Mobile Agent Synchronization And Security Issue

Anil B. Dongardiye
ABHA Gaikwad Patil
College of Engineering, Nagpur

Prof. Girish Agrawal
ABHA Gaikwad Patil
College of Engineering, Nagpur

Prof. Pragati Patil
ABHA Gaikwad Patil
College of Engineering, Nagpur

Abstract

Mobile Agent Systems is a new expertise it was developed for the communication between different mobile devices they have some good features but security remains the major problem in all Mobile Agent Systems for research point of view. In mobile based Communication System, there were many problems in network like low bandwidth, slow data rate, data are not secure (because signals being available in open). The subject communication runs into cyber security problems. Our main objective is to provide a highly secure environment that is simple to use and deploy. Software security to protect mobile agent consists of lots of aspects like cryptography, access control and trust management, intrusion detection and tamper resistance, authentication and privacy, signature schemes, e-commerce, security analysis, mobile computing security etc. So, to design and develop system to synchronize two or more mobile using mobile agent and JADE platform for monitoring the flow of information and execution of a running mobile agent in a secure environment.

1. Introduction

The mobile agent paradigm is a further extension to distributed computing paradigms. A mobile agent is a software piece of program with mobility which can be sent out from a computer into a network and roam among the computer nodes in the network [28]. It can be executed on those computers to finish its task on behalf of its owner. The transferring of a mobile agent state facilitates it in working automatically to travel between one or more remote computer. The key characteristic of the mobile agent paradigm is that any host in the network is allowed a high degree of flexibility to possess any mixture of know-how, resources and processors. Its processing capabilities can be combined with local resources [4]. Know- how (in the form of mobile agent) is available throughout the network. Since, the mobile agent has many salient merits, so it has attracted tremendous attention in last few years and become a promising direction in distributed computing and processing as well as high performance network area. In mobile agents, the mobile code generated by one party transfers and execute in an environment controlled by another party so several security issues arise in various mobile agent computing. These issues include authentication, authorization (or access control), intrusion detection etc. Because of mobility of mobile agent, the security problems becomes more complicated and have become a bottleneck for development and maintenance of mobile agent technology especially in security sensitive applications such as e-commerce, military applications, scientific applications etc[35]. Security issues are becoming more significant in this age of pervasive mobile network computing where we have different types of information being used by mobile and fixed large scale distributed applications interacting over wireless and wired network to deliver useful services to enterprises and users, fixed and mobile. So, the research on synchronization of two or more mobile agent in secure environment and security issues of mobile agent differs in its aim, emphasis, base and technique.

2. Introduction to Mobile Agent

Mobile agent is a new expertise that makes it much easier to design, implement and maintain spread system. Mobile agents are able to diminish network traffic load and supports functions to beat network latency. To satisfy the user need Mobile agent can implement highly robust and fault-tolerant system [9, 11].

Agent Definition

A mobile agent is a piece of program functions on behalf of a user in a distributed environment, and is able of migrate independently from one node to other to accomplish the assigned task of user [10, 15].

Mobile agent = agent + mobility

Mobile agent is the mixture of Software agent expertise and Distributed computing technology. Mobile agents are dissimilar from Remote Procedure Call (RPC) i.e. because mobile agents can move constantly from one host to another host and travels based on its own

requirements and choices. Mobile agents are unlike the common process migration, because the common process migration system cannot decide where to go and when to go by itself. However, mobile agents can migrate to anywhere at any time. Mobile agents are diverse from Java Applets, since applets can travel only one way from server to client, while mobile agents can move in between the client and the server bi-directionally.[15] Following is the architecture of a typical mobile agent system.

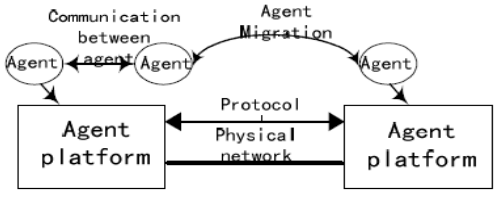

Fig 1

This system consists of two major parts, Agent platform, which provides running environment; and mobile agents, which moves between platforms to accomplish tasks using resources provided by agent platforms. Agent platforms will authorize the agents to decide their access priority[1].

