ASAMO: Authentication and Secure Communication using Abstract Monitoring Objects for Mobile Grid Computing

Parveen Begam H¹, Maluk Mohamed M A²

Software Systems Group, M.A.M College of Engineering, Tiruchirappalli, India
¹²ssg_parveen@mamce.org; ²ssg_malukmd@mamce.org

Abstract

The prominent feature of mobile grid computing is the collaboration of multiple entities to perform collaborative tasks using mobile devices. Currently, most of the security solutions for mobile grid environment use static set of algorithms and protocols. Despite the increased usage of mobile computing, exploiting its full potential is difficult due to its inherent problems such as resource scarcity, frequent disconnections, and mobility. Our focus is to provide security and efficient power management. In this paper, a framework of dynamic secure routing protocol called Select Successive Hop Routing (SSHR) algorithm using Abstract Monitoring Objects (AMOs), Secure Service Certificates (SSC), and layer based encryption for each data transfers to improve the security level, anonymity and dynamicity of the data are proposed. This includes (i) Authentication of the mobile node (ii) Security flow between mobile nodes (iii) Saving battery power (iv) Hand-over of authentication information. The proposed framework solves the issues like asymmetry in network connectivity, computing power and mobility. The outcome is compared with certain existing security protocols and demonstrates how the proposed protocol is able to adapt itself over different conditions of the mobile device, and how it can provide a performance gain in the execution.

Keywords

Mobile Grid Computing; Authentication; Secure Communication; Secure Routing; Digital Signature; ECDSA.

Introduction

Mobile Grid computing extends the traditional Grid computing paradigm to include a diverse collection of mobile devices that communicate using radio frequency, infrared, optical and other wireless mechanisms. The prominent feature of mobile grid computing is the collaboration of multiple entities to perform collaborative tasks using mobile devices that rely on two fundamental functions: communication and resource sharing. The fundamental function is to enrich one another and provide new solutions that solve many of the limitations and problems found in different technologies, such as reduced CPU performance, limited secondary storage, heightened battery consumption sensitivity, and unreliable low-bandwidth communication. Although the individual computing devices may be resource-limited in isolation, as an aggregated sum, they have the potential to play a vital role within grid computing.

Security is a very important factor in mobile grid Computing and is also difficult to achieve owing to the open nature of wireless networks and heterogeneous and distributed environments. Since Internet is not security-oriented by design, there exist various threats, in particular, malicious internal and external users. Securing communication and fine-tuning controlling access to shared resources are the important issues for mobile grid services. Currently, most of the security solutions for the mobile grid environment use a static set of algorithms and protocols. The countermeasures against threats utilize encryption/decryption for confidentiality, message authentication code for integrity, digital signature for authentication, undeniable digital signature for non-repudiation, access control for authorization, and intrusion detection/defense for availability/DOS. The Internet-based grid computing encounters similar threats and involves all the security requirements discussed above. As a result, the threats to the mobile grid systems may become more serious and defending them becomes more difficult. For instance, centralized authentication is generally unavailable and multipletsite co-authentication is difficult to implement due to the distributed and heterogeneous features of grid computing systems. Thus, the Single-Sign-On authentication comes into play. As long as communication and information exchange is conducted over the Internet, communication messages should be encrypted to provide confidentiality.
Initially, the integration of mobile wireless consumer devices into the Grid, seems unlikely, due to the inherent limitations typical of mobile devices such as reduced CPU performance, limited secondary storage, heightened battery consumption sensitivity, and unreliable low-bandwidth communication. However, the millions of laptops and PDAs sold annually suggest that this untapped abundance should not be prematurely dismissed. Given that the benefits of combining the resources of mobile devices with the computational grid are potentially enormous, one must compensate for the inherent limitations of these devices in order to utilize them successfully in the Grid. The research challenges arising from this problem, propose the vision of a potential architectural solution. Proxy-based, clustered system architecture with favorable deployment, interoperability, scalability, Adaptivity, and fault-tolerance characteristics as well as an economic model to stimulate future research in the emerging field has been suggested.

A survey of the current state of wireless grid computing, includes a discussion of the cooperation between wired and wireless grids, including ways in which wireless grids extend the capabilities of existing wired grids. It also discusses many of the new capabilities and resources available to wireless grid devices and a sampling of several applications of these new resources. It provides a sampling of many current research endeavors in the wireless grid arena and an examination of a number of the potential challenges resulting from the unique characteristics of wireless grid devices.

