2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering

Power-Grid Controller Anomaly Detection with Enhanced Temporal Deep Learning

Zecheng He
Princeton University
Princeton, NJ
zechengh@princeton.edu

Aswin Raghavan
SRI International
Princeton, NJ
aswin.raghavan@sri.com

Guangyuan Hu
Princeton University
Princeton, NJ
gh9@princeton.edu

Sek Chai
SRI International
Princeton, NJ
sek.chai@sri.com

Ruby Lee
Princeton University
Princeton, NJ
rblee@princeton.edu

***Abstract*—Controllers of security-critical cyber-physical systems, like the power grid, are a very important class of computer systems. Attacks against the control code of a power-grid system, especially zero-day attacks, can be catastrophic. Earlier detection of the anomalies can prevent further damage. However, detecting zero-day attacks is extremely challenging because they have no known code and have unknown behavior. Furthermore, if data collected from the controller is transferred to a server through networks for analysis and detection of anomalous behavior, this**

loophole of secure communication in the power-grid system, but did not protect controllers and cannot detect new attacks.

Besides the physical sensors and network, protecting the control code running on the industrial programmable logic controllers (PLCs) is an essential and fundamental task in protecting the power-grid systems. No matter how the adversary spreads the malware or bad programs through system vulnerabilities, his ultimate goal is taking control of the power-