Enhancing Security Measures by Tunnelling Protocol in Distributed Grid Network

Victor Jose M [#], V.Seenivasagam[*]
#Assistant Professor in CSE Dept, #Noorul Islam University, # Kumaracoil, Tamilnadu, India,
** Professor in CSE Dept -*National Engineering College, *Kovilpatti, Tamilnadu, India*

Abstract

Grid is a distributed computing architecture that integrates a large number of data and computing resources into a single virtual data management system. A Computational Grid is a natural extension of the former cluster computer where large computing tasks have to be computed at distributed computing resources. A safe registration and communication is essential in Computational Grid networks. This paper reports a secure tunnelling protocol which enhances the quality of Point-to-Point Tunnelling Protocol (PPTP), Layer Two Tunnelling Protocol (L2TP) and Internet Security Protocol (IPSec) in a framework. The proposed model has equipped with Data Encryption Standard (DES) as an encryption algorithm. The new packet offers a secure communication in the grid network.

Key words: Grid computing, PPTP, L2TP, IPSec, DES

Introduction

Grid computing is a network increasingly capturing the attention of computing community. It uses clusters of personal computers, servers or other machines. They link together to tackle complex calculations. The grid computing lets companies harness their unused computing power, or processing cycles, to create a type of supercomputer.

Grid computing is an important and developing computing initiative that involves the aggregation of network connected computers to form a large-scale, distributed system for coordinated problem solving and resource sharing [1,2]. To speedup computing workload across the distributed system of computers, grid users can take advantage of enormous computational, storage, and bandwidth resources that would otherwise only be available within traditional multiprocessor supercomputers. To give an analogy, grid computing is similar to power grids, where user does not need to know anything about what stays beyond the socket. One can absorb all the power they wants according to the agreement with electrical society. A world wide attraction is given to Grid computing due to the variety of applications ranging from physics, chemistry, environment, aerospace and healthcare systems [3], [4].

The term “the Grid” was made in the mid 1990’s to denote a proposed distributed computing infrastructure for advanced science and engineering. Considerable progress has since been made on the construction of such an infrastructure but the term “Grid” has also been conflated, at least in popular perception, to embrace everything from advanced networking to artificial intelligence. The Computational Grid is a novel, evolving infrastructure that provides unified, coordinated access to computing resources such as processor cycles, storage, etc. Wide variety of systems, from small workstations to supercomputers can be linked to a grid to form a powerful virtual computing environment. Much complexities involved in managing resources of a grid are hidden from the clients to clients, providing a seamless access to computing resources. As a great advancement towards cost reduction, computational grids can be used as a replacement for supercomputers that are presently used in many computationally intensive scientific problems like genome analysis, medical imaging, computer graphics etc.

A computational grid consists of a set of resources, such as computers, networks, communication channels, servers or sensors that are tied together by a set of common services which allow the users of the resources to view the collection as a seamless computing or information environment [5]. A standard grid services include security services that support user authentication, authorization and privacy. Grid offers information services, which allow users to see what resources (hardware, software and services) are available for use. Grid networks give high level computational job submission services, which allow user submission jobs to any compute resource that the user is authorized to use and co-scheduling services, which allow multiple resources to be scheduled concurrently. Grid gives user support services, which provide users access to "trouble ticket" systems that span the resources.

Grid Security Architecture

Grid architecture defines the fundamental system components of grid computing environment, specifies the purpose and function of these components. This indicates how these components interact with one another. Grid architecture is one of the first and foremost protocol architecture, with protocols defining the basic mechanisms by which Virtual Organization (VO) users and resources negotiate, establish, manage, and exploit sharing relationships. A set of individuals and/or institutions defined by such sharing rules form what we call a VO [1]. Virtual organisations are often called grids [6]. Here, VOs are connected through a high bandwidth communication medium. A standards-based open architecture facilitates extensibility, interoperability, portability, and code sharing; standard protocols make it easy to define standard services that provide enhanced capabilities of resource sharing and co-ordination between the clients. So there are communication channels established between these virtual organisations.

