Security of Mobile Agent in Ad hoc Network using Threshold Cryptography

S.M. Sarwarul Islam Rizvi, Zinat Sultana, Bo Sun, Md. Washiqul Islam[1]

***Abstract*—**In a very simple form a Mobile Agent is an independent piece of code that has mobility and autonomy behavior. One of the main advantages of using Mobile Agent in a network is - it reduces network traffic load. In an, ad hoc network Mobile Agent can be used to protect the network by using agent based IDS or IPS. Besides, to deploy dynamic software in the network or to retrieve information from network nodes Mobile Agent can be useful. But in an ad hoc network the Mobile Agent itself needs some security. Security services should be guaranteed both for Mobile Agent and for Agent Server. In this paper to protect the Mobile Agent and Agent Server in an ad hoc network we have proposed a solution which is based on Threshold Cryptography, a new vibe in the cryptographic world where trust is distributed among multiple nodes in the network.

***Keywords*—**Ad hoc network, Mobile Agent, Security, Threats, Threshold Cryptography.

I. Introduction

WITH the introduction of wireless network and advancement of 802.11 protocols, the concept of wireless ad hoc network has been evolved from the necessity of having a mobile, dynamic and self-organized network where there will be no specialized nodes (i.e., routers to provide routing and packet forwarding service). The procedure to ensure security services in such network is a bit different from traditional wired or wireless networks and also not so trivial. Several methods have been developed in this arena. Among them the use of Mobile Agent has got a lot of attention among the security people. But mobile agent is also not out of threats. So security of mobile agent is important because security of mobile agent and security of the network that use mobile agent for security purposes are complementary.

In this section, a brief discussion has been presented about the ad hoc network, threshold cryptography and mobile agent. In the next section some light have been shaded on different security issues and potential threats in a mobile agent system. Some researches have been conducted in the relevant field. Those have been discussed in third section. Then we have presented our proposed model or solution. At last there is a conclusion included where some outcomes of the work and ideas of some future works have been discussed.

A. Ad hoc Network

'Ad hoc' is a Latin phrase. It means "for this purpose" [1]. And an ad hoc network is usually a small network (e.g., LAN), which is built spontaneously as wireless devices get connected with each other [2]. In an ad hoc network there is no concept of central dependency. So, there is no central router or server for providing routing decisions, network monitoring, analysis and management. Nodes in the network work together while taking and generating routing decisions. A frequently cited example of the usage of ad hoc network is – in military units for communicating through wireless devices in the battle field. In battle field there is hardly any chance to have a pre-established network infrastructure. Here ad hoc network provides flexibility, scalability, robustness and a cost-effective way of communication. Due to its alluring features ad hoc network has a great potential to be used in commercial applications like virtual classrooms or sensor networks, law enforcement, shopping mall, car parking etc [4], [8].

B. Mobile Agent

A mobile agent is an independent piece of code with autonomy and mobility features [6]. A mobile agent can migrate from one host to another autonomously to resume its execution [5]. Here autonomy means to take decision and to execute an action without direct user or human interaction. One of the main advantages of using mobile agent is – it reduces network traffic load noticeably as it does not require any continuous connection or communication between the server and the client [7]. Besides, use of mobile agent makes access of remote resource more efficient and flexible. Agent can adapt dynamically to an environment and can operate in heterogeneous environments. It is robust and fault tolerant. Though origin of the term 'Agent' was in the field of 'Artificial Intelligence', it has gained a lot of potential in the field of network monitoring, analysis and Intrusion Detection/Prevention System [6]. Besides these, the mobile agent can also be used for information retrieval, server configuration backup, dynamic software deployment etc [3]. The use of mobile agent, its life cycle, components and system architecture can found in more detail in [8]-[11].

C. Threshold Cryptography

[1] S.M. Sarwarul Islam Rizvi. Author is with The Royal Institute of Technology, KTH, Sweden (corresponding author to provide phone: +46735973469; e-mail: ssirizvi@kth.se).

