Modeling and Simulation of Distributed Security Models

Hee Suk Seo[1], Tae Ho Cho[1], and Sung Do Chi[2]

[1]School of Information & Communications Engineering, Modeling & Simulation Lab, Sungkyunkwan University, Suwon, 440-746, South Korea.
{histone , taecho}@ece.skku.ac.kr

[2]Department of Computer Engineering, Hangkong University, Koyang-si, Hwajeon-dong 2001-1, Seoul, 411-791, South Korea.
sdchi@mail.hangkong.ac.kr

Abstract. It is quite necessary that an organization's information network should be equipped with a proper security system based on its scale and importance. One of the effective methods is to use the simulation model for deciding which security policy and mechanism is appropriate for the complex network. The need arises for systems to coordinate with one another, to manage diverse attacks across networks. The coordination issue is the essential problem since it is beyond the scope of any one IDS (Intrusion Detection System) to deal with the intrusions. This paper shows a modeling and simulation of network security in which the multi-security agents coordinate by sharing attacker's information for the effective detection of the intrusion.

1 Introduction

Networks are developed to make computers more accessible to the outside world. Making computers more accessible to the outside is a mixed blessing. Network security is a problem that has gotten larger with the growth of the Internet [1].

For the simulation, ID agent, SVDB (Simulation based Vulnerability Database) and Firewall models are constructed based on the DEVS (Discrete EVent system Specification) formalism [2]. Since evaluating the performance of a security system directly in real world requires heavy costs and efforts, an effective alternative solution is using the simulation model. In concrete terms, using the model we can build various simulation situations, perform iterative runs, and decide which security configuration is effective in meeting the change of network environment.

As intrusions become more sophisticated, it is beyond the scope of any one IDS to deal with them [3]. Thus we placed multiple IDSes in the network where the information helpful for detecting the intrusions is shared among these agents to cope effectively with attackers. Each agent coordinates through the BBA (Blackboard architecture) [4] for detecting intrusions. If an agent detects intrusions, it transfers attacker's information to Firewall [5] model. Using this mechanism attacker's packets detected by IDS can be prevented from damaging the network.

P.M.A. Sloot et al. (Eds.): ICCS 2003, LNCS 2660, pp. 809–818, 2003.

2 Overview of the Security Model

Security models capture policies for confidentiality (Bell-LaPadula) and for integrity (Biba). Some models apply to environments where policies are static (Bell-LaPadula), others consider dynamic changes of access rights (Chinese Wall). This section explains a few security models.

2.1 The Bell-LaPadula Model

Security models are an important concept in the design and analysis of secure systems. They capture the security policy that should be enforced in the system. The Bell-LaPadula model (BLP) is the most famous of the security models. It was developed by Bell and LaPadula. BLP is a state machine model capturing the confidentiality aspects of access control. Access permissions are defined both through an access control matrix and through security levels. Security policies prevent information flowing downwards form a high security level to a low security level. These policies are commonly referred to as multi-level security (MLS). BLP only considers the information flow that occurs when a subject observes or alters an object. BLP defines security as the property of states. Multi-level security policies allow a subject to read an object only if the subject's security level dominates the object's classification [6].

2.2 The Biba Model

The Biba model addresses integrity in terms of access by subjects to objects using a state machine model very similar to that of BLP. Integrity levels form the basis of expressing integrity policies that refer to the corruption of clean high level entities by dirty low level entities. In the integrity level, information may only flow downwards. Unlike BLP, there is no single high-level integrity policy. Instead, you find a variety of approaches [7].

3 The Structure of Target Network and Simulation Model

3.1 ID Agent

ID agent have four components: PCL, Audit, Alarm, AGENT. PCL (Packet Classify Library) model receives network's packets that are generated by the intrusion generator model and classifies them according to its usage. Then it filters the classified packets to reduce processing time as the following process. For example, for the mailbomb case, TA (Task Allocator) of PCL model receives packets from the generator model and then it transmits the packets to one of the three different types of models. These are MTONE, MTTWO, MTTHREE. If the packets that are sent to MTTWO are of TCP protocol and port number is 25 then PCL model transfers the packets to an agent model for further processing. Otherwise, MTTWO ignores it since it is useless.

AGENT model has a rule-based ES (Expert System) which plays a core component role in detecting the intrusion. It also transforms the packets, that are delivered by PCL model, into facts to be used by ES. ES inferences according to the facts thus generated. If a new attack is to be added to ID model later on, the administrator classifies the attack based on packet's type and adds a proper subcomponent model to PCL model and its corresponding rules to the AGENT model.

