Multi-Domain Security Management Framework and Its Performance Evaluation to Protect BcN Infrastructure

Jung-Sook Jang, Yong-Hee Jeon°, Jong-Soo Jang†

Catholic University of Daegu, Gyeongsan, Gyeongbuk, Korea
†Applied Security Group, Information Security Division, ETRI, Daejeon, Korea

Summary

BcN(Broadband convergence Network) is being deployed in order to support a variety of network applications, with enhanced capabilities of QoS(Quality of Service) provisioning and security, and IPv6. In a high-speed network environment such as BcN, it is more likely for the network resources to be exposed to various intrusion activities. The propagation speed of intrusion is also expected to be much faster than in the existing Internet. In this paper, we present a multi-domain security management framework which may be used for a global intrusion detection at multiple domains of BcN and describe its characteristics. For the performance evaluation, we first present test results for the security node and compare with other products. Then we design and implement an OPNET simulator for the proposed framework, and present some simulation results. In the simulation model, we focus on the performance of alert information in the security overlay network.

Key words:

Broadband convergence Networks, Intrusion Detection System, Security Management, Communication Model, Performance Evaluation, Simulation.

1. Introduction

BcN (Broadband convergence Network) is a network which allows users to use seamless quality-guaranteed broadband multi-media services which converge communications, broadcasts and Internet at anytime and anywhere. For this purpose, BcN transport network must be a communication network which adopts open API which helps to create various services easily through a high degree of management function and security, guaranteed QoS (Quality of Service), IPv6 addressing scheme. And it must adopt characteristics of various subscriber networks such as wireline, wireless and broadcasts and be able to provide environments which enable various application services developments and their uses through a standard interface.

The three infrastructures in the u-IT839 project which was led by the Ministry of Information and Communication of Korea are BcN, IPv6 and USN (Ubiquitous Sensor Network). The network security plans are needed desperately in broadband convergence network environments such as BcN since a single security intrusion can be propagated over the whole network rapidly and can cause serious damages, the cyber intrusions are getting more intelligent and vicious, and the access to the communication network is easy using various paths.

The network or service providers have to decide which security plans they will devise based on the results of threat analysis and risk evaluation. Considering different architectures of transmission, the main types of possible threats to BcN are as follows [1]:

· Denial of Service (DoS): Flooding networks with data so that other users can't access to the networks.

· Eavesdropping: Threatening the privacy by intercepting information between sender and receiver.

· Hacking or intrusion attack: The intruder gets illegal access to some areas or resources.

· Virus or warm: Spread over the network and destroy or modify information.

· Masquerade: Disguise someone's identity and get access to resources.

· Replay attack: Re-transmit packets or packet streams at a later time.

· Unauthorized access: Unauthorized access can cause DoS, eavesdropping or masquerade and it can also be caused by the treats which are mentioned above.

· Information modification: Attacks which modify packets, manipulate data or destroy database.

· Repudiation : A user in a communication can repudiate part of or whole communication with other users.

In Korea, the government has devised and is promoting security plans to build an effective BcN. The security in primary plans of BcN construction means the actions on the threats and side effects which obstruct information communication environment such as paralysis of information communication networks, leak of personal information and flow of unwholesome information [2]. She is building safe, reliable and healthy cyber network environments through advanced information protection technologies and integration of information security schemes.

In this paper, we discuss security issues which need to be considered to implement BcN and introduce technologies to protect the BcN infrastructure. In Chapter 3, we present multi-domain security management

Manuscript received January 5, 2008
Manuscript revised January 20, 2008
– o: The corresponding author

frameworks which use Security Overlay Networks (SON). And in Chapter 4, we present results of performance tests for hardware-based advanced security nodes which are implemented to protect BcN infrastructures and we will also construct simulators to evaluate the performance of intrusion detection information delivery and present its results of performance evaluation.

2. Background

2.1 Security requirements and countermeasures

(1) Security requirements

The security policy means the strength of mechanisms and set of security services which are defined by the administrator of a domain. The security plans have to be established based on the situations. It is quite abstract to establish well-defined security requirements using formal and accurate methods. They used TIPHON [3] as a threat analysis guide in Alcatel NGN. The general security requirements are as follows:

· Accountability: the feature which allows tracing an object for its actions.

· Authorization: the functionality which allows access based on their access rights.

· Authentication: the functionality which confirms the source of the received data.

To protect BcN infrastructure information, security management technology which actively detects and reacts on network threats at the ingress point of the network, high-performance network threat coping technology which considers the speed of network development, detection technology which detects known intrusion attacks and excessive traffics which are caused by unknown intrusions and control technology which cuts off malicious traffic and controls bandwidth are required [4].

(2) Countermeasures

The countermeasures are generally classified into preventive ones and detective ones. The general countermeasures which can cope with the threats mentioned above are as follows [1]:

· Authentication: the functionality which confirms the source of the received data.

· Digital signature: it guarantees the source of message and integrity by attaching the signature of the message creator through authentication mechanism.

· Access control: the control which only allows the users who have the access right to access to objects.

· Virtual Private Network (VPN): it uses encryption to protect the data which are transferred through Internet. The only users who have the access right can connect through VPN.

