International Journal of Electrical, Electronic and Communication Sciences
ISSN: 2517-9438
Vol:2, No:6, 2008

A New Approach for Mobile Agent Security

R. Haghighat far, H. Yarahmadi

Abstract**—**A mobile agent is a software which performs an action autonomously and independently as a person or an organizations assistance. Mobile agents are used for searching information, retrieval information, filtering, intruder recognition in networks, and so on. One of the important issues of mobile agent is their security. It must consider different security issues in effective and secured usage of mobile agent. One of those issues is the integrity's protection of mobile agents.

In this paper, the advantages and disadvantages of each method, after reviewing the existing methods, is examined. Regarding to this matter that each method has its own advantage or disadvantage, it seems that by combining these methods, one can reach to a better method for protecting the integrity of mobile agents. Therefore, this method is provided in this paper and then is evaluated in terms of existing method. Finally, this method is simulated and its results are the sign of improving the possibility of integrity's protection of mobile agents.

Keywords**—** Integrity, Mobile Agent, Security.

I. INTRODUCTION

REGARDING to growth and exposition of internet application, it seems that usage of tools which help user to manage this network, is a necessary matter[1]. One of the technologies that attract the attention and uses frequently nowadays, is mobile agent technology. mobile agents are software entities which have the ability to move in an unknown environment such as internet and help the user to do some tasks. There are many subject and problems about using mobile agent technology which one of them is security of mobile agents[2].

At the beginning, we first concern with mobile agents security and those aspect which threaten it. Then we examine the existing methods for protecting mobile agent. At the end we will provide a new method for integrity protection of mobile agents.

II. MOBILE AGENT SECURITY

In order to study mobile agent matter, we must consider two elements: Mobile agent and Host. Regarding to these two parts, there would be four security threats that are as follows [3]:

1) Threats from hosts to hosts.
2) Threats from hosts to mobile agent
3) Threats from mobile agent to another mobile agents
4) Threats from mobile agent to host

R. Haghighat far is with Islamic Azad University Broujerd Bramch. (e-mail: r_rambod2001@ yahoo.com).
H. Yarahmadi is with Islamic Azad University Broujerd Bramch. (e-mail: hsyar@yahoo.com).

This paper focuses on mobile agent's integrity, protecting the integrity of mobile agent including protecting the data, and mobile agent's code against the intentionally or unintentionally illegal changes. So if the data or mobile agent code changed, the mobile agent integrity changes too. Mobile agents integrity threats are classified into two classes: Interfere into integrity and change the information.

A. Interfere to Integrity

Interfere into integrity happens when host interfere into executive or implementing tasks, but does not change the mobile agents data. For example, when host send mobile agent incorrectly or when mobile agent performs imperfectly, or when mobile agents transmit to host which is not in its itinerary, or when host performs mobile agents arbitrarily, this threat occurs.

B. Change the Information

Changing the information happens when host changes mobile agent's code or mobile agent's data animus or by interfering into different communication agents, host changes them for his own purposes.

III. METHODS OF PROTECTING THE MOBILE AGENT

Both prevention mechanisms and recognition mechanisms are used for protecting mobile agents. Prevention mechanisms refer to protection of mobile agents while recognition mechanisms use for exploring possible security violation. Four methods that used for protecting the mobile agents are [4]:

1) Environment Securing
2) Record and Maintain
3) Cryptography
4) Time Technique

As we have stated before, security of mobile agents could be studied in different aspect which is matter of mobile agent's integrity discussion in this paper. There are many methods for protecting mobile agents which are included into two classes as recognition and protection.

Those methods that are including in "Recognition Class" and are applying for keeping integrity of mobile agents are as follows.

Methods based on recording and maintaining the itinerary, environment security .In contrast, those methods which are in

"Protection Class" and are using for keeping mobile agents security are: Methods based on cryptography and using cooperator agents.

IV. Proposed Method

As stated before, we are used protection mechanisms and recognition mechanisms for protecting mobile agent's integrity.

Each of these methods and mechanisms have advantages and disadvantages. Regarding to this matter these mechanisms are each other complementary, so it has been suggested that we are used their combination for increasing advantages and decreasing disadvantages. Therefore, we use both mechanisms to protect mobile agent integrity in proposed methods. In this method, we use three cooperator agents RA for recording itinerary, encryption and KA as keeping mobile agent data and lastly DA for recognition or detection malicious host.
This mechanism acts in this way:

First mobile agent uses dummy cooperator mobile agent for detecting host to determine whether it is malicious or not .If it is determined to be malicious then another host is considered to move. If it is determined to be safe, then the mobile agents informs Record agent that this host is secure, RA encrypts this path and records it. Next, mobile agent's data are given to KA too. Then, this agent encrypts data and keeps it. After these actions complete, the mobile agent moves to the host. Here we suppose that the environment is an unknown environment that include dangerous hosts with insecure probability P(DH=1), less dangerous hosts with insecure probability (0< P(DH) <1) and safe dangerous hosts with insecure probability P(DH=0).