Specialized Grids focused on close and routine interactions between people, instruments and information in support of widely distributed scientific research projects are often called *collaboratories* [7]. Such grid network is providing to process important and safe computational activities. So a high level safety communication is required for registration and division of jobs submitted by a user. One of the major principle should meet the safe need in grid computing is that offer the authentication solution, to guarantee to mutual verification between the subject and object. Which considering access control mechanism, visit cross-domain and visit in domain will be referred. Try one's best to guarantee but not to change existing local access control mechanism. Authentication mechanism is the foundation of the access control mechanism and each local safe tactics is built up on this foundation.

Security in grid computing is categorized into three main aspects consisting of architectural, infrastructural, and management-related issues [8]. Architecture security is concerned with information, authorization, and service security. Infrastructure security, which is the topic of interest in this paper, is related to host protection and network related issues. Here needs an important secure communication medium network for secure transmission. Trust management along with credential and monitoring issues are the components within management security.

Many security architectures in the communication have been proposed in order to offer a secure environment for grid users. But security gaps still exist when volunteering a host to a grid computing environment. In computer volunteering, the user or owner of the computing resources becomes subject to some threats which are specific to on-demand computing [9]. Such services are demanded a high level protocol with safe and secure transmission in the communication channel in a grid network. This paper discusses contents related to access control mechanism in a secure communication method.

Protocol Security Design

Grids provide protocols and services at five different layers as identified in the Grid protocol architecture [10]. A promising security mechanism is essential for communicating in network due to the importance of the jobs carried out in the grid network. This section discusses a new tunnelling protocol design for secure data transmission in grid network. There is design of a new pack associated with point-to-point tunnelling and a Layer two tunnelling mechanism by using the TCP/IP protocol. This security mechanism enhances basically for registration and division of the work submitted to the grid network.

Various password based schemes and Challenge Handshake Authentication Protocol (CHAP) can be used to authenticate users on a grid network and control access to network resources. Encrypting the data as it travels through the grid connection guards the privacy of corporate information. Tunnelling allows senders to encapsulate their data in Internet Protocol (IP) packets that hide an underlying routing and switching infrastructure of the Intranet or Virtual Private Network (VPN) from both senders and receivers. At the same time, these encapsulated packets can be protected against snooping by outsiders using encryption techniques.

Tunnels consist of two types of endpoints, either an individual computer or LAN with a security gateway. Only two combinations of these endpoints are considered in designing grid network. First, LAN-to-LAN tunnelling, a security gateway at each endpoint serves as the interface between the tunnel and the private LAN. In this case, users on either LAN can use the tunnel transparently to communicate with each other. Second, client-to-LAN tunnels is the type usually setup for a mobile user who wants to connect to the corporate LAN of a Virtual Organisation. There are different types of protocols used for creating communication channel across the grid network.

Point-to-Point Tunnelling Protocol (PPTP): Router to router connection and remote access are easily done by this protocol. PPTP is documented in Request for Comment (RFC) 2637 [11]. In PPTP, tunnel is maintained by using the connection of Transmission Control Protocol (TCP), Point-to-Point Protocol (PPP) frames for tunnelled data [12, 13] are encapsulated using advanced version of Generic Routing Encapsulation (GRE). These PPP frames can be encrypted. The port used is TCP 1723 and Internet Protocol type 47(GRE).

Layer Two Tunnelling Protocol (L2TP): In L2TP best features of PPTP and Layer 2 Forwarding (L2F) are combined together. This is used to encapsulate PPP frames to be sent over the Internet. L2TP can be used as a tunnelling protocol over the Intranet or a VPN. L2TP is documented in RFC 2661 [14]. The encapsulated PPP frames can be decrypted. The L2TP packet format is shown in Figure 1. The PPP payload is encrypted before encapsulation using Data Encryption Standards (DES) algorithm, a symmetric key algorithm before data is transferred**.** The port used for User Datagram Protocol (UDP) is 1701.