The Surrogate Object (SO) is a software entity that acts as a representative of a particular Mobile Host (MH) in the wired network and maintains application specific data structures and methods. The major advantages of using a surrogate object are: Maintaining location information about each mobile device, acting as a place-holder that can realize local caching for faster information access, handling message delivery for the MH, when it is out of reach from the MSS and acts as data sink that can collect data from diverse sources and delivering appropriate data to the MH depending upon the current position of the mobile devices to progress in a mobile grid environment in a secured manner. It is very important that the downstream node may or may not be malicious to provide secure communication.

A development methodology for Secure Mobile Grid Systems is proposed in which the security aspects are considered from the first stages of the life-cycle and in which the mobile Grid technological environment is always presented during each activity. The analysis activity, in which the requirements (focusing on the grid, mobility and security requirements) of the system are specified and driven by reusable use cases through which the requirements and needs of these systems are defined. These use cases have been defined through a UML-extension for security use cases and Grid use cases which capture the behavior of these kinds of systems.

Mobile cloud computing can address some security problems by executing mobile applications on resource providers external to the mobile device. An extensive survey of mobile cloud computing research, while highlighting the specific concerns in mobile cloud computing, will be done. The paper is concluded with a critical analysis of challenges that have not yet been fully met.

The security service, which works as a middleware, with the ability to dynamically change the security protocols used between two peers, is proposed. These changes can occur based on variations on wireless medium parameters and system resource usage, available hardware resources, application-defined QoS metrics, and desired data “security levels”. The compared solution to certain widespread static security protocols demonstrates how the middleware is able to adapt itself over different conditions of medium and system, and how it can provide a performance gain in the execution of cryptographic primitives, through the use of data semantics.

The security support for a middleware framework supporting Mobile Grid Services is proposed. Mobile Grid Services, the extension of the original static Grid services, are characterized by the ability of being able to move from nodes to nodes during execution. By combining an existing mobile agent system (JADE) and a generic grid system toolkit (Globus), the Mobile Grid Services framework is achieved. Security is a critical issue when deploying Mobile Grid Services to the real-world applications, where the resources of the services must be protected in potentially hostile environments. The Mobile Grid Services Framework is not practical, if no security measures are provided. The details of security mechanisms consisting of authentication, authorization, message integrity and confidentiality, agent permission and agent protection as well as their realization in the MGS API are presented.
In this paper, a framework of secure routing protocol using Abstract Monitoring Objects (AMOs), Secure Service Certificates (SSC) and layer based encryption in each mobile device to improve the security level and dynamicity of the data is proposed. The Surrogate Object (SO) is a software entity that acts as a representative of a particular Mobile Host (MH) which helps in storing the service certificates and also in solving issues like asymmetry in network connectivity, computing power and mobility. In wireless environment, the downstream node may be authorized or malicious. ECDSA (Elliptic Curve Digital Signature Algorithm) is used for anonymous communication with the receiver and the encryption of sender’s information to maintain the secrecy of the message. Usage of hop to hop TTL increases the reliability and time constraints of the message. The proposed system overcomes the existing security related drawbacks upto a certain extent.

The rest of the paper is organized as follows. Section 2 describes the importance of security in a mobile grid environment over which the Abstract Monitoring Object (AMO) model has been built to provide effective authentication and secure communication. Section 3 describes the AMO model in detail, including Secure Service Certificates, Layered Routing. Section 4 analyzes security-related measures, robustness and complexity of the proposed architecture. Section 5 compares the performance with some existing methods. Section 6 concludes the paper and provides directions for future research.

**Brief Overview of the Security Issues in Mobile Grid**

Security is a very important factor in Mobile Grid Computing and is also difficult to achieve, owing to the open nature of wireless networks and heterogeneous and distributed environments. In a distributed job execution environment, the potential risks rise for both the integrity of the application and the resource provider. The prime motivation of combining the mobile and grid computing is to carry out the user’s work while on move. Due to various constraints to the wireless network, the environment and the user may rapidly change their environment from stationary to mobile and location dependent. The combination of mobile and the grid may lead to a lot of security issues like authentication of a mobile node and mobile code, prevention of attacks in the base station, secure communication between two mobile nodes, communication cost of constructing the session keys and computing complexity of authenticity and security. Particularly in a mobile grid environment, some of the risks like the integrity of processing results are compromised by malicious mobile node, unnecessary free riding of MN without contributing the resources which in turn reduces the system utility, spoiling the data confidentiality, destruction of files and applications by malicious mobile code and acting as owner are to be solved. Providing a countermeasures for the security issues is crucial.

