Integrated Notification Architecture based on Overlay against DDoS Attacks on Convergence Network *

Mihui Kim, Jaewon Seo, and Kijoon Chae

Dept. of Computer Science and Engineering, Ewha Womans University, Korea
{mihui,seojw}@ewhain.net, kjchae@ewha.ac.kr

Abstract. The distributed denial of service (DDoS) attack that is one of the most threatening attacks in the wired network has been already extended in the wireless mobile network, owing to the appearance of DDoS attack tool against mobile phone. In the future, the latent threats for the converged form of DDoS attack should be resolved for the induction of successful convergence network. However, because of the current problems in defending against converged DDoS attacks on convergence network, such as the absence of a converged defense, research on cooperation architecture between defense processes is critical. In this paper, we analyze possible converged attacks, thus we propose a scalable and dynamic notification architecture based on overlay routing against DDoS attacks in consideration of the capacity of each node. A main feature of this architecture is the speedy notification of attack detection to each highest defense system in the network of the attack agents as well as in the victims. Thus it makes it possible not only to fast defense at the network of victims but also to identify attack agents. We analyzed the overhead for constructing our hierarchical overlay, simulated the transmission rate and speed of detection notification, and found a marked improvement using our defense compared to general routes.

1 Introduction

Recently, the International Telecommunication Union-Telecommunication (ITU-T) standardization sector recognized ”next generation network” (NGN) factors in the telecommunication industry, including the need to converge and optimize the operating networks and the extraordinary expansion of digital traffic. Among other research topics such as quality of service (QoS), interoperability, generalized mobility, and service capabilities and architecture, security issues are as crucial to the NGN as they are to today’s network environment. In Korea, a broadband convergence network (BcN) is being created to provide seamless and

* ”This research was supported by the MIC(Ministry of Information and Communication), Korea, under the ITRC(Information Technology Research Center) support program supervised by the IITA(Institute of Information Technology Advancement)” (IITA-2006-C1090-0603-0028)

secure, quality-guaranteed broadband multimedia service, which includes converged communication, broadcasting, and Internet access. Because of security threats and defense problems in this converged environment, security is thus a main area of research.

A converged network is characterized by factors such as host heterogeneity, dynamic topology, and scalability, and services that are provided should consider these characteristics. Although each network has existing security systems, they are insufficient to defend against converged attacks on the nodes of other networks, such as a short message service (SMS) Flooder attack. This was the first DDoS attack tool on computers in a wired network directed at mobile phones. The attack commanded all infected Microsoft Outlook software to send SMS messages to a certain victim's mobile phone, to inundate it. In a converged attack, the victims and the attack agents are located in different types of networks. Because of the power of the converged attack and the damage it could cause, the converged DDoS attack may be the most threatening of the various attacks in a converged network, that is in a ubiquitous environment. In addition, because of the open network structure of ubiquitous environments, it is easy to access the communication network, raising the imminent possibility of hacking and the dissemination of the virus. In the case of a converged attack, the defense systems on each network should collaborate to provide a fast defense. Therefore, a systematic integrated defense system is needed, but until now has been lacking because of the difficulty in gathering information and distributing it in a heterogeneous environment [1].

In this paper, we design an overlay structure for notification of converged DDoS attacks on converged networks. Most defenses against DDoS attack consists of detection, identification of attack agents, and filtering of attack traffic. However, our overlay structure is mainly used for notification of the detection of an attack. Both defense systems in the networks of victims and attack agents are notified, making possible not only fast defense in the network of victims but also the identification of attack agents. This overlay has hierarchical structure like the hierarchy of the most networks, such as wired network, NEMO (NEtwork MObility) network, and hierarchical sensor networks. The each overlay of networks is connected through the overlay nodes with multiple interfaces, for example, Ethernet and wireless LAN interfaces. Also, each overlay is composed in consideration of the capacity of the each node. This structure pursues the following design goals and we will confirm the performance by simulation and analytical results.

- **Speedy notification of attack detection** to each highest defense system in the network of attack agents, as well as victims.
- **Scalable and dynamic defense structure** of overlay in consideration of the capacity of each node

This paper is divided into five sections. In Section 2, we explain the threats of DDoS attacks on converged networks. We introduce in Section 3 our integrated notification architecture. And next, we evaluate our mechanism in various views, and explain the analysis of simulation results. Finally, a brief conclusion is presented.