· Encryption: changing normal data format to hard-to-read format using encryption algorithms.

· Intrusion detection and prevention: monitoring network traffics to detect potential misuses or policy violations and detect intrusion by analyzing attack signature. Intrusion prevention is used with intrusion detection to prevent the success of intrusion attacks as soon as possible.

· Auditing and logging: to provide the reporting tool for system status information.

·Non−repudiation countermeasure: the countermeasure to prevent repudiation of sending and receiving data.

In the next chapter, we will describe intrusion detection and prevention which are most related to this paper among the countermeasures described above.

2.2 Countermeasure technology

(1) Intrusion Detection

Intrusion Detection System (IDS) can be defined as a tool, method or resource which helps to recognize, estimate and report network activities which are not authorized or approved [5]. The IDS is only a small part of whole security system. The firewalls, IDS and IPS (Intrusion Prevention System) are used together to alert and prevent intrusions to network. They only use different technologies.

The commercial network-based IDS (NIDS: Network-based IDS) has been used since mid 1990s [6]. The 1st generation commercial NIDS was a pure signature-based model. The 2nd generation NIDS used rules instead of signature to solve problems of the pure signature-based systems. It compares the packet signatures with set of rules instead of exploit signature. The technology which prevents wrong interpretation of data must be used in packet signature detection to process traffics accurately [7]. The 3rd generation NIDS uses protocol anomaly detection to detect attacks and solve the performance and accuracy issues of 2nd generation NIDS. The protocol anomaly NIDS can detect attacks by monitoring inappropriate usage of protocols which are allowed in networks. The advantages of protocol anomaly detection are as follows [7]:

- It can detect new unknown attacks based on the fact that the attacks are against the protocol standards.
- It detects attacks which bypass systems implementing different detection methods.

- It detects attacks which modified their known attack patterns to avoid signature-based system without reducing their attack strength.

The examples are FTP bounce attack detection and un-documented buffer overflow attack detection.

(2) Intrusion Prevention

The Intrusion Prevention System (IPS) is also divided into host-based system and network-based system [8-10]. According to the definition of Gartner, host-based IPS (HIPS) must be software products and be able to protect weak application programs through set of firewall rules or learning of normal/abnormal access. And it can operate independently with kernel or operate together with kernel. The former host-based IPS (operating independently with kernel) can be classified as products which filter events which are against certain rules using signature and behavior-based analysis algorithms. The later host-based IPS (operate together with kernel) can be classified as trust operating system products which have access control functionalities.

According to the definition of Gartner, again, network-based IPS (NIPS) must be the products which are located on the line of network for fast reaction speed and intrusion prevention abilities and must be the system which can support session aware inspection. And it is essential to cut off malicious sessions using various prevention methods such as signatures, abnormal behavior detection of protocols.

2.3 Requirements and performance parameters of IDS

In this section, we describe the requirements and performance decision factors of communication framework of IDS [11]. Based on this, we will decide the parameters which are needed for performance analysis of the proposed communication framework. Some characteristics which classify the distributed IDS are as follows:

· Number of E (event) boxes and their locations
· Number of A (analyzer) boxes and their locations
· Coordination between components
· Communication frameworks

Where, E-box is data collecting device and A-box is data analyzing device. The frameworks consist of communication mechanisms and communication models. The existing approaches which are used for communication mechanisms are TCP, UDP, SSH (Secure Shell) and SNMP (Simple Network Management Protocol).

The desirable characteristics of communication methods for IDS are as follows: reliability, security, authentication, integrity, confidentiality, non-repudiation, non-duplication, resistance against DOS attack, scalability and speed.

The important functionality of distributed intrusion detection system is the communication between different components. By exchanging messages, the components know the status of the whole system. The collapse of communication can cause system failure and malfunctions. The following factors are interdependent but not mutually exclusive [12]: Number of components and their locations, types of considered data, data amount, frequencies of data generation, data presentation method and sensitiveness of data.

3. Proposed security management framework

3.1 Overview

As a policy-based system, the proposed system establishes law or rules which control the dispersion of important information and resources in a certain system. The security policy system consists of Security Policy Database (SPD), Security Policy Server (SPS) and Policy Client (PC), and it exchanges data using Security Policy Protocols (SPP). The rule-based policy, as one example of the policies, enables automated operations of security policy using qualifiers such as IP address, time, protocols, cutoff, login, alerts and access permission [13].

The standard protocols of these policy-based IDS are COPS, IAP/IDXP and SNMP, and have the following characteristics.

· Common Open Policy System (COPS): the COPS of IETF is a simple TCP-based query/reply protocol which enables the transmission of policy information between policy servers (PDP) and clients (PEP) in policy-based networks. It supports various types of clients through expansion without changing the protocol itself. The COPS is TCP-based policy delivery protocol which aims to provide and control policies of higher domains [14].

· Alert protocol: the IDWG of IETF suggested the Intrusion Alert Protocol (IAP). It is an application layer protocol to exchange intrusion alert data among intrusion detection components (sensor/analyzer and managers). The transferred alerts are detailed in IDMEF (Intrusion Detection Message Exchange Format). The two IDMEF which are currently defined are alert and heartbeat [15].