Zinat Sultana. Author is with The Royal Institute of Technology, KTH, Sweden (corresponding author to provide phone: +46707173280; e-mail: zinat@kth.se).

Bo Sun. Author is with The Royal Institute of Technology, KTH, Sweden (corresponding author to provide phone: +46707304506; e-mail: bo4@kth.se).

Md Washiqul Islam. Author is with The Royal Institute of Technology, KTH, Sweden (corresponding author to provide phone: +46735974279; e-mail: mwislam@kth.se).

Symmetric and Asymmetric Key Cryptography are the two most well known and widely used cryptographic mechanisms available today. In Symmetric Key Cryptography a common key is shared by two parties of communication for both encryption and decryption purpose [12]. The problem here is distributing or exchanging the key in a secured manner. For Asymmetric Key Cryptography there is no such problem. Here each party has a unique pair of keys: one public key and one corresponding private key. The public key is known by everybody but the private key is kept secret [13]. Certificate Authority (CA) issues certificate which is used to bind a public key to its owner and to protect the integrity of the public key. To verify the public key of the CA there is another top level CA and at the top of the chain there is a Root CA (a trusted party). But problems arise in a case like ad hoc network where there is no way to verify the certificate by the central trusted party (CA).

Under these circumstances here rises the concept of Threshold Cryptography where trust is distributed among the network nodes. According to (n, t+1) threshold cryptography system, n entities share the ability to perform a cryptographic operation (e.g., creating a digital signature, sign certificate). t+1 entities can perform these operations collectively whereas it is not feasible for at most t entities to do so, even by secret agreement [4]. More detail on Threshold Cryptography is available in [4], [16].

II. Security Issues and Threats

Security of mobile agent is essential in any mobile agent based application. Besides security of agent platform is also important. To discuss the security aspects of a mobile agent system we have considered the following security services: Confidentiality, Integrity, Authentication, Authorization and Non-Repudiation.

A. Confidentiality

Confidentiality ensures that, data and code carried by an agent is not accessible by unauthorized parties (unauthorized agent or unauthorized agent server).

B. Integrity

Integrity guarantees that agent's code and baggage cannot be altered or modified.

C. Authentication

Authentication enables a mobile agent to verify its identity to an agent server as well as an agent server to a mobile agent. Without authenticity an attacker could masquerade an agent's identity and could gain access to resources and sensitive information.

D. Authorization

Authorization ensures that an agent can access the resource or information only those are allowed for it to access.

E. Non-Repudiation

Non-repudiation assures that the agent-server or the mobile agent cannot repudiate the actions it has performed.

Threats in a Mobile Agent system can be categorized as [11]:

- *Threats from mobile agent to agent server*
- *Threats from agent server to mobile agent*
- *Threats from mobile agent to mobile agent*

F. Threats from Mobile Agent to Agent server

Potential threats from a mobile agent to an agent server can be listed as: illegal access to services and resources of agent server, steal or reveal of secret information from server, denial of service, damage of software and data, penetrate virus/worms and finally action repudiation [11].

G. Threats from Agent server to Mobile Agent

Similarly an agent might face some threats from an agent server those can be listed as: illegal access to mobile agent's resources, steal code and valuable information carried by agent, reveal private or sensitive action performed by mobile agent, damage of code and baggage, execute agents code incorrectly, sending agent to unintended destination, cheat agent with false information and information or action repudiation [11].

H. Threats from Mobile Agent to Mobile Agent

Finally an agent could face threats from another agent. These threats are stealing agent information, convey false information, render extra messages, accusing processor time, denial of service, information or action repudiation and unauthorized access [11].