2 Threats of DDoS attacks on Converged Networks

Convergence could be considered from three viewpoints: user services convergence, device convergence and network convergence. Among them, network convergence implies consolidation of the network to provide different user services, with telecom-grade quality of service, to several access types with an emphasis on operator cost efficiency. In this paper, we mainly consider the network convergence. The characteristics of converged network are as follows, and the converged network services should consider these characteristics.

- **Host heterogeneity** Nodes may vary widely in their capacities in terms of CPU power, memory, or network bandwidth.
- **Dynamic topology** Nodes may join and leave to a network at any time by mobility or by node redeployment. The system must be able to efficiently maintain a dynamic topology.
- **Scalability** The system must be able to scale to very large nodes in converged networks.
- **Convergence** Results of management service can be properly linked and merged.

In future ubiquitous environments, the following converged DDoS attacks are likely. We therefore need to design integrated defense service against these potential converged attacks.

(1) Wired network → Mobile network

For example, SMS Flooder is a DDoS attack tool against mobile telephones that has already emerged in wired networks. Because most mobile devices have extremely limited functionalities and bandwidth, a host with a powerful capacity in the wired network could easily break down the mobile network.

(2) Mobile network → Wired network

Most mobile networks are interconnected with a wired network, to allow the connection of distant mobile nodes or to provide mobile nodes with the various Internet services in a wired network. Mobile nodes, for example, a mobile phone using a RFID reader, can severely request these connections to the servers in the wired network, thus threatening the availability of servers.

(3) Sensor network → Mobile network

Numerous technologies exist for mobility support, such as the Mobile Internet protocol (MIP), code division multiple access (CDMA), International Mobile Telecommunications-2000 (IMT-2000), and so on. Network mobility has been realized among these after the foundation of the Network Mobility (NEMO) Working Group (WG) in the IETF. This WG is concerned with managing the mobility of an entire network that changes, as a unit, its point of attachment to the Internet. NEMOs can include a sensor network, for example, a vehicle that includes sensors for its control. In this case, compromised sensors in a NEMO can generate a great deal of sensing information that will congest the NEMO.

(4) Mobile network → Sensor network

Mobile routers or nodes performing as a mobile sink are infected with virus, then can request the sensing information in a sensor network, pretending other mobile sinks. In this case, the flood of request traffic can affect all of the sensor nodes, aggregator nodes, and sink nodes in the sensor network.

(5) Wired network → Sensor network
Static nodes in a wired network can severely request the sensing information to sinks in a sensor network to induce tremendous traffic from sensors.

(6) Sensor network → Wired network
Compromised sensors in the sensor network can transmit the sensing information to the server in the wired network that manages the sensor network, creating sudden traffic that influences the server or the wired network connected to the server.

3 Notification Mechanism using Overlay

We introduce integrated notification architecture against DDoS attack on converged network using overlay as shown in the figure 1, in order to fast notify the attack detection to both highest defense systems in the network of victims and attack agents, through detouring victims. In figure 1, three overlays are connected through the connection of overlay nodes, and we assume the highest defense system exists at the highest overlay. However, our defense can apply to networks that are different from that of figure 1 if the overlay nodes know the location and overlay level of the defense systems. In the converged network, each hierarchical overlay networks are interconnected by the overlay nodes with multiple interfaces. We also assume secure communication between the highest defense systems and the overlay nodes. We will explain our defense overlay architecture in detail below.

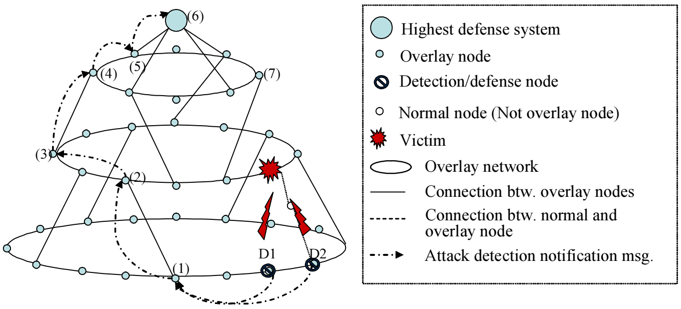

(6)
(5)
(4)
(7)
(3)
(2)
(1)
D1
D2
Highest defense system
Overlay node
Detection/defense node
Normal node (Not overlay node)
Victim
Overlay network
Connection btw. overlay nodes
Connection btw. normal and overlay node
Attack detection notification msg.

