UDC 004.8: 004.056.57

A.V. SKATKOV, A.A. BRUHOVECKIY, V.S. LOVIAHIN

Sevastopol national technical university, Sevastopol, Ukraine

DEVELOPMENT OF METHODS FOR ADAPTIVE PROTECTION AND COMPUTER SECURITY BASED ON THE THEORY OF ARTIFICIAL IMMUNE SYSTEMS

Immune algorithms are very powerful combinatorial search in a multidimensional space, which base their decision on the basis of sorting multiple options and selecting the best of them. Problem of Artificial Immune Systems using in a computer security area is considered in this article. Comparison of Artificial Immune Systems and Natural Immune Systems are made. Basic analytical model of viral attack in computer system are shown. Basic model and methods of analytical researching of adaptive protection and computer security are purposed in the end of paper.

Keywords: *adaptive protection and security, artificial immune systems, computer systems and networks.*

Introduction

The natural immune system is a complex and adaptive system that defends humans and animals from foreign pathogens. Immune system is able to categorize all cells within the body as self-cells or nonself ones. It does this with the help of a distributed task force that has the intelligence to take action from a local and also a global perspective using its network of chemical messengers for communication.

Nowdays computational intelligence technique, inspired by immunology, has emerged, known as Artificial Immune Systems (AIS) [1].

Several concepts from immunology have been extracted and applied for the solution of real-world science and engineering problems, such as:

- optimization problems,
- security in computer systems and networks,
- recognizing of situatuons in computer systems.

1. Implementation of Artificial Immune Systems in computer security area

Problem: security analysis of access management in computer systems (CS) as a part of the actual theory, named general computer security.

Subject – a CS component initiating an operation execution in CS.

Object – a CS component that has no opportunity to initiate an operation execution in CS.

Axiomatic statements[2]:

1. The problems of the CS security can be described with the help of the process, in which subjects access to objects.

2. All data flows in computer systems are generated by the process, in which subjects access to objects.

The access management system: regulates and delimits resource security; also supports their competent allocation in computer systems on the base of the special rules set.

The access management policy:

- discretionary;
- mandatory;
- role.

Models, describing access rights and realizations of data flows in CS :

- classical Take-Grant model and its basic model extension;
- classical Bell-LaPadula model;
- military systems message model;
- role access control model;
- capability access management model.

Two-dimension data flows:

- by time,
- by memory.

Limitedness of known models:

- static nature (absoluteness of current access graphs);
- conservatism (a priori given access management policy);
- determinism (a set of access types, data flows are determined);
- particular access cases:
  - read,
  - write:
  - append.

Proposal: an approach to access policy management realization on the base of the artificial immune system with adaptation.

