Design of a Mobile Agents Based Solution to Distributional Management of Computer Networks, Taking into Account the Security Mechanisms

Saeed Bahrami
Department of Science
Farhangian University
Qazvin, Iran
saeedbahrami13@chmail.ir

Abstract—**Mobile agents (MAs) is one of the technologies considered in the recent years to perform management processes. This technology provides the ability to move code in distributed environments and to connect with other resources and agents locally which makes it an appropriate technology in the development of software applications of distributed network, especially management systems. For using mobile agent technology, an infrastructure for the management of MAs is needed. In this project, an infrastructure called MCT management is introduced for network management. In this infrastructure, some protocols like SNMP are used to get management data for the network administrator. With respect to management ability, MAs can dynamically access the database SNMP (i.e. MIB) and extract the data required by the managers. Most well-known methods are characterized by being static relative to code and location in which components cannot modify their location or code in a lifetime. However, the MAs method can dynamically increase communications, reduce costs and overcome certain limitations by changing location and components.**

Keywords-design; Mobile Agent; security mechanisms; MCT

I. Introduction

For a long time the Client-Server (C/S) model has been applied for various network affairs. In this model, a computer, taken as the Client, demands a request from another device as a server and returns the response. The relationship between the two is done in sync format and can be done in RPC and Message Passing [1]. This method is frequently used in network management systems including distributed systems. Network management can be a process of controlling a network with complex data for maximizing its efficiency. Given that network systems are constantly increasing their size, their management with modern styles is not efficient, because of the stability, synchronous operation, transfer of massive data and homogeneous acts. In order to overcome such limitations, various decentralized methods have been recommended. One of these methods is the use of Mobile Agents (MAs). Agents are actually codes moved from a network element to another and communicate with local resources and other agents, returning the data of one network element to the manager. Because of their movement, agents are called mobile. Due to their ability to move in distributed environments, MAs are very suitable for the development of distributed software applications, especially in network management systems where the decentralization of management operations is one of the main characteristics. In this mode of operation, management duties are delegated to the Agents and a number of them can be dynamically distributed between management entities in the network management system. Using migration capacities, they can communicate locally using this protocol, and according to information already stored, use the hardware and software necessary for the operations management.

In this paper, first the case of MA technology and its management is introduced and then the managing infrastructure called MCT is presented and its connection with SNMP is also expressed. Then, in simulation mode, the communication of MA and MIB, SNMP for administrators is designed in order to monitor and control the network.

II. Network Management by the MA Scheme

One of the major problems in the C/S method occurs due to large data volumes that do not improve network's efficiency. As noted earlier, client-server communication is synchronous in C/S model. Although this method performs well in some aspects, higher applications in distributed systems will reduce the quality of connections and cause problems in applications due to the synchronous nature of communications. Therefore, MAs are proposed as a new method that instead of moving the data to the code, it moves code towards the data. The efficiency of the method depends on the code/data volume relation. This method basic function is that a code form agent is sent to the station(s). The code carries the operations defined on it and then returns the required information in two ways: directly or by assigning it to another agent [2]. According to the motion, this method is particularly suitable for distributed environments. With respect to their performance (mobility) MAs have enormous potential. For example, they can stop their run at one point and resume execution at another location until the interruption point [3]. Agents can also communicate with stations locally [4, 5]. These capabilities have advantages over the traditional method of C/S that include: overcoming network latency, reducing network load, working in heterogeneous environments, being adaptable to dynamic form and being fault-tolerant. This feature also makes this method capable of being used in various fields, one of them being the field of network management. SNMP protocol is widely used for network management [6]. In this protocol, all properties of the system either software or hardware are stored in a table called MIB. In reality, regarding the existence of different types of Agents, they can be moved towards various stations, as the required data is extracted from MIB table and report to the manager. Therefore, Agents can be used in different network management fields including fault management, configuration management, performance management and audit management applications.

