Mobile Agent Security based on Code Obfuscation and Locator Mechanism

Veershetty Dagade
JCE, Belgaum
Jain college of engineering,
Belgaum, Karnataka, India

Chinmay Kulkarni
JCE, Belgaum
Jain college of engineering,
Belgaum, Karnataka, India

S R Dhotre
GIT, Belgaum
Gogte Institute of Technology,
Belgaum, Karnataka, India

ABSTRACT
Mobile agent is a software program comprising of decision making code and data that have the potential to migrate from one node to another node in a network. A mobile agent works on behalf of the owner who created it. Mobile agent operates in a distributed environment in which agents with specific functionalities roam in the network to execute a task in the target hosts. Mobile agent systems are more efficient compared to client server architecture, because they help in reducing network traffic to a larger extent. Mobile agents being vulnerable to various threats and attacks on the network are a major concern in this system. In a non trusted environment, care should be taken to protect the mobile agent from getting tampered. Existing work on mobile agent systems with different mechanisms doesn't provide complete security. In this paper a trust model is proposed with code obfuscation and frequent monitoring of mobile agents using locator mechanism along with data encryption which helps in protecting the data and code which agent carries, thus providing an additional layer of security.

Keywords
Mobile Agent, Agent Security, Cryptography, Locator Mechanism, Code Obfuscation.

1. INTRODUCTION
An agent is a software program that assists people and acts on behalf. They function by allowing people to delegate work to them. Agents are self-governing pieces of software capable of acting autonomously in response to input from their environment. To be described as 'intelligent', software agents should also have the ability of acting autonomously that is without direct human interaction, be flexible and adaptive, and in a distributed system, be able to communicate with other agents. 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 others, can help to reduce network traffic and to overcome network latencies. An agent's ability to move does however introduce significant security concerns.

Security attack refers to any action that compromises the security of information owned by an organization. Possible security attacks are **Passive** Attacks that include Release of message contents and Traffic analysis where as **Active** attacks include Masquerade, Replay, Modification of messages, Denial of service, etc. Strong policies must be enforced to provide security, here security are of two types one that corresponds to host security and another that corresponds to agent security. In order for agent technology to gain widespread use and provide viable solutions on a wider scale for commercial applications, security issues in particular agent security need to be properly addressed

2. SECURITY ISSUES IN AGENT

2.1. Malicious Agent
It is an intruders program or software that functions with a purpose to attack the itinerary host or another genuine agent. It can pose a severe risk to the genuine agents and the hosts serving a platform to the mobile agent. Hence care should be taken about the hosts on which malicious agents are executing because they are vulnerable to many more security issues. Some of the malicious agent programs can be interpreted as virus, worms or spying agents.

2.2. Malicious Host
When an agent moves from one host to another host in the network to perform its task, there can be some hosts who try to hinder the integrity, functionality and confidentiality of the agent in order to benefit themselves in some way. For example they can change the agent data and code with intent to do some malicious task on its behalf and as agent moves to other hosts it harm the reputation of the agent owner or to harm the other hosts in some way. Also a malicious host may try to gain unauthorized access of information or data that belongs to an agent thus confidentiality is under breach. The task of protecting a mobile agent from a malicious host rather than protecting a host from a malicious mobile agent is very difficult.

3. RELATED WORK
Early work in mobile agent security centered on policy management and malicious code protection based on credentials [24]. Distributed policy tools for mobile agents are developed in [25]. Zwierko and Kotulski [23] categorized the threats in agent system into four groups: an agent attacking an agent platform, an agent platform attacking agent, an agent attacking another agent on the agent platform and other attacks. The use of mobile agent raises a number of security issues. The communication medium is not secured and due to which variety of attacks can be conceived. For example, eavesdropping on network traffic and agents activities observation by the unauthorized users may occur. In a worst case scenario, active intruder may modify the code, data or state of an agent in the traffic [20]. Shilpa Budhkar, Anshita Mishra, Ferdous A. Barbhuiya, Sukumar Nandi [27] in their paper "Security in Mobile Agent Systems with Locator Mechanism" have highlighted a hierarchical way of encrypting agents and provided a good locator mechanism to deal with major security threats. Collberg, Thomporson and Low [16] have shown some classification of obfuscation technique. Parul Ahuja, Vivek Sharma [33] in their paper "A Review on Mobile Agent Security" have highlighted various security issues in mobile agents. Dave Singel´ee, Bart Preneel [32] in their article "Secure e-commerce using mobile agents on untrusted hosts" have highlighted how mobile agents can

