International Journal of Latest Trends in Engineering and Technology
Vol.(11)Issue(2), pp.082-086
DOI: http://dx.doi.org/10.21172/1.112.13
e-ISSN:2278-621X

TOWARDS ANALYSIS OF MOBILE AGENT SYSTEM IN NETWORK ENVIRONMENT

Arihant Khicha[1], Dr Praveen Kumar[2]

Abstract. Mobile agents are a modern and optimistically better network computing pattern compared with the currently used approach to remote computing, based on a client–server model. Generally a network environment is a system which can take advantage of vulnerability of the mobile agents that has come to the host machine to get it work done. Threats against mobile agents involve the protection from the remote host, other mobile agents and entities outside the mobile agent system, such as attacks on the transport mechanisms. It is difficult to guard against these type of attacks because of the fact that traditional protection mechanisms were developed to address threats generating from attacks on the execution environment by the application and not the other way around. Proposed work is about the mobile agent, the various security threats that can be posed by malicious host and consequently the solutions. This paper proposed a solution by combining few approaches and distilling the best so that it can provide a better solution.
Keywords: Mobile agents,

1. INTRODUCTION

Mobile agents are a modern and optimistically better network computing pattern compared with the currently used approach to remote computing, based on a client–server model. Mobile agents are self-contained software modules and data that can be launched by a human user and then, they paralleled migrate through the network. They visit remote hosts, perform there their tasks; migrate to the next host, ultimately returning to the management station, where their actions were initiated. To perform complex network tasks addressed in this research, mobile agents must be organized in the form of teams and their actions must be supported by different specific components in the networking environment. Mobile agent paradigm is one such technology where it has numerous application where it can be beneficial, to name a few areas where the mobile agents have potential deployment are database research, distributed system and e commerce. This technology has given new directions to networking. It can produce very good result in limited resources or in deficient environment where bandwidth, memory are significant constraints. But still it is not widely accepted due to its security issues.

1.1 Mobile Agent Model

The mobile agent model generate from two different approaches, namely the distributed artificial intelligence environment and the distributed systems environment. Several different metaphors and architectures exist to describe mobile agent model because of these environments being a recent research area. The aim of this chapter is dual, namely to describe the fundamental nature of a mobile agent as well as a mobile agent system and secondly, to initiate the specific security threats which relates to this model, as this is the basis of our research.

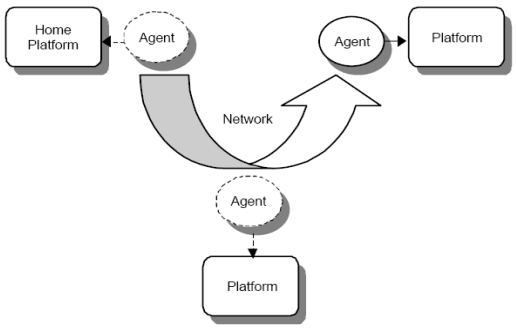

Figure1: Mobile agent System

[1] Research Scholar, Department of Computer Science, NIMS University, Jaipur
[2] Professor, Department of Computer Science, NIMS University, Jaipur

There are two main components of Mobile Agent System [4]: mobile agents and mobile agent platforms as given in figure 1. Mobile agents are goal-directed software and they repeatedly hang up their execution on one platform and migrate to another platform, where they restart execution to complete their tasks. Mobile agent platforms [4] are implementation environments for mobile agents on different computers, together with the guest platforms and home platform. A home platform of a mobile agent is in charge for creating, initializing, dispatching, receiving, and eliminating a mobile agent.

By using communication protocols the interactions in a distributed system are repeatedly achieved and it can reduce the network load. These protocols basically transfer large volumes of data stored at remote hosts over the network to a central processing site in high network traffic. The use of mobile agents is an alternative to using communication protocols. Mobile agents are dispatched to the remote hosts containing the data and then it performs the computations at the remote hosts and return back with the results. Instead of moving data to the computing location, computations are moved to the data storage location so network load is reduced.

