

SECURED MOBILE AGENT COMMUNICATION

D. S. ADANE AND S. R. SATHE

Abstract

Communicating with confidential data requires special attention in a Mobile Agents environment, especially when the other hosts must be prevented from eavesdropping the communication. We propose two methods for secured communication between the agent and a host (or other agent). The first approach for an untrusted environment uses on the fly Encryption-Decryption sequence to directly convert the message or plaintext into one that is encrypted directly with the public key of receiver thus reducing the overhead of retrieving the public key of sender. The technique uses AlGamal encryption/decryption. Theoretically it is proved that this scheme indeed gives the desired result. The second approach uses a trusted central authority for supply of public keys. It uses DES and RSA algorithm to provide a secured communication. Our minimal implementation of this technique suggests that it is possible to embed the entire functionality for communication security within an agent. Finally, we also state and explain how the second approach is useful in context of mobile agents with itinerary.

Keywords: Mobile Agents, AlGamal, RSA, DES, Aglets.