Prevention of DDoS Attacks for Enterprise Network Based on Traceback and Network Traffic Analysis

Yun-Ji Ma, Hyun-Chul Baek, Chang-Geun Kim and Sang-Bok Kim

Abstract—With the wide usage of internet in many fields, networks are being exposed to many security threats, such as DDoS attack and worm/virus. For enterprise network, prevention failure of network security causes the revealing of commercial information or interruption of network services. In this paper, we propose a method of prevention of DDoS attacks for enterprise network based on traceback and network traffic analysis. The model of traceback implements the detection of IP spoofing attacks by the cooperation of trusted adjacent host, and the method of network traffic analysis implements the detection of DDoS attacks by analyzing the traffic characteristic. Moreover, we present the result of the experiments, and compare the method with other methods. The result demonstrates that the method can effectively detect and block DDoS attacks and IP spoofing attacks.

Index Terms—DDoS attacks, Network traffic, Traceback, Network security.

I. INTRODUCTION

With the wide usage of internet in many fields, networks are being exposed to many security threats, such as DDoS attack, worm/virus, and so on. For the enterprise network, prevention failure of network security causes revealing of confidential commerce information or interruption of network services. To defend network resource from these threats, several network security systems are developed, such as firewall and Intrusion Detection System (IDS). Firewall is to respond to attacks by blocking the traffic, but it can not prevent attacks from intranet and the access control policy is static. IDS is mainly focused on monitoring and detecting well-known attacks. So it is not appropriate for IDS to detect abnormal traffic caused by unknown attack, and it is passive and does not let us identify the attack source.

In this paper, we propose a method of prevention of DDoS attacks for enterprise network (PDAEN), which is based on traceback and network traffic analysis. Firstly, we propose the network architecture based on trusted adjacent nodes information, in which each trusted host has the access information of the others and the information includes IP address of trusted hosts, hop count and traceback information in hop-by-hop from itself to the other trusted hosts. Only the trusted host can access each other after it passes the authentication of the proposed prevention method. Secondly, IP spoofing attacks by disguising the IP address of trusted hosts are detected by the model of traceback. Thirdly, by analyzing the characteristic of network incoming traffic and outcoming traffic, we implement the detection of DDoS attack.

The remaining part is organized as follows. In Chapter 2, the related work is briefly introduced. Chapter 3 elaborates the method of PDAEN. Implementation and analysis are presented in Chapter 4, and finally we conclude the paper in Chapter 5.

II. RELATED WORK

Many network security threats, such as DDoS and worm/virus, cause serious network performance degradation by introducing large amount of malicious traffic into network. By analyzing the abnormal network traffic [1, 2, 3], the hidden attack can be detected. The other method is to identify the true IP by tracing packets to the source host, even an attacker forges its IP address [4, 5]. Thomas Dubendoefer et al. [6] propose a distributed traffic control system that enables ISPs to deploy new applications within the network and delegate partial network control to network users. The authors [7] discuss traffic analysis method, and propose an abnormal traffic detection method. They firstly calculate traffic forecast value by using exponential smoothing model that is a kind of

Manuscript received April 29, 2009; Revised June 2, 2009. First Author: Yun-Ji Ma is with the Dep. of Computer Science, Gyeongsang National University, Korea, and University of Science and Technology LiaoNing, China. Corresponding Author: Sang-Bok Kim is with the Dep. of Computer Science, Gyeongsang National Univ., Jinju, 660-701, Korea (Tel: +82-055-751-5994, Email: ma3682@gmail.com, sbkim@gnu.ac.kr)

time series analysis model [8], then get the mean absolute deviation value, thereby set limit of normal traffic. But it is key that how to adjust model's operating parameters and it is difficult to distinguish the difference between an abnormal traffic and the normal flash crowds when a huge number of users use the target host at the same time.

