving victim hosts or victim networks are the goal of the attack detection. Therefore, many people are studying to improve the security of attack detection by reducing the false negative rate. As described in previous chapter, it is used to analyze the performance of the attack detection not only false negative rate but also false positive rate. The false negative rate affects to the security of the IDS and the false positive rate affects to the QoS of the network services. Therefore, an attack detection that has low false negative and false positive rate can be an ideal model. However, reducing the false negative rate causes increase of the false positive rate. Some applications have minimum threshold of QoS to be guaranteed and multimedia service is one of QoS sensitive services. It is necessary to consider tradeoff between a security and a QoS of the attack detection. Even if an attack detection has low false positive rate, normal packets classified as attack packets will be dropped. Therefore, users will be provided the lower QoS than the QoS of before applying the attack detection. Generally, the period of normal state is much longer than the period of attack state of network. If the period of the normal network state is so much longer than that of attack network state, the number of dropped normal packets by classified as attack packets will be larger than that of by attack packets in attack network state. If we can decide network states, we can make a filtering strategy that packets classified as attack packets in normal case will be passed and only drop packets classified as attack packets in attack case. Therefore, we propose the method that can decide network states as normal case or attack case.

4. Network States Decision Algorithms

In this chapter, we propose the method to decide attack and normal state of networks.

4.1 Analysis of Classified Packets Variation

In general, DoS/DDoS attacks achieve their goal by transmitting huge volumed attack traffics to the victim hosts or victim networks. Because of this reason, the number of packets classified as attack packets in attack network state is larger than that of in normal network state. Fig. 9 shows the number of packets classified as attack and normal packets in attack network state.

When the false negative rate increase, we can find out that the number of packets classified as attack packets decrease and the number of packets classified as normal packets increase in Fig. 9. All of graphs is not affected much by false positive rate. However, they are affected by false negative rate. When the false negative

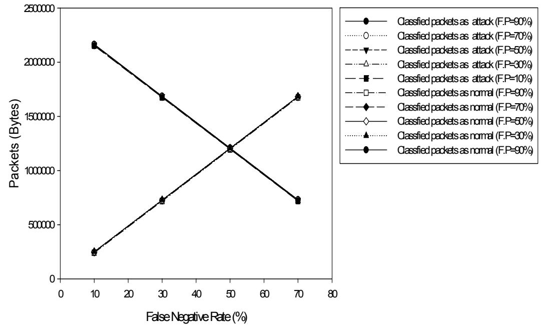


Fig. 9. The Number of Packets Classified as Attack and Normal in Attack Network State

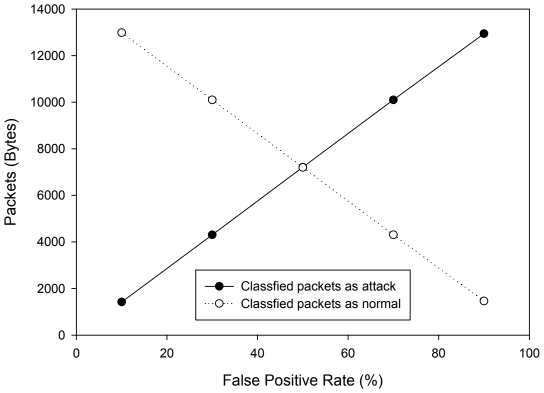


Fig. 10. The Number of Packets Classified as Attack and Normal in Normal Network State

rate is bigger than 50%, the number of packets classified as normal packets is larger than the number of packets classified as attack packets and the number of packets classified as attack packets is larger than the number of packets classified as normal packets when the false negative rate is less than 50%. When the false negative rate decrease, the gap between both graphs increase.

Fig. 10 shows the number of packets classified as attack and normal packets in normal network state, there are no attack packets. Therefore, incoming packets are not affected by false negative rate. However, false positive rate affected to incoming packets in normal network state. When the false positive rate is bigger than 50% in normal network state, the number of packets classified as attack packets is bigger than the number of packets classified as normal packets. However, when the false positive rate is less than 50%, the number of packets classified as normal packets is larger than the number of packets classified as attack packets.