gather information, protect the gathered information against unauthorized hosts, and how they can digitally sign transactions in an untrusted environment. Hyungjick Lee, Jim Alves-Foss and Scott Harrison [34] in their paper "The Use of Encrypted Functions for Mobile Agent Security" have emphasized on various encryption techniques and proved that their approach provides a practical idea for implementing mobile cryptography by suggesting a hybrid method that mixes a function composition technique and a homomorphic encryption scheme that they have found well secured. Elhum (Elhum et al., 2008) [24] has presented a new model for Aglet security based on existing Aglets architecture. M. Vigilson Prem S. Swamynathan paper [30] "Securing Mobile Agent and its Platform from Passive Attack of Malicious Mobile Agents" This paper provides an environment that protects the legitimate mobile agent from the malicious mobile agent that performs passive attacks like eavesdropping.

Several protocols have been proposed for the protection of mobile agent, its execution and its itinerary. Ibharalu et al. proposed a dynamic protection architecture for mobile agent system [10], using travel diary protection scheme and platform registry. The scheme protects and allows mobile agents to roam freely in open networks environment without being compromised by an unauthorized malicious hosts. Though the data is protected from hosts, the code is vulnerable to attack by other malicious agents residing in the host. The key management scheme [11] provides a way to authenticate code and secure data by obtaining necessary cryptographic keys through web services which act as a trusted third party. This mechanism does not support dynamic itinerary in which hosts are discovered at run time. Nisha et a!. presented a security solution [8] that protects both the mobile agent itself and the host resources that encrypt the data before passing it to mobile agent and decrypt it on the visited host sides. The method of "computing with encryption function" has been used. It solves the problem of malicious host that can harm mobile agent or the information it contains. A novel secure-image mechanism [9] is presented that protects agents against unauthorized non genuine malicious hosts. The aim is to protect mobile agent by using the symmetric encryption and hash function in cryptography science to face the eavesdropping and alteration attacks. It is must here to have knowledge of unauthorized host in advance and for every visit to non trust host, additional overhead exists in requesting the secure image generator. The problem of keeping sensitive data and algorithms contained in a mobile agent from discovery and exploitation by a malicious host is overcome by providing distributed security protocol for multi agent environments [10]. The security is guaranteed for one to one communication between client and server through multi agents and so not suitable for free-roaming mobile agent. Further, the code and data is secured and not the itinerary.

4. PROPOSED SYSTEM

4.1 System Design

The proposed system comprises of zones comprising of hosts that are responsible for communication and agent migration, we also have a zone controller who coordinates and is responsible for the overall activities in the zone, apart from the zone controller we have an agent tracker or agent locator that helps locating the location of the agent, in our proposed system with the agent tracking privilege we are able to locate the agent on which host it is executing. In a non trusted network there are many security issues to be addressed. In this proposed model the agent is allowed to migrate from one node to another node to reach a particular destination, during the hops the agent is appended with the message digest required for authentication process next the data is encrypted using asymmetric encryption if the agent is migrated from one host to another host in the same zone or from one host in one zone to another host in another zone later to provide an additional layer of security the agent itself migrating is in obfuscated format. Data encryption with message digest helps agent to thrive safely in the network. As the agent moves to a new host it first authenticates itself hence during the process of authentication the message digest for the data that the agent is carrying is computed and comparison is made to check whether the data is not tampered.

