

# A Detailed Anatomization of Mobile Agents

Payal Beniwal<sup>1</sup>, Dr. Mukesh Kumar<sup>2</sup>

<sup>1</sup>M.Tech Scholar, Computer Science Department, TIT&S, Bhiwani

<sup>2</sup>Assistant Professor & HOD, Computer Science Department, TIT&S, Bhiwani

**Abstract:** *Nowadays mobile agents have become more popular and are an impressive paradigm for distributed computing where security is of supreme importance. Mobile Agents migrate through one platform to another platform autonomously to execute some computations or collect important matter as according to human user need or an application. But this mechanism constitutes some kind of threats also. This paper describes an overhead view of the mobile agents and its chief security problems related to the mobile agent system.*

**Keywords:** Mobile agents, Security, Mobility

## 1. Introduction

Computers have evolved from huge massive devices with very less storage to client & server mechanism that permits varied and complicated forms of distributed computations. With the growth of computing technology and distributed applications, the issue of performance and network overhead create problems which cannot be efficiently solved by client server paradigm. To solve the problems of performance and maintenance cost of network, the idea of mobile agents came. [1], [2], [3]

The mobile agents can be recognised as an intelligent software or process agent which has the properties of autonomous, intelligence, self-determination, reactive, communicative, mobility and adaptability. It can move from one platform to another platform or we can say that in a heterogeneous network or environment and uses the resources of that platform to perform its specified task. The agents can give an appropriate and systematic environment for executing the distributed systems and smart frameworks for many of the reasons, including up-gradation to the bandwidth of client-server applications, latency and reduction of vulnerable network. [3] and [4]. Mainly, the mobile agents accomplish on a platform/machine that allows the access of the resources/services that it needs to achieve its specific task. If the platform/machine does not hold the required resource/services, or if the mobile agents are in requirement of a different services/resources on another platform, the residing content/data of the mobile agent gets reserved in the already defined pattern, then transmits to a platform/machine residing the required resource/service starts, and the mobile agent restarts implementation at the another machine. The mobile agents possessing multiple functions transmit in different zones implementing a task in the target platform/host.

## 2. Literature Survey

Suri, Knoll, & Bradshaw in [3] proposed a mechanism for security of mobile agents which were pathway-based. The pathway-based security has given a system that increased the security of the NOMADS agent system in the multi-level systems. NOMADS supported safe agent execution and strong mobility [16]. A light protocol had been developed

for checking mobile agent's track records that was based on combining the IP addresses. After receiving host environment a trust level has been evaluated for the mobile agents, which was afterwards has to pick and implement a rule of security to the upcoming mobile agent. To give more trust-worthy track data, a 'Faithful Third Party' was kept non-forcefully. Though, just three levels of trusts have been used by this execution: low, high and medium. Hence, the system didn't want enough for support of an outstanding composition of faith amount. So, a computation should be found through transitive faith connections that will maintain faith content to be computed.

Tsekouras, Gavalas & Anagnostopoulos in [11] presented a technology of mobile agents for the distributed and networking systems management for solving the problems of scalability. The authors putted schema of complete research prototype of MAP that efficiently showed up all the matters for instance security issues, fault tolerance. MAP was being optimized for network and systems management applications. It has been implemented in Java. They brought the implementation aspects and design decisions of a complete prototype of MAP research that adequately presented all the aforesaid matters. In contrast to existing issues, that MAP counterbalanced the many novel blueprint characteristics, mentioned by their options of design and showed upon their implementation of researches: (a) a mechanism loading by a class at runtime that permits the alteration of mobile agent based NSM task, (b) a distribution scheme based on light-weight coding, (c) the tool which stands by customizing the service-oriented mobile agents which is user-friendly, (d) a component that constructs close to the optimal network-dependent itineraries of mobile agent. Additionally, other important NSM-related requirement has been satisfied, such as security (authorization, encryption and authentication), lightweight footprint on systems resources, modularity, platform independence, incorporation of agent migration optimization techniques, recovery from basic software faults etc. In realistic management application scenarios, MAP's performance has been evaluated.

Picco in [16] checked out the related fields of research by giving proofs of the benefits of mobile/software agents, then showed the technologies and architectures foundations for agents, and described many of the problems that still

affecting the approval of this agent system. The conception of standardized distributed systems framework has been taken by the author and contrasts the settings of the systems in accordance of mobile and logicity. The motive of the task was to establish the research field related to mobile agents to the reader. The paper described the theoretical basics that has their rules and regulations in logicity and mobility at huge, described the statistic of art in the technology of agent. This paper has also discussed most fundamental reasons for usage of mobile agents, clues in when or why the mobile agents are advantageous over other results, examined core system of architecture for mobile movement of the coding, inclusive of the agents, finally showed up results on the current position and the research area future scope. That work has gone through the two case studies, one is networking management of mobile agents and second, the agents for database access were being discussed for the research in this area of field.

