4-3 Grid Communication Library Allowing for Dynamic Firewall Control

HASEGAWA Ichiro, BABA Ken-ichi, and SHIMOJO Shinji

Current Grid technologies tend not to consider firewall system properly, and as a result cause the decline in the security of Grid-sites on the wide area open network in practical use. This paper discusses the dynamic firewall control working with the Grid communication library to connect each resource on the Grid safely and flexibly. It shows a reduction of an administration load.

Keywords
Dynamic firewall control, Grid communication library, Access control, Administrative cost

1 Introduction

In an environment in which two or more organizations provide computational resources (such as CPUs and storage), it is difficult to centralize administration of all resources. In particular, as the number of people accessing the environment increases, more resources need to be added, deleted, and transferred, which makes it impossible for a small number of administrators to provide administration by manual operation. Current technology requires such manual operation by administrators when adding or deleting resources. This poses a large problem when constructing Grid environments across two or more organizations. It would therefore be extremely significant if we could develop a security (i.e., access-control) implementation method that enables users to add or delete resources based on user permission while ensuring that the added resources were inaccessible to the public.

This paper first discusses the problems related to the firewall configuration in Grid technology, and then in Section **3** proposes a method for dynamic modification of the firewall configuration. The proposed method controls the firewall for each transaction and restricts the IP addresses and ports involved in the connection to the nodes, allowing for secure communication between nodes. Section **4** shows how the proposed method ensures a reduced administration load in terms of the problematic firewall configuration.

2 Dynamic firewall configuration mechanism

2.1 Conventional technology

Grid technology is used to connect resources across different organizations. In current attacks on systems, two or more nodes connected by the Grid tend to be attacked in a series once one of the nodes allows unauthorized access. This suggests that damage in Grid systems tends to expand, allowing these systems to become springboards for cyberterrorism or to serve as sites for illegal file sharing. To prevent unauthorized access at each node, appropriate firewall management is essential. However, it is difficult to maintain appropriate rules for the firewall configuration at each node due to three specific characteristics of Grid technology, as follows.

(1) Certain applications dynamically determine the ports for communication with

external nodes when executing a job.
(2) The network configuration of a virtual organization includes many interconnected nodes, and it is not guaranteed that the configuration will always remain the same.
(3) It is impossible to predict at which point during job execution communication between the nodes actually takes place.

In other words, current Grid technology does not take firewall systems sufficiently into consideration, tending to be configured for permanent connection to the resources in the network even from unnecessary ports. This leads to poor security, which in turn may facilitate unauthorized node access from external networks.

One of the conventional techniques for more secure connections establishes VPN for resource sharing. However, establishment of VPN requires highly skillful configuration of the network layer. This method is also inflexible when connecting many nodes. With the aim of providing an environment for the flexible sharing of resources among many nodes—without demanding advanced network skills of users or system administrators—this study is designed to address these problems in the application layer.

2.2 Requirements of firewall configuration in Grid technology

When constructing an environment for resource sharing among many nodes while maintaining security at these nodes, resource providers shall uphold the following requirements relating to the firewall configuration:
(i) Minimal exposure of the resources to open networks
(ii) Establishment of the necessary connections for resource sharing among nodes

In particular, when sharing resources involving ad-hoc external network connections, as with sensor devices, it is difficult to establish the appropriate firewall configuration at each node every time the connection is established or cut, due to administrative costs. A technique is required that will provide a minimum of on-demand permission within the firewall configuration in order to allow resource sharing via external access, and that will implement resource sharing without requiring administrators to take the presence of the firewall continually into account within the virtual organization.

3 Proposed method

To change the firewall configuration according to each communication event occurring between nodes, the opportunity to change the firewall rules is provided at each transaction—this feature is thus not limited to long-term units (sign-on or job events, for example).

To implement firewall control for each transaction, we have proposed a method that applies an extension function for the accurate detection of the transaction as resources are shared with the Grid middleware communication library. The proposed method does not only detect the start of each communication between nodes but also detects the IP address and port of the remote site. Here, the HTTP protocol is used to transmit to the remote site the transaction information required to change the firewall configuration.

