Qeios

Peer Review

Review of: "On Process Awareness in Detecting Multi-stage Cyberattacks in Smart Grids"

K. Shanti Swarup[1]

1. Electrical Engineering, Indian Institute of Technology, Madras, India

The paper addresses an important issue of process awareness in detecting multi-stage cyberattacks in smart grids. Machine learning methods for intrusion detection systems (IDS) were used in the work.

Fig. 1 and Fig. 3 are good, where multi-stage cyberattacks on a CIGRE-based power network are considered in this paper.

Why is there a need to consider multi-state cyber attacks (MSCA)? Initially, the work should focus on individual cyberattacks sequentially and then move to simultaneous attacks. This will be more logical.

The paper addresses only IDS, which is only partly possible. Attack mitigation should also be considered, which would make the paper complete in all aspects.

More information on process awareness is to be provided.

Situational awareness for smart power grids is more widely used and appropriate.

How is process awareness different from situational awareness, and how does it outperform it?

Corresponding to Fig. 1, four anomalies (user behavior, communication, network topology, process data) are listed. Which one of the four is considered in this work?

Sec. IV on investigation should be dealt with in detail.

It is not clear how Figs. 5 to 8 are obtained.

The work appears to be mostly theoretical and conceptual, with well-known information provided in Tables I and II.

The conclusions need to be rewritten to bring out quantitative information.

doi.org/10.32388/PoRD51

Detailed simulation results of the system under study are to be provided.

Declarations

Potential competing interests: No potential competing interests to declare.