JADE (http://jade.tilab.com/), developed by *Telecom Italia Lab* since July 1998, was released as *open source* in February 2000 (last version: JADE 3.4.1, November 2006). It is a very popular *FIPA-compliant* agent platform. An agent is composed of different concurrent (and non-preemptive) *behaviors*, which can be added dynamically. Among the benefits, we could indicate that there is a wide variety of tools provided (e.g., for remote management and monitoring of agents, and to track interchanged messages) and it can be integrated with different software such as *Jess*1 (a rule engine which allows JADE agents to "reason" using knowledge provided in the form of declarative rules). Finally, it is also worth mentioning its support for the development of ontologies to represent the knowledge of agents. Probably, the main disadvantage is that mobility is not a key element in JADE. Thus, it focuses on other functionalities relevant to the development of multiagent systems. The JADE built-in *Agent Mobility Service* supports mobility among containers within the same *JADE platform* (similar to the idea of *region* in Grasshopper and SPRINGS), and researchers at the *Autonomous University of Barcelona* provide an *Inter-Platform Mobility Service* (https://tao.uab.cat/ipmp/). Proxies do not exist; instead, an agent searches the current location of its target by querying the *AMS* (*Agent Management System*), according to the FIPA specifications.

3. Proposed Work

In this project, we look into the general issues in mobile agent security, paying special attention to the problem of synchronization and monitoring the flow of information and execution of a running mobile agent. A classification of threats is given and some suggested solutions are examined in detail. Then, we discuss the various security issues that arise in 'data collection agents' – agents which visit various hosts to collect data from them. In particular to synchronize two or more mobile agent and to detect the flow of information between two or more mobile agent on JADE platform.

4. SECURITY ISSUES IN MOBILE AGENTS

4.1 Attacks on Mobile Agents by Mobile Agent Platforms

In case of strong mobility of mobile agent all its code, data and state are exposed to the mobile agent platform in which it migrates for execution of operation. Because of this mobile agent faces more severe security risks. Following are possible attacks by malicious platforms [29]:

4.1.1 Leak out/ modify mobile agent's code

Since the mobile agent's code has to be readied by a guest platform, so this malicious platform can read and remember instructions going to be executed to infer rest of the program based on that knowledge .By this process, platform knows the strategy and purpose of mobile agents[15]. If mobile agents are generated from standard building libraries, the malicious platform knows a complete picture of mobile agent's behavior and it finds out the physical address and can access its code memory to modify its code either directly or by insertion of virus. It can even change code temporarily, execute it and finally resuming original code before the mobile agent leaves.

4.1.2 Leak out/ modify mobile agent's data

There are many data which are very security sensitive like security keys, electronic cash, social security number that cause leak of privacy or loss of money. If the malicious platform get to know the original location of data it can modify the data in accordance with the semantics of data[24]. Above tasks can lead to severe consequences. Even if data is

not sensitive, malicious platform can attack on normal data like traveling data of person and leaking it to somebody.

4.1.3 Leak out/ modify mobile agent's execution flow

By knowing the mobile agents physical location of program counter, mobile agent's code and data the malicious platform can predict what will be set of instructions to be executed next and deduce the state of that mobile agent. By help of this process, it can change the execution flow according to its will to achieve its goal[30]. It can even modify mobile agent's execution to deliberately execute agent's code in wrong way.

4.1.4 Denial of Service (DoS)

This attack causes mobile agent to miss some good chances if agent can finish its execution on that platform in time and travel to some other platform. DoS causes not to execute the mobile agent migration and put it in waiting list carrying delays.

4.1.5 Masquerading

Here malicious platform pretends as if it is the platform on which mobile agent has to migrate and finally becomes home platform where mobile agent returns. By this mechanism, it can get secrets of mobile agents by masquerading and even hurts the reputation of the original platform[35]. For example: malicious platform pretends an original airline company and give mobile agent a fake ticket and after receiving money, mobile agent founds the fakeness of the received ticket which in turn leads to dispute with real airline company later on.

4.1.6 Leak out/ Modify the interaction between a mobile agent and other parties

Here malicious platform eavesdrop on the interaction between a mobile agent and other parties like another agent or another platforms. This leads to extraction of secret information about mobile agent and third party. It can even alternate the contents of interaction and expose itself as part of interaction and direct the interaction to another unexpected third party. By this way, it can perform attacks to both mobile agent and third party.

4.2 Security Requirements to protect Mobile Agents

4.2.1 Authentication and Authorization

Authentication of a entity is the process of verifying the identity or other relevant information about the entity. The outcome of the authentication processes is that the user/agent knows the identity of the server/agent execution environment and the server/agent execution environment knows the identity of the user/agent. The process of deciding whether or not to grant a request after confirmation about the authentication of the principal is called authorization or access control[8]. To achieve those security properties, digital signatures are required in addition to password access.

4.2.2 Privacy and Confidentiality

Privacy requirement includes problems of confidentiality of exchanges and interactions in a mobile agent system. Since platforms are responsible for entire state of a mobile agent so mechanisms are needed that allow privacy of the information being accumulated and carried by agents to other platforms.

