A Mobile-agent Security Architecture

DeShu Lin
Computer and Control College
Guilin University of Electronic Science and Technology
GuangXi, China
e-mail:tea027@163.com

TingLei Huang
Computer and Control College
Guilin University of Electronic Science and Technology
GuangXi, China
e-mail: tlhuang@guet.edu.cn

***Abstract*—Increasingly widespread application of mobile agent, mobile agent system's security is a prominent problem to be solved, mobile agent's security question is critical. In this paper, based on cryptography, computer network security, mobile agent security architecture at the same time gives the practical methods and suggested ways can be used in other new security measures. The core problem is how to use measures to ensure the security of mobile agent communication and mobile agent execution environment of security, at the same time ensure that mobile agent can be applied more widely.**

Keywords-mobile agent ; security ； cryptography； reputation

I. INTRODUCTION

Mobile agent (MA) is a kind of agent, agent research originated in the field of artificial intelligence, agent is a simulation of human behavior and relationships, has certain intelligence and is able to independently run and provide the appropriate service procedures. Mobile agent is a heterogeneous network can autonomously migrate from one host to another host, and can interact with other agent or resource programs.[1] Mobile agent is an important component of distributed computing. At present a variety of mobile devices access to the internet, the network speed and bandwidth are relatively limited, thus limiting the development of mobile networks, mobile agent can be dynamically moved to the request agent server-side implementation. And there are many cases mobile network due to bandwidth limitations can not be at all times so that each mobile network equipment at the same time online, so that the user can submit tasks to the mobile agent processing, when the network connection to access the network and through mobile agent and return the calculations results, you can greatly reduce the amount of network data transmission. As mobile agent is cross-platform, heterogeneous network transmission can be done; mobile agent has been widely applied in many systems.

With the development of electronic commerce, mobile agent research has become increasingly frequent. Security is one of the most challenging issues particularly. In networked environments there are dispersed numbers of system users. In mobile agent applications, the core of the problem is to ensure the security of mobile agent communication and mobile agent execution environment of security, at the same time ensure that mobile agent can be applied more widely. If there are too many security restrictions, it will make the mobile agent applications ineffectively be used in a larger range, but also to reduce the widespread use of the program. If the security is not enough there is no way to conduct genuine commercial mobile agent software.

II. THE PROPOSED SECURITY MODEL

Mobile agent because of its run in a networked environment, it may encounter a lot of network attack and deception. Until now, mobile agent system, the main security issues mainly has two aspects. [2]

(1) A malicious agent on the target host harm, it can move to the host in the theft of critical and important information on the system and become a threat.

(2) A malicious service hosts threat mobile agent, affecting the normal operation of the interfering systems and destruction of information.

View of the above two issues, this paper proposed a specific solution. The main security has two aspects.

(1) Mobile agent communications, critical data and information are encrypted, and the mobile agent communications environment according to safety requirements, based on SSL (Secure Socket Layer) protocol or VPN network.

(2) The adoption of mobile agent security trust model TMMARC [3], the security trust model is mainly for mobile agent system, each entity uses the reputation of the assessment, and dynamic management of reputation value, based on the reputation value as the basis for communication supporting judgments

Based on the above points, the security measures are proposed by the mobile agent framework shown in Fig. 1.

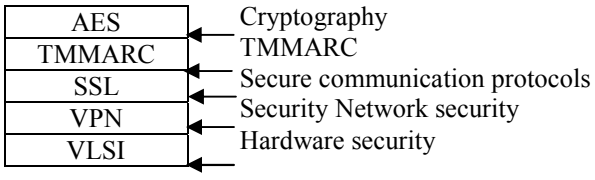

Figure 1. Mobile-agent security framework

978-1-4244-5895-0/10/$26.00 ©2010 IEEE

III. MOBILE AGENT COMMUNICATION SECURITY

Mobile agent communication security measures can make use of cryptographic algorithms and digital signatures to solve. Based on TCP / IP protocol communication networks can also use SSL (Secure Socket Layer) protocol to ensure secure transmission of data network.