Figure 3 illustrates the proposed method. The following outlines the series of processes performed by the Grid middleware in a single transaction. Specifically, the Grid middleware:
(1) Collects and stores the transaction information, including the IP address and the port number of the local site, immediately before the transaction, and then transmits this information to the remote site in the form of request messages to change the firewall configuration at the remote site
(2) Transmits request messages incorporating the transaction information to the remote site using the HTTP protocol
(3) Provides user authentication at the remote site
(4) Changes the firewall configuration based on the transaction information included in the request messages received at the remote site

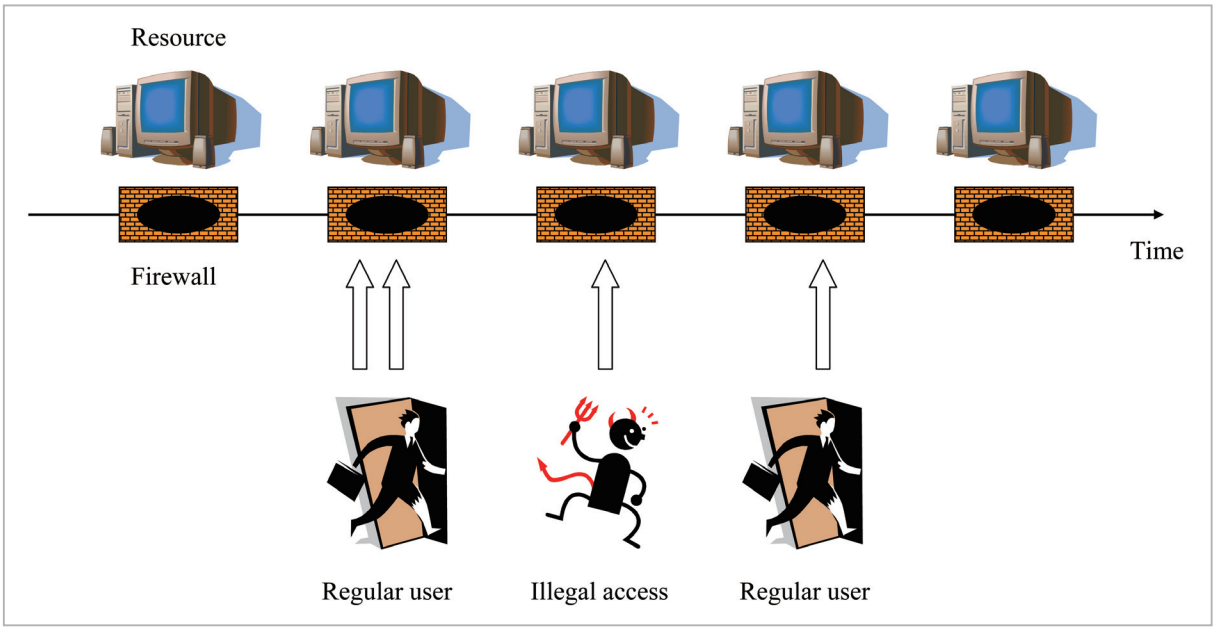


Fig.1 *Firewall configuration with existing Grid technology*

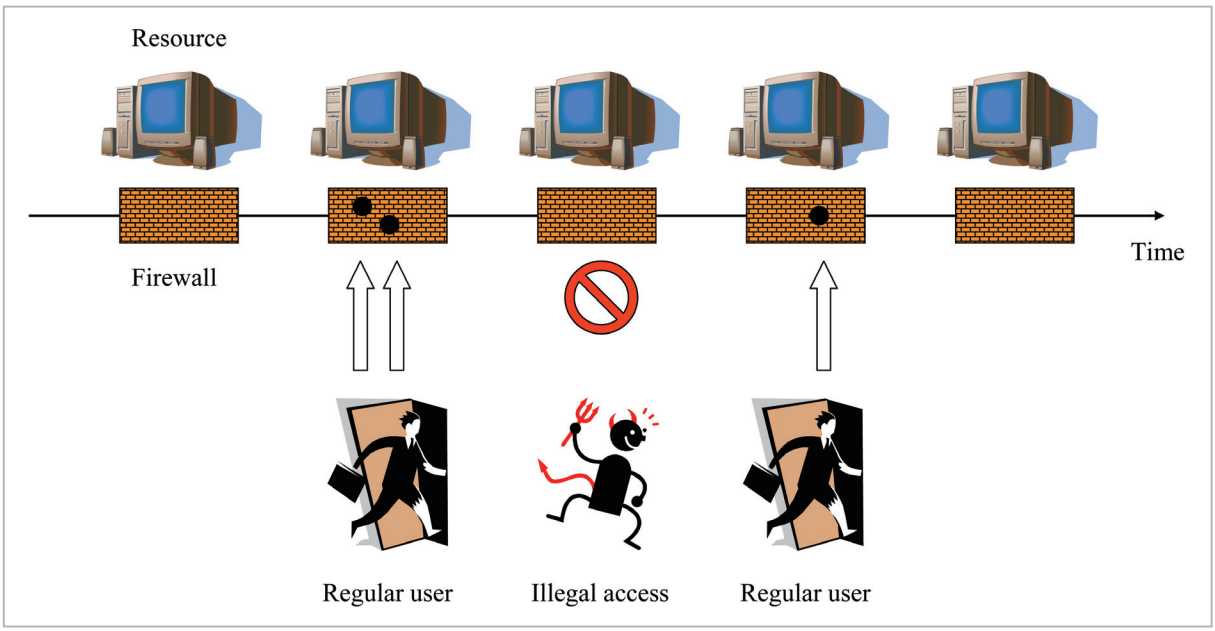


Fig.2 *Firewall control for each transaction*

(5) Establishes connection from the local site to the remote site and performs the originally intended I/O processes

Directly after the end of the transaction, the Grid middleware extracts the information stored in (1) above, performs operations (2) through (4), and then restores the firewall configuration of the remote site.

