SECURITY OF MOBILE AGENTS ON NETWORK FOR DISTRIBUTED DATABASE

Bharti Chouksey*
Ravi Mohan*
Rajneesh Argawal**
Dushyant Sharma***

ABSTRACT

In distributed dabtabase networks Mobile agent is a very important concept & utilization of the resources available on the connected network can be improved using mobile agents because of their capability of operation on different environments, that is why, the approach is used for many network based applications like data crawling, information exchange, distributed system integrity etc. but it lacks the security aspects when applied to open network where nodes cannot be classified as they are malicious or not, hence for the cases where the security of data or reliability of agent become must we need some method to insure the security of mobile agents. Situation becomes critical when mobile agent has travelled multiple nodes and contains information from multiple nodes.

Although many other methods are proposed by many authors but some of them required a pre survey [1], encryption of important data [2] acknowledgement schemes [3], transfer of dummy & monitoring agents [4].

Here I am proposing a scheme which not only confirms the security of data but also guarantees the uninterrupted operation of agent by utilizing a dummy agent and composite acknowledgement technique as by [4] but improving the same by encryption of the data sent. This algorithm will keep two databases on each sender nodes to classify the intended nodes in two different categories. One database if of malicious nodes in which they will keep the details of the malicious nodes for which they will keep information related with the nodes informed to be malicious by the dummy agents and second will keep the information of the healthy nodes, which are found to be non malicious by the dummy agents. This will reduce the unnecessary delays in retrieving information from the distributed database network system and will avoid lot of security setback beforehand. Introduction of the database at the sender will be updated periodically by sending dummy packets on the intended nodes so it will have updated information all the times. The proposed mechanism also ensures that if in case any where mobile agent is being captured by the malicious node its upstream node will

send the available information to the starting node so that the collected information will not be lost up to the upstream node.

***Keywords**: Mobile Agent, Security, Distributed database, Computing, Encryption.*

*Shri Ram Institute of Technology, (SRIT), Jabalpur, M.P., India.

**CTA Branch, Shri Ram Institute of Technology, (SRIT), Jabalpur, M.P., India

***Assistant Professor, Shri Ram Institute of Technology, (SRIT), Jabalpur, M.P., India

1. INTRODUCTION

Mobile agents are mobile autonomous processes operate on behalf of users in a distributed computing environment. The autonomous agent concept has been proposed for a variety of applications on large, heterogeneous, distributed systems (e.g., the Internet) [5]. These applications include a specialized search of a middleware services such as an active mail system, large free-text database [6], electronic malls for shopping, and updated networking devices. Mobile agent systems have many advantages over traditional distributed computing environments. They use less network bandwidth, increase asynchrony among clients and servers, dynamically update server interfaces and introduce concurrency [7].

Due to the problems with security of Mobile agents have limited their popularity. Mobile agents are composed of code, data, and state. Agents migrate from one host to another taking the code, data and state with them. The state information allows the agent to continue its execution from the point where it left in the previous host. For example, a mobile agent could be migrated from the home platform with the task of buying an airplane ticket for its owner. The agent would visit all the known hosts of airline companies, one after another, to search for the most reasonably priced ticket, and then purchase one for its owner. Each time the agent moves to the next host, it summarizes the current state, execution pointer on the current state, etc., so that it can start searching for reasonable tickets on the next host. The state of the agent will contain a set of possible tickets to be considered for purchase. When the agent has finished its search, it may return to the host where it found the cheapest or best ticket and purchase it.

While agents roam around the Internet, they are exposed to many threats and may also be a source of threat to others. Sander and Tschudin present two types of security problems that must be solved [8]. The first is host protection against malicious agents. The second is agent protection against malicious hosts. Many techniques have been developed for the first kind of problem, such as password protections, access control, and sand boxes, but the second problem seems to be difficult to solve. It is generally believed that the execution environment (host) has full control over executing programs; thus, protecting a mobile agent from malicious hosts is difficult to achieve unless some tamper-proof hardware is used. For example, Yee proposed an approach in which a secure coprocessor is used that executes critical computations and stores critical information in secure registers [9].

In his paper [4], has proposed to protect the agent data and agent itself a method which not only protects the data but also agent have been proposed. The algorithm did not required

previous travelling path of node and even the encryption is not required. Here, agents with dummy data are created and service monitoring agent which generates the acknowledgment for host which is malicious or not, but this method lacks the security in case when the agents fails to be malicious after some time, as malicious programs can be programmed to start executing after a little delay in which the dummy agent decides that the node is not malicious. Therefore I am proposing to this algorithm as the information on the actual mobile agent will be encrypted and also if the next node in path found to be malicious then it will send the collected information to the source till the malicious node.

3.0 DISTRIBUTED DATABASE

A distributed database is a database in which storage devices are not all attached to a common CPU. It may be stored in multiple computers located in the same physical location, or may be dispersed over a network of interconnected computers.