3.2 Global network security management architecture

To protect communications and systems on networks, we need security managements on the network side. The network side security management can be only achieved by the share of security information with neighboring service providers. The importance of data protection

services on network side increases and this has introduced many network data protection products which can process from hundreds Mbps to Gbps but there still exists security limits in individual systems.

To solve these problems, defining global network security management structure which performs overall intrusion detection analysis on network side becomes the main issue. And if we can apply policy frameworks and overall analysis skills to distributed intrusion detection system, the global network security management will be possible.

3.2.1 System structure

If we can disperse security nodes to entire networks and manage them in the center to provide the network sided data protection service, we can solve the problems which the existing single environmental data protection services have. That is, to react effectively to various attacks and high increase of traffic, we have to expand current local security environment to wide security environment so that we can manage the security of networks using policy-based frameworks which enables systematic inter-working between systems. We can also apply hierarchical overall analysis methods to react quickly by collecting various data and analyzing them.

Therefore, we can solve the problems of existing single environments by managing the highest policy server by separating intrusion detection and countermeasure functionality from the policy-based frameworks and disperse them to whole wide networks. And the decisions and permissions of proper countermeasure policy are possible which is suitable for intrusion prediction and environments using hierarchical analysis.

Figure 1 represents a multi-domain security management model which enables complete network security management which has host-based, network based, distributed intrusion detection system and center intrusion detection system architectures. The proposed multi-domain security management model is based on IETF policy frameworks to perform complete intrusion detection. And it also has hierarchical structure of complete domains which consist of analyzers, local domains and security policy servers. The lowest level analyzer consists of each domain agents which detect various forms of intrusions and each agent reports the detected information to its higher local domain manager. The analyzers which are consisted of agents analyze the intrusion based on their established security policy [11, 16].

The analyzer has agents which detect various intrusions. They are agents which analyze and alert network-based intrusions, agents which check the status of the analyzer and report to higher manager and agents which transmit data based on host-based logs. Each analyzer reports the alerts and logs messages to higher manager asynchronously and reports the status of the analyzer to higher manager regularly. The higher manager analyzes the reported intrusion detection information and reports them to the highest complete domain and stores the records. The highest complete domain manager establishes security policies through security policy server based on the reported detection information and then delivers the security policy to lower nodes.

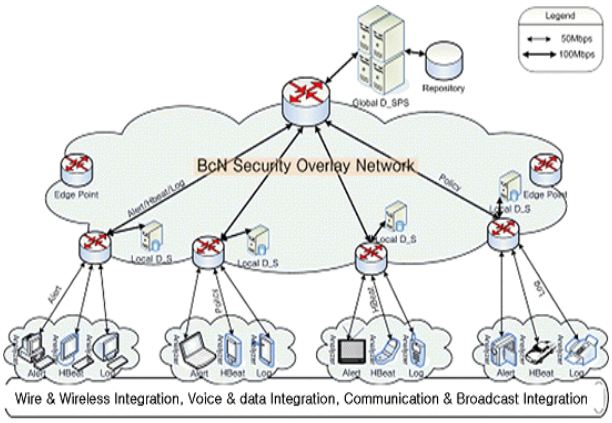

Fig. 1 Proposed multi-domain security management model

The proposed communication model, in this paper, can be treated as distributed intrusion detection since each agent performs independent intrusion detections. And the main characteristic of this model is that it transmits the alerts or other important event data from local domain to higher manager and allows information exchange between intrusion detection systems in a huge distributed system. Under the distributed intrusion detection system structure, it uses hierarchical intrusion analysis method which provides judgment and method for overall security situation and it also provides policy-based management structure which allows systematic security managements for global network security control framework [17, 18]. The main characteristics of proposed multi-domain security management framework are as follows:

A. Global framework

The global network security management technology is the network side security management which complements local networks security management. It prevents the performance degradation of networks by analyzing and blocking malicious traffics in the network ingress point and protects resources and main communication equipments of networks.

The global security management network has security overlay network structures and guarantees constant

security services in the wide-area networks which users use by exchanging of security related information and complementary cooperation with neighboring domains. It can also strengthen the security of core networks and provide stable service traffics.

B. Security policy-based management structure

We can securely manage networks by applying IETF policy-based frameworks which provide structural, systematic and overall management. The policy-based network security management frameworks provide stable controls over network resources and security managements. The security policy-based security management framework has centered management structures which are consisted of multi-policy target systems (STS) which are managed by security policy servers of security policy system (SPS). The area which is managed by the security server using a consistent policy is called domain. And all the security related information which occurs in the domain are transmitted to security policy server of the domain and are managed systematically. And if necessary it can be transmitted to neighboring domains. Fig. 2 shows the security policy management structure.

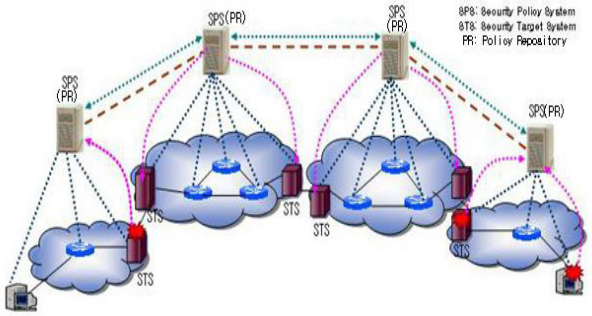

Fig. 2 Security policy management structure

In the policy frameworks, the security policy system consists of policy server and policy storage, and the security target system has the functional components of policy targets. The policy server consists of policy management tools and policy decision functionality and the policy storage can possibly exist as an independent system from policy server. And also, the policy targets are network systems which operate the policy. The area border router will be the policy target in resource management point of view.