4.2 Host to Zone Controller Communication

The entire process of the agent migrating from host to zone controller can be seen in Figure1. In Figure 1 we can observe how an agent carries data from one host to the zone controller in that the host calculates the message digest using SHA-1 in first step next it appends the message digest with the message to be sent later encrypts the message digest + message with the private key shared among the host and the zone controller, next the encrypted data is given to the agent. Now the agent receives a certificate form DSS for authentication purpose later itself gets obfuscated to provide an additional layer of security. After reaching the zone controller the obfuscated code is interpreted in a usual manner as code obfuscation is not encryption rather it is a way of replacing some of the identifiers by some meaningless names, because reverse engineering of your java applications by unfair competition or malicious hackers may result in highly disagreeable exposure of your algorithms and ideas, proprietary data formats, licensing and security mechanisms, and, most importantly, your customer's data. More about obfuscation is discussed in next section. Upon reception of the mobile agent the encrypted data that it is carrying is decrypted to get the message and the message digest appended to the message. Now the received message is applied to SHA-1 again at the receiving end and comparison is done on the newly computed message digest and the sent message digest, if comparison function returns false then a signal is sent to the agent locator specifying that the data is no more genuine and is useless.

4.3 Host to Host Communication

The entire process of the agent migrating from host to another host can be seen in Figure2. In this figure we can observe that first the host computes the message digest(using SHA-1) and then concatenates the message and message digest later encrypts the concatenated data and gives it to the agent, next the agent upon receiving DSS certificate obfuscates itself and migrates to the destined host. The only difference here is instead of using private key encryption we are using public key encryption where the message digest is encrypted using the senders private key ($\mathbf{K_{prs}}$) and at the receiving end decrypted using senders public key ($\mathbf{K_{pus}}$).

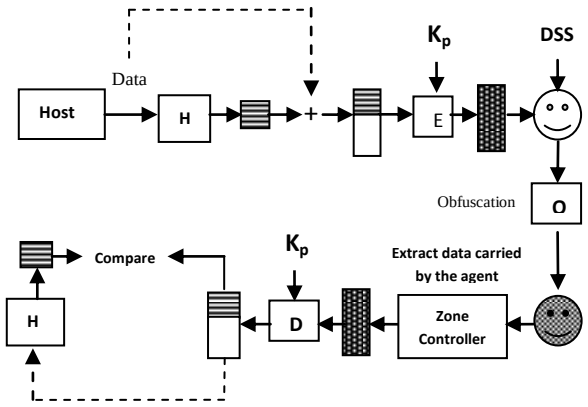

Fig 1: Agent carrying data from one host to zone controller process

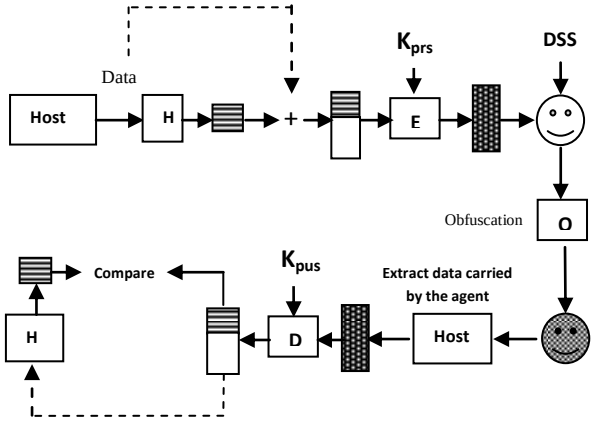

Fig 2: Agent carrying data from one host to another host process

As mentioned in our proposed model we rely on the locator mechanism i.e we maintain a dedicated server that is responsible for locating the agents which helps in keeping track of the agent and its status. If during authentication it is found that the data that agent carrying is not tampered then a positive signal is sent to the server stating the agent's safe status else a negative signal is sent to the server. After receiving a positive signal the server directs the agent to move to the next hop, else the server with the centralized control will dispose or kill the agent and sends another agent to finish the objective. As the server knows at which host the agent was tampered hence the newly created agent directly moves to that host and move further instead of beginning from the owner host who had created the first agent for performing the task. The entire process of agent getting created and registration with the zone controller and agent being tracked by the locator mechanism can be depicted through the Figure 3. As you can see from the figure a node responsible for agent creation first registers the agent to the zone controller and upon the direction from the zone controller the agent locator starts keeping track about the ip addresses that the agent is going to visit in order to reach a particular destination.