A. Using AES encryption security for mobile agent

In the mobile agent system can be used in the encryption algorithm AES (Advanced Encryption Standard), this algorithm is also known as Rijndael encryption. [4] AES is proposed by the U.S. National Institute of Standards and Technology （NIST）to replace DES encryption standard. AES encryption algorithm uses symmetric block cipher system, the key length of the support for the 128,192,256, length of 128 bits; the algorithm should be easy to achieve a variety of hardware and software.

We can use different information security level, with different key lengths to achieve. As shown in Table 1. [5]Here not only to consider the classification of data security requirements, taking into account the network and the hardware implementation cost of the actual operation process, we put the wireless network data communications using 128-bit key length, this mainly in order to save mobile networks in the computational overhead.

TABLE I. ENCRYPTION-LEVEL CLASSIFICATION

Security level	Example	Key length
High	Private information，bank and Confidential b usiness information	256
Normal	Private information	192
Little	Wireless info	128
not require	Public information	no encryption

B. AES encryption algorithm through the implementation process

AES algorithm accepts a 128-bit plaintext, and a 128,192,256 for the key under the control to generates a 128-bit ciphertext. Specific operations by known round (round) a collection of steps, in which the number of rounds can be 9, 11, 13(depending on key length). AES has a four-step operation: 1.SubBytes 2.ShiftRows 3.MixColumns 4.AddRoundKey. [6]

1) SubBytes function

SubBytes function is the only non-linear mixing step of AES algorithm, the 16 bytes of each of parallel map for new bytes. SubBytes function is the implementation shown in Fig. 2.

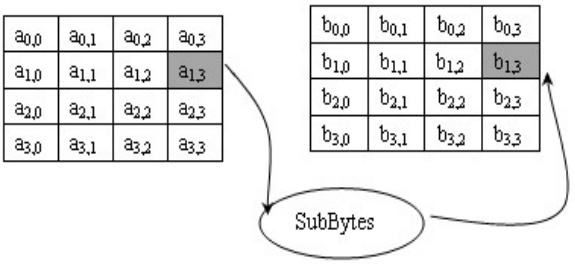

Figure 2. SubBytes function

2) ShiftRows function

ShiftRows function is to state data in each row in the rotate right 0,1,2,3 bits, respectively. The state transformation is very easy to implement. ShiftRows function implementation is shown in Fig. 3, where ROLi representatives Rotate Right i bits.

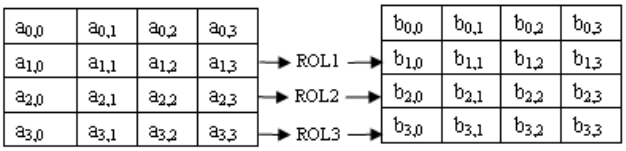

Figure 3. ShiftRows function

3) MixColumns function

MixColumns function main aim is to transform the column encryption process, and its operation is a matrix multiplied by the state matrix to be a new matrix for each column in a repeat operation to get a new state of matrix data. The implementation of MixColumns function shown in Fig. 4.

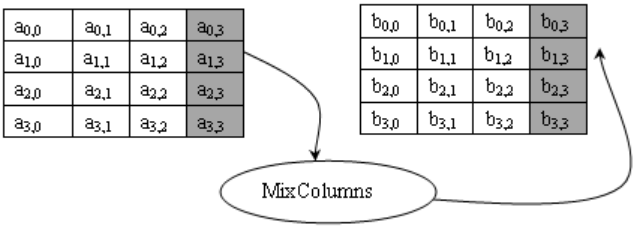

Figure 4. MixColumns function

4) AddRoundKey function

AddRoundKey function is to bring the key and state data to be exclusive or a new state data, the implementation in Fig. 5.

