World Academy of Science, Engineering and Technology
International Journal of Electronics and Communication Engineering
Vol:1, No:12, 2007

Mobility Management Enhancement for Transferring AAA Context in Mobile Grid

Hee Suk Seo, and Tae Kyung Kim

***Abstract*—**Adapting wireless devices to communicate within grid networks empowers us by providing range of possibilities.. These devices create a mechanism for consumers and publishers to create modern networks with or without peer device utilization. Emerging mobile networks creates new challenges in the areas of reliability, security, and adaptability. In this paper, we propose a system encompassing mobility management using AAA context transfer for mobile grid networks. This system ultimately results in seamless task processing and reduced packet loss, communication delays, bandwidth, and errors.

***Keywords*—**Mobile Grid, AAA, Mobility Management.

I. Introduction

MODERN computer applications are becoming increasingly complex and demanding, creating a need for powerful distributed networks, supplying shared processors and storage. The advent of a grid infrastructure brings the ability to dynamically cluster resources gathering, this enables the creation of large scale resource intensive distributed applications [1]. Mobile computing encompasses new areas of mobility, portability and wireless communications [2], creating a distinct discipline within the field of distributed systems. Mobile users may in the future, create powerful mobile grid networks. However, there are many obstacles that must be overcome when we envisage an efficient practical solution. New computing resource models and interfaces bring new problems. For example, there is no constant bandwidth supply as of a typical wired network. Wireless devices are characterized by intermittent connectivity due to the increased exposure of noise and the resulting signal degradation. In order to create an efficient network, the duration and frequency of network connections, as well as mobility, must be addressed [3]. In these environments, to apply the efficient AAA mechanism to a mobile grid, using heterogeneity security mechanism, we used the AAA context transfer capabilities.

The Authentication, Authorization, and Accounting (AAA) protocol specifies appropriate networking interaction schemes for a distributed system. Also AAA architectures address the inter-working between various components. The increasing popularity of mobile devices has generated a need for an individual to access a central authority, from any location. AAA provides the capacity to efficiently, and securely access information over a network infrastructure.

For grid computing to be successful, a single user account with a username and password is sufficient for pervasive (any time, any place) access to the computational resources required. Security permissions are handled transparently between the distributed systems. This requires the deployment of robust technology to establish the identity and trustworthiness of the user, control access permissions, and accept or reject resource requests. The subsequent sections of this paper are organized as follows. In section 2, related works are described. In section 3, we suggest the AAA context transfer method based mobile grid architecture. In section 4, we evaluate the performance of suggested mechanisms using a test bed. We illustrate our conclusion in section 5.

Manuscript received October 15, 2007.

H. S. Seo is with the Korea University of Technology and Education, Byungcheon, Chungnam 330-708 Korea (e-mail: histone@kut.ac.kr).

T. K. Kim is with the Seoil College of Department of Information Electronics, Seoul 77005 Korea (corresponding author to provide phone: +82-2-490-7241; e-mail: tkkim@ seoil.ac.kr).

II. Related Works

A. Current Mobile Grid Systems

New research methodologies for enabling mobile devices to perform grid operations or be a part of a clustered grid network are currently being explored.

Foster and Iamnitchi [4] have identified problematic similarities between P2P and Grid computing. They argue that Grid computing has added to the notion of a persistent, standards-based service infrastructure while P2P computing has addressed resource sharing in the face of unreliable networks and consumer devices.. The success of the SETI@home project [5] proves that large P2P systems can effectively be deployed in a high performance environment by aggregating the unused cycles of desktop PCs. In a P2P system, users are free to join and leave the network at any time. Thomas Phan et al. [6] favored 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 this emerging field. Dan C. M. et al. [7] introduced the ad hoc Grids as a hierarchy of mobile devices with different computing and communication capabilities. They described the generic architecture of an ad hoc grid and outlined the communication architecture. This also led to discussions on power consumption for different types of activities, depicting an agent-based power management system for ad hoc Grids. J. Hwang et al. [8] presented middleware architecture capable of

integrating mobile devices with existing grid architecture for conducting peer-to-peer operations. They suggested a range of different applications for which their architecture would provide optimum levels of efficiency.

