World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:13, No:01, 2019

Machine Learning Invariants to Detect Anomalies in Secure Water Treatment

Authors : Jonathan Heng, Yoong Cheah Huei

Abstract : A strategic model that does not trigger any false alarms to detect anomalies in Secure Water Treatment (SWaT) test bed is presented. This model uses machine learning invariants formulated from streamlining the general form of Auto-Regressive models with eXogenous input. A creative generalized CUSUM algorithm to integrate the invariants and the detection strategy technique is successfully developed and tested in the SWaT Programmable Logic Controllers (PLCs). Three steps to fine-tune parameters, b and τ in the generalized algorithm are stated and an example used to demonstrate the tuning process is discussed. This approach can swiftly and effectively detect various scopes of cyber-attacks such as multiple points single stage and multiple points multiple stages in SWaT. This technique can be applied in water treatment plants and other cyber physical systems like power and gas plants too.

Keywords : machine learning invariants, generalized CUSUM algorithm with invariants and detection strategy, scope of cyber attacks, strategic model, tuning parameters
Conference Title : ICMLCS 2019 : International Conference on Machine Learning and Communications Systems
Conference Location : Tokyo, Japan
Conference Dates : January 07-08, 2019