C. Hierarchical intrusion analysis method

Since individual managements of security analysis equipment and their inter-working are impossible, the network managers have difficulties in overall managements and it shows the limit of security system operations. Since the individual security devices operate single-sided intrusion analysis in the single system level, they can't operate overall network level intrusion analysis and predictions.

To solve this problem, we use the hierarchical analysis method which consists of simple analysis and statistical analysis which allows the overall network analysis based on event information and path information which are from security device analysis.

The hierarchical intrusion analysis collects all security event information which occurs in policy domains and operates security status analysis through systematic managements of the security event information. This allows us to construct overall network security management frameworks.

The security nodes, which are located in the entrance of networks, operate lower-level intrusion analysis through comparison analysis which operates signature-based intrusion detection and observation analysis which monitors traffic patterns. Based on the lower-level intrusion analysis, the security nodes react against the intrusions in real time or transmit the alerts to higher-level security policy server. This enables the prediction of higher-level intrusions.

Fig. 3 shows the hierarchical communication process of proposed model.

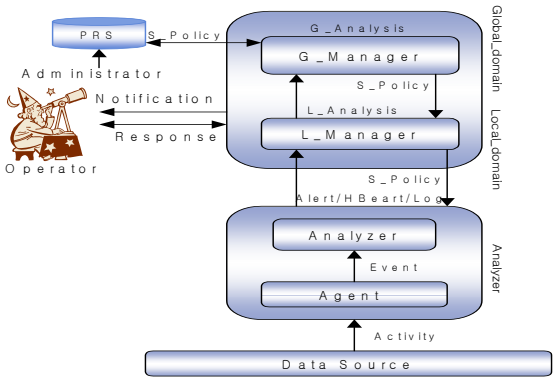

Fig. 3 Communication process of proposed model

The security policy server, which collects and manages the security related information of the whole networks, operates intrusion predictions in higher-level by intrusion possibility analysis, potential analysis and similarity analysis based on statistical data. Based on this intrusion prediction, we can decide the countermeasure policy which will be applied in the networks and share the intrusion information with neighboring domains through communications. This enables overall security

management since we can construct network-level intrusion countermeasure structures.

3.2.2 Node structure

Due to the dramatic growth of Internet, the network environments for high-speed and high-capacity, such as Ethernet, are being widespread. And the developments of many security mechanisms which detect and prevent intrusions are under progress. It also requires to process large data with high-performance. The studies on structures which allows the developments of giga-level intrusion detection systems and system performance analysis which allows us to predict the system performances are very important. The system performance is decided by the hardware characteristics on the chip and the software which it runs. We can examine the bottle-neck effects of system using system performance analysis of intrusion detection nodes. We can also find the problems in packet processing using this and improve the structures. Furthermore, we can improve the intrusion detection performance by finding effective packet processing algorithms.

In this section, we analyze the structures of security nodes in giga-bit intrusion detection systems to provide the countermeasures and intrusion detection in high-speed network environments. Due to the network speed increases, we need to have suitable high-speed intrusion detection technologies. Therefore, it requires the developments of security engines and security appliance which is faster than 10G-bits. Therefore, the study on performance analysis according to system structures is very important and essential. Fig. 4 is a system block diagram of security node structure of giga-bit intrusion detection system which provides high-speed intrusion detection and countermeasures [19].

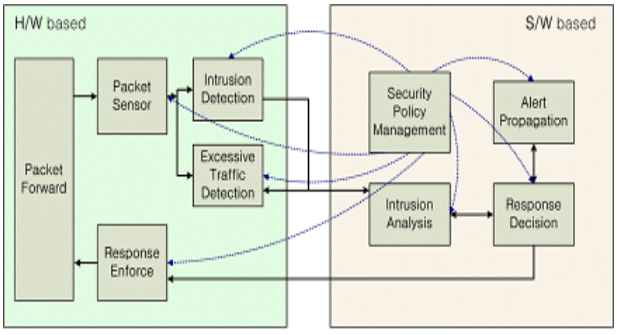

Fig. 4 Security Node Block Diagram

The security nodes use Ethernet interface security cards which use hardware-based high-speed signature detection for intrusions. And this accelerates the detection and blocks malicious network traffics and supports giga-bit network speed. It also supports not only traffic monitoring but also real time countermeasures and it is easy to provide self system security using stealth operations in the networks. After the intrusion analysis, if it turns out to be malicious traffics, it countermeasures immediately to minimize the damages.

4. Performance evaluation

4.1 Performance test of security node

Fig. 5 shows the test bed which consists of the IXIA Traffic Generator, Analyzer, Giga-bit L2 Switch and Security Card which were used for the security nodes (Gateway system) performance evaluation.

