Abstract

Objective of this paper is to examine the principles of biological and artificial immune systems and to design a generic scheme of the transport control system.

The authors review the features of artificial immune systems and currently available railway and electric safety devices and evaluate them for use in the railway electric transport control system.

Keywords

Artificial immune systems, railway electric transport, modeling.

Introduction

The global aim of the research is to provide a way for the electric railway transport to avoid dangerous situations.

Artificial immune systems (AIS) were mentioned in some papers in mid 1980s but became a subject in its own right in 1994 in papers on negative selection by Forrest et al. and Kephart et al. Currently the systems are actively explored for possible use cases.

There are many embedded transport control systems on the market which are designed to provide safety for the vehicle, its passengers or cargo, and other traffic participants.

In the railway transport segment an example of such a system is KLUB-U, currently used in Russian Railways. It is installed in the locomotives and by interacting with existing signaling systems and its own modules provides information about the train’s and its closest neighbors’ coordinates, diagnostics of the brakes, current railway segment profile and maximum allowed speed, and controls the vigilance of the locomotive driver. Still, despite the wide array of features, it lacks automation and many decisions require manual operation.

Objective of this paper is to examine the principles of biological and artificial immune systems and to design a generic scheme of the automatic transport safety control system.

Biological immune systems

The immune system (IS) of vertebrates is composed of various molecules, cells and organs spread throughout the body where different elements perform decentralized complementary tasks. The main role of the IS is to protect the organism against disease-causing cells called pathogens and own malfunctioning cells. This is accomplished by searching the organism for such elements, recognition, and immune action. The IS is also able to recognize the organism’s own properly functioning cells to prevent their destruction. All elements recognizable by the IS are called antigens: pathogens, malfunctioning cells and healthy cells. The organism’s native and harmless cells are termed self antigens, while the disease-causing elements are named non-self antigens. The process of distinguishing between them is termed self/non-self discrimination.

In order to be effective in reacting to new pathogens and to improve response to pathogens already encountered, the system needs memory and the ability to learn. The mechanisms of identification, memory, and learning are facilitated through the processes of pattern recognition, clonal selection, negative selection, and affinity maturation.

Pattern recognition is carried out by white blood cells (lymphocytes) of two types: B-cells and T-cells. The other elements in the IS, such as antigen-presenting cells, natural killer cells, message molecules serve various auxiliary functions and are beyond the scope of this paper.

Both B-cells and T-cells have receptors on their surfaces that recognize antigen patterns, detecting different features: B-cells can recognize isolated antigens from outside the antigen cell, while T-cells operate on the antigen-cell complex and can recognize parts of the complex presented by organic molecules (see Fig. 1).

In response to a specific antigen B-cells produce antibodies which are capable of further recognition and binding to that type of antigen. They also directly participate in deactivation of pathogens by tagging them, activating responses of other parts of the IS and neutralizing toxins entering the organism.
T-cells activate B-cells to grow and switch into an antibody-secreting state, and killer T-cells eliminate intracellular pathogens presented by B-cells.

The recognition process is based on matching the shape of an antigen with the one on the surface receptors of B-cells and T-cells, or shape complementarity. The degree of binding is termed affinity – the attraction between an antigen and a receptor cell.

There are two theories that explain how the immune memory works. The traditional explanation is that the most stimulated B-cells remain in the host body transformed to the long living memory cells, thus the information about previous encounters of the given antigen is still present in the immune system. The second is the theory of immune network, where a network composed of interconnected B-cells is proposed, where each B-cell reacts not only to the antigens but also to the presence of other B-cells and also stimulates the other B-cells upon recognizing an antigen.

Artificial immune systems

Immune programming is an evolutionary data processing paradigm based on biological immune systems. It differs from computational immunology which models biological immune systems.

Immune algorithms are mainly used to solve anomaly recognition, data collection and analysis tasks. From the computational point of view immune systems’ most interesting features are self-learning, diversity maintenance and memory.

The problem is represented as an antigen and solution candidates as antibodies which are randomly generated from the library of available solutions or genes. The evaluation of affinity or degree of binding between the antigen an an antibody is similar to complementarity level in biological IS and it defines the fate of each individual antibody as well as termination of the whole algorithm.

Individual antibodies are replaced, cloned and hypermutated until satisfactory level of affinity is reached. Partial replacement of the solutions’ population with fresh randomly generated candidates maintains diversity which allows solving a wider set of problems. The probability of cloning or hypermutating a candidate depends on its affinity.

AIS usage examples

As mentioned before, AIS can be used to solve different data analysis tasks. In the traveling salesman problem each city to be visited could be labeled as an antigen and the set iteratively combined with the antibody network, simulating antigen intrusion in the organism and driving through cities in the random order.

Network intrusion detection is related to unauthorized access to computer systems connected to the network and the problem is solved using anomaly or misuse patterns detection. Anomaly detection systems build a model of normal system activity and then regard deviations from this as potential intrusions, while misuse detection systems look for known attack patterns by signature matching. The key advantage of anomaly detection systems is their ability to detect novel attack patterns for which no signature exists, while their most notable disadvantage is a larger false positive rate. Already being close to the immune approach, by introducing its memory feature such systems could also provide further information about the consequences of the attack and possible future actions instead of simply reporting the actions [7] (see Fig. 3).

