CROSS-DOMAIN IDENTITY TRUST MANAGEMENT FOR GRID COMPUTING

Amr Farouk, Mohamed M. Fouad and Ahmed A. Abdelhafez

Department of Computer Engineering, Military Technical College, Cairo, Egypt

ABSTRACT

The grid computing coordinates resource sharing between different administrative domains in large scale, dynamic, and heterogeneous environment. Efficient and secure certificateless public key cryptography (CL-PKC) based authentication protocol for multi-domain grid environment is widely acknowledged as a challenging issue. Trust relationships management across domains is the main objective of authentication protocols in real grid computing environments. In this paper, we discuss the grid pairing-free certificate-less two-party authenticated key agreement (GPC-AKA) protocol. Then, we provide a cross domain trust model for GPC-AKA protocol in grid computing environment. Moreover, we analysis the GPC-AKA protocol in multiple trust domains simulated environment using GridSim toolkit.

KEYWORDS

Certificate-less authenticated key agreement, cross-domain identity trust, grid computing.

1. INTRODUCTION

For fully secure and efficient grid entities authentication, it is required to build a provable secure authenticated key agreement (AKA) protocol. Moreover, it should meet with the requirements of large scale distributed, heterogeneous and dynamic grid virtual organizations (VO), that usually spans multiple trust domains [1]. Hence, trust in grid computing is the firm belief between grid entities to enable grid systems to work normally in the context of the fundamental grid functions [2]. Trust relationship in grid computing environments is classified based on trust domain boundaries into three categories [3]: i) intra-domain trust refers to the trust relationship between members and the power institutions of the domain. ii) interdomain recommendation trust is a kind of trust relationship which is set up by the power institutions in the grid levels. iii) cross-domain trust means the trust relationship among members of different domains. As well, based on trust approaches, trust relationship is classified into the following categories [2]: i) identity trust (i.e., objective trust) is associated with verifying the authenticity of an entity and focuses on the objective credentials. ii) behavioral trust (i.e., subjective trust) deals with a wider notion of an entity's "trustworthiness", which depends on certain contexts. The relationship can take many directions. First, in resource allocation process, the resource provider want to know the trust level (i.e., acceptable code and not harmful) of the grid user requested job. Second, the resource provider guarantees to the grid user, the process execution without interruption and the user's privacy protection [2].

Grid computing as a VO for resources collaboration and coordination, has become so prevalent that grid trust relationship become an intensive topic. In the trust research area, the numerous literatures proposed the different trust models. These have provided the valuable thoughts for

DOI : 10.5121/ijsptm.2014.3202

trust research in the grid environment. As different management domains take different security policies to mange intra-domain security in the grid, it's difficult to form an overall management strategy among different domains [3]. In order to build trust relations between entities and different trust domains, we give the ring framework of objective trust model. Ring topology has no root KGC, so no single point of trust. This approach construct a global trust infrastructure composed of group of trust authorities (i.e., KGCs) without the hierarchy level limitation, so it has a scalability advantage. A objective trust modeling method suitable in grid environment is proposed based on the characteristics of grid computing and the features of objective trust.

This paper addresses trust management issues in grid computing and analyses some relevant cross-domain scenarios. Then it derives main requirements in terms of cross authentication. We discuss the efficient GPC-AKA protocol based on GDH complexity problem. As well, we propose a cross-domain grid trust model based on GPC-AKA protocol. In addition, we design and implement a simulation of the proposed grid trust model based on a world wide grid testbed. The testbed is composed of multiple organizations, each have its own KGC, and concerned to build a trust relationships with the others. Furthermore, we analyses the performance of cross-domain GPC-AKA protocol in complex simulated scenarios.

The rest of this paper is organized as follows. Trust in grid computing is described in Section II. The grid pairing-free CLAKA protocol is presented in Section III. Section IV shows the proposed Grid trust management model based on GPC-AKA protocol. Simulation experiment of cross-domain GPC-AKA using GridSim is introduced in Section V. Finally, Section VII provides our research conclusions.

