IEEE Nigeria 4th International Conference on Disruptive Technologies for Sustainable Development (NIGERCON), Lagos, Nigeria, 5-7 April 2022

Supervised learning based intrusion detection for SCADA systems

Alimi, OA; Ouahada, K; Abu Mahfouz, Adnan MI; Rimer, S and Alimi, KOA

Abstract:
Supervisory control and data acquisition (SCADA) systems play pivotal role in the operation of modern critical infrastructures (CIs). Technological advancements, innovations, economic trends, etc. have continued to improve SCADA systems effectiveness and overall CIs' throughput. However, the trends have also continued to expose SCADA systems to security menaces. Intrusions and attacks on SCADA systems can cause service disruptions, equipment damage or/and even fatalities. The use of conventional intrusion detection models have shown trends of ineffectiveness due to the complexity and sophistication of modern day SCADA attacks and intrusions. Also, SCADA characteristics and requirement necessitate exceptional security considerations with regards to intrusive events' mitigations. This paper explores the viability of supervised learning algorithms in detecting intrusions specific to SCADA systems and their communication protocols. Specifically, we examine four supervised learning algorithms: Random Forest, Naïve Bayes, J48 Decision Tree and Sequential Minimal OptimizationSupport Vector Machines (SMO-SVM) for evaluating SCADA datasets. Two SCADA datasets were used for evaluating the performances of our approach. To improve the classification performances, feature selection using principal component analysis was used to preprocess the datasets. Using prominent classification metrics, the SVM-SMO presented the best overall results with regards to the two datasets. In summary, results showed that supervised learning algorithms were able to classify intrusions targeted against SCADA systems with satisfactory performances.