Spoofing the source IP address of packets on the internet is one of the major tools used by hackers to mount DDoS attacks. In such attacks, the attackers forge the source IP of packets that are used in the attack by using an arbitrary IP address which is selected either randomly or intentionally. In the paper [9], they present a spoofing prevention method, by which each packet leaving a source network is tagged with the key, which is associated with the source network and the destination network. Once arrival at the destination network, the routers verify the key to decide if the packet is discarded. The paper [10] discusses attacks using spoofed packets and variety of methods for detecting spoofed packets. These include both host-based methods and the more commonly discussed routing-based methods. The authors [11] propose an IP traceback method to identify the true IP address of a host originating attack packets by checking the source IP address filed of an IP packet. But some special tracing equipment, such as the sensors and the tracers should be deployed at some point in the network and it is difficult to reply the DDoS from a large number of attackers at the same time.

III. PROPOSED METHOD

In this chapter, we propose the method of PDAEN. By this method, we can effectively detect and prevent DDoS attacks, including IP spoofing attacks by disguising IP address of trusted host, which cause the interruption of network services or the degradation of network performance. In section A, we describe the enterprise network architecture based on trusted adjacent nodes information, thereby we elaborate the model of traceback for detecting IP spoofing attacks in section B. Section C explains the method of network traffic analysis. In section D, system model is introduced.

A. Enterprise network architecture based on trusted adjacent nodes information

We firstly propose enterprise network architecture based on trusted adjacent nodes information, which is shown as Fig. 1. In the structure, these trusted hosts can be located different cities. They include hosts of A, B, C, D, E and F, in where each trusted host has the access information of the others, such as IP address, hop count and traceback information in hop-by-hop from itself to all the other trusted hosts. In a packet-switching network, a hop is the trip a data packet takes from one router or intermediate point to another in the network. Only the trusted host can access each other after it passes the authentication of the proposed method, namely A= {B, C, D, E, F}, B= {A, C, D, E, F}, ..., F={A, B, C, D, E}. So that, when one host from outside site wants to access one of trusted hosts, it can not pass the authentication of destination host, because it is not trusted host, here the other method can be used, such as the scheme of one-time password authentication. So, in this network, we mainly take into account the attacks as follows: IP spoofing attacks by disguising IP address of controlled trusted hosts, DDoS attacks from external network. For the former, we prevent them by a model of traceback, and for the latter, we propose a method of network traffic analysis to reply them, whether DDoS attacks come from the inner of the enterprise network.

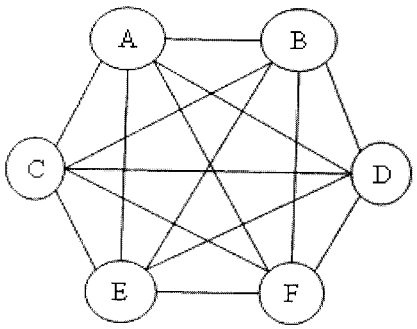


Fig. 1 Proposed enterprise network architecture

B. The model of traceback

In order to implement IP spoofing attacks from external network, the hacker first attacks and controls a trusted host, next gets its IP address and blocks it from connecting with internet, then attack the target host by disguising IP address of the controlled trusted host. Thereby, they can get confidential commercial information. As shown in Fig. 2, we suppose that the hacker intrudes the host B by disguising the IP address of host A. Here we call host A as source host, host B is victim/destination host, and host H is the attacker. After attacks happened, according to three-way handshake of TCP, host H will intercept the synchronize-acknowledgement (SYN-ACK) from victim host to host A. So if we directly traceroute from the victim host to host A, the result of traceroute will not be affirmed. Because the hosts within the enterprise network are mutual trusted, and each trusted host has the access information of the other trusted hosts, we can implement the detection of IP spoofing

attacks with the help of trusted host C. Namely, we implement the traceback from the IP address of host C to IP address of host A. Here, we call the trusted host C as detection host.

Fig. 2 shows the model of traceback for detecting IP spoofing attack. When IP spoofing attacks occur, because the hacker H has controlled host A, the traceback result should be "host unreachable".

