IGI PUBLISHING ITJ 5100
701 E. Chocolate Avenue, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.igi-global.com

This paper appears in the publication, International Journal of Grid and High Performance Computing,Volume 1, Issue 3
edited by **Emmanuel Udoh** and **Frank Zhigang Wang** **© 2009, IGI Global**

A Security Prioritized Computational Grid Scheduling Model: An Analysis

Rekha Kashyap, Jawaharlal Nehru University, India
Deo Prakash Vidyarthi, Jawaharlal Nehru University, India

ABSTRACT

Grid supports heterogeneities of resources in terms of security and computational power. Applications with stringent security requirement introduce challenging concerns when executed on the grid resources. Though grid scheduler considers the computational heterogeneity while making scheduling decisions, little is done to address their security heterogeneity. This work proposes a security aware computational grid scheduling model, which schedules the tasks taking into account both kinds of heterogeneities. The approach is known as Security Prioritized MinMin (SPMinMin). Comparing it with one of the widely used grid scheduling algorithm MinMin (secured) shows that SPMinMin performs better and sometimes behaves similar to MinMin under all possible situations in terms of makespan and system utilization. [Article copies are available for purchase from InfoSci-on-Demand.com]

Keywords: *Cipher Suite; Makespan; SSL; Secured Grid Scheduling; Site Utilization; TCP/IP; TLS*

INTRODUCTION

The grid, introduced in 1998, is an emerging field for compute-intensive tasks (Foster, Kesselman, Tsudik and Tuecke, 1998; Foster, Kesselman and Tuecke, 2001). A computational grid is a collection of geographically dispersed heterogeneous computing resources, providing a large virtual computing system to users. Idle computers across the globe can be utilized for such computations. Such an arrangement ultimately produces the power of expensive supercomputers which otherwise would have been impossible.

There are four factors behind the growing interest in grid computing: the evolution of key standards such as TCP/IP and Ethernet in networking; the ever-increasing bandwidth on networks reaching into the gigabit range; the increasing availability of idle megaflops on networked PCs, workstations and servers; and the emergence of Web services as a logical and open choice of software computing tasks (Prabhakar, Ribbens and Bora, 2002; Naedela, 2003). Grid scheduling software considers a job composed of tasks; finds suitable processors and other critical resources on the network; distributes the tasks; monitors their progress and reschedules any tasks that fail. Finally, the grid scheduler aggregates the results of the tasks so that the job is completed.

Grid computing has extensively supported collaborated science projects on the internet. Most of these projects have stringent security requirements. To a certain extent, the security may be provided by the application itself, but more usually it should be ensured and supported by the grid environment. The dynamic and multi-institutional nature of these environments introduces challenging security issues that demand new technical approaches for solutions. Scheduling algorithms play an important role in any distributed system. In an environment where security is of concern, responsibility is delegated to the scheduler to schedule the task on the resource that can meet the security requirement of the task. Such a scheduler is referred as the security aware scheduler (Jones, 2003; Tonelloto and Yahyapour, 2006). The goal of a security aware scheduler is to meet the desired security requirements as well as providing a high level of performance metric e.g. site utilization and makespan.

The most common public key authentication protocol used in the grid today is the Transport Layer Security (TLS) (Dierks and Allen, 2007; Apostolopoulos, Peris and Debanjan, 1999) protocol that was derived from the Secure Sockets Layer (SSL) (Freier, Karlton and Kocher, 1996). Different versions of SSL/TLS provide different level of security. Different version supports various cipher suites (security algorithms) for different security services like authentication, encryption and integrity. Thus it is the job of scheduler to allocate the tasks on the resources which supports the required security version and even supports required algorithm on a particular version to satisfy the demand.

Various grid scheduling models (algorithms) have been proposed in the past, but addressing little about security-aware scheduling. In this article, the thrust is security-aware scheduling model to optimize performance characteristics such as makespan (completion time of the entire job set) and site utilization along with the security demand of the task. The model is to consider the constraints exerted by both the job and the grid environment. In the proposed model, security prioritization is incorporated in MinMin scheduling strategy, resulting in renaming the model as Security Prioritized MinMin (SPMinMin).

The next section discusses the related work done in this field. Section 3 explains the proposed grid scheduling SPMinMin model. Section 4 shows some experiments and the observations over the results. Finally, section 5 concludes the work.

RELATED WORK

Often, grids are formed with resources owned by many organizations and thus are not dedicated to specific users. There are