Towards Monitoring Security Aspects in Mobile Grid Computing Systems: a Survey

Abdulghani Suwan, Francois Siewe and Nasser Abwnawar
School of Computer Science and Informatics
Faculty of Technology
De Montfort University
Leicester, LE1 9BH, UK
{p02318242, FSiewe, p05110127}@dmu.ac.uk

***Abstract*— In recent years, the proliferation of mobile devices has led to the emergence of mobile grid computing, that is extending the reach of grid computing by enabling mobile devices both to contribute to and utilise grid resources. Thus, the pool of available computational and storage resources can be significantly enriched by leveraging idle capacities of mobile devices. Nevertheless, the emergence of the mobile grid gives rise to challenges, which have not hitherto been addressed thoroughly. Among those is the security threat, which arises from the multitude of mobile devices accessing grid resources and associated network connections, spanning across the globe. Accordingly, the aim of this paper is two-fold. First, it surveys prominent grid monitoring systems and attempts to identify any potential limitations with respect to the security aspect. The results of the survey indicate that existing solutions fail to address the security concerns, which arises from enabling the mobile devices interacting with the grid. To this end the second aim of the paper is to propose a monitoring system which continuously tracks the geo-location of the mobile devices accessing the grid and thereby ascertains that the location-based security policies are not violated.**

Keywords—Mobile Grid Computing, Grid Computing, Monitoring System

I. INTRODUCTION

Mobile grid computing is an emerging computing paradigm, which lies at the intersection of two research areas – namely, grid computing and mobile computing [1]. Its main concept is to extend the traditional capabilities of grids – that is, sharing of a large pool of aggregated computational and storage resources in order to address computational intensive tasks [2] – with computational capabilities of mobile devices over the network. From this perspective, mobile grid computing can be seen as an evolution of concept of grids from traditional, in-premises deployments to a distributed computer architecture, consisting of both server clusters residing in a data centre and multiple mobile devices, such as smartphones, tablets and laptops, connected to the main cluster via a wireless network.

What was regarded as impractical and impossible just a decade ago today is attracting more and more investigation both from the industry and the academia. Indeed, portable mobile devices are becoming more and powerful in terms of their CPU and memory capabilities and the speed of 5G mobile networks is approaching 1GB per second. In this light, the potential of integration of grids with mobile computing is becoming even more promising.

The inherent benefit of mobile grid computing is that it allows the users to access grid resources from a mobile device from virtually anywhere at any time, without the requirement to be sitting next to a terminal. Moreover, in mobile grid architectures, mobile devices are expected to act not just as resource consumers, accessing grid resources, but also act and as resource providers in their own right, contributing to the shared pool of available resources [3]. This latter feature may enable forming of 'ad-hoc' mobile grid compositions on the spot. In other words, it is possible to create local, short-term mobile grids at various venues and locations with an increased concentration of smart mobile devices, such as, for example, conferences and universities [1].

Along with these promising opportunities for increased computational capabilities and ubiquitous network access to computational and storage resources, come emerging challenges so as to how to manage these resulting complex environments and maintain stable quality of service (QoS). The issue of delivering promised QoS to mobile grid users is multi-faceted, and includes can be seen from several perspectives.

In the first instance, QoS depends on the networking capabilities of a mobile grid system. Mobile network bandwidth remains the main factor to guarantee smooth and undisrupted data exchange between mobile devices and grid servers. Another important concern in satisfying QoS requirements is the implementation of the resource management mechanism responsible for resource discovery and selection, job scheduling and replication, data migration and monitoring [4]. In the presence of a considerably higher number of computational nodes constituting the mobile grid system, it is important to organise how various computational tasks are split, scheduled and executed in the most efficient manner.