III. The security mechanisms of mobile agents

A. Security Threats

Agents provide great opportunity for misuse and improper use, widening the range of threats [7-9]. To discuss on security is enough for one to select a simple method that consists of two parts: Agent and Agent Platform. An Agent includes code and data that required performing calculations. Mobility provides the possibility of movement and circulation of Agent among the Platforms. Agent Platform provides the necessary environment for the Agent to perform calculations and computing affairs. A Platform that an Agent stems by is called a Home Platform, which is usually the safest environment for an Agent. A Host may contain one or more Agent Platforms and an Agent Platform may protect several computing environment and meeting places where Agents are connected. Four categories of threats have been detected including threats created by the attacks of an Agent to an Agent Platform or an Agent Platform to the Agent and an Agent to another Agent in the Agent Platform, or when other entities attack to System Agent. The last classification covers the attack of an Agent to another Agent and attack of an Agent Platform to another Platform because these attacks at first focused on Platform communication capabilities and benefit from potential vulnerabilities. The last classification also includes conventional attacks against the operating system under Agent Platform. For more studies about security, readers can refer to [10-13].

B. Security Requirements

Users of networked computer systems, have four kinds of security requirements: the ability to be faithful, integrity, responsibility or accountability and accessibility. Agent users and framework of MA also need the above requirements (confidentiality, integrity, responsibility or accountability, accessibility, and anonymity.)

C. Countermeasures

Many Agent systems relied on a series of hypothetical demarcation lines with regard to the issue of safety. First, an Agent relies on its Home Platform, where it has been established and its implementation begins. Afterwards, Home Platforms and other Agent Platforms who rely in this case can be safely realized without defect or deficiency. Third, coding or encryption which is in the beginning in the form of digital signage and used in the list of revoked or certificated, is supervised and managed by a specific and general infrastructure based on Mobile Agent. In order to create a system based on MA, a sub-structure is required. Each infrastructure should be capable of running a defined Agent and can move it in different machines, and even, if necessary, is able to establish communication between Agents. Also it provides the necessary security operations for the Agent and infrastructure. Unfortunately no infrastructure with the desired security could have been created so far. All MAs based infrastructures work on the Java Virtual Machine (JVM). So first the JVM is installed; then, the working infrastructure will be installed. Of course there are a lot of infrastructures, but very few of them are standardized. There are two standards named MASIF and FIPA for them, as we select one of them named Grasshopper which is based on MASIF standard for simulation of one of the network management operations. In the simulation process, we created 3 locations where one of the Agents starts to move on the other two virtual machines and reports on a management accounting in telecommunication networks.

IV. Simulation and results

Various experiments in the following manner were conducted to evaluate both types of network management, each one was individually investigated and the results were recorded.

A. Effect of the Number of Network Managed Elements (MNE)

First, we investigate the effect of managed network elements to assess the response time. Assumptions: the request / response length was fixed (50 bytes), with 2 Mbps rate of data communication, the delay of data connections was within milliseconds and initial number of the MAs was five obtained as a result of the experiments. Test: behavior of MAs does not change according to the type of topology and is almost constant, but in SNMP response times in different topologies increase faster by increasing the number of managed elements, because packets surveyed in SNMP are dependent on the type of topology. This experiment shows that if the number of managed elements is low, SNMP works better than MA because the SNMP message is smaller than the initial value of MA. As managed elements increases, the response time for SNMP shows a proportionate growth, while is faster for MA. Result: Between the two areas, by increasing managed elements, MA performs better than SNMP.

B. Effect of Initial Value of MA

In this section, we investigate the effect of initial value of MA on response time. Assumptions: data communication rate was in Mbps and connections delay was 4 Ms. Testing was started by different initial values of MA (1, 3, 5, 7, 9 KB) and other affairs are as noted before. Experiment: Conducted tests showed that for smaller number of elements less bites are used for MA. But when the number of MNEs increases, MA is more suitable, according to the PDU Getreguest, UDP and Ipheader. As the size of MA increases, the number of bytes depended on the management station also relatively increases. In the case of response time, as the number of MNE increases the difference between the types of MA size increases faster. For example, MA with size of 5 K has a better performance than SNMP in MNE less than 200. But in more than 200, response time of SNMP is less. Results: The lower initial value of MA, the better it performs than the SNMP.

