Computer Standards & Interfaces 35 (2013) 365–373

Contents lists available at SciVerse ScienceDirect

Computer Standards & Interfaces

journal homepage: www.elsevier.com/locate/csi

Artificial immune system based mobile agent platform protection

S. Venkatesan [a,*], R. Baskaran [b], C. Chellappan [b], Anurika Vaish [a], P. Dhavachelvan [c]

[a] Division of MBA (IT) and Cyber Law & Information Security, Indian Institute of Information Technology-Allahabad, India
[b] Department of Computer Science & Engineering, Anna University, Chennai, India
[c] Department of Computer Science, Pondicherry University, Pondicherry, India

ARTICLE INFO

Article history:
Received 4 March 2011
Received in revised form 3 July 2011
Accepted 3 October 2012
Available online 27 October 2012

Keywords:
Software agent
Mobile agent security
Artificial immune system
Mobile agent platform protection

ABSTRACT

An emerging technology for systems to communicate efficiently in the distributed environment is the mobile agent. The features of the mobile agent are too big when compared with the static agent and conventional communication system. However, the security issues of the mobile agent and mobile agent platform lags its usage. Even though the protection models are available for the mobile agent environment, the vulnerabilities still exist or the models need more computational time. To mitigate these issues related with the agent platform, this paper proposed an artificial immune system (AIS) based model. The proposed model will give the separation of duties and clones to handle multiple foreign agents simultaneously to achieve the computational efficiency. The experimental results and the constructed results from the experimental results have proved that this proposed model will consume less computational time when compared with the existing models. It will detect the malicious agent by extracting and matching the patterns with the available malicious patterns and also it can identify the new malicious patterns through monitoring the agent process.

1. Introduction

Software agent is a program which will act on behalf of its owner with features like autonomy, persistency, etc. Generally the agent is divided into two types: static and mobile agents. Static agent will always stay in one place and it will perform the operations for what it has created. Mobile agent is the one which will migrate from one host to another host to perform the operations for its owner. It will minimize the network traffic through minimizing the data transmission. Further, mobile agent is divided into two types to minimize the network traffic more and more. The types of the mobile agent are: single hop mobile agent (which will visit only one remote host and get back to the home) and multi-hop mobile agent (which will visit multiple remote hosts and return to the home with the required result). Because of agent versatility, nowadays static or mobile agent concept is applied in most of the applications like sensor network [7,9,14], network fault detection [22], e-services [28], m-commerce [29], etc. However, the vulnerabilities available in this concept lags it usage. Compared with static agent, mobile agent is more vulnerable. This is the major motivation for us to concentrate on the mobile agent environment protection especially on the agent platform where the agent get executed.

The mobile agent platform is facing a number of issues from foreign agents like denial of service attack (spamming the agent with dummy requests, suspending the agent, sending a signed message with a fake sender ID, etc.) and unauthorized access (shutdown the platform, modifying policy file, killing an agent in the platform, etc.). To protect the agent platform from these kinds of attacks, we are proposing the platform protection mechanism by incorporating the artificial immune system. Apart from our incorporation, artificial immune system have been applied for many models like anomaly detection including intrusion detection [17,20], computer security [6], and misbehavior detection [12,13] because of its efficiencies.

1.1. Basic immune system

The biological immune system generally begins when a pathogen enters the biological structure [27]. The representation of the immune system is shown in Fig. 1. It shows that whenever a pathogen enters the body, the macrophages ingest it, process it and display its antigen fragments on their cell surfaces (if the pathogen comes first time to the body). The macrophage having the antigen on its surfaces is called the Antigen Presenting Cell (APC). After that, APC interacts with a T-helper cell that can recognize the antigen available on the surface. At the time of interaction, the macrophage will release a chemical alarm signal called interleukin-1, which stimulates the T-helper cell to secrete interleukin-2, which then causes the proliferation of certain cytotoxic T cells and B cells [18,26]. The immune response from this point will go in two paths, one through cytotoxic T cells and the other one through B cells.

T cells: Normal cells of the body that become infected will be able to digest some of the pathogens and display antigen fragments on their cell surfaces. The body makes millions of different types of cytotoxic T cells (killer T cells). Each type is able to recognize a particular antigen. The cytotoxic T cells that are capable of recognizing the antigen on the infected cell surfaces bind to the infected cells and produce

* Corresponding author.
E-mail address: venkalt_s@yahoo.co.in (S. Venkatesan).

