IMC Applications

Jing Yu
Table of Contents

- Review of Immune System
- A Distributed Architecture for a Self-Adaptive Computer Virus Immune System
- Immunity By Design: An Artificial Immune System
Review of Immune System

- Immune system is a distributed system which deploys a multilevel defense against invaders through non-specific (innate) and specific (acquired) immune mechanisms.
- Two types of lymphocytes: B cells and T cells
A Distributed Architecture for a Self Adaptive Computer Virus Immune System

Gary B. Lamont, Robert E. Marmelstein, and David A. Van Veldhuizen

- Introduction
- Generic CVIS
- A Distributed Architecture for a Self Adaptive CVIS
- Discussion
Introduction

- Problem Domain
- Terms
  - Antigen: virus
  - Virus signature: bit patterns
  - Detecting: matching
The Generic CVIS Algorithm

- Computer Viruses
  - Search/Detect/Match (recognize virus signature)
    - No → Is signature found?
    - Yes → Classify computer virus → Produce cleansing agent → Purge/Repair files (clean)
  - Possible Computer Virus Signatures
    - Known Computer Virus Signatures
      - Virus Signature Database (‘Memory’) → Virus Signature Memory Management/Control
Self/Non-Self Determination Algorithm

Possible Computer Virus Signatures (Random Strings)

Self Strings (Static and Dynamic Files)

Is it a self string?

Possible Virus Signature

Virus String Signature

Dynamic memory updating due to changing self

Add virus string to memory

Compare / Match strings

Delete / Suppress Self String

Known Computer Virus Signatures

Virus Signature Database ('Memory')
Virus Decoy Algorithm

Computer Viruses

Search for anomalies.

Possible Computer Virus Signatures

Search/ Detect/ Match (recognize virus signature)

Known Computer Virus Signatures

Generation of non-self signatures (strings); suppress self-strings

Virus Signature

Decoys capture virus signature(s) samples

Analyze code/data strings for new virus structure(s)

Generate new virus signature(s)

Add virus string to memory

Signature control

Virus Signature Database (‘Memory’)

Is signature found?

Yes

Classify computer virus

Produce cleansing agent

Cleansing Agent

Purge/ Repair files (clean)

No
Towards a distributed and adaptive CVIS

- Concept of IA - intelligent agent
  1) Mobile agent
  2) Three operations: sensing, recognizing and responding
- IAs at three levels:
  local level, network level and global level
Distributed CVIS Architecture

Global Level:
- Resource Adaptation
- Detector Generation
- Resource Warehouse

Network Level:
- Virus Classification
- Alert Generation
- Metrics Reporting

Local Level:
- Vulnerability Analysis
- Virus Detection
- Virus Elimination
- System Repair

Messages:
- Resource Request
- Infected Decoy
- Metrics

Messages:
- Resource
- Virus Alert
- Resource Request
- Infected File
Discussion
Immunity by Design: An Artificial Immune System

Steven A. Hofmeyr and Stephanie Forrest

- Introduction
- AIS
- Discussion
Introduction

- Terms
  1. Self: the set of normal pairwise connections
  2. Non-self:
  3. Detector cell:
  4. T cell?
The Architecture of the AIS
The Lifecycle of a Detector
Conclusion