B. Authorization Systems and Mechanisms

The Community Authorization Service (CAS) is a new component that comes with the Globus Toolkit 3.2. CAS [9, 10] this allows resource providers to specify broad access control policies when dealing with communities as a whole, and delegating specific fine-grained access control policy management to the community itself. Resource providers maintain ultimate authority over their resources but are spared day-to-day policy administration tasks, such as adding or deleting users, and modifying user privileges. CAS functions as a "push-model" authorization service; this is shown in Fig. 1. Security Assertion Markup Language (SAML) defines a language and protocol to exchange authentication and authorization information.

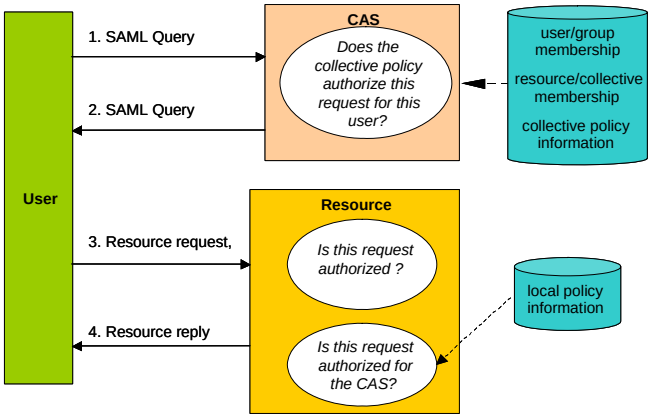

Fig. 1 CAS Architecture

1. The client sends a signed SAML AuthorizationDecisionQuery request to the CAS server indicating which resources they wish to access and their desired actions.

2. The CAS server establishes the user's identity. Using the identity it determines the rights as established by the VO's policy. It then returns a signed SAML assertion containing an AuthorizationDecisionStatement. This assertion contains the user's identity and a subset of the user's requested actions.

3, 4. The user presents the SAML assertion to a resource along with an authenticated invocation request. The resource uses the SAML assertion, subject to local policy regarding how much authority was delegated to the CAS service to authorize the request. The user may use the assertion to potentially make multiple requests, to multiple resources.

Within the CAS architecture, it is common for a client to ask for an assertion containing a complete set of rights they may have on a given resource, set of resources, or even on all resources for which a CAS server has authority. Since the SAML statement returned is typically valid for a number of hours, an assertion with multiple rights allows the user to undertake a number of different actions, which may not be known a priori, without having to re-contact the CAS server [11].

Akenti Authorization Service [12] can be used in either as a push or pull model, while providing access control decision functions. At the most fundamental level, this mode takes the identity of the client and the name of the resource, returning the access rights for that user in a signed capability certificate. Cardea [13] is a distributed authorization system, developed as part of the NASA Information Power Grid. This system dynamically evaluates authorization requests according to specific resource request characteristics rather than considering specific local identities. PRIMA [14, 15] is a system for privilege management and access control. In addition, this system provides middleware tools for end users and administrators to manage privileges for the resources within their level of authority. The EDG Security Architecture [16] is based on two types of authorization components: Virtual Organization Membership Services which are used for managing attributes, and several Authorization Decision Functions which are available as resources.

In this paper, we suggest the context transfer scheme for utilizing AAA information while the user migrates from one network to other network. We also compare the performance of other suggested mechanisms with respect to conventional AAA mechanisms.

III. AAA Context Transfer Mechanisms in Mobile Grid

A. Conventional Authorization

When analyzing with regard to handoff performance, one of the key issues in the development of a robust mobility management scheme for mobile grid networks is the minimization of handoff delay when a mobile device roams distributed heterogeneous networks. Mobile grid user accounts with a single log-on and password must be sufficient for pervasive access to all the computational resources required. When a user migrates from one virtual organization to another, security permissions must be handled between the separate systems in a manner transparent to the user.