In a manufacturing plant where many critical real time systems are controlled through a network which involves significant delays, not satisfactory for critical real time systems. To come out of this problem, mobile agents can be directly dispatched from the central controller in the manufacturing plant to the real time systems. The agents act locally and directly implement the controller's directions and it can overcome network latency. Mobile agents propose a solution to protocols enable components of a distributed system to communicate and co-ordinate their activities. However, protocols evolve over a period of time and new features such as better security may be introduced in the protocol. To upgrade the protocol code at all locations in the distributed system is a weighty task. The mobile agent code can encapsulate the protocol and the mobile agent has to be altered when a protocol is upgraded. Mobile agents operate asynchronously as once a mobile agent is dispatched from the home machine, the home machine is disconnected from the network. The mobile agent executes separately without the interference of the home machine. The home machine can reconnect at a later time and collect the agent. Mobile agents react energetically and separately to the changes in their environment, which makes them robust, and fault tolerant. Mobile agents have the ability to distribute themselves in the network in such a way as to maintain the optimal pattern for solving the particular problem. If a host is being shut down, the warning will be given to all agents executing on that machine and time is also given to dispatch them and then they can continue their operation on another host in the network. Mobile agents can also be used in network management maintenance, fault diagnosis, testing, and for energetically upgrading the capabilities of existing services. Other uses consist of air traffic control, workflow management, information retrieval management and education.

Mobile agent operation of the program execution state and program code. Primarily a mobile agent resides on a computer called the home machine. Then it is dispatched to execute on a remote computer called a mobile agent host. When a mobile agent is dispatched its entire code and the execution state is transferred to the host. For the mobile agent to execute the host it provides a suitable execution environment. The mobile agent uses resources of the host to perform its task. Once its task is completed on the host, the mobile agent migrates to another computer. Since the state information is also transferred to the host, mobile agents can restart the execution of the code from where they left off in the previous host instead of having to restart execution from the starting. This continues until the mobile agent returns to its home machine after completing execution on the last machine in its schedule.

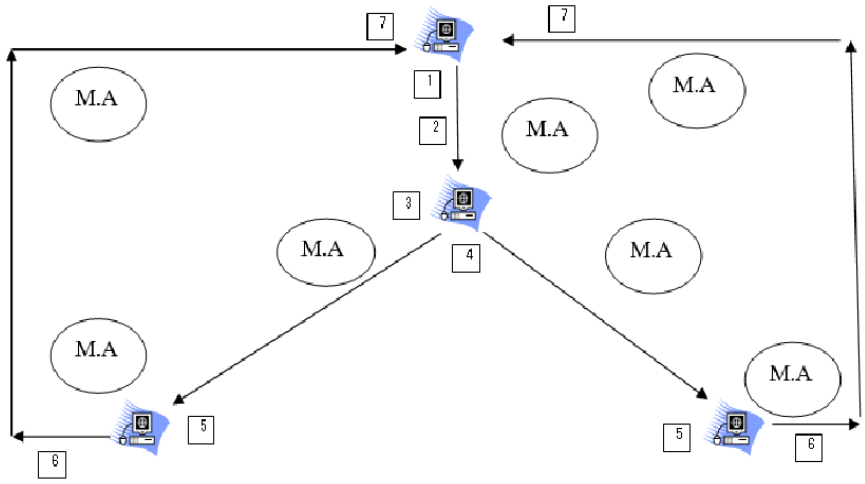

Figure 2: Mobile agent life cycle

1.2 Security Issues in Mobile Agents

Security remains a major problem for the agent paradigm. It is difficult to prevent a malicious agent from stealing or corrupting information on its host and in other agents on the host, or from launching denial of service attacks by over-

consuming resources. Further, a malicious host can steal or corrupt agent information, or even kill the agent. An agent infrastructure must work around these security problems and offer compensating security properties.

The protection of mobile agents against malicious hosts has introduced a new field in the security arena. For the first time it is deemed necessary to protect an application from manipulations by the executor of the application. As can be summarized from previous chapters in the mobile agent paradigm, the agent is sent between hosts in order to achieve its goal. At every host the agent is executed, information is exchanged between the agent and the host and the state of the agent is updated accordingly. This execution at a foreign site introduces specific security challenges in relation to the protection of the agent.

