

The 47th Annual Conference of the IEEE Industrial Electronics Society (IECON), Toronto, Canada, 13-16 October 2021

A machine learning approach to intrusion detection in water distribution systems – A review

Ignituous V. Mboweni

Department of Electrical Engineering, University of Cape Town, Cape Town, South Africa

mbwign002@myuct.ac.za

Adnan M. Abu-Mahfouz

Council for Scientific and Industrial, Research (CSIR), Pretoria, South Africa

a.abumahfouz@ieee.org

Daniel T. Ramotsoela

Department of Electrical Engineering, University of Cape Town, Cape Town, South Africa

daniel.ramotsoela@uct.ac.za

<https://ieeexplore.ieee.org/document/9589237>

Abstract

The confidentiality, integrity and availability of critical infrastructure is crucial for any economy to operate efficiently. Water distribution critical infrastructure is a target of many attackers who aim to penetrate the system for malicious reasons. The use of cyber-physical systems (CPSs) in Water Distribution Systems unveils many vulnerabilities that attackers can use. Although preventative security mechanisms are put into place they too can be defeated, and in this case, a second layer of security is essential. Intrusion detection mechanisms are important reactive security mechanisms to limit the damage done by a successful attack in the system. In this paper machine learning (ML) techniques for anomaly detection (AD) are reviewed.