A Framework of Agent Protection Protocol for Secure Execution of Mobile Agent

Chang-Ryul Jung*

ABSTRACT

As an agent is applied into various fields, it is suggested as the paradigm of new application technology in the area of computer communication. However, the mobile agent brings the problem of security on an agent due to mobility. This study proposals the mobile agent protection protocol framework for more effective protection and safety. The designed Framework of protocol uses the public key, the private key and the digital signature in PKI environment based on JAVA. This is the mechanism accomplishing safely the work of an agent by tracking the pattern of execution and the mobility plan through the VS(verification server). This also secures the security and the flawlessness of an agent through the VS guaranteeing safety from malicious attacks.

요 약

에이전트는 다양한 분야에 적용이 가능하기 때문에 컴퓨터 통신 분야의 새로운 응용기술의 패러다임으로 제시되었다. 그러나 이동 에이전트는 이동성으로 인하여 에이전트에 대한 보안에 대한 문제가 제기되었다. 본 논문은 이동 에이전트를 보다 효과적인 보호와 안전성을 보장할 수 있는 이동 에이전트 보호 프로토콜의 프레임워크를 제안한다. 설계된 프로토콜은 JAVA기반의 PKI환경에서 공개키와 개인키 그리고 전자서명을 이용한다. 이는 VS를 통하여 에이전트의 실행 패턴과 이동계획의 패턴을 추적하여 안전하게 에이전트 임무 수행을 하는 메커니즘이다. 또한 악의적인 공격으로부터 안전함을 인증하는 VS을 통해서 에이전트의 무결성과 기밀성을 보장한다.

KeyWord

Mobile Agent, Execution Tracking, Agent Protection, Public Key Infrastructure

Ⅰ. Introduction

The computer technology and the development of information communication technology bring users the change of information paradigm. Like in the real world, users develop the agent technology to freely utilize the IT in cyber space. An agent reduces the time and the cost of users as having the characteristics such as autonomy, social ability, reactivity and pro-activeness[1].

Contrary to a message base and RPC, this goes around among hosts by controlling itself in different networks, interacting with another host or an agent. And by using each other's resource, it implements the work of an agent.

Therefore, the communication between modules is made by RPC in normal environment as the extended concept of RPC and RP(remote programming) type.

* 순천대학교 컴퓨터과학과

접수일자 : 2004. 4. 3

As the mobile agent moves around by accomplishing the mobile code of a program, the network traffic can be reduced. And the parallelism of works is increased for multi-users and the flexible and active service is provided.

The study on an agent continues the development of the agent platform by using an agent language. Recently, there are many platforms based on Java. Table 1 shows the present condition of the mobile agent system.

But, there are cases in the mobile agent that an agent is threatened by malicious elements or a malicious host and a host is by the malicious agent.[4].

Table. 1 Mobile Agent System

system	development/language/security
AgentTcl	Dartmouth College, USA/Tcl/ Not Supported
Ara	Univ. of Kaiserslautern, Germany/ Java
Aglets	IBM/Japan/Java/Not Supported
Concrdia	Mitsubishi/USA/Java/Not Supported
GrassHopper	IVK++/Germany/Java/Supported
JATLite	Stanford University/USA/Java
Mole	Univ. of Stuttgart/Germany/Java
Messengers	ICU/Korea/Java/Supported
JADE	TeleCOM LAB/Italia/Java/Supported
Odyssey	Gerneral Magic/USA/Java
Tacoma	Univ. of Tromso & Conel Univ.
Voyager	ObjectSpace Inc./USA/Java/ Not Supported

Due to these cases, the security of the mobile agent is to be preceded for the exact execution of user's work. Especially, the protection of the mobile agent requires the protection of an agent while it is moving and the protection of agent's codes or data while they are executed. However, the code or the state of an agent are to be considered and then accessed during the execution of an agent. As the program or the state of execution can not be executed without exposing themselves to a host[4][8], it is very difficult to prevent malicious behaviors (forgery, fabrication).

Therefore, this study suggests the mechanism protecting the mobile agent for the safe execution of the mobile agent against malicious elements in the distributed computing environment by using the mobility plan and the pattern of execution tracking. The suggested technique transmits the results to an agent owner or a host as an agent completes the execution.

This study is composed of five chapters: in chapter two are explained the security techniques of an agent and the mobile agent and in chapter three are the execution tracking and the VS and in chapter four are the execution of the mobile agent and the algorithm on tracking pattern of mobile process and in chapter five are the protocol and the mechanism protecting the mobile agent and in chapter six are the conclusion and further studies.

