A Novel Certificate-based Authentication Hybrid Broker Model using Multi-party Key Agreement in Data Grids

Wen-Chung Chiang, Chao-Tung Yang, Hsiu-Hsia Lin

Abstract

Several recent studies have demonstrated that co-allocation techniques can improve network bandwidth and network transfer times by concurrently utilizing as many data grid replicas as possible. In our previous work, the anticipative recursively adjusting mechanism plus (ARAM+) model, It was based on co-allocation strategies and decentralized service broker, which provide comprehensive capabilities of data access for users' application. Although most of current grid systems use traditional PKI to authenticate grid members as also to secure resource allocation to them, it only provides the security of inter-grid communication. However, the challenges of co-allocation architectures continue to lie in the secured intra-grid communication against internal attacks. It is presented in this paper a new certificate-based authentication hybrid broker model by using multi-party key agreement for redundant parallel file transfer in ARAM+ model, where we designed and implemented service broker agent called "resource broker", that takes over the works of job monitoring of the service broker for each dynamic resource-group. Moreover, the multi-party key agreement protocol is used to provide security services for resource-group communications. Experimental results show that our approach achieves dependable performance with various loads of services, broker failures and possible attacks.

Keywords: co-allocation, data grid, internal attacks, hybrid broker, multi-party key agreement, resource broker.

Wen-Chung Chiang , Department of Information and Network Technology, Hsiuping University of Science and Technology. wcchiang@mail.hust.edu.tw
Chao-Tung Yang , Department of Computer Science, Tunghai University
Hsiu-Hsia Lin , Craniofacial Research Center, Chang Gung Memorial Hospital

運用於資料網格中多方密鑰協議之憑證認證及授權之混合式資源代理模型

姜文忠、楊朝棟、林秀霞

摘 要

資料協同配置(Co-allocation) 架構，實現了可透過網路同時傳輸從多個站台平行下載檔案資源，以達到共享的目的，此一新開發的技術，利用多個副本透過建立多個連接並聯以進行檔案資料下載。從而提高了單一伺服器的傳輸效率，進而緩解網路擁塞問題。在我們之前提出以協同配置(Co-allocation)和提供資源代理功能為基礎的增強式動態預測調整機制模型(Anticipative Recursively Adjusting Mechanism plus：ARAM+)中，已包含服務分配，資源發現，作業調度，作業監控和資料存取等機制；然而，此一架構所面臨最大的挑戰，在於使用傳統的公開金鑰基礎 結構(PKI)作為網格群組間成員之認證機制，換句話說，它只能做到網格間(inter-grid)的通訊安全，對於網格內(intra-grid)的內部攻擊(internal attacks)則無法抵擋。為了克服以上問題，我們提出一個新的透過多方密鑰協議，以憑證授權和認證為基礎之混合式資源代理模型的協同分配傳輸網格架構。我們設計了一個所謂的資源中介代理，稱為“Resource broker”，當每次動態資源群組形成時便自動產生，並負責群組成員監督及工作分配以分擔資源中介(Service broker)的工作量。此外，我們還提出了”多方密鑰協議協定”提供一個安全的內部網路資源中介的溝通。實驗結果證明，我們的方法提供了更可靠的性能與各種負載服務，以及克服了單一資源中介故障與各種可能的攻擊。

關鍵詞：協同配置，資料網格，內部攻擊、混合式資源代理，多方密鑰協議，資源中介代理。

姜文忠：修平科技大學資訊網路技術系助理教授
楊朝棟：東海大學資訊工程系教授
林秀霞：長庚紀念醫院顱顏研究中心助理研究員
投稿日期：102 年 8 月 26 日　接受刊登日期：102 年 9 月 14 日

1.Introduction

The next-generation of scientific applications in domains as diverse as high energy physics, genomics, medicine, molecular chemistry, geology and astrophysics involve the production of large datasets from simulations or from large-scale experiments [1, 2, 3, 4, 5]. The archival, retrieval, and analysis of such datasets, that are usually disseminated among researchers located over a wide geographic area, requires the coordinated usage of high capacity computing, network, and storage resources. Data Grids [6, 7, 8, 9, 10, 11] has recently received attention as the generation platform by many scientific communities and provided services and infrastructure for distributed data-intensive application requests that need to connect, share, access, transfer and manipulate in a wide variety of geographically distributed computational and data storage resources. Co-allocation techniques [9, 12, 13, 14] are most recently developed to enable clients to download data from multiple locations by establishing multiple connections in parallel, thus improving performance as compared to the single-server case and alleviating the internet congestion problem [15, 16, 17] in Data Grids.

A service broker is an infrastructure in the Data Grids and one of the most important components of Grid systems, in building collaborative environments for large-scale data [18, 19, 20, 21]. It offers a uniform and transparent interface to heterogeneous storage systems that include disks, tape archives and databases. As part of this, the task of a Grid service broker is to allow the grid clients to state the specifications and attributes of requested resources, and then the broker dynamically identify and characterize the available resources that match the specifications and the attributes, and allocate the most appropriate resource for task execution (Fig. 1) [22]. In general, the Grid service brokers can be classified into three types according to the scope of service broker functions, namely centralized, decentralized (distributed) and hybrid [23, 24, 25, 26, 27]. In the centralized model, all requests for resources and access to the resources available in the Grid are fully controlled by one broker. The centralized model has well-known drawbacks regarding single point of failure, performance bottleneck and scalability. The decentralized model are then proposed to conquer these defects in which, individual users have their own resource brokers. This type of broker typically manages only a fraction of the total number of jobs submitted to the Grid. Advantages of the distributed brokering approach include scalability and

fault-tolerance. However decentralized broker model suffer from the lack of knowledge about the global state of the system, and they do not have full control over the grid resources. Hybrid broker is a hierarchical organization, where distributed broker are controlled by a centralized broker.