The last but not the least, the emergence of mobile grid computing poses new challenges as to how these distributed systems should be properly protected and secured. As opposed to traditional grid architectures, where networking is not regarded as one of the primary issues to take into account, in mobile grids the networking dimension plays a dominant role. The wireless nature of network connections introduces new threats and makes resulting mobile grid systems vulnerable to a wide range of threats such as eavesdropping, data tampering and data tracing [4]. Accordingly, novel appropriate monitoring and detection mechanisms are required in order to address these security issues and enable mobile grid systems with sufficient self-protective capabilities to maintain required QoS.

Given these considerations, in this paper we survey existing grid monitoring solutions focussing specifically on the supported security-related capabilities. Our goal in this survey is to identify potential limitations of the state-of-the-art approaches with respect to their capacity to detect potential security threats. As we will demonstrate below, the survey results suggests that existing monitoring frameworks seem to successfully address typical issues, associated with maintaining QoS (i.e., monitoring resource utilisation, application performance, job scheduling, etc.), they typically do not consider the mobile dimension and associated network security threats.

The rest of the paper is organised as follows – Section II introduces and briefly explains main factors leading to security breaches in mobile systems. It provides a statistical overview of this problem domain and aims to provide the reader with an understanding of how serious the mobile security is. Next, Section III surveys the state of the art in grid monitoring and attempts to identify existing limitations, which need to be addressed by the mobile grid research community. Section IV summarises the survey results and provides an overview of what a potential grid monitoring solution bridging identified gaps might look like.

II. MOBILE THREATS

In this section we will familiarise the reader with the pressing concern of security and data privacy in the domain of mobile computing. To do so, we provide some statistical information.

Even though it was predicted that mobile phones would be well protected against potential security-related issues when they first appeared [5], since the emergence of truly ‘smart’ phones – that is, mobile phones equipped with an operating system – the security and data privacy has been always an ever-growing concern. For example, a research by Juniper Networks Mobile Threat Center [6] conducted in 2013 indicated that the amount of malware specifically developed for mobile platforms grew immensely by 614% just in one year from March 2012 until March 2013! Another research by Arxan [7] surveyed top-100 most expensive mobile apps both for Android and IOS platforms and attempted to investigate if the surveyed apps are potentially vulnerable to various hacking attacks. The survey results are ruthless – 100% of Android and 56% of IOS apps can be potentially hacked. Same applies to freely-distributed mobile apps – 73% of widely used Android apps 53% apps running on IOS exhibit potentials breaches to be attacked by malicious software [7].

Besides security issues associated with software design and implementation, another contributing factor to the ever-growing mobile security threat is the unpredicted or inappropriate user behaviour. A recent research [8] indicates up to 69% of employees to lesser or greater extent are using mobile devices (e.g., smartphones, tablets, and laptops) to connect to their work environments remotely over the network. Indeed, the role of mobile devices in running everyday business tasks is rapidly increasing. It was predicted by Gartner that by 2015, 40% of US enterprise employees would use their mobile devices to accomplish some of their job duties [9].

This trend, known as Bring Your Own Device (BYOD), is becoming increasingly popular among businesses, which even encourage their workers to minimise money expenditure on acquiring (often unnecessary and redundant) personal computers by using their own portable mobile devices both for personal and work-related purposes. This, however, opens unprecedented opportunities for hackers to breach enterprise network and get access to potentially sensible data. Hackers often aim at accessing financial data through vulnerable mobile devices, which act as entry-points into the company’s internal network, with an intention to sell this data to competitors or blackmail the owners. Even though there seems to be no detailed and truthful information on the financial losses such malicious attacks may lead to due to privacy policies, IBM estimates the overall losses caused by various data breaches as $3.79 million [10]. This number includes security threats ranging from simple ‘phishing’ web sites and unauthorised phone calls using leaked personal data, to much more serious leakage of an enterprise’s financial and banking data.

Nevertheless, enterprises tend to see more benefits in using employers’ personal mobile devices at work despite these threats, or simply seem to ignore them. Admittedly, going mobile may increase business

productivity, shortens time to take important business decisions, and enables offering services to customers anywhere and at any time. This claim is supported by statistical research, which shows that more and more companies are migrating to mobile platforms at least partially in spite of the potential vulnerability to security threats and risk of financial losses [11].

