ABSTRACT

In recent years, mobile agent technology is a promising paradigm in distributed computing, because of its flexibility, dynamic customization and robust interaction in unreliable networks. In addition to these benefits, mobile agent technology has the ability to reduce the network load and improve the network latency. Although mobile agent technology finds various benefits, security risks related to the agent and platform restricts its usage in various applications. Currently available security mechanisms do not efficiently handle all the existing threats. Security mechanisms must protect both the agent and the platform where the agent is executing. This thesis addresses the security issues and proposes a new security architecture with multi-level protection and recovery models in an open mobile agent environment for both the agent and platform.

The first protection model of the proposed architecture is the Malicious Identification Police (MIP) to prevent the execution of the malicious agent in the platform with the help of the Attack Identification Scanner (AIS). The second model, Code Integrity Checker (CIC) is to protect the mobile agent code from malicious alterations during the agent’s journey in the untrusted environment. The third model is the Information Verifier and Generator (IVG) to protect the mobile agent data from the malicious single attacker or set of attackers during the journey. Lastly, the K-response
recovery model is to rollback the original agent in case of any failure of the agent. It is possible to recover the data, state, itinerary and code after the single malicious host or set of malicious hosts attack.

The security features of all these models are carefully analyzed, and are demonstrated through experimental study on a real-time mobile agent platform. The proposed models rely heavily on well-established cryptographic primitives, such as encryption, decryption and digital signature functions. The proposed security architecture and models, yield new contributions to the mobile agent environment.

The encapsulated Information Verifier and Generator (IVG) model and the recovery model are incorporated in the e-health environment and experimented to test the performance of the models. The comparison results of these proposed models with those of the existing models proved that the proposed models are efficient for mobile agent environment security with respect to computation time and agent size.