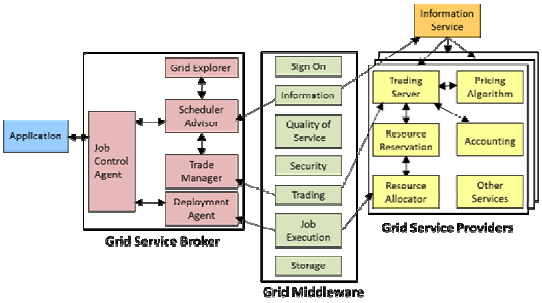

Figure 1. Resource broker architecture and its interaction with other Grid entities.

In our previous research, we presented an anticipative recursively adjusting mechanism plus (ARAM+) model [28] which was also based on the architecture of co-allocation file transfer and decentralized broker model in Grid environments. This scheme integrated the TCP bandwidth estimation model (TCPBEM) [29] to evaluate dynamic link states by detecting TCP throughputs and packet lost rates between grid sites. Burst Mode (BM) function was used to increase transfer rates and speed up total performance especially considering congestion control. The ARAM+ not only adapts to the worst network links, but also speeds up the overall performance especially in wide-area grid networks.

For the outstanding features of co-allocation services in Data Grids, such as group-oriented communication, coordinated resource sharing and dynamic, multi-institutional virtual organizations (VO), it is essential to provide group-oriented communication privacy and information integrity to others outside the group of shared resources. However, the Internet contains many threats, including hacker, virus and eavesdropper. One cannot ensure everybody on the Internet to be trustworthy. Thus, it is important that members of the group can establish a common secret key for encrypting communication data. Although most of the Globus Security Infrastructure (GSI) uses traditional PKI (X. 509) to provide integrity, protection, confidentiality and authentication for sensitive information transferred over the network in addition to the facilities to securely traverse the distinct organizations that are part of collaboration, it only provides the security of inter-grid communication. The challenges of co-allocation architectures; however, usually lie in the secure intra-grid communication against internal attacks.

However, due to the high dynamic nature of group members in Data Grids, ways how to update group key efficiently and effectively become a critical problem.

For practice purposes, especially for preventing the grid resources being illegally visited, strong mutual authentication should be guaranteed for grid entities. However, user authentication is the first step in ensuring a secure service. The extended problem after authentication is how to protect the sensitive information transmitted between entities. The most effective method to solve this problem is negotiating a shared session key, and then using the secret key to encrypt/decrypt the multicast shared information. A protocol that involves user authentication and key establishment can provide conformance security requirements mentioned above referred to as authenticated key exchange protocol.

Several of widely used key agreement protocols are based on the assumption that discrete logarithm problem is indeed hard to be solved. Recently, new key agreement protocols based on the bilinear pairing from elliptic curve cryptosystem are proposed. However, most of these protocols still suffer from some type of attacks, such as insider and key-compromise impersonation attacks that are similar to the attacks on current co-allocation model. Moreover, the communication round for n entities is $\log_3 n$ in these protocols, which is proportional to the number of participants. The proposed secured multi-party key agreement protocol based-on Weil pairing with authentication [30] can conquer the security problems and just need two communication rounds. Thus, it provides a faster and more efficient method for key generation.

In this paper, we present a certificate-based authentication hybrid broker model using multi-party key agreement for secure communication on file transfer in Data Grids. This is a new approach for combining multi-party key agreement and hybrid service broker model based on the proposed ARAM+ co-allocation model. We design and implement a resource-oriented broker agent with authorization and authentication to enhance the function of service broker in ARAM+ model. When the service broker queries available resources and gets replica locations from resource information services and replica management service, it will then choose the best suitable sites for the application requirements from the candidate file servers. Next, the requested users and selected resource sites will form a dynamic resource-group, since members can join or leave a group at any time, and groups are organized in real-time according to the availability and workload of various

resources. Subsequently, a secure conference for communication among members of this resource group is initiated by the service broker. Then a conference key using proposed multi-party key agreement is generated as shared common secret key and used for One-Time-Pad encrypted communication data, and a service broker agent is voted by all members of resource-group to take over the work of monitoring jobs processing. This agent is named “resource broker” in the sequel. Using the multi-party key agreement, it is easy to distribute the group key to members whenever there is any change in the group membership (e.g., a new member joins or an existing member leaves).

Our experimental results show that the proposed model can achieve an efficient failure handling for resource sites and provide a dependable performance under various loads of services. Additionally, some possible attacks are discussed for secure communication among the members of resource-group.

The remaining of this paper is organized as follows. In Section 2, we shall describe background and related work. The proposed model is presented in Section 3. Section 4 demonstrates experimental results and performance evaluations. Finally, we offer discussion and concluding remarks in the last section.

The Grid environment for our research is based on the TigerGrid, which consists of more than one hundred processors distributed over ten clusters located at seven educational institutions: Tungs' Taichung MetroHarbor Hospital (TUNG), Tunghai University (THU), National Changhua University of Education (NCUE), National Taichung University (NTCU), Hsiuping Institute of Technology (HIT), National Da_Li Senior High School (DL), Lizen High School (LZSH) and Long Fong Elementary School (LFPS).

2. Background and Related Work

2.1 Co-allocation architecture

The architecture proposed in [8] consists of three main components: an information service, a broker/co- allocator, and local storage systems. Fig. 2 shows co-allocation of data grid transfers, an extension of the basic template for resource management [9, 13] provided by the Globus Toolkit [31]. The Grid Security Infrastructure (GSI) [32, 33] is the portion of the Globus Toolkit that provides the fundamental security services for Data Grids. Applications specify the characteristics of desired data and pass attribute descriptions to a broker. The

broker queries available resources, gets replica locations from the Information Service [2, 3] and Replica Management Service [3], then get lists of physical file locations. Then it will choose the sites that best suitable sites for the application requirements from the candidate file servers and submit them to these select data sites. In addition the resource broker must continually monitor the status of all jobs executing among these file server in order to make the suitable schedule adjustment.