In fact, a recent global study of more than 4,600 IT and IT-security professionals revealed that 74% surveyed employers admit that use of personal mobile devices at work put the enterprise security at serious risk. Despite these numbers, most organisations (i.e., 65% of the surveyed audience) have not introduced any additional policies to address this emerging BYOD trend, only half of them require enabling security settings on mobile devices, and only 3% claim that their corporate IT ecosystem is fully protected and compliant with emerging mobile security policies [12]. Moreover, in the previous year, 60% of the survey respondents admitted an increased number of malware infections, and 51% of the audience experienced incidents related to security breaches and consequent data losses due to insufficient (or absolutely no) protection of mobile devices and network connections [12].

In fact, any relatively complex and advanced computational devices such as mobile phones, PCs or servers can be potential victims of malware. In this context, smart mobile devices are particularly vulnerable due to their network connectivity features, which make them attractive targets for hackers. The inherent mobility of portable devices implies that smartphones and tablets are supposed to be used anywhere by establishing ad-hoc short-term connections to networks, which are not necessarily reliable and secure. In the presence of numerous mobile devices, monitoring and controlling network environments are becoming an increasingly difficult task. Additionally, users often tend to pay little or no attention whatsoever, when sharing their devices with others and downloading and installing potentially unreliable and unsecure mobile applications.

A common way for hackers to identify potential security breaches in mobile applications is to first download target software and then, by applying reverse engineering techniques, modify the behaviour of the target application by equipping it with malicious code. Then, in order to distribute the malware, hackers either send it via common channels such as e-mails, or publish it on various app stores and web sites for further download and installation on user devices. According to Juniper Networks [6], more than 500 third party web sites and app stores host and distribute Android mobile software infected with such hidden malicious code to lesser or greater extent.

Such infected malware can pursue a wide range of goals, such as, for example, getting unauthorised access to users' sensitive data or disabling data encryption mechanisms. It may also be configured to extract necessary information from a mobile device and expose to a third party. A more sophisticated and advanced family of mobile malware, after having been installed on a target device, can even get access to other installed applications, which are regarded as more protected and would not be hacked in a direct way. Gaining control over such a proprietary application (e.g., e-banking apps) may lead to even more harmful consequences for the user, and tracing down the actual root of the problem is often problematic.

We are currently witnessing a paradigm shift in IT – from personal desktop computers we are moving towards portable mobile computing, supported by the powers of clouds. In 2011, smartphone sales exceeded PC sales for the first time in the history [13], and as it was recently declared by Apple CEO Tim Cook, the PC is now officially dead [14]. Admittedly, with this mobile revolution the mobile security issue has been attracting much attention. The market of portable and mobile devices would not be exponentially growing if it was not properly supported by advances in security and data protection. Accordingly, as the mobile technology was advancing and the number of mobile devices was growing, the research and industrial community has been consequently putting more and more efforts into investigating possible approaches to provide efficient and secure solutions for mobile platforms. In the 1990s the mobile technology was in its infancy and security issues were among the minor concerns with little or attention. Then, in the 2000s, the community focused on enabling mobile platforms with reactive self-protective mechanisms, which would fix potential harmful consequences of detected malware. And now we are seeing how more and more proactive mechanisms are attempting to predict and prevent possible attacks and threats before they even happen.

A. Geography of Mobile Threats

The number of Android devices exceeded 2 billion in 2014, and there have been detected and identified 2.8 million malware samples, which demonstrated an increase of 329% since the previous year, as reported by CM Security Research Lab [15]. The majority of the identified malware samples were targeted at payments and user privacy. Many users of mobile phones and tablets are affected by these malware, worldwide; in 2014, around 280 million people have been affected which is 800,000 users daily on average.