II. Related Work

The mobile agent is the software accomplishing the role of a user instead by moving among hosts. The mobile agent is composed of the agent code, the state variable and the Itinerary showing the list of next destination. The protection from the attack occurring in the detector in which an agent is responsible for the actual execution is meaningless.

That is why it is impossible, in this case, for a host to rightly execute and complete an agent and to secure the safety from the threat such as the forgery or the drain of agent's data.

The study on the protection of the mobile agent is seeking in the prevention and the

mechanism of error detection[4, 10, 11].

The prevention mechanism lays physical device to make the malicious approach to the code and the state of an agent impossible. Therefore, the safety of system is increased, but the overhead of purchasing expensive H/W devices occurs. So the code shuffle[4] and the component cryptography are suggested as the approaching method based on S/W. The former is the method protecting the original movements of the code by making it difficult to alter or re-engineer the code, because the mobile code is "re-arrayed" before being transmitted to a remote site. The latter can encode and decryptography because the execution host uses the encrypted component of an agent. But there is the drawback that it has to be used in the pre-determined sites and should know the mobile route. So the error detection mechanism[3, 4, 8, 9, 11, 12] as the new and promising method is to use the cryptography function[3, 11, 12]. In this case, the behavior illegally accomplishing the code, the state and the execution flow of the mobile agent is detected. There are schemes such as the code tracking, the state estimation, the recording and the mobile route according to the plan. This uses the static code and other codes having dynamic elements because the static code is easily protected by using the digitized signals and the flow of state and execution is the dynamic element.

When the techniques actually used in the error detection mechanism combines the mobile agent with the state estimation function and the moving agent arrives to new execution environment, the estimation function is the mechanism to be estimated as the current state of an agent passing as a parameter[7].

There is the protection method of execution results relating between result values by appling the hash function to the execution result obtained from the host[12].

Table. 2 Method for Protection of Mobile Agent

분 류	Error Detection Mechanism
result protection	Slidng Encryption
	Mutual Itinerary Recording
	Itinerary Recording with Replication and Voting
	Path History
error detection	Crypographic Trace
	State Appraisal Mechanism
	Protection of Results

As the method to detect the illegal alteration to the code, the state and the execution flow of an agent, there is the cryptography tracking method which tracks the execution of a host and verifies the result value.

III. Execution of Mobile Agent through VS and Tracking Pattern of Mobility Route

The execution tracking used as the method executing the remote code begins to be applied to the mobility during the execution of an agent code.

The execution tracking of the traditional mobile agent tracks the code of an agent being executed in the host platform. So when the system overhead of a host and a host analyze the execution results, the overhead is occurred by returning the execution results to an owner. In the process of treating the results in the data Detector, it can be attacked from malicious elements.

And as the work of an agent is accomplished inside a host, it is difficult to secure the flawlessness of data which an agent has by the malicious host. The mobile agent should follow the rule about the security and the network to interact with the transmission of an

agent inside the network.

If not, it would be impossible for an agent to safely interact and treat information in other hosts or the agent server. As the security of an agent is very important[6-8], the authentication of the mobile agent and the flawlessness and the secrecy of data should be secured to make safe activation of an agent.

Table. 2 Encrypted key used in verification

ciper key	specification.
$Pub_{(K)}$	public key
$Pvt_{(K)}$	private key
$HA_{(asw)}$	digital signature
i_A	agent identifier

For it, this study designs the agent protection protocol to apply the encrypted execution tracking technique based on the VS and to safely and accurately accomplish the work of an agent. An agent waits in the waiting list for VS to verify and treat data. The verification and the authentication of an agent are treated in the comparison authentication module.

The process of verifying actual safety of the mobile agent is made by the execution tracking through the authentication module.

The process of treatment compares the agent identifier, the value of an agent and the agent code enrolled by an owner of the mobile agent and is treated through the process of the digital signature and the cryptography and decryptography. The keys used in authentication are shown in Table 3.

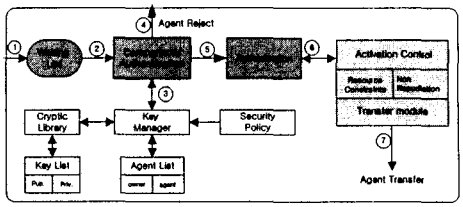


Fig. 1 Structure of VS and execution work flow

As such a process is finished, the execution tracking of an agent is treated with the authentication authorized by access control.

