Technical Roadmap - Part II

Part II of your term project does not require running any experiments but rather focuses on conceptual and foundational aspects of a popular and well established machine learning paradigm, called **Reinforcement Learning.** This methodology is widely used for anomaly detection, in general, and *cybersecurity intrusion detection*, in particular. Completing this part will require undertaking research using online and/or print media sources. There is a wealth of information available and your group may gather information from any source available to you as long as all text used is marked and the source is properly quoted.

Your group is expected to write a **technical essay** on the basic principles of reinforcement learning (what it is and how it works) and its application as an *online machine learning method* for intrusion detection. You may use one or more examples. The essay should describe the key aspects of reinforcement learning clearly and concisely **in your own words** in not more that 2,000 words (4 pages single spaced text). The essay is considered part of your term project report and the oral presentation with Q&A. Concepts you need to describe include the agent, states, rewards, the learning process and how to model an objective environment in terms of a *Markov Decision Process*.

To help you getting started, please read the below article "Anomaly Detection through Reinforcement Learning" by Hari Koduvely, published online on January 19, 2018. In addition to textbooks offering more technical descriptions[1], there are plenty of online sources readily available.

Anomaly Detection through Reinforcement Learning

"As Artificial Intelligence is becoming a mainstream and easily available commercial technology, both organizations and criminals are trying to take full advantage of it. In particular, there are predictions by cyber security experts that going forward, the world will witness many AI-powered cyber attacks[1]. This mandates the development of more sophisticated cyber defense systems using autonomous agents which are capable of generating and executing effective policies against such attacks, without human feedback in the loop.

In this series of blog posts, we plan to write about such next generation cyber defense systems. One effective approach of detecting many types of cyber threats is to treat it as an anomaly detection problem and use machine learning or signature-based approaches to build detection systems. Anomaly Detection Systems (ADS) are also used as the core engines powering authentication and fraud detection platforms, for applications such as continuous authentication which Zighra provides through its SensifyID platform.

[1] For example, the textbook: John D. Kelleher et al. "Fundamentals of Machine Learning for Predictive Data Analytics", MIT Press, 2020.

Anomaly Detection using Machine Learning

Anomaly Detection Systems (ADS) are designed to find patterns in a dataset that do not conform to expected normal behavior. Most of the anomaly detection problems can be formulated as a typical classification task in machine learning, where a dataset containing labelled instances of normal behavior (also of abnormal behavior if data is available) is used for training a supervised or semi-supervised machine learning models such as neural networks or support vector machines[2]. Though unsupervised learning also could be used for anomaly detection, they are shown to perform very poorly compared to supervised or semi-supervised learning[3].

Since in domains such as cyber defence, the attack scenarios change continuously due to constant evolution by the attackers to avoid detection systems, it is important to have a continuous learning system for anomaly detection. This could be achieved in principle using online learning where a continuous supervised signal (whether the past predictions were correct or not) is fed back into the system and the model is continuously trained with more weights given to recent data to incorporate concept shifts in the dataset.

However, there are many anomaly detection problems where a straightforward online learning is either not feasible or not good enough to provide highly accurate predictions. In such scenarios, one could formulate the anomaly detection problem as a reinforcement learning problem[4,5], where an autonomous agent interacts with the environment and takes actions (such as allowing or denying access) and gets rewards from the environment (positive rewards for correct predictions of anomaly and negative rewards for wrong predictions) and over a period of time learns to predict anomalies with a high level of accuracy. Reinforcement learning brings the full power of Artificial Intelligence to anomaly detection.

In this blog, we will describe how reinforcement learning could be used for anomaly detection giving an example of network intrusion through Bot attacks. To begin with, let us see how a reinforcement learning problem can be described in a mathematical framework called Markov Decision Process or MDP.

Reinforcement Learning in Nutshell

…" (see source or attached copy for full text)

Source: https://zighra.com/blogs/anomaly-detection-through-reinforcement-learning/

Thank you for your cooperation!