4.2 Proposed Algorithms

As we analyzed above, we can propose two methods that decide attack and normal network state.

First, when the false negative and false positive rate are less than 50%, we can decide the network state using the ratio of the number of packets classified as normal and attack packets. If the number of packets classified as attack packets is larger than the number of packets classified as normal packets, the network state is the attack network state. On the other hand, If the number of packets classified as normal packets is larger than the number of packets classified as attack packets, the network state is the normal network state. This method only can be adapted when the false negative and false positive rate are less than 50%. However, as we analyze above, when the false negative rate decreases the false positive rate increases. Therefore, the situation can be happened in case of the false negative rate is less than 50% and the false positive rate is bigger than 50%. In this case, we must increase the false negative rate until the false positive rate decrease to less than 50%. That means the security of the IDS decrease.

Second, there is a method that decides the network states using only the number of packets classified as attack packets. In Fig. 9 and Fig. 10, the number of packets classified as attack packets in the attack network state is larger than 55 times of that in the normal network state. Therefore, after defining a specific threshold, we can decide the network state is as attack network state when the number of packets classified as attack packets is greater than the threshold and decide the network state is as normal network state when the number of packets classified as attack packets is less than the threshold. This method can be adapted when the gap between the numbers of packets classified as attack packets in attack and normal network states. However, in the low-rate attack case, the number of packets classified as attack packets may not be large enough to decide the network states.

Therefore, we should adapt a suitable method after analyzing the network property.

5. Conclusion

In this paper, we analyze the performance of attack detection against DoS/DDoS attacks. The goal of attack detection is to save victim hosts or victim networks from attacks. The false negative rate is the most important factor in the security point of view. Therefore, there are a lot of researches for the attack detection with low false negative rate. However, the false positive rate is also important to evaluate the performance of the attack detection.

After analyzing the impact of false alarms on the attack detection in different network states, we find out that the false negative rate affects to the security of the IDS only in attack network state and the false positive rate affects the QoS in attack network state whereas the false negative rate is equal or less than 10% or in the normal network state. Using the result of analyzing passed attack and normal packets with different false alarm rates in different network states, we find out that the performance of attack detection can be ideal when false alarm rates are closed to 0%. However, the false negative rate is getting lower the false positive rate is getting higher due to the property of the IDS. We show this situation in performance results of the attack detections such as HCF, PI, SC and NAC. Therefore, it is hard to get low false positive rate when the false negative rate is low. And the false positive rate can be a major problem of QoS when the period of normal network state is so long.

We proposed two methods that decide network states as attack and normal network states to reduce the impact of the false positive rate in normal network state based on the idea that we can pass all packets classified as attack packets in normal network state.

First, we can decide network states using the ratio of the number of packets classified as attack and normal packets. In attack network state, the number of packets classified as attack packets is larger than that of classified as normal packets. Moreover, the number of packets classified as attack packets is less than that of classified as normal packets in normal network state. However, this method can be adapted when the false alarms is less than 50%.

The second method is that deciding the network states using only the number of packets classified as attack packets. As analyzed in previous chapter, the number of packets classified as attack packets in attack network state is much larger than that of in normal network state. Therefore, we can decide the network state is the attack network state when the number of packets classified as attack packets is larger than a defined threshold. However, it is hard to define proper threshold in low-rate attack. A suitable method should be adapted after analyzing the network property.