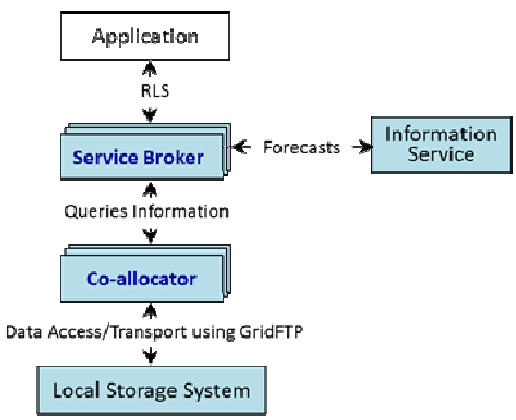

Figure 2. Data Grid co-allocation architecture.

2.2 Anticipative recursively adjusting mechanism plus (ARAM+)

The main idea of Anticipative Recursively-Adjusting Mechanism (ARAM) [16] is to assign transfer requests to selected replica servers according to the finish rates for previous transfers, and adjusts workloads on selected replica servers according to anticipated bandwidth statuses. By continuously adjusting selected replica server workloads, the ARAM scheme measures actual bandwidth performance during data file transfers and regulates workloads by anticipating bandwidth statuses for subsequent transfers according to the finish rates for previously assigned transfers.

Our presented ARAM+ approach is based on the ARAM co-allocation strategy for Data Grid environments, in which TCPBEM and BM is designed and implemented to enhancing the original ARAM algorithm. The system design model has some assumptions illustrated as follows: (1) all grid nodes are installed GlobusToolkit4 previously; (2) all grid nodes are supporting Simple Network Management Protocol (SNMP); (3) the time for transferring, stopping/assigning processes, and calculating TCPBW to selected replica servers is negligible.

2.2.1 Anticipative recursively adjusting mechanism plus (ARAM+)

ARAM+ continually adjust the workloads of all selected replica servers by measuring actual bandwidth performance and detecting TCP throughputs and packet lost rates between grid nodes via TCPBEM during data file transfers. The alpha values

have been adapted for subsequent transfer sections according to previous job finish rates. Simultaneously, faster servers get double or even quadruple throughputs via BM enabling. This model also can be more reliable and fair than ARAM and any other scheme.

There are some interesting ideas, such as P2P networks and distributed denial-of-service (DDoS) attacks will be incorporated into in our approach. P2P Network is a high level logical network architecture build over end-user sites interconnected by a physical network infrastructure. It is share based which shares data and downloads in parallel. The performance in data access over the P2P networks is one of the main issues; more numbers of share point get more speedup. Therefore, P2P networking was applied to ARAM+ which pre-selects many candidate replicas from various servers then chooses appropriate servers and allocates only enough workload to fit server capacities. Another typical example is DDoS attacks that occur when multiple compromised systems flood the bandwidth or resources of a targeted system. The multithreading in the BM design comes from DDoS attacks, BM ‘‘floods’’ the target replica server bandwidth to speed up download performance.

Both of our previous works [12, 14, 34], the anticipative recursively adjusting mechanism and recursively adjusting mechanism (ARAM) were based on co-allocation architecture and relied on tuning alpha values by hand to adapt to specific data grid situations. The ARAM+ uses the same strategies, but differs in that alpha values are tuned dynamically.

ARAM+ adapts to real-time network statuses and calculates appropriate alpha α values continually with TCPBEM Total TCPBW, to ensure good download flexibility and to speed up overall performance.

2.2.2 TCP bandwidth estimation model (TCPBEM)

TCP/UDP is one of the core protocols in the Internet protocol suite. TCP provides reliable, in-order delivery of a stream of bytes, making it suitable for applications such as GridFTP file transfers. Parallel TCP sockets is a generic ‘‘hack’’ that improves TCP throughputs during bulk data transfers by opening several TCP connections and striping the data files over them [34]. In practice, it is often unclear how many sockets one needs to open in order to achieve satisfactory throughput, and opening too many connections may be undesirable for various reasons [29, 34, 35, 36, 37]. The TCP Bandwidth Estimation Model [29] as a function to assessing TCP packet loss rate, such as round trip time,

maximum segment size, other miscellaneous parameters, etc

2.2.3 Burst Mode (BM)

Like many network accelerator methods, and multithreading, Burst Mode first splits one huge bandwidth into small pipelines all working at the same time. Burst Mode focuses on the fastest group of servers and can differentiate among the various candidate server network bandwidths. Second, BM chooses the faster one than others. Ultimately, the BM has made single jobs into many.

The k-means simulation results showed that fewer local replica servers are high efficiency than many remote replica servers. Accordingly, the main ideas in Burst Mode are to find the fastest server group, and to make it download via multithreading. BM also deals with cutting blocks properly for various data sets

2.3 Multi-party Key Agreement (MKA) Protocol with Authenticated

A group of users can hold a conference securely over an open network by running a multi-party key agreement (MKA) protocol to generate a common secret key. With the common secret key, data transmission over the internet is protected for confidentiality.

Our proposed MKA protocol for secure teleconferencing is based on Weil pairing which provides both round number and computation efficiency. The details of this protocol are described below.

MKA Protocol with Authenticated

Step 1: Messages exchange (Round 1):

Each U_i, $i = 1, \ldots, n$, chooses a random number x_i, computes $T_i = x_i \cdot Y_i = x_i \cdot (a_i \cdot P)$ and broadcasts T_i and certificates $Cert_i$.