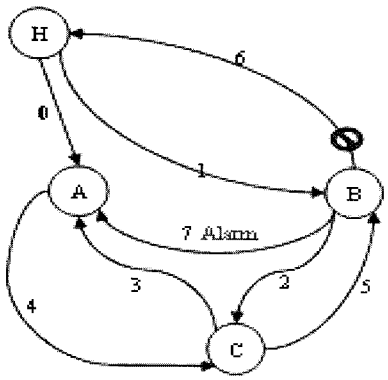


Fig. 2 The model of Traceback

In order to explain the model, we describe the algorithm of traceback as Fig. 3.

The algorithm of traceback

1. Host A sends access request to host B, or Hacker H sends access request to host B by disguising IP address of host A
2. Host B sends traceroute request to trusted host C
3. Host C traces the route information from C to A
4. Host C gets the trace result (Host reachable/unreachable)
5. Host C informs the trace result to host B
6. If (Host reachable) Target B accepts source host else blocks the Hacker
7. If (Host unreachable) Host B sends an alarm information to host A

Fig. 3 The algorithm of Traceback

According to this algorithm, when host A accesses host B in normal network state, the result of traceback from detection host C to source host A is "host reachable".

C. The method of network traffic analysis

In order to detect DDoS attacks and DoS attacks, we propose a method of network traffic analysis based on standard deviation [12] in probability and statistics, which is a measure of the variability or dispersion of population. The standard deviation σ of a discrete variable is the root-mean-square (RMS) deviation of its value from the mean of the sample of data. If the random variable X takes on N values X_1, X_2, ..., X_N with equal probability, then the calculation of σ is described by the following formula:

$$\sigma = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(Xi - \overline{X})^2} \qquad (1)$$

Here $\overline{X}$ is the arithmetic mean of the values X_i, defined as

$$\overline{X} = \frac{1}{N}\sum_{i=1}^{N} Xi \qquad (2)$$

We denote respectively $Traffic_{\_in}$ (kb/s) the incoming traffic and $Traffic_{\_out}$ the outcoming traffic in a second, namely we sample a traffic value per-second. Then we collect the latest network traffic in normal network state during a predefined time period, such as one week or one day, and calculate the mean of traffic using the formula (2), which the mean value is denoted as $\overline{Traffic_{\_in}}$.

We thereby get the standard deviation $\sigma(Traffic_{\_in})$ of incoming traffic. Here σ is considered as the dispersion of traffic for normal network traffic and is denoted as $\Delta Traffic_{\_in}$, we set the limit of normal traffic as formula (3).

$$\begin{aligned} &\overline{\text{Traffic}_{\_\text{in}}} - \Delta\text{Traffic}_{\_\text{in}} \le \text{Traffic}_{\text{in}} \\ &\bigcap \text{Traffic}_{\_\text{in}} \le \overline{\text{Traffic}_{\_\text{in}}} + \Delta\text{Traffic}_{\_\text{in}} \end{aligned} \qquad (3)$$

Here $Traffic_{\_in}$ is the real-time incoming traffic that is being monitored. Because the abnormal traffic generally is the unusual increase of traffic, we only consider the upper limit, which is shown as formula (4).

$$\text{Traffic}_{\_\text{in}} \le \overline{\text{Traffic}_{\_\text{in}}} + \Delta\text{Traffic}_{\_\text{in}} \qquad (4)$$

If real-time network traffic within a shorter period of time Δt (such as Δt = 10s) is almost satisfied the formula (4), we consider the current traffic as normal traffic, Otherwise, we further calculate the ratio of traffic:

$$\text{Ratio}_{\text{traffic}} = \frac{\text{Traffic}_{\_\text{in}}}{\text{Traffic}_{\_\text{out}}} \qquad (5)$$

According to the basic principle of DDoS attacks [9], when a host is compromised by DDoS attacks, it can not reply after a maximum waiting time (MWT). The value of $Traffic_{\_out}$ is always very low and that of $Traffic_{\_in}$ is always very high. So the higher the value of $Ratio_{traffic}$, the higher the possibility that the destination host is attacked by DDoS attacks. If the value of $Ratio_{traffic}$ is higher than a predefined limit of $Ratio_{limit}$ (for example, $Ratio_{limit}=100$) and increases continuously within a shorter period of time Δt, namely the increment of $Ratio_{traffic}$ ($\Delta Ratio_{traffic}$) during Δt is larger than 0, we affirm it is abnormal traffic.