Steps below specify the entire process depicted in Fig 3

1. Agent Creation in zone A
2. Agent Registration and getting keys from the zone controller for encryption
3. Agent encrypts the data and migrates to the next node [Details of encryption for host to zone controller and host to host is specified in section 3.2 and section 3.3]
4. If the agent finds that the next hop is next zone then it first with the direction from the current zone controller gets a DSS certificate for authentication purpose, the zone controller appends information about the home agent locator and to which zone the agent belongs to the migrating agent
5. Next the agent migrates to the next zone to register itself to the next zone controller in the mean while the agent always keeps sending its status information to the home agent locator
6. Now the agent being in zone B authenticates itself and registers itself with the zone controller and the zone controller directs the agent locator in this zone to keep track of the agent
7. Next is wherever the agent migrates in the remote zone, the remote zone controller in coordination with the remote agent locator will always keep track of the agent and periodically send the status signal to the home agent locator

5. OBFUSCATION

Protection of the agent itself on remote host: Obfuscation is an approach in which code is transformed or messed up in such a way, it becomes hard to understand, but performs the same function as the original program. Collberg, Thomporson and Low [16] have shown some classification of obfuscation technique. Here according to Collberg, Thomporson and Low the obfuscation can fall into few categories, these are:

5.1. Layout Transformation

It is a transformation with low potency as there is very little semantic formatting is done. So no great confusion is created. Scrambling of identifiers name is a way to do free transformation of this type.

5.2. Control Transformation

Control transformation randomizes the order in which computation are supposed to carry out. It may insert new code or dead code or make algorithmic changes to the source application.

In e-commerce, a mobile agent usually visits several hosts gathering information about the goods required for purchase. After collecting offers from these seller hosts, the agent is meant to take a decision as to which seller to choose the agent usually is equipped with a decision making algorithm. After which the agent can use such data as credit card details, e-coins to purchase the goods. If the decision making code is executed on a seller host, the host gets complete access to the code and can completely understand the decision making process of the agent and thus change its offer in order to influence the agents decision such that it is made to choose the malicious seller host for the transaction. Thus, it is important that code confidentiality prevents code inspection. The simplest mechanism to provide agent code confidentiality would be to allow mobile agent to migrate to known and trusted hosts only. Thus, agents are sent in encrypted form from host to host and are executed only after authentication of the hosts. owever, mobile cryptography is expensive. Basically, this approach is based on homomorphic encryption

scheme and it is very hard to find those schemes for building mobile encryption function. Furthermore those functions can support only restricted execution. Code obfuscation, is a much more practical approach to providing code confidentiality. Code obfuscation, tries to make the agent's program illegible and data hidden; thus difficult to understand and manipulate.