The countermeasures under investigation include the authentication, confidentiality, secure communication, access control and so on. In each situation, our aim is to balance functionality, performance and security while achieving solutions and without imposing restrictions (e.g. increased power consumption) on the personal use of a mobile device. In order to provide security in a holistic manner, a new and efficient dynamic secure routing for mobile grid environments with the help of secure service certificates and Abstract Monitoring Objects along with layered routing for mobile grid computing is proposed. It is as follows.

**The Proposed Security Object-based Model**

The supervisory host model for mobile grid systems defines an architecture that helps in generating the Secure Service Certificates (SSC) and digital signatures for mobile hosts to have efficient security and power management. Some of the existing methods to generate digital signatures and certificates are Symmetric or Asymmetric algorithms, Identity based algorithms, biometric-based algorithms. In the existing systems, mobile hosts depends on Certificate Authority (CA) for generation of certificates using various certificate generation methods. Issues arise when the CA becomes malicious and when it consumes more battery power. The focus is to provide security and power management, this includes (i) Authentication of a mobile node - achieved by providing certificates with digital signature stored in the Surrogate Object(SO), (ii) Security flow between two mobile nodes - achieved by providing layered routing to the original data and preventing it from hackers, (iii) Saving the battery power - achieved by introducing a Supervisory Host (SH) (a static node located at Mobile Support Station (MSS) of each Mobile Grid Network (MGN) and it takes care of certificate generation and signing) and (iv) Hand-over of authentication information - done using ECDSA.
which has 168 bit key size which is far less when compared to RSA algorithm. The introduction of SH will enhance the security, anonymity and power consumption.

Certificate Generation

Any mobile node (MHi) entering into Mobile Grid Network (MGNi) should perform single sign-on process for authentication. A node (say MHs) from one grid establishing communication with other node (MHd) in another grid, must notify the receiver that it is an authenticated mobile node. To achieve this, the Secure Service Certificate (SSC) is used. Figure 1 explains the certificate generation process with the help of supervisory host which resides in the base station. The mobile node which communicates with another node, firstly requests for the public key to the common (public key information) pool of that grid network. The pool is a database with a collection of public keys of all the mobile grid nodes that exists in Mobile Station Subsystem (MSS). After receiving the public key, the mobile host prepares the necessary components to generate its Secure Service Certificate. The mobile host sends those components to the Supervisory Host (SH). The Supervisory Host is a special host residing in static environment generating a digital certificate and sending it to the mobile grid node. After verification, the certificate is accepted by mobile node. There are individual Supervisory Hosts for each individual mobile grid network (MGNi).

![FIG. 1 CERTIFICATE GENERATION PROCESS USING SUPERVISORY HOST](image)

The Mobile Host issues the necessary components to SH in an encrypted format. After receiving the contents, SH starts generating the certificate along with a digital signature with the help of sender’s and receiver’s public key. Figure 2 shows the Secure Service Certificate model. The components of the certificate are: serial number, certificate identifier algorithm, issuer’s unique id, validity period, subject id, subject public key, algorithm identifier, TTL and Nonce. (IDs||TTL||Kpu(s)||IDd||N1). Certificate identifier algorithm helps to identify the encryption algorithm in which the certificate has been encrypted. Issuer’s unique id is the identity of the supervisory host. The validity period is the time for which the certificate is valid. Subject id is the id of the receiver. Subject public key is receiver’s public key. The sender node communicates with the receiver using this public key. Algorithm identifier is a type of algorithm where the data are encrypted. Finally, SH makes a copy of the SSC and sends it to the corresponding mobile node.