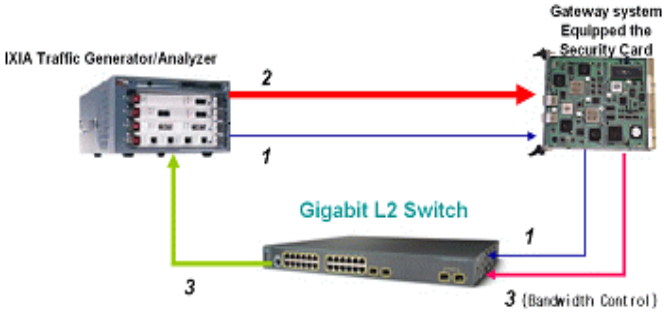

Fig. 5 Security nodes test bed

Table 1 shows the results of the performance tests on the functions of sensors and countermeasures of the abnormal traffics, and detection and blocking of the intrusions among the functionalities of the security nodes. It shows the same performance compared to other products in the performance of sensors and countermeasures of the abnormal traffics of 64, 1500 byte intrusion packet, and better performance of processing per second in connection set-up capacity. In detection and blocking of the intrusions, it also shows the better performance than the products of other companies both in network capacities and signature-based detections.

Table 1:Security nodes test results

SGS Function		Plan Level	Result Level (Note1)	Comm. Prod. Compare1 (Note2)	Comm. Prod. Compare2 (Note2)
Abnormal Traffic Detection & Respones	Processable Network Capacity	790 Mbps(64 byte), 1 Gbps(1500 byte) Lossless	790 Mbps(64 byte), 1 Gbps(1500 byte) Lossless	'A' IPS : 790 Mbps (64 byte) (Note3), 1 Gbps(1500 byte) Lossless	'B' IPS : 790 Mbps (64 byte), 1 Gbps(1500 byte) Lossless
	Connection Setup processing capacity	60000/s	64000/s	'A' IPS : 54000/s	'B' IPS : 25000/s
Intrusion Detection & Isolation Function	Processable Network Capacity	790 Mbps(64 byte), 1 Gbps(1500 byte) Lossless	790 Mbps(64 byte), 1 Gbps(1500 byte) Lossless	'A' IPS : 600 Mbps (64 byte), 1 Gbps(1500 byte)	'C' IPS : 150 Mbps (64 byte), 500 Mbps(1500 byte)
	Signature Based Detection Function	100%	100%	'A' IPS : 80%	'C' IPS : 92%

(Note 1) Test device measurements
(Note 2) Reference: Tolly Group report no.204146
(Note 3) Maximum theoretical bps of 64byte packet in giga-bit Ethernet

We executed the following scenarios to test against the attacks on DDoS.

· The generation of the abnormal traffics was increased to 1Gbps by increasing it from traffic generator port(2) of the (Fig. 5) by 40Mbps unit.

· Enforcing rate-limiting rule against the abnormal traffics (3 of the Fig. 5): Generating and enforcing of the rules for the Security Card would be done by the policy manager.

· Policing each flow to 40Mbps in the receiving end of the Traffic Analyzer.

· Policing only abnormal traffics, and transporting normal traffics.

In the scenarios above, bandwidth controller controls output traffics at the 40Mbps rate. Thus, the sum of eight flow traffics is 320 Mbps. The output traffic rate is 320 Mbps, and normal traffic at 40 Mbps was transferred without any losses in the test as it is shown in Fig. 6.

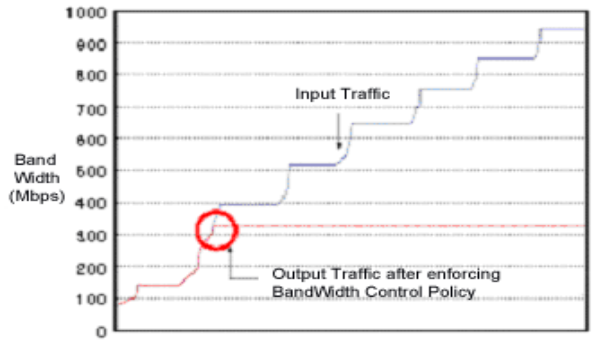

Fig. 6 Controlling excessive traffics (320Mbps) by bandwidth

4.2 Design and Implementation of the Simulator

OPNET Modeler was used in designing and implementing the simulator to evaluate the performance of the alert information and the implementation of the proposed multi-domain security management model. Fig. 7 shows an example of the network model, the node model and the process model of implemented simulator.

Table 2 is the size of each event data which is applied to this IDS evaluation model. In implementing simulator, transmission rate of 50 Mbps was used in link between analyzers and local domains, while 150 Mbps was used in connection between analyzers and total area domains, and finite buffer was used in each analyzer and policy server for scheduling and processing of the data.