Now we conclude the rules as Fig. 4. Here condition 1 denotes that the traffic is normal or light load, condition 2 denotes that the crowds which normal occur when a huge of trusted hosts use the target host at the same time (another word for overloading), and condition 3 means the incoming traffic is much greater than the outcoming traffic and the increment of $Ratio_{traffic}$ is larger than 0.

The algorithm of network traffic analysis

1. calculate the mean of traffic $\overline{Traffic_{\_IN}}$
2. calculate the $\Delta Traffic_{\_IN}$
3. sample real-time network traffic
4. judge the term
   1) normal traffic: (condition 1 or condition 2)
   condition 1: $Traffic_{t\_in} \le \overline{Traffic_{\_in}} + \Delta Traffic_{\_in}$
   condition 2: $Traffic_{t\_in} > \overline{Traffic_{\_in}} + \Delta Traffic_{\_in}$ and $Ratio_{traffic} \le Ratio_{limit}$
   2) abnormal traffic: (condition 3)
   $Traffic_{t\_in} > \overline{Traffic_{\_in}} + \Delta Traffic_{\_in}$ and $Ratio_{traffic} > Ratio_{limit}$ and $\Delta Ratio_{traffic} > 0$
   3) suspicious traffic: (condition 4)
   $Traffic_{t\_in} > \overline{Traffic_{\_in}} + \Delta Traffic_{\_in}$ and $Ratio_{traffic} > Ratio_{limit}$ and $\Delta Ratio_{traffic} \le 0$
5. implement
   1) accept the normal traffic
   2) discard the abnormal traffic
   3) keep a close watch on suspicious traffic
6. continue monitor, return step 3

Fig. 4 The algorithm of traffic analysis

D. Proposed system model

Based on the model of traceback and the method of network traffic analysis, we propose the method of PDAEN. Fig. 5 shows the architecture of proposed system model. Now, we describe the model as follows in detail.

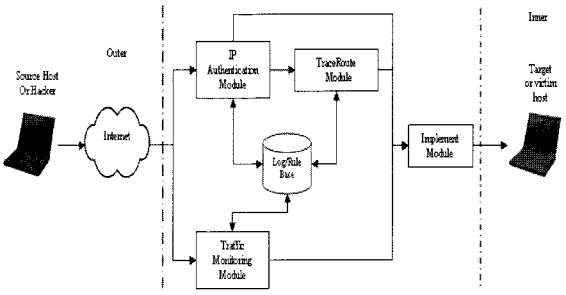


Fig. 5 The architecture of proposed system model

1) IP Authentication Module

Based on the network architecture including trusted adjacent nodes information, only the trusted hosts can be accessed each other. IP authentication module is used for judge if source host is a trusted host. In this module, we first get the authentication of source host, such as host name, host IP address, host MAC address, hop count, and so on, especially the IP address is binding with MAC address, then compare them with the information of rule base in destination host. Only when the user passes the IP authentication, it is considered as an trusted host, Otherwise the user is considered as an host from outer site, then One-Time Password is used for it. For trusted host, we further trace route from detection host to source host, and judge if destination host is exposed to IP spoofing attack.

2) Traceback Module

In this module, we implement the detection of IP spoofing attacks based on the algorithm of traceback. If source host is normal trusted host, the result information of trace route is "Destination host reachable", otherwise, if IP spoofing attack occurs, the result information is "Destination host unreachable". At the same time, the rule base and the log base are updated dynamically. The result of trace route is sent to the implementation module.

