International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:3, No:11, 2009

Using Secure-Image Mechanism to Protect Mobile Agent against malicious Hosts

Tarig Mohamed Ahmed

Abstract**—**The usage of internet is rapidly increasing and the usage of mobile agent technology in internet environment has a great demand. The security issue one of main obstacles that restrict the mobile agent technology to spread. This paper proposes Secure-Image Mechanism (SIM) as a new mechanism to protect mobile agents against malicious hosts. . SIM aims to protect mobile agent by using the symmetric encryption and hash function in cryptography science. This mechanism can prevent the eavesdropping and alteration attacks. It assists the mobile agents to continue their journey normally incase attacks occurred.

Keywords**—**Agent Protection, Cryptography**,** Mobile agent security

I. Introduction

A mobile agent is an autonomous entity that can move from host to another under self-control. It is a new methodology for computation and communication as subarea of distributed system. The mobile agent can perform many tasks on behalf of its owner in different places. Through a journey, the mobile agent interacts with different hosts to accomplish tasks. The mobile agent starts the journey by using an itinerary table. The itinerary table can be static or dynamic [1]. Mobility is a key feature that allows to mobile agent to move form place to another. In addition, the mobile agent can communicate with different parts of the mobile agent system through communication messages. Also, agents' owner can monitor his/her mobile agents during their journeys.

Mobile agent systems are not fully utilized because many security problems need to be solved. The security of the mobile agent has received significant attention. Gary [4] defines four points in security area for mobile agent systems which are: (1) Protection of the host against the malicious mobile agents. (2) Protection of the mobile agent against the malicious host. (3) Protection of other mobile agents. (4) Protection of the underlying network.

This paper introduce a new mechanism called Secure-Image Mechanism (SIM). This mechanism aims to protect the mobile agent against malicious hosts. SIM deals with some types of attacks like eavesdropping and alteration attack. The mechanism uses the cryptography mechanisms. The rest of the paper has been organized as following: section 2 presents some solution proposed by research in the area of the mobile agent protection. Section 3 explains the symmetric encryption and hash function concept. Section 4 present SIM and its components. Section 5 concludes this paper and provides some guides to future works.

Tarig Mohamed Ahmed is an assistant Professor, Dept. Computer Sciences, Faculty of Mathematical Sciences, University of Khartoum., Sudan.; e-mail: Tarig_Harbi71@ hotmail.com.

II. Related Work

A mobile agent may contain sensitive data. It is important to protect the mobile agent from malicious hosts. The following points define some risks around the mobile agent [5]:
- Eavesdropping: Try to know the behavior and content of the mobile agents.
- Intercepting and Altering: Try to intercept the duties of the mobile agents or change the content by deleting or substituting.
- Reply: Send a copy of the mobile agent for illegitimate purpose.
- Masquerade: An entity pretends to be a different entity.

Many solutions proposed in the area of mobile agent protection against malicious host. Most of these solutions tried to detect not prevent the attacks [6, 7]:

A. Host Revocation Authority

This mechanism aids to solve the problem of malicious hosts by using a Trusted Third Party, the Host Revocation Authority. The HoRA controls which are the hosts that acted maliciously in the past. The agent sender must consult the HoRA before sending an agent in order to remove from the agent's itinerary all the revoked hosts. The HoRA can also revoke a malicious host if the agent sender detects and proves that this malicious host did not act honestly [8].

B. A Secure Mobile Agents Platform

This mechanism uses the authentication of mobile agents and the access control. The system resources are controlled by the mobile-agents platform. Each agent defines its own access control policy with regard to other agents using an Interface Definition Language (IDL), thus enforcing modularity and easing programming task [9]

C. Execution Tracing

Gary [10] proposes to detect attack when the mobile agent returns to home. Vigna [11] proposes a mechanism to detect misbehavior by using cryptographic traces and looking to the mobile agent history file (log) where the owner of the mobile agent will know if the mobile agent has achieved its duties correctly or not [12]. However, by using this mechanism, the mobile agent system must maintain a large log file. Also, a secure protocol is required for transferring cryptography hashes for external entities.

