Abstract—As a recently emerging distributed computing paradigm, mobile-agent technology attracts great interests because of its salient merits. However, it also brings significant security concerns, among which the security problems between a mobile agent and its platforms are of primary importance. While protecting a platform (platform or host security) can benefit from the security measures in a traditional client-server system, protecting a mobile agent (mobile-agent or code security) has not been met in traditional client-server systems and is a new area emerging with mobile-agent technology.

We analyzed the different types of security issues related to mobile agent. After analysis, we found that there are many kind of technology available to ensure mobile agent security. But not a single technology provides complete solution for the same. We proposed an algorithm in which we use monitoring agent and dummy agent in place of original mobile agent. Monitoring agent checks the behavior of next node in the network. If monitoring agent finds the node suspicious, it sends the alert acknowledgment to original agent and original agent doesn’t travel to that suspicious node.

Index Terms—Mobile agent, distributed systems, security.

I. INTRODUCTION

Mobile agent is a heterogeneous network can autonomously migrate from one host to another host, and can interact with other agent or resource programs. Mobile agent is an important component of distributed computing. Increasingly widespread application of mobile agent, mobile agent system’s security is a prominent problem to be solved, mobile agent’s security question is critical.

Mobile agents are the objects oriented software codes, which have the characteristics like intelligence, autonomy, responsiveness, communication ability and adaptability that build them more advantageous than any other mechanism like client server in network infrastructure. Nevertheless various applications and advantages are offered by mobile agents; but these are not sufficient for its acceptance on a wider scale because of inherent security risk.

One of the main concerns with a mobile agent system is ensuring that mobile agent’s hosts are able to prevent both the theft and damage of sensitive information. The other security issue is protection of the mobile agent from malicious host.

II. PREVIOUS WORK

Mobile agent protection is difficult because of a host’s complete control over executing programs. While many approaches have been proposed to defend mobile agents from malicious hosts, none adequately addresses every aspect of security.

We survey many approaches for the problem of mobile agent protection. [1] Presents multilevel security architecture for solving the challenges of malicious host problems. They explain a multi-phase approach which preserves the flexibility and autonomy characteristics of mobile agent and ensures the protection of agent’s code, data and itinerary. [2] Use Pedersen’s verifiable secret sharing scheme and the theory of cross validation to propose an optimistic payment protocol with the following features:

(a) Protect the confidentiality of sensitive payment information from spying by malicious agents,
(b) Use a trusted third party in a minimal way, (c) can verify the validity of the share by the merchant,
(d) allows agent to verify that the product which he is about to receive is the one he is paying for. [3]
Present a scheme that aims to rescue the results being carried by blocked agent.

The significant contribution of the scheme is the real time applicability in mobile agent based applications and maximum reduction of data loss in case of blocking attacks. [4] Proposed new security mechanism which can not only satisfy security demands, but can also solve the bottleneck problem caused by trusted third party, they call the new mechanism ISTCM. In ISTCM, task sponsor first chooses a certain number of hosts as partners at random.

When agent reaches a host, the host consults the partners of encryption key. Data generated by the host is encrypted into a divisible whole for protection. At the same time, the host sends its identity information to partners according to threshold scheme. When agent comes back to task sponsor, it will compare path from passing data with path from the partners to find out if there exists attack.

Yee [5] introduced Partial Result authentication Codes (PRACs). The idea is to protect the authenticity of an intermediate agent state or partial result that results from running on a server. PRACs can be generated using symmetric cryptographic algorithms. The numbers of encryption keys are used by agent. The agent’s state or some other result is processed using one of the keys, producing a MAC (message authentication code) on the message when the agent migrates from a host. The key that has been used is then disposed of before the agent migrates. The PRAC can be verified at a later point to identify certain types of tampering. A similar functionality can be achieved using asymmetric cryptography by letting the host produce a signature on the information instead.

Hohl proposes what he refers to as Blackbox security to scramble an agent’s code [7] in such a way that no one is able to gain a complete understanding of its function. However, no general algorithm or approach exists for providing Blackbox security. A time-limited variant of Blackbox protection is proposed as a reasonable alternative.

This could be applicable where an agent only needs to be protected for a short period. One serious drawback of this scheme is the difficulty of quantifying the protection time provided by the obfuscation algorithm.

III. PROPOSED ALGORITHM

After analyzing the security issues, we proposed an algorithm to ensure the security of mobile agent from the suspicious hosts.

There will be some important steps of our proposed algorithm-

Step 1: The original agent creates a monitoring agent and a dummy agent with same script but with dummy data. With dummy agent, we send the actual script and dummy data but minimize the size of the dummy data to reduce the overhead. Monitoring agent sends the acknowledgement to original agent.

Step 2: Original agent sends the monitoring agent and dummy agent to next node to check the behavior of next node in the network.
agent finds the node suspicious, it sends the alert acknowledgment to original agent.

Step 3: If there is no harmful activity in next node then monitoring agent sends an ok acknowledgment to original agent to certify the security of original agent.

IV. CONCLUSION

After analysis, we found that there are many kind of technology available to ensure mobile agent security. Related work is done by many contributors by implementing their thoughts regarding mobile agent security. Srivastava and G.C Nandi [1] suggested multilevel security architecture for solving the challenges of malicious host problems. Liu1 and Yong [2] used Pedersen’s verifiable secret sharing scheme and the theory of cross validation to propose an optimistic payment protocol. Rajwinder and Mayank [3] present a scheme that aims to rescue the results being carried by blocked agent. Linna and Jun [4] proposed new security mechanism which can not only satisfy security demands, but can also solve the bottleneck problem. But not a single technology provides complete solution for the same. We proposed an algorithm in which we use monitoring agent and dummy agent in place of original mobile agent. Monitoring agent checks the behavior of next node in the network. If monitoring agent finds the node suspicious, it sends the alert acknowledgment to original agent and original agent doesn’t travel to that suspicious node.

We can get the success in protection of the mobile agent using dummy and monitoring agents. It solves the problem of malicious hosts occurred during the travel of mobile agent to the nodes in the networks. There may be other situation when our mobile agent is malicious; this is also a major problem of mobile agent. Lots of work is done to solve this problem and many of them are many important

REFERENCES