Collections of data (e.g. in a database) can be distributed across multiple physical locations. A distributed database can reside on network servers on the Internet, on corporate intranets or extranets, or on other company networks. The replication and distribution of databases improves database performance at end-user worksites.

To ensure that the distributive databases are up to date and current, there are two processes: replication and duplication. Replication involves using specialized software that looks for changes in the distributive database. Once the changes have been identified, the replication process makes all the databases look the same. The replication process can be very complex and time consuming depending on the size and number of the distributive databases. This process can also require a lot of time and computer resources. Duplication on the other hand is not as complicated. It basically identifies one database as a master and then duplicates that database. The duplication process is normally done at a set time after hours. This is to ensure that each distributed location has the same data. In the duplication process, changes to the master database only are allowed. This is to ensure that local data will not be overwritten. Both of the processes can keep the data current in all distributive locations.

Besides distributed database replication and fragmentation, there are many other distributed database design technologies. For example, local autonomy, synchronous and asynchronous distributed database technologies. These technologies' implementation can and does depend on the needs of the business and the sensitivity/confidentiality of the data to be stored in the database, and hence the price the business is willing to spend on ensuring data security, consistency and integrity.

2.0 EXISTING SYSTEM

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. I have surveyed three proposed approaches for the Neelesh kumar Panthi et al. / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 1 (4), 2010, 208-211 208 problem of mobile agent protection. The three approaches are chosen because each approach is very uniquely implemented and has strengths that other approaches do not have; we choose Partial result authentication code approach because it can protect results from mobile agents. Computing with encrypted functions approaches is chosen because it tries to scramble code and data together. An obfuscated code approach is chosen because it scrambles an agent's code in such a way that no one is able to gain a complete understanding of its function.

Mobile agent is software written in platform independent language or package. Because of self mobility of software through which it can transfer to itself from one to another system connected in network. During this operation it can exchange the required data from each system as per requirement or according to script.

Because of mobility of agent it is very helpful for utilizing the network resources. But the problem with this type of system is security of the agent, because it holds the important data and when it executes on some platform the platform takes on the complete control of it, and hence retrieves the complete data or can temper the agent. Hence, to protect the agent data and agent itself we are proposing a method which not only protects the data but also agent. The proposed algorithm did not required previous travelling path of node and even the encryption is not required.

3. PROPOSED SYSTEM

The above algorithms, as stated in existing system, suffers the problem of delayed processing of malicious nodes and information loss when the node is found to be malicious in between the path. My proposed algorithm is going to address to the above problems and will provide a feasible solution for the same. Steps in providing the secured implementation of the same are as follows:

Here I am proposing a scheme which not only confirms the security of data but also guarantees the uninterrupted operation of agent by utilizing a dummy agent and composite acknowledgement technique as by [4] but improving the same by encryption of the data sent. This algorithm will keep two databases on each sender nodes to classify the intended nodes in

two different categories. One database if of malicious nodes in which they will keep the details of the malicious nodes for which they will keep information related with the nodes informed to be malicious by the dummy agents and second will keep the information of the healthy nodes, which are found to be non malicious by the dummy agents. This will reduce the unnecessary delays in retrieving information from the distributed database network system and will avoid lot of security setback beforehand. Introduction of the database at the sender will be updated periodically by sending dummy packets on the intended nodes so it will have updated information all the times. The proposed mechanism also ensures that if in case any where mobile agent is being captured by the malicious node its upstream node will send the available information to the starting node so that the collected information will not be lost up to the upstream node.

REFERENCES

1. Mei Wu, "The Application of MA-based distributed database in the measurement" School of Business, China West Normal University, Nanchong, China, Biabia220@126.com
2. Ichiro Satoh. Selection of Mobile Agents. In Proceedings of the 24th International Conference on Distributed Computing Systems (ICDCS'04). IEEE Computer Society Press, 2004.
3. J. White, "Mobile Agents White Paper," General Magic Inc., 1996.
4. D. Milojici, "Mobile agent applications", IEEE concurrency, July-Sep 1999, pp 80- 90.
5. Neelesh Kumar Panthi, Ilyas Khan, Vijay k. Chaudhari "Securing Mobile Agent Using Dummy and Monitoring Mobile Agents" Department of Information Technology, T.I.T. Bhopal, India.
6. Chandra Krintz, Security in agent-based computing environments using existing tools. Technical report, University of California, San Diego, 1998.
7. Joshua D. Guttman and Vipin Swarup. Authentication for mobile agents. In LNCS, pages114–136. Springer, 1998.
8. Neeran Karnik. Security in Mobile Agent Systems. PhDthesis, Department of Computer Science and Engineering. University of Minnesota,1998.
9. Tomas Sander and Christian F. Tschudin. Protecting Mobile Agents Against Malicious Hosts.In Giovanni Vigna, editor, Mobile Agent Security, pages 44–60. Springer-Verlag: Heidelberg,Germany, 1998.

10. Bennet Yee. Using Secure Coprocessors. PhD thesis, Carnegie Mellon University, 1994.