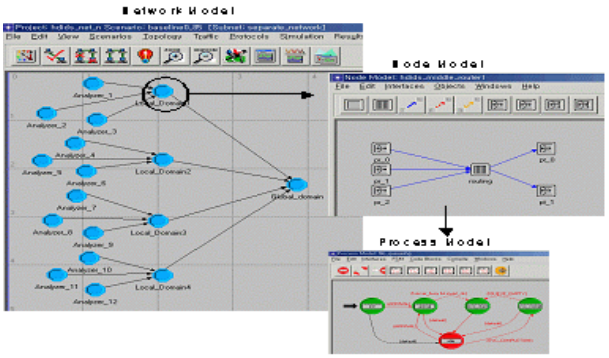

Fig. 7 An Example of each simulator model

Table 2: Data Size per Event Type(unit: byte)

Event Type	Alert	HeartBeat	Log Data
Size	512	512	440

4.3 Simulation and Performance Analysis

In the simulation and performance analysis, we will provide the results of the performance simulation using the simulator which is developed for the multi-domain security management model and analyze the results. In the simulation, we assumed that the reports of the detected information and delivery of security policies of security policy server are independent separate networks. The performance analysis was carried in the two different stages. The first stage of performance analysis starts from the analyzer which detects the intrusion and then to the top of the total area domain security policy server, according to the delivery of the information, and in the second stage, we analyze the performance of delivery of security policy from the security policy server to the analyzer. Only the delay is used as the parameter of the performance analysis. The parameter used in this performance analysis was determined by considering the factors of performance determination described in Chapters 2 and 3 and parameters of general network performance analysis, but performance analysis on the expression method of data and sensitivity were not executed.

A. Parameters of the Performance Evaluation

Points of observation of each parameter are described in Table 3.

Table 3: Simulation Evaluation Items based on Performance Parameters

Simulation Evaluation Items
Effect of Network Utilization
Effect of Event Date Type and Size
Effect of the Number of Agents
Effect of Data Generation Frequency
Effect of Hot-Spot
Effect of Back Ground Traffic

B. Performance Evaluation

(1) The Effects of Network Usage Rate

Fig. 8 and Fig. 9 show the average delay performance of each event when reporting the information of detected intrusions to the security policy server in the global domain. Fig. 8 shows the average delay of the transported packet according to the variation of the size of input load (that is, network utilization rate) at the global domains and the local domains. The delay increases exponentially at 0.7 or higher utilization rate.

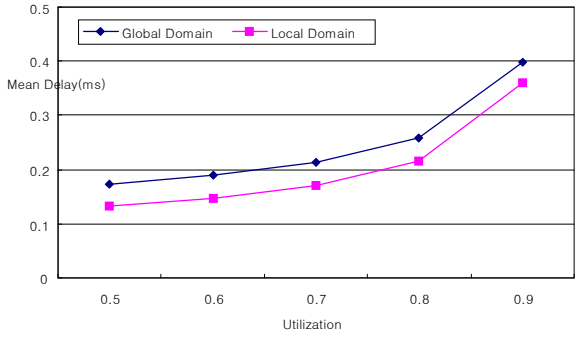

Fig. 8 Effect of Network Utilization

(2) The Effects of the Pattern and Size of the Event Data

Fig. 9 shows the delay performance of different types of event.

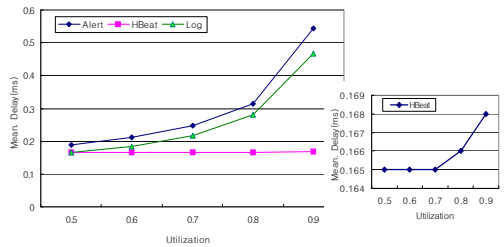

Fig. 9 Effect of Event Date Type and Size.

Since the alert and the log event show the clear trend of increasing of delay which follows the trend of utilization rate, but since the status information of analyzer is reported regularly regardless of variation of status of network, visible delay performance shows relatively small variation of delay comparing to other event data. However, the detailed analysis of the status information in Fig. 9 shows delicate increase of delay by the utilization rate.

(3) The Effects of the Number of Agents

In distributed intrusion detection system of the global security, one of the determinant factors of the communication mechanism through hierarchy is the number of components which detects the intrusions, that is, the number of agents. Fig. 10 shows the increase of the delay as the number of agents increases. It shows the delay performance of the network increases tremendously when the number of agent increases by 3 times, 6 times and 12 times.

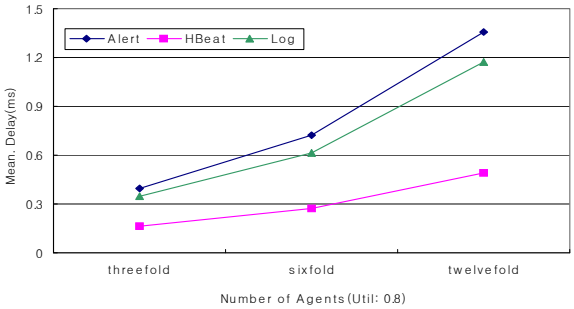

Fig. 10 Delay by the Number of Agents

(4) The Effects of Frequency of Data Generation

We analyzed the effects of excessive frequency of event generation on the network performance when the frequency of events increases. Fig. 11 presents the delay performance in accordance with the frequency of the data generation.

