

Abstract

Immune system is one of the essential system that is responsible for one's existence . The greatest example of immune system is created by nature itself . Our purpose in this paper is to make study of various aspects of artificial immune system and to converge this study towards computer viruses detection.

Keywords-Fitness, Replication.

Introduction

Nature provides protective measure to each species called the immune system that gives one the capability to defend itself . The foreign elements make attack on the body elements called non self and self respectively .Various essential terms used in immune system:---

1. Antigen---Foreign protein , attacker
2. Antibody---make binding to antigen for their destruction

It is just similar to scenario of computer virus the external element or files contain malicious activities in them like antigen that it is duty of our computer immune system to make detection of that intruder and make removal .It's inspiration can be taken from immune system and a specific activity can be performed as done by antibody for the detection of computer virus and all this is to be done under the framework of artificial immune system.

Step of Immunology in Computer

However natural immune system is very much different from computer immune system but there are various key factors that we can adopt . The concept of clonal theory and negative selection are very effective in term of designing artificial immune system and the system thus designed can be used for providing a solution of classification and detection problem of computer viruses .According to Forrest , these features include[1]---

1. Multilayered protection
2. Distributed detection
3. Diversity across different systems
4. Inexact detection

Forrest in their paper of computer immunology explained the two process that are inspired from natural immunology [1]:---

1. Intrusion detection method
2. Distributable change detection algorithm

The process of antibody generation is very specific and it includes various mutation , The following diagram explains antibody production from gene library.

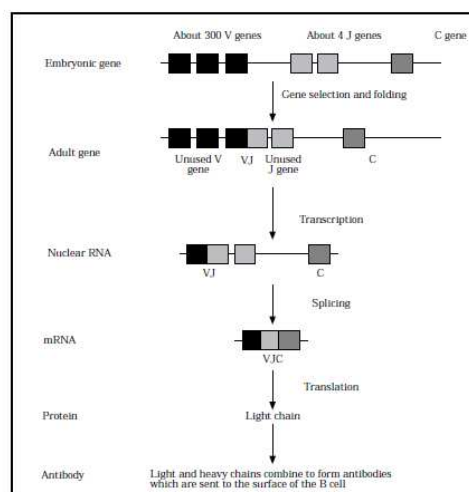


Fig1. Antibody production process from gene library[2]

Another important term that are widely used in immunology and used in jerne's idiotypic network hypothesis are[4]:----

1. Epitope
2. Paratope
3. Idiotope

The process used by natural system involves the antibodies generation , it is very important to know for us the generation of specific antibodies and randomness for which negative selection process is

used .The analysis of antibody antigen binding is crucial for detection . The whole process gives us the working criteria and strength of it's working , we can take several motivation and observational approaches to solve various problems basically we are concerned with computer virology problem.

Dipankar dasgupta in his paper immunity based intrusion detection system : a general framework proposed immunity based intrusion detection system including the concept of [3]:

1. Mobility
2. Adaptivity
3. Collaboration
4. Learning

With this activities of various agents in model is of utmost importance[3]:-----

1. Monitoring agents
2. Communicator agents
3. Action agents
 - o Helper agents
 - o Killer agents
 - o Suppressor agents

Monitoring agents are associated with various behaviour at user level which includes type of user and user privileges , Login\Logout period and location ,Access of resources and directories ,type of software use , key stroke pattern activities secondary system level includes cpu usage , usage of real and virtual memory , amount of free memory , input output and disk usage parameters and Thirdly packet level includes connection status , average number of packets sent and received , duration of the connection , type of connection , protocol and port used parameters. With this process level parameters includes number of process and their type , relationship among processes , time lapsed since the beginning of processes , current state of process , percentage of various process time . Communicator agents works as carrier of messages. Action agents are for making decision activities .Helper agents involves in telling status produced by environment to the end user[3].

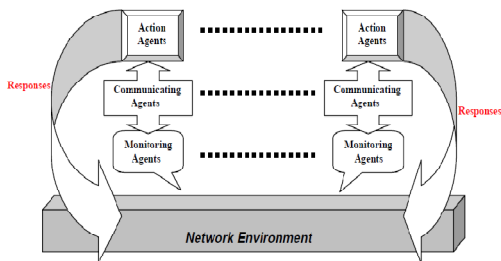


Fig2. View of multi-agent detection system conceptual model[3]

Akio Ishiguro ,Toshiyuki Kondo , Yuji Watanabe , Yasuhiro and Yoshiki Uchikawa in their paper Emergent construction of artificial immune networks for autonomous mobile robots focus on the problems of arbitrary mechanism construction and design of appropriate competence modules .

Authors finally proposed an innovative model to solve the issues of concerned problem .Following diagram explains the whole scenario .

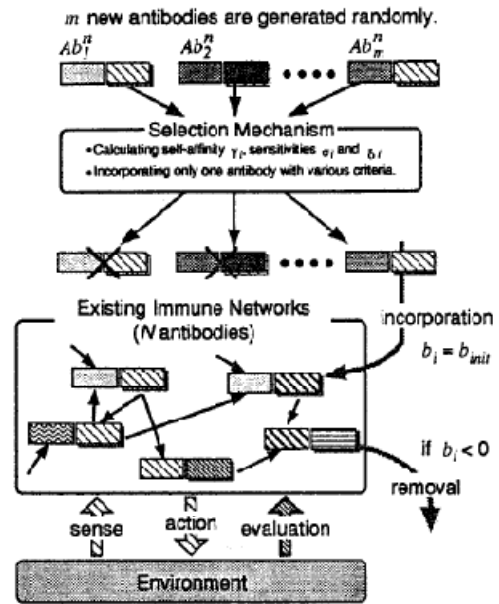


Fig3. Mechanism of immune system[4]

Irrespective to all this in 1995 kephart , in 1997 Forrest , in 2003 Knapp , in 2004 Goel and bush , in 2004 Boudec and sarafijanovic did lot of work in the field of artificial immune system. They explored the concepts of biology of cellular environment and try to implement it in information security. The important issues explored are[5]:----

1. genomics
2. proteomics
3. physiology

Jun Li ,Paul knickerbocker in their paper functional similarities between computer worms and biological pathogens analyse the activities of biological pathogens and try to make conclusion to apply increment in computer immune system against viruses and worms. For making the analysis author take six most fatal diseases and determine the individual and environmental tactics regarding this .

Conclusion

In this paper we discussed various approaches artificial immune system and show how these approaches get used to solve the security issues of

computer world and implementation of certain crucial concept surely can improve the efficiency of computer immune system .With this various proposed models are also discussed to make a analysis of various existing solutions . The whole study will be beneficial for those working in area of immunology and computer virology.

References

- [1] Stephanie Forrest , Steven A. Hofmeyr , Anil Somayaji , “ Computer immunology “ ACM , 1996.
- [2] John E. Hunt and Denise E. Cooke , “ Learning using an artificial immune system “ university of wales .
- [3] Dipankar Dasgupta ,”Immunity –Based intrusion detection system : A GENERAL FRAMEWORK” university of Memphis .
- [4] .Akio Ishiguro , Toshiyuki Kondo ,Yuji Watanabe , Yasuhiro shirai and Yoshiki Uchikawa , “ Emergent construction of artificial immune networks for autonomous mobile robots”.
- [5] Jun Li , Paul Knickerbocker ,”Functional similarities between computer worm and biological pathogens “ university of Oregon.