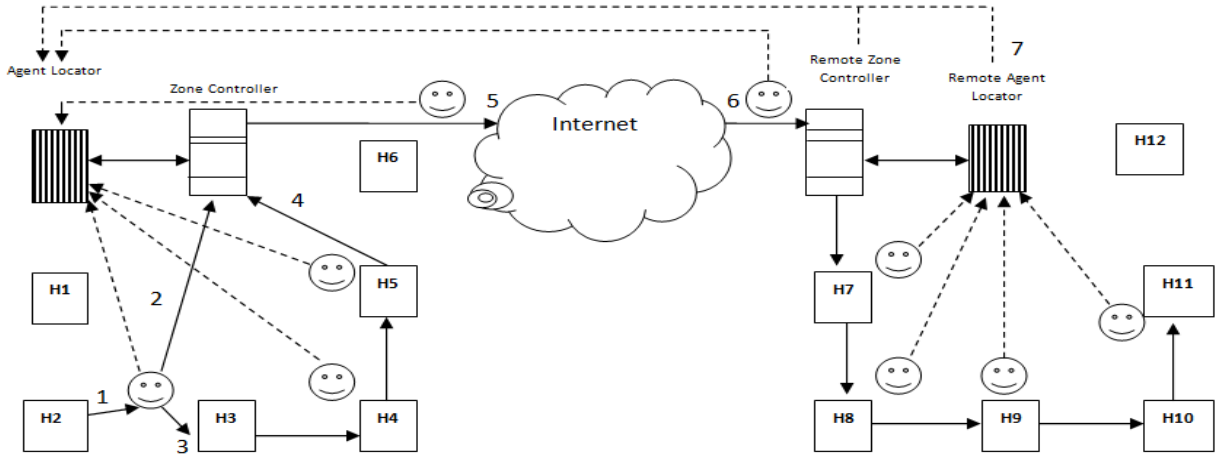

Fig: 3 Agent locator mechanisms with zones and zone controller

6. CONCLUSION AND FUTURE WORK

In this paper, an architecture is proposed to provide a potential scheme of providing authentication, confidentiality, integrity and reliability to the mobile agents. The proposal is scalable as the zonal domain provides hierarchy and control for deployment of mobile agents over larger coverage of area. The proposed scheme tries to capture the issues in a way to secure the propagation of mobile agent in both inter and intra zone mobility. With the additional security through agent obfuscation this framework can be extended to provide security from malicious agents and hosts in the existing circumstances of new threats emerging in the networking scenario. As there is no generic solution to all the attacks on mobile agents, using this model we will measure performance against particular application or domain and will analyze it in different domains of application as future work.

7. REFERENCES

[1] W. Jansen, "Countermeasures for mobile agent security", Computer Communication, Special issue on Advances in Research and Application of Network Security, November 2000.

[2] Danny B. Lange and Mitsuru Oshima. Seven Good Reasons for Mobile Agents. Communications of the ACM, 42(3):88–89, March 1999.

[3] WANG Ru-Chuan, HU Tao, XU Xiao-Iong, "Research in to mobile agent security", Joumal of Chongqing University of Posts and Telecommunications, Volume 16, Issue 3, pp.81-86, 2004.

[4] Zhidong Shen, Xiaoping Wu, "A Trusted Computing Technology Enabled Mobile Agent System", Proceedings of International Conference on Computer Science and Software Engineering, pp. 567-570,2008.

[5] Lukasz N, Marcin P, Michal R, "Mobile agent security", Thomas edition, Information assurance and computer security, lOS press, pp.l02-123,2006.

[6] Ibharalu F.T., Sofoluwe A.B., Akinwale A.T., "A reliable protection architecture for mobile agents in open network system", International journal of computer applications, Volume 17, Issue 7, pp.6-14, 2011.

[7] Ahmed Sameh Mohamed, Dalia Fakery, "SECURITY in MOBILE AGENT SYSTEMS," Applications and the Internet, IEEE/IPSJ Inter- national Symposium on, p. 4, 2002 Symposium on Applications and the Internet (SAINT'02), 2002

[8] Sreedevi, R.N.; Geeta, U.N.; Kulkarni, U.P.; Yardi, A.R.; , "Enhancing Mobile Agent Applications with Security and Fault Tolerant Capabilities," Advance Computing Conference, 2009. IACC 2009. IEEE International, vol., no., pp.992-996, 6-7 March 2009

[9] Qi Zhang, Yi Mu, Minjie Zhang, Robert Huijie Deng, "Secure Mobile Agents with Designated Hosts," Network and System Security, Interna- tional Conference on, pp. 286-293, 2009 Third International Conference on Network and System Security, 2009

[10] M.Gnanasekar and V. Ramachandran, "Distributed cryptographic key management for mobile agent security", International journal of recent trends in engineering, Volume I, Issue I, pp.164-167, 2009.

[11] Nisha P, Sunil Kumar, Ashu B, "Security on mobile agent based crawler", International journal of computer applications, Volume I, Issue IS, pp.5-11, 2010.

[12] Danny B. Lange and Mitsuru Oshima, (1998). "Mobile agents with Java: The Aglet API", Programming and Deploying JavaTM Mobile Agents with Aglets, Addison-Wesley Professional, 1998.

[13] Luca Ferrari, "The Aglets 2.0.2 User's Manual", October 2004.

[14] Java Programming Concepts From The Tutorial, http://java.sun.com/docs/books/tutorial/java/index.html.