2. Comparison of natural and artificial immune systems

NIS	AIS
(Petrov R.V., Marchuk G.I., Burnet, Hood) The multilevel organism protection from the influence of the external antigens (viruses, bacteria).	(S. Forest, Ishida, Shiguro) Goal system function – access management in CS
The basic functional evolutional property: the training processes of external antigens recognition.	AIS organization on the base of adaptive management using complex viral attack model.
Intelligent Functions	
Cell recognition, contained in organism and classification «self»/«not self».	Primary intelligent specific function of a neural net
Further «not self» recognitions for stimulation of protection special type mechanisms.	Secondary intelligent specific function of genetic distribution algorithm
Dynamic elements	
Transposed unit – lymphocytes. Immune-competent cells generation, circulating through the body.	Transposed unit – transact. Transact generation with event-trigger–temporal categories maintenance.
Basic processes	
in lymphatic organs: 1. Generation and cloning of cells 2. Cells differentiation: - effector-cells (antigens killers); - suppressor-cells (supporting insensibility to own antibodies); - non-specific cells (naïve, i.e. untrained).	in simulation model 1. Generation and creation of transacts copies in the given classes 2. Transacts differentiation on the base of their test filtration an training Models of Bush-Mosteller, Hull.
Competence and immune responsibility basis	
Lymphocyte system: structures of two goal- and functional connected sets of elements. 1. First set: T-type cells with function of amplification or suppression reactions of B-type cells 2. Second set: B-type cells with recognition and training functions of effect or activity	Simulation model of immune responsibility • T-type transacts – active element functionally determined in its class, managing B-type transacts • B-type transacts – managed by element with effector-cells function
Macrophages – functionally distinguishable cells of a special type with specific antigenic cells presentation function, and they also attract B и T-type cells for recognition. The auxiliary function: reproduction processes are stimulated by the positive recognition results and lymphocyte differentiation with the following antibody clone generation with immune-competent cells, which are particularly for this antibody.	Special-purposed monitoring subsystem in the AIS composition. Neural network Adaptive management using a sample model
Immune memory	
Data storage supporting in NIS: The structure unit – immune memory (it stores a part of mutant cells) The function: increases the speed of secondary immune reactions in future	Analytical viral attack model with managing initial conditions and feedback on the base of finite-state set model of initial conditions
The function: supporting circulation of B- and T- cells in primary and secondary immune organs, control and maintenance of storing cells	Stationary mode – death viruses conditions.
Localization process	
Overcoming phases of antigenic attacks: - first meeting with antigen (macro-phage) - activation immune-responsible cells - division - immune attack - immune memory - Function: T-cells increase or suppress immune answer on the base of helper or suppressor reactions.	Overcoming phases of access violation: - event identification: access violation - initialization; - active transacts generation of T and B - functional answer on the base of interaction of system simulation models and viral attack model Feedback in modified viral attack

3. Basic model of viral atack

Factor area of the model:

V(t) – viruses concentration;

F(t) – antibodies concentration ;

C(t) – plasmacells concentration (antibodies generator);

m(t) – relative characteristic of the damaged organ (fragment) or the tissue type;

α, β, γ… - model parameters.

First equation of the model (viruses quantity alteration in organism):

– viruses increment because of reproduction;

– coefficient of viruses reproduction;

– viruses increment, neutralized by antibodies;

– coefficient of virus neutralization by antibodies.

Second equation (quantity increase):

- plasmacells generation taking into account the time delay ;

– coefficient , considering probability to the «virus – antibody» meeting, cascade reaction stimulation and the quantity of cells recently appeared;

– describes quantity plasmacells reduction because of their aging;

– coefficient, inversely proportional to plasmacells lifetime.

Third equation (balance of antibodies reacting with antigens):

– antibodies generation by plasmacells for the time space *dt;*

– production rate of antibodies, generating by plasmacell;

– quantity plasmacells reduction cause their connection with viruses;

– coefficient, considering antibodies quantity, needed for neutralization per virus;

– a quantity of antibodies population reduction because of their aging;

– coefficient, inversely proportional to antibodies decay time.

Relative characteristic of target-organ affection or a type of tissue:

– volumetrical healthy organ characteristic;

– volumetrical characteristic of healthy affected organ part.

Forth equation

– degree of organ or a type of tissue affection;

– constant, effected by viral attack type ;

– summand, considering regeneration epoch with constant of proportionality.

The basic mathematical viral attack model:

Fundamental viral attack modal properties

Theorem 1. Existence and uniqueness of the solution:

For non-negative initial values, for all $t \geq 0$ the singular solution of the system exists.

Theorem 2. Non-negativity of the solution:

Non-negativity of initial values involves non-negativity of equation solutions for all $t \geq 0$.

Modifications of the base model:

1. Model with the controlled initial conditions.
2. Non-lineal viral attack model.
3. Non-stationary viral attack model.
4. Discrete event-trigger feedback model.
5. Integrated model.

4. The purpose of AIS models research

The development of flexible, adaptive methods to protect computer systems and determine optimal strategies for protection through the use of theory of artificial immune systems (AIS) [3,4]. The use of AIS due to their high efficiency and ability to adapt to constantly changing conditions. It is being to develop applications in the field of computer security, based on a combination of methods of artificial immune systems in combination with various methods of data mining: fuzzy systems, genetic algorithms, evolutionary computation, clustering of data, decision trees, Bayesian networks naive, factor analysis, problem solving multivariate optimization, etc.

