Adaptive Behavior Selection of Autonomous Objects in the Bio-Networking Architecture

Junichi Suzuki (jsuzuki@ics.uci.edu) and Tatsuya Suda (suda@ics.uci.edu)
Department of Information and Computer Science
University of California, Irvine
Irvine, CA 92697-3425

1. Introduction

Future network environment will connect heterogeneous objects and services, and be larger and more complex than the current network environment. A radical shift in network design paradigms is necessary to realize this vision. We believe that making this future a reality requires a network that exhibits self-organization with inherent support for mobility, scalability, adaptability to changes in network conditions, and survivability/availability from massive failures and attacks.

We believe that key features of the future network applications, such as scalability, adaptability, and survivability/availability, have already been realized by various large-scale biological systems. Accordingly, future network applications may be able to achieve these desirable properties by adopting certain key biological principles and mechanisms. In the Bio-Networking Architecture we proposed, key biological principles and mechanisms are applied in the network application design. It is designed to operate on large-scale, highly distributed, heterogeneous and dynamic network environments.

This paper describes a mechanism to support adaptive behavior selection of autonomous objects in the Bio-Networking Architecture. Due to space limitation, please see [1] for details of key biological principles and concepts in the Bio-Networking Architecture.

2. Biological Behaviors of Autonomous Objects

In the Bio-Networking Architecture, a network application is modeled as a decentralized collection of autonomous distributed objects called *cyber-entities*. A cyber-entity provides a functional service related to the application, and performs biological behaviors. Some behaviors are explained below:

- *Energy exchange and storage*. Cyber-entities gain, expend and store energy. They gain energy in exchange for performing a service, and they expend energy to use computing resources such as CPU cycles and memory space on a node that they reside on.
- *Migration.* Cyber-entities migrate from network node to node.
- *Replication and reproduction.* Cyber-entities may make a copy of themselves (replication), possibly with mutation in the replica's behavior. Two parent cyber-entities may produce a child cyber-entity (reproduction), possibly with mutation and crossover in the child's behavior.
- *Death.* Cyber-entities may die because of old age or lack of energy. If energy expenditure of a cyber-entity is not balanced by the energy units it receives from providing services to other cyber-entities, it will not be able to pay for using network resources, i.e., it dies from lack of energy.
- *Relationship establishment.* Cyber-entities have their own relationships with others to discover other cyber-entities, communicate with other cyber-entities, or form a group of cyber-entities to collectively provide an application. A cyber-entity establishes a relationship with another cyber-entity through actively searching for other cyber-entities nearby, through introduction via other cyber-entities, and through discovery-related interactions.
- *Resource sensing*. Cyber-entities sense its local environment. For instance, a cyber-entity may sense which cyber-entities are in the environment and what services they provide. Cyber-entities also sense available network resources (e.g., network topology, communication link bandwidth, CPU processing power, and memory space).

---

[1] M. Wang and T. Suda, "The Bio-Networking Architecture: A Biologically Inspired Approach to the Design of Scalable, Adaptive, and Survivable/Available Network Applications," *Proc. of the 1st IEEE SAINT*, January 2001.

- *Communication*. Cyber-entities may communicate with other cyber-entities for the purposes of, for instance, requesting a service, fulfilling a service, and forwarding discovery messages.

3. Behavior Selection Mechanism of Autonomous Objects

In the Bio-Networking Architecture, behavior selection of each cyber-entity is an important issue. The behavior selection is a process for a cyber-entity to examine the current environment conditions, identify behaviors suitable for the current conditions, and decide which behavior to invoke. Each cyber-entity autonomously adapts themselves to the dynamic environmental changes by performing behaviors suitable for the current environment from a variety of behaviors described above.

In our existing design of behavior selection, each cyber-entity contains functions, or *factors*, that evaluate its environment and return numeric values. For example, a cyber-entity may have factors affecting the replication behavior, such as *stored energy level* and *replication cost*. Each factor is given a certain weight relative to its importance, and a behavior is activated if the total result of its evaluating function (e.g. weighted sum of factor values) exceeds a certain threshold. The mechanism that we propose in this paper provides an alternative for cyber-entities to select their behaviors. It introduces new three features, which are not provided by the exiting mechanism, such as *prioritization of behaviors*, *short-term behavioral adaptation*, and *memory of behavior selection history*.

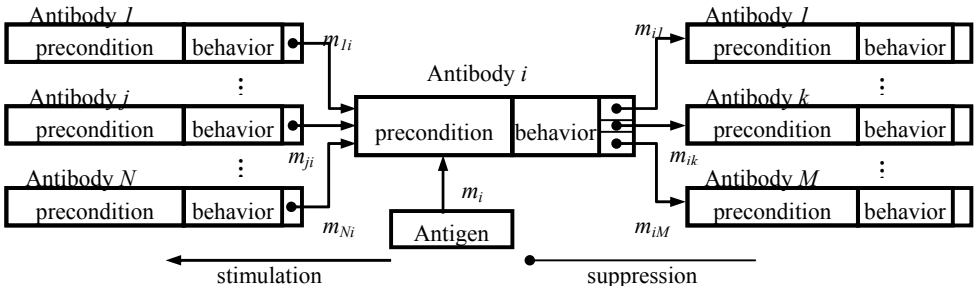
The prioritization of behaviors is used for a cyber-entity to select the most suitable behavior to the current environmental condition. In the existing mechanism, when multiple evaluating functions associated with multiple behaviors are satisfied simultaneously, all of the behaviors are invoked. In the worst case, a cyber-entity may die due to energy starvation after performing the multiple behaviors because energy is required to invoke each behavior. Also, after a cyber-entity performs the first behavior, the second one may not be suitable to invoke because environmental condition should be changed by the first one.