[15] R.L.Rivest, A.Shamir, And L.Adleman, "A Method For Obtaining Digital Signatures And Public-Key

Cryptosystems", February 1978 Communications of the ACM, Volume 21 Issue 2.

[16] C. Collgerg, C. Thomborson and D. Low, "A Taxonomy of Obfuscating Transformations", Department of computer Science, The university of Auckland, New Zealand, Technical Report #148.

[17] W. Jansen and T. Karygiannis, "Mobile Agent Security ", Nist Special Publication 800-19 -, 2000. National Institute of Standards Technology.

[18] Joris Claessens, Bart Preneel, Joos Vandewalle , "(How) Can Mobile Agents Do Secure Electronic Transactions On Untrusted Hosts? A Survey Of The Security Issues and The Current Solutions", pp. 38-41, ACM Transactions on Internet Technology, Vol. 3, No. 1, February 2003.

[19] William M.Farmer, Joshua D. Guttman, and Vipin Swarup, "Security for Mobile Agents: Authentication and State Appraisal", pp. 5-11, European Symposium on Research in Computer Security (ESORICS).

[20] T. Sander and C. F. Tschudin, "Protecting Mobile Agents Against Malicious Hosts". G. Vigna, editor, Mobile Agents and Security, volume 1419 of LNCS, pp. 44–60. Springer-Verlag, June 1998.

[21] T.W.How, H.Y.Chen and M.H. Tsai, "Three Control Flow Obfuscation Methods For Java Software", The Institution of Engineering and Technology 2006, IEE Proceedings online no. 20050010.

[22] Vijil, E.C. Security Issues in Mobile Agent. Indian Institute of Technology. 2002.

[23] Zwierko, A., Kotulski, Z. Integrity of Mobile Agents: A new Approach. International Journal of Network Security 4(2) : 2007. 201-211

[24] Bellavista, P., A. Corradi, C. Federici, R. Montanari, and D. Tibaldi, Security for Mobile Agents: Issues and Challenges, chapter in "Handbook of Mobile Computing" (2004).

[25] Antonopoulos, N., K. Koukoumpetsos, and K. Ahmad, A Distributed Access Control Architecture for Mobile Agents, Proc. of Intl Network Conference, Plymouth, UK, July 2000.

[26] Niklas Borselius, (2002). "Mobile agent security", Mobile VCE Research Group Information Security Group, Royal Holloway, University of London Egham, Surrey, TW20 0EX, UK.

[27] Shilpa Budhkar, Anshita Mishra, Ferdous A. Barbhuiya, Sukumar Nandi "Security in Mobile Agent Systems with Locator Mechanism" 1st Int'l Conf. on Recent Advances in Information Technology | RAIT-2012 | Dept. of Computer Science & Engineering Indian Institute of Technology Guwahati Guwahati, India, 781039

[28] N. Borselius, Mobile agent security, Electronics & Communication Engineering Journal, October 2002, Volume 14, no 5, IEE, London, UK, pp 211-218

[29] Owen Arden Michael D. George Jed Liu K. Vikram Aslan Askarov Andrew C. Myers "Sharing Mobile Code Securely With Information Flow Control "2012 IEEE Symposium on Security and Privacy

[30] M. Vigilson Prem S. Swamynathan paper "Securing Mobile Agent and its Platform from Passive Attack of Malicious Mobile Agents" IEEE-International Conference On Advances In Engineering, Science And Management (ICAESM -2012) March 30, 31, 2012

[31] Kristian Schelderup1, Jon Ølnes1 paper "Mobile Agent Security – Issues and Directions "

[32] Dave Singel´ee, Bart Preneelin their article "Secure e-commerce using mobile agents on untrusted hosts" COSIC Internal Report May, 2004

[33] Parul Ahuja, Vivek Sharma in their paper "A Review on Mobile Agent Security "International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-1, Issue-2, June, 2012

[34] Hyungjick Lee† Jim Alves-Foss and Scott Harrison paper "The Use of Encrypted Functions for Mobile Agent Security" in the Proceedings of the 37th Hawaii International Conference on System Sciences – 2004