Free Roaming Mobile Agent Security

Vishal Nerani, Shubham Sartape, Pranit Revandkar, Nikunj Lapasia, Mrs. Ameya Jadhav
Department of Electronics Engineering
Atharva College of Engineering,
Malad (W), Mumbai – 400067, INDIA

***Abstract* – Security in free roaming agents is especially hard to achieve when the mobile code is executed in hosts that may behave maliciously. Data security in free roaming agent without itinerary information may face more complex attacks. This paper focuses on data security in free roaming mobile agents.**

Mobile agents migrate from originating hosts to intermediate servers to generate and collect data, and return to the originators to submit after completing scheduled tasks.

Free roaming mobile agents are free to choose their respective next hops dynamically based on the data they acquired from their past journeys. Free roaming agents have no pre-defined migration paths. They select their next hop at each hop they visit based on initial requirements and current conditions.

There are many security issues to be addressed in data security in free roaming mobile for example data confidentiality, non reputability, insertion defence and truncation defence etc.

Generally security issues in mobile agents are

1. **Protection of the host from malicious code.**
2. **Protection of the agent from a malicious host trying to tamper the code and the agent data.**

Agents security is divided into code security and data security. Methods used in protect data in mobile agents count on move forms. The move forms the agents are predefined itinerary and free roaming.

Keywords – Mobile; Security; Agent; Data; Host; Malicious.

I. INTRODUCTION

Mobile agents are autonomous programs that can travel from computer to computer in a network, at times and to places of their own choosing. The state of the running program is saved, by being transmitted to the destination. The program is resumed at the destination continuing its processing with the saved state. They can provide a convenient, efficient, and robust framework for implementing distributed applications and smart environments for several reason including improvements to the latency and bandwidth of client-server applications and reducing vulnerability to network disconnection. In fact, mobile agents have several advantages in the development of various services in smart environments in addition to distributed applications.

General idea of trust enhanced symmetric key cryptography is based on encryption, decryption, and signature verification principle. By using KBS, data was encrypted into a divisible whole for protection. Getting identity information from trusted third party via KBS to make key agreement with trusted host. If the host is trusted host, verification and summarization of previous offers are done. If it is not a trusted host offer collected according to security policies to resist colluded truncation attack. When agent reaching a host, it concatenates the data generated on it with data carried by agent then encrypts them and verifying identity information. KBS gets identity information from the trusted third party periodically. When a agent comes back to the host after completes its work without any attack.

- Reduced communication costs distributed computing need interactions between different computers through a network. The latency and network traffic of interactions often seriously affect the quality and coordination of two programs running on different computers.
- Asynchronous execution after migrating to the destination side computer, a mobile agent does not have to interact with the source side computer. Therefore, even when the source can be shut down or the network between the destination and source can be disconnected, the agent can continue processing at the destination. This is useful within unstable communications, including wireless communication, in smart environments.
- Direct manipulation a mobile agent in locally executed on the computer is visiting. It can directly access and control the equipment for the computer as long as the computer allows it to do so. This is helpful in network management, in particular in detecting and removing device failures. Installing a mobile agent close to a real time system may prevent delays caused by network congestion.
- Dynamic development of software mobile agents are useful as a mechanism for the development of software, because they can decide their destinations and their code and data can be dynamically developed there, only while they are needed. This is useful in smart environments, because they consist of computers whose computational resources are limited.

II. LITERATURE SURVEY

A. Introduction

In general, an agent is a person whose job is to act for, or manage the affairs of other people. Within the context of computers, a software agent is a program that is goal directed, and performs certain tasks on behalf of its owner. The software agent is classified as a mobile agent and static agent. A mobile agent is capable of suspending their execution on one platform and moving to another platform, where it resumes execution in the network, but a static agent works on one host computer in the network, including accessing resources which are on other hosts. Computer communication in the distributed environment is enriched via the new and emerging mobile agent technology. The advantages of the mobile agent are too many and cannot be got form the static agents and conventional wed technology. Features of the mobile agent shows that it is one of the most prominent technologies for various intranet and internet applications especially in e-commerce applications. However, mobile agent technology has not been successful because of development concerns, such as reliability and security.

B. Mobile Agent Platform Protection

An agent platform has to be protected against the attacks of a malicious agent and malicious platform. Remote platforms are disrupted by the mobile agent from a malicious platform. The malicious agent that attacks the platform category represents the kind of threats, in which agents exploit the security weakness of an agent platform, or launch attacks against an agent platform. This set of threats includes masquerading, DoS and unauthorized access. The other attacks to agent platform category represent the set threats in which external entities, including agents and agent platform, threaten the security of an agent platform. This set of threats includes masquerading denial of service, unauthorized access, and copy and reply. Techniques developed for protection the agent platform include the following:

- □ Software based fault isolation
- □ Safe code interpretation
- □ Signed code
- □ Path histories
- □ Proof carrying code
- □ Policy model (authorization and attribute certificates)