3) Network Traffic Analysis Module

The module implements the detection of DDoS attacks from external network according to the method of network traffic analysis. The network traffic is monitored in real-time, once it is abnormal, alarm information will be sent to destination host B. Here the value of $\overline{Traffic_{\_in}}$, $\Delta Traffic_{\_in}$ and $Ratio_{limit}$ in rule base should be predefined and updated after a period time.

4) Implementation Module

Implementation module receives the result from the above three modules, and implement it. If only the detection result of three modules is also normal, the

source host is considered as legal trusted host and can access the target host, else the host will is blocked.

IV. EXPRIMENTATION AND ANALYSIS

We simulate the experiments by using winsock programming in Visual C++ language. In the hardware, we use four computers to implement the detection of IP spoofing attack. It takes us three months to trace the route information in hop-by-hop from one host to the other trusted hosts. We calculate the data of network traffic, set the limit, where the value of $\overline{Traffic}_{in}$, $\Delta Traffic_{in}$ and $Ratio_{limit}$ is 230.2KB/sec, 50.3KB/sec and 100 in turn. These data are stored into access rule base. The traceback information is stored into the route information table. These are the three tables, which are shown as the following:

Host Information Table, which is used for storing the information of trusted hosts: host name, host IP and hop count of traceback; Route Information Table, which is used for storing the route information from detection host to source host: host IP, sequential number of traceback, hop IP, and Traffic Information Table storing the parameters information of network traffic, as previously stated in section 3. 3.

In order to confirm the effectiveness of the method, we first implement the simulation experimentation within local network of our lab based on the model of traceback in section 3.2. Fig. 6 shows the main information of detection process when host A accesses host B in normal state, which the steps are in accordance with the steps of the algorithm of traceback shown as Fig. 3. Here, IP address of source host A and detection host C is 203.255.3.170 and 203.255.3.97 in turn.

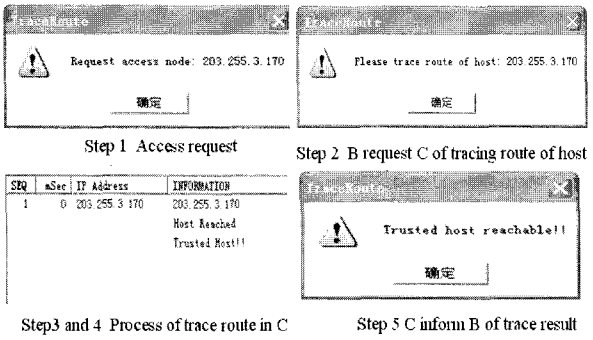


Fig. 6 Access information of trusted host

Fig. 7 shows the main information for detecting IP spoofing attack. Here, IP address of spoofed host A is 203.255.3.170. This figure shows the information of the steps 1, 2, 3, 4 and 5 based on the algorithm of traceback. The information of Step 4 is "host unreachable", and the information of step 7 is sent to the spoofed host A, which the information is similar with the step 5.

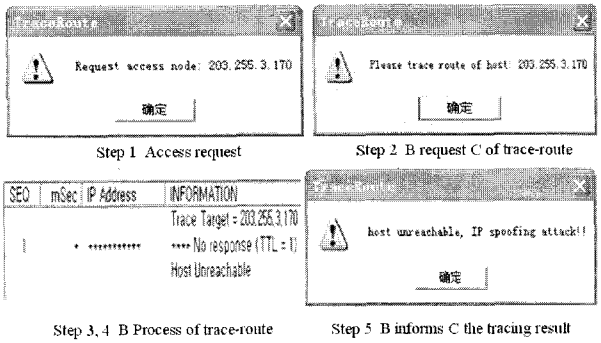


Fig. 7 Detection information of IP spoofing attack

The detection result of IP spoofing attacks is shown as table 1. From the result of detection, we confirm that the IP spoofing attacks can be detected exactly.

Table 1 Detection results

IP Spoofing	Access host	Detection host	Detection times	Rate (%)
×	210.125.186.29	203.255.3.97	30	100
√	203.255.3.170	203.255.3.97	30	100
×	203.255.3.170	203.255.3.97	30	100

For DDoS attacks, we ping the trusted host by using ping flood with 65536kb packet from 5 computers to implement the simulation.