Figure 4 shows the configuration of a prototype system based on the proposed method. The firewall control communication mechanism features a Grid API, a firewall-control transmission function, and a firewall-control communication receiving function. The Grid API is designed to operate the proposed system simultaneously with the Grid system (using the Globus Toolkit), which calls the API. The firewall-control communication transmission function is called when the Grid system connects to another site. This function

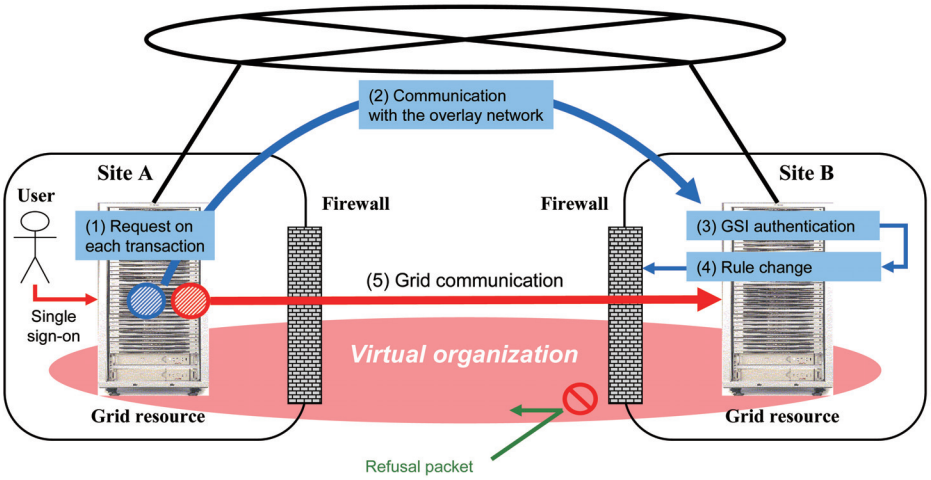


Fig.3 *Firewall control by Grid middleware*

establishes a connection to the developed software installed at the remote site and directs firewall control at this remote site. The firewall-control communication receiving function is called by the developed software installed at the remote site and calls the firewall control mechanism to control the firewall of the local site, such that the Grid system of the remote site can connect to the local Grid system. The firewall control mechanism is called by the firewall-control communication mechanism and controls the firewall of the local site. We have also developed a system of evaluation using a GUI that displays the status and allows for the configuration of these mechanisms.

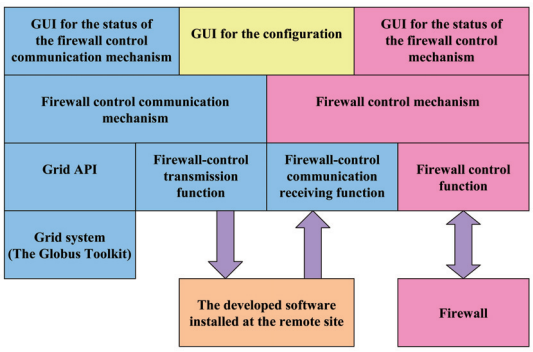


Fig.4 *Configuration of firewall control system*

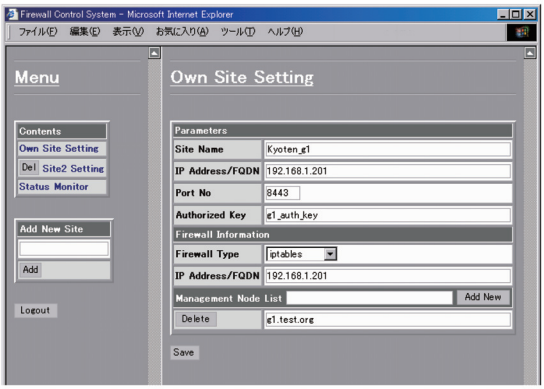


Fig.5 *GUI for configuration*

4 Evaluation

The prototype system based on the proposed method can dynamically modify the firewall configuration of the remote site, while restricting the ports, addresses, and time required for communication between the nodes according to requests from the local site.