As far as individual countries are concerned, studies reveal that Russia is a country with the highest rate of

mobile malware attacks, among which mobile banking attacks using Trojans are particularly wide-spread [16]. China and India also have experienced increasingly considerable problems related to mobile malware. The study explains these findings with a conclusion that users in these countries are more vulnerable, since they tend to use illegal app stores hosted by unauthorised and potentially untrusted third parties, which facilitate wide spread of malware [16].

A slightly different view on malware threat statistics shows that Vietnam seems to be at highest risk with a 2.34% possibility that a downloaded app is already infected with malicious code. Although Russia is a leading region as far as the overall number of attacks is concerned, it is only ranked 22nd according to the infection risk with a rate of 0.69%. In Spain, Italy, the UK and Germany the infection risk has been estimated as 0.54%, 0.18%, 0.16% and 0.09% respectively. Japan and USA have been identified as most protected countries with 0.01% and 0.07% possibility of a malware attack respectively [16].

III. Survey of Existing Monitoring Frameworks

We have attempted to identify and survey most prominent and widely used monitoring frameworks specifically designed and developed to monitor grid systems. The surveyed frameworks are widely used for grid monitoring purposes all around the globe (with a particularly wide adoption in Europe). In our survey we attempted to address the most necessary relevant aspects of the existing grid monitoring frameworks. It has to be noted that due to space constraints we only provide an overview, and refer the interested reader to a comprehensive study in [17], where authors compare available monitoring systems and classify them into application-, resource-, performance- and job status-oriented approaches. Accordingly, we have identified 12 grid monitoring systems, which we now consider in more details one by one. The survey results are summarised in Table 1 (with indication of supported features), whereas an actual critical analysis and discussion of the survey results are provided in the concluding section.

A. Monitoring and Discovery System (MDS)

MDS[1] is one of the most prominent monitoring frameworks widely used as a part of Globus Toolkit (GT) – a toolkit for building and managing grids – or independently. Hierarchically structured, it enables management of static and dynamic information related to the current status of grid components. MDS provides an index service, which is used by managed grid systems to deliver collections of low-level data via a special registration protocol and caching mechanism so as to minimise the amount of non-stale data being transferred [18]. In recent years, MDS has considerably evolved; the second version of this system is based on the Lightweight Directory Access Protocol (LDAP), and the third edition relies on GT Information Services (GIS) and implements the Open Grid Services Architecture (OGSA). The latest (i.e. fourth) release of MDS was implemented using the Web Services Resource Framework (WS-RF) specification proposed by OASIS.

B. Ganglia Monitoring System

Ganglia[2] is widely used in high-performance computing environments in order to primarily monitor computational resources [19]. Its main focus is on monitoring clusters, grids, and cloud infrastructures. Ganglia is based on carefully designed and engineered data structures and algorithms in order to achieve efficient monitoring of grid resources [17]. As claimed by its description, this system is highly optimised and advanced to be capable of monitoring clusters with more than 50,000 running hosts. However, the application scope of Ganglia is limited – it is strictly targeted at monitoring resources, and typically neglects other important areas, such as security.

C. GridICE

GridICE[3] was created at Istituto Nazionale di Fisica Nucleare (INFN) in the frame of the European DataTAG project. GridICE is distributed under a BSD-based license, and has been used in the context of several EU projects, including INFN-GRID, CMS-LCG0 and LCG2 [17]. GridICE facilitates the process of monitoring of scattered resources in grid architectures, and can be described as a multi-dimensional monitoring framework capable of capturing a wide range of monitored metrics. It relies on data collection capabilities of GIS to gather, aggregate and display the monitored data to the user. GridICE can be configured to aggregate collected data based on user requirements and specifications – e.g. to monitor certain aspects of the grid virtual organisation or the grid operation centre. GridICE is enabled with detection and notification services, and can also capture network-related statistics.