0920-5489/$ – see front matter © 2012 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.csi.2012.10.003

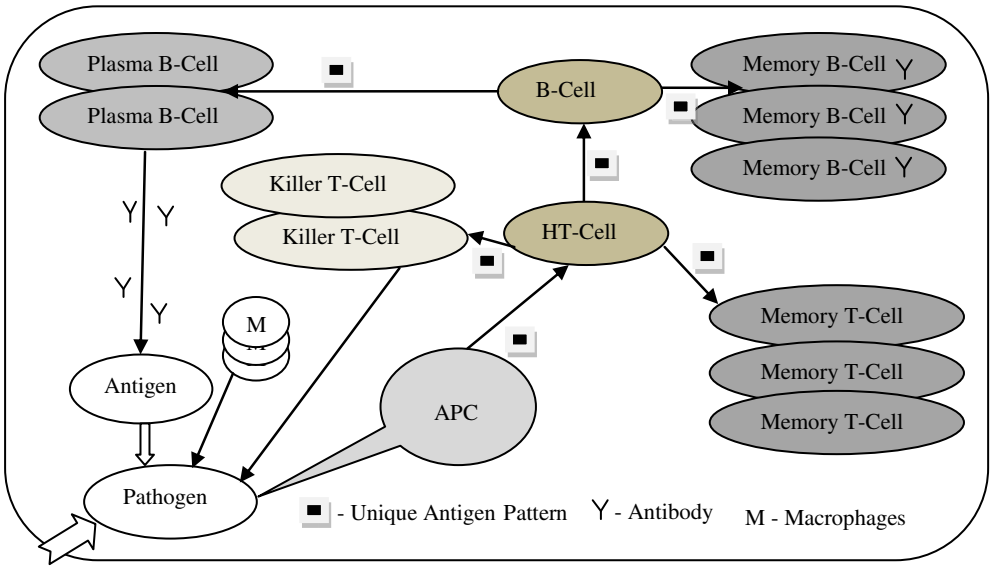

Fig. 1. Biological immune system.

chemicals to kill the infected cell. The death of the infected cells results in killing of the pathogen [27]. The helper T cell also generates the memory T-cell for the respective pathogen to prevent it in future.

B cells: It will also come in millions of different types; each can recognize a particular antigen. Whenever B cells get activated by T-helper cells (HT cell), they differentiate into plasma cells. These plasma cells become antibody producing factories, flooding the bloodstream with antibodies that can bind to the antigen involved in this infection. Antibodies bind to the antigens on the surfaces of the pathogens, marking them for destruction by macrophages. Also some of the B cells do not turn into antibody factories but instead become memory B cells that may survive for several years to prevent the same pathogen in the future. The secondary immune response which will come from the memory B-cell is what gives strong immunity to the same disease after you have had them once or after you have been vaccinated [27]. If the same pathogen enters the body again, the memory B-cell or memory T-cell will directly start the functions to kill the pathogen instead of once again processing the pathogen by the macrophages (APC).

The immune system in our body is working in two scenarios: one is innate immune system (work with our own cell) and the second is adaptive immune system (vaccinated cell). In innate immune system, responses are non-specific, meaning these systems respond to pathogens in a generic way [8]. However, both of them use to follow the same procedure to kill the pathogens.

For agent platform protection, already we had proposed simple and policy based Malicious Identification Police (MIP) model with the Attack Identification Scanner, which will also work moreover the same as the above biological immune system but we did not discuss that perspective, also the separation of duties is not like the immune system and there is also no cloning (proliferation) concept. Now, this paper proposes the model by incorporating biological immune system as artificial immune system to protect the agent platform. The main motivation behind this paper is, these days the agent or mobile agent concept is used everywhere. Even the artificial immune system is applied into many of the environments like robotics [21], sensor network [24], etc. with the help of the mobile agent. Hence protecting the mobile agent platform is most important.

The remaining section of this paper is organized as follows: Section 2 gives a brief description over the related works. Section 3 describes the proposed model to protect the mobile agent platform against the malicious agent by incorporating the artificial immune system. Section 4 discusses about the experimental and constructed result analyses of the proposed model and lastly, Section 5 concludes the paper with future works.

2. Related works

To protect the mobile agent platform from the malicious agents, various techniques are available. However all the techniques are facing certain issues like time complexity, false positive, false negative, etc. This section discusses some of the existing techniques and its issues.

Sandbox [1] technique is introduced to isolate the non-trusted mobile agents. Since the non-trusted agents are isolated it cannot alter or disturb the platform or other agents running in the platform. Access to the resources outside the isolated environment is controlled by the security controller. This is achieved with the help of the static check. It will verify the byte code to check the type correctness, stack overflow or underflow, code containment, registration initialization and object initialization [10]. However the sandbox is having the "all-or-nothing" problem [11].

Joseph and Luis [4] introduced the signing concept to protect the platform. The agents should be digitally signed by the owner of the agent. The signature will be verified at the remote side for authentication. If the signature is authenticated and signature is of the known agent owner then the client will be accepted to access all the resources otherwise the agent will be rejected to enter.

Since, code signing is safe from "all-or-nothing" problem; it has been mixed with the sandbox technique. That is the partially trusted mobile agent will be executed in the restrictive area and allowed to access only the public resources. The mobile agent from the registered user with proper signature will be allowed to execute without any restriction to access the resources.

The major drawback here is that the host which registered with the remote host may change to malicious and sign the agent code to pose

Table 1
Component mapping between IS and AIS based agent platform protection.

Immune system components	Artificial immune system components for agent platform protection
Pathogen	Foreign mobile agent
Antigen	Pattern
APC	Pattern extractor
HT-cell	Malicious detector
Memory cell	Knowledge base
Killer T-cell	Killer agent