![FIG. 2 SECURE SERVICE CERTIFICATE MODEL](image)

Authentication

1) Storage of Certificate in SO

After generating the certificate, it is very necessary to store the certificate in a secure location such that no intruder can access the certificate. Figure 3 explains the procedure to store the certificate in its SO. To achieve this, each mobile node stores the SSC in its Surrogate Object (SO). The Surrogate Object is a database which stores all the details about the mobile node in a secure manner. The mobile nodes move out of grid network anytime and anywhere. If a mobile node has an incomplete process and if that node is not present in that particular grid, the process becomes tedious and remains undone. To overcome such situations, the SO acts as a virtual mobile node and performs all the jobs performed by that particular mobile node. To store a certificate in SO, the mobile node sends the request message to the SO.
Surrogate Object stores the certificate securely for future use.

**Secure Communication**

A communication between two mobile nodes is said to be secure, only if the data sent from one node to another cannot be opened by a malicious node and the sent data reaches the destination safely. The data are forwarded to the next node only after the authentication of the node. The authentication is done by the SSC. The process of checking the authenticity of next node is done by a monitoring object called Abstract Monitoring Object (AMO). This object monitors the entire data transmission and ensures the security and reliability of data. This also triggers secure routing process for secure and fast transfer of data to the destination.

1) **AMO Processing**

Figure 4 shows the complete architecture of AMO (Abstract Monitoring Object) which is used to monitor the nearest nodes and locate intruders. The mobile host sends a dummy data to the nearest mobile node. This dummy data are called as AMO. When the nearest node is able to decrypt the AMO, then the node is an authorized node. If the node is authorized, the mobile node sends the original data to that node. The primary step in this module is AMO generation. To generate an AMO, the mobile node encrypts a dummy data and makes it look like the original message. This AMO is transferred to the nearest mobile node. The mobile node receives the AMO and tries to decrypt the message. When the mobile node succeeds in decrypting the message, an automated ACK signal is received at the sender node. After that, the sender node sends the original data. If the nearest node is an intruder, the node cannot decrypt the data. When the Time To Live (TTL) expires, an automated NACK signal is received. After that, the mobile node redirects the path of the data transfer to the net nearest node. The process is repeated until the data reach its destination successfully.

When the ACK signal is received by the sender node, it indicates that the nearest node is an authorized node. Then the mobile node encrypts the original data with ECDSA algorithm with 168 bits of key size. After encryptions, the data are padded with the certificate along with the digital signature and the data are transferred securely to the nearest node from which the ACK signal is
received. If the receiver node is the destination, the node decrypts the data directly and uses it. If the node is not the destination, the entire operation is repeated.

(SSH) Routing algorithm is designed. It is designed in such a way that a drastic enhancement in reliability and security within a short transmission time is explicitly seen.

**Without AMO:**

1. A mobile node (say MHi) enters a Mobile Grid Network (say MGNi) using Single Sign-on authentication
2. Before the source mobile host (MHs) communicating with the destination mobile host (MHd), a certificate from Certificate Authority (CA) is received by sending a request message as (IDs||TTL||Kpu(s)||IDd||N1)
3. CA receives the request message and checks for the authentication
   a. If yes, the CA returns the public key of the destination host (Kpu(d)) to MHs
   b. Else, CA returns an error message to MHs
4. After receiving the Kpu(d) from CA, MHs integrates all necessary components and generates an X.509 Digital Certificate using RSA algorithm
5. MHs & MHd performs Mutual Authentication
6. After the mutual authentication, the original data transfer takes place

**With AMO:**

1. A mobile node (say MHi) enters a Mobile Grid Network (say MGNi) using Single Sign-On authentication
2. Before communicating with destination mobile host, the source mobile host (MHs) contacts Supervisory Host (SH) and gets a certificate
3. To achieve this, MHs gets the public key of the destination (Kpu(d)) from a public key database (data pool) located at MSS
4. Then it generates all the necessary components (IDs||TTL||Kpu(s)||IDd||N1) for SSC (Secure Service Certificate) and sends it to the SH
5. SH receives the request message and checks for authentication
   a. If yes, SH generates and provides the SSC to MHs
   b. Else, SH returns an error message to MHs