D. UK Grid Network Monitoring (GridMon)

GridMon[4] is a grid network monitoring system which monitors network-related information, aggregates the collected data and displays it to the user [20]. The system is a collection of tools which can measure such metrics as connectivity, network performance, network jitter, packet loss rate, round trip time, TCP and UDP throughput.

[1] http://toolkit.globus.org/toolkit/mds/

[2] http://ganglia.sourceforge.net/

[3] http://sourceforge.net/projects/gridice/

[4] http://gridmon.dl.ac.uk/gridmon/graph.html

GridMon was developed in the context of creating a connected grid infrastructure across the UK, and is not publicly available for download and usage [17].

E. R-GMA

R-GMA [21] is based on the Grid Monitoring Architecture (GMA), which uses relational model for data storage. This allows the users the ability to run customised SQL-like queries to retrieve required information from the system. R-GMA also offers its users a global view on the grid system, including service availability and application monitoring [17].

F. GridRM

This is another monitoring system for networks which implements the GMA. A GridRM [22] gateway is deployed on each grid site to access information about local resources. Equipped with a relational database, it is capable of collecting data from other monitoring services (e.g. MDS) over the Simple Network Management Protocol and presenting it to the users via standardised views. It also provides a Web-based user interface to access monitored data remotely and run custom queries to retrieve required aggregated information.

G. Nagios

Nagios[5] [23] enables resource and application monitoring based on an extensible architecture. It offers various monitoring services such as monitoring of host resources (e.g., CPU/memory utilisation, response times, etc.) and monitoring of network services and protocols (e.g., SMTP, POP3, HTTP, PING etc.). Being an advanced and well-developed grid monitoring solutions, Nagios, however, seems to be lacking tools for monitoring access control security policies.

H. Mercury Grid Monitoring System

Mercury[6] was designed to meet the requirements of grid performance monitoring. It supports data monitoring and metrics collection based on both *pull* and *push* models, and is targeted at controlling grid resources and applications in a scalable way. Mercury partially implements the GMA, and also follows a modular approach, which facilitates simplicity, proficiency, convenience and low insensitivity.

I. G-PM/OCM-G

The OCM-G system [24] is a grid application monitoring framework, which offers online monitoring tools, configurable by the central manager which orchestrates the monitoring process and passes monitoring requests to local monitoring agents. G-PM is a graphical extension to this system for visual performance analysis (in the form of charts, diagrams, etc.). It offers standard performance metrics and also supports creating user-defined custom metrics.

J. MapCenter

MapCenter [25] is a flexible monitoring system, enabled with user interface to present and visualise run-time information on services and applications running on the grid. It relies on R-GMA to automatically collect data, and MDS for web browsing. It also supports dynamic discovery, based on optimised and transparent monitoring techniques, which enable rapid deployment of MapCenter in multiple grids. MapCenter is backed up with a data replication mechanism and a storage system.

K. visPerf

visPerf [26] is another grid monitoring system, which support visualisation of grid resources. This system uses agents which can extract the necessary information from log files and/or can access the grid middleware API in system. Developed in the frame of GridSolve project, it allows connecting to NetSolve servers for accessing system information for monitoring purposes.

L. Scalea-G

Scalea-G [27] is a generic performance analysis and monitoring system for grid systems. It provides an OGSA-based setup for performance analysis and monitoring of various parameters belonging to network resources, computational resources and applications. Both push and pull data collection models are supported to enable scalable and flexible monitoring solution. Scalea-G supports dynamic source code instrumentation to enable tracing and profiling of grid applications.

Table 1. Survey summary.

