26 NOVEMBER 2020

30th CIGRE Greece National Conference "e-Session 2020"
Transmission & Distribution Challenges in Greece

CYBERSECURITY ANALYSIS IN ENERGY CONTROL CENTERS

V. Boutlas
DTU

C. Stamatakis
NTUA

G. Korres
NTUA[1]

N. Manousakis
UNIWA

ABSTRACT

Over the last few years the electric energy industry is undergoing profound changes, due to the liberalization of electric energy market and the rapid evolution of digital technologies. In this environment, the secure operation of power systems requires close monitoring of their operating conditions, through the state estimator, in energy control centers. Until recently, the conventional real-time measurement systems included measurements of active and reactive power flows and injections, as well as bus voltage magnitudes, provided by the supervisory control and data acquisition (SCADA) system. With the emergence of the global positioning system (GPS), the measurement set was augmented by synchronized phasor measurements, which are acquired by measuring devices called phasor measurement units (PMUs), providing very high sampling rate and accuracy, as well as time-stamping based on GPS.

The integration of new computing and communication technologies in power systems, introduces new threats to their security, which can be deliberate or the result of an error caused by malicious organizations, such as terrorist groups or competing governments. The target of these cyber attacks may be to damage, steal, alter, or destroy specified information by hacking into a susceptible communication system. Besides the physical impacts these malicious attacks may provoke, they can also cause significant economic losses. One of the possible consequences of these cyber attacks, is the malfunction of the state estimation algorithm, by inserting false data which could mislead the control center to take wrong decisions. From the attacker's point of view, achieving access requires partial or complete knowledge of the system's configuration as well as the in depth understanding of the state estimation and bad data detection methods. The attacker must also have the capability to break into the support infrastructure and the configuration of authentication system. The analysis of a power system cyber security against such attacks is a key factor for its smooth operation and protection. In this work we analyze the different types of single or multiple attacks, the ways they affect the state estimation operation, as well as the necessary procedures that have to be performed by the control center, in order to encounter them. Also, the definition of the term "stealthy attack" will be introduced, in combination with an optimization algorithm. Numerical simulations are conducted in MATLAB environment using the IEEE 14-bus test system.

[1] e-mail: gkorres@cs.ntua.gr