For efficient AAA in a mobile Grid network, we propose the context transfer method, which transfers AAA state information from the old proxy server to the newly arrived proxy server. We consider the optimum mobile Grid architecture as a proxy-based, clustered system, suggested in [6]. The motivation for this stems from the benefits of avoiding the re-establishment of AAA and providing seamless task processing.

Authorization architecture generally consists of a set of entities and functional components that allow decisions to made and enforced based on attributes, parameters and policies. Fig. 2 depicts the authorization system when based on a pull structure.

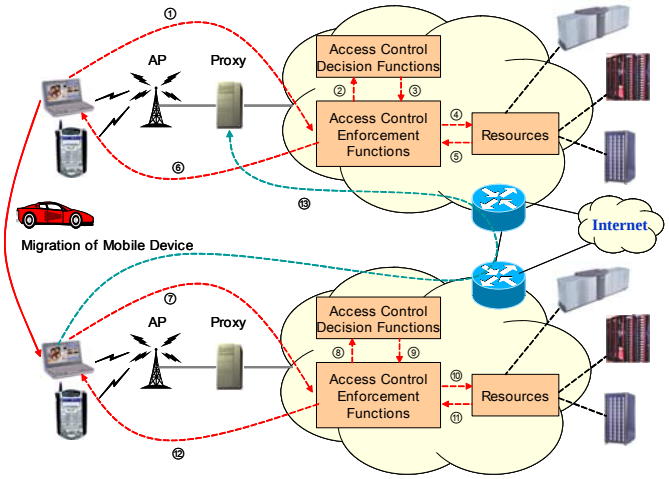

Fig. 2 Abstract Authorization Architecture based on pull sequence

Initially, mobile grid users send service requests (①) to the access control enforcement function. The access control enforcement component sends these authorization requests (②) to the access control layer.. The access control layer checks the specific mobile Grid user and returns an unsecured or secured message (③) (token or certificate) that act as a proof of right (Authorization Assertion). This assertion can subsequently be used by a mobile grid user to contact a resource and request specific services such as data, computational, or access. (④). The resource will either accept or reject the authorization assertion (⑤) and return the result back to the specific mobile Grid user. (⑥).

During movement from one network to another (or one Virtual Organization to another), the mobile Grid user must be re-authenticated in the new proxy system. The re-authorization process (⑦~⑫) is the same as the above processes (①~⑥). The migrated mobile Grid user notifies his or her position and job status to the previous proxy (⑬). The migrated mobile Grid user can receive his or her results of requested jobs or send the results of a distributed sub tasks on a mobile device to the previous proxy system, which can provide reliable job processing.

B. AAA Context Transfer based Authorization

The context transfer protocol [17] is designed to work seamlessly with other protocols to provide an overall robust architecture.. This protocol supports both IPv4 and IPv6 and provides feature context support, initiation and authorization content transfer, status notification, and transferring context during and after handovers.

In our design, context transfer is used to re-authenticate and re-authorize the mobile devices to a new Virtual Organization (VO) within a mobile Grid architecture without requiring the mobile devices to explicitly perform all protocol flows for the associated services from scratch. This technology can provide an interoperable solution that supports various Layer 2 radio access technologies. Fig. 3 shows the authentication architecture based on this AAA context transfer model.