IP header	UDP header	L2TP header	PPP header	PPP payload (IP data- gram, IPX datagram)

Figure 1. L2TP Packet format

Internet Security Protocol (IPSec): Key Management IPSec uses the Internet Key Exchange (IKE) to securely establish and pass shared keys between sites [15]. Keys and security associations may also be passed. Authentication Header (AH) protocol defines methods of establishing the identity of the message originator and ensuring that the transmitted data has not been tampered with. Encapsulating Security Protocol (ESP) protocol provides the same functions as the Authentication Header protocol but additionally defines encryption methods for the data [15]. All three components are designed in modular way to incorporate new algorithms and schemas, ensuring forward compatibility as new advancements in encryption or key exchange mechanisms are made. However, IPSec defines lowest level denominators to enable at least minimal interoperability between different vendors’ implementations of an IPSec gird. For instance, all IPSec grid network must include the DES (Data Encryption Standards) encryption algorithm for data encryption [16].

Implementation

Grid network provide bulk computational needs such as forensic analysis, genomics analysis, image processing etc. The data integrity during transmission in this work is very less. With the implemented grid network, the encrypted data is wrapped with a header. That provides routing information, it allows data to traverse the shared passage, inter network to reach its endpoints to emulate a private link. For the confidentiality an encryption scheme is used at both ends should be Data Encryption Standards techniques is used to visualize the security mechanism. The main phases are discussed below.

Connection Establishment: This is the phase where a link is established between a server and a client in the grid network. The client system presents the user’s credentials such as username and password to the access server. If a valid user, a connection is established between the server and the client. The authentication is done using the CHAP’s authentication scheme. The server provides a file transfer service or a message transfer service to the client upon successful login. If the client is a new user, then registration is required for the server by providing details such as IP address, subnet mask, and default gateway. After registration, the client machine will get a username and password which will be used for further login. These details are stored in the server so that these valid users can be listed or viewed later. The connection establishment is shown in Figure 2.

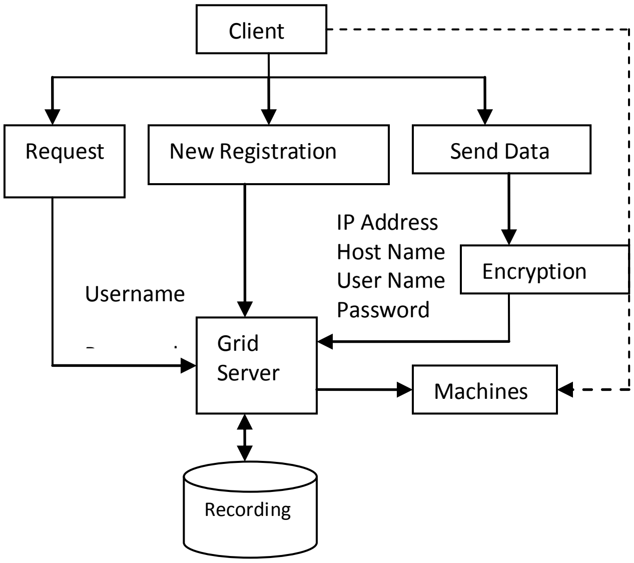

Figure 2. Request, Registration and Send data

Encryption Phase: The client can sent a file or any form of data to some other client through the tunnel server. The file may be a job from the user. The data of file can be encrypted using the Data Encryption Standard (DES), a symmetric encryption mechanism [17]. Both the client and the server use DES for encryption and decryption.

Address Specification: During this phase the server in the grid assigns a dynamic address to the client. There after data transferring is done, based on this dynamic or virtual IP address. When a server in the grid network is configured, a set or a pool of static IP addresses can be set. When the client gets connected to the virtual private network, it is assigned an IP address from this address pool. In the basic configuration, when the client sends a packet to a monitoring server, the server in the grid translates the client's IP address into some virtual or global IP address. Similarly, when an outside network sends a packet to the inside network, the user sends the packet to the virtual IP address. The server in the grid translates the virtual IP address into an inside address and sends the packet to the appropriate device on the client system in the private network.