D. Obfuscated Code

This mechanism is to create a Black Box out of an original mobile agent to perform the same work of the mobile agent as an original mobile agent, but by different structure [13]. Obfuscated Code has disadvantages, for example, no black-box algorithms exist that work for arbitrary data. Sander and Tschudin [14] used cryptography in their approach in special cases by having the mobile agent programme compute not the

original, but an encrypted version of it. The result of this function is decrypted by the mobile agent's owner. But, cryptography theory has not a schema that computes arbitrary function in a non-interactive manner.

E. The Ajanta system

This system uses an approach for protecting the mobile agent [15]. The approach consists of three mechanisms, the first is to allow the programmer to declare parts of the mobile agent state as Read-Only and if any modification occurs to these parts, the mobile agents' owners can detect it by using the digital signature mechanism. The second mechanism is let the mobile agent create append-only data states container where the data stored in this container can not be deleted or altered without detection by the mobile agent's owner. The third mechanism is to let programmers to define data states to specific hosts and no other hosts can deal with these data states. These mechanisms use the encryption, the decryption and the digital signature.

F. Partial Result Encapsulation

This mechanism detects tempering by using encapsulating the results of the mobile agent actions at each place, for subsequent verification or when it returns to the base place [16]. The disadvantage of this mechanism, for example, does nothing to ensure mobile agent privacy. Also, the results to encapsulate may not be immediately clear.

G. Environment Key Generation

When some environment condition is true, this mechanism allows the mobile agent to take an action. A key is generated is used to unlock some executable code that was encrypted [17]. This approach has weakness such as: the control of the mobile agent could simply modify. The host limits the capability to execute a mobile agent code that ireated dynamically, sense it is considered an unsafe operation. The mechanism is connected with other protection mechanism.

H. KeyLets

This mechanism partitions a mobile agent as components according to the task type [18]. By using secret keys, it encrypts each component to protect them. The distribution of keys to different hosts is done through the execution of specific type of mobile agent that is termed a Keylet. The disadvantages of this approach: Propagation requires a third party code producer that can supply the mobile agent by a template the mobile agent owner. Also, a large number of transactions related to the keylet and a host may not be willing to support the increased of computation. Moreover, key revocation is not good in quality. In addition, it requires a complicated mechanism to categorize tasks of the mobile agent. Also, this mechanism does not protect the mobile agent code completely.

III. Cryptographic Mechanisms

Cryptography is used in security fields. The concept of using has a long history. One of the earliest cryptographic systems, Julius Caesar sent military messages to his generals [19]. The cryptography mechanisms are used to make secure communication among different parts. It has many concepts:
Encryption: This process converts a message from readable to be unreadable by using a key. The key is a numerical value used by the encryption process to change the information.
Decryption: This is opposite to the encryption process. It converts the encrypted message to its origin by using the same key or another key (depend on the mechanism).
Algorithm: The well-defined set of roles that are used to encrypt and decrypt the message. It is represented in mathematical function.

In cryptography world, the message that needs to be secured is called plaintext. After the message is encrypted it is called cipher text. The cryptography mechanisms are used in wide areas of the data communication fields. The researcher continually improves the cryptography mechanisms to be more trustful and powerful. There are many cryptography mechanisms as follows

A. Symmetric Encryption

A symmetric encryption is one of the cryptography mechanisms. It uses the same key for encrypting and decrypting. The key is called a secret key. The users who exchange data and use this mechanism must keep this key securely. The algorithm that is used in this mechanism is called a Secret-Key Algorithm. It uses the key to encrypt the message and the same key to decrypt the message. There are some popular secret-key algorithms and key size such as [20]:

- RC2 – 64 bits.
- DES – 64 bits.
- 3DES – 192 bits.
- AES - 256 bits.
- IDEA – 128 bits.
- CAST -128 bits (CAST256 uses 256 bits key)

Fig. 1 shows the encryption and decryption processes.

