Secure Air-Gapped Radio Monitoring of Power Systems (#7932)

A system to securely monitor power grids for detecting sophisticated cyberattacks using lightning-authenticated radio frequency measurements

Georgia Tech inventors developed an air-gapped distributed intrusion detection system (ADIDS) for power system substations, where the entire SCADA system is considered untrusted. For clarification, an air-gapped system is one that is isolated from unsecured networks and is not in any way connected directly to the internet or any other system. The proposed solution is to utilize a radio receiver as a diagnostic tool to provide air-gapped, independent, and verifiable information about the radio emissions from substation components, particularly at low frequencies. At least four types of diagnostic information can be extracted from radio emissions of power system substation components. ADIDS consists of two independent algorithms; the local method, which can use all of the four diagnostics, and the remote method, which can only utilize one diagnostic tool. The nature of the encoding is infeasible to synthesize the resulting signal, making this process a one-way function. This property greatly reduces the possibility that data can be falsified, and the overall security for power grids and components increases greatly.

Benefits/Advantages

- **Safer** – provides an extra layer of security via a remotely monitored power grid diagnostic
- **Power outage prevention** – the impulsive signal can be detected non-invasively
- **Transformer protection** – detect and prevent widespread damages by monitoring the transformer current

Potential Commercial Applications

- Power grids/ Power Systems
  - Securely monitoring substation components (e.g., circuit breakers and transformers)
    - Securely monitoring power lines- checking for possible power theft
- Transformers
- Circuit breakers
- Electric Train System
  - Monitoring system of electric trains for possible cyber attacks
- Any system that used in outdoor areas and generates electromagnetic signals
Background/Context for This Invention

The power grid, as a critical cyber-physical system, is continuously being transformed into the “Smart Grid,” with the goal to monitor and track diagnostic and operational information for a more flexible and resilient system. However, the number of power outages due to cyberattacks has recently increased dramatically. There has been a significant effort in the research community, ultimately contributing to the industrial control system market of $13B, to develop effective intrusion detection systems (IDSs) to reliably detect malicious activities in power systems. However, all of these techniques require some level of trust from components on the supervisory control and data acquisition (SCADA) network; hence, they are still vulnerable to sophisticated attacks that target the SCADA system itself.

Dr. Raheem A. Beyah
Professor - Motorola Foundation Professor - Georgia Tech School of Electrical and Computer Engineering

Dr. Morris B. Cohen
Associate Professor - Georgia Tech School of Electrical and Computer Engineering

Dr. Lukas Graber
Assistant Professor and Director of Plasma and Dielectrics Laboratory – Georgia Tech School of Electrical and Computer Engineering

Christian Bayens
Research Engineer - Georgia Tech School of Electrical and Computer Engineering

Tohid Shekari
PhD Student – Georgia Tech School of Electrical and Computer Engineering

RFDIDS: Radio Frequency-based Distributed Intrusion Detection System for the Power Grid

Signals from Distant Lightning Could Help Secure Electric Substations, 2/26/2019
Georgia Tech researchers Tohid Shekari, Raheem Beyah, Morris Cohen, and Lukas Graber hold an antenna and home-built recording equipment for the very low frequency (VLF) radio receiver, which is capable of detecting lightning radio bursts from around the world. (Image: Christopher Moore, Georgia Tech)

For more information about this technology, please visit: https://industry.gatech.edu/technology/secure-air-gapped-radio-monitoring-power-systems