Available online at www.sciencedirect.com
ScienceDirect
Computer Standards & Interfaces 31 (2009) 40–47
COMPUTER STANDARDS & INTERFACES
www.elsevier.com/locate/csi

Efficient migration for mobile computing in distributed networks

Kuo-Hsuan Huang [a], Yu-Fang Chung [b,*], Chia-Hui Liu [a], Feipei Lai [a,c,d], Tzer-Shyong Chen [e]

[a] Department of Electrical Engineering, National Taiwan University, Taiwan
[b] Department of Information Management, Chaoyang University of Technology, Taiwan
[c] Department of Computer Science and Information Engineering, National Taiwan University, Taiwan
[d] Graduate Institute of Biomedical Electronics and Bioinformatics, National Taiwan University, Taiwan
[e] Department of Information Management, Tunghai University, Taiwan

Received 12 February 2007; received in revised form 16 September 2007; accepted 10 October 2007
Available online 22 October 2007

Abstract

The speed and convenience of the Internet makes it advantageous to online applications. Basing on the elliptic curve cryptosystem, this study proposes a hierarchical mobile agent framework for handling key management and access control problems between mobile agent and host. It raises the security of key management, and also controls access to distributed environment in non-specific network. The proposed method successfully secures the accessing relationship between the mobile agent and the host while economizing the exhaust of storage space. Such an achievement lets the mobile agent operate efficiently, and puts in order a secure execution environment for mobile computing.

Keywords: Elliptic curve cryptosystem; Mobile agent; Access control; Mobility; Distributed environment

1. Introduction

The increasing popularity of the Internet has made distribution of information via the Network increasingly common. Therefore, networks have become complex and bulky. The work of the network administrator is also increasingly important. In the conventional centralized network administration method, a host must exchange messages and data with clients. However, large networks increase workload which in turn increases net dataflow. The heavy dataflow leads to a drop in work efficiency. Also, the frequent exchange of data between host and clients also uses up large amount of network bandwidth and eat into efficiency. Thus, the current system administration, which tends toward large and distributed networks, faces a considerably large problem. Questions regarding its dependability, expandability, interactivity, and inelasticity are raised.

A Mobile agent is a kind of software program that can migrate from one host to another in a heterogeneous network. It can communicate and interact with other agents and the distributed resource system on heterogeneous networks. A mobile agent can also decide when to migrate, and which nodes to access. After migrating to the desired host, the mobile agent resumes the execution of previously broken off or awaiting tasks. On completing the task, the mobile agent returns the result to the client. Therefore, the client need not be constantly connected to the server. This not only saves a lot of unnecessary transmission load, but also helps in the application of mobile calculation. The mobile agent can single-handedly execute all tasks assigned by the user. It can meet and interact with other agents when necessary while still executing its task. Therefore, a mobile agent can be viewed as an independent program. A manager need only assign tasks to a mobile agent. The agent then migrates to the remote network management servers to assign tasks to the servers. Once the tasks are completed, the mobile agent brings the result back to the manager for analyses and processing. With this kind of entrusted distributed network management server, increased workload which is often brought

* Corresponding author.
E-mail address: yfchung@cyut.edu.tw (Y.-F. Chung).

0920-5489/$ - see front matter © 2007 Elsevier B.V. All rights reserved.
doi:10.1016/j.csi.2007.10.011

on by expansion of network can be prevented. Generally speaking, mobile agent has qualities like enhanced flexibility, network traffic reduction, support for disconnected operations, roaming ability on heterogeneous environment, and fault tolerance [1]. Because of the afore-mentioned qualities, mobile agent is currently widely in use in numerous areas like distribution information retrieval [2–4], electronic commerce [5–7], medical data transmission [8,9], and network management [10].

A mobile agent continuously visits other agents to exchange information while roaming around the servers in the networks carrying out its tasks. However, convenient as a mobile agent is, there are several potential security risks [11] in making contact with others in the Internet, especially for business activities. The security risks occur in different situations as described below.