Monitoring framework	Type of monitoring								
				Resource-oriented			Performance-oriented		
	Application-oriented	Job status-oriented	**Mobility-oriented**	Computing	Storage	Network	Sampling	Tracing	Profiling
MDS	+	+	-	+	+	+	+	-	+
Ganglia	-	-	-	+	+	+	+	+	-
GridICE	-	-	-	+	+	-	+	+	-
GridMon	-	-	-	-	-	+	+	-	-
R-GMA	+	+	-	+	+	+	+	+	+
GridRM	-	+	n/a	+	+	+	+	-	-
Nagios	-	-	-	+	+	+	+	+	-
Mercury	+	-	-	+	+	+	+	+	+
G-PM/OCM-G	+	-	-	+	-	-	+	+	-
MapCenter	-	-	n/a	-	-	-	+	-	-

[5] https://www.nagios.org/
[6] http://www.lpds.sztaki.hu/mercury/

VisPerf	-	+	n/a	+	+	+	-	-	+
Scalea-G	+	-	n/a	+	-	+	+	+	+

CONCLUSION

There are two main observations to be derived from this survey. The research work on grid monitoring mainly dates back to the 2000s; there is relatively little recent literature related to open problems and challenges. However, the situation is expected to change with the emergence and development of mobile grid systems. Even though the existing solutions seem to be successfully tackling problems of monitoring grid systems, running applications and resources, they will require novel intelligent ways of addressing the newly-introduced mobile dimension, and particularly the related security aspects. This leads us to the second observation. Existing solutions seem to be incapable to address this issue, as they were designed for traditional grid systems. Our survey indicates that none of the surveyed approaches actually has the capacity to monitor security policies. With the introduction of mobile grids, there seems to have appeared a research gap, which urgently needs to be addressed. We need to develop novel or extend the existing solutions to support monitoring of the security dimension in general, and mobile security in particular.

REFERENCES

[1] A. Litke, D. Skoutas, and T. Varvarigou, "Mobile grid computing: Changes and challenges of resource management in a mobile grid environment," in *5th International Conference on Practical Aspects of Knowledge Management (PAKM 2004)*, 2004.

[2] I. Foster and C. Kesselman, Eds., *The Grid: Blueprint for a New Computing Infrastructure*. San Francisco, CA, USA: Morgan Kaufmann Publishers Inc., 1999.

[3] K. Katsaros and G. C. Polyzos, "Mobility-Aware Grid Computing," *Encycl. Inf. Sci. Technol.*, 2009.

[4] A. Bichhawat and R. C. Joshi, "A Survey on Issues in Mobile Grid Computing," *Int J Recent Trends Eng. Technol.*, vol. 4, no. 2, 2010.

[5] T. Dunnewijk and S. Hultén, "A brief history of mobile communication in Europe," *Telemat. Inform.*, vol. 24, no. 3, pp. 164–179, Aug. 2007.

[6] "Juniper Networks Third Annual Mobile Threats Report," Juniper Networks, 2013.

[7] "State of Mobile App Security: Apps Under Attack," Arxan, Research Report, Nov. 2014.

[8] "Bring Your Own Device: Acceptability rises," *http://www.livemint.com/*. [Online]. Available: http://www.livemint.com/Industry/zufyfhu3HkzYmzkmNexrsO/Bring-Your-Own-Device-Acceptability-rises.html.

[9] "Gartner Says 40 Percent of U.S. Employees of Large Enterprises Use Personally Owned Devices for Work." [Online]. Available: http://www.gartner.com/newsroom/id/2881217.

[10] "2015 Cost of Data Breach Study: Global Analysis," 21-Nov-2015. [Online]. Available: https://www-01.ibm.com/marketing/iwm/dre/signup?source=ibm-WW_Security_Services&S_PKG=ov34982&S_TACT=C405001W&ce=ISM0484&ct=SWG&cmp=IBMSocial&cm=h&cr=Security&ccy=US&cm_mc_uid=42044176331714480655390&cm_mc_sid_50200000=1448065539.

[11] M. Finneran, "Research: 2013 State Of Mobile Security," Juniper Networks, 2013.

[12] "Ponemon Institute© Research Report Mobility Risks." [Online]. Available: http://www.websense.com/content/ponemon-institute-research-report-2012.aspx?cmpid=prnr2.29.12.