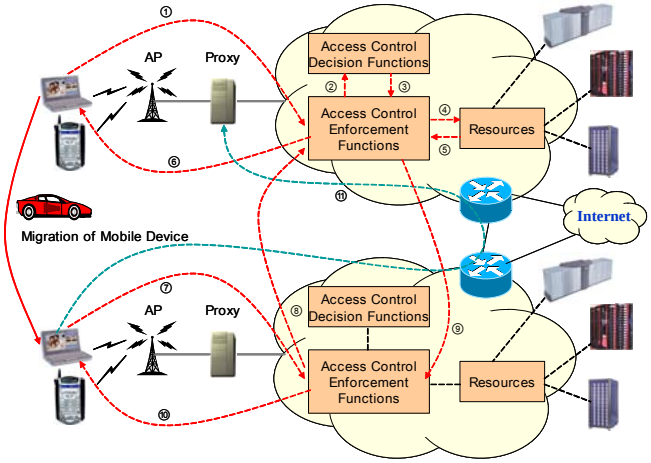

Fig. 3 Abstract Authorization Architecture based on AAA context transfer

The process of ① to ⑥ is the same as shown in the Fig. 2 process described previously. In the case mobile devices migrate from one network to another (or one Virtual Organization to another), the mobile node sends a CTAR (Context Transfer Activate Request) message (⑦) to the proxy in the newly arrived network. The AAA authentication module then sends a CT-Req (Context Transfer Request) message (⑧) to the previous authentication module in the previous network. The CTD (Context Transfer Data) message (⑨) is finally transmitted to the authentication module in the current network. The detailed message type and specific function of this context transfer protocol is described in [17].

To ensure the consistency and validity of AAA context transfer, EAP [18] (Extensible Authentication Protocol) is considered. EAP provides a mechanism for supporting various authentication methods over wired line and wireless networks and also allows wireless client adapters to communicate with different back-end servers, such as RADIUS or DIAMETER [19]. Without any loss of generality, RADIUS has been chosen [20].

In Figs. 4 and 5, we have compared the process of exchanging messages between the signaling flow of AAA messages and the signaling flow for AAA using context transfer.

The figures clearly show how the numbers of message exchanges are reduced and how communication with the RADIUS server is avoided. As suggested in [19], it has been observed that although the actual times vary, context transfer enabled handoff is much faster than handoff without context transfer. The improvement is almost 10 times.

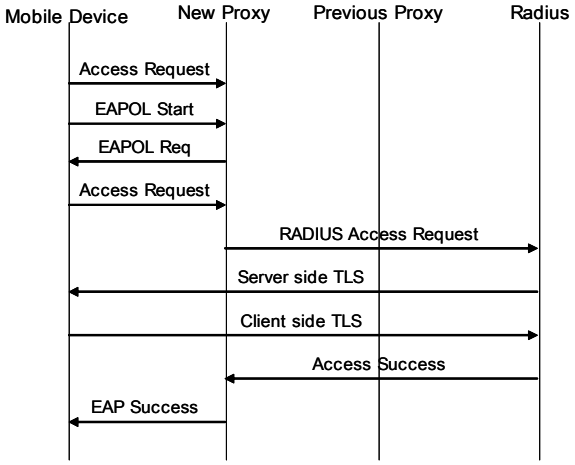

Fig. 4 Signaling flow of AAA messages

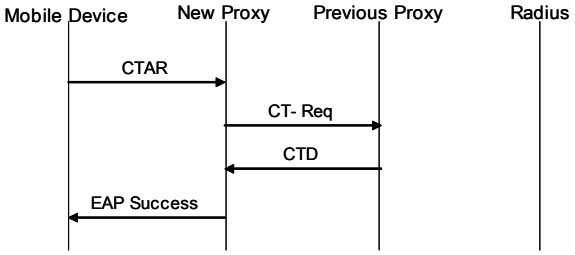

Fig. 5 Signaling flow of AAA messages using context transfer

IV. Performance Evaluations

A. Test Bed Architecture

We implemented the test bed using the PDAs in wireless network environments. The implementation environments are like these:

- Proxy System

CPU: Intel Pentium III 1GHz
RAM: SDram 256MB
O.S: Redhat Linux 7.3 Kernel 2.4.18-3
Compiler: gcc version 2.96
Database: mysql Ver 11.16 Distrib 3.23.49

- Mobile Device (PDA)

Hardware: Sharp Zaurus SL-6000/C860 (CPU 400MHz)
CDE (Cross Development Environment): Linux Kernel, binutils, gcc, glibc, Qt/Embedded - Cross Development Kit

We used the MPICH module to distribute the job to different mobile devices and receive the results of requested jobs. The test bed of Mobile Grid is shown in Fig. 6.

