

## **Minitrack on Security and Survivability in Mobile Agent Based Distributed Systems**

Prithviraj (Raj) Dasgupta and Azad Azadmanesh  
*Computer Science Department, University of Nebraska at Omaha*  
*E-mail: azad@unomaha.edu, pdasgupta@mail.unomaha.edu*

### **1. Introduction**

An agent is a piece of software code that can execute autonomously without continuous supervision by a central authority. Intelligent agents are also capable of interacting and learning from their environment and can react to changes in their environment. Mobility is also an attractive feature of software agents that allows the agent to move to a remote location and continue its thread of execution on the remote machine. Mobile agents are particularly attractive for designing distributed and decentralized applications as they can reduce the processing time and network bandwidth usage by moving the code closer to data that is located on a remote machine. However, the autonomy of a mobile agent on the remote sites can be used maliciously either by creator of the agent or by other entities to subvert and sabotage the entire system. For example, rogue mobile agents can be used to encapsulate apparently harmless code that is capable of installing viruses on the sites that the mobile agent visits.

Equally important is the issue of reliability of the applications built using mobile agents. Reliability is most frequently implemented in software systems using transaction-based mechanisms for providing a mutual consensus among the different nodes of the system. Using these techniques, we can address reliability issues in a mobile agent based distributed system by exchanging messages to implement a distributed consensus algorithm. However, excessive message passing in mobile agent based systems can compromise the security of the system by providing an avenue for attackers to exploit the system by sending incorrect and malicious messages. Therefore, the issues

of security and reliability are somewhat orthogonal in mobile agent based distributed systems.

Over the past few years several mobile agent system architectures, platforms and applications have been applied to solve problems that are decentralized and distributed in nature. However, crucial issues such as security and survivability in mobile agent systems have been relatively less addressed. Unless these issues are addressed adequately, mobile agent systems cannot be adapted widely for commercial and practical applications.

The minitrack attracted diverse and interesting research papers out of which two papers were accepted for presentation at the conference. The paper titled "Agent Survivability: An Application for Strong and Weak Chain Constrained Scheduling" by Krings describes a formal framework for fault tolerance in mobile agent systems using secret sharing. The mobile agent survivability problem is mapped to a scheduling problem which is then optimized according to the functionality desired by the application. In the paper titled "The Use of Encrypted Functions for Mobile Agent Security", Lee and Alves-foss describe a two phase encryption scheme for securing a mobile agent's code which employs homomorphic encryption followed by functional composition. These papers describe techniques that address existing challenges in the area of security and survivability in mobile agent systems and provide interesting research directions for further investigation to enhance the reliability of software systems.