ACKNOWLEDGMENT

This research was supported by the MKE(Ministry of Knowledge Economy), Korea, under the ITRC(Information Technology Research Center) support program supervised by the NIPA(National IT Industry Promotion Agency)(NIPA-2010-(C1090-1031-0005))

REFERENCES

1. Tao PENG, Christopher Leckie, and Kotagiri Ramamo hanarao, "Survey of Network-Based Defense Mechanisms Countering the DoS and DDoS Problems," ACM Computing Surveys, vol. 39, no. 1, 2007.
2. Jelena Mirikovic, and Peter Reiher, "A Taxonomy of DDoS Attack and DDoS Defense Mechanisms," ACM SIGCOMM Computer Communications Review, vol. 34, no. 2, pp. 39-53, Apr. 2004.
3. Rocky K. C. Chang, "Defending against Flooding-Based Distributed Denial-of-Service Attacks: A Tutorial," Communications Magazine, IEEE, vol. 40, no. 10, pp. 42-51, Oct. 2002.
4. Glenn Carl, George Kesidis, Richard R. Brooks, and Suresh Rai, "Denial-of-Service Attack-Detection Techniques," IEEE Internet Computing, vol. 10, no. 1, pp. 82- 89, Jan.-Feb. 2006.
5. Amey Shevtekar, Karunakar Anantharam, and Nirwan Ansari, "Low Rate TCP Denial-of-Service Attack Detection at Edge Routers," IEEE Communications Letters, vol. 9, no. 4, pp. 363-365, Apr. 2005.
6. Wei Chen, Dit-Yan Yeung, "Defending Against TCP SYN Flooding Attacks Under Different Types IP Spoofing,"

Proceedings of the International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies, pp. 38, 2006.

7. Michael Collins, Michael K. Reiter, "An Empirical Analysis of Target-Resident DoS Filters," Proceedings of IE EE Security and Privacy, pp. 103-114, May 2004.
8. P. Ferguson, and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing," RFC 2827, May 2000
9. Ghosh A, Wong L, Di Crescenzo G, and Talpade R, "In-Filter: predictive ingress filtering to detect spoofed IP traffic," Proceedings of Distributed Computing Systems Workshops, pp. 99-106, Jun. 2005.
10. Mirkovic J, and Prier G,Reiher P, "Attacking DDoS at the source," Proceedings of IEEE International Conference on Network Protocols, pp. 312-321, 2002.
11. Haggerty J, Qi Shi, and Merabti M, "Early detection and prevention of denial-of-service attacks: a novel mechanism with propagated traced-back attack blocking," IEEE Selected Areas in Communications, vol. 23, no. 10, pp. 1994-2002, Oct. 2005.
12. Tu Xu, Da Ke He, and Yu Zheng, "Detecting DDOS Attack Based on One-Way Connection Density," Proceedings of IEEE International Conference on Communication systems, pp. 1-5, Oct. 2006.
13. Bremler-Barr, and A,Levy, H, "Spoofing prevention method," Proceedings of IEEE INFOCOM 2005, vol. 1, pp. 536-547, Mar. 2005.
14. Siaterlis C, and Maglaris V, "Detecting incoming and outgoing DDoS attacks at the edge using a single set of network characteristics," Proceedings of IEEE Symposium on Computers and Communications, pp. 469-475, Jun. 2005.

장 범 수 (ray@piolink.com)

2007 인천대학교 정보통신공학과 학사
2009 한양대학교 전자통신컴퓨터공학과 석사
2009～현재 (주)파이오링크 AT팀 대리

관심분야 : 네트워크 보안

이 주 영 (jylee@skuniv.ac.kr)

1990 한양대학교 전자공학과 학사
1992 한양대학교 전자공학과 석사
2001 한양대학교 전자공학과 박사
2002～현재 서경대학교 전자공학과 조교수

관심분야 : 네트워크 토폴로지, 스위칭 및 라우팅 알고리듬, 통신시스템 설계

정 재 일 (jijung@hanyang.ac.kr)

1981 한양대학교 전자공학과 학사
1984 한국과학기술원 전기 및 전자공학과 석사
1993 프랑스 국립통신대학교 네트워크공학과 박사
1997～현재 한양대학교 정교수

관심분야 : 인터넷 QoS, VANET, Security