U_i : a participant in a communication round, Where, U_{n+1} is U_1, and U_n is U_0. In each communication round, the initiator has to randomly assign a unique index from $\{1, 2, \ldots, n\}$ for each entity.

a_i : the long-term secret (private) key randomly chosen by U_i.

Y_i : the long-term public key computed by $Y_i = a_i \cdot P$.

P : Let $P \in E/F_p$ be a generator of the group of points with order $q = (p+1)/6$.

$Cert_i$: U_i's long-term

public-key certificate.

x_i : the short-term (ephemeral) secret key randomly chosen by U_i.

T_i : U_i's public messages in this communication round.

Step 2: Messages exchange (Round 2):

Each U_i, $i = 1, \ldots, n$, computes and broadcasts

$X_i = e((Y_{i+1}+T_{i+1}), (Y_{i+2}+T_{i+2}) - (Y_{i-1}+T_{i-1}))^{(a_i + a_i x_i)}$.

X_i : U_i's public messages in this communication round.

Step 3: Key generation:

Each U_i, $i = 1, \ldots, n$, computes K_i as follows:

$K_i = e((Y_{i+1}+T_{i+1}), n(Y_{i-1}+T_{i-1}))^{(a_i + a_i x_i)} \cdot X_i^{n-1} \cdot X_{i+1}^{n-2} \ldots X_{i-2}$

$= e(P, P)^{[(a_n + a_n x_n)(a_1 + a_1 x_1)(a_2 + a_2 x_2) + (a_1 + a_1 x_1)(a_2 + a_2 x_2)(a_3 + a_3 x_3) + \ldots + (a_{n-1} + a_{n-1} x_{n-1})(a_n + a_n x_n)(a_{n+1} + a_{n+1} x_{n+1})]}$

Furthermore, the common shared secret key is then obtained as $K = kdf(K_1 \| U_1 \| U_2 \| \ldots \| U_n) = kdf(K_2 \| U_1 \| U_2 \| \ldots \| U_n) = \ldots = kdf(K_n \| U_1 \| U_2 \| \ldots \| U_n)$, where *kdf* is a key derivation function and string U_i is an unique identifier of entity U_i.

3.The Proposed Model

Our approach is based on the ARAM+ co-allocation model and MKA mechanism for secure communication on file transfer in Data Grids. We exploit a multi-party key agreement protocol to generate shared common secret key which provides a secure authenticated broadcast communication in the dynamic resource-group for the various resources requirement. Based on the hybrid resource broker model, we design and implement a "resource broker" to enhance the decentralized service broker in the ARAM+ co-allocation architecture. This resource broker is voted by all members of the dynamic resource-group and then takes over the works for monitoring the job processing with respect to the responsibility of service broker. The various security attributes required for group communication in our proposed model are discussed.

3.1 The architecture

Once the user's requirements are submitted to the service broker, and then this broker queries available resources and gets replica locations from resource information services and replica management service. Then the sites that best suitable for the resource requirements will be chosen from the candidate data servers. These selected data servers provide the collaborative services and form a dynamic resource-group because of the members can join or leave a group at any time, and groups are organized in real-time according to the availability and workload of various resources. Subsequently, a secure conference for communication among members of this resource group is initiated by the service broker. Then a conference key using proposed multi-party key agreement is generated as shared common secret key used for One-Time-Pad encrypted communication for the specific file requirement. Then a resource broker agent is voted by all members of resource-group to take over the work of resource to monitor jobs processing. Here, one member may belong to multiple groups simultaneously. Thus, the following challenges must be considered: how to authenticate the group members, how to generate the group key for encrypting the communication message, how to exchange information securely and how to against the various attacks. The architecture is shown as in Fig. 3.

3.2 The Certificate-based Authentication Hybrid Broker Model using Multi-party Key Agreement

3.2.1 Assumptions

Some assumptions for the proposed model are described as below:

- Each resource site just belongs to one grid.
- The request resources sites may belong to different grids.
- In each grid, there is a Certificate Authority (CA) which issues the certificates for hosts, users and services when they are first registered to the grid system.

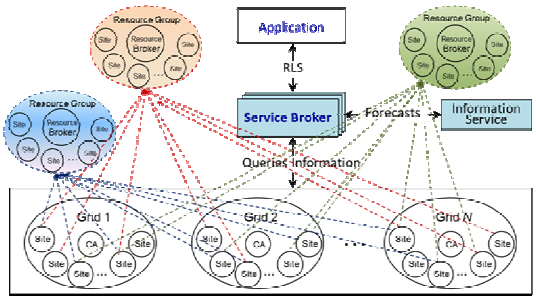

Figure 3. The architecture of certificate-based authentication hybrid broker model.

3.2.2 Algorithm

Based on the above architecture design, the hybrid resource broker algorithm with authentication for redundant parallel file transfer in Data Grids is illustrated as follows:

Step 1: A user submits a request for a certain file service to the replica location service (RLS), and then the service broker will receive the request including applications specify the characteristics of desired data.

Step 2: The service broker queries available resources and gets replica locations from resource information services and replica management service.

Step 3: The service broker chooses the sites that best suitable for the application requirements from the candidate file servers and submits the request to them.

Then the requestor and these selected resource sites will form a dynamic resource-group.

Step 4: A conference for dynamic resource-group is initiated by the service broker.

Step 5: A conference key using proposed multi-party key agreement is generated as shared common secret key and used for One-Time-Pad encrypted communication data, and a resource broker is voted by all members of resource-group to take over the work of monitoring jobs processing.

Then the communication message will be encrypted by this key for privacy.

Step 6: The file transfer will be performed using ARAM+ model.

Step 7: The service broker will pass a message to RA when file transfer is finished.