Moussa & Agha in [21] showed up the designing of "Bosthan", ie. a simulation tool based on multi-agent system that controlled the consumption of resources in smart spaces of multiple-residents. The Bosthan was ranked on the head of platform of ActorNet mobile agent to manage various topologies of smart space with varying numbers of residents. It depicted planning for solving the issues between agents, and for securing inhabitant's intractability and anonymity in the smart spacing. The architecture which is presented is of simulator which is agent-based for bosthan consisting of ten modules like bosthan simulation engines, sensors, generator for patterns in motion, layout creator, floors planner, location predictor, events generator for matter, recognise hider, actor-net generator, conflict solver, run analyser.

Juneja, Sharma and Singh in [19] , the working of community of agents that works on the main idea of delegation and cooperation of tasks have been discussed, which in turn must be get avoided also kept away from any infectious use. In according to restrict this infectious use, a tool for making secure and proficient conversation among these associating agents is faith. The writers gave a security engine based on elliptical curve cryptography which extended a novel schema naming CNTEP that victoriously rooted the faith among the mobile agents. Securing or encrypting the conversation or transmitted messages of mobile agents is one of the best results/requirements for maintaining safety. Although conventional encrypting algorithms such as DSA, DH [18] and RSA [15], utilize basic sizes of very large sizes resulting in big space and time complexities. In comparison with this ECC (Elliptical Curve Cryptography) technique [20, 22] is the public key cryptographic system. It has been utilizing many tiny key sizes that are capable to give a challenging security measure as that of other remarkable encrypting algorithms. The most special characteristic of ECC (Elliptical Curve Cryptography) is its comparatively short operand length as in contrast to RSA and also it is based on the discrete log in the finite field.

Rizvi, Sultana, Islam & Sun in [23] described an answer for making agents secure in an ad hoc networking. The Cryptography using threshold has been used by the author in their module, as because it gave answer to the problem of

trusted third party in PKI and central certificate authority (CA), by spreading faith in various networking nodes. Some of the safety services have been provided by this model like integrity, confidentiality, and authentication. But the agent is not secured from attacks. Although, the design/model gives a secured way not only for agents, but also for the agent's platform and the agent's server, but still this is quite tough to provide full safety in an ad hoc networking, to find and avoid intrusions and vulnerabilities. In accordance with threshold cryptography this has been supposed that the value 'th' be a value of threshold for the network ad hoc. Resulting that the system can face up to the compromised servers. Although in this, the schema of cryptography has not been used to create the private key shares of 'Key Management Services'. And also the process of combining the partial signatures or the process to generate the private key of Key Management Services by th+1 servers have not been told by them. In addition, this has not been mentioned that how authorization will be given and control access service will be provided. To solve these issues future research is needed.

### **3. Characteristics of Mobile Agents**

Many explanations about the mobile agents have been given. In basics most are having a collection of significant features that each mobile agent should perform. Like for example, "Jennings and Woodridge" the weak agents [2] should be independent to move, responsive and communicative. Also according to Franklin & Graesser [5] lists autonomous, responsive, communicative, robust, movable, manageable, motive-oriented, constant and with composed of feelings or emotions.

#### **3.1 Independent/Autonomous**

They must have the ability to act without the external interferences and also the agent should be capable to execute without the human's interaction need.

#### **3.2 Communicative/Social**

Mobile Agents should be interactive in communicating with the environment and the rest of the agents. The key protocol for agent's conversation is KQML (Knowledge Query and Manipulation Language). [17]

#### **3.3 Adaptive**

Mobile Agents should be having the capability to adjust according to the environment around them. They should adapt the changes occurred in the environment and change accordingly.

#### **3.4 Mobility**

It is the core property in a mobile agent conception. The agent has the ability to move itself from one network or machine to another within the same environment or in a different environment while maintaining persistence.

### 3.5 Responsive/ Reactive

A mobile agent should have the capability to grasp the changes in the framework around them and also should react wisely if they encounter some changes in the environment.

### 3.6 Intelligence

Agents should have the capability of reasoning, learning and adaptive over time. They behave intelligently while performing their tasks.

### 3.7 Honesty

Agents should be able to pass on the original and exact information. Mobile agents should be honest that means perform all their tasks or processes as per the human or user's need.