Data Transfer Phase: When a division of job is to be sent to another system, the destination machine's IP address is specified. The data transferring takes place by L2TP protocol's tunnelling technology. When data reaches the receiver's end, it is first decrypted and then stored in the destination machine.

Client-Server Communication: The client-server communication is made possible by the use of Java's Remote Method Invocation (RMI). Java Remote Method Invocation Technology supports method calls between distributed Java objects [18]. RMI uses classical RPC-based client-server interaction, precisely remote method calls. The methods and parameters must somehow be shipped to other machine. The server must be informed to execute a method, and return value must be shipped back. The grid system network is implemented as a client-server system with a server and two or more clients.

Client: A client comes for the first time it has to register with the server through a registration form. It includes textboxes for entering the *IP Address, Host Name, User Name and Password* of the client system. These details are sent to the server and the server will calculate a message digest for the password using Secure Hash Algorithm (SHA-1) [19]. The output of this algorithm is a 160-bit binary hash value. The server stores the username and this message digest value of the password. These details are used for user authentication for later time. The server will assign a dynamic or virtual IP address to the registering client, which will be stored in the table named, *map*. Later this virtual address is used for data communication.

When the client specifies the IP address of another client to which data is to be sent, the server will look in the details stored to obtain the virtual address of the destination machine. The data is then sending to the virtual address of the destination machine. When the user wants to send a file or a job, the specified file or division of job can be sent to some other system with the specified physical IP address. The static IP address of the destination machine is specified by selecting an IP address from the list box. The user has to make a selection of whether to sent text message or file to the other system. It is provide a text area for senders and receivers. The message in the textbox is send to the server. If the user chooses to send a file, the client interface provides a file dialog to browse and select a file from the local hard disk of the client system with the help of an *open file dialog* implemented using a *File Chooser* component in Java. The user can directly specify the file path.
A grid communication tunnel is enabled between a client and a server system, through which the data can be transferred. When the client system specifies the physical IP address of the destination system, the server in the grid network will map this address with its virtual IP address. The data to be sent is encrypted using DES, and is encapsulated in an L2TP packet and is send to the server in the network. This server directs this packet to the corresponding system depending on the virtual address. On receiving a file or a job, the data packet is first un-encapsulated, and then it is decrypted. When the user wants to get a connection to the server in the grid network, he needs to raise a connection request. The user enters username and password. The username and one way hash value of the password is sent to the server in the network.

The server receives a communication request that retrieves username and hash value of the password stored in the table during the registration process. The L2TP tunnel is established between the client and server, and a session is initiated for a successful authentication. An acknowledgement message is sent by the server to the client. The two endpoints of the tunnel created on acceptance of the tunnel are the client and the server. When the user intends to send data, IP address of the destination machine can be selected from the client's machine, available in the client list.

Server: The server waits for the client's requests for getting its connected. Upon authenticated connection, the server will provide various services to the client systems. The services include calculating the one-way hash-value of the password during the registration process and store these details. Moreover, the server will assign a virtual IP address to the client system. The server also handles the request send by the client and retrieves the username and the hash value of the password stored and compares this with that send by the client. If it matches, a communication tunnel will established between the server and the client. The server also sends an acknowledgement to the client. The server lists the IP address, Host Name and login time of the valid client that gets connected in the server interface.

The idea designed in Java objects that are integrated to GridSim package for grid enriched works. GridSim is a software platform that enables users to model and simulate the characteristics of Grid resources and networks with different configurations. By using GridSim, one is able to perform repeatable experiments and studies that are not possible in a real dynamic Grid environment.