Fig. 1. Basic architecture for our notification

3.1 Chord Overlay Routing

Our defense architecture uses chord overlay routing to transmit the attack detection message and detour normal traffic, before excluding attack agents. The *chord* *protocol* is a distributed lookup protocol that efficiently locates the node that stores a particular data item. In the N-node chord system, each node maintains information only about O(log$N$) nodes, and resolves all lookups via O(log$N$) messages to other nodes. The chord maintains its routing information as nodes join and leave the system. A high probability exists that each event will result in no more than O(log^2N) messages. The chord protocol resolves the inability of previous methods to scale to a large number of nodes, and is referenced in more than 1000 papers using overlay routing in various fields.

In chord, each node is assigned a numerical ID via a hash function in the range [0, 2^m-1] for some predetermined value of m. The nodes in the overlay are ordered by these identifiers. The ordering is cyclic (i.e., wraps around) and can be viewed conceptually as a circle, where the next node in the ordering is the next node along the circle in the clockwise direction. Each overlay node maintains a table that stores the identities of other overlay nodes. The i^{th} entry in the table is the node whose identifier equals or, in relation to all other nodes in the overlay, most immediately follows x+2^{i-1} (mod 2^m). When the overlay node receives a packet destined for ID y, it forwards the packet to the overlay node in its table (called a finger table) with the ID that precedes it by the smallest amount.

As other overlay routing applications, the chord protocol has multicasting [2] or attack defense [3,4]. Secure overlay services (SOS) architecture using chord overlay [3] was proposed to proactively prevent DDoS attacks. SOS architecture is geared toward supporting emergency services or similar types of communication and introduces randomness and anonymity into the forwarding architecture, making it difficult for an attacker to target nodes along the path to a specific SOS-protected destination. HOURS [4] using hierarchical overlays achieved DoS resilience in an open service hierarchy, such as a domain name server (DNS), lightweight directory access protocol (LDAP), or public key infrastructure (PKI). However, the former is for the protection of a specific server against a DDoS attack and the latter is for DDoS defense between servers with the specific service hierarchy; thus, their goals are different from our goal, which is the transmission protection of control and normal traffic in converged DDoS attacks.

3.2 Hierarchical Overlay Construction

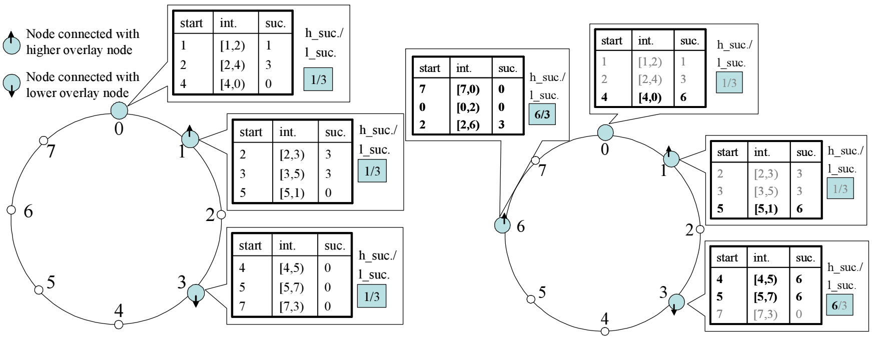
Our defense overlay is hierarchically constructed according to the capacity and connections of the nodes. Two methods exist of joining the overlay network, one set up by the operator and the other by messages. The former is applied at the beginning of the network setup, while the chord overlay construction method is used after the overlay level and capacity are configured. The latter redeploys newly joined nodes or supporting mobile nodes in the dynamic topology, with the following ***join inquiry message (JIM)*** and ***join response message (JRepM)***. We will explain the latter steps in detail.

A newly joining node n_{new} first sends the *JIM*, including the node's capacity, to neighbor nodes. Neighbor nodes are the upper or lower nodes directly connected to the n_{new}, or in the Ethernet case, the nodes in the broadcast domain.

The overlay nodes n_is receiving the *JIM* send *JRepM*s, including their capacity ($Capacity_i$) and overlay Level ($Level_i$). The newly joining node n_{new} waits a specified amount of time for the *JRepM*s, then determines its own overlay level with reference to $Capacity_i$s and $Level_i$s according to table 1, and sends a ***join request message (JReqM)*** to an overlay node in that overlay level. If no *JRepM*s is received in the specified time period, the node n_{new} sends a *JReqM* directly to the highest defense system.