2. TRUST IN GRID COMPUTING

Recently, trust has been recognized as an important factor for grid computing security. Several interesting trust models have been proposed for integration into the Grid computing systems [4]–[7]. However, we have found that theses trust models specialize in applying trust for enhancement of resource allocation functions of a grid system; also the trust mechanisms are mainly based on behavioral methods, which is not scalable nor efficient.

A grid computing environment is a virtual organization (VO) that is composed of several autonomous domains in which different security policies are applied. The grid computing environment features are [8]: The user population and resource pool (e.g., quantity, location) are large and dynamic. A computation is composed of a dynamic group of processes (i.e., created and destroyed dynamically during program execution) running on different resources and sites. The pre-trust relationships establishment between different grid sites is impractical due to the dynamic nature of the grid computing environment [8].

The trust management is a distinct and crucial component of grid services security. Aspects of the trust management problem include formulating security policies and security credentials, determining whether particular sets of credentials satisfy the relevant policies, and deferring trust to third parties.

First, security policy, is a set of rules that define the grid users (i.e., security subjects), grid resources (i.e., security objects) and relationships among them [8]. Resources may require different local policies (e.g., authentication and authorization mechanisms), that apply at the different sites, which we will have limited ability to change. Authentication is the first line of defence in the grid security policy that provides mapping from local security policies into a global framework [8].

Second, security credential can be defined as a piece of information that is used to prove the identity of a subject [8]. Federation of identities when grid entities have different identities and/ or credentials in different security domains. Identity federation is a set of organizations that establish trust relationships with respect to the federated identity information. Identity federation technology (e.g., Shibboleth) enables that no need for direct trust relationship between users and accessed domains. However, the identity server store the individual credentials securely, the main challenge is to protect the user's privacy.

Third, trust domain can be defined as a logical, administrative structure that holds a single, consistent local security policy [8]. In this study, we will focus on the third point which is grid trust relationships using grid authentication protocol.

We can solve grid trust management problems using grid authentication protocols based on identity that distinguishes a distinct user, process or resource within the context of a specific namespace. Identity Authentication: proving as association between an entity and an identifier. Attribute Authentication: proving as association between an entity and an attribute.

We will use the proposed GPC-AKA protocol based on the general grid security architecture of Foster et. al. [8]. Our approach to trust management is based on the following general principles: unified mechanism, flexibility, locality of control and separation of mechanism from policy.

3. EFFICIENT AND SECURE GRID PAIRING-FREE CL-AKA

Wang et. al. [9] present the first grid certificate-less authentication based on certificate-less public key cryptography (CL-PKC), that is a kind of cryptography between certificate based and identity-based PKC. The bilinear pairing is then considered as an expensive cryptography primitive. Therefore, a number of pairing-free CL-AKA protocols, have been proposed to improve efficiency. These protocols, either have a security issues or are not efficient to be practical implemented in real environments.

We focus on the more recent efficient pairing-free CL-AKA protocol, as formal prove the protocol security to be suitable for practical grids. Recently, Amr et. al. [10] proposed an efficient and provable secure grid pairing-free certificate-less two-party authenticated key agreement (GPC-AKA) protocol. The GPC-AKA protocol uses a user proxy (UP) and resource proxy (RP) to support the grid single sign on (SSO) and frequent mutual authentication requests [8].

GPC-AKA protocol requires 3 elliptic curve point multiplications, 5 elliptic curve point additions, 2 hashing functions, and 2 message exchanges. The proposed Pairing-free certificate-less two party authenticated key agreement for grid (GPC-AKA) is introduced into two phases, as illustrated in Fig. 1 and Fig. 2, respectively.