B. Performance Evaluation

We simulated the Mobile Grid Architecture with regard to the response time. The application program used in this simulation calculates the fine prime numbers (primem.c), 4 mobile devices (PDAs) are used.

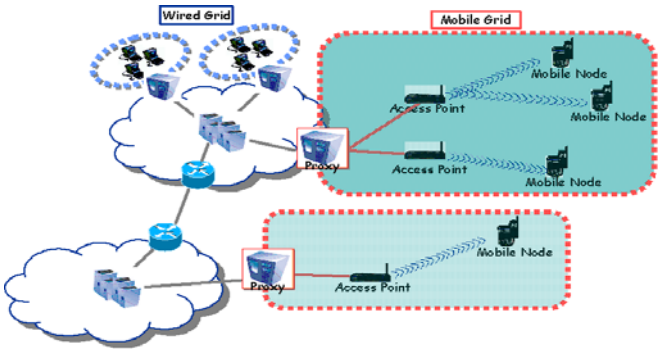

Fig. 6 The Test bed of Mobile Grid Architecture

Fig. 7 showed the efficiency of a mobile grid when there is no handoff. As the number of participating mobile nodes increase, the job execution time is decreased. Fig. 8 showed the response time of the processing mobile Grid application when one of the mobile devices moves from one network to another (resulting in handoff).

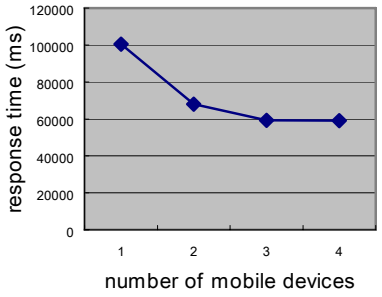

Fig. 7 Response Time of Mobile Grid

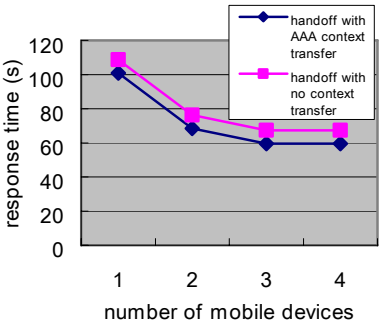

Fig. 8 time for use and no use of context transfer

As shown in Fig. 8, AAA context transfer mechanisms demonstrates how improves the overall response time of job execution. Also this technology can suggest the seamless and secure mobility management.

V. Conclusion

Grid infrastructure provides us with the ability to dynamically link resources together in a shared architecture to enable the implementation and sustained support of large scale resource intensive distributed applications. This mobile grid architecture creates complicated issues when used over

networks because of the requirement of providing services to users over multiple networks, regardless of location. At the heart of these issues, is user migration, in case of a mobile device migrating from one network to another (or one Virtual Organization to another), the handoff delay considerably influences the response time of a parallel-distributed job.

With regard to the above point, we suggest the AAA context transfer mechanism in a mobile grid. To compare this against other mechanisms, we implemented a test bed of different mobile grid architectures and analyzed the job execution of handoff with no context transfer vs. handoff with AAA context transfer performance response time. As shown in the 4.2 performance evaluation, this mechanism contributes to the seamless operation of task processing, and reduces packet loss, delay, bandwidth, and error.