The join process through the *JReqM* is based on the chord method, but the *JRepM* also includes the connection information (to high, low, and other networks), and if a direct connection to other overlay nodes exists, their overlay level joins information. In the join process, joining overlay nodes should update the information of the upper/lower/other interface successor node, if necessary, so that information can be used in the attack detection notification. The information stored at each overlay node contains the predecessor in the overlay network (used for the join process), the routing table (called the finger table), the high/low_successor directly connected to the higher and lower layer, and the otherif_succcessor directly connected to other type networks. The high/low/otherif_succcessor is the first node directly connected to the higher/lower layer/other network in a clockwise direction in the ring.

The modified join process sets up the predecessor, finger table, and high/low/otherif_successor at node n_{new}, and then updates their information at previously joined overlay nodes, if necessary. The configuration method for the high/low/otherif_successor is as follows. If the already joined overlay nodes n_i receive the *JReqM*, they compare their *high/low/otherif_successor*$_i$, and update themselves with those in the *JReqM* when *high_successor*$_i$ $>$ *new* $>$ *i, low_successor*$_i$ $>$ *new* $>$ *i, or otherif_successor*$_i$ $>$ *new* $>$ *i.* Figure 2 shows an example of an overlay and finger table after the joining of node 6. In this example, the *high_successor*$_3$ of node 3 and *otherif_successors* are updated. In addition, for a more practical overlay construction, the modified chord can be used to reduce routing latency if IPv6 is used [7].


Node connected with higher overlay node
Node connected with lower overlay node
0
1
2
3
4
5
6
7
h_suc./ l_suc.
1/3
6/3

start	int.	suc.
1	[1,2)	1
2	[2,4)	3
4	[4,0)	0

start	int.	suc.
2	[2,3)	3
3	[3,5)	3
5	[5,1)	0

start	int.	suc.
4	[4,5)	0
5	[5,7)	0
7	[7,3)	0

(a) Example of overlay with node 0,1, and 3(m=3)

start	int.	suc.
7	**[7,0)**	**0**
0	**[0,2)**	**0**
2	**[2,6)**	**3**

start	int.	suc.
1	[1,2)	1
2	[2,4)	3
4	**[4,0)**	**6**

start	int.	suc.
2	[2,3)	3
3	[3,5)	3
5	**[5,1)**	**6**

start	int.	suc.
4	**[4,5)**	**6**
5	**[5,7)**	**6**
7	[7,3)	0

(b) Finger tables after node 6 joins in black and unchanged in gray

Fig. 2. Example of overlay and finger table after node 6 joins

Table 1. Level decision method of a newly joining node

$if(Capacity_i \leq Capacity_{new} < Capacity_{(i+1)})$	$(Level_{new} = Level_i)$
$elseif(Capacity_1 \geq Capacity_{new})$	$(Level_{new} = Level_1)$
$elseif(Capacity_K \leq Capacity_{new})$	$(Level_{new} = Level_K)$

- $n_i (1 \leq i \leq K$, K: Number of nodes sending $JRepM)$
- $Capacity_i$: Capacity of node n_i (capacities in increasing order, thus $Capacity_i \leq Capacity_{(i+1)})$
- $Level_i$: Overlay level of node n_i
- $Capacity_{new}$: Capacity of a newly joining node n_{new}
- $Level_{new}$: Determined level of a newly joining nod n_{new}

3.3 Notification of Attack Detection

In our defense structure, we assume that existing distributed detection methods are used. For example, there are a monitoring method for IP address or the change rate of IP/MAC address using the network configuration information at the middle nodes[5], a data mining method[6], and so on. Thus detection mechanism is beyond the research scope of our defense structure.

If overlay nodes detect a DDoS attack, they send an ***attack detection message (ADM)*** to the highest defense system through hierarchical overlays, that is, to its high_successor using the finger table. To defend against and identify attack agents, the *ADM* includes detection node information (IP address and overlay level), victim information (IP address and overlay level, if it exists), the connection relationship of the detection node and the victim, and information about the neighbors of the detection nodes (connection information of neighbors). The high_successor receiving the *ADM* also sends its high_successor, and finally the highest defense node receives the *ADM*, after repeating this transmission through the hierarchical overlay. In the example shown in Figure 1, after overlay nodes D1 and D2 detect a victim, they send the *ADM* through (1)-(5), and finally the *ADM* arrives at the highest defense node (6).