**2) Select Successive Hop Routing Algorithm**

The AMO is created just after the successful verification and storage of the SSC. The AMO consists of an encrypted dummy data along with the SSC. As soon as the AMO is created, it triggers the Select Successive Hop Routing algorithm (SSH) to find the next nearest node. After finding the next nearest node, the AMO consisting of dummy data and the SSC is transferred to the nearest node to check whether it is authenticated or not. If the node is authenticated, the AMO automatically returns an acknowledgement signal (ACK) to the upstream node. If the nearest node is unauthorized or when the TTL expires, a negative acknowledgement (NACK) is automatically sent to the upstream node. In a mobile grid environment, all devices are dynamic and unstable. Hence maintaining a routing table and finding the destination becomes a major issue. Thus to ensure and enhance the security and reliability of data that are transferred through this mobile grid environment, a new routing algorithm called Select Successive Hop

---

**FIG. 4 AMO (ABSTRACT MONITORING OBJECT) ARCHITECTURE DIAGRAM**

- 1. Request for certificate
- 2. Get the certificate
- 3. Store the certificate
- 4. Construct AMO and send to nearest MH
- 5. ACK
- 6. Get the certificate
- 7. Store in MH
- 8. Store in MD
- 9. Construct AMO and send
- 10. ACK
- 11. Send original data with learning
- 12. Request for certificate
- 13. Get the certificate
- 14. Store the certificate
- 15. Construct AMO and send
- 16. ACK
- 17. ACK
- 18. Return the certificate
- 19. Send original data with learning
- 20. Request for certificate
- 21. Get the certificate
- 22. Store in MH
- 23. Construct AMO and send to next MH
- 24. ACK
- 25. Send original data with learning
6. Each MHi has an individual Surrogate Object (SOi) which acts
   a. As a cache memory and stores all the details about the corresponding MHi securely
   b. As an object, the SOi does the process of its corresponding MHi when it is unavailable in the corresponding MGNi
7. The MHs stores the SSC in its SO in a secure manner
8. Communication between two mobile nodes can be done using the Abstract Monitoring Object (AMO)
9. As soon as the AMO is created, it automatically triggers the Select Successive Hop Routing algorithm (SSHR) to locate the next nearest node
10. After knowing the location, the AMO senses the corresponding direction for a nearest neighbor
11. When a nearest host (MHn) is found, the AMO sends a dummy data to that node
12. After receiving the dummy data, the MHn tries to read the data
   a. If the received data are authorized, an ACK is sent to MHs and original data transfer takes place
   b. If the data are unauthorized, then NACK will be sent to MHs. Then the path is redirected to the next nearest node
13. MHs encrypts the original data and forms a layer wrapping along with the certificate
14. MHn receives the data and reads the data
   a. If the MHn is an original destination, it removes the layer and reads the original message
   b. If the node is not the destination, it removes the existing layer, makes another layer of encryption and transfers it to the next nearest neighbor. The process is repeated from step 10 until destination (MHd) is reached

The different possible scenarios that could occur are:

Case 1: “Best Case”

The next nearest node MHi is the destination node, i.e., (i=d) or all the MHi are authorized nodes. Thus the constraint is

\[ t(n) \geq MH(g(n)) \] where \( t(n) \) is the time constraint and the \( MH(g(n)) \) is the mobile host function

Case 2: “Average Case”

There are some considerable amounts of unauthorized nodes in the network where the constraint is \( MH2(g(n)) \leq t(n) \leq MH1(g(n)) \) where MH is the mobile host

Case 3: “Worst Case”

All the nearest nodes MHi are unauthorized nodes. Hence the time constraint will be maximum or infinite. Thus the method fails as \( t(n) \leq MH(g(n)) \) where \( t(n) \) is the time constraint and the MH is the mobile host

Performance Analysis

To study the performance of the model, the data loss probability scenario explained in the previous section were considered, and were implemented over a simulated model of a Mobile Grid network. The scenario was studied over both the Abstract Monitoring Object and Supervisory Host along with and without Abstract Monitoring Object and Supervisory Host. Throughout this section, the algorithm without Abstract Monitoring Object and Supervisory Host is referred to as the old model and the one with Abstract Monitoring Object and Supervisory Host is termed as the new model. Typical performance studies include the actual number of packets lost for different number of mobile hosts in both the old and the new models, such as proportionate increase in the packet loss for different number of mobile nodes in both the models; impact of movement of Abstract Monitoring Object and Supervisory Host in terms of packet loss and message traffic. Query time both in the old and the new model is also taken into account for performance comparison.