Shape-space concept

AIS are modeled after biological IS and carry the terms of antigens and antibodies. They can be modeled using the shape-space concept. The shape-space S allows defining antigens, receptors and their interactions in a quantitative way.

\[
\text{Fig. 1. Pattern recognition in an immune system: (a) B-cell recognizing an isolated antigen; (b) T-cell recognizing an antigen within an antigen-cell complex.}
\]

\[
\text{Fig. 2. A shape-space model of an antigen and an antibody.}
\]
antigen, \( Ag \), and an antibody, \( Ab \), can be defined, for example, using a general class of Minkowski distance measures:

\[
D_M(Ag, Ab) = \left( \sum_{i=1}^{n} |Ag_i - Ab_i|^p \right)^{\frac{1}{p}}
\]

(2).

By varying the value of the parameter \( p \) a suitable measure of distance can be obtained.

**Immune programming adaptation algorithms**

The procedures of adaptation govern the evolution of the behavior of an AIS. The algorithms for adaptation can be classified as population-based and network-based algorithms. Only population-based algorithms are relevant to the development of immune programming. They can be further categorized as clonal selection and negative selection algorithms, corresponding to simulation of B-cell (pattern recognition) and T-cell (anomaly detection) behavior, respectively [4].

**Clonal selection**

1. Generate a population \( P \) of candidate solutions (B-cells).
2. Determine the \( n \) most stimulated individuals.
3. Clone the selected cells. The number of clones is an increasing function of the stimulation level.
4. Submit the clones to a hypermutation scheme.
5. Reselect the improved clones to the population \( P \).
6. Perform the suppression (remove from \( P \) the less stimulated lymphocytes).
7. Add a number of newly generated B-cells (diversity introduction).
8. Repeat from step 2 until the terminating condition is satisfied.

This general framework was applied to several problems, such as optimization or data analysis and clustering. The B-cell representation is an important issue in clonal selection algorithm. In many works, B-cells are represented only as antibodies for simplicity.

**Negative selection**

Negative selection is the paradigm describing the evolution of the T-lymphocytes where they are randomly generated and learn to recognize all except the self structures, specific to the host. Negative selection algorithms need training samples only from one class (self, normal), thus, they are especially suited for the tasks such as novelty, anomaly or change detection including those in engines and other devices.

The algorithm:

1. \( n \) candidate detectors are generated.
2. Each candidate \( C_i \), \( i = 1, 2, ..., n \), is compared to the set of protected, known elements \( PE \).
3. If a match occurs, individual \( C_i \) is discarded.
4. Otherwise the candidate is stored in the detector set \( D \).

This algorithm produces a set of detectors capable to recognize non-self patterns. The action following the recognition varies according to the problem under consideration.

To increase the effectiveness of the AIS it’s recommended to use both adaptation algorithms in conjunction, which is also illustrated by the network intrusion detection system example.

**Fig. 3. Hybrid intrusion detection system (IDS) design.**

In this case the incoming data connections are antigens with such features as the requested port, time, number of attempts, the data itself etc., and the firewall software modules with a database of immune memory is a set of antigens.
AIS usage in transport control system

In the transport control system each vehicle T will possess an additional embedded module M which collects data from the sensors $S_E, S_W$ etc. about the technical state of the engine $E$, wheels $W$ and other critical parts. The incoming data, or antigens, will be presented to the antibody set to recognize dangerous situations and make a decision whether it’s possible to start or continue movement regardless of driver’s actions or traffic lights’ signals (see Fig. 4).

Fig. 4. Generic railway electric transport control system design.

The agents in the system I interact with the immune memory database D and, if necessary, send a signal to stop the engine via the controller.

Analogous to the hybrid IDS the most feasible way to implement such a system would be through the two phases of anomaly detection and determination of their type to draw a conclusion.

In this case the incoming data from the sensors is the set of antigens. The data includes but is not limited to speed, acceleration, voltage, rotation, temperature, and presence of smoke.

Electric engine diagnostics

While the most complete diagnostics can be performed only in the technical service environment, most failures can be detected during its operation using spectral current analysis. It consists of recording data about current and voltage from clamps placed on the electric engine and a special spectral analysis designed to uncover electrical and mechanical damage.

The design of the diagnostic complex could look like presented on Fig. 5.

Fig. 5. Design of the diagnostic complex.

All kinds of damages which could lead to failures have their distinctive harmonic graphs, thus recognizing them in the specter of the current allows early identification of problems in the engine.

Conclusions

- The most relevant features of immune algorithms are self-learning, diversity maintenance, memory about the past decisions and detection of previously unknown but related elements.
- The most feasible way to implement a railway electric transport safety control system would be through the two phases of anomaly detection and determination of their type to draw a conclusion about further action.
- A possible way to diagnose problems in the electric engine is by spectral current analysis.
- The action following the recognition varies according to the problem under consideration.

References