In the converged network, hierarchical overlays such as depicted in Figure 1 are constructed for each network, and are connected with each other through the overlay node with multiple interfaces. Each overlay node manages successors that connect to other networks in the finger table. If the converged attack is detected, the attack detection is relayed to the highest defense system (node (8) in Figure 3) in the network of the attack agents as well as in its own network (node (2)). The route (node (1)-(2)) of notification in the network of detection node D follows the pattern described in the previous paragraph. The network of the attack agents is notified; first, the detection node sends the *ADM* to successors connecting to the network in its overlay layer (node (3)-(5)), then the *ADM* is routed through the hierarchical overlay (node (6)-(8)). The notification to the highest defense system in the network of the attack agents provides the information for follow-up measures against the attack agents. The route through this hierarchical overlay makes it possible to randomize the notification route for all detection nodes, in comparison to a direct route between each highest defense system, which can be a point of failure or attack.

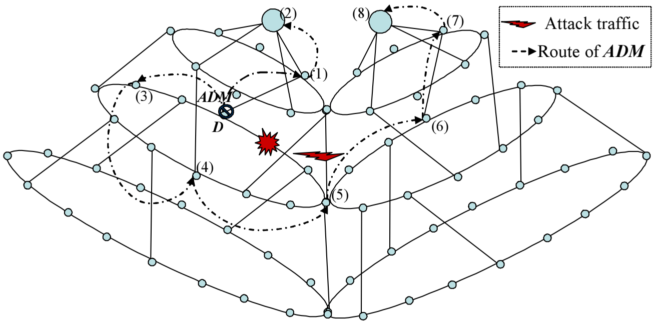


Fig. 3. Attack detection notification in the case of converged attack

4 Evaluation

In this chapter, we attempt to provide an analysis of the advantages and usefulness of our defense architecture. At first, we analyze the construction overhead of hierarchical overlay relative to only one big overlay, and we simulate the detection notification speed in converged DDoS attack on converged network with GloMoSim that provides a scalable simulation environment for wireless and wired network systems[8].

4.1 Overhead of Overlay Construction

Table 2. Decision method of defense nodes

Construction of one overlay
$\geq$ Construction of β overlays with the different number of nodes
$\geq$ Construction of β overlays with the same number of nodes,
$N \cdot logN \geq \sum_{i=1}^{\beta} \alpha_i \cdot log\alpha_i \geq \beta \cdot N/\beta \cdot log(N/\beta)$

We assume that our defense overlay is hierarchically constructed based on node capacity. To provide scalability or heterogeneity, one of the design issues in a converged network, the defense architecture should support a variety of nodes, making the construction of several overlays profitable. Moreover, a small overlay can be favorable for nodes with low capacity, such as the aggregators on the sensor network. Our defense overlay is based on the construction method of chord, thus O($\log^2 N$) message transmission is required for a node join/leave in N-size overlay network, and this can be reduced to O($\log N$) with practical optimization[3]. The construction overhead of our hierarchical overlays is smaller than for the construction of one overlay, and the construction overhead of overlays with the same number of nodes is smaller than that of overlays with a different number of nodes, as shown in table 2. The bigger the N in an N-node network is, the larger the overhead difference is, as shown in figure 4. In figure 4, the hierarchical overlay is made with three overlays; for example, a hierarchical overlay (1:10:100) in a 1000-node network is composed of an overlay with 10 nodes, an overlay with 100 nodes, and an overlay with 890 nodes.