Based on the proposed model, security is applied according to the level of trust allocated to each host visited by the agent. This implies, that the hosts to be visited are known beforehand (and trusted to various degrees), which compromises the requirement of autonomy. Furthermore, the autonomy of an agent is inextricably related to its mobility. Therefore, it is important that integrated security techniques do not compromise its mobility either. These two characteristics of mobile agents (and also mobile agent systems) increase the complexity inherent to the design and maintenance of such a system. Added to the mentioned complexity is the fact that multifaceted systems with many components have a higher possibility of failure or breach; on the other side, simplistic systems can be vulnerable.

2. RELATED WORK

Agents are independent pieces of software capable of acting autonomously in response to input from their environment. Agents can be of differing abilities, but typically possess the required functionality to fulfill their design objectives. To be described as ‘intelligent’, software agents should also have the ability of acting autonomously that is without direct human interaction, be flexible, and in a multi-agent system, be able to communicate with other agents that is to be social. Agents are, to various degrees, aware of their environment, which often also can be affected by the agents’ actions.

A mobile agent is a particular class of agent with the ability during execution to migrate from one host to another where it can resume its execution. It has been suggested that mobile agent technology, amongst other things, can help to reduce network traffic and to overcome network latencies. An agent’s ability to move does however introduce significant security concerns.

The concept of an agent originates from the area of Artificial Intelligence (AI) but has now gained more widespread acceptance in mainstream computer science. The term ‘agent’ has become rather fashionable, and a more mature technology than currently available is often implied. This is in particular true for security in multi-agent systems. Over-simplified assumptions and non-applicable references to security solutions are not uncommon in the literature. Naturally, security is not a driving force for research and development of multi- agent systems, and therefore has not received much attention from the agent community. Nevertheless, in order for agent technology to gain widespread use and provide viable solutions on a wider scale for commercial applications, security issues need to be properly addressed. Autonomous agents and multi-agent systems represent a relatively new way of analyzing, designing, and implementing complex software systems. In this article we are only concerned with the security of the system and its components (leaving design methodologies to others). Several multi-agent systems are available as commercial products and many more have been implemented in various research projects, with varying success. Recent standardization efforts have proven rather successful and are still evolving. Today there is growing interest and research in implementing and rolling out (open) multi-agent systems on a wider scale 1. Mobile VCE is undertaking one such project where the agent paradigm is researched in a mobile telecommunications setting.

3. PROPOSED MODEL

The identification of the challenges and the requirements discussed in last section of a mobile agent security framework brings us closer to establishing a security framework that is appropriate for different mobile agent applications.

According to the criteria of a mobile agent security framework, as well as the analysis and discussions in the previous chapters regarding the countermeasures, frameworks, systems and applications, this paper propose the following six levels of security within the framework:

Basic closed: The basic closed level is a trusted environment in which the mobile agent is deployed. This trusted environment is typically a local area network (such as an Intranet) within a specific organization. The level of trust in this environment is high. The mobile agent system executing on the basic closed level will mainly be used for information conveying and retrieval with no computations taking place on the different hosts.

Extended closed: This security level is a local area network that can possibly be extended by incorporating two or more Intranets. It is basically a trusted network of nodes and the mobile agent deployed at the extended closed security level is used not just for information searching and conveying, but also for computations. The level of trust is high.

Basic Restricted: Applications operating on the basic restricted level will make use of hosts on the Internet, where the hosts are pre-determined by the owner. Applications operating in the basic restricted level are mainly for information retrieval and conveying, but with no computations. The level of trust on this level is low.

Extended Restricted: As in the previous framework level, hosts to be visited in this type of framework are predefined. Additional to the information retrieval and conveying, mobile agents will also have no restrictions on the functions executed at the different hosts, which means that computations are allowed. As before, the level of trust is low.

Basic Open: In the basic open framework level, Internet hosts are included without the restriction of a predefined itinerary. However, at this level, mobile agents are only used for information conveying and retrieval with no computations on the different hosts. The level of trust is nil.
Extended Open: As in the previous framework level, the extended open framework level includes Internet hosts without the restriction of a predefined itinerary. Applications in this environment have no restriction on accessing and computational functions on the different hosts. Since the level of trust is extremely low, it is important that all components of the agent are protected.