Audit model is composed of Auditlog and Buffer model. Auditlog model plays a following role. Intrusion detection systems often provide an audit log of their own, particularly in on-the-fly systems. Audited information is generally considered security critical and deemed suitable for storage in a protected log. Auditlog model stores the audit log of the intrusion detection system like these. Next Buffer model is explained. Generally intrusion detection system processes many information, it requires the storage for these process. This is considered buffering (or cache storage) and requires that fast hardware and software be available to keep up with target system capabilities and performance.

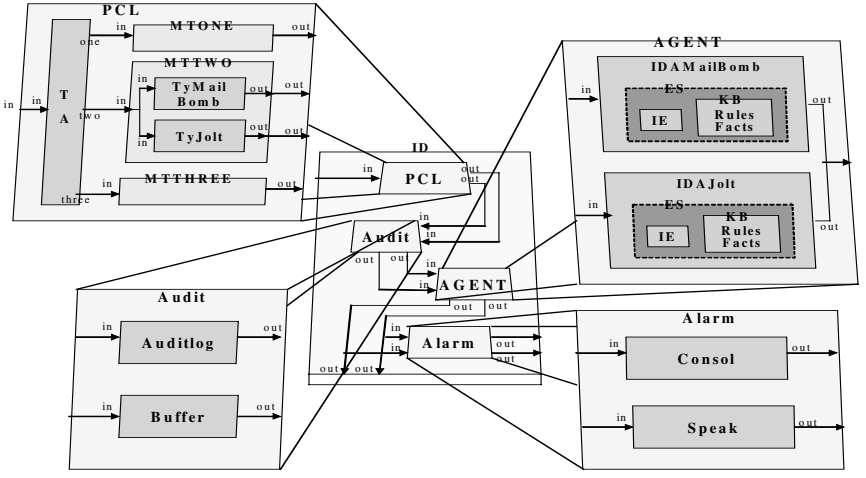

Fig. 1. Structure of intrusion detection model

Once intrusions or suspicious actions have been detected via the processing capability of the intrusion detection system, the response action most often found in available systems involves alarms. These alarms can range from simple textual messages to more involved procedures such as the sending of email to specified users, the initiation of phone calls or faxes to specified locations, or the execution of arbitrary programs in a local or remote computing environment. Alarm model has two sub-models: Consol and Speak model. Consol model send a textual messages to the monitor and Speak model rings out a alarm signal.

3.2 Vulnerability Scanner

Errors in computer systems and programs are called bugs [8]. Vulnerability scanner helps the system manager to find bugs that enable users to violate the network security policies. Vulnerability scanner is used to prepare the intrusion. We construct the SVDB for analyzing the vulnerabilities. Fig. 2 shows the structure and function of SVDB interface. SVDB has vulnerabilities of systems and policy information that can be used by security agents. Security agents-ID agents, vulnerability scanner and firewall- query the SVDB by DB interface then SVDB responses them.