Figure 6 illustrates transmission and receipt of the firewall-control request messages when the "globusrun" command included in the Globus Toolkit is executed. The request messages for connection and disconnection are exchanged between the host that has executed the globusrun command and the host that is executing the gatekeeper command; this changes the firewall configuration

dynamically at each host according to the requests. Sub-figures 1–4 show the user authentication, and Sub-figures 5–6 show user job transfer. After the job is performed on the gatekeeper side, Sub-figures 7–10 show transference of the results of the job execution.

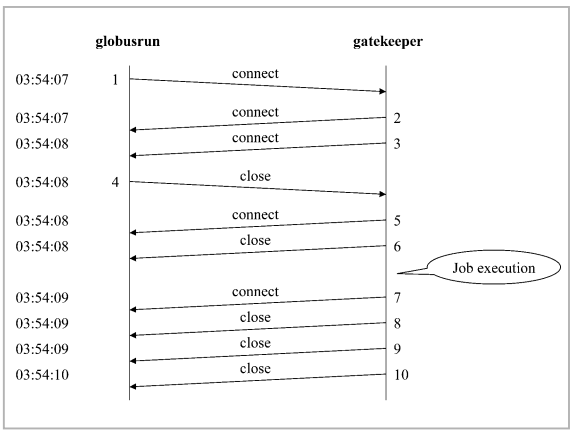


Fig.6 *Firewall-control request messages when executing globusrun command*

Under the proposed method, the Grid middleware dynamically performs a series of processes for firewall control, enabling it to set a minimum configuration for the firewall of each site as needed for communication between the nodes. The system administrator does not need to be conscious of the firewall.

If the same purposes were to be served using conventional methods, the following steps would be required to maintain security.

(1) The opportunity to control the firewall is provided for each job, which is the minimum unit that an individual can control.
(2) If the hosts between which the communication will be generated cannot be determined prior to job execution, connection must be permitted for all hosts to which the job is assigned.
(3) If the ports to be used for communication between the nodes cannot be determined prior to job execution, connection must be permitted for all ports.
(4) The firewall configuration is modified for all nodes involved in job execution.
(5) The user executing the job communicates to the administrators of all resources used in the job, informs them of the job schedule, and then notifies them of the end of the job.
(6) The system administrators at each node wait for the user to notify them of the start and end of the job, and change the firewall configuration promptly upon communication.

These steps would all be required to maintain the security of the nodes. Obviously, it is extremely difficult to implement this process correctly. Job execution may also take a significant length of time, leading to the risk of compromised security among the nodes.

The proposed method can respond to a change in the configuration of resources while sparing system administrators the troublesome burden of firewall configuration; this method is thus particularly effective when sharing sensor devices.

5 Conclusions

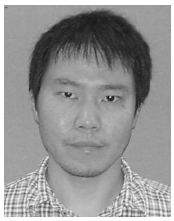
We have proposed a dynamic firewall-control technique to secure collaboration between nodes and have evaluated its effectiveness. The proposed dynamic firewall configuration mechanism applies extension functions to the Grid communication library to enable dynamic modification of the firewall configuration according to application requests. In this manner, the mechanism enables the configuration of fine access control in restricting addresses, ports, and period. The prototype system based on the proposed method demonstrated that the series of middleware processes for firewall control provides for secure collaboration between many nodes without requiring the users to be conscious of the firewall. The mechanism can facilitate data processing involving diverse resources, which many have been hesitant to undertake given the complexity involved in constructing the appropriate environment. This technique can be used in a wide range of applications, including a variety of research and development uses and numerous practical operations.

References

1 The Globus Alliance, http://www.globus.org/

2 Ian Foster, Carl Kesselman, and Steven Tuecke, "The Anatomy of the Grid", Enabling Scalable Virtual Organizations, http://www-unix.globus.org/alliance/publications/papers/anatomy.pdf (2001).

3 Von Welch: Globus Toolkit Firewall Requirements: Version 7, http://www.globus.org/toolkit/security/firewalls/Globus%20Firewall%20Requirements-7.pdf (2005).



HASEGAWA Ichiro

Expert Researcher, Osaka JGNⅡ Research Center, Collaborative Research Management Department

Grid Computing

***BABA Ken-ichi**, Dr. Eng.*

Expert Researcher, Osaka JGNⅡ Research Center (Associate Professor, Cybermedia Center, Osaka University)

Studies on Broadband Communication Network, Computer Network, and Photonic Network Systems

***SHIMOJO Shinji**, Dr. Eng.*

Expert Researcher, Osaka JGNⅡ Research Center, Collaborative Research Management Department (Professor, Cybermedia Center, Osaka University)

Focusing on a Wide Variety of Multimedia Applications, Peer-to-peer Communication Networks, Ubiquitous Network Systems, and Grid Technologies