Performance Evaluation of Mobile Agent within Domain Using Security Bank

Hans Raj
Research Scholar
Department of computer and System Sciences
Jaipur National University, Jaipur, Rajasthan, India
shavirajkumar786@gmail.com
Dr. V.S. Dhaka
Department of computer and System Sciences
Jaipur National University, Jaipur, Rajasthan, India
vijaypal.dhaka@gmail.com

---ABSTRACT---

Data transmission through computer network using Mobile agent system is very popular way. Mobile agent is a software entity, it can travel through communication channel and execute there and accomplish the given task. It can travel hope to hope. During the journey it can suspend their execution in one host and resume its execution in another host. When mobile agent suspends their execution and resume then there faces various security threats. It can be threatened by the host platform as well as by another mobile agent within which the mobile agent is executed. My presentation is focus on the risks and various security issues in the field of mobile agent. There are various kinds of risks faces by the mobile agents. We try to overcome the risk and provide some security mechanism how to avoid from such types of risk.

KEYWORD: ***Security, Domain, Agent Platform, Security Issues, SAB.***

---

1. INTRODUCTION

Mobile agents are independent software entities and can executes in agent platform and can make there journey from one platform to another platform in a network to do their operation assigned by their creator. In the journey of hope to hope of the mobile agents, they can face various numbers of security problems and threats. Mobile agents can suspend its operation of execution of task in one host platform and resume its operation of execution of task in another host platform [9] .When mobile agent resume its operation of task, It can loss some of its important and secret information and secret data. Mobile agent have their personal information like, secret code, state and some of its personnel information and secret password .These personal information are corrupted by host platform and another mobile agent operated under that host platform environment. So in Mobile system Number of agents works together and uses the personal resources of concerned host platform in their own way. Mobile Agent platform is a framework that can provides the environment for mobile agents to be operated there. A mobile agents can make a visits on agent platform and operate its task according to the owner of mobile agent and task assigned by the owner of mobile agent This paper focus on Security risks, issues and method through which mobile agent is able to determined whether the particular domain is beneficial to operate or not. Through this proposed mechanism the percentage of an attack from malicious agent platform on mobile agent is less up to some extent. A Domain has mainly two parts i.e. agent Platform and mobile agent and these both parts are controlled by the Security Alert Bank (SAB). SAB provides the security tips to the mobile agent in advance. It can have all previous history of visits on that particular domain. SAB works with all domains to guide the mobile agents. Mobile agent can move around the domain and do their necessary computation and send result back to the SAB and their owner. In the fields of mobile agents there are various security issues, these security issues are Transfer Security, authentication and Authorization Security, Host system Security, Computational environment Security.

2. OBJECTIVES

1 To study the behaviors of mobile agents and make there analysis according to their personal state and code.
2 Study about various attacks in the field of mobile agent.
3 Apply security techniques to overcome the risk and attacks.
4 To compile the research work in the form of Ph. D thesis based on the results obtained.

3. EXISTING TECHNIQUES [6] TO PROTECTING THE AGENT AND AGENT PLATFORM:

1. Software-Based Fault Isolation,
2. Safe Code Interpretation,
3. Signed Code,
4. Authorization and Attribute Certificates,
5. State Appraisal,
6. Path Histories,
7. Proof Carrying Code.

4. RESEARCH METHODOLOGY

The proposed techniques can provides the mobile agents a past visited history about the mobile agent platform behaviors in advance and alerts the mobile agents either the visited domain is safe to make a visit or not to do their necessary operation. Through this approach the mobile agent is awakened about the security risk to lose their data or code. SAB has full knowledge about all security weakness of the particular domain. Domain has the harmful level , this value tells about the unfair behavior of the domain to mobile agents and Status Value of agent Platform tells the reputation value of agent platform. This reputation value tells about the malicious behavior of the agent platform. Mobile agent is a defined as an entity that can be travels from hope to hope in the network to do their task and move back and give response to their owner. In the field of mobile agent there are various kinds of threats and security weakness and issues that can create the problem in the operation of code or task of mobile agent. In our proposed security mechanisms the security Alert bank can provides the advance security to the mobile agent and make the mobile agent very secure.

