TOPIC: A Novel Approach for Identification of Cyber Physical Data Attack in Power Systems using Spy Node

AREA	Cyber Security, SCADA system, Power System
SPEAKER	Khaled Alotaibi, PhD students, ACIT Center, North Carolina A&T State University
DATE	17 Jun 2015, Wednesday
TIME	11:00 PM to 12:00 PM
VENUE	ACIT Center, Room 342, Fort IRC Bldg., North Carolina A&T State University, 1601 East Market Street, Greensboro, NC 27411
FEES	No Charge

SYNOPSIS

Electrical power is needed for both domestic and industrial activities. The need to make power systems reliable cannot be over emphasized. Different sensors are therefore needed to measure the system's parameters. Most often, the measuring site is separated from the systems monitoring/control center site. Therefore, data needs to be transmitted from the measuring center to the control center for analysis. To test whether this data has not been contaminated, many techniques have been used in literature to determine whether the measured data is significantly different from the estimated values. A cyber physical data attacker in power infrastructure could introduce contamination in the system measurement when he/she break into the network and access the data used in the electric power network. By utilizing the system information a hacker will play a role that could result in an interruption in the power flow. This is the main reason researchers in the power system field are recently increasing their focus on this issue. Malicious data caused by a cyber-physical data attack or failure in hardware performance is the main cause of system unreliability. When malicious data injected is not identified and does not trigger the alarm immediately, the reliability level of the system will become extremely risky, especially when it is maliciously created by adversary. In this work, we introduce the spy node to identify malicious data (contamination) in power system measurements. To identify the contaminated data, our approach intends to change the information of the system being exploited by the adversary through adding virtual buses to the network referred as spy nodes. These nodes, considered as extra measurements along with the actual network measurements are the kind of data that the attacker may access, and are able to change the perceived topology of the network. Candidate locations of the spy nodes are determined by using spanning tree algorithm. Considering the spy nodes as well as the actual nodes in power flow calculations leads to extra measurements in data set. The contaminated data after executing smart attack scenarios based on the data set and the perceived configuration of the system is sent to the Supervisory Control and Data Acquisition (SCADA). The SCADA removes the spy data from the measurements set using the proposed criteria and compares the norm of the remaining measurements with the clean data set. This practical procedure gives different norms for the data set before and after attack and detects the malicious data and identifies whether the data of the system is manipulated or not. It assumes the power system having a virtual bus referred to as spy node leading to spy data. This data is free from error and can be used as another method to detect cyber smart attack. The results are verified by simulating IEEE 9-bus standard system.

ABOUT THE SPEAKER

Khaled Alotaibi, received his bachelor in Computer Engineering from King Abdulaziz University Jeddah, Saudi Arabia and his MSc in Computer Science from North Carolina A&T State University. He is a PhD student in electrical and computer engineering at North Carolina A&T State University. His interest areas are Cyber Physical Data Attack, Graph theory, SCADA protection, data mining, and state estimation.