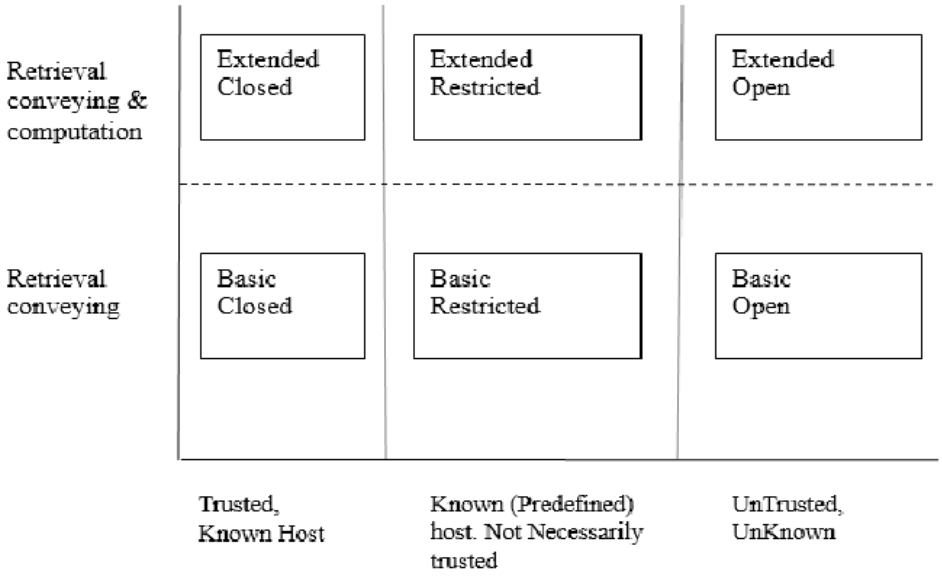

Figure 3: Proposed framework security levels

It is necessary to distinguish between mobile agents that is tasked to convey and / or retrieve information and mobile agents whose ultimate goal include computations on the different hosts. Agents that fall in the latter category will need additional protection in terms of information required throughout their journey as well as the protection of the actual computational results. Figure 3 summarizes the discussion on the different security levels. The x-axis depicts the different types of execution environments, while the application categories are depicted along the y-axis.
The different framework security levels depend on the definition of specific application environments in which mobile agents are likely to be deployed. These application environments range from a highly trusted environment to an untrusted open environment. In the rest of this section, we consider the most appropriate countermeasures to be integrated into a particular environment in order to improve the security without risking performance. The suggested framework has a dynamic nature. Although the framework itself appears static in the number of solutions it seems to offer, the ability to use any countermeasure or combination of countermeasure for different security demands, lends a dynamic character to the proposed framework. This implies that although there may be various appropriate countermeasures available for a specific security level, only a selected few of these may be suitable for a particular application. This in turn depends on what degree of security the application is expecting from the framework.

4. EVALUATION

When Before considering the outcomes of our research effort, the objective and relevance of this study are revisited for a moment. To determine whether the objective of this study is scientifically sound, we asked ourselves why it was necessary to design a security framework, rather than, for example, design new countermeasures for the malicious host problem. The necessity for a framework can best be described by using an analogy to that of the processes involved in the building of a factory (industrial unit). The development of an industrial unit involves steps such as the design, construction of the structure, building or assembling of walls, interior decoration, et cetera. The inclusion of the design plan and building of the structure processes is essential to the ultimate assembly of the factory. A structure is needed to establish the outlines and requirements of the design, as well as to provide specifications of how and where the building blocks have to be placed. Without such a structure (in our case the framework), the building blocks (in our case the countermeasures) will be unorganized modules lying in disarray.
The importance of a mobile agent security framework can be seen in the large number of proposals in this area. The process of proposing a mobile agent security framework necessitates the establishment of criteria and subsequently a set of requirements to which the framework needs to abide to. Yet, literature reveals the inexistence of such a set of requirements

and as a result, also a lack of a comprehensive model that is based on such a set of requirements. In fact, our literature review described the details of many different countermeasures for malicious host attacks, without much interaction and integration possibilities. Furthermore, literature pointed out that different degrees of protection are required for the malicious host problem, but lack due to the non-availability of requirements to aid mobile agent developers to design of secure systems. Our proposal thus answers to a research problem that has been expressed by more than one researcher in the field of mobile agent technology.