C. Mobile Agent Protection

The hardest security problem is protection the mobile agent from the malicious remote host. the platform and hosts have complete control over the agents, while they are in execution. In order to protect the mobile agent, the trusted node method, trusted hardware and co-operating agent's model were developed. However, a malicious platform may cause an agent to operate incorrectly, but the existence of enough replicates ensures the correct end result. The drawbacks are the high cost to develop the model, in deciding the best offer. Some more general purpose techniques for protecting an agent included the following:

- □ Obfuscated code (time limited black box)
- □ State appraisal
- □ Digital signatures
- □ Execution tracing
- □ Mutual itinerary voting
- □ Replication and voting
- □ Encrypted functions
- □ Environment key generation
- □ Code on demand
- □ Factor of time

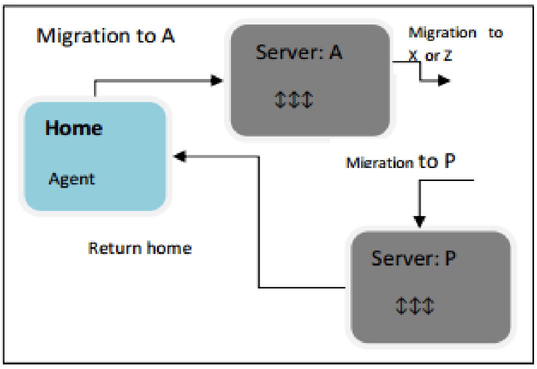
D. Mobile Agent Recovery

Apart from the protection schemes, the recovery of the mobile agent is most essential in the mobile agent environment, because an agent destroyed in the nth remote host will lose all the preceding remote host's data, and also agent originator should once again send the agent to collect the data from all the N return hosts, but there is no guarantee that the agent will return to the originator in the second round. Hence, it is required to recover the mobile agent when it I either in an unsafe mode, or destroyed. An unsafe mode is the modification of the agent code or the modification of the data collected from the preceding hosts.

Pair processing is a famous technique for improving process reliability. It is a collection of two processes which provide a service. One is considered as the primary and the other as the shadow. If the primary gets any changes, then the shadow would also gets the changes. If the primary fails, then the shadow will take over. The two primary and shadow processes ping each other to determine that each in still alive. This pair process is not applicable to the colluded host's attack in a multi-hop mobilr agent environment.

There is a significant interest in the mobile agent fault tolerance community, concerning the loss of mobile agents at remote agent servers that fail by crashing. Hence, researchers concentrated on the shadow model. However, in the event of an agent server crash, the replica remains unavailable for an unknown period.

E. Block Diagram



F. Application

Many researchers have started that there are no killer application for mobile agent technology, because almost everything you can do with MAs can done with almost traditional technologies. However, mobile agents make it easier, faster and more effective to develop, manage and execute distributed applications that other technologies. We describe typical applications of mobile agents a follows:

- □ Remote information retrieval.
- □ Network management.
- □ Cloud computing.
- □ Mobile computing.
- □ Software testing.
- □ Reduction of the network traffic.
- □ Active networking.
- □ Asynchronous autonomous interaction.
- □ Robust and fault tolerant.

III. CONCLUSION

To resolve the problem of mobile agent's security, especial on attacks on mobile agent data, paper analysed current protection mechanism and put forward KBS to enforce its security with symmetric key cryptography. The analysis shows that trust enhanced symmetric key cryptography can protect data of free roaming mobile agent effectively and realize some security needs such as data confidentiality integrity and anonymity.

ACKNOWLEDGEMENT

Our sincere thanks to the technology that allowed us to explore computer clusters by providing relevant information from different authors research papers. We would like thank Hon. Shir Sunil Rane sir for conducting this conference and giving us opportunity to present this. We are thankful to our college Principal Dr. S. P. Kallurkar, Head of Department Prof. Disha Bhosle and Project Guide Prof. Ameya Jadhav, and all staff members of Electronics department who have provided us various facilities and have guided us whenever required. We would like to express my heart-felt gratitude towards our parents and all those who encourage us to accomplish and support us in our work.

REFERENCES

[1] Salima Hacini, Zahia Guessoum, Zizette Boufaida "TAMP; a new trust based approach for mobile agent protection" Journal of Compute Viro 1. 2007 vol 3, page no 267-283.

[2] M. Yao, E. Foo, E. P. Dawson and K. Pengo An Improved Forward integrity Protocol for mobile

[3] Agents. In proceedings of 4th International Workshop on Information Security Applications (WI SA 2003), Compute Science, 2004, page no 272-285.

[4] Darren XU, Lein Ham, Mayur Narasimhan, Luo Junzhou "Improved Free Roaming Mobile Agent Security Protocol again Colluded Truncation Attacks. Proceeding of the 30th Annual (COMPSAC2006), IEEE Compute Society 2006 volume 2, page no 309-314.

[5] Y. C. Jiang, Z. Y. Xia, Y. P. Zhong, S. Y. Zhang.Defend mobile agent against malicious hosts in migration itineraries[J]. Microprocessors and Microsystems 28 (2004), page no 531-546.

[6] S. Green, L. Hurst. Software Agents: A review [J].Trinity College Dublin Broadcom Eireanm Research Ltd, 1997.

[7] Zhang Yunyong. Liu Jinde, Mobile agent technology[M]. Beijing: Tsinghua University Press, 2003.