Intrusion Detection in Circular Frustrated Systems: An Eminently Parallel Processing Algorithm (POSTER)

Patricia Mostardinha and Fernão Vistulo de Abreu

Departamento de Física, Universidade de Aveiro,
Campus de Santiago, 3810-193 Aveiro, Portugal
{pmostardinha,fva}@ua.pt

Abstract. The cellular frustration framework (CFF) is a new approach capable of performing single intrusion detections in large populations of very diverse agents[1]. A classical approach in the literature consists in defining a set of detectors where each one surveys a sub-domain of the space of patterns that characterize non-self agents. The intrusion detection task is computationally demanding because it requires matching every new agent against all possible detectors. Also the set of detectors has to be carefully selected to avoid false positive and false negative detections. In these approaches the outcome of detection events depends only on the two agents that interact and is essentially a serial processing computation.

Cellular frustration uses a different conceptual approach to solve intrusion detection tasks. First it is assumed that any agent can interact and potentially react with any other agent in the system. However, instead of instantaneous reactions, agents perform time lasting decisions, during which they interact with other agents and can change pair to optimize their previous choices. Reactions, (i.e. the triggering of detection events) only take place if agents form stable interactions that last longer than a characteristic time. False positive detections, which lead to elimination of self agents, can thus be avoided in populations that are organized in a highly frustrated dynamics where all agents never establish sufficiently long interactions. Furthermore, the population should be maximally frustrated so that intruders will always produce more stable interactions that are used to signal detection events.

In this presentation we discuss this general framework. In particular we discuss how it is possible to organize a large population (e.g. with 1000 different agents) so that any intruder will always be detected because it will always perform longer interactions than self agents. We also show that even if an intruder copies exactly another self agent, then it cannot spread in the population, as its outgrowth would change the dynamical interactions and lower its frustration. This corresponds to a form of homeostatic response.

As detection events in the CFF are triggered as a result of an emergent property of the dynamical system, intrusion detection becomes a whole system property that requires an inherently parallel processed computation.

Reference

[1] de Abreu, F.V., Mostardinha, P.: Maximal frustration as an immunological principle. Journal of the Royal Society Interface 6, 321–334 (2009)

C.S. Calude et al. (Eds.): UC 2009, LNCS 5715, p. 290, 2009.