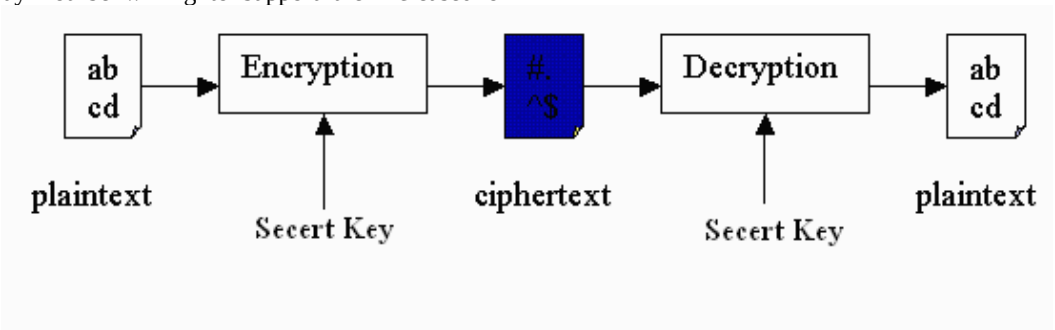

Fig. 1 Symmetric Key Encryption

B. Hashing Algorithm

A hash function is mathematical function that is used to generate message-digest from a message [20]. It uses the original message as an input and the output is a message-digest. The message-digest is a unique for the message (fingerprint of the message). Also, this function is called one way hash function.

IV. Secure-Image Mechanism

Secure-Image is a new mechanism to protect mobile agent against malicious hosts. The main idea behind this mechanism is to use symmetric encryption and the hash function in the cryptography science. The mechanism prevents eavesdropping and alteration attacks. The main benefit of this mechanism is to allow the mobile agent to continue its journey without problem incase these types of attacks occurred. SIM consists of many entities and each one has a specific role. The following sections describe the role of each one:

A. Mobile Agent in SIM

A mobile agent in SIM is an entity can travel among hosts to perform some tasks. All performed tasks are grouped per host. Therefore, we can look to the mobile agent as collections of task groups T1, T2... Tn and each task group will be implemented in a host. Therefore, the mobile agent visits in this case N hosts. T1 is implemented in H1 (Host 1), T2 is implemented in H2 and Tn implemented in Hn. The mobile agent visits these hosts according to its itinerary table. All hosts in the itinerary table should be classified either trust or untrust hosts. the mobile agent is encrypted when it moves from host to another to protect the mobile agent in communication channels. The mobile agent is decrypted when it arrives to the host. Therefore, some parts of the mobile agent may face security problems if the host is untrusted. From this point, the importance of SIM comes to protect all parts of the mobile agent in untrust hosts.

B. Host in SIM

A host provides mobile agents with services. The mobile agent may visit many hosts during a journey. A mobile agent system must classify hosts as trusted and untrusted hosts. The untrusted hosts may attack the mobile agents by altering some tasks not relevant to it or stealing sensitive information. The main objective of SIM is to protect the mobile agents against malicious hosts. SIM generates a secure image for the mobile agent before it arrives to the hosts that are classified as untrust hosts. SIM not make any types of obstacles to hosts to provide the mobile agents with services. Secure-Image controller plays the main role of generating the secure Image.

C. Secure-Image Controller

A Secure-Image Controller (SIC) is a trust place. It plays the main role in this mechanism. The mobile agent must visit SIC before going to the untrusted hosts. SIC generates a Secure-Image for the mobile agent. It dispatches the Secure-Image of the mobile agent not mobile agent itself to the untrusted host. The secure image is a version mobile agent with different content. The untrusted host deals with the mobile agent in the new picture without feeling any change. Normally, the mobile agent will perform its task in the untrust host and return to SIC. SIC makes investigation to be sure there is no altering attack occurred to the mobile agent.

D. Secure-Image Generation

SIC generates for each mobile agent a secure image any mobile agents wants to visit untrusted hosts. The image is generated by implementing the following tasks:

1) Generating Hashed Data for the Tasks

This task is used to protect mobile agent against alteration. As mentioned above, the mobile agent consists of groups. Each group represents a task that will be performed in a host. By using Hash Function, for each task a digest data is generated except the group that relates to the untrust host. SIC keeps this information away from the mobile agent. It uses this information to make sure that the untrust host does not make alteration attack against the mobile agent.