Status of system and data processing are an n-dimensional feature vectors, which is obtained by processing the real IP-traffic.

In turn, the state space formed by the set of vectors V. It includes a feature vector corresponding to all possible states of the system - normal and abnormal. We consider four classes of intrusion: Denial of service - DoS, User to root - U2R, Remote to local - R2L, Probing - Probe.

File format used for training and testing of models is in the public databases of network traffic patterns KDD Cup 1999, University of California, Irvine. An example of a string describing the feature vector of network traffic patterns from the database file:

91, udp, domain u, SF, 87, 45, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0.00, 0.00, 0.00, 0.00, 1.00, 0.00, 0.00, 147, 140, 0.95, 0.01, 0.18, 0.00, 0.00, 0.00, 0.00, 0.00, normal.

The string consists of 42 fields. The first 41 field describe the features of network traffic, the latter, forty-second field indicates the type described by the traffic. The specified field can be set to «normal» or - the type of intrusion (e.g. «ipsweep»).

Intrusion detection model determine the belonging of input feature vector, which contains information about the real IP-traffic, one of the above categories.

To calculate the effectiveness of the model we determine the output parameters: the errors of the first and second kind, the accuracy of detection, false alarm rate and others. Quality evaluation of classification is performed by ROC-curve, which is based on experimental data and displays the ratio of the level of true and false alarms.

The main areas of research in the field of modeling.

Models and methods of data pre-processing:

• normalization of the data;

• clustering of data;

• statistical evaluation.

Models to identify the informative features of network traffic:

• factor analysis;

• the principal components analysis(PCA);

• evaluation model based on the information gain measure;

• construction of decision trees (algorithms ID3, C4.5).

Models of intrusion detection.

1. Models based on negative selection methods:

• Generating a set of detectors, describing the space of the anomalous behavior of the system;

• the model k-nearest neighbor(KNN);

• the model kdd-tree;

• a model based on n-dimensional hyperspheres with variable radius.

2.Adaptive fuzzy models:

• building the fuzzy rules base;

• structural optimization rules;

• parametric optimization of fuzzy membership functions;

• identifying the most informative linguistic variables based on the measurement of entropy;

• ant colony optimization models;

• optimization of the fuzzy rules using genetic algorithms.

3.Naive Bayesian networks models.

4.Support vector machine models.

The developed models are functional completeness, built in a modular, open and are being used to develop applications and tools.

The implementation of applications is a high level language with Visual C #, IDE Microsoft Visual Studio 2010, package Mathlab.

The project includes the following main subsystems:

Management, UI, Planning and conducting experiments, Support the model of AIS, Learning, testing and analysis.

In the area of artificial immune systems with adaptation are developed:

• models of intelligent functions artificial immune system;

• simulation models of immune competence and responsibility;

• a model of immune memory based on a model with controlled viral attack by the initial conditions and feedback;

• structures and models of information object monitoring;

• models of virus attacks: an analytical model of virus attack, an integrated model of a virus attack, steady-state model (the stabilization mode) - the conditions to eliminate viruses in the aftermath of a virus attack;

• models of the basic functionality built-in support for AIS modules: agent control systems, embedded systems diagnostics and management, expert system load analysis, multi-function network monitoring tools of analysis and diagnosis;

• algorithms for adaptive choices of structures and organization of the operation of AIS subsystems;

• software major functional subsystems of AIS: specialized subsystem monitoring and parameter identification, decision support subsystem, the subsystem to adapt to the reference model and the self-tuning.

Architecturally the proposed firmware complex consists of the following subsystems:

• monitoring and parametric identification;

• diagnostics and management;

• immune competence and defence;

• adaptation on the base of a sample model and self-tuning;

• generation and variant assessment;

• interface interaction with the decision-maker.

Conclusion

Immune algorithms are very powerful combinatorial search in a multidimensional space, which base their decision on the basis of sorting multiple options and selecting the best of them. At the same time the immune system provides a balanced strategy for finding a solution that combines local and global search. Therefore, having such important properties as high adaptability and decentralized information processing, AIS effectively used to solve applied computing tasks such as optimization, pattern recognition, data classification, identification systems, safety and security of computer networks and others.