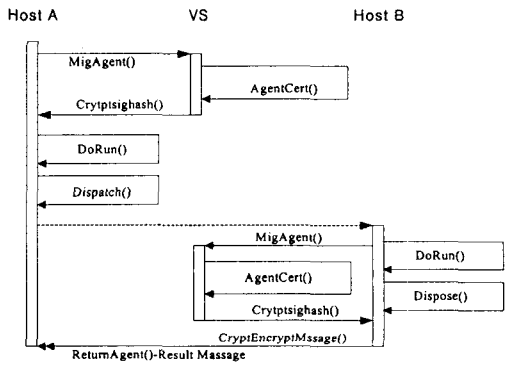


Fig. 2 Execution pattern of mobile agent

Fig. 3 shows the execution tracking and the verification in the verification server.

First, the agent transmitted from a host is received in the verification server(①). As the process to compare, authenticate and confirm the received agent, the safety is verified for the safe execution of an agent(②).

$$\{\{AgtA(t_A, i_A, S_A, C, It), (T_{(AgtA)}, HA_{(vs)})\} SP_{(vs)}\} Pb_{(A)}$$

The token of an agent($AgtA()$) includes a time stamp(t_A) recording the transmission

```
public abstract class MigAgent{
URL destination =Null
 public void CratAgentCert{
  try{
   destination = (URL)((object[])args[])[0]
   AgentCert()
    if (CryptSignhash(HA, Null, 0, PubSignature ,Pub
      &MobileAgt)){
       printf("Mobile Agent Singnature\n",MobileAgt);}
        else { handleError("This is a malicious agent");}
        executAgt(
          new MobiltyAdapter(){
           public void MobileAgt(MobliliyEvent){
            try {
             MobileAgt.Message(update)(sucess, DoRun());
              Dispatch(); }
               Dispatch(destination();  }}}
```

Fig. 3 Algorithm of execution pattern of mobile agent

of an agent and the replying time, an agent identifier(i_A), an agent state(S_A) and a code of an agent(C).

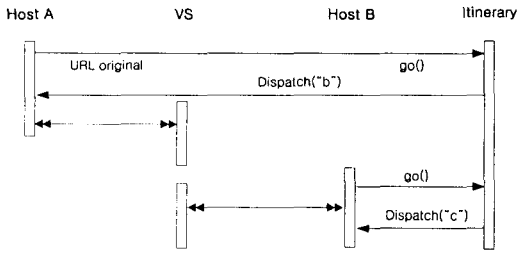


Fig. 4 Pattern of itinerary of mobile agent

The control is managed with the transmission by the condition and the transmission module. The agent execution pattern and the pattern of Itinerary managed by the VS are shown in Fig. 3 and Fig. 4 respectively.

The digital signature($HA_{(vs)}$) and (T_{AgtA}) showing that the tracking of an agent A is made are encrypted into the secret key of the VS and transmitted as the public key of a host A. The key manager treats the security policy and the encrypted key related with security in the process of ② and ④(③). The agent reject means the malicious agent which can not be authenticated as a normal agent(④). As ⑤, ⑥ and ⑦ are authenticated, the empowerment of authority and the control are occurred for an agent to operate normally.

```
public abstract class Itinerary {
protect URL origin = Null
public void Itinerary(URL original){
 original=origin;
 }
 public void init(MoileAgt) {
 mobileAgt=Mobileagt.getMobileAgtContext
  MobileAgt.getMobileAgtId(),
   MobileAgt.getMobileAgtSat(),
    MobileAgt.getMobileAgtISat());
     go(); }
     public URL getOrigin() {return original; }
      protected void go(URL destination) throws Exception
       { MobileAgt.dispatch(distination);
        }}
```

Fig. 5 Itinerary pattern algorithm of mobile agent

IV. Mobile Agent Protection Mechanism

4.1. Mobile Agent Protection Protocol and Entity

While being executed to protect the mobile agent, the mobile agent protection protocol shows the protocol of execution tracking authenticated by the VS. The VS authenticates the mobile agent and the authentication is made on the PKI base. PKI is the cryptography-based technology securing the flawlessness by enabling the digital signature made up of public key technology.

Execute Tracking

For the safe execution of a mobile agent, the execution tracking is the process to ask the VS for authentication through a host platform and to track the execution condition. This is processed until the work of an agent is finished and the state of an agent informs end.