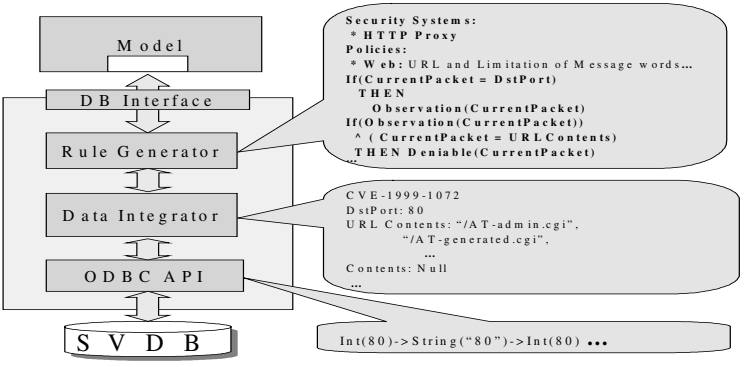

Fig. 2. Structure and function of SVDB interface

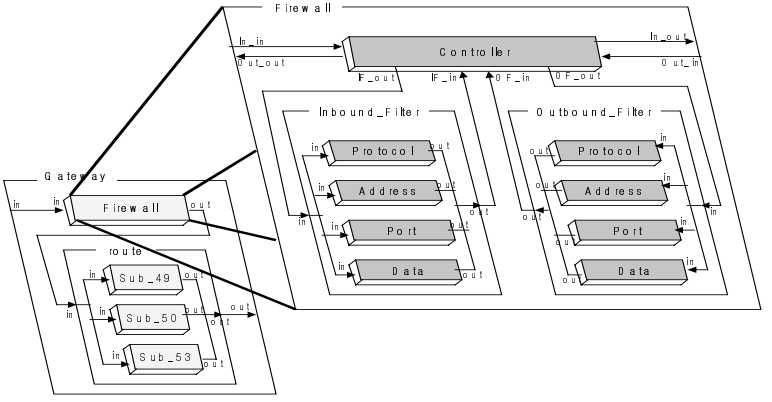

Fig. 3. Structure of firewall model

3.3 Firewall

The firewall is a way to restrict access between the Internet and the internal network [5]. Fig. 3 shows a composition of Firewall model exploited in this simulation. Firewall model is composed of a controller model, a Inbound_Filter model and a Outbound_Filter model. Inbound_Filter model includes Protocol model, Address model,

Port model and Data model. Controller model receives the packets from the internal network or from the Internet, and transfers the packets to Inbound_Filter model or Outbound_Filter model. Each Filter model processes the packets according to the security strategies and sends the packets to Controller model. Controller model sends the packets that are delivered by Inbound_Filter model or Outbound_Filter model to the network. For example, for the mailbomb case, Inbound_Filter model receives the packets from Controller model and examines the IP (Internet Protocol) address. If the packet contains the blacklist, it is ignored. If a e-mail contains harmful information, Data model of Inbound_Filter model filters the packet.

4 The Coordination among the Multi-security Agents

4.1 Communication among Agents of BB

The BBA, within the field of the distributed artificial intelligence, provides an approach to solving the coordination problem among distributed agents. BB (Blackboard) that is one of the components in the BBA is usually partitioned into several levels of abstraction appropriate for the problem at hand. The hierarchy in BB is set according to Joseph Barrus & Neil C. Rowe [9]. They proposed Danger values to be divided into five different levels. These five BB levels are Minimal, Cautionary, Noticeable, Serious and Catastrophic. We classify BB levels into each five levels for a host attack and a network attack based on these divisions. Each agent communicates by two types of messages. One is the control messages, the other is the data messages. The control messages are used to communicate between agents and controller and the data messages are required to send data between agents and blackboard.

In this paper, the BB levels for the host attack case are presented. The host attack is defined as single host out of the network hosts is attacked. In this case the attacked host inserts the intrusion related information to the Host-Attack of the BB. Each agent must request the permission, sends a BB_update_request message, to the controller in order to manage consistency and contention problems. The controller sends a BB_update_permit message to the agent when the agent can write some information to BB. The agent which receives this message writes (BB_update_action) the intrusion related information to BB. After updating is done, the agent sends the BB_update_completion message to the controller. Controller, sends a BB_broadcasting_of_action_request message, reports this event to other IDSes. IDSes, which have received the necessary information from BB, send the BB_information_acquisition_completion message to the controller. The BB levels are transit according to these steps. When the BB level is at Serious level, the agent adds the source IP address to the blacklist of the Firewall model, then all packets coming from these sources are blocked.

4.2 Problem Solving by the BB

This section presents the transition procedure of each BB level and response to the transition. As example, the transition of the BB for mailbomb attack case are shown. The levels of the BB are divided by threshold values. Threshold values are selected according to the following contents.

— the policies of the network administrator and system security level : the administrator can enforce the system security configuration to protect the network system. In this case threshold values can be a little low.
— network speed and configuration environment : threshold values can be varied by the network speed and configuration environment. Namely threshold values of network, support the high speed network environment, can be a little higher than relatively low speed. And a case of having many internal processes in a local host is a little higher than many networking processes.
— system performance (CPU, memory) : threshold values of system, have a fast CPU speed, can be a little higher than relatively low. A memory isn't different from a CPU.
— operating system types : threshold values, OS enforce the security level, can be a little higher than those not.
— attack types : threshold values can be varied according to the attack types.

Consider a case out of the various attack scenarios. There are host A and host B which are mail server and these two servers are attacked by mailbomb attack. Though there are various attack scenarios, we select one scenario.

