**GOALS**

- To prevent attackers from accessing a utility's control network by tampering with its remotely deployed embedded devices.
- To determine whether a tamper signal sent from a device is malicious, is benign (i.e., a technician is servicing the device), or represents an emergency situation, such as a natural disaster.
- To use data from sensors attached to an embedded device, as well as signals from similar devices nearby, to decide whether a tamper signal coming from the device is legitimate or a false positive.

**BACKGROUND**

- Utilities collect and monitor data from a number of devices, such as reclosers, that are distributed across their service area. These devices are often mounted on utility poles in both remote and densely populated areas, and have physical security beyond the cabinet in which they are placed.
- These devices require a connection to the utility’s SCADA network. If attackers were to defeat the physical security of the cabinet, they would have direct access to this network.
- The goal for a utility is to shut down access to the control network if one of their devices reports that it has been compromised. However:
  - The utility must also allow for “legitimate” tampering, such as when a technician is sent to service a device.
  - The utility also wants to leave the connection open in the event of a natural disaster, to simplify and expedite recovery efforts.

**RELATED TECHNIQUES**

Prior efforts in distributed sensing did not solve the problem, because:
- They do not consider the device’s physical environment in their risk assessment.
- They do not consider user preferences for certain events.
- They are focused only on detecting events rather than responding to them. Those that do respond are limited to a single course of action.
- The attack detection models used are not powerful enough to look for the event indicators with which we are concerned.

**OUR PROPOSAL: T.E.D.D.I.**

We propose a distributed approach to tamper detection, consisting of three components:

- **Tamper Information Points (TIPs)** live inside a utility’s cabinets, use their sensors to monitor the cabinet for possible intrusions, and send tamper signals upstream when they see an abnormal reading.
- Their sensors can be placed both on the cyber side (function probes, network monitors, etc.) and on the physical side (accelerometers, voltage monitors, etc.).
- **Tamper Decision Points (TDPs)** reside in a high-security area of the network, collect information from the TIPs within the network, and send tamper-event detection decisions to the TEPs in the network.

**RESEARCH PLAN AND CHALLENGES**

Our tool will include:
- A method for adding probability values to augment