C. *Effect of Task*

In this section, we examine the effect on response time regarding the kind of action. Assumptions: first action is 5 bytes in length (like the previous sections), the second action has a request / response with a length of 400 bytes and the third action has a variable length of 150 bytes. MA size is 5 KB and topologies are like the previous section. Experiment: According to test carried out on these three different size actions, it showed that when the MA or SNMP are used for network management, different response times are obtained. In SNMP type of operation does not have a high impact on response time (very small difference), because in fact the number of bytes exchanged between the management station and MNEs is low, but in MA, because the number of exchanged bytes increases (for example, from the first to the third action) response time also increases because MA is transmitted with more problems. The result: By increasing the size of an action, response time increases in MA and is nearly constant in SNMP.

D. *Effect of Unload Strategies*

In this part, two strategies are considered for MA. First their performance is explained and then we examine which of them is better. Assumptions: We consider the three different actions of previous section. The maximum number of visited elements is from 1 to 240. MA topologies and sizes are as the previous section and the number of visited elements in sweep is the same. Test: In the previous sections was revealed that size of MA has a direct relationship with number of visited elements, which means that as the number of visited elements increase, MA size also increases and as a result migration is more difficult. Now consider two strategies to evaluate this issue:

- The first strategy (S1): MA is returned to the management station with the results.
- Strategy 2 (S2): MA only returns the results to the management station. (Number of elements that MA passes during the sweep is fixed.)

1) *Strategy 1 (S1)*

Experiments show the response time of strategy S1, when the number of managed elements in the path of movement visited by the Agents is greatly reduced. If the visited nodes during movement are rising up to a specific point, the response time is decreased, and it increases if the number of Agents raises and creates problems for motion. The optimum point for the number of nodes for this strategy is 16. The tests are shown in Table I.

TABLE I. RESPONSE TIME IN S1 STRATEGY WITH DIFFERENT OPERATIONS

Numbers	Elements per trip	Taskt1(s)	Taskt2(s)	Taskt3(s)
1	1	32.54	32.63	32.73
2	2	19.44	19.53	19.63
3	8	9.80	10.02	10.25
4	16	8.34	8.75	9.16
5	30	8.54	9.29	10.03
6	60	8.82	10.28	11.75
7	120	10.03	12.93	15.83
8	240	12.78	18.56	24.35
9	SNMP	10.21	10.75	11.30

Based on the data of this Table, the response time is up to 62% compared with optimal point (16 elements) of t1 and t2 operations, and is reduced by accumulation of all 240 variables in path. The strategy optimized for all operations works better than SNMP. For a smaller number of elements in motion, size of operation has no effect when MA has a low size, but when number of elements in the movement is bigger, for example, 240, difference between practices is significant. Therefore, increase of the size effect, makes this strategy better.

2) *Strategy 2 (S2)*

Response time in S2 strategy has an optimum point. The following Table shows the results of tests performed in accordance the results. Based on Table II, the response time is up to 64% compared with optimal point of t1, t2 and t3 operations and is reduced with accumulation of all 240 variables in path.

TABLE II. RESPONSE TIME IN S2 STRATEGY WITH DIFFERENT OPERATIONS

Numbers	Elements per trip	Taskt1(s)	Taskt2(s)	Taskt3(s)
1	1	21.22	21.54	21.86
2	2	13.86	14.19	14.51
3	8	8.58	9.03	9.48
4	16	7.84	8.45	8.86
5	30	8.38	9.13	9.87
6	60	8.74	10.20	11.67
7	120	9.99	12.89	15.79
8	240	12.76	18.54	24.33
9	SNMP	10.21	10.75	11.30

Comparison of both strategies for action, t1, indicates that S2 performs better when the number of managed elements in path is low, compared to the case where MA's code is not sent to the management station. As the number of elements in path is increased, both methods act in the same way, because the size of the data collected by the Agent becomes more than the size of MA code. In this experiment, the initial value of MA also has an effect. Because the initial value of MA is lower response time is also less. The result: if the number of elements met in path is high (more than 16) and if results are returned to origin or MA is returned associated with MA, they act in similar ways.