1. An attacker starts to attack from the external network. If a threshold value of the host A reaches at the Minimal level, the initial Passive state is transit to the Minimal state of the Host-Attack.
2. While the host A is attacked, the attack for the host B is started. At last the BB transits the Minimal level. In this case the BB transits the Minimal level of the Network-Attack since the state of the BB was the Minimal state of the Host-Attack.
3. The threshold value of the host A reaches at the Cautionary level by continuing to attack then the BB transits to the Cautionary level of the Host-Attack.
4. The BB level is at the Cautionary level now and the host B is continually attacked. If the threshold value of the host B reaches at the Cautionary level, the BB transits the Cautionary level of the Network-Attack.
5. The BB level is at the Cautionary level of the Network-Attack now and the threshold value of the host A reaches at the Noticeable level. The BB transits the Noticeable of the Host-Attack.
6. The level of the BB is at the Noticeable level and the host B level reaches at the Noticeable level. The BB level transits to the Noticeable level of the Network-Attack. Since the BB level reaches the Noticeable level of the Network-Attack, the controller informs all IP addresses coming from attacker's source to the firewall. Firewall, blocks these packets, protects from damaging the host A and host B.

7. The level of the BB is at the Noticeable level and the host A level reaches at the Serious level. All network packets coming from the external network to the host A are blocked since the BB level is at the Serious level.

8. The level of the BB is at the Noticeable level and the attacker continually attacks the network so the BB level reaches at the Serious level. If the BB level is at the Serious level of the Network-Attack, this case is regarded to seriously damage the network. Finally the controller transfer these information to the firewall then the firewall blocks all packets coming to the network. By these follow-up measures the administrator grasps the extent of the damage, restores the network and prepares for the post attack.

4.3 Coordination between the IDSes and a Firewall Model

The IDSes and a firewall also communicate by two types of messages. One is a control messages, the other is a data messages. The control messages are used between the ID agent and the controller and the data messages are used between the firewall and the controller.

The coordination between the IDSes and the firewall is presented for the host attack case. The BB level is at the level, packets are blocked by firewall. A attacked ID agent transfers the BB_update_completion message to the controller then the controller sends the BB_unicasting_of_action_request message to the firewall. The firewall received this message reads (BB_information_retrieval_action) the intrusion related information on the BB. Reading is done, it transfers the BB_information_acquisition_completion message to the controller. It changes its rule table with these acquisition information and prevents the intrusion packets from coming the network.

5 Simulation Result

We have executed simulations for two cases. One is the case for 5 levels of BB to detect the intrusion, the other is the case for 10 levels of BB to detect the intrusion. Mailbomb attack and jolt attack are used for the simulation in both cases.

