World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:12, No:04, 2018

Off-Policy Q-learning Technique for Intrusion Response in Network Security

Authors : Zheni S. Stefanova, Kandethody M. Ramachandran

Abstract : With the increasing dependency on our computer devices, we face the necessity of adequate, efficient and effective mechanisms, for protecting our network. There are two main problems that Intrusion Detection Systems (IDS) attempt to solve. 1) To detect the attack, by analyzing the incoming traffic and inspect the network (intrusion detection). 2) To produce a prompt response when the attack occurs (intrusion prevention). It is critical creating an Intrusion detection model that will detect a breach in the system on time and also challenging making it provide an automatic and with an acceptable delay response at every single stage of the monitoring process. We cannot afford to adopt security measures with a high exploiting computational power, and we are not able to accept a mechanism that will react with a delay. In this paper, we will propose an intrusion response mechanism that is based on artificial intelligence, and more precisely, reinforcement learning techniques (RLT). The RLT will help us to create a decision agent, who will control the process of interacting with the undetermined environment. The goal is to find an optimal policy, which will represent the intrusion response, therefore, to solve the Reinforcement learning problem, using a Q-learning approach. Our agent will produce an optimal immediate response, in the process of evaluating the network traffic.This Q-learning approach will establish the balance between exploration and exploitation and provide a unique, self-learning and strategic artificial intelligence response mechanism for IDS.

Keywords : cyber security, intrusion prevention, optimal policy, Q-learning
Conference Title : ICCSCPS 2018 : International Conference on Cyber Security of Cyber Physical Systems
Conference Location : Boston, United States
Conference Dates : April 23-24, 2018

Open Science Index, Computer and Information Engineering Vol:12, No:04, 2018 publications.waset.org/abstracts/88356.pdf