4.Experimental Results and Performance Analyses

The network model for our experiments is the Tiger grid (Fig. 4), which consists of more than one hundred

processors distributed over ten clusters located at seven educational institutions: Tungs' Taichung MetroHarbor Hospital (TUNG), Tunghai University (THU), National Changhua University of Education (NCUE), National Taichung University (NTCU), Hsiuping Institute of Technology (HIT), National Da_Li Senior High School (DL), Lizen High School (LZSH) and Long Fong Elementary School (LFPS).

They are interconnected by the 1 Gbps Taiwan Academic Network (TANET). The Tiger grid platform is built around 60 computing sites, more than 224 CPUs with differing speeds, and total storage of more than 5 TB. All the institutions are in Taiwan, at least 10km from THU. All machines have Globus 4.0.7 or above installed. We performed wide-area data transfer experiments using Cyber Transformer, our GridFTP GUI client tool, on our co- allocation testbed at Tunghai University (THU), Taichung City, Taiwan, and fetched files from replica servers at National Da-Li Senior High School (DL), Li-Zen High School (LZ), Tungs' Taichung Metro Harbor Hospital (TUNG), and Hsiuping Institute of Technology School (HIT). These institutions are all in Taichung, Taiwan, 10–30km from THU.

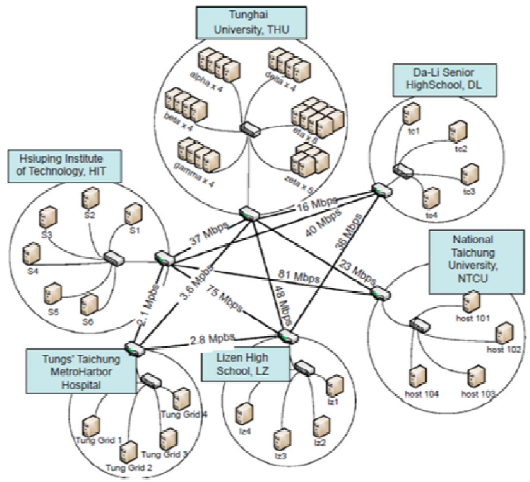

Figure 4. Tiger grid network.

Experimental results show that our approach can achieve an efficient failure handling for resource sites and provides a dependable performance under various loads of services. Moreover, the secure intra-grid communication against internal attacks is another important issue, in which some possible attacks are discussed for secure intra-grid communication and file transfer. The experimental results for single point of failure and bottleneck are also illustrated as follows.

4.1 Attacks

Since GSI can achieve mutual entity authentication between user and resource for co-allocation architectures in Data Grids. Therefore, user and resource have identity certificates which are under the

organization of the standard certificate-based X.509. This kind of security is secure for inter-grid communication, but the secure for intra-grid communication against internal attacks is another crucial issue. The secure multi-party key agreement protocol should withstand both passive and active attacks. Passive attackers steal useful information by eavesdropping and/or performing traffic analysis. Active attacks interfere with legal communication and are typically in the forms of masquerading, replaying, modification, and denial of services (DOS). Our approach can against these attacks utilize encryption/decryption for confidentiality, message authentication code for integrity, certificate and access control for authentication.

4.1.1 Passive attacks

A passive attack is that there is an adversary who is not a participant who tries to compute the common shared secret key by listening to the broadcast messages among the legal participants. If a multi-party key agreement protocol is secure against passive adversary, a passive adversary is unable to obtain information about the common shared secret key by eavesdropping messages transmitted over the broadcast channel.

We use the bilinear Diffie-Hellman problem assumption to prove our protocol is secure against passive adversary. The similar technique is used in literatures such as Boneh's scheme. We say that passive adversary cannot work under the assumption that solving the bilinear Diffie-Hellman problem (BDHP) will be infeasible.

The definition of BDHP is to compute $\hat{e}(P, P)^{abc}$ by given (P; aP; bP; cP). That is, given $T_1 = x_1P$, $T_2 = x_2P$, $T_3 = x_3P$, and x_1, x_2, x_3 are randomly chosen from Z, the two tuples of random variables, (T_1, T_2, T_3, $\hat{e}(P, P)^{x_1x_2x_3}$) and ($T_1$, T_2, T_3, T), where T is a random value in μ_q, are *computationally indistinguishable*. In other words, there is no efficient algorithm $\boldsymbol{A}$ satisfying

$\left|\Pr[\boldsymbol{A}\ (x_1P,\ x_2P,\ x_3P,\ \hat{e}(P,\ P)^{x_1x_2x_3}) = true]\right| - \left|\Pr[\boldsymbol{A}\ (x_1P,\ x_2P,\ x_3P,\ T\ ) = true]\right| > \frac{1}{Q(|q|)}$ for any polynomial Q, where the probability is over the random choice of x_1, x_2, x_3 and T.

If E intends to compromise K_i (equals to $e((Y_{i+1}+T_{i+1}), n(Y_{i-1}+T_{i-1}))^{(a_i+a_ix_i)} \cdot X_i^{n-1} \cdot X_{i+1}^{n-2} \cdot \cdot X_{i-2}$) in the authenticated protocol, she needs to compute $T=e((Y_{i+1}+T_{i+1}),$