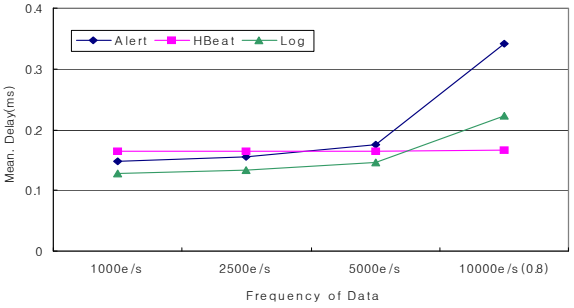

Fig. 11 Delay of Data Generation Frequency

We may know that excessive number of events can be generated by attacks from the existing agents in other

domains when distributed DoS attack happens. Also, we can know that this has great effects on network performance. On the other hand, the delivery performance of transmission of regular status information is affected relatively less.

(5) The Effects of Hot Spots

Hot Spot is the phenomenon of concentrated occurrence of events which have specific data patterns. Using the Hot Spot, the performance on the specific part of network can be analyzed. Fig. 12 shows the influence of the Hot Spot on the alert data. In Fig. 12, at constant utilization rate, the delay of alert data increases while delay performance of log data of the non-Hot Spot data decreases in accordance with increase of the Hot Spot of the alert data. The variation of the delay of status information agents is little because of the regular occurrence of events.

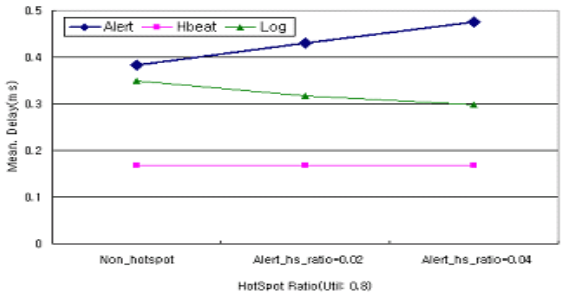

Fig. 12 Hot-Spot Effect of Alert

(6) Effects of background traffic

All capabilities of mixed-type IDS evaluation model for multi-domain security management were analyzed based on the assumption that they are all separate-networks. Non-separate network means that there are traffics which are used in the existing networks, so we analyzed the influence according to the amount of background traffic usage. Fig. 13 shows the performance of network when using background traffics.

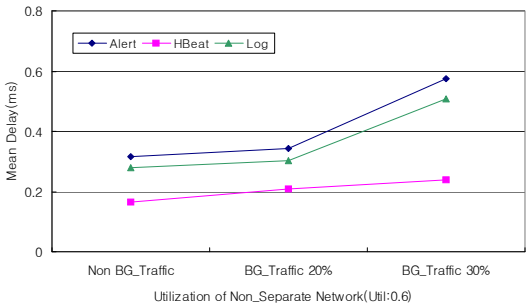

Fig. 13 Effects of background traffics.

We can see that as the rate of background traffic increases, network delay in every types of data including status information data increases greatly.
Considering that the delay for encryption is also included when sending IDS information with general network traffics, usage of separate network for security information transmission must have many advantages.

(7) Fault tolerant structure and analysis

The structure of hybrid type IDS model for multi-domain security management which is suggested in this paper manages security through all area with hierarchical organization from distributed IDS to security policy server of center-concentrated type. Policy server in global domain is organized in a single structure. The failure of policy server, the top manager, means the practice of every security policy is impossible. Therefore, through duality of security policy server, we designed structure which is well adapted to the defects, implemented the structure, and analyzed the performance. Each local domain analyzer reports detection information to the local domain server and the server reports to the global security policy server, which is organized in dualistic structure.

In the fault tolerant structure, each domain server sends the information to the security policy server through different links. Information of analyzers in the origin is reported to primary security policy server and the packet that is copied in local domain server is sent to backup security policy server. The delay performance that reached main security policy server seems to have no large difference in network performance compared to single security policy server system. Yet, additional expense is needed due to duality of security policy server and addition of links.

5. Conclusions and further research

The characteristic of BcN network can be summarized to have QoS security, provision of security function, IPv6 provisioning, and open API. In circumstances, when security accident happens, the damages caused by the accident can be spread faster and more widely than it used to be in the existing information communication infrastructures, so more serious communication damages are expected. Therefore, proper countermeasure for security of BcN must be established. However, it is hard to find literatures of BcN security technology in the country. Therefore, in this paper, we inquired into vulnerability and demands of BcN security as a related study and described about BcN infrastructure protection technology.

To deal more actively with excessive traffic analysis of individual system units and various types of intrusion for

BcN security, global network security control framework technology for expansion of the range of security circumstance from region to much broader area is needed. In the global network security control framework, intrusion is predicted through synthetic analysis of output traffics of each local network and multilevel analysis of network, status information, management information and statistic information. Through these processes, proper countermeasures for the circumstance can be decided. For this, high-speed intrusion detection engine, development of delivery protocol and techniques for abridgment of transmitted information, establishment of cooperation mechanism for information sharing, and synthetic countermeasure scenario for synthetic invasion are needed.

In this global framework, communication between components is an important part of functionalities of the whole system. Since components can learn general status of system through communication message, collapse of communication can cause wrong motions of whole system or failure. Therefore we suggested a model that enables security management of multi-domain in the BcN environment. We executed modeling for the proposed communication model, designed and implemented a simulator. Also, we executed trial examination about number of components which are the main determinant factor of communication mechanism of global framework, usage of network, type and size of event data, and data formation frequency. As the result, we found that excessive number of agents affects the performance of network. Next, we analyzed performance of network according to the frequency of generation of event. We found that as frequency of alert increases, the excessive traffics were created and affected the performance of network greatly. We think that the results which are suggested in this paper can be applied to the system design for overall network security management.

