CoreGRID Researcher Exchange Programme (REP): **CR02 CETIC – CR27 UCO**

Investigating Sabotage Tolerance Techniques to Defeat Colluding Nodes in Desktop Grids

Syed Naqvi
syed.naqvi@cetic.be
Centre of Excellence in Information and Communication Technologies (CETIC)
Rue des Frères Wright 29/3, 6041 Charleroi, Belgium

Hosted by
Luis M. Silva
luis@dei.uc.pt
University of Coimbra
Pólo II, 3030-290 Coimbra, Portugal

1. Introduction

This report provides a summary of the activities performed during the CoreGRID sponsored research exchange programme (REP) in the Department of Informatics Engineering of the University of Coimbra, Coimbra, Portugal in June and July 2008.

2. Specific links and added value with the CoreGRID

The research exchange contributed to the general objective of the WP4 roadmap [1]. The security activity in CoreGRID runs as a horizontal integration activity related to all the research areas. In WP4 of CoreGRID, Sabotage Tolerance is a major topic of the trust and security issues that covers techniques and strategies to make Desktop Grid Middleware sabotage tolerant.

3. Description of the activities carried out during the research exchange

- Context

As grids grow in size and assume several different forms such as desktop grids made of volunteer computers, the topic of sabotage tolerance gains considerable importance. In a classical service grid, the environment is trustable in the sense that its resources and their ownership are strictly controlled. When a grid resource is malfunctioning, the grid owner has the necessary tools to fix it. Whereas in the open and un-trustable environment of the volunteer grids, some contributors may jeopardise the computations by providing bad results. Since computation provided by volunteers is unreliable, the central supervisor needs to check the validity of results, usually with simple computing replication. However simple replication falls short on preventing many forms of attack such as collusion to compromise a voting pool.

We have considered several models to represent different types of nodes: honest nodes, naïve saboteurs and colluding saboteurs. While naïve saboteurs decide to sabotage alone, colluding saboteurs have the means to contact each other and only act against the project when they are sure they can win a voting pool. In this way, they reduce the traces of their action against the system. In other words, if they know that in some voting pool they will vote against a majority of honest workers they also pretend to be honest. However, when they know that they form a majority, they attack the project, by voting together against remaining honest workers. Interestingly, in this way, they even expose honest workers as if they were malicious. Current desktop grid projects running on middleware like BOINC (Berkeley Open Infrastructure for Network Computing) [2] are unable to protect themselves from such colluding attacks.

- Work done

The post-processing analysis used in [3] is improved by simplifying statistical analysis on all voting pools to spot out malicious nodes. This statistical analysis takes place off-line, after the central supervisor receives all (or part of) client results. It runs as a post-processing operation, divided in two stages. First, nodes acting alone (naïve saboteurs) submitted wrong results are identified. This is usually simple, as they should have votes against in their voting pools. Second, the colluding nodes are identified by using the principle that malicious nodes act together (colluding saboteurs), should have won some of their voting pools against honest workers; which were not identified in the first step. The simplified algorithm is implemented in Java. Experimentations are performed with different number of voting polls with variable number of iterations.

4. Acknowledgements

This research activity was sponsored by the European funded Network of Excellence CoreGRID (Project number IST-2002-004265). I would also like to thank my scientific host Professor Luis M. Silva and his team member Filippe Araujo for valuable help and fruitful discussions.

5. References

1. CoreGRID Roadmap version 3 on Architectural Issues: Scalability, Dependability, Adaptability (D.SA.05), 15 October 2007
2. Berkeley Open Infrastructure for Network Computing (BOINC) Project – http://boinc.berkeley.edu
3. Gheorghe Cosmin Silaghi, Filipe Araujo, Luis Moura Silva, Patricio Domingues, and Alvaro E. Arenas. Defeating colluding nodes in desktop grid computing platforms. In 2nd Workshop on Desktop Grids and Volunteer Computing Systems (PCGrid 2008), Miami, Florida, USA, April 2008.