International Journal of Innovative Computing, Information and Control
Volume **7**, Number **5(A)**, May **2011**

ICIC International ©2011 ISSN 1349-4198
pp. **2389–2404**

A NOVEL MOBILE AGENT AUTHENTICATION SCHEME FOR MULTI-HOST ENVIRONMENTS USING SELF-CERTIFIED PAIRING-BASED PUBLIC KEY CRYPTOSYSTEM

Woei-Jiunn Tsaur[1] and Lo-Yao Yeh[2]

[1]Department of Information Management
Da-Yeh University
168 University Rd., Dacun, Changhua 51591, Taiwan
wjtsaur@yahoo.com.tw

[2]Department of Computer Science
National Chiao Tung University
1001 University Rd., Hsinchu 300, Taiwan
lyyeh@cs.nctu.edu.tw

Received December 2009; revised April 2010

Abstract. *The mobile agent technology has been widely proposed for the management of networks and distributed systems. Consequently, the security issues of mobile agents are more and more important. The security issues of mobile agents are classified into two aspects: (1) protecting hosts against unauthorized and hostile agents and (2) protecting mobile agents against malicious hosts. Current researchers mainly focus on protecting mobile agents from malicious users or hosts. This paper proposes an authentication scheme for effectively protecting multiple hosts against unauthorized mobile agents. The proposed scheme employs a proxy signature scheme to design an authentication scheme so that a mobile agent can register only once for multiple services. Multi-host environments are taken into consideration in the proposed scheme for better scalability. To the best of our knowledge, this work is the first attempt to protect mobile-agent-based hosts for multi-host environments. In summary, this proposed authentication scheme can achieve the requirements of authentication and authorization of mobile agents. Also, the performance evaluation shows that the proposed scheme is more desirable to multi-host environments owing to the merits of better scalability and low computational and communicational cost.*

Keywords: Authentication scheme, Agent security, Proxy signature, Self-certified public key cryptosystem

1. **Introduction.** Mobile agents are one of the fastest growing areas of information technology. Currently, mobile agents are widely applied in various applications. The mobile agent technology offers a new computing paradigm in which a program can suspend its execution on a host, transfer itself to another agent-enabled host on the network and resume an execution on the new host [1]. Therefore, the ability to remote execution across a wide area network (WAN) facilitates the deployment of e-commerce services and applications in a more dynamic, flexible and customizable way. Although the mobile agent extends the capabilities of remote communication and distributed computing, it also brings new security challenges [2]. In general, the security challenges of mobile agent are classified into two areas [3]: (1) protecting hosts against unauthorized and hostile agents and (2) protecting agents against malicious hosts. In the past few years, a lot of researchers [4-9] concentrated their attention on protecting mobile agents. However, the problem of protecting hosts against malicious mobile agents is also complicated and cannot be omitted.