$n(Y_{i-1}+T_{i-1}))^{(a_i+a_ix_i)}$ (equals to $\hat{e}(P, P)^{n(a_{i-1}+a_{i-1}x_{i-1})\ (a_i+a_ix_i)\ (a_{i+1}+a_{i+1}x_{i+1})}$), and $X=X_i^{n-1}\cdot X_{i+1}^{n-2}\cdot\ \cdot\ X_{i-2}$, where T, $X \in \mu_q$, and then obtains $K_i=T\cdot X$. We assume that she can compute the value of X from the public messages X_i's. However, she cannot compute correctly a_i and a_ix_i form the public $X_i = e((Y_{i+1}+T_{i+1}), (Y_{i+2}+T_{i+2}) -(Y_{i-1}+T_{i-1}))^{(a_i+a_ix_i)}$. Without correct a_i and a_ix_i, she cannot compute $T = e((Y_{i+1}+T_{i+1}), n(Y_{i-1}+T_{i-1}))^{(a_i+a_ix_i)}$. Because that she faces the hardness of the BDHP problem for the pair of groups G_q , μ_q: To compute $T = e((Y_{i+1}+T_{i+1}), n(Y_{i-1}+T_{i-1}))^{(a_i+a_ix_i)}$ by given P, $(a_{i-1} + a_{i-1}x_{i-1})P$, $(a_i + a_ix_i)P$ and $(a_{i+1} + a_{i+1}x_{i+1})P$, with that a_{i-1}, a_i, a_{i+1}, x_{i-1}, x_i and x_{i+1} are chosen randomly. That is, the two tuples of random variables $((Y_{i-1}+T_{i-1}), (Y_i+T_i), (Y_{i+1}+T_{i+1}), \hat{e}(P, P)^{n(a_{i-1}+a_{i-1}x_{i-1})\ (a_i+a_ix_i)\ (a_{i+1}+a_{i+1}x_{i+1})})$ and $((Y_{i-1}+T_{i-1}), (Y_i+T_i), (Y_{i+1}+T_{i+1}), T)$, where T is a random value in μ_q, are *computationally indistinguishable*. In other words, there is no efficient algorithm $\boldsymbol{A}$ satisfying

$$\left|\Pr[\boldsymbol{A}((a_{i-1}+a_{i-1}x_{i-1})P, (a_i+a_ix_i)P, (a_{i+1}+a_{i+1}x_{i+1})P, \hat{e}(P, P)^{n(a_{i-1}+a_{i-1}x_{i-1})\ (a_i+a_ix_i)\ (a_{i+1}+a_{i+1}x_{i+1})}) = true] - \Pr[\boldsymbol{A}((a_{i-1}+a_{i-1}x_{i-1})P, (a_i+a_ix_i)P, (a_{i+1}+a_{i+1}x_{i+1})P, T) = true]\right| > \frac{1}{Q(|q|)}$$

For any polynomial Q, where the probability is over the random choice of x_{i-1}, x_i, x_{i+1} and T. Therefore, she cannot compute easily the correct K_i.

4.1.2 Active attacks

An active attack is a dishonest participant who tries to disrupt the establishment of a common key among all of the participants. An active adversary can fool an honest participant into believe that he has computed the same common key as the other honest participants do. Our approach is secure against active attacks which are analyzed as follows:

- Known-key security: An entity in each run of the protocol computes a new ephemeral private keys x_i to generate a unique session key. Thus, the knowledge of a previous key does not help in deducing a new key.
- Forward secrecy: Suppose that an adversary has compromised one or more long-term private keys a_i. However, he cannot compute a previously established session key $K_i = e((Y_{i+1}+T_{i+1}), n(Y_{i-1}+T_{i-1}))^{(a_i+a_ix_i)}\cdot X_i^{n-1}\cdot X_{i+1}^{n-2}\cdot\ \cdot\ X_{i-2}$ without knowing the ephemeral private key x_i.

- Key compromise impersonation resilience: The key-compromise impersonation attack means that the attacker E who has compromised the long-term private key of one entity U_i would not only impersonate the compromised entity but also impersonate any other one to fool the compromised entity. For example, an outsider attacker E, who has compromised U_1's static private key a_1, can also impersonate the other entities to fool U_1. Suppose that E who impersonates U_2 to fool U_1 can then forge a message $T_2' = u \cdot P$. Then E broadcasts $\{T_2', Cert_2\}$ and claims that it is sent by U_2, where u is chosen by E. Now, U_1 will compute $K_1 = e((Y_2+T_2), n(Y_n+T_n))^{(a_1+a_1x_1)} \cdot X_1^{n-1} \cdot X_2^{n-2} \cdot \cdot \cdot X_{n-1} = e(P, P)^{[(a_n+a_nx_n)(a_1+a_1x_1)(a_2+u)+ (a_1+a_1x_1)(a_2+u)(a_3+a_3x_3) + \cdots + (a_{n-1}+a_{n-1}x_{n-1})(a_n+a_nx_n)(a_{n+1}+a_{n+1}x_{n+1})]}$. However, E cannot compute $K_2' = e((Y_3+T_3), n(Y_1+T_1))^{(a_2+u)} \cdot X_2^{n-1} \cdot X_3^{n-2} \cdot \cdot \cdot X_n$ (equals to $e((Y_3+T_3), n(Y_2+T_2))^{(a_1+a_1x_1)} \cdot X_2^{n-1} \cdot X_3^{n-2} \cdot \cdot \cdot X_n$). It fails because she does not know the correct value of a_2 or a_1x_1. The proposed protocol provides the property of key-compromise impersonation resilience.
- Insider attack: Assume insider B fools A into accepting the C's forged messages, and let A believe that C participates in the protocol run. Suppose that B, who impersonates C to A, can then forge the message $T_C' = w \cdot P$ and compute $m_C' = H(w)$, $s_C' = (w)^{-1}(m_C'+c')$ mod q. Then B broadcasts $\{T_C', Cert_C, m_C', s_C'\}$ as C's messages, where w is chosen by B. Then A verifies B's forged messages and found the error. That is, B cannot forge C's message without the long-term private key c. Therefore, B cannot masquerade C to A. The attack fails because every message is authenticated.
- Unknown key-shared resilience: The identity of a participant is included in the key derivation function of our proposed protocol. It provides unknown key-shared resilience as well as public-key substitution unknown key-shared attack.
- No key control: Each entity in a run of the protocol chooses a new ephemeral private keys x_i to generate a unique session key. In our protocol, no participant does control and predict the value of a common session key.