The construction of global countermeasure system through effective cooperation between networks for the BcN security and scheme for standardization of information related to information protection which can be exchanged between the networks and imposition of exchange are needed. Also, we think that studies and developments of security technology which is related to BcN need to be promoted systematically for realization of safe BcN.

References

[1] B. Gamm, B. Howard, O. Paridaens, "Security features required in an NGN", Alcatel Telecommunications Review, 2nd Quarter 2001, pp.129-133.

[2] The Ministry of Information and Communication BcN Construction Basic Plan, NIA, pp. 76-83, February 2004,

[3] "Telecommunications and Internet Protocol Harmonization over Networks(TIPHON) Security; Threat Analysis", DTR/TIPHON - 08002 V0.1.9 (2001-02-09).

[4] Seo D.L., Kim K.S., Jang J.S., Sohn S.W., "Information Security Technology Development Trend for IT 839 Strategy Promotion", ETRI, Electronic Communication Trend Analysis 20-1, February 2005.

[5] Carl Endorf, Eugene Schultz, and Jim Mellander, Intrusion Detection & Prevention, McGraw-Hill, 2004.

[6] Eric Ahlm, Is Intrusion Prevention Changing Information Security, Rev. Ver. 1.1, March 2004, Vigilar Inc.

[7] A White Paper by NetScreen Technologies Inc., Intrusion Detection and Prevention: Protecting your network from attacks, version 2.0, http://www.netscreen.com

[8] Ian Poynter and Brad Doctor, Beyond the firewall: The next level of network security, StillSecure, Jan. 2003.

[9] Top Layer White Paper, Beyond IDS: Essentials of Network Intrusion Prevention, pp.1-18, Nov. 2002.

[10] Neil Desai, Intrusion Prevention Systems: the Next Step in the Evolution of IDS, http://www.securityfocus.com/printable/infocus/1670, Feb. 2003.

[11] Diego Martin Zamboni, “Using Internal Sensors for Computer Intrusion Detection”, Ph. D. dissertation, Purdue University, CERIAS TR 2001-42, August 2001.

[12] Rajeev Gopalakrishna, "A Framework for Distributed Intrusion Detection using Interest-Driven Cooperating Agents", CERIAS Tech. Report 2001-44, Purdue University, 2001.

[13] Madalina Baltatu, Antonio Lioy, and Daniele Mazzocchi, "Security Policy System: status and perspective", pp. 278-284. 1999.

[14] IETF, RFC 3084, "COPS Usage for Policy Provisioning (COPS-PR)", March 2001.

[15] D. Curry, H. Debar, "Intrusion Detection Message Exchange Format Data Model and Extensible Markup Language (XML) Document Type Definition", IETF Internet Draft, draft-ietf-idwg-idmef-xml-07.txt, Jun 2002.

[16]IP Security Policy, http://www.ietf.org/html.charters/ipsp-charter.html

[17] Jang J.S., Kim K.Y., Ryu K.W., "Global Network Security Control Framework for Safe Information Security Infrastructure", The Journal of The Korean Institute of Communication Sciences 19-8, pp.1146-1156, August 2002.

[18] M. Stevens, Policy Framework Internet Draft, draft-ietf-policy-framework-05.txt, Sep. 1999.

[19] Kim B.G., Kim I.K., Lee J.K., Jang J.S., "Gigabit IDS Implementation for High Speed Intrusion Detection and Response", 8th COMSW, pp. 51-55, July 2003.

Jung-Sook Jang received the B.S degree in Computer Engineering from Kyungil University in 1991. She received her M.S and Ph. D degrees in Computer Engineering from Catholic University of Daegu in Gyeongsan, ROK, in 1995 and 2004, respectively. From 2004, she is an IT Professor at the School of Computer and Information Communications Engineering in Catholic University of Daegu(CUD), Gyeongsan, Korea.

Yong-Hee Jeon received the B.S degree in Electrical Engineering from Korea University in 1978 and the M.S and Ph. D degrees in Computer Engineering from North Carolina State University at Raleigh, NC, USA, in 1989 and 1992, respectively. From 1978 to 1985, he worked at Samsung and KOPEC(Korea Power Engineering Co.). Before joining the faculty at Catholic University of Daegu(CUD) in 1994, he worked at ETRI(Electronics and Telecommunications Research Institute) from 1992 to 1994. Currently, he is a Professor at the School of Computer and Information Communications Engineering in the CUD, Gyeongsan, Korea**.** Since January 2008, he has been a Vice-President of KIISC(Korea Institute of Information Security & Cryptology).

Jong-Soo Jang received the B.S and M.S degrees in Electronics Engineering from Kyungpook National University in 1984 and 1986, respectively. He received his Ph. D degree in Computer Engineering from Chungbuk National University in 2000. Since 1989, he has been working with ETRI, Daejeon, Korea and now is the Director of Applied Security Group.