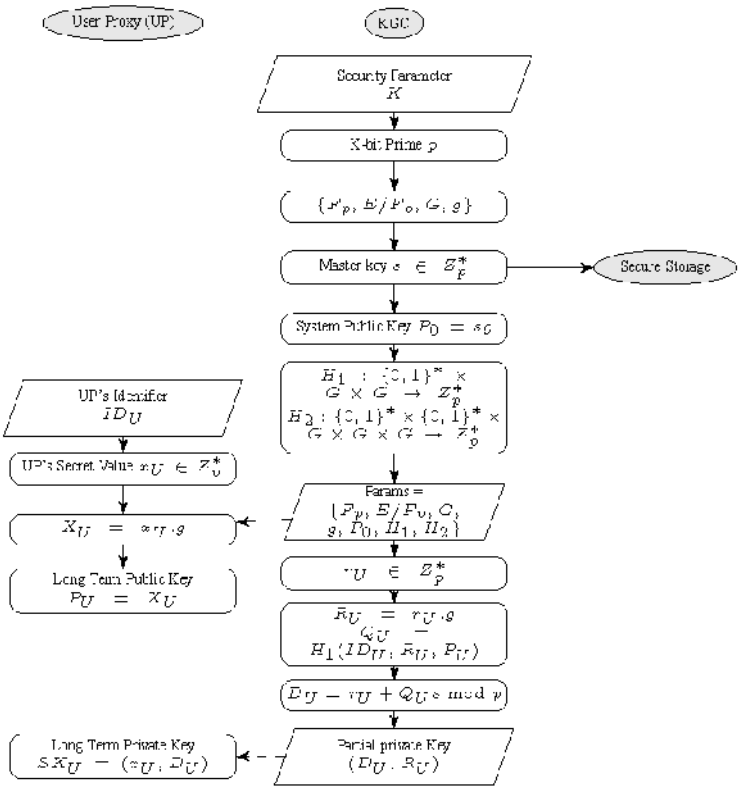

Figure 1. Proposed GPC-AKA key generation setup scheme (Phase 1).

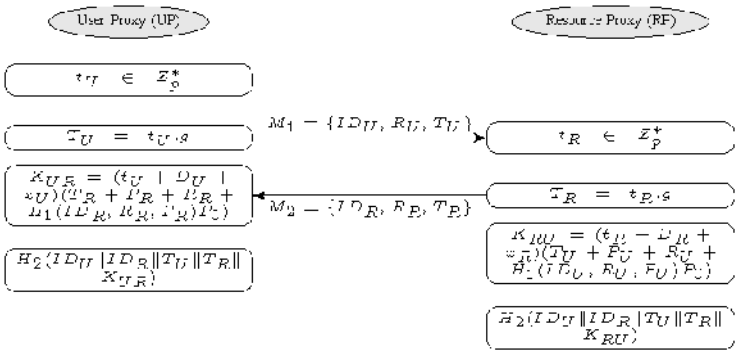

Figure 2. Proposed key agreement scheme GPC-AKA (Phase 2).

4. CROSS-DOMAIN GRID TRUST MANAGEMENT

Grid computing environments include different resources through cross-organizational boundaries on a large scale basis. This heterogeneous environment consists of multiple disconnected trust domains, applying its own policies and mechanisms for authentication. Consequently, an important challenge for the GPC-AKA is to provide a cross-domain authentication service. It should be pointed out that existing identity trust models suffer from a

restricted and static vision of trust (i.e., strict hierarchies where trust flows from the root to the leaves).

We propose a novel trust model reflecting the required dynamic nature of trust for grid entities, through cross organizational boundaries, with little administrative overhead. Based on cross-domain grid computing GPC-AKA authentication protocol, a Grid Trust Management (GTM) model has been designed to establish trust relations between grid entities. Cross-domain GPC-AKA trust model is shown in Fig. 3.

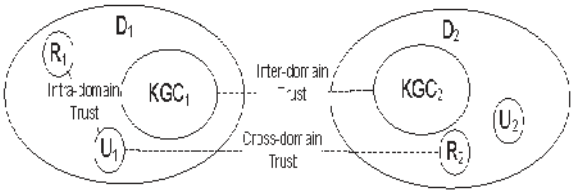

Figure 3. Grid Trust Model.