4.2 The single point of failure

Our proposed approach utilizes the light broker instead of the resource broker when the jobs are submitted to the resource group. One of responsibility of light broker is recursively adjusting mechanism works by continuously adjusting each replica server's workload to correspond to its real-time bandwidth during file transfers. An experiment and a case design were devised to test single point of failure for the resource broker.

We design one scenario to verify the efficiency of enabling light broker while the resource broker is failure. We make a failure simulation by using shutdown for resource broker at regular intervals, for example 5, 10, 20 minutes in experiment. The experimental results show that all file transfers can be finished for the file requirements submitted to resource group before a resource broker is fail to operate. The reason for it is that the light broker takes over the work for monitoring the job processing when the jobs are submitted to the resource group.

4.3 The bottleneck

We designed two scenarios to evaluate the effect of light broker for solving the bottleneck problem. Details of the test cases we designed are described and shown as follows.

4.3.1 Average transfer time

Our test data are applied on the ARAM+ without decentralized mechanism and our approach, respectively. It takes about 100 seconds of average transfer time for ARAM+. It takes about 2 seconds of average transfer time for our approach. The reason for this result is that in ARAM+, resource broker provides capabilities such as service allocating, resource discovery, job scheduling, job monitoring and data access to users' application. That is the resource broker must continually monitor the status of job executing until final file block have been delivered. Therefore, its workload is heavy. However, our approach presents the light broker to share the workload of resource broker. Hence Overall performances for average transfer time in this scenario have obviously been improved.

4.3.2 Network communication

Similarly, the test data are applied on the ARAM+ and our approach, respectively. Data for experiments is set with as below:

- Each request file size equals to 4G.

- Each file is divided into 400 disjoint transfer blocks of size equals to 10 MB.

Under the assumption, it takes about 800 network communications between file server and resource broker for each block transfer. The reason for this result is that the resource broker must assign the block transfer to a file server and receipt the message when the block has been transferred. But our proposed light broker can actually share this network communication loads.

5.Conclusions

Co-allocation architectures can be used to enable parallel transfers of data file from multiple replicas in data grids which are stored at different grid sites. Schemes including our previous proposed ARAM+ co-allocation model provides capabilities such as service allocating, resource discovery, job scheduling, job monitoring and data access to users' application. However, the challenges of co-allocation architectures; however, usually lie in the secure intra-grid communication against internal attacks. Due to the high dynamic nature of group members in Data Grids, how to update group key efficiently and effectively becomes a critical problem.

In this paper, we present a new certificate-based authentication hybrid broker model using multi-party key agreement for secure communication on file transfer in Data Grids which integrates multi-party key agreement and hybrid service broker model into ARAM+ model. We design and implement a resource-oriented broker agent with authorization and authentication to enhance the function of service broker in ARAM+ model. First, a secure conference for communication among members of dynamic resource group is initiated by the service broker. Then a conference key is generated as shared common secret key and used for One-Time-Pad encrypted communication data, and a service broker agent is voted by all members of resource-group.

Our experimental results show that the proposed model can achieve an efficient failure handling for resource sites and provide a dependable performance under various loads of services. Moreover, the secure intra-grid communication against internal attacks is another important issue, in which both passive and active attacks can be provided for secure intra-grid communication and file transfer.

References

[1] Allcock B, Bester J, Bresnahan J, Chervenak A, Foster I, Kesselman C. et al. Data management and transfer in high-performance computational grid environments. Parallel Computing 2002;28:749–771.

[2] Czajkowski K, Foster I, Kesselman C. Resource co-allocation in computational grids. In: Proceeding of the 8th IEEE international symposium on high performance distributed computing (HPDC-8 ’99), August 1999.

[3] Czajkowski K, Fitzgerald S, Foster I, Kesselman C. Grid information services for distributed resource sharing, In: Proc.10th IEEE international symposium on high-performance distributed computing (HPDC-10 ’01), August 2001.

[4] Foster I, Kesselman C, Tuecke S. The anatomy of the grid: enabling scalable virtual organizations. In: Proceedings of the first IEEE/ACM international symposium; 2001. p. 200–22.

[5] Hoschek W, Jaen-Martinez J, Samar A, Stockinger H, Stockinger K. Data manage- ment in an international data grid project. In: Proceedings of the first IEEE/ ACM international workshop on grid computing, Bangalore, India; 2000.

[6] Foster I, Kesselman C. Globus: a metacomputing infrastructure toolkit. International Journal of High Performance Computing Applications 1997;11:115–28.

[7] Stockinger H, Samar A, Allcoc B, Foster I, Holtman K, Tierney B. File and object replication in data grids. Cluster Computing 2002;5:305–314.

[8] Vazhkudai S, Schopf J. Using regression techniques to predict large data transfers, International Journal of High Performance Computing Applications 2003;17:249–68.

[9] Vazhkudai S, Schopf J. Predicting sporadic grid data transfers. In: Proceedings of the 11th IEEE international symposium on high performance distributed computing (HPDC-11 ’02); 2002. p. 188–96.

[10] Yang L, Schopf J, Foster I. Improving parallel data transfer times using predicted variances in shared networks. In: Proceedings of the 5th IEEE international symposium on cluster computing and the grid (CCGrid ’05); 2005. p. 734–42.

[11] Zhang X, Freschl J, Schopf J. A performance study ofmonitoring and information services for distributed systems, In: Proceedings of the 12th

IEEE international symposium on high performance distributed computing (HPDC-12 '03); 2003. p. 270–82.

[12] Yang CT, Yan IH, Li KC, Wang SY. Improvements on dynamic adjustment mechanism in co-allocation data grid environments. The Journal of Supercomputing 2007;40:269–80.

[13] Vazhkudai S, Tuecke S, Foster I, Replica selection in the globus data grid, In: Proceedings of the first international symposium on cluster computing and the grid (CCGRID 2001); 2001. p. 106–13.