### 3.8 Emotion

Agents should be able to convey/show human-being like moods/emotions. Such kind of mobile agents might also have some humanoid appearance.

### 3.9 Proactive

These kinds of agents are not just reactive to the environment but can also perform some actions to modulate that framework in accordance to their choices.

### 3.10 Motive-oriented/ Intentions

The agents under this category have a specific set of actions to achieve a goal or objectives. They should not deviate from their task until they achieve their aim or goal.

### 3.11 Continuous/Persistence

Persistence Agents remains stabilized over the time. This is an internal by-default state that the agents possess. These agent characteristics lead to many favourable features. Some natures like social entities and independency can lead to respond and modify their environments provide a powerful base for the creation of durable, mouldable, trust-worthy, scalable and boundless/extensible systems.

## 4. Security Warnings/Threats

This mobile agent system, which works on coding, state and mobility of data, brings much newly security warnings/threats that are quite unlike from traditional system's security issues.

### 4.1 Agents-to-Platform

The agents-to-platform type depicts the collection of threats in which mobile agents harm the safety vulnerabilities of an agent platform and affect the platform. This kind includes the following types of threats. [7], [9]

#### 4.1.1 Unauthorized access

This type of threat tells that the mobile agent must not have the permission to access the data of the platform representing several users or organizations. Also it does not have the access to secured data that may be saved in cache or storages.

#### 4.1.2 Masquerading

The masquerading agent may bluff as another unauthorized agent and hence can regulate the responsibility of the actions for which the malicious mobile agent does not need for being blamed. A malicious agent may harm the faith of the authenticated agents that have gained in the band of agents and its reputation regarding it.

#### 4.1.3 Denial of service

A mobile agent can cast the attack naming denial of service by the consumption of computing resources of the agent platform largely. In this, the attack can be set purposely by executing the activity of attack list to use system services, or un-intentionally by the bugs.

### 4.2 Agent-to-Agent

The type of threat depicts the set in which the mobile agent harms the other agents or exploits the other agents in the same or other environments. This set includes following threats. [7], [9]

#### 4.2.1 Masquerade

A mobile agent may try to hide its real motive just to mislead the mobile agent with which it is doing conversation. They act as a safe agent with which other agents can communicate very easily. This is a very common technique used by the malicious agent in agent-to-agent threat.

#### 4.2.2 Repudiation

The Repudiation happens when a mobile agent, taking part in transmission or passing on the data and then later on it denies that the communication has ever been held. The reason for repudiation can be purposely or accidental. Whatsoever be the reason is, repudiation can result in complex matter that cannot be solved easily until the required corrective measures are taken.

#### 4.2.3 Unauthorized Access

An agent can intentionally interrupt the other agent by imposing its general procedures (example- attempting buffer overflows, etc.), also by interfering and modifying the data or code of agent.

### 4.3 Platform-to-Agent

This type shows the collection of threats in which malicious platform affect the safety of mobile agents and it includes following parts. [7], [9]

#### 4.3.1 Masquerade

The malicious platform can attack the platform and the incoming agent as well whose identity it is supposed to be. The agent that bluffs as the other agent can damage other agents just only by exchanged messages and the resultant

activities takes place, but an infected platform that bluffs as a valid host/platform may harm more to the fair agent than a single mobile agent can affect to itself. [10], [18]

#### 4.3.2 Eavesdropping

In eavesdropping threat, the platforms can not only track the conversations, but can also track each and every task thread performed by the mobile agent.

#### 4.3.3 Alteration

When a mobile agent's information is modified by a malicious platform that's what we call alteration. This modification or alteration may result in harmful execution of the mobile agents on other platforms.

### 5. Conclusions

The mobile agent paradigm is a very promising and effective distributive system that provides security and has already introduced its presence in many fields inclusive of e-commerce, personal information management, artificial intelligence, interface design, distributed processing etc. This impressive mobile agent system has given some very serious safety issues and highlighted some existing security issues. In this paper we have discussed about the basics of mobile agents, what are they, the types of threats that have been found in this concept and the basic problems arising in the security of mobile agents. Also we have discussed some of the delicate areas that need more attention to be paid for increase of growth in optimistic direction.