E. Encryption Task:

This task is used to protect the mobile agent behavior from the eavesdropping attack. By using symmetric encryption each group of task is encrypted by one secret key except a group that relates to the untrust host. The untrust host could not understand the behavior of the mobile agent that related to the other hosts.
SIC keeps a copy of the mobile agent as backup and creates a modified copy of the mobile agent by using Secure Image Generation Process. Figure (2) presents the generating of the secure image of the mobile agent that will visit untrusted host i.

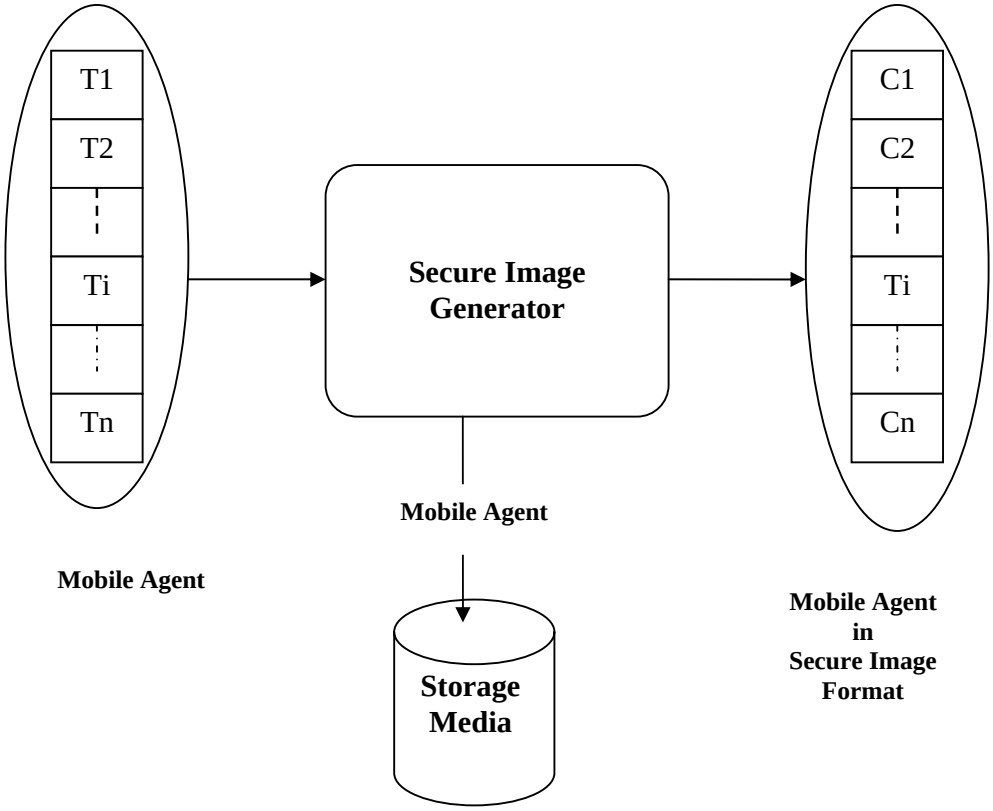

Fig. 2 Generating Secure Image Process

F. SIM Scenario

The following steps explain how SIM work:

1. A mobile agent system provides the mobile agent with classification of all hosts in the itinerary table (Trust/Untrust)
2. If the next station of the mobile agent is untrust host , the mobile agent visits the near Secure-Image Controller (SIC).
3. SIC saves a copy of the mobile agent on its storage media as backup.
4. SIC generates the secure image for the mobile agent.
5. SIC Sends the Secure-Image to the untrusted host.
6. SIC waits the mobile agent for specific time, her there are two possibilities:
   - 6.1 If untrust host prevents the mobile agent to continue its journey, SIC uses the backup copy of the mobile agent to allow the mobile agent to continue its journey with ignoring the untrusted host. SIC may notify the mobile agent system by this action.
   - 6.2 If the mobile agent return to SIC, the following tasks will be performed:
     - 6.2.1 All encrypted tasks will be decrypted by using the secret key.
     - 6.2.2 Generate the digest data of all tasks except the task that implemented in the untrust host by using hash function.
     - 6.2.3 Compare between two data digest to detect the alteration attack:
       - 6.2.3.1 If there is some change, that means the untrusted host attacked the mobile agent and SIC can replace the effected part by using the backup copy of the mobile agent.
       - 6.2.3.2 If there is no change that means there is no alteration attack occurred.

Fig. 3 presents SIM in the mobile agent system.

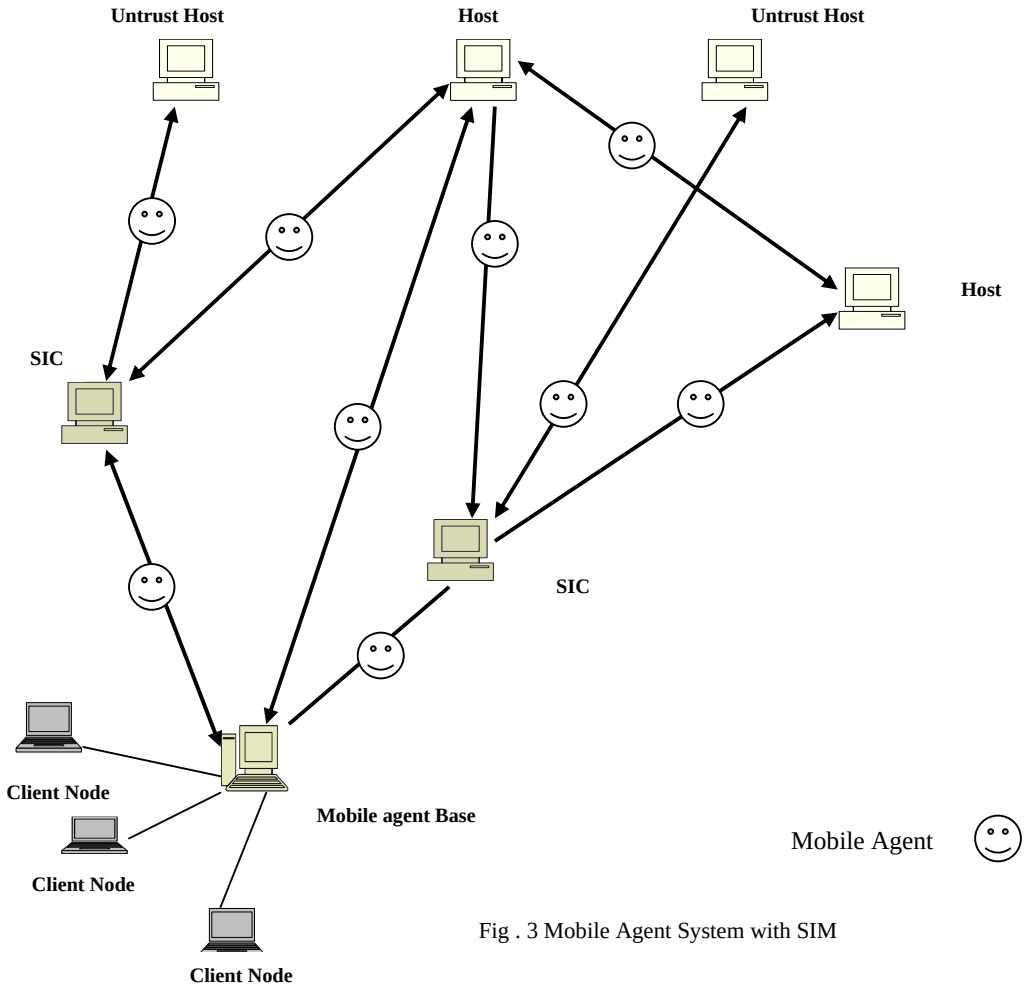

Fig . 3 Mobile Agent System with SIM

V. Conclusion and Future Work

This paper has introduced a new mechanism called Secure-Image Mechanism. SIM aims to protect mobile agent against malicious hosts. It uses cryptography mechanisms to achieve its tasks. This mechanism can prevent the eavesdropping and alteration attacks. It assists the mobile agents to continue their journey normally incase these attacks occurred. In this mechanism, the measuring of performance is required as future work to see the impact of SIM to mobile agent systems

