CHAPTER 9

CONCLUSION AND FUTURE ENHANCEMENTS

9.1 SUMMARY

New techniques, languages and paradigms have appeared to create distributed application in several areas. The mobile agent concept is the one incorporated in it to improve its performance. Because of this, mobile agent-based research has drawn much attention in recent years to upgrade its performance in all areas. Despite most of its benefits, the security issue is a paramount problem in its usage. The major security issues in the mobile agent environment are the agent code alteration, data alteration, agent platform attack and the loss of the agent. To protect the mobile agent environment from all these security issues, a new security architecture with the advanced protection and recovery model is designed. The protection models of the architecture perform the integrity test sequentially one after the other. It may also be possible for every protection model to perform the parallel integrity test to reduce the waiting time of the agent for computation.

9.1.1 Contributions

The Malicious Identification Police (MIP) in the security architecture has the Attack Identification Scanner (AIS) to scan the incoming agent before allowing it to execute in the environment. Agent scanning will be based on the privileges given to the agent owner and based on the AIS intelligence. The MIP is equipped to identify both the known (signature
based) and unknown attack codes through lexical analyze feature. The advantages of the MIP model show its effectiveness to be more than that of the existing platform protection models.

The second model of the architecture is the Code Integrity Checker (CIC) with the Root Canal algorithm proposed to detect the malicious change in the agent code. The proposed Root Canal (RC) is used to detect any malicious change in the agent code done by the platform in the middle of the journey and eXtended Root Canal (XRC) algorithms is used to prevent the false malicious claim against the legitimate host. The comparison results with the existing models proved that the proposed model is better both in size and computation.

The third model, Information Verifier and Generator (IVG) is to verify the integrity of the agent data gathered from the preceding servers and to provide the required data to the agent. The integrity of the agent data is maintained with the use of the 3-ID algorithm for both computation and verification of the agent data. This 3-ID model can protect against all types of attacks generated against the agent data.

The fourth model of the architecture is the recovery of the agent after any failure in the agent. The K-response of the recovery model is to rollback the original agent after the single or set of host attacks by having the mirror of the original agent at every host until the successful dispatch response from the succeeding host. The experimental results of this model proved that the preceding host will get the response of the successful delivery within the time-out period.

The proposed security architecture with protection and recovery model provides the confidence to the legitimate agent originator that the agent will be back without any negative impact. This integrated security model will
increase the usage of the mobile agent in all network applications with more trust and confidence.

9.2 FUTURE ENHANCEMENTS

The work reported in this thesis provides multiple types of mechanism to protect the mobile agent environment. To make the environment more secure, it needs to have further enhancements related to the agent code and platform.

i) The agent migrating to the remote host may execute dummy (spam) requests to make unavailability of resources. The MIP mechanism is extended to prevent this spam attack on the mobile agent hosts.

ii) The active attack of the mobile agent code is prevented by the Root Canal (RC) or eXtended Root Canal (XRC) algorithm, but it is not able to protect against the passive attack. It is required to have an extension to the XRC algorithm to prevent the passive attack.

iii) The $K$-response model has to be extended to identify and recover the agent while it is killed by the $K+1$ set of hosts.

iv) The trustworthiness of hosts and mobile agents has to be estimated to relax the security mechanism.