### References

- [1] H.S. Nwana, "Software Agents: An Overview", Knowledge Engineering Review, 11(3):1- 40, 1996.
- [2] M. Woodridge and N. Jennings, "Intelligent Agents: Theory and Practice", The Knowledge Engineering Review, 10(2):114-152, June 1995.
- [3] G. Knoll, N. Suri, and J.M. Bradshaw, "Path-based Security for Mobile Agents", Electronic Notes in Theoretical Computer Science, Vol. 58, No. 2 , pp. 16, (2002).
- [4] D. Gavalas, G.E. Tsekouras, C. Anagnostopoulos, "A mobile agent platform for distributed network and systems management", In Journal of Systems and Software 82 (2), 355-371, 2009.
- [5] S. Franklin, A. Graesser, "Is it an Agent, or just a Program?: A Taxonomy for Autonomous Agents", University of Memphis, Proceedings of the Third International Workshop on Agent Theories, Architectures, and Languages, Springer-Verlag, 1996.
- [6] N. Borselius, "Mobile agent security", Electronics & Communication Engineering Journal, IEEE London 14(5), 211-218(October 2002).
- [7] W.A. Jansen, "Countermeasures for Mobile Agent Security", National Institute of Standards and Technology, Gaithersburg, MD 20899, USA, wjansen@nist.gov.
- [8] C. Xiaorong, L. Su, L. Mingxuan, "Research of Network Security Situational Assessment Quantization Based on Mobile Agent", Volume 25, 2012, Pages 1701-1707, International Conference on Solid State Devices and Materials Science, April 1-2, 2012, Macao.
- [9] W. Jansen and T. Karygiannis, "Mobile Agent Security", Nist Special Publication 800-19-, 2000. National Institute of Standards and Technology.
- [10] D.M. Chess, "Security issues in mobile code systems. In: mobile agents and security", Editor Vigna, vol. LNCS1419. Springer-Verlag 1998.
- [11] N. Jennings and M. Wooldridge, "Software Agents", IEE Review, January 1996, pp. 17-20.
- [12] A. Ojesanmi and A. Crowther, "Security Issues in Mobile Agents", International Journal of Agent Technologies and Systems, 2(4), pp.39-55, October-December 2010, University, Nigeria.
- [13] D. C. Smith, A. Cypher and J. Spohrer (1994) "Programming Agents without a programming language" Communications of the ACM 37(7) pp 55-67.
- [14] P. C. Janca (1995) "Pragmatic Application of Information Agents: BIS Strategic Decisions.
- [15] R. Shanmugalakshmi and M. Prabu, "Research Issues on Elliptic Curve Cryptography and its applications", In International Journal of Computer Science and Network Security, Vol. 9, No.6, pp 19- 22, June 2009.
- [16] G.P. Picco, "Mobile agents: an introduction", Microprocessors and Microsystems 25(2001) pp. 65-74, Dipartimento di Elettronica e Informazione, Politecnico di Milano, Milan, Italy.
- [17] T. Finin, Y. Labrou & J. Mayfield, "KQML as an Agent Communication Language", J. Bradshaw (Eds), MIT Press, 291-316, 1997.
- [18] K. Lauter, "The Advantages of Elliptic Curve Cryptography for Wireless Security", In IEEE Wireless Communications, pp. 62-67. February 2004.
- [19] A. Singh, D. Juneja, and A.K. Sharma, "Elliptical Curve Cryptography Based Security Engine for Multiagent Systems Operating in Semantic Cyberspace", In International Journal of Research and Review in Computer Science (IJRRCS), Vol. 2, No. 2, April 2011.
- [20] N. Koblitiz, "Elliptic Curve Cryptosystems", Mathematics of Computation, Vol. 48, pp. 203-209, 1987.
- [21] S. M.. Moussa, G.A. Agha, "Integrating Encrypted Mobile Agents with Smart Spaces in a Multi-agent Simulator for Resource Management", Journal of Software, Vol 5, No 6 (2010), 630-636, Jun 2010.
- [22] V.S. Miller, "Use of Elliptic Curves in Cryptography", Advances in Cryptology- CRYPTO'85, NCS, vol. 218, Springer-Verlag, pp. 417- 426, 1986.
- [23] S.M.S.I. Rizvi, Z. Sultana, B. Sun, and Md. W. Islam, "Security of Mobile Agent in Ad hoc Network using Threshold Cryptography", World Academy of Science, Engineering and Technology 70- 2010.
- [24] V. Roth & M. Jalali-Sohi, " Access Control and Key Management for Mobile Agents", Fraunhofer Institute for Computer Graphics, Rundeturmstr. 6, 64283 Darmstadt, Germany, 8 November, 2001.
- [25] P. Dadhich, Dr. K. Dutta, and Prof.(Dr.) M.C. Govil, "Security Issues in Mobile Agents", International Journal of Computer Applications(0975-8887), Volume 11-No.4, December 2010.