III. Related work

Many researches have been conducted regarding the security issues of Mobile Agent system. Some are to protect only the code and some are to protect the agent server. Few researches have been conducted about all the security aspects of mobile agent system in an ad hoc network. Some of the prime works is listed below:

A. Secure Image Mechanism

One way to provide security to mobile agent and to protect the partially processed data is to introduce a SIC (Secure Image Controller) in the system. When a Mobile Agent head towards an Agent Server it looks up the itinerary table to check whether the host is trusted or not. If the host is not trusted then the Mobile Agent goes to SIC (Secure Image Controller). SIC generates an image (a version) of the agent and sends the image to the untrusted host rather sending the original one. After completion of execution the agent image is compared with the original agent by the SIC. If the verification is failed SIC just drop the returned image of agent and use the original agent to complete the rest of the task [5]. Advantage of this method is, in this way an agent can be sent to an untrusted host and verify it. By using SIM eavesdropping and alteration attack can be prevented. But there is no solution to protect the agent server from malicious

agents. There is also no solution for Authorization, Access Control and Non-Repudiation service.

B. Protecting Mobile Agent Through Tracing

Geovanni Vigna has proposed a schema to detect any possible undesired modification of a roaming agent by any malicious site using cryptographic traces [14]. Cryptographic Traces are nothing but log or history of operations done by agent during its life time. An agent program is checked against an assumed history of the agent's execution. The agent owner can check whether the agent has performed its tasks correctly or not from the log file. But in this method the agent system must maintain a large log file and special mechanisms are needed to reduce the log size.

C. Partial Result Encapsulation

In this procedure Symmetric Key Cryptography is used. Bennet Yee proposed this idea to protect the intermediate state of partial result of an agent after being executed on a server. When an agent moves from a host its state and result is encrypted with a symmetric key to produce MAC (Message Authentication Code) on the message. This authentication code is used to verify any types of modification of the agent's partial result [15]. Problem of this method is to maintain and generate a large scale of symmetric keys.

D. Sandboxing

The main goal of sandboxing is to protect the agent platform from a malicious mobile agent. Typically a sandbox provides a controlled set of resources for a guest program to run. While the guest program runs in the restricted environment its movement and activities are observed. If it does not show anything unusual and executes the tasks it supposed to do, then the program is considered safe for the actual environment and is allowed to execute there [6].

E. Signed Code

This method provides a way to secure mobile agent using Digital Signature. This sign may be provided by either the creator of the agent or the owner or by some third party. Authenticity, Non-Repudiation and Integrity of an agent can be ensured by this technique. For Authorization and Access Control, Attribute Certificate can be associated with the signed code [6]. This method requires a CA (Certificate Authority). So it is not applicable for an ad hoc network where there is no central trusted party.

IV. Proposed Model/ Architecture

To describe our model we will take help of the following figure (Fig 1.) of an Ad hoc network.

As we know that in an ad hoc network it is not possible to use a central server or a single point of trust, so trust should be distributed here among the available nodes. Distribution of trust in our proposed model is attained by using 'Threshold Cryptography'.

According to Threshold Cryptography to sign a certificate (for a service or server) there is a Master public/private key pair (K_{pb} / k_{pr}) which is called the key pair of the Key Management Service. The master public key is known by all the Agent Servers and all nodes in the network trust any certificate signed by the master private key (k_{pr}).

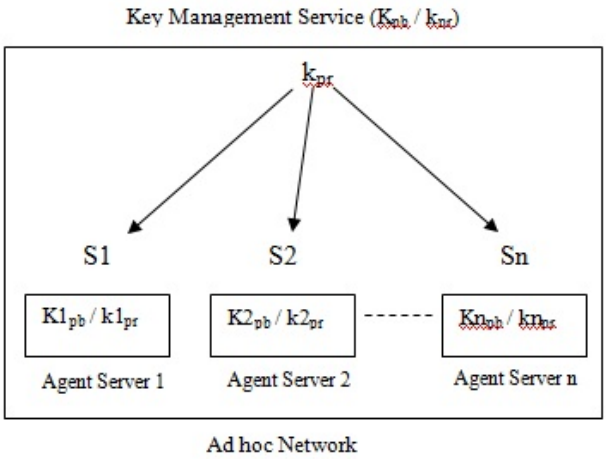

Fig. 1. Mobile agent security in ad hoc network using threshold cryptography.

This master private key is divided into n shares. Each server has one share of the private key (k_{pr}). So S1, S2, S3…..Sn are the key shares for Agent-Server1 to Agent-Server-n respectively.