Fig. 8 shows the detection of normal network traffic. From this figure, the traffic in the interval between t1 and t2 is normal load, the traffic in the interval between t2 and t3 is light load, and the traffic in the interval between t3 and t4 is overloading.

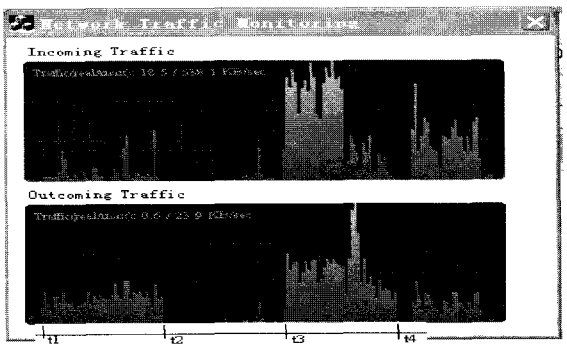


Fig. 8 Normal Network Traffic

Fig. 9 shows the detection of abnormal network traffic. In this figure, the maximum value of incoming and outcoming traffic is 2830.8 KB/sec and 79.3KB/sec in turn. Before the time of t1, the traffic is normal, and after the time of t1, the traffic is abnormal.

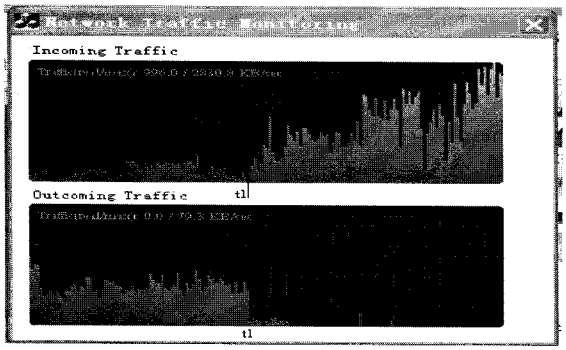


Fig. 9 Abnormal Network Traffic

Additionally, we further compare the method with other methods. Table 2 shows the evaluation result with other methods.

Table 2 Compare with other algorithms

Elements / Methods	Advantage	Disadvantage
SPM (Spoofing prevention method)	To tag a simple key for leaving packet, then verify the key in target host	The algorithm is complicated and practical application is difficult
ATD (Abnormal traffic detection and its implementation)	A method based on traffic forecast, low computing complexity	Difficult to identify normal crows and abnormal traffic
ADTCS (Adaptive distributed traffic control)	A new distributed traffic control system, effectively stop attack traffic close to the source	No demonstration of experiments
TNA (Tracing network attacks to their source)	IP traceback to identify the true IP address of the attack host	Difficult to reply the DDoS attacks from large number hosts
Proposed Method	No additional hardware, dynamic update rule base, cooperate with the other trusted hosts	it is key that how to find the relationship among the parameters better

V. CONCLUSION

In this paper, we propose a method of prevention of DDoS attacks for enterprise network (PDAEN), which is based on traceback and network traffic analysis. Firstly, we propose enterprise network architecture based on trusted adjacent nodes information. Secondly, IP spoofing attacks by disguising the IP address of trusted hosts are detected by the model of traceback. Thirdly, by analyzing the characteristic of network incoming traffic and outcoming traffic, we implement the detection of DDoS attack. The result of experiments demonstrates the effectiveness of the method. The major benefits are that the scheme is only implemented by software method, not depends on some additional hardware, the structure of database is easily constructed, and rule base can be updated dynamically. In the future, we consider how to further analyze packet information and how to find relationship among the parameters of network traffic better.

REFERENCES

[1] S. Mohiuddin, S. Hershkop, R. Bhan and Stolfo, "Defending against a large scale denial-of-service attack", *In Proceedings of IEEE Workshop on Information Assurance and Security*, US. Military Academy, NY, pp.1555-1562, Jun. 2002.