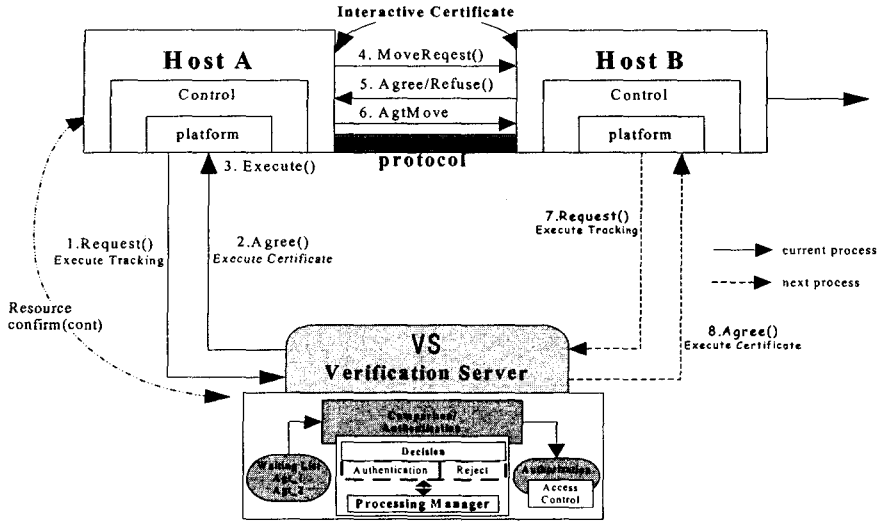


Fig. 6 A mobile agent protection protocol by using execution tracking

Interactive Certificate

When the execution of an agent is finished, an agent moves to another host according to the Itinerary. This is the interactive reliable process between hosts. The safety is authenticated by the digital signature and the public key of the VS.

Execute Certificate

For the mobile agent and a host to be executed properly, the VS certificates by encrypting them into the digital signature $HA_{(con)}$ and the public key $Pub_{(K)}$. Then the host platform is checked for the mobile agent to be executed in the host platform and to become the right execution result.

Agent Migration

The mobile agent accomplishes the work of an agent by moving to another host located in different location in network.

Resource Confirm

An agent accomplishes the work and provides the agent owner of the first departure with the results of execution. When the safety of execution results is confirmed, the owner(host) of an agent uses them as useful data.

4.2. Protection Mechanism according to Accomplishing Process of Protocol

step 1. A requester or an owner of an agent's transmitting an agent to the VS .

The agent identifier which confirms the code of an mobile agent and the uniqueness of an agent is compared with an agent transmitted first. And for an agent to be verified from the verification server, the authentication of the verification server is to be preceded. To receive the authentication of the VS, the owner of an agent encrypts an agent by the public key of the VS and transmits it to the VS.

step 2. Request : the execution authentication of an agent to the VS

For the execution of an agent, the safety of an agent and a host is to be guarded. So the

authentication is requested to the VS to be safe and reliable.

step 3. Authentication permission : transmission of the VS to a host

An agent is authenticated through the process manager of the VS. The authenticated agent is encrypted with the certification of the VS into the public key of a host $Pub_{(X)}$ and transmitted.

The digital signature of certification is needed for transmission. This is the process that is necessary for the mobile agent to be executed in the host platform and to obtain exact results.

If the mobile agent did not get the execution authentication, it would be rejected and not accomplish the work of an agent.

step 4. Requiring mobility: from host A to host B

Through the execution authentication, the mobile agent accomplishes the work of an agent in the host platform and moves according to the Itinerary. In this process, the mobility is requested to the host of destination.

step 5: Agree/Reject: Mobility of an agent

The host of next destination goes through the safety of an agent and the process of interactive authentication between hosts. This process confirms that there is the consistent authentication level between the host sending the mobile agent and the host receiving it. It means that they trust each other as the host authenticated from the VS.

So the agreement or rejection of the mobile agent is decided after checking safety. If the mobile agent is not safe, the platform of a host does not permit the mobility. The rejected mobile agent tries to move to the dynamic remote host according to the Itinerary.

When the mobility of the mobile agent is agreed, an agent moves to the host platform and through the authentication process of the VS safely accomplishes the work of an agent in the host platform. This process is repeated till the stage of an agent is finished. As the mobility is finished, the mobile agent returns back to the host of departure.

As the execution tracking is made, this mechanism manages safely and effectively the safe communication between host platforms by having the verification server treat mainly the host platform or the mobile agent.