Each Agent-Server has its own public-private key pair. Each server knows public keys of all other Agent Servers.

As our model is based on (n, t+1) cryptography, where n >= t+1, here in the network n number of servers shares the ability to sign digital certificate and generate the corresponding private key of the Master Public Key (K_{pb}). Any (t+1) servers can perform this operation jointly. Here, *t* is the threshold value for the network and the system can tolerate up to *t* compromised servers.

An important use of Mobile Agent may be to collect data from a network. For example, in a meeting people may want to share real time data among them. Here we consider that, the people in the meeting have established an Ad hoc network to get connected. We also consider that communicating devices (i.e. Laptop) they are using have the ability to process an Agent code, means agent platform is installed there. Now, assume that person 1 (Agent Server 1) wants to gather some data from other members and has launched a mobile agent for that purpose. That agent will move from one agent server to another, collect data and at last return with the collected data to the agent server who launched it.

The whole processing or workflow can be described by the following steps:

1. At first Agent-Server1 launches a Mobile Agent. The agent traverses to Agent-Server2. Before launching the agent, Agent-Server1 calculates Message Integrity Code (MIC) of the agent code and digitally sign with its private key ($k1_{pr}$). This digital signature provides authentication service. After

signing Agent-Server1 encrypt the package (agent code plus digital signature) by the master public key (k_{pb}). This provides confidentiality service.

2. Now when Agent-Server2 receives the full package it calculates the master private key by using its own partial share of the key with share of other t agent servers. After generating the key Agent-Server2 verifies it using Master Public Key (k_{pb}). If any Agent Server is compromised and it provides incorrect key share then it will not be able to generate the correct private key (k_{pr}). If it happens then Agent-Server2 tries another set of *t+1* shares. This process continues until Agent-Server2 gets the correct key.

3. After having the master private key Agent-Server2 decrypts the package which it has got from Agent-Server1. Then it verifies the signature of Agent-Server1 as it knows Agent-Server1's public key ($k1_{pb}$). Then Agent-Server2 becomes ensured that the package is from Agent-Server1. Then Agent-Server2 calculates the MIC of Agent code and compare, thus check the integrity of the code. Then the Mobile Agent executes its operation on Agent-Server2.

4. After finishing its execution on Agent-Server2 the Mobile Agent moves to Agent-Server3. But before that, Agent-Server2 calculates the MIC of the agent code, data and sign digitally with its private key ($k2_{pr}$). Then encrypt the whole package with the master public key (k_{pb}).

5. This process repeats until the Mobile Agent finishes its tasks and return to the launcher agent server (Agent-Server1).

V. Conclusion and Discussion

This paper provides a solution for securing mobile agent in an ad hoc network. We have used Threshold Cryptography in our model, because it provides solution to the problem of central certificate authority (CA) and trusted third party in PKI, by distributing trust among several network nodes. Though it is tough to provide 100% security in an ad hoc network, to detect and prevent vulnerabilities and intrusions, use of mobile agent can play a tremendous role. But mobile agent is not free from threats. Our model provides a way to secure not only mobile agent, but also the agent server and the agent platform. It provides prime security services like confidentiality, integrity, authenticity. According to threshold cryptography we have considered the value *t* as a threshold value for the ad hoc network. It means the system can tolerate up to *t* compromised servers. Here the point of trust is the consideration that - the compromised servers cannot generate correct private key of the Key Management Service and to sign certificate, because the compromised servers can generate maximum t partial signatures. But it will be possible only when the other servers in the network know about the compromise of those servers and then they will not co-operate those servers by providing their partial signatures. In our paper we have not discussed about the cryptographic schema used to generate shares of the Key Management Service's private key. Also we have not discussed about the process of combining the partial signatures or the process to generate the private key of Key Management Service by t+1 servers. Besides these, how authorization and access control service will be provided has not been mentioned in this paper. Future research is needed to solve the issues.

References

[1.] Wikipedia the free encyclopedia. Ad hoc. [Online] (Updated 1 March 2010) Available at: http://en.wikipedia.org/wiki/Ad_hoc [Accessed 3 March 2010].