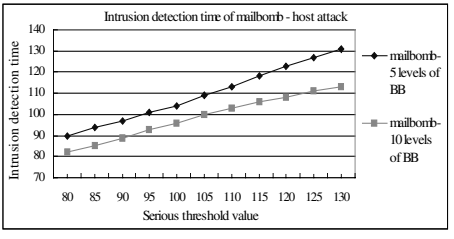

Fig. 4. Intrusion detection time of mailbomb attack – a case of host attack

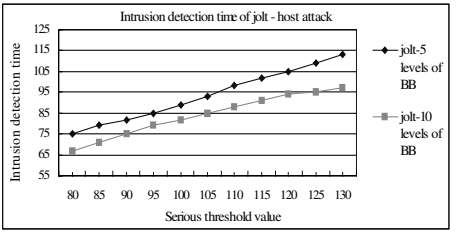

Fig. 5. Intrusion detection time of jolt attack – a case of host attack

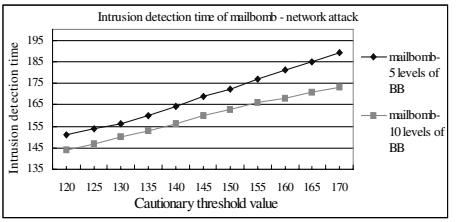

Fig. 6. Intrusion detection time of mailbomb attack – a case of network attack

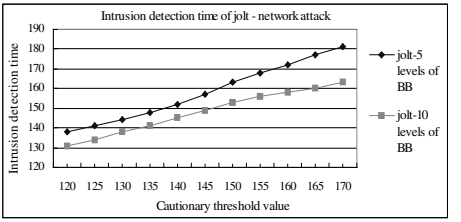

Fig. 7. Intrusion detection time of jolt attack – a case of network attack

Mailbomb attack is a type of DoS (Denial of Service) attacks. It attacks by sending a large number of mails to a mail server. Jolt attack is also a type of DoS attacks. It slices a IP datagram into small pieces and then transmits the packets of these pieces to the target system. Then the CPU (Central Processing Unit) of target system that receives these packets is over loaded since the target system has to store and reassemble all these packets. As a result, the utilization of the CPU reaches close to 100 percents and can't handle any other processes. The intrusion detection time, false positive and false negative error ratio are measured for the performance indexes in the simulation. We present in the previous studies that the multiple IDSes are superior in intrusion detection to single one [10]. In the previous research the levels of the BB are divided into 5 levels-Minimal, Cautionary, Noticeable, Serious and Catastrophic level. We have executed the simulation for the comparison the case of five BB levels with that of ten BB levels. This research shows that the proposed system with ten BB levels detects effectively the intrusion than the previous system with five BB levels.

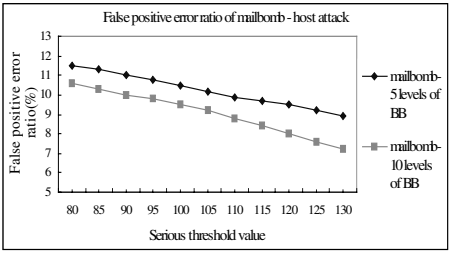

Fig. 8. FPER of mailbomb attack – a case of host attack

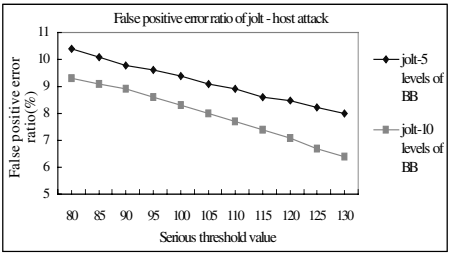

Fig. 9. FPER of jolt attack – a case of host attack

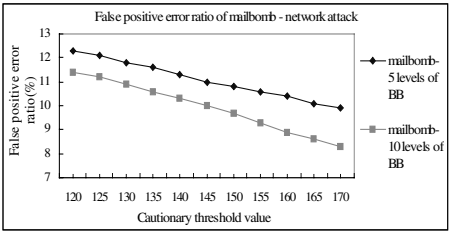

Fig. 10. FPER of mailbomb attack – a case of network attack

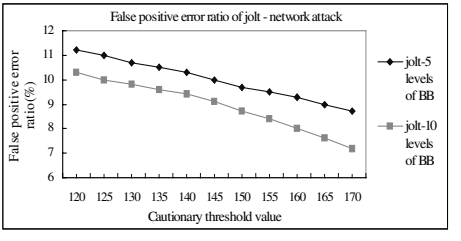

Fig. 11. FPER of jolt attack – a case of network attack

Fig. 4,5,8,9,12,13 are the case for a single IDS is attacked and Fig. 6,7,10,11,14,15 are the case for multiple IDSes are attacked. Fig. 4-7 present the intrusion detection time of the proposed system with 10 BB levels and the previous system with 5 BB levels for the mailbomb and jolt attack. The selected BB levels for the simulation are the Serious level of the Host-Attack and the Cautionary level of the Network-Attack. The other threshold values are changed according to the same ratio of change in these two threshold values. The proposed system with the 10 BB levels detects the intrusion faster than the previous system with the 5 BB levels for all the threshold values. The result shows that the proposed system coordinates effectively through BBA for detecting the intrusion. The faster the intrusion is detected, the earlier the administrators can correspond to the intrusion. It is important that the network administrator to respond at the early stage of the intrusion for the safety of the network. When the security level is weakened by increasing the serious threshold value in our system, the difference in the intrusion detection time between the proposed system and the previous system becomes larger. Because the lower the security level, the stronger the sensitivity becomes due to the information sharing among IDSes. This phenomenon related to the sensitivity applies to all other cases of the simulation results.

Fig. 8-11 show the false positive error ratio of the proposed system with the 10 BB levels and the previous system with the 5 BB levels for the mailbomb and jolt attack. A false positive is basically an alarm on acceptable behavior. Fig. 8-11 show that the false positive error ratio is increased by strengthening of the security level. This increase in the error ratio is due to the fact that the higher the security level, the more error IDSes make in both cases. Fig. 8-11 shows that the proposed system has lower error ratio than the previous system. These results means that the intrusion detection performance is improved since the sensitivity of the detection is increased by the subdivided BB level.