We adopt some common approaches for scalability and flexibility in our design. To our knowledge, the following discussion represents the first such grid trust management model that has been defined to this level of detail. Our proposed GTM design model answers the following questions:

1) How to add new KGC? According to the grid virtual organization concept, we can add a new KGC to the virtual organization KGCs group in ring topology avoiding the hierarchal problems, by sharing the same system parameters. Since, in the real grid, most trust domains are autonomous, using different system parameters. So in our GTM model, all the system parameters of PKG are the same, except the system public key and master key.

2) How to do key revocation? key expiration in GTM is straightforward, used for key revocation. Short-term key revocation using fine-grained identifier (e.g., extend the user's identifier to include another field that specifies a validation period). The validation period inversely proportional to the KGC server load.

3) How to do key renew? In a grid environment, it is normal practice to renew the user's long-term keys on a monthly or yearly basis. This can be done through the KGC issuing a new private key directly to the user through a secure channel. Short-term keys are used for various security service such as mutual authentication, single sign-on and delegation.

4) How to build trust between KGCs? Trust relationships between KGCs can be established as follows, system parameters of the KGCs are then assumed to be trusted by all users and recognized by the grid system, as shown in Table I.

5) How to build cross-domain trust between entities? Cross-domain GPC-AKA protocol consistency is proved as follow.

Table 1. Cross-Domain GPC-AKA.

Parameters	**D_1**		**D_2**	
	U_1	KGC_1	KGC_2	R_2
Public	P_{u1}	P_{01},Params	P_{02},Params	P_{r2}
Secret	X_{u1}, t_{u1}	S_1, D_{u1}	S_2, D_{r2}	X_{r2}, t_{r2}

Where Params = {Fp,E/Fp,G, g,H_1,H_2} are the same in both KGCs (*i.e.*, KGC_1,KGC_2) and grid entities (*i.e.*, U_1,R_2).

Cross-domain GPC-AKA protocol consistency is proved:

$K_{U1R2} = (t_{U1} + D_{U1} + x_{U1})(T_{R2} + P_{R2} + R_{R2} + H_1(ID_{R2},R_{R2}, P_{R2})P_0)$
$= (t_{U1} + D_{U1} + x_{U1})((t_{R2}.P) + (x_{R2}.P) + (r_{R2}.P) + (Q_{R2}.sP))$
$= (t_{U1} + D_{U1} + x_{U1})(t_{R2} + x_{R2} + r_{R2} + Q_{R2}.s)P$
$= (t_{U1} + D_{U1} + x_{U1})(t_{R2} + x_{R2} + D_{R2})P = K_{R2U1}$
where $ID_{R2}= ID_{KGC2}||ID_{R2}$.

5. CROSS-DOMAIN GPC-AKA SIMULATION EXPERIMENT

In this section, we present the simulation experiment of cross-domain GPC-AKA protocol in grid computing environment. Grid network topology is explained in Section V-A. Furthermore, a GPC-AKA simulation using GridSim toolkit is provided in Section V-B.

The only feasible way to analyze repeatable experiments and studies that are not possible in real dynamic grid environment is the using of grid simulator. We choose the Java-based simulation platform GridSim Toolkit [11] with network extension package to simulate the message exchange of the proposed multiple trust domains GPC-AKA protocol. As well, GridSim is based on SimJava which is a discrete event simulation tool based on Java and simulates various entities by multiple thread. This aligns well with randomness of grid computing entity action.

5.1. Grid Network Topology

In this section, we provide a scenario of the cross-domain authentication using GPC-AKA protocol. We have created an experiment based on the World Wide Grid testbed [12], as shown in Fig. 4.