4.2.3 Non-Repudiation

This problem of repudiation arise when party involved in communication or activity denies its involvement. For this we should log important communication exchanges to prevent later denials. This is very important when mobile agent and mobile agent platforms commit to a digital agreement, contract, sale or any other such transactions.

4.2.4 Accountability

Since every user, agent or process on a platform is responsible for its action so we need to record not only unique identification and authentication but also an audit log of security relevant events to which both agent or process responsible for those events. All security related activities must be recorded for auditing and tracing purposes. Also, audit logs must be protected from unauthorized access and modifications.

4.2.5 Availability

This requirement ensures availability of both data and services of a mobile agent to local agents and incoming mobile agent. This mobile agent platform should ensure availability of controlled concurrency, support for simultaneous access, deadlock management and exclusive access when required[40]. Agent platform should able to detect and recover from software and hardware failures. It should have the ability to deal with and avoid Dos attacks as well.

4.2.6 Anonymity

The security policies of agent platform and their auditing requirements should be carefully balanced with agent privacy expectations. Here platform should keep agent's identity secret from other agents and maintains anonymity so as to determine agent's identity when necessary and legal.

4.2.7 Fairness

Fairness requirement means that no party can give advantage over other parties. So, in mobile agent system, mechanisms are necessary to ensure fair agent platform interaction in electronic exchange.

5. Conclusion

For mobile code computing and to realize its full potential as the software infrastructure of truly distributed computing, we must understand and develop security mechanisms that both detect and prevent malicious attacks against mobile code program[27]. All security mechanisms discussed are effective to some degree and the use of them should be retained. But most of the security measures are not adequate because they are not geared towards software i.e. mobile, works cooperatively, interacts with its own environment and reacts unpredictly to unexpected events like software flaws, human errors etc.

6. References

[1] "Designing Autonomous Agents,pgs 49-70,The MIT Press:Cambridge,MA,!990.P.Maes:Situated agents can have goals.
[2] A.S.Rao and M.P.Georgeff. a model-theoretic approach to the verification of situated reasoning systems. In proceedings of thirteeth International Conference on AI(IJCAI-93)pg 318-324,Chambery,France,1993.
[3]SHOHAM.Y.'Agent-oriented programming', Artificial Intelligence 1993,60(1)pp,51-92.
[4] S.Franklin and A.Graesser. Is it a agent or just a program? In J.P.Muller, M.Wooldridge and N.R. Jennings, editors, Intelligent Agents III(LNAI Volume1193).Springer-Verlag:Berlin,Germany,1997,pp.21-36.
[5] S.Kraus,J.Wilkenfield and G.Zlotkin. Multiagent negotiation under time constraints.Artificial Intelligence.vol.75(2)pp.297-345,1995.
[6] GENESERETH,M.R. and KETCHPEL,' software agents ',commun,ACM,1994,(7),pp 48-53.
[7] S.Russell and P.Norvig. Artificial Intelligence: A Modern Approach,Prentice-Hall,1995.
[8] Joris Claessens, Bart Preneel, Joos Vandewalle , "(How) Can Mobile Agents Do Secure Electronic Transactions On Untrusted Hosts? A Survey Of The Security Issues and The Current Solutions", pp. 38-41, ACM Transactions on Internet Technology, Vol. 3, No. 1, February 2003.
[9] J. Vitek,M. Serrano and D.Thanols. "Security and Communication in Mobile Object Systems," Mobile Object Systems: Toward the programmable Internet, J.Vitek and C.Tschudin, Eds ., Springer-Verlag, 1997.
[10] Sergi Robles, Mobile Agent system and Trust, a combined View toward Secure Sea-Data applications. July 2002. Http://www.tdx.cesca.es/TESIS_UAB/ AVAILABLE/TDX-1128102-173916//srmldel.pdf
[11] U. G. Wilhelm," A Technical Approach to Privacy based on mobile Agents Protected by Tamper-resistant Hardware", PhD Theses nr. 1961. Dept. of D'Informatique, Ecole polytechnique Federale de Lausanne,1999.URL: http:// lsewww.epfl.ch/~wilhelm/Papers/thesis.pdf.
[12] . B. Yee. Using Secure Coprocessors . Ph.D thesis , Carnegie Mellon University. 1994.
[13] Zachary ,John.2003. Protecting Mobile Code in the Wild . Internet Computing, IEEE,7(2).
[14] Wu, Xiaoping ; Shen, Zhidong; and Zhang, Huanguo.2006. The Mobile Agent Security Enhanced by Trusted Computed Technology, Proceedings of Int. Conf. ,pp. 1-4.
[15] Schelderup, K.olnes, J: Mobile agent security-Issues and Directions. In: Proceedings of the 6th Int. Conf. on intelligence and services in networks Barcelona, Spam, Apr 1999.