REFERENCES

[1] F. Berman, G. Fox, T. Hey, The Grid: past, present, future, Grid Computing - Making the Global Infrastructure a Reality, Wiley and Sons, 2003.
[2] M. Satyanarayanan, "Fundamental Challenges in Mobile Computing," In proceedings of the fifteenth annual ACM Symposium on Principles of Distributed Computing, Philadelphia, Pennsylvania, 1996.
[3] B. Clarke, M. Humphery, "Beyond the "Device as Portal": Meeting the Requirements of Wireless and Mobile Devices in the Legion Grid Computing System," Proceedings of the International Parallel and Distributed Processing Symposium (IPDPS'02), 2002.
[4] I. C. Foster and A. Imanitchi, "On Death, Taxes and the Convergence of Peer-to-Peer and Grid Computing", 2nd International Workshop on Peer-to-Peer Systems.
[5] SETI@home. http://setiathome.ssl.berkeley.edu, March 2001.
[6] Thomas Phan, Lloyd Huang, and Chris Dulan, "Challenge: Integrating Mobile Wireless Devices Into the Computational Grid", MOBICOM 02, September 23~26, Atlanta Georgia, USA.
[7] D. C. Marinescu, G. M. Marinescu, Y. Ji, and L. Boloni, "Ad Hoc Grids: Communication and computing in a Power Constrained Environment," Workshop on Energy-Efficient Wireless Communications and Networks (EWCN) 2003, Phoenix, USA, 2003.
[8] J. Hwang, P. Aravamudham, "Proxy-based Middleware Services for Peer-to-Peer Computing in Virtually Clustered Wireless Grid Networks," International Conference on Computer, Communication and Control Technologies (CCCT '03), Orlando, Florida, July 2003.
[9] L. Pearlman, V. Welch, I. Foster, C. Kesselman, and S. Tuecke, A Community Authorization Service for Group Collaboration. IEEE 3rd International Workshop on Policies for Distributed Systems and Networks, 2002.
[10] L. Pearlman, V. Welch, I. Foster, C. Kesselman, and S. Tuecke, The Community Authorization Service: Status and Futures. Computing in High Energy Physics (CHEP03), 2003.
[11] M. Lorch, B. Cowles, R. Baker, L. Gommans, P. Madsen, A. McNab, L. Ramakrishnan, K. Sankar, D. Skow, M. Thompson, Conceptual Grid Authorization Framework and Classification, 2004.
[12] M. Thompson, A. Essiari, S. Mudumbai, "Certificate-based Authorization Policy in a PKI Environment", ACM Transaction on Information and System Security (TISSEC), Volume 6, Issue 4 (Nov. 2003) pp 566-588.
[13] R. Lepro, "Cardea: Dynamic Access Control in Distributed Systems", NASA Technical Report NAS-03-020, Nov. 2003.
[14] M. Lorch, D. Kafura, "Supporting Secure Ad-hoc User Collaboration in Grid Environments", 3rd Int. Workshop on Grid Computing, Baltimore, Nov. 18th, 2002.
[15] M. Lorch, D. Adams, D. Kafura, M. Koneni, A. Rathi, and S. Shah, "The PRIMA System for Privilege Management, Authorization and Enforcement in Grid Environments", 4th Int. Workshop on Grid Computing, Grid 2003, Nov. 2003, Phoenix, AR, USA.
[16] R. Alfieri et al. (EDG Security Co-ordination Group), "Managing Dynamic User Communities in a Grid of Autonomous Resources", Proceedings of Computing in High Energy and Nuclear Physics, 2003.
[17] J. Loughney, M. Nakhjiri, C. Perkins, and R. Koodli, Context Transfer Protocol, IETF Draft, Aug. 2004.
[18] B. Aboda, D. Simon, J. Arkko, P. Eron, and H. Levokowetz, "Extensible Authentication Protocol (EAP) Key Management Framework", Internet Draft, work in progress.
[19] C. Politis, K. A. Chew, N. Akhtar, M. Georgiades, R. Tafazolli, and T. Dagiuklas, "Hybrid Multilayer Mobility Management with AAA Context Transfer Capablities for All-IP Networks", IEEE Wireless Communications, Aug. 2004.
[20] " RADIUS", IETF RFC 2508, Jan. 1997.