In addition, we suppose only hosts that their dangerous probabilities are between 0 and smaller or equal with 1 (0<P(DH)<=1) destroy mobile agent's integrity that run on it and do not destroy mobile agent's integrity that only across on it. According to this assumption the propose method is:
MA (mobile agent): the agent that we want protect its integrity
DA (dummy agent): the agent that detects malicious hosts
RA (record agent): the agent that records mobile agent's itinerary.
KA (keep agent): the agent that keeps encrypted data.

A. Algorithm

1) Before MA moves toward the target host, first DA moves toward the target host in order to detect.
2) DA must do the actions that MA do in host, because its representative of MA. . DA is similar to MA through it has dummy data and code.
3) DA sends back to the location that MA is in it, after its action finished. If DA does not send back, be sure the host is malicious.
4) MA compares new results with old results.
5) If the results of comparison shows that host is malicious, so it selects another path and starts the actions from step 1 to 5 again. Otherwise:
   5.1) First MA shows the next moving path to RA and RA record it.
   5.2) MA encrypts its data and sends it to KA
   5.3) MA moves to host
   5.4) Another agents move to the host with MA(only agents run in host their data will be alter so data of RA and KA will be protect because they do not need to run in host).
   5.5) At last in destination, first the host of destination encrypts data of KA by private key then compares it with data of MA. if results of comparison be the same mobile agent's integrity will protect otherwise mobile agent's integrity destroy. Because data of agents are record in KA and KA is safe so data of mobile agents could be recover. In addition with considering RA it's certain that agents move from which host. Fig.1 shows this method in graphic case.

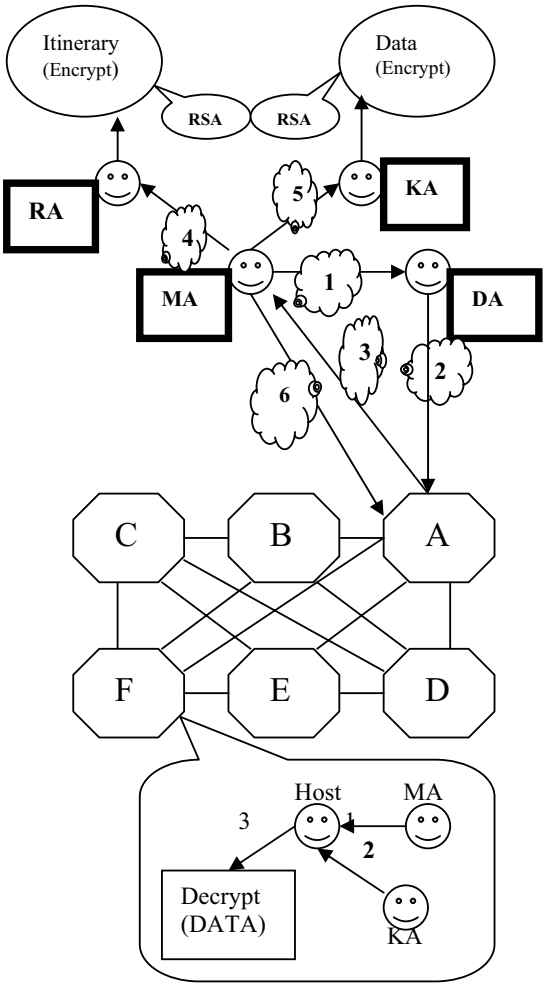

Fig.1 Proposed method

VI. Simulation

For simulate the proposed method we use BRAHMS environment and java language [7]. The scenario that we simulate is:
The network contains 7 hosts (can more or less)

Place A, Place B, Place C, Place D, Place E, Place F, Place G and we suppose that Place B and Place C are dangerous hosts. Addition we suppose that the network is a complete graph. In this simulation the selected path as random is:

Place A_ Place D _Place B_ Place C _Place G

To pay attention the propose method, according the fig.2, MA selects the Place A_ Place G_ Place D path and avoids to go Place B and Place C. fig.2 present the result of this simulation.

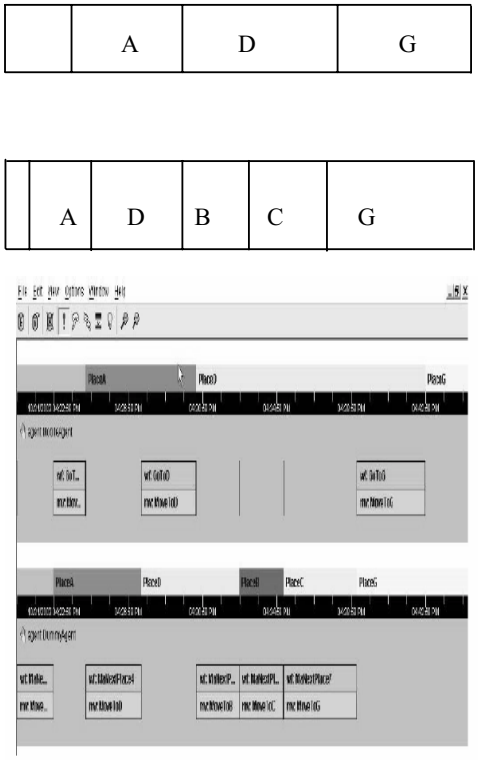

Fig. 2 Simulated Method

VII. Conclusion

According the previous the proposed method uses the protection and detection mechanisms for protecting the integrity of mobile agent. Both these mechanisms have advantages and disadvantages.