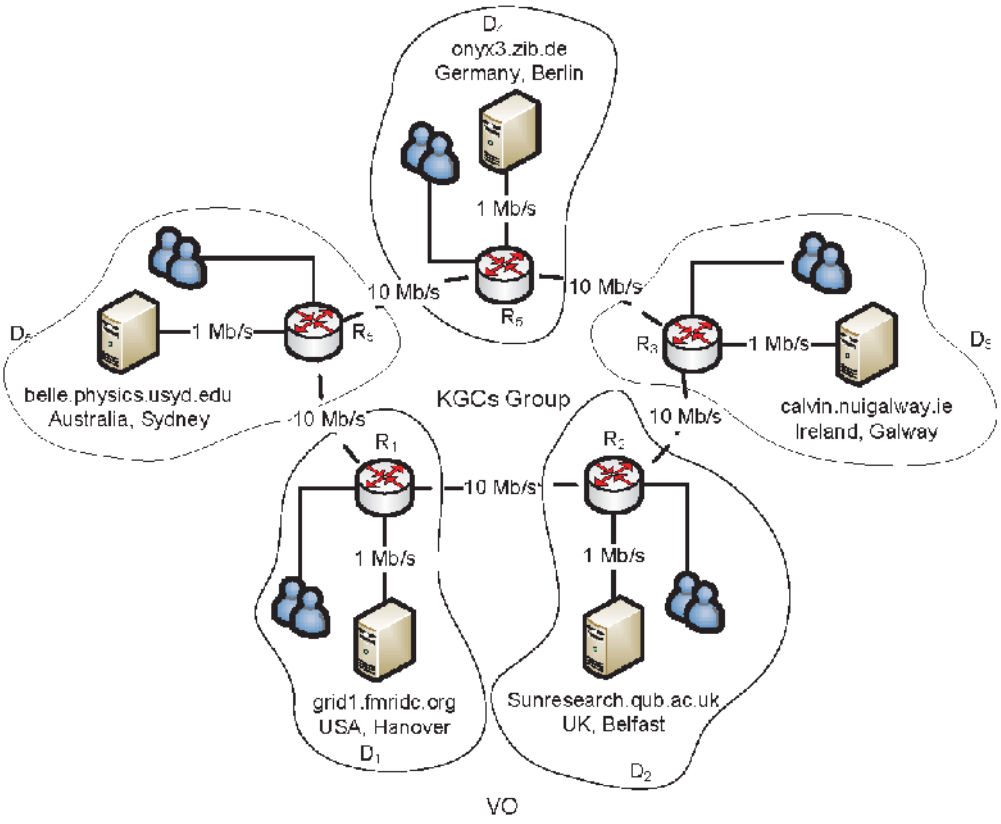

Figure 4. Cross-Domain Grid Network Topology.

A Grid resource contains one or more Machines. Similarly, a machine contains one or more processing elements (PEs) or CPUs. For this experiment, we are simulating five VO domains and each resource belongs to one of them, with three Machines that contains one or more PEs. The VO mapping is done by taking into account a geographical dissemination among the resources. Table II summarizes the characteristics of simulated resources, which were obtained from a real World Wide Grid testbed.

Table 2. Grid Topology and Resources Characteristics.

Domain	Resource Name	Resource Characteristics	Host name & Location	No. CPU	Time Zone
D_1	N_1	UltraAX-i2, SunOS, Sparc	grid1.fmridc.org, USA, Hanover	16	-4
D_2	N_2	Sun HPC 3500, GridEngine, Solaris, Sparc	sunresearch.qub.ac.uk, UK, Belfast	6	+1
D_3	N_3	SGI Origin 3800, IRIX 6.5.17m, Irix, MIPS	calvin.nuigalway.ie, Ireland, Galway	40	+1
D_4	N_4	SGI Onyx 3000, IRIX64, Irix, MIPS	onyx3.zib.de, Germany, Berlin	20	+2
D_5	N_5	IBM eServer, Linux, IA-32	belle.physics.usyd.edu.au, Australia, Sydney	4	+11

We created five scenarios, each time we increased the total grid users {5,10,15,20,25} to simulate the concurrent requests and uniformly distributed them among the five trust domains, each domain has {1,2,3,4,5} user(s). In our simulation setup, some parameters are set identical for all network elements, such as the maximum transfer unit (MTU) of links is set to 1,500 bytes and the latency is set to 10 milliseconds. We can conclude the simulation experiment parameters in Table III.