V. Conclusion

By using various applications developed by information technology, the mobile agent is used for convenience of users. The use of such a mobile agent requires the safety of an agent.

For an agent to safely accomplish by solving the safety problem of the mobile agent, this study suggests the mechanism to be able to protect an agent through the execution tracking.

Among techniques that protect the mobile agent, the software method is applied because it is better off than other protection techniques in terms of economic and efficient reasons. By appling the software tracking technique, the mobile agent is protected against malicious elements. And the VS for the execution tracking is made for protection of the mobile agent. The VS is the server system comparing and authenticating by using the encrypted key to detect errors such as the false alteration to the code or the state of the mobile agent.

The execution authentication of an agent enables the mobile agent to accomplish the work in the host platform and the execution tracking protocol uses the private key, the

public key and the digital signature in PKI.

By using the protocol confirming the flawlessness and the secrecy, the mobile agent and the host platform protect the mobile agent's execution.

The safety of the mobile agent, the effectiveness of system which can reduce the dealing time, and the problem of overhead are to be improved and the study on the model to be protected from malicious elements is to be continued.

Reference

[1] P. Dasgupta, L. E. Moser, P. M. Melliarsmith, "MagNet:Mobile Agents for Networked Electronic Tracing", IEEE Transaction on Knowledge and Data Engineering, Vol. 11, No.4, July, 1991.

[2] A. Villazon and W.Binder, "Portable Resource Reification in Java-based Mobile Agent Systems", In Mobile Agents : Proc. of the 5th International Conference, Number 2240 in LNCS, Springer-Verlag, Altanta, USA, 2001.

[3] H. K. Tan, L. Moreau, "Extending Execution Tracing for Mobile Code Security", In Proc. of the 2nd International Workshop on Security in Mobile Miti-Agent Systems, associated to AAMAS-2002, Bologna, Italy, July, 2002.

[4] F. Hohl, "Time Limited Blackbox Security : Protecting Mobile Agents from Malicious Hosts", G. Vigna (Ed), in Proceeding of Mobile Agents and Security, Springer-Verlag, Lecture Notes in Computer Science No.1419, pp.92-11, 1998.

[5] T. Taka, T. Mizuno, T. Watanabe, "A Model of Mobile Agent Services" in enhanced for the International Conference on Parallel and Distributed Systems, pp. 274-281, 1998.

[6] C. Raibulet, C. Demartini, "Mobile Agent Technology for the Management of Distributed System-a Case Study", in Journal of Computer Networks Vol.34, pp.823-830, 2000.

[7] V. Roth, "Secure Recording of Itineraries through Co-operation Agents", in Proceeding of the ECOOP Workshop on Distributed Object Security and 4th Workshop on Mobile Object Systems: Secure Internet Mobile Computations, pp.147-154, INRIA, Frince, 1998.

[8] J. Alesheimer, C. Cachin, J. Camenisch, G. Karjoth, " Crytographic Security for Mobile Code", In Proc. IEEE Symposium on Security and Privacy(S&P 2001), pp.2-11, may, 2001.

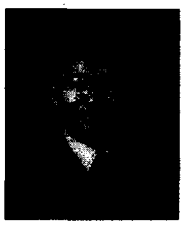
[9] H. Reiser, G. Vogt, "Security Requirments for Management System using Mobile Agents", In the Proc. of the 5th IEEE Symposium on Computer and Communication:ISCC 2000, Antibes, France, July, 2000.

[10] C. R. Jung, J. G. Koh. "Mobile Agent Protection Scheme through Execution Tracing of Agent Code and Status", in the Journal of KICS, Korea, Vol.28, No.7C, pp.743-751, 2003.

[11] T. Sander, C. Tschudin, "Towards Mobile Cryptography", In Proc. of the 1998 IEEE Symposium on Security and Privacy, Oakland, CA, May, 1998.

[12] G. Vigna, "Cryptographic Traces for Mobile Agents", Mobile Agents and Security, pp.137-153, LNCS1419, Springer -verlag, 1998.

저자 소개



정창렬(Chang-Ryul Jung)

1999년 8월 순천대학교 대학원 컴퓨터교육학과 졸업(석사)
2000년-현재: 순천대학교 대학원 컴퓨터과학과 (박사수료)
2003년 6월 : Dept. of Computing Science, Alberta State University, Visiting Researcher.
※ 관심분야 : Information Security, Mobile, Agent, Watermarking, Image processing, Electronic Commerce System