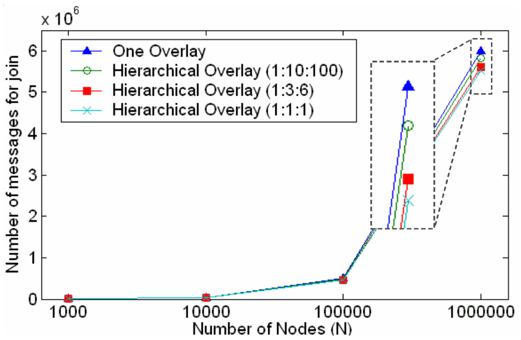


Fig. 4. Comparison for construction overhead

4.2 Simulation Results

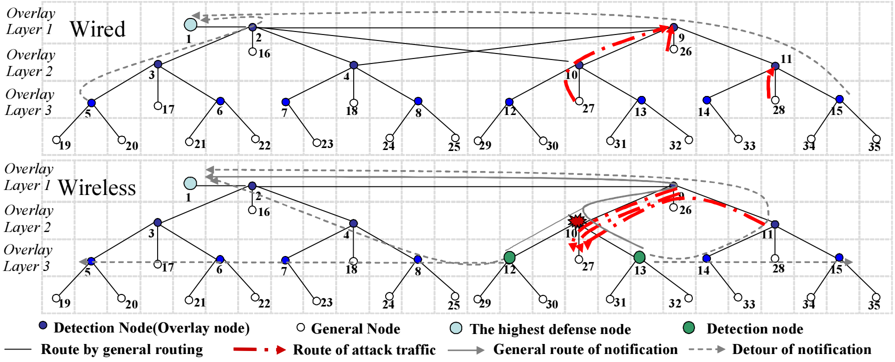


Fig. 5. Simulation network for converged network

We configured the converged network as in Figure 5 to analyze the influence on the converged attack. In figure 5, we depict the wired and wireless networks differently to clearly differentiate them, but they share the same area, and wired nodes 2, 3, 5, 9, 11, and 15 are the same as the wireless nodes with the same respective numbers. We mounted the DDoS attack from the wired node 26, 27 and 27 to wireless node 27, and attack traffic is generated at 1-ms intervals. If overlay nodes detected the converged DDoS attack, they sent five ADMs at 1-s intervals to the highest defense nodes n1 of the networks of both victims and attack agents, through overlay routing.

In results, general routes incur the low transmission rate and long delay of notification to the highest defense system (Wireless, Wl_n1) in comparison with overlay routes like table 3, because the general routes pass via victims. Moreover, the overlay route provides the fast and exact notification to highest defense system (Wired node, Wd_n1) in wired network where attack agents exist, to take immediate follow-up measure such as the identification of attack agents.

Table 3. Key re-distribution message

Node ID	Transmission rate (pkts or %)			Transmission time (sec)		
	General routing	Overlay routing		General routing	Overlay routing	
		Wl_n_1	Wd_n_1		Wl_n_1	Wd_n_1
12	1	5	5	0.436562669	0.019297497	0.037087675
13	0	1	5	-	1.219606000	0.025713102
	10%	60%	100%	0.436562669	0.019297497	0.025713102

5 Conclusion

In this paper, we proposed an integrated notification architecture using hierarchical overlay in consideration of node capacity, in order to interconnect defense systems on each network, and guarantee the speedy notification for attack detection through detour victims. It is especially important to defense possible converged attacks in the future. We constructed hierarchically the overlay in due consideration of the various capacities of nodes and lots of nodes on converged environment, and we extended the chord overlay routing to interconnect overlay layers and hierarchical overlays on different networks. The hierarchical overlays can decrease the overhead for construction in comparison with the construction of a big overlay. In simulation results on converged environment, we gained the fast and high notification rate for the attack detection. Moreover, our overlay route could notify the fast and exact attack detection to highest defense system where attack agents exist, to take immediate follow-up measure.

References

1. Y. Won, "BcN security Issues," Proc of Korea Internet Conference (KRNET), 2006.
2. Z. Zhang, S. Chen, Y. Ling, R. Chow, "Capacity-Aware Multicast Algorithms on Heterogeneous Overlay Networks," IEEE Transactions on Parallel and Distributed Systems, vol.17, no.2, pp.135-147, February 2006.
3. A. Keromytis, V. Misra, D. Rubenstein, "SOS: An Architecture for Mitigating DDoS Attacks," IEEE JSAC, vol.22, no.1, January 2004.
4. H. Yang, H. Luo, Y. Yang, S. Lu, L. Zhang, "HOURS: Achieving DoS Resilience in an Open Service Hierarchy," Proc. of DSN, pp.83-92, June 2004.
5. M. Kim, K. Chae, "Detection and Identification Mechanism against Spoofed Traffic Using Distributed Agents," Proc. of ICCSA, LNCS 3043, pp.673-682, May 2004.
6. M. Kim, H. Na, K. Chae, H. Bang, J. Na, "A Combined Data Mining Approach for DDoS Attack Detection," Proc. of ICOIN, LNCS 3090, pp.943-950, February 2004.
7. J. Xiong, Y. Zhang, P. Hong, J. Li, L. Guo, "Reduce Chord Routing Latency Issue in the Context of IPv6," IEEE COMM. LETTERS, vol.10, no.1, January 2006.
8. GloMoSim, http://pcl.cs.ucla.edu/projects/glomosim/