A Hybrid Method for Protecting the Integrity of Mobile Agents

H. Yarahmadi † , M. Dehghan ±

† Islamic Azad University broujerd bramch
± Amirkabir University of Technology

Abstract
A mobile agent is a computer program which performs an action autonomously and independently on behalf of a person or an organization. Mobile agents are used for searching information, retrieval applications, filtering, detecting errors, intrusion detection systems and so on. One of the important issues of mobile agents is their security. Because of their software nature, their security is vulnerable against malicious hosts. One of the important security issues of using mobile agents is the integrity. In this paper, after describing the existing methods and analyzing the advantage and disadvantage of them, a complex method is presented to guarantee the integrity of mobile agents. In order to evaluate the performance of the proposed method, This method along with the related works are simulated.

Keywords
Mobile Agent, Integrity, security.

1- Introduction
To pay attention the growing and extend of internet application, the use of tools that help user to management and work with this network is a necessary matter. One of the technologies that used and should pay attention to it is mobile agent technology. Mobile agents are software entities that can move in a uncertain environment such as internet and can help users to do some tasks [1]. There are many subjects and problems about use of mobile agents technology that one of them is mobile agent security [2]. In this paper we first describe mobile agent security and their threats. In the next we consider the existing methods for protection of mobile agent and the last we will propose a new method for protect the integrity of mobile agents.

2- Mobile Agent Security
For consider the mobile agent security we should consider two part of agent systems: mobile agent and host. To attention these parts there are four security threats that they are:
1- Threats that done from hosts to hosts
2- Threats that done from hosts to mobile agents
3- Threats that done from mobile agents to hosts
4- Threats that done from mobile agents to hosts
For protect mobile agent, recognition the security requirements is necessary. Attack’s base from hosts to mobile agents are:

1- Integrity
2- Availability
3- Confidentiality
4- Authentication
5- Non-Repudiation
The focus of this paper is mobile agent’s integrity.
Protecting the integrity of mobile agent involves protecting the data and code of mobile agent against the oversight or intentionally alteration. So if alteration of mobile agent’s data or code occur then integrity of mobile agent is destroyed. Mobile agent’s integrity threats involves interference to integrity and alter the information.

2.1- interference to integrity
Interference to integrity when occur that host interferences to mobile agent’s duty, but does not alter the mobile agent’s data. For example when host does not send mobile agent correctly or when mobile agent does not exactly execute or host executes mobile agent desired then this threat is occurred.

2.2- Alter mobile agent’s data or code
Alteration of data (code) when occur that host alters the mobile agent’s data (code) maliciously.

3- Methods of protecting the mobile agents
For protecting the mobile agents there two mechanisms that are: protection mechanisms and detection mechanisms. Protecting mechanisms are used for protect the mobile agents. Detection mechanisms are used
for detecting the violation the security. Four methods that used for protecting the mobile agents are:

Trust - Recording Tracing – Cryptography – Time Technique

According the previous mobile agent’s security problem is considerable in many view that subject of this paper is mobile agent’s integrity. The methods are used for protecting the integrity of mobile agents divide into two parts that are protecting and diction. Detection methods that used are:

Methods that their base is Cryptography
Methods that their base is using of cooperating agents.

4- Propose method

For protecting the integrity of mobile agents according the previous both protecting and detection mechanisms are used[4]. To attention this point that these mechanisms are complement for each other, so for increase theirs benefits and reduce theirs imperfections combination this methods is proposed. So for protecting the integrity of mobile agent, in proposed method we use both protection mechanisms and detection mechanisms.

In this way we use three cooperating mobile agents for recording the mobile agent’s itinerary, encryption and keeping the mobile agent’s data and the last for detection malicious host.

This mechanism acts in this way:

First mobile agent uses dummy mobile agent for detect host for this purpose that if it is malicious or not. If it detects that host is malicious then mobile agent select another host. If it detects that host is safe then the mobile agents informs selected path to record mobile agent and it encrypts it’s path and records it as it’s data. As the next a copy of mobile agent’s data are given to keep mobile agent. Then this agent encrypts received data and keeps it too. After doing these tasks mobile agent moves to host. here we suppose that the environment is a unknown environment that involves malicious hosts with dangerous probability \( P(DH) = 1 \).

Hosts with any malicious that theirs dangerous probability are \( 0 < P(DH) < 1 \) and

Safe hosts with dangerous probability \( P(DH) = 0 \).

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 the mobile agent run on it and do not destroy mobile agent’s integrity that only across on it. With 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

The algorithm is below:

1- Before MA moves to host DA moves to host for detection malicious hosts.
2- Because DA is a representative of MA so it should does tasks that if MA will run on host are similar to MA’s tasks with this difference that dummy agent has dummy data and dummy code that they are similar to MA’ data and MA’s code.
3- DA backtracks to the location that MA is on it. If DA does not backtrack to the location then we can assure that host is dangerous and destroyed DA.
4-If DA backtracks to the location then MA compare the DA’s data(code) with MA’s Data(code)
5- If the compare presents that host is dangerous then MA selects another host and the algorithm starts from 1 else:
   5.1- First MA informs the next path (host) to RA then RA encrypts this path and 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 (To attention this suppose that malicious hosts may be only change mobile agents that run on them and do not change agents data(code) that move and cross over them so their data or code remain without any change).
   5.5- In the last on the destination host (it may be a stationary agent) with private key the data (code) of KA will be decrypt then these data will compare with data of MA. If there is not any difference between data(code) then mobile agent’s integrity will protect else mobile agent’s integrity destroyed. But to attention this fact that MA’s data were keep on the KA and data of KA do not change so MA’s data will be recover additional with consider the RA we can found the MA itinerary and found the malicious hosts.

Figure 3.1 presents this method and
Figure 3.2 presents the sequential diagram.

5- 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 run 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 objects.

To pay attention this fact that the environment is a unknown environment (such as internet) that contains malicious hosts, semi malicious hosts and safe hosts so the safety environment is not in our purpose.

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 changes 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:

\[ P(IKA) = 1, P(IRA) = 1, 0 \leq P(IDA) \leq 1, 0 \leq P(IMA) \leq 1 \]

If in the tracing mobile agent’s data or code will be change and theirs integrity will be destroy (That means \( P(IMA) = 0 \)) 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 task. 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 host in the worst case the mobile agent should visits 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 ways Such as RPC (To attention this point that in remote calling ways sender should receive the results so there is minimum a send and receive but by using mobile agents this transmission is once so there is $O(n)$ against the $O(n^2)$)

6- Simulation
For simulate the proposed method we use BRAHMS environment. The scenario that we simulate is:
The network contains 7 host (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 figure 3, MA selects the Place A_ Place G _Place D path and avoids to go Place B and Place C. figure 6.1 present the result of this simulation.

7- 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.

8- References