Abstract

Security of information is of utmost importance to any organization or individual, which depend on computer system or internet for business transaction or source of information or research. Many viruses are able to recognize certain anti-virus software, and respond differently to such software than to programs designed for other purposes. Some viruses go after the databases stored by anti-virus products. Some viruses simply go after anti-virus products, trying to erase them. Immune systems also face this daunting control challenge. On the one hand, they need to minimize damage from pathogens, without wasting energy and resources, but on the other must avoid initiating or perpetuating autoimmune responses.

Several preventive measures including identification and authentication, logic access control, audit trails, digital signature and firewalls have been developed for the purpose of information security on system. As a result of inadequacies of these measures intrusion detection was introduced to complement these techniques and hence guarantee full protection of computing resources. Detection system is the process of identifying and detecting unauthorized access or
abnormal incursions, actions and events in the system, which provides information for timely counter measures.

This paper presents a systematic approach to intrusion detection using artificial immune system (Dendritic Cell) to purging in order to avoid attack subversion and autoimmunity on network. In nature, dendritic cells function as natural anomaly detection agents, instructing the immune system to respond if stress or damage is detected. Dendritic cells are a crucial cell in the detection and combination of ‘signals’ which provide the immune system with a sense of context. The Dendritic Cell Algorithm which is based on an abstract model of dendritic cell behaviour, with the abstraction process performed in close collaboration with immunologists will be used. This algorithm consists of components based on the key properties of dendritic cell behaviour, which involves data fusion and correlation components. In this algorithm, four categories of input signal are used.

The DCA algorithm will be validated with a standard machine learning dataset. The validation of the Dendritic Cell Algorithm is performed. This is assessed through the algorithm’s application to the detection of intrusion and classification problems.

References


Index Terms

Computer Science

Algorithms

Keywords

Dendritic Cell Algorithm (DCA), Security, Auto–immune, K–means, Algorithms