In this proposed work, the search for an existing security framework that adhere to our set of requirements, proved to be futile. However, as illustrated in Chapters 4 and 6, a number of proposals for an integrated security framework do indeed exist, but an analysis indicated that they don't provide adequate protection for all components of the mobile agent. This corresponds with about the requirement for an integrated security framework that provides protection for the mobile agent against malicious hosts. In the next three subsections, we briefly point out why our proposed framework overcomes deficiencies of current solutions by considering problems in current systems, problems in countermeasures and security level issues.

5. CONCLUSION

In this work, we have proposed a proficient analysis of mobile agent method based on the network environment. While the MA paradigm has been for the last decade and a half, the lack of killer application has hindered its popularity and acceptance. One of the major reasons for the slow progress in the acceptance of the MA paradigm has been the lack of a secure computing infrastructure. The lack of a reliable security mechanism and the dynamic nature of the MA functionality cause it to be regarded as a malicious entity. MAs possess the destructive capabilities of viruses and while they are developed for constructive reasons, they can be easily subverted to assume a malicious form. While encryption has been widely regarded as one of the potential choices for developing tamper resistant security techniques for MAs, it puts pressure on the cost-effectiveness of the MA operation. While encrypting the code of MA guarantees to some extent, its imperviousness to code tampering attacks, it can also lead the host MoAS to regard the MA as a malicious entity.

6. REFERENCES

[1] Ng, Choon Boon, Yong Haur Tay, and Bok-Min Goi. "Recognizing human gender in computer vision: a survey." Pacific Rim International Conference on Artificial Intelligence. Springer Berlin Heidelberg, 2012.

[2] R.Jeganlal , V.Gopi and S.Rajeswari," Robust Automatic Face, Gender and Age Recognition Using ABIFGAR Algorithm", International Journal of Emerging Trends in Electrical and Electronics IJETEE – ISSN: 2320-9569.

[3] Thai Hoang Le, Len Bui, "Face recognition based on SVM and 2DPCA", International Journal of Signal Processing, Image Processing and Pattern recognition Vol. 4, No. 3, September, 2011.

[4] A R . Ardakany, M ember, IACSIT and A. M. Jou la," Gender Recognition Based on Edge Histogram", International Journal of Computer Theory and Engineering Vol. 4, No. 2, April 2012.

[5] Chaichulee, Sitthichok, et al. "Multi-task Convolutional Neural Network for Patient Detection and Skin Segmentation in Continuous Non-contact Vital Sign Monitoring." 2017.

[6] R.Jeganlal, V.Gopi and S.Rajeswari," Robust Automatic Face, Gender and Age Recognition Using ABIFGAR Algorithm", International Journal of Emerging Trends in Electrical and Electronics (IJETEE – ISSN: 2320-9569).

[7] Yujie Dong, Damon L.Woodard," IEEE-Eyebrow Shape-Based Features for biometric recognition and gender classification", 978-1-4577-1359, 2011.

[8] P. Sasikala ,Miss.N. Niirosha 2 et.al,"identification of gender and face recognition using recognition using adaboost and SVM ",Volume 3 Issue 11 November ,2014 page No. 9305-9312.

[9] Ding, Changxing, et al. "Multi-directional multi-level dual-cross patterns for robust face recognition." IEEE transactions on pattern analysis and machine intelligence 38.3: 518-531, 2016.

[10] Liao, Pin, et al. "Nesting Differential Evolution to Optimize the Parameters of Support Vector Machine for Gender Classification of Facial Images." the 3rd International Conference on Technological Advances in Electrical, Electronics and Computer Engineering (TAEECE) 2015.

[11] Swathi Kalam et. al, "Gender Classification using Geometric Facial Features", International Journal of Computer Applications (0975 – 8887)Volume 85 – No 7, January 2014.

[12] Arun Kumar Nagdeve et al, "Automated Facial Fetures points extraction ",International Journal of Computer and Electronics Research [Volume 1, Issue 3, October 2012.

[13] Khan, Sajid Ali, et al. "A comparative analysis of gender classification techniques." Middle-East Journal of Scientific Research 20.1 , PP-1-13, 2014.

[14] Amr EI Manhraby,et.al."Detect and analyse face parts information using viola jone and geometric approces", IJCA volume 101-No 3 september 2014.

[15] Amitabh Mukherjee of CSE,IIT Kanpur, Facial Image database taken from : http://vis-www.cs.umass.edu/~vidit/AI/dbase.html