Some of the ways such as trust and keep the itinerary with the mobile agent's path informs about hosts that mobile agent run on them.

If mobile agent runs on a malicious host then there is probability that mobile agent change to a malicious agent. However in this way (recording the itinerary) has not authority to mobile agent for run on host but mobile agent changed to a malicious agent. Of course these ways attend to host security however with consider the mobile agent's itinerary we can detect that mobile agent's integrity is exist or not.

In the safety environment mechanism there are two ways that are: trust environment and detection object To pay attention this fact that the environment is an unknown environment (such as internet) that contains malicious hosts, semi malicious hosts and safe hosts so the safety environment is not in our purpose[5].

In the another way(detection objects) before mobile agent go to the host , first send an object to host in RPC way and with using this object can detect that if host is malicious or not.

If host be malicious then cause any changes to object, if it is safe then does not any change in object. Then object returned to mobile agent by host, so with attention to results mobile agent decision to go the host or not. Methods that protect mobile agent's integrity only use of protecting ways and do not use of detection ways therefore if protecting method are weak methods then host can change agent's data or code.

Proposed method use combination existing ways for protecting the mobile agent's integrity. So addition to benefits of using the cooperating agents there are below benefits.

By suppose that we mentioned the probability of protecting the agent's integrity will be:

$P(IKA)=1, P(IRA)=1, 0 =< P(IDA) <=1, 0=< P(IMA) <=1$

If in the tracing mobile agent's data or code will be change and theirs integrity will be destroyed.

(Means that P(IMA)=0) then to attention this fact that the data in previous saved in KA and P(IKA)=1 so the main data can be recover. In this manner, to attention that we use public and private key encryption method (such as RSA) so decryption of cooperating agent's data is not easy. In this method for recording the itinerary we use another cooperating mobile agent named RA and destination host (can be stationary agent) can found that mobile agent move from which hosts and learn which host is dangerous.

Against we should focus this problem that for moving a mobile agent to host three cooperating mobile agents should move to the host, therefore the overhead of network will be increase. So if the network contains N hosts in the worst case the mobile agent should visit N hosts and the overhead of network will be 4n and 4n is a member of $\theta(n)$.

Against the benefits of this method we should remember that this way has more overhead than another ways that protect mobile agent but involves all protecting and detection ways so it has more security than another ways. Although we should remember that the agent systems have less overhead rather than another ways Such as RPC.

(To attention this matter that in remote calling ways sender should receive the results so there is minimum one send and receive in any task but by using mobile agents this transmission is once so there is $O(n)$ against the $O(n^2)$).

VIII. Related works

According the previous mobile agent security can be considered in many ways. In this paper we focus on mobile agent's integrity. In the next works the others can consider another security problems such as protecting the confidentiality, protecting against the availability attacks authentication the agent for hosts and etc. about the mobile agent security there are four problems that are:

1) The security of agents against the another agents
2) The security of agents against the hosts
3) The security of host against the agents
4) The security of host against the another hosts

In this paper we focus on the second subject. In the next works the others can work on the 3 subjects.

REFERENCES

[1] Martin L. Griss , " *Software Agents as Next Generation Software Components,"* Component-based Software Engineering: Putting the Pieces Together, pp.: 641–657.
[2] Borselius N., *"Mobile agent security,"* Electronic & Communication Engineering Journal, Vol. 14, No. 5, 2002.
[3] Jansen W., "C *ountermeasures for Mobile Agent Security," C*omponent-based Software Engineering.
[4] Bierman E., Cloete E., *"Classification of Malicious Host Threats in Mobile Agent Computing,"* ACM International Conference, Vol. 30, pp.: 141-148, 2002.
[5] Roth V., *"On the Robustness of Some Cryptographic Protocol for Mobile Agent Protection,"* The Second Int. Joint Conference on Autonomous Agents and Multiagent Systems, Melbourne, Australia, pp.: 851-858, 2003.
[6] Acquisti A., William J., Van Hoof R., Scott M., Sierhuis M., " *Brahms Tutorial version 1.00,"* 2003.
[7] Grand M., *"Java Language Reference,"* ISBN: 1-56592-326-x, 450 pages, 1997.