Conclusion

A grid network allows users to connect to corporate network for high computational work in a useful manner through a network. A secure communication channel is essential for such computation work after its registration. . A secure communication appears to the grid user as a private network that a communication occurs over an Intranet or a VPN. The system is user friendly, high reliability and work on heterogeneous networked computer systems. Scope of a new protocol exists at this point due to safe communication requirements. The tunnelling is one of the better solutions which offer a new design. The enhanced protocol out performed in a grid network environment with secure transmission by the use of TCP/IP protocol.

References

[1] I. Foster, C. Kesselman, and S. Tuecke, “The anatomy of the grid,enabling scalable virtual organization”, International Journal on Supercomputer Applications, vol. 15, no. 3, 2001.

[2] I. Foster, C. Kesselman, J. M. Nick, and S. Tuecke, “The physiology of the grid, an open grid services architecture for distributed systems integration” , Open Grid Service Infrastructure WG, Global Grid Forum, June 2002.

[3] Pin Hu, Lingfen Sun and Emmanuel Ifeachor, “An Approach to Structured Knowledge Representation of Service-oriented Grids”, Proceedings of UK e-Science Programme All Hands Meeting 2007

[4] Lingfen Sun and Emmanuel C. Ifeachor, The impact of grid on healthcare.

[5] Foster, Ian; Kesselman, Carl, “The Grid: Blueprint for a New Computing Infrastructure”, 2nd Edition, Elsevier, 2004.

[6] Foster, I. and C. Kesselman, eds. The Grid: Blueprint for a New Computing Infrastructure, Morgan Kaufmann publ., 1999

[7]. Agarwal, D.A., S.R. Sachs, and W.E. Johnston, The Reality of Collaboratories. Computer Physics Communications, 1198. 110: p. 134-141.

[8] Anirban Chakrabarti, Anish Damodaran, Shubhashis Sengupta, "Grid Computing Security: A Taxonomy," IEEE Security and Privacy, vol. 6, no. 1, pp. 44-51, 2008.

[9] David P. Anderson, Carl Christensen, Bruce Allen, "Designing a Runtime System for Volunteer Computing," ACM/IEEE SC 2006 Conference (SC'06), pp. 33, 2006

[10] I.Foster, C. Kesselman, C. Lee, R. Lindell, K. Nahrstedt, A. Roy., “A Distributed Resource Management Architecture that Supports Advance Reservations and Co-Allocation”, Intl Workshop on Quality of Service, 1999.

[11] K. Hamzeh, G. Pall, W. Verthein, J. Taarud, W. Little, G. Zorn, “RFC2637: Point-to-Point Tunneling Protocol”, RFC Editor, July 1999.

[12] D. Farinacci, T. Li, S. Hanks, D. Meyer, P. Traina, “RFC2784: Generic Routing Encapsulation (GRE)”, RFC Editor, March 2000

[13] G. Dommety, “RFC2890: Key and Sequence Number Extensions to GRE”, RFC Editor, September 2000.

[14] Naganand Doraswamy, Dan Harkins, “IPSec: The New Security Standard for the Internet, Intranets, and Virtual Private Networks”, Prentice Hall PTR, October 1999.

[15] S. Kent, R. Atkinson, “RFC2406: IP Encapsulating Security Payload (ESP)”, RFC Editor, Nov 1998.

[16] Srivaths Ravi, Anand Raghunathan, Nachiketh Potlapally, “Special session on security on SoC: Securing wireless data: system architecture challenges”, Proceedings System Synthesis, ACM Press, Oct 2002.

[17] C. Madson, N. Doraswamy, RFC2405: The ESP DES-CBC Cipher Algorithm with Explicit IV, RFC Editor, Nov 1998.

[18] Rüdiger Kapitza, Michael Kirstein, Holger Schmidt, Franz J. Hauck, “FORMI: an RMI extension for adaptive applications”, ARM '05, ACM Press, November 2005.

[19] Mao-Yin Wang, Chih-Pin Su, Chih-Tsun Huang, Cheng-Wen Wu, “Exploration for advanced SoC design: An HMAC processor with integrated SHA-1 and MD5 algorithms”, Proceedings of ASP-DAC '04, January 2004.