Human-centric Computing and Information Sciences, vol. 9(13): 1-22

Attack detection in water distribution systems using machine learning

Free fulltext link: https://rdcu.be/bRWGz

Ramotsoela, DT
Hancke, GP
Abu-Mahfouz, Adnan MI

ABSTRACT:

The threat to critical water system infrastructure has increased in recent years as is evident from the increasing number of reported attacks against these systems. Preventative security mechanisms are often not enough to keep attackers out so a second layer of security in the form of intrusion detection is paramount in order to limit the damage of successful attacks. In this paper several traditional anomaly detection techniques are evaluated in the context of attack detection in water distribution systems. These algorithms were centrally trained on the entire feature space and compared to multi-stage detection techniques that were designed to isolate both local and global anomalies. A novel ensemble technique that combines density-based and parametric algorithms was also developed and tested in the application environment. The traditional techniques had comparable results to the multi-stage systems and when used in conjunction with a local anomaly detector the performances of these algorithms were greatly improved. The developed ensemble technique also had promising results outperforming the density-based techniques and having comparable results to the parametric algorithms.