Table 3. Simulation Parameters.

Parameter	Value
number of grid users	{5,10,15,20,25}
number of grid resource	5
number of gridlets	1
baud rate	1000 bits/sec
propagation delay	10 msec
max. transmission unit (MTU)	1500 byte

5.2. Simulation using GridSim Toolkit

Object-oriented GridSim toolkit allows modeling of heterogeneous types of resources, located in any time zone. As well, multiple user can simultaneously submit tasks for execution in the same resource, that may be timeshared or space-shared. In addition, statistics of operations can be recorded and they can be analyzed using GridSim statistics analysis methods.

GridSim Toolkit V5.2 is run, on a 2 GHz Intel core 2 duo with 6 GB RAM. This simulation scenario shows how to create user and resource entities connected via a network topology, using link and router. In addition, background traffic functionality is explained in this scenario. Fig. 5 shows GPC-AKA simulation steps using GridSim.

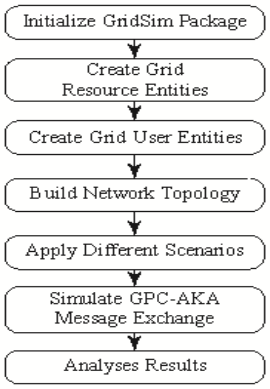

Figure 5. Main GPC-AKA Simulation Steps using GridSim.

Independent tasks are heterogeneous in terms of processing time and input files size. In GridSim, such tasks can be created and their requirements can be defined through gridlet objects [13]. We simulate GPC-AKA message exchange using the gridlet concept in GridSim. One gridlet for mutual GPC-AKA instance for each pair of grid entities.

6. DISCUSSION AND ANALYSIS

In the first experiment, we simulate the cross-domain GPCAKA message exchange without background traffic, as shown in Fig. 6. We simulate 5 trust domains and increase the number of users per each domain {1,2,3,4,5} who send concurrent requests to check GPC-AKA scalability and get the minimum, maximum, and the average of the response time. For 1 user per domain, with 5 total grid users, the minimum response time 126.30 seconds, maximum response time 140.52 seconds, and average response time 136.72 seconds. For 2 users per domain, with 10 total grid users, the minimum response time 169.30 seconds, maximum response time 214.14 seconds, and average response time 191.96 seconds with 71% increased. For 3 users per domain, with 15 total grid users, the minimum response time 197.30 seconds, maximum response time 290.15 seconds, and average response time 246.20 seconds with 78% increased. For 4 users per domain, with 20 total grid users, the minimum response time 233.30 seconds, maximum response time 366.13 seconds, and average response time 301.94 seconds with82% increased. For 5 users per domain, with 25 total grid users. the minimum response time 269.30 seconds, maximum response time 440.92 seconds, and average response time 357.54 seconds with 84% increased.

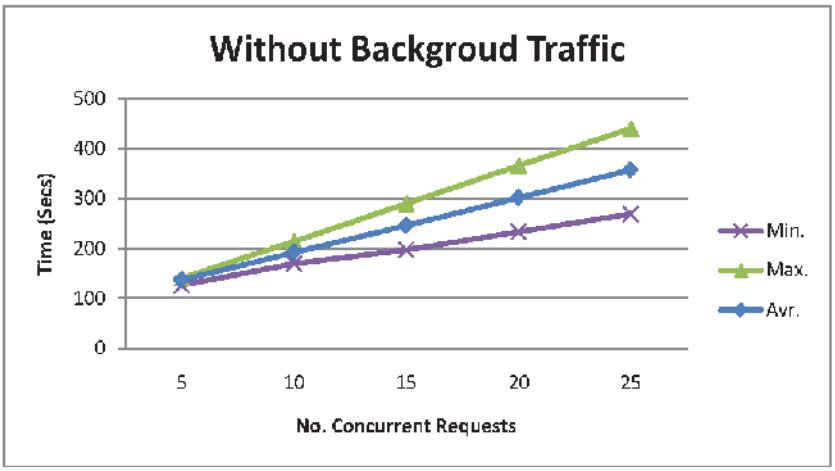

Figure 6. Concurrent Requests versus Time without Background Traffic.