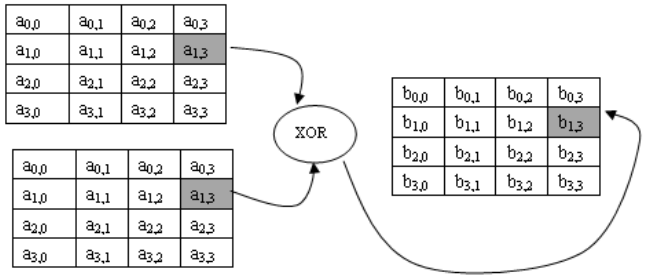

Figure 5. Figure 5 AddRoundKey function

Several rounds of the above function (9,11,13) Executive on the possible to the encrypted data, to use such encrypted data transfer although it will cost a large computational cost, but it can be secure data.

C. *Mobile agent communication based on SSL*

SSL to guarantee the safety of Internet, data transmission, using data encryption technology, to ensure data transmission on the network of the process will not be intercepted and the interception. At present, ordinary common specifications for the 40 bit of the safety standards, the United States already launched 128 bit of a higher safety standards. SSL protocol is in the TCP /IP protocol and between the various application layer protocols for data communications to provide security support. So in terms of security, limited processing capacity network applications can communicate using SSL protocol.

D. *Mobile agent combination of methods using AES and SSL communication*

For data security requirements for mobile agent can use a higher encryption algorithm AES and SSL protocols operate simultaneously. Of course, a combination of the two ways to spend a lot of hardware processing costs.

IV. MOBILE AGENT RUN ENVIRONMENT SECURITY

Mobile agent network environment where have some malicious hosts, in order to distinguish between these malicious hosts, Ghada Derbas proposed TRUMMAR model, reference [3] proposed a security trust model TMMARC[3], which is the former improvement. The main idea is using TMMARC model of the host to evaluate the security by the reputation of the value, to assess what the host is secure. To ensure that only secure communication between hosts.

Trusted environment, mobile agent communication model shown in Fig. 6, TC1 is trusted center.

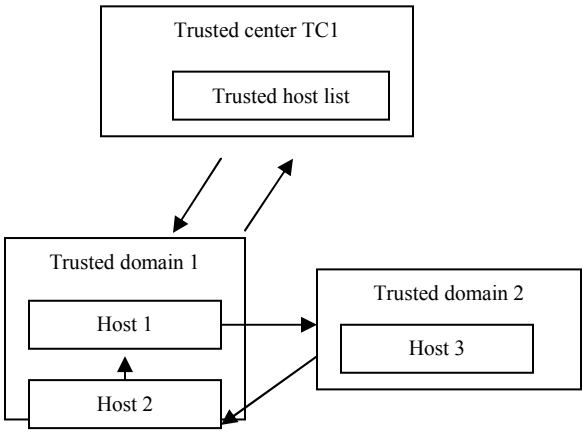

Figure 6. Reputation based on security of mobile agent

Host1 first look at the list to inquire about their reputation in whether there is sufficient trust in mobile agent host to complete the task, if not need to obtain the trust of the host Trust Center. Here, first of all to be a trusted host Host2.

If the trust fails to match the host2 a mobile agent to complete the task, host1 look up Trust Center to check list of trusted hosts, which can be trusted domain 2 of the hosts allocated to the three hosts.

If the host a choice of mobile agent hosts three tasks, so that is also the host 3 to check whether your host a list of trusted hosts. If it is acceptable for the completion of the implementation with mobile agent or it can not be implementation. This will ensure that the entire communications environments are carried out under the operation of credit based on security.

V. SIMULATION RESULTS

In the mobile agent communication, we were using the process of 128,192,256-bit encryption key experiment, a total of 10 experiments carried out statistical data obtained in Fig 7.