[13] A. Cocotas, "SMARTPHONE MARKET FORECAST: Sales Will Exceed 1.5 Billion Units A Year By 2016," *Business Insider Australia*, 01-Mar-2012. [Online]. Available: http://www.businessinsider.com.au/smartphone-market-forecast-sales-will-exceed-15-billion-units-a-year-by-2016-2012-2.

[14] "Tim Cook says the PC is dead, but Apple still makes computers," *The Next Web*. [Online]. Available: http://thenextweb.com/insider/2015/11/10/tim-cook-says-the-pc-is-dead-but-apples-still-making-desktops-and-laptops/.

[15] "2014 Cheetah Mobile Security Report." [Online]. Available: http://www.cmcm.com/article/share/2015-01-19/526.html.

[16] M. Garnaeva, V. Chebyshev, D. Makrushin, and A. Ivanov, "IT threat evolution in Q1 2015," Kaspersky Lab, 2015.

[17] M. Gerndt, R. Wismüller, T. U. München, Z. Balaton, G. Gombás, P. Kacsuk, Z. Nemeth, N. Podhorszki, H. Truong, U. Wien, T. Fahringer, U. Innsbruck, E. Laure, M. Bubak, and T. Margalef, *Performance Tools for the Grid: State of the Art and Future*. 2004.

[18] K. Czajkowski, S. Fitzgerald, I. Foster, and C. Kesselman, "Grid information services for distributed resource sharing," in *High Performance Distributed Computing, 2001. Proceedings. 10th IEEE International Symposium on*, 2001, pp. 181–194.

[19] M. L. Massie, B. N. Chun, and D. E. Culler, "The ganglia distributed monitoring system: design, implementation, and experience," *Parallel Comput.*, vol. 30, no. 7, pp. 817–840, Jul. 2004.

[20] M. Leese and R. Tasker, "Building the e-Science Grid in the UK: GridMon-Grid Network Performance Monitoring."

[21] A. Cooke, A. J. G. Gray, L. Ma, W. Nutt, J. Magowan, M. Oevers, P. Taylor, and D. O'Callaghan, "R-GMA: An Information Integration System for Grid Monitoring," in *On The Move to Meaningful Internet Systems 2003: CoopIS, DOA, and ODBASE*, R. Meersman, Z. Tari, and D. C. Schmidt, Eds. Springer Berlin Heidelberg, 2003, pp. 462–481.

[22] M. Baker and G. Smith, "GridRM: an extensible resource monitoring system," in *2003 IEEE International Conference on Cluster Computing, 2003. Proceedings*, 2003, pp. 207–214.

[23] E. Imamagic and D. Dobrenic, "Grid Infrastructure Monitoring System Based on Nagios," in *Proceedings of the 2007 Workshop on Grid Monitoring*, New York, NY, USA, 2007, pp. 23–28.

[24] M. Bubak, W. Funika, and R. Wismüller, "The CrossGrid performance analysis tool for interactive Grid applications," in *Recent Advances in Parallel Virtual Machine and Message Passing Interface*, Springer, 2002, pp. 50–60.

[25] F. Bonnassieux, R. Harakaly, and P. Primet, "MapCenter: An Open Grid Status Visualization Tool," in *proceedings of ISCA 15th International Conference on parallel and distributed computing systems*, 2002, pp. 2–3.

[26] D. Lee, J. J. Dongarra, and R. S. Ramakrishna, "visPerf: Monitoring Tool for Grid Computing," in *Computational Science — ICCS 2003*, P. M. A. Sloot, D. Abramson, A. V. Bogdanov, Y. E. Gorbachev, J. J. Dongarra, and A. Y. Zomaya, Eds. Springer Berlin Heidelberg, 2003, pp. 233–243.

[27] H.-L. Truong and T. Fahringer, "SCALEA-G: A Unified Monitoring and Performance Analysis System for the Grid," in *Grid Computing*, M. D. Dikaiakos, Ed. Springer Berlin Heidelberg, 2004, pp. 202–211.