References

1. Искусственные иммунные системы и их применение [Текст]: пер. с англ. / под ред. Д. Дасгупты. – М.: Физматлит, 2006. – 344 с.

2. Skatkov, A.V. The artifical immune system with adaptation [Text] / A.V. Skatkov //Critical infrastructure safety and security (CrlSS-DESSERT'11), First International Workshop. Kirivograd Ukraine May 11-13 2011. – P. 41.

3. Брюховецкий, А.А. Обнаружение вторжений в компьютерных сетях на основе иммунологических принципов [Текст]/ А.А. Брюховецкий, А.В. Скатков // Оптимизация технологических процессов: сб. науч. тр. – Севастополь, 2011. – №14. – С. 198–203.

4. Скатков, А.В. Модель вирусных атак в компьютерных системах с ограниченным доступом, основанных на искусственных иммунных системах [Текст]/ А.В. Скатков, В.С. Ловягин. // Зб. наук. пр. СНУЯЕтаП. – Вып.3 (39). – Севастополь: Изд-во «СНУЯЕтаП», 2011. – С.149-153.

Поступила в редакцию 2.04.2012

Рецензент: д-р техн. наук, профессор, заведующий кафедры «Техническая кибернетика» Л.А. Краснодубец, Севастопольский национальный технический университет, Севастополь, Украина.

РОЗРОБКА МЕТОДІВ АДАПТИВНОГО ЗАХИСТУ ТА КОМП'ЮТЕРНОЇ БЕЗПЕКИ, ЗАСНОВАНИХ НА ТЕОРІЇ ШТУЧНИХ ІМУННИХ СИСТЕМ

О.В. Скатков, О.О. Брюховецкій, В.С. Ловягін

Імунні алгоритми – дуже могутній засіб комбінаторного пошуку в багатовимірному просторі, вони базуються на сортуванні багаторазових відборів і виборі кращих з них. У статті розглядається проблема використання штучних імунних систем в області комп'ютерної безпеки. Проводиться порівняння штучних імунних систем і природних імунних систем. Наводиться базова аналітична модель вірусних атак в комп'ютерних системах. Основні моделі та методи дослідження адаптивного захисту та комп'ютерної безпеки надані наприкінці статті.

Ключові слова: адаптивний захист та безпека, штучні імунні системи, комп'ютерні системи та мережі.

РАЗРАБОТКА МЕТОДОВ АДАПТИВНОЙ ЗАЩИТЫ И КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ, ОСНОВАННЫХ НА ТЕОРИИ ИСКУССТВЕННЫХ ИММУННЫХ СИСТЕМ

А.В. Скатков, А.А. Брюховецкий, В.С. Ловягин

Иммунные алгоритмы – очень мощное средство комбинаторного поиска во многомерном пространстве, они основываются на сортировке многоразовых отборов и выборе лучших из них. В статье рассматривается проблема использования искусственных иммунных систем в области компьютерной безопасности. Производится сравнение искусственных иммунных систем и естественных иммунных систем. Приводится базовая аналитическая модель вирусных атак в компьютерных системах. Основные модели и методы исследования адаптивной защиты и компьютерной безопасности предоставлены в конце статьи.

Ключевые слова: адаптивная защита и безопасность, искусственные иммунные системы, компьютерные системы и сети.

Скатков Александр Владимирович – д-р техн. наук, профессор, заведующий кафедры «Кибернетика и вычислительная техника» Севастопольского национального технического университета, Севастополь, Украина.

Брюховецкий Алексей Алексеевич – канд. техн. наук, доцент, доцент кафедры «Кибернетика и вычислительная техника» Севастопольского национального технического университета, Севастополь, Украина.

Ловягин Вячеслав Сергеевич – аспирант кафедры «Кибернетика и вычислительная техника» Севастопольского национального технического университета, Севастополь, Украина, e-mail: lovyagin88@gmail.com.