The short-term behavioral adaptation allows cyber-entities to continuously adapt to changing environment. The existing mechanism implements long-term adaptation through evolution. Cyber-entities evolve by generating behavioral diversity among them and executing a natural selection. Behavioral diversity is generated by changing the weight values dynamically through mutation and crossover. Natural selection is executed based on the abundance or scarcity of stored energy. Using the proposed mechanism, cyber-entities can adapt in short-term (i.e. continuously, not limited when creating offspring) as well as in long-term. This can shorten the adaptation speed of cyber-entities.

The memory of behavior selection history makes behavior selection process faster by skipping the behavior prioritization phase. When a behavior is invoked, the information regarding the behavior selection is memorized for future behavior selection. There is no concept of memory in the exiting mechanism.

Our behavior selection engine is designed through applying concepts and mechanisms in the natural immune system. The natural immune system detects environmental changes (e.g. antigen invasion) and responds specifically to the changes (e.g. by producing antibodies specific to them). It also exhibits the above three features. We apply mechanisms of how the natural immune system chooses a specific immune response to an environmental change.

In our behavior selection engine, an environment condition and a behavior are modeled as an antigen and an antibody, respectively. Each behavior (i.e. antibody) has its own concentration value. It corresponds to the number of a specific type of antibody that exists in the immune system (a behavior corresponds to a specific type of antibody.). Concentration value is used as priority in behavior selection. Behaviors (antibodies) are linked with each other using stimulation and suppression relationships. When an environment changes (i.e. when an antigen invades to the immune system), our behavior selection engine (i.e. the immune system) identifies candidate behaviors (antibodies) suitable for the current environment condition, prioritizes them based on their concentrations, and then selects the most suited behavior (antibody) from the candidate behaviors. When our engine prioritizes behaviors (antibodies), stimulation relationship between behaviors contributes to increase the concentration value, and suppression relationship contributes to decrease it. Each relationship has its own strength. The relationship strength indicates the degree of stimulation or suppression.



The above figure shows a generalized network view of antibodies. Each cyber-entity has a network of antibodies. An antibody consists of (1) a precondition under which behavior is invoked, (2) description of behavior, and (3) relationships with other antibodies. Each antigen represents an environmental condition (e.g. request load, local resource cost, etc.). In the above figure, the *i*-th antibody stimulates *M* antibodies and suppresses *N* antibodies. In order to prioritize behaviors (antibodies), the concentration value of each behavior (antibody) is calculated by using the following equation.

$$\frac{dA_i(t)}{dt} = \left(\frac{1}{N} \sum_{j=1}^{N} m_{ji} \cdot a_j(t) - \frac{1}{M} \sum_{k=1}^{M} m_{ik} \cdot a_k(t) + m_i - k \right) a_i(t)$$

A_i(t) denotes the current concentration value of antibody *i*. In the above equation, the first and second term of the right hand side denote the stimulation and suppression from other antibodies. m_{ji} denotes the strength of a relationship between antibody *j* and *i*. m_i is an affinity between an antigen and antibody *i*. The affinity indicates the degree of stimulation from an antigen to an antibody. *k* denotes the dissipation factor representing the antibody's natural death. Our behavior selection engine chooses an antibody (behavior) based on the calculated concentration values. If no antibody exceeds a threshold during certain calculation steps, the antibody of the highest concentration is selected, i.e. winner-tales-all strategy. If an antibody's concentration exceeds the threshold, an antibody is selected based on the probability proportional to the current concentrations, i.e. roulette-wheel strategy.

After a cyber-entity invokes a behavior, our behavior selection engine will evaluate the effectiveness of the behavior in terms of the cyber-entity's fitness (i.e. the degree of adaptation) to environment. Then, relationship strength values are modified based on the effectiveness. If a cyber-entity selects a behavior that increases its fitness, the strength of relationships connected with the behavior will be increased. Otherwise, it will be decreased. The relahionsip topology changes dynamically. When the strength of a relationship becomes 0, the relationship is removed. When it becomes positive value, a relationship is established. This reinforcement learning over relationship strength allows cyber-entities to adjust relationship topology so that they can choose more suitable behavior in near future. In other words, it allows cyber-entities to adapt themselves to dynamic environmental changes continuously (i.e. in short-term).

If a cyber-entity invokes a behavior that increases its fitness, oru behavior selection engine memorizes (i.e. caches) the pairs of the behavior and environment condition. This memorized information is used for future behavior selection: when the future environment matches memorized condition, a corresponding memorized behavior will be invoked. This makes behavior selection process faster because the behavior selection engine can skip the behavior prioritization phase (i.e. the phase of calculating concentration values of all the behaviors). Memorized information is deleted when

Through preliminary simulations in relatievly small-scale network environment, we have confirmed that our behavior selection engine selects reasonable behaviors under a set of environmental conditions (we used 20 antibodies, 42 relationships among antibodies, and 7 antigens for these simulation runs.). We will expand the scale of simulated network environment. We will also conduct extensive sumulations to examine how reinforcement learning over relationships among behaviors increase adaptability of cyber-entities with simulation results and how memory capability affects behavior selection process.