5. SIMULATION RESULTS

In our process of simulation, we virtually build a SAB (Security Alert Bank) and Domain. Each Domain reference one SAB. Here SAB has the information about the HL (Harmful Level) and ST (status Value) of the concerned Domain. Initially the HL build a SAB (Security Alert Bank) and Domain. Each Domain reference one SAB. Here SAB has the information about the Harmful Level value for the domain assigned 0 and Status value for Agent platform is 1.Agent platform connected within each Domain. In this scenario there are five Domains and Five SAB. Domain 1 has connected to SAB 1, Domain 2 connected to SAB 2, Domain 3 connected to SAB 3, Domain 4 connected to SAB 4 and Domain 5 connected to SAB 5. In Domain 1 there are five numbers of AP's (Agent Platforms). If any mobile agents want to visit any Domain then it can first check HARMFUL LEVEL and STATUS Value of that Domain and platform for that mobile agent concerned to the SAB of that Domain for verification of HARMFUL LEVEL and STATUS values. If these HARMFUL LEVEL and STATUS values are acceptable then mobile agent can make a visit to that domain. Otherwise if the HARMFUL LEVEL and STATUS value of the domain is not acceptable then mobile agent can migrate on to the next domain and check the HARMFUL LEVEL and STATUS values of next domain from there concerned SAB. In this simulation any mobile agent sent on to the domain 1. Mobile agent assigned HARMFUL LEVEL and STATUS values by the creator of mobile agent, in domain 1 mobile agent can visit in AP 1(Agent Platform 1) .In AP 1 there are two check points, one for visit and other for malicious agent. When mobile agent enters in the domain 1 then visit check point of AP 1 make checked. So that in AP1 mobile agent make a first visit, after this visit we can check the HARMFUL LEVEL and STATUS values for that we simulate by making click on simulate button . This simulation can verify the HARMFUL LEVEL and STATUS values of the domain and agent platform. In first visit the HARMFUL LEVEL value of platform is 1 and HARMFUL LEVEL values for the domain is -1 , next time if another mobile agent visit the domain 1, then the HARMFUL LEVEL value of the domain is -2 and STATUS value is remained unchanged i.e.1, STATUS value remain unchanged because mobile agent has successfully completed their task. In next time another mobile agent visit that domain and at that time the agent platform can change or update the information of the mobile agent, this is due to the malicious behavior of agent platform ,in that visit the malicious check point of the AP1 make checked. In this visit (3rd visit) the STATUS value and HARMFUL LEVEL value of domain is changed. HARMFUL LEVEL value incremented by 1 and STATUS value is decreased. So that HARMFUL LEVEL and STATUS value for the domain has been changed in every step it will incremented or decremented depends upon the nature of the visit. If the mobile agent has successfully completed their task then STATUS value increased and if the mobile agent doesn't complete their task successfully then STATUS value decreased. So that HARMFUL LEVEL value also changed according to their visit on the basis of the nature of visit of the mobile agent

Table 1: Show simulation results for AP-1 in Domain 1

Sr. No.	Mobile Agents visit in the AP-1	No. of effected Mobile Agents from risky AP	Status Value For AP-1	Harmful level for Domain-1
1	1	0	1	-1
2	2	0	1	-2
3	4	2	0.7	-1
4	7	2	0.892857	0
5	10	5	0.727272	1

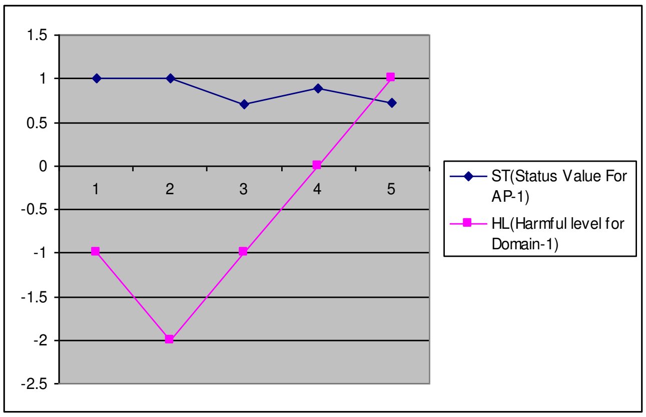

Figure 1: Represents HL and ST values for AP 1 in Domain-1 Simulation Results for Domain-2