E. Effect of the Data Rate of Domain Links

In this section, we want to know how data rate affects the connections made between domain links. Assumptions: Each request / response possess 50 bytes data, data rates are of 1, 2 and 0.064 Mbps, connections delays of 4 ms and the initial MA value of 5 kb. According to the operation performed on different data rates, the results show that in lower data rate (0.064), SNMP and MA both have more response time (but response time of MA is more than SNMP). But for other data rates, both have almost the same response time. Results: When data rates are higher, MA and SNMP have a better performance compared to the case where data rates are lower.

V. Conclusion

Considering their performance, MAs have many capabilities. They can stop running in one point and continue running from that stop point in another location. They perform synchronously and they can communicate with stations locally. These capabilities offer them advantages over the traditional Client-Server scheme. SNMP protocol is widely used for network administration. In this protocol, all traits and characteristics of the system are stored in a MIB table. In fact, different existing agents can be moved to different stations to extract data required by administrator from MIB table of each station and report to the administrator. In this study, an MA based solution was designed to manage distributed computer networks, taking into account security mechanisms. In this project, an infrastructure called MCT is introduced for network management. Results of simulation have revealed that between the two areas, by an increase of the managed elements, MA works better than SNMP. If the initial MA value is lower, it performs better than SNMP. Increasing the size of an action leads to an increase of MA response time but it is almost constant at SNMP when the number of visited elements in the path is large (more than 16). MA acts almost the same and in higher data rates, if the MA is returned by the result or the result only is returned to the source. MA and SNMP work better in the conditions where data rates are lower.

References

[1] K. Fall, K.Varadhan, NS Notes and Documentation, VINT project,2015

[2] A. Campeau, Managing Networks with Mobile Code, Tech. Report SCE-97-O9, Carleton University, 1997

[3] S. Green, L. Hurst, B. Nangle, P. Cunningham, Software agents: A review, Trinity College Dublin, 1997

[4] G. Goldszmidt, Y. Yemini, “Distributed management by delegation, Distributed Computing Systems”, 15th IEEE International Conference on Distributed Computing Systems, pp. 333-340, 1995

[5] T. White, A. Bieszczad, B. Pagurek, “Distributed fault location in networks using mobile agents”, in: Intelligent Agents for Telecommunication Applications, Springer Berlin Heidelberg, 1998

[6] A. Bieszczad, B. Pagurek, T. White, “Mobile agents for network management”, Communications Surveys, Vol. 1, No. 1, pp. 2-9, 1998

[7] A. Fuggetta, G. P. Picco, G. Vigna, “Understanding Code Mobility”, IEEE Transactions on Software Engineering, Vol. 24, No. 5, pp. 342-366, 1998

[8] W. A. Arokiasami, P. Vadakkepat, K. C. Tan, D. Srinivasan, “Interoperable multi-agent framework for unmanned aerial/ground vehicles: towards robot autonomy”, Complex & Intelligent Systems, Vol. 2, No. 1, pp. 45-59, 2016

[9] P. D. O'Brien, R. C. Nicol, “FIPA—towards a standard for software agents”, BT Technology Journal, Vol. 16, No. 3, pp. 51-59, 1998

[10] S. Javanmardi, M. Shojafar, S. Shariatmadari, S. S. Ahrabi, “Fr trust: a fuzzy reputation–based model for trust management in semantic p2p grids”, International Journal of Grid and Utility Computing, Vol. 6, No. 1, pp. 57-66, 2014

[11] Z. S. Daliri, S. Shamshirband, M. Amiribesheli, “Railway security through the use of wireless sensor networks based on fuzzy logic”, International Journal of Physical Sciences, Vol. 6, No. 3, pp. 448-458, 2011

[12] M. Shojafar, S. Javanmardi, S. Abolfazli, N. Cordeschi, “FUGE: A joint meta-heuristic approach to cloud job scheduling algorithm using fuzzy theory and a genetic method”, Cluster Computing, Vol. 18, No. 2, pp. 829-844, 2015

[13] S. Shamshirband, S. Kalantari, Z. Sam Daliri, L. Ng, “Expert security system in wireless sensor networks based on fuzzy discussion multi-agent systems”, Scientific Research and Essays, Vol. 5, No. 24, pp.3840-3849, 2010