In the real grid environment there is a background traffic. So, the second experiment, simulates the GPC-AKA message exchange with background traffic, as shown in Fig. 7. For 1 user per domain, with 5 total grid users, the minimum response time 139.64 seconds, maximum response time 172.02 seconds, and average response time 151.14 seconds. For 2 users per domain, with 10 total grid users, the minimum response time 172.92 seconds, maximum response time 229.65 seconds, and average response time 202.42 seconds with 75% increased. For 3 users per domain, with 15 total grid users, the minimum response time 211.63 seconds, maximum response time 352.02 seconds, and average response time 278.84 seconds with73% increased. For 4 users per domain, with 20 total grid users, per minimum response time 233.30 seconds, maximum response time 420.43 seconds, and average response time 321.41 seconds with 87% increased. For 5 users per domain, with 25 total grid users, the minimum response time 269.30 seconds, maximum response time 580.02 seconds, and average response time 417.20 seconds with 77% increased.

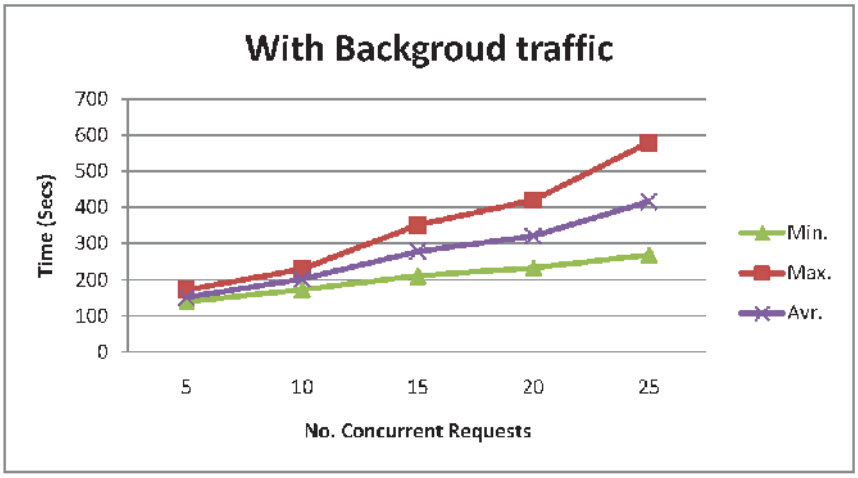

Figure 7. Concurrent Requests versus Time without Background Traffic.

7. CONCLUSIONS

According to the trust relationships between different security domains, an authentication protocol suitable for multiple security (i.e., trust) domains in grid computing is proposed in this paper. We present an efficient and secure pairing-free two party certificate-less authenticated key agreement protocol for grid computing (GPC-AKA) based on GHD complexity problem. Based on GPC-AKA, a grid trust management (GTM) model is proposed. At last, the authentication protocol is analyzed with simulated grid environment using GridSim. So, we can infer that GPC-AKA is a cross-domain authentication protocol suitable for large scale and dynamic grid computing environments.

REFERENCES

[1] A. Farouk, A. A. Abdelhafez, and M. M. Fouad, "Authentication mechanisms in grid computing environment: Comparative study," in *IEEE International Conferencce on Engineering and Technology*, Oct. 2012, pp. 1–6.

[2] J. Luo, X. Ni, and J. Yong, "A trust degree based access control in grid environments," *Information Sciences*, vol. 179, no. 15, pp. 2618–2628, 2009.