Table 2: Represents Simulation results for AP-1 in Domain -2

Sr. No.	Mobile Agents visit in the AP-1)	No. of effected Mobile Agents from risky AP	Status Value For AP-1	Harmful level for Domain-1
1	1	0	1	9
2	3	0	1	10
3	5	2	0.8	11
4	8	5	0.583333	12
5	10	7	0.490909	13
6	12	9	0.423076	14
7	13	10	0.395604	15

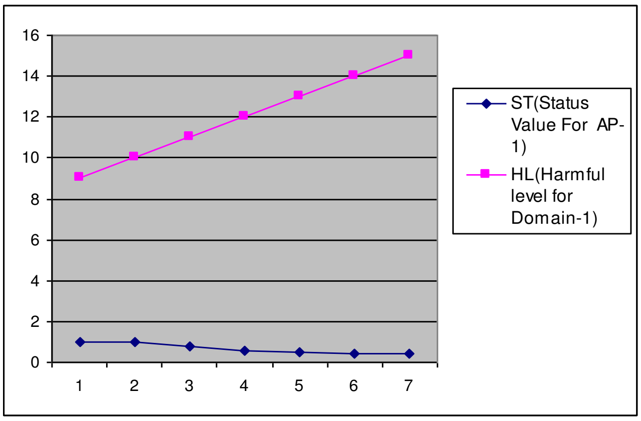

Figure 2: Represents HL and ST values for AP 1 in Domain 2

CONCLUSION

The proposed method is implemented for mobile agents and behalf of results obtained that may possible to avoid from the risk of malicious attack of agent platform in the particular domain for data transmission in secure way.

REFERENCES

[1] Fragkakis, M., Alexandris, N., “Comparing the Trust and Security Models of Four Mobile Agent Platforms”, RCIS’07, April 2007.

[2] Fragkakis, M., Alexandris, “Threats to the Trust Model of Mobile Agent Platforms”, ICSOFT 08, 5-8 July, 2008.

[3] J. Ametller, S. Robles, J. A. Ortega-Ruiz, “Self-Protected Mobile Agents”, AAMAS'04, New York , July 19-23, 2004.

[4] P. Ahuja1, V. Sharma,” A JADE Implemented Mobile Agent Based Host Platform Security”, Computer Engineering and Intelligent Systems, ISSN 2222-1719 (Paper) ISSN 2222-2863 (Online) Vol 3, No.7, 2012.

[5] Najmus Saqib Malik, Friedrich Kupzog Institute of Computer Technology Vienna University of Technology Vienna, Austria malik, kupzog@ict. tuwien.ac.”Domain based Security for Mobile Agents”.

[6] R. Shrivastava, P. Mehta (Gahoi),” Analysis of Secure Mobile Agent System”, International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-1, March 2012.

[7] M. Aggarwal, Nipur, Pallavi,” Hierarchal Model to Prevent DoS Attack in Mobile Agents”, International Conference in Recent Trends in Information Technology and Computer Science (ICRTITCS - 2012) Proceedings published in International Journal of Computer Applications® (IJCA) (0975 – 8887),vol 4, issue 2, no 7 to 11 2012.

[8] A. Orso, M.J. Harrold, and G. Vigna, “MASSA: Mobile Agents Security through Static/Dynamic Analysis” Proceedings of the First ICSE Workshop on Software Engineering and Mobility Toronto, Canada April 2001.

[9] R M. Dikaiakos and G. Samaras, “A performance analysis framework for mobile-agent systems,” Proceedings of 1st Annual Workshop on Infrastructure for Scalable Multi-Agent Systems, 4th International Conference on Autonomous Agents 2000, ACM, Barcelona June 2000.

[10] L. Ismail College of IT United Arab Emirates University P.O.Box 17551, Al-Ain, United Arab Emirates Journal of Communications, Vol. 3, no. 2, April 2008.