International Journal of Innovative Computing, Information and Control
Volume **7**, Number **12**, December **2011**

ICIC International ©2011 ISSN 1349-4198
pp. 7077–7090

THE DESIGN OF ID-BASED ACCESS CONTROL SYSTEM WITH TIME-SENSITIVE KEY FOR MOBILE AGENT'S MIGRATION

Chia-Hui Liu[1], Yu-Fang Chung[2], Tzer-Shyong Chen[3] and Sheng-De Wang[1]

[1]Department of Electrical Engineering
National Taiwan University
No. 1, Sec. 4, Roosevelt Road, Taipei 10617, Taiwan
{ d96921027; sdwang }@ntu.edu.tw

[2]Department of Electrical Engineering
[3]Department of Information Management
Tunghai University
No. 181, Sec. 3, Taichung Port Road, Taichung 40704, Taiwan
{ yfchung; arden }@thu.edu.tw

Received August 2010; revised December 2010

Abstract. *Due to the maturity of e-commerce and the ability of mobile agents to migrate freely in heterogeneous networks, mobile agents have become very popular for e-commerce applications in the distributed networks. However, once a user applies a mobile agent to execute his task on the Internet, the mobile agent exposes itself to danger. This is an obstacle when using mobile agents. It is, therefore, urgent to build up a secure structure for mobile agents. In this paper, a new structure is suitable for mobile agents on the basis of improving the tree-based scheme. In the novel structure, the concept of access control and a key assignment scheme are used to ensure the privacy of the data being transmitted. To convenient the computation in the key generation phase, we use the ID-based characteristics in bilinear pairings over elliptic curves to construct a hierarchical key management scheme. Moreover, the concept of time sensitive is integrated into our scheme, which ensures our scheme more secure and more efficient. Finally, from our security analysis, the new scheme should be able to resist malicious attacks, promote the key management efficiency and protect mobile agents.*

Keyword: Mobile agents, Access control, Key management, Bilinear pairings, Time sensitive

1. **Introduction.**

Owing to the popularization of the network, hosts might share their information with each other. Thus, this resulted in the development of distributed system technology. The network is overloaded when the distributed systems are dealing with a large volume of data. In order to solve this problem, the relevant technology of mobile agents is developed.

A mobile agent is a kind of autonomous software. Once a mobile agent is sent to the Internet by its owner, it can control itself and move freely among different hosts [4,5]. It also can transmit information to the other mobile agents and it can interact and distribute resources with the other distributed systems. The figure given below is a simple illustration of the concept of mobile agents.

In Figure 1, after the owner tasking the mobile agent, it will roam in the corresponding servers to execute the task till the completion of the task or the end of the life cycle return the result to the owner.

When a mobile agent performs its task, it can exchange messages with other agents which are surfing on the Internet. Thus, a mobile agent may encounter some security threats. Hence, many researchers have begun to propose various mobile agent structures