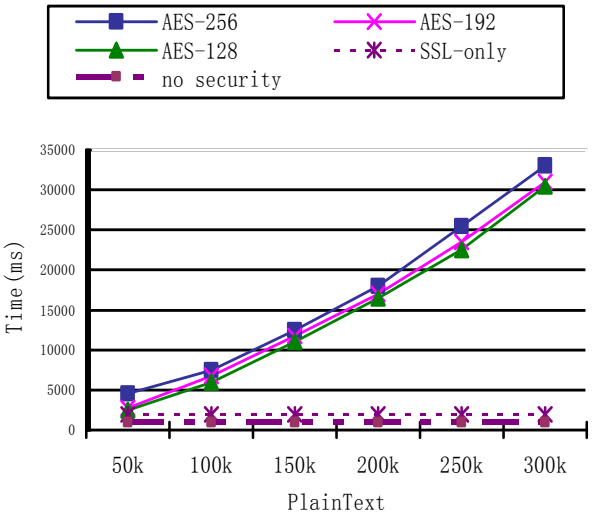

Figure7. The execution time for agent-based communications

Through this Figure we found that, in the absence of measures in the case of encryption security ONLY using SSL, the system time-consuming with not use any security measures are similarly, using AES algorithm is due to the time to encryption, decryption, hashing process computing time consumed by a larger, and because after the cipher text by encrypting the data is basically twice the original data, so this part of the greater consumption of both the transmission time, resulting in more time than just encryption using AES encryption algorithm increase in transmission time. The calculation process is used to measure the time of launch recoverable. Because the two sides' communication time is not synchronized, we use this method.

VI. OTHER SAFETY MEASURES

A. *Using a hardware approach to encryption algorithm for the calculation of AES algorithm.*

This strategy is mainly to reduce the mobile agent system for computing time of encryption, can reduce the burden of dealing with encrypted data, and improve the system speed. In reference [7] there were proposed a kind of solution.

B. *Based VPN (Virtual Private Network) for mobile agent communication*

VPN router has the technology was originally one of the key technologies, in the switch, device or operating system software inside the firewall also supports VPN functionality, simply say, VPN core is in the use of public networks to create a virtual private network. As the VPN network itself has a very good security, and allows for the local area network applications can be extended, so the use of VPN network transmission, not only security, but also conducive to LAN resources for remote access to mobile agent.

In addition to other security measures provided above, with the mobile agent to further improve the development platform. There are a lot of mobile agent's development platform to consider security issues, and in the system on the integration of mobile agent security solutions, this of course able to secure mobile-agent solve the problem with ease.

VII. CONCLUSIONS AND FUTURE WORK

In this paper, security issues for mobile agent, mobile agent security is given a specific solution. The application of mobile agent security, the key is to balance mobility and safety, in ensuring better mobility at the same time, is able to make full use of software algorithms or hardware way to improve the system's security. Mobile agent security, related to the field of data security technologies. This paper presents a mobile agent secure access methods of mobile agent access to information security management and authentication to improve the security of mobile agent, mobile agent system to improve the flexibility and maintainability, and reduce the system's coupling. Such safety measures proposed to expand the use of the mobile agent.

REFERENCES

[1] YunYong Zhang and JinDe Liu. "Mobile Agent Technology". Tsinghua University Press, Beijing,2003.

[2] DING Jianguo, LIU Huiling, CHEN Hansheng etc, "A Method of Security Authentication for Mobile Agent", vol. 27.NO.2. Computer Engineering.

[3] SHEN Yong-jun SHI Xiao-ping LI Xiao-qing, "The Research bout Security Trust Model of Mobile Agent," in Micro Computer Information, vol.25,2009.

[4] XiaoYuan Yang, LiXian Wei. "Computer cryptography". Xi'an: Xi'an Jiaotong University Press, 2007

[5] Rossilawati Sulaiman, Dharmendra Sharma, Wanli Ma. "A Multi-agent Security Architecture"[C]// 2009 Third International Conference on Network and System Security. Australia: [s. n.], 2009: 184-191.

[6] Tom ST Denis, Simon Johnson a, Shen Xiaobin translation. "Cryptography for Developers".Beijing: Mechanical Industry Press, 2007.

[7] CHEN Jun, WANG Jing, ZENG Xiaoyang, HAN Jun, VLSI Implementation of Low Cost AES Algorithm, 2007 vol.33.NO.4. Computer Engineering.