World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:11, No:03, 2017

Machine Learning Approach for Anomaly Detection in the Simulated Iec-60870-5-104 Traffic

Authors : Stepan Grebeniuk, Ersi Hodo, Henri Ruotsalainen, Paul Tavolato

Abstract : Substation security plays an important role in the power delivery system. During the past years, there has been an increase in number of attacks on automation networks of the substations. In spite of that, there hasn’t been enough focus dedicated to the protection of such networks. Aiming to design a specialized anomaly detection system based on machine learning, in this paper we will discuss the IEC 60870-5-104 protocol that is used for communication between substation and control station and focus on the simulation of the substation traffic. Firstly, we will simulate the communication between substation slave and server. Secondly, we will compare the system's normal behavior and its behavior under the attack, in order to extract the right features which will be needed for building an anomaly detection system. Lastly, based on the features we will suggest the anomaly detection system for the asynchronous protocol IEC 60870-5-104.

Keywords : Anomaly detection, IEC-60870-5-104, Machine learning, Man-in-the-Middle attacks, Substation security
Conference Title : ICSCICS 2017 : International Conference on Cyber Security for Industrial Control Systems
Conference Location : Madrid, Spain
Conference Dates : March 26-27, 2017