ABSTRACT

The Mobile Agent technology has become 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 thereby reduces network latency. Although Mobile Agent technology possesses 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. The research work addresses the security issues and proposes advanced security architectures with multi-level protection and recovery mechanism in an open Mobile Agent environment for both the agent and platform.

The first part aims in providing security to the Mobile Agent platform by means of two approaches namely Dual Check Point Analysis, which focus on tailgating attacks and Malicious Identifier with Tripmarker, which mainly focus on the replay attacks. The data carried by the Mobile Agent is protected using Address Forward Data Backward (AFDB) protocol which safeguards the data from Colluded Truncation Attacks. Finally, the Mobile Agents are recovered by the usage of Trusted Environment with Reference Clone (TERC) and eXtended Volunteer Algorithm (XVA) which uses the Adaptive Mobile Agents to provide a fault tolerant system. From the
experimental results, it is evident that all the mechanisms implemented satisfy the Security Services without compromising any attack.

All the above said techniques rely on the basic information security and cryptographic techniques. The architectures that are proposed exhibit the same to the Mobile Agent Environment.

The first technique namely the Dual Check Point Analysis uses a system comprising of two gates, the inner and the outer for the verification of the Mobile Agent. This technique uses the verification based on digital signature as well as checksum, which ensures the validity of a Mobile Agent. The Malicious Identifier with the Tripmarker uses a concept of Tripmarker which acts as an identification marker for the Mobile Agents path-of-execution. This greatly helps in overcoming the External Replay Attacks.

The Address Forward and Data Backward protocol ensures the protection of Mobile Agents against Colluded Truncation Attacks. This mainly focuses on the identification of the malicious host when the system is subjected to Colluded Truncation Attacks. The next technique namely the Trusted Environment with Reference Clone is a mechanism for the recovery of Mobile Agents when it is found that a Mobile Agent is subjected to an attack. This employs two mechanisms in which the Trusted Environment is either integrated with the server or is isolated from the server and kept in a standalone system. The XVA proposes a new category of agent namely Adaptive Mobile Agents which are capable of attaining roles from other agents or from the Mobile Agent Environment. This, when used proves to be
more effective in the processing of data as well improves the Fault-tolerant capability of the system.

The security features of all the above techniques are analyzed. From the experimental results obtained, it is found that the proposed techniques are better in providing the security to the Mobile Agents than the existing systems.