Comparison of the Old and the New Models

The comparisons of the query time in the caching application over both the old and the new models were discussed. Query time was the overall time taken from an action request and the reception of the reply by a source node. Figure 5 shows the query time in the old model. The systems were implemented from a source to destination TTL. If the data were lost in between or they were sent to any unauthorized node, the sender would have to wait until the TTL elapsed. Thus the query time was much higher and there was a higher magnitude in waiting time.
FIG. 5 QUERY TIME COMPARISON IN THE OLD MODEL

Figure 6 shows the query time in the new model. In the model, hop to hop TTL is used addition to source to destination TTL. In hop to hop TTL, the magnitude of TTL is low. Thus, the sender need not wait until the TTL elapses, if the data were lost in between or they were sent to any unauthorized node. Thus the query time was much reduced and there was a lower magnitude in waiting time. The immediate reply can be obtained if any unauthorized node is detected. Hence, the query time is far less than the existing model.

FIG. 6 QUERY TIME COMPARISON IN NEW MODEL

One of the key advantages of the security objects (Surrogate object and Abstract Monitoring Object) model is that it is free to migrate to any node in the wired network. This flexibility is desirable for various reasons, including failure recovery, security, load balancing and network latency reduction. The effects of the query latency for various migration frequencies were discussed. Figure 7 shows the migration of security objects across the many numbers of nodes. The query latencies are considerably high. This is due to the increase in the percentage of time spent for generation of certificates and verification of certificates by certificate authority itself.

FIG. 7 QUERY TIME BASED ON NUMBER OF NODES TRAVELLED IN OLD MODEL

Figure 8 shows the migration of security objects across many numbers of nodes. The query latency is considerably less, because of the increase in the percentage of time spent on the generation of certificates and the verification of certificates by supervisory host itself. But as the move frequency is reduced, the query time improves. Surprisingly, further change in the move frequency seems to have almost no impact on the query time. A closer study of the network traffic generated as a result of performance, reveals the reason for providing migration freedom for the security objects.

FIG. 8 QUERY TIME BASED ON NUMBER OF NODES TRAVELLED IN NEW MODEL

Figure 9 shows the comparison of query time in both Old and New models in terms of number of messages exchanged versus simulation time for various move frequencies.
This paper proposes the secure routing based model for providing security and faster routing without drastic fall in performance of data transfer. Authentication of the mobile node can be achieved by providing certificates with digital signature stored in the Surrogate Object (SO). Security between two mobile nodes can be achieved using AMO (Abstract Monitoring Objects). Mobile devices are battery powered. So better power consumption of mobile devices can be achieved through Supervisory Host (SH) where SH is located at Mobile Support Station (MSS) and takes care of certificate generation and signing. The hand-over of authentication information can be done using ECDSA (168 bit key size) where the key size is far less when compared to RSA algorithm.

It is felt that it is the first practical model in the literature for providing security and reliability under various conditions, and the first integrated model in all of the literature to consider individual variability and behavior of each mobile host using security objects for the enhancement of security and reliability. The routing based security model is used to improve security without degrading the performance of the system.

REFERENCES


David G. Rosado a, Eduardo Fernández-Medina a,*, Javier


Key Sizes Selection in Cryptography and Security Comparison between ECC and RSA- M.J. Wiener, Efficient DES key search, manuscript, ell-Northern Research, August 20, 1993.


Kwok-yen Lam, Xi-Bin Zhao, Siu-Leung chung, Ming Gu and Jia-Guangum, "Enhancing Grid Security Infrastructure to support Mobile Computing nodes” ,Springer verlog Berlin Heidalberg,2005.


Randy Butler, Von Welch, Douglas Enhert, Ian foster, Steven Tweke, John volmer, Carl Kesselman “A national scale Authentication Infrastructure”, 2000,IEEE.


The SSL Landscape – A Thorough Analysis of the X.509 PKI Using Active and Passive Measurements Ralph Holz, Lothar Braun, Nils Kammenhuber, Georg Carle, IMC’11, November 2-4, 2011, Berlin, Germany. Copyright 2011 ACM.


Vipul Gupta, Sumit Gupta, Sheueling Chang Performance Analysis of Elliptic Curve Cryptography for SSL, WiSe’02, September 28, ACM 2002, Atlanta, Georgia,
USA.