[2] L. Lersak and R. Arnon, "Distributed denial of service detection using TCP/IP header and traffic measurement analysis", *Inter. symposium on communications and information technologies 2004*, Vol. 1, pp. 605-610, Oct. 2004.

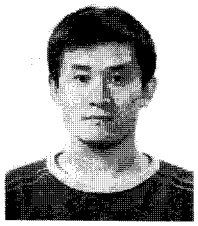
[3] S. Augustion, S. Kave, and T. Nina, "Combining filtering and statistical methods for anomaly detection", *Internet measurement conference 2005*, pp.331-244, 2005.

[4] Y. Xiang and W. Zhou, "Trace IP packets by flexible deterministic packet marking (FDPM)", *Proceedings IEEE Workshop on IP Operations and Management*, pp. 246-252, Oct. 2004.

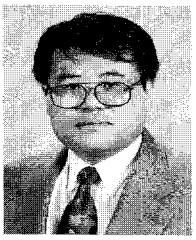
[5] C. Gong and K. Sarac, "A More Practical Approach for Single-Packet IP Traceback using Packet Logging and Marking", IEEE Transactions on Parallel and Distributed Systems, vol. 19, pp. 1310-1324, Oct. 2008.

[6] T. Dubendorfer, M. Bossardt, and B. Plattner, "Adaptive distributed traffic control service for DDoS attack mitigation", *proceedings of the 19th IEEE inter. parallel and distributed processing symposium*, April, 2005.

[7] S. H. Lee et al., "Abnormal traffic detection and its implementation", *The 7th International Conference on Advanced Communication Technology*, vol. 1, pp. 246-250, 2005.
[8] G. Box, G. Jenkins, and G. Reinsel, *Time series analysis*, 3rd edition, Prentice Hall, 1994.
[9] A. Bremler-Barr, and H. Levy, "Spoofing prevention method", *Conference of the IEEE Computer and Communications Societies*, vol. 1, pp. 536-547, March 2005.
[10] S. J. Templeton, and K. E. Levitt, "Detecting spoofed packets", *DARPA Information Survivability Conference and Exposition*, vol. 1, pp. 164-175, April 2003.
[11] T. Baba, and S. Matsuda, "Tracing network attacks to their sources", *Internet Computing, IEEE*, vol. 6, pp. 20-26, March-April 2002.
[12] Wikipedia, free encyclopedia, [Online]. Available: http://en.wikipedia.org/wiki/Standard_deviation.

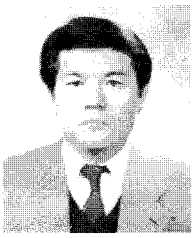


Yun-Ji Ma
received the B.S. degree in Computer Science from AnShan Institute of Iron and Steel in 1993, and M.S. degree in Computer Science from Gyeongsang National University in 2006, now he has been studying for Ph.D. degree in Gyeongsang National University since Sep. 2006. He has been an instructor in University of Science and Technology LiaoNing, China since Sep. 1993. His research interests include CDMA communication and computer network and security.



Hyun-Chul Beak
received the B.S., M.S. and Ph.D. degree in Electronic Computing and Statistics, Education, and Computer Science from Gyeongsang National University in 1988, 1997, 2002 respectively. He is now working in the Institute of Electronic Computing, Jinju Medical Center, Korea. He is also a part-time professor in Jinju Health College. His research interests include network communication and security.

Chang-Geun Kim
received the B.S. degree in Computer Science from Gyeongsang National University, M.S., and Ph.D. degree in Computer Science from Gyungnam University respectively. He is a professor in the Department of Computer Science, Jinju National University. His research interests include data and mobile communication, home networking and ubiquitous networking.



Sang-Bok, Kim
received the Ph.D. degree in Electronic Engineering from Chung-Ang University in 1989. He has been a professor in the Department of Computer Science at Gyeongsang National University since 1984. He is a researcher of the Research Institute of Computer and Information Communication, Gyeongsang National University. His current research interests include multimedia communication, computer architecture, computer network and security.