[3] H. Hai-sheng and W. Ru-chuan, "A new subjective trust model in grid computing," in *Computer Application and System Modeling (ICCASM), 2010 International Conference on*, vol. 9. IEEE, 2010, pp. V9–360.

[4] Z. Yongqiang, L. Qiang, and T. Haibo, "A hybrid system for authentication service," in 5th *International Conference on Intelligent Networking and Collaborative Systems*, 2013, pp. 821–826.

[5] L. Guoyuan, B. Yuyu, and L. Min, "Trust based access control policy in multi-domain of cloud computing," *Journal of Computers*, vol. 8, no. 5, pp. 1357–1365, may 2013.

[6] T. Liye and J. Wei, "A multi trust chain scheme in trusted crossdomain interaction," in *International Conference on Industrial Control and Electronics Engineering*, 2012, pp. 550–553.

[7] Z. Shaomin, Z. Yue, and W. Baoyi, "A novel grid trust model based on fuzzy theory," in *Third International Conference on Network and System Security*, 2009, pp. 203–207.

[8] I. Foster, C. Kesselman, G. Tsudik, and S. Tuecke, "A security architecture for computational grids," in *Proceedings of the 5th ACM conference on Computer and communications security*. ACM, 1998, pp. 83–92.

[9] W. Shengbao, C. Zhenfu, and B. Haiyong, "Efficient certificateless authentication and key agreement (CL-AK) for grid computing," in *International Journal of Network Security*, vol. 7, no. 3, Nov. 2008, pp. 342–347.

[10] A. Farouk, M. M. Fouad, and A. A. Abdelhafez, "Analysis and improvement of pairing-free certificate-less two-party authenticated key agreement protocol for grid computing," *International Journal of Security, Privacy and Trust Management (IJSPTM)*, vol. 3, no. 1, 2014.
[11] S. Anthony, P. Gokul, B. Rajkumar, and T. Chen-Khong, "Constructing a grid simulation with differentiated network service using gridsim," in *IEEE*, 2004.
[12] A. Barmouta, "Authorisation and accounting services for the world wide grid," Master of Science, School of Computer Science and Software Engineering, University of Western Australia, jun 2004.
[13] B. Rajkumar and M. Manzur, "Gridsim: a toolkit for the modeling and simulation of distributed resource management and scheduling for grid computing," in *Concurrency and Computation: Practice and Experience*, vol. 14. John Wiley & Sons, Ltd, Feb 2002, pp. 1175–1220.

Authors

Amr Farouk received the Bachelor engineering from the Military Technical College (MTC), Cairo, Egypt, in 1997, and the Masters' engineering degrees from Engineering faculty, Mansoura university, Mansoura, Egypt in 2009. He is currently a PhD arguing from Computer engineering, MTC, Cairo, Egypt. His research interests include network security, authentication protocols, certificate-less authenticated key agreement.

M. M. Fouad received the Bachelor engineering (honors, with great distinction) and Masters' engineering degrees from the Military Technical College (MTC), Cairo, Egypt, in 1996 and 2001, respectively. As well, he received the Ph.D. degree in Electrical and Computer engineering from Carleton University, Ottawa, Ontario, Canada, in 2010. He is currently a faculty member with the Department of Computer Engineering, MTC. His research interests are in online handwritten recognition, image registration, image reconstruction, super-resolution, video compression and multiview video coding.

Ahmed A. AbdelHafez; received the B.S. and M.Sc. in Electrical Engineering from Military Technical College (MTC) in 1990, 1997 respectively, and his Ph.D from School of Information Technology and Engineering (SITE), University of Ottawa, Ottawa, Canada in 2003. Dr. Abdel-Hafez is the head of the Cryptography Research Center (CRC), Egypt where he is leading many applied researches in communication security field. He is a visiting lecturer in Communication Dept. MTC, and other universities in Egypt. Dr. Abdel-hafez published more than 40 papers in specialized conferences and periodicals. His research interests include wireless networks and data security, mathematical cryptography and provable security.