[14] Wang CM, Hsu CC, Chen HM, Wu JJ. Efficient multi-source data transfer in data grids, In: Proceedings of the 6th IEEE international symposium on cluster computing and the grid (CCGRID '06); 2006. p. 421–24.

[15] Mathis M, Semke J, Mahdavi J, Ott T, The macroscopic behavior of the TCP congestion avoidance algorithm. Computer Communication Review 1997;27.

[16] Yang C., Chi YC, Han TF, Hsu CH. Redundant parallel file transfer with anticipative recursively-adjusting scheme in data grids, In: distributed and parallel computing, 7th international conference on algorithms and architectures for parallel processing, ICA3PP 2007, Lecture Notes in Computer Science; 2007. p. 242–53.

[17] Padhye J, Firoiu V, Towsley D, Kurose J. Modeling TCP throughput: a simple model and its empirical validation, In Proceedings of the ACM SIGCOMM '98 conference on Applications, technologies, architectures, and protocols for computer communication; 1998. p. 303-14.

[18] Azab AA, Kholidy HA. An adaptive decentralized scheduling mechanism for peer to peer Desktop Grids, In: Proceedings of international conference on computer engineering & systems; 2008. p. 364–71.

[19] Casanova H, Obertelli G., Berman F, Wolski R. The AppLeS parameter sweep template: User-level middleware for the grid, In: Proceedings of ACM/IEEE conference on Supercomputing (SC'00), Dallas, TX, IEEE CS Press, Los Alamitos, CA, USA, 2000.

[20] Frey J, Tannenbaum T, Livny M, Foster I, Tuecke S, Condor-G S. A Computation Management Agent for Multi-Institutional Grids, Cluster Computing 2002;5:237–46.

[21] Venugopal S, Buyya R, Winton L. A Grid Service Broker for Scheduling e-Science Applications on Global

Data Grids, Concurrency and Computation: Practice and Experience 2006;18:685-99.

[22] Haji MH, Gourlay I, Djemame K, Dew PM. A SNAP-based community resource broker using a three-phase commit protocol: A performance study, The Computer Journal 2005;48:333-46.

[23] Dias M, Nadiminti K., Venugopal S, Ma T, Buyya R. An integration of global and enterprise grid computing: Gridbus broker and Xgrid perspective, In: Proceedings of the 4th International Conference on Grid and Cooperative Computing (GCC 2005), Beijing, China, LNCS, Springer-Verlag, Berlin, Germany; 2005.

[24] Dumitrescu C, Raicu I, Foster I. DI-GRUBER: A Distributed Approach to Grid Resource Brokering, In: Proceedings of ACM/IEEE conference on Supercomputing, Seattle, WA, IEEE CS Press, Los Alamitos, CA, USA; 2005.

[25] Baru C, Moore R, Rajasekar A, Wan M. The SDSC Storage Resource Broker, In: proceedings of the conference of the centre for advanced studies on collaborative research, 1998.

[26] Hoschek W, Jaen-Martinez J, Samar A, Stockinger H, Stockinger K. Data Management in an International Data Grid Project, In: Proceedings of 1st International Workshop on Grid Computing (Grid 2000, Bangalore, India), Springer-Verlag, Berlin, Germany; 2000.

[27] Abramson D, Giddy J, Kotler L. High Performance Parametric Modeling with Nimrod/G: Killer Application for the Global Grid, I In: Proceedings of the International Parallel and Distributed Processing Symposium (IPDPS 2000); 2000.

[28] Yang CT, Yang MF, Chiang WC. Enhancement of anticipative recursively adjusting mechanism for redundant parallel file transfer in data grids, In: Proceedings of the14th IEEE International Conference on Parallel and Distributed Systems; 2009. p. 834–45.

[29] Hacker TJ, Athey B, Noble B. The end-to-end performance effects of parallel TCP sockets on a lossy wide-area network, parallel and distributed processing symposium. In: Proceedings of the 16th International Parallel and Distributed Processing Symposium; 2006.

[30] Lin CH, Lin HH, Chang JC. Multi-party Key Agreement for Secure Teleconfernecing, In In: Proceedings of the IEEE International

Conference on Systems, Man, and Cybernetics (SMC 2006); 2006. p. 3702–07.

[31] Foster I, Kesselman C. Globus: A Metacomputing Infrastructure Toolkit, International Journal of Supercomputer Applications 1998;11:115-29.

[32] Butler R, Engert D, Foster I, Kesselman C, Tuecke S, Volmer J, Welch V. A National-Scale Authentication Infrastructure, Journal of Computers 2000;33:60-66.

[33] Foster I, Kessekan C, Tsudik G, Tueckel S. A security architecture for computational grids, In: Proceedings of the 5th ACM Conference on Computer and Communications Security; 1998.

[34] Yang CT, Chen CH, Li KC, Hsu CH. Performance analysis of applying replica selection technology for data grid environments, Lecture Notes in Computer Science, Berlin: Springer 2005;3603: 278–87.

[35] Altman E, Barman D, Tuffin B, Vojnovic M. Parallel TCP sockets: simple model, throughput and validation, Parallel TCP sockets: simple model, throughput and validation. In: Proceedings of the 25th IEEE International Conference on Computer Communications; 2006. p. 1–12.

[36] Bolliger J, Gross T, Hengartner U. Bandwidth modelling for network-aware applications. In: 18th Annual Joint Conference of the IEEE Computer and Communications Societies; 1999. p. 1300–09.

[37] Padhye J, Firoiu V, Towsley D, Kurose J. Modeling TCP throughput: a simple model and its empirical validation, In: Proceedings of the ACM SIGCOMM '98 conference on Applications, technologies, architectures, and protocols for computer communication; 1998. p. 303–114.