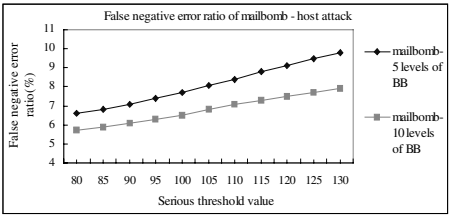

Fig. 12. FNER of mailbomb attack – a case of host attack

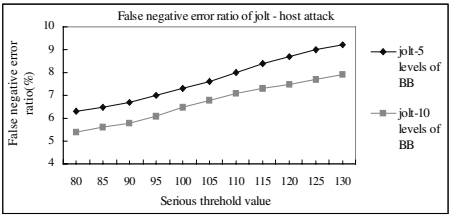

Fig. 13. FNER of jolt attack – a case of host attack

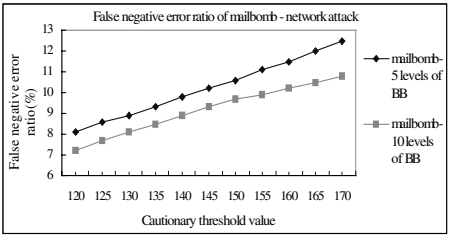

Fig. 14. FNER of mailbomb attack – a case of network attack

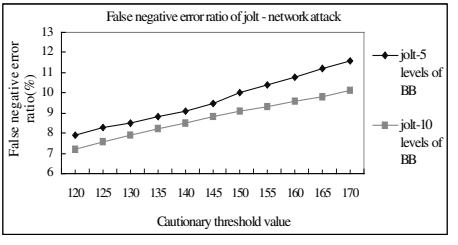

Fig. 15. FNER of jolt attack – a case of network attack

Fig. 12–15 show the false negative error ratio of the proposed system with the 10 BB levels and the previous system with the 5 BB levels for the mailbomb and jolt attack. A false negative is basically an a missed alarm condition. Fig. 12–15 show the decrease of the false positive error ratio as the security level is strengthened. For all cases, the error ratio of the proposed system is lower than that of the previous system since the intrusions are detected based on the shared information.

6 Conclusion and Future Work

As the usage of the network increases, intrusions occur more frequently and become more widespread and sophisticated. If multiple agents share the intrusion related information with one another, the detection capability can be enhanced. The system which uses BBA for the information sharing can be easily expanded by adding new agents and increasing the number of BB levels. The coordination between the Firewall component and IDS will provide the added efficiency in safe guarding the network. In the future, diverse types of intrusions should be simulated and the simulation environment should also provide a proper set of threshold values according to the specific target system being modeled.

References

1. S Mclure, J. Scambray and G. Kurtz, "Hacking Exposed: Network Security Secrets and Solutions," McGraw-Hill, 1999.
2. B. P. Zeigler, "Object-Oriented Simulation with Hierarchical, Modular Models," San Diego, CA, USA:Academic Press, 1990.
3. S. Northcutt, "Network Intrusion Detection – An Analyst's Handbook," New Riders Publishing, 1999.
4. K. Decker, A. Garvey, M. Humphrey and V. R. Lesser, "Control Heuristics for Scheduling in a Parallel Blackboard System," International Journal of pattern Recognition and Artificial Intelligence, Vol. 7, No. 2, pp. 243–264, 1993.
5. E. D. Zwicky, "Building Internet Firewalls," 2nd Ed., O'Relly & Associates, 2000.
6. Dieter Gollmann, "Computer Security," Wiley, 1999.
7. K. J. Biba. "Integrity consideration for secure computer systems," Technical Report ESDTR-76-372, MTR-3153, The MITRE Corporation, Bedford, MA, Apr. 1977.
8. J. Forristal and G. Shipley, "Vulnerability Assessment Scanners," Network Computing, 8 Jan. 2001.
9. J. Barrus and N. C. Rowe, "A Distributed Autonomous-Agent Network-Intrusion Detection and Response System," Proceedings of Command and Control Research and Technology Symposium, Monterey CA, pp. 577-586, Jun. 1998.
10. H.S. Seo and T.H. Cho, "Modeling and Simulation for Detecting a Distributed Denial of Service Attack," Lecture Notes in Artificial Intelligence, Springer Verlag, Dec. 2002.