[2.] SearchMobileComputing.com Definitions. ad-hoc network**.** [Online] (Updated 5 Dec 2000) Available at: http://searchmobile computing .techtarget.com/definition/ad-hoc-network [Accessed 3 March 2010].

[3.] Wikipedia the free encyclopedia. Mobile agent. [Online] (Updated 1 March 2010) Available at: http://en.wikipedia.org/wiki/Mobile _agent [Accessed 3 March 2010].

[4.] Lidong Zhou, Zygmunt Haas, 1999. *Securing Ad Hoc Networks.* [Online] Cornell University Ithaca, NY, USA. Available at: http://www.cs.cornell.edu/home/ldzhou/adhoc.pdf [Accessed 2 March 2010].

[5.] Tarig Mohammad Ahmed, 2009. *Using Secure-Image Mechanism to Protect Mobile Agent against malicious Hosts.* [Online] World Academy of Science, Engineering and Technology. Available at: http://www.waset.org/journals/waset/v59/v59-82.pdf [Accessed 2 March 2010].

[6.] Niklas Borselius, *Mobile agent security.* [Online] Information Security Group, Royal Holloway, University of London. Available at: http://www.agent.ai/doc/upload/200402/bors02_1.pdf [Acces sed 1 March 2, 2010].

[7.] Mieso K. Denko and Qusay H. Mahmoud, *Mobile Agents for Clustering and Routing in Mobile Ad Hoc Networks,* In : S. Pieere, M. Barbeau, E. Kranakis, Eds. 2nd International Conference on Ad Hoc Networks and Wireless (ADHOC-NOW'03), 8-10 oct. 2003, Montreal, Canada, Springer, 2003, pp. 271-276.

[8.] ZHANG Yi, ZHU Lina and FENG Li, 2009. *Key Management and Authentication in Ad Hoc Network based on Mobile Agent* [Online] JOURNAL OF NETWORKS, VOL. 4, NO. 6, AUGUST 2009 Available at: http://www.academypublisher com/ ojs/index. php/jnw/article/viewFile/0406487494/817 [Accessed 2 March 2010].

[9.] Dale, J. and DeRoure, D. C. (1997) *A Mobile Agent Architecture for Distributed Information Management*. In: Proceedings of the International Workshop on the Virtual Multicomputer. 1997.

[10.] David Kotz and Robert S. Gray**,** 1999. *Mobile Agents and the Future of the Internet.* [Online] Available at: http://www.cs .dartmouth.edu/~dfk/papers/kotz:future2/ [Accessed 2 March 2010].

[11.] Wayne Jansen, Tom Karygiannis, *NIST Special Publication 800-19 – Mobile Agent Security.* [Online] National Institute of Standards and Technology. Available at: http://csrc.nist.gov/ publications/nistpubs/800-19/sp800-19.pdf [Accessed 1 March 2010].

[12.] The University of Birmingham, 2004. Symmetric-key cryptography. [Online] Available at: http://www.cs.bham.ac. uk/~mdr/ teaching/modules04/security /lectures/symmetric-key.html [Accessed 2 March 2010].

[13.] Sun Microsystems Documentation. Introduction to Public-Key Cryptography. [Online] (Updated 10 September 1998) Available at: http://docs.sun.com/source/816-6154-10/contents.htm [Accesse d 1 March 2010].

[14.] Giovanni Vigna, 1997. *Protecting Mobile Agents through Tracing* [Online] Research Publication Repository of KFUPM (King Fahd University of Petroleum & Minerals) Available at: https://eprints.kfupm.edu.sa/59734/1/59734.pdf [Accessed 2 March 2010].

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

[16.] YANG Ya-tao, ZENG Ping, FANG Yong, CHI Ya-Ping, 2007. *A Feasible Key Management Scheme in Ad hoc Network.* [Online] IEEE. Available at: http://ieeexplore.ieee.org/stamp/stamp.jsp ?arnumber=04287521 [Accessed 6 March 2010].