One, protecting hosts from access by unauthorized parties. Two, protecting hosts from attacks by malicious agents, e.g., an agent might assume the identity of legal agent to request for services. Three, protecting agents from attacks by another agent, e.g., an agent tries to hinder another agent by constantly sending messages to the agent, causing the receiving end server to overload and the computation time to increase. Finally, protecting agents from attacks by malicious hosts, e.g., a host might impersonate an agent so as to deceive the agents or to ignore the requests of the agents. A malicious host deliberately delays an agent's request, or even terminates an agent's connection without warning causing other agents awaiting response from this agent to enter into a deadlock. Also, a malicious host can deliberately make an agent fail to carry out his task causing the agent to be live locked.

The first three risks are caused by the agents. They are resolvable through cryptography technologies that can control agents' access. The final risk is caused by a malicious host that controls the accessing and roaming activities of mobile agents. It is quite difficult to prevent a malicious server from attacking. Therefore, this work is intended as a solution to the attacks from the host authorities.

Numerous attempts to raise the security of mobile agents were made by scholars. Corradi et al. [12] presented a mobile agent structure called SOMA. The structure was built with an agent, agent server, management system, and security approach. With the same functions as SOMA, Karnik and Tripathi [13] proposed a structure called Ajanta. Besides, a tree structure was developed by Volker and Mehrdad [14], with the functions of mobile agent authorization, key management, and access control. However, the scheme did not take into consideration the efficiency of key management. Therefore, the scheme has two faults, bulky mobile agent codes and excessive calculations for encryption/decryption of keys. In recent years, Chang and Lin [15] proposed a key management scheme with hierarchically-based structure to reform the inefficient key management in Volker and Mehrdad's scheme. Although Chang and Lin corrected the faults in Volker and Mehrdad's scheme, their proposal remained inefficient as the scheme required the use of RSA exponential operations for key generation and derivation. Therefore, accessing confidential files consumes considerable system resources. To raise efficiency so as to make its application more convenient, we hope to be able to reduce its key derivation computation as well as the needed memory.

In 1985, Miller [16] and Koblitz [17] each proposed an elliptic curve algorithm-based crypto-technology for designing public key algorithm. This facilitated the development of many international standards for the Elliptic Curve Cryptosystem (ECC), such as ISO 11770-3, ANSI X9.62, IEEE P1363, FIPS 186-2, etc. The greatest feature of the ECC is that on the same level of security its key-size is comparatively smaller than that of the currently widely used RSA cryptosystem. For instance, the ECC whose key-size is 160 bits is as secure as the RSA with a key-size of 1024 bits. The smaller key-size of the ECC allows lower memory requirement and greater execution speed.

This study explores an approach to key management and access control for mobile agents, in which the framework is established in hierarchical environment. Besides, the proposed method will be based on the ECC whose small key-size and lower computations shall benefit the scheme by allowing the agents to execute the assigned tasks in optimal efficiency under reliable security measures.

After the introduction to the characteristics and the security risks of mobile agents, Section 2 examines the key management and access control method for mobile agents by Volker and Mehrdad with emphasis on performance efficiency. Section 3 shows the mathematic background of the elliptic curve cryptosystem, and put forth a new method to solve the key management problems of mobile agents. Section 4 discusses potential attacks that could damage the system, and interprets the measures of the proposed scheme against these security risks. Section 5 analyzes the performance efficiency from two points, the required space complexity for key storage and computation complexity for key derivation. Section 6 furnishes the conclusions.

2. Overview of Volker and Mehrdad's scheme

For access control and key management of mobile agents, Volker and Mehrdad [14] proposed a security method under tree-based structure, as illustrated in Fig. 1. The method is devoted to realizing agent authorization, dealing with key management, and controlling access of agents.

According to the data patterns — either static or mutable, the mobile agent framework is separated into two branches. The static branch stores constant data that will not change during the agent's lifetime, such as class codes, security policies, and so on. As to the mutable branch, the contents are alterable data like the return results, the instances of the classes, and the confidential contexts. Confidential information, whether static or mutable, always remains private. Also, after an agent achieves the target on a host, the host can alter the state of the agent and the information carried by the agent on the spot. Access control methods are competent so as to protect the secret resources from being accessed by unauthorized personnel; there are numerous similar related studies. In this section, the key management and access control method [14] presented by Volker and Mehrdad is given as an introduction to the subject, as follows.