References

[1] G. Karjoth, N. Asokan, C. Gulcu , *Protecting the Computation result of Free-roaming Agents*, Proceedings of Second International Workshop, Mobile Agent 98. Verlage Lecture Notes in Computer Science, Vol. 1477, PP 195-207, 1998.

[2] Karnik, Neeran, *Security in Mobile Agent Systems*, Ph.D. dissertation. Department of Computer Science and Engineering, University of Minnesota, 1998

[3] B.H. Tay, A. Ananda, *A Survey of Remote Procedure Calls*, Operating system Review, 24(3), PP 63-79, July 1990.

[4] R. S. Gary, *Agent Tcl: A flexible an Secure Mobile Agent System*, Fourth Annual Tcl/Tk Workshop (TCL 96) (Monterey, California, July 1996), M Diekhans and M Roseman, editors, July 1996.

[5] G. Karjoth, D. B. Lang, Oshima, *A Security Model for Aglet. IEEE Internet Computing* , 1(4) , 1997.

[6] M. Giansiracusa, *Mobile Agent Protection Mechanisms*, and the Trusted Agent Proxy Server (TAPS). Information Security Research Center, Australia, 2003.

[7] W. Jansen, T. Karygiannis, *NIST Special Publication 800-19- Mobile Agent Security*, Technical paper , National Institute of Standards and Technology, Computer Security Division.

[8] J.M. Cueva Lovelle et al. (Eds.): ICWE 2003, LNCS 2722, pp. 289–292, Springer-Verlag Berlin Heidelberg 2003

[9] Leila Ismail, A Secure Mobile Agents Platform, JOURNAL OF COMMUNICATIONS, VOL. 3, NO. 2, 2008

[10] TACOMA. University of Tromso, july 1999. *http://www.tacoma.cs.uit.no/*.

[11] G. Vigna, *Cryptography Traces for Mobile Agents*, In G. Vigna , editor, Mobile Agent and Security, volume 1419, 1998.

[12] A. Suen, *Mobile Agent Protection with Data Encapsulation and Execution Tracing*, Master Thesis, The Florid State University, 2003.

[13] F. Hohl, *Time Limited Blackbox Security: Protection Mobile Agent From Malicious Hosts*, In G. Vigna , editor, Mobile Agent and Security , PP 92-113 ,1998.

[14] T. Sander , C. F. Tschudin , *Protecting Mobile Agent Against Malicious Hosts*,In G. Vigna , editor, Mobile Agent and Security, Vol. 1419, 1998.

[15] Anand Tripathi, Neeran Karnik, *A Security Architecture for Mobile Agents in Ajanta*, Proceedings of the International Conference on Distributed Computing Systems, April 2000.

[16] B. S. Yee, *A Sanctuary for Mobile Agents, In Secure Internet Programming*, PP 261-273, 1999.

[17] J. Riordan and B. Schneier, *Environment Key Generation Toward Clueless Agents*, Technical Report, 1998.

[18] Hock Kim Tan and L. Moreau, *Mobile Code For Key Propagation*, Paper, Notes in theoretical Computer Science 63, UK, 2001.
[19] G. Paramasivam, *Cryptography in Microsoft.NET Part I: Encryption*, technical paper,
[20] G. Paramasivam,*Cryptography in Microsoft.NET Part II: Digital Envelop and Digital Signatures*, technical paper, *http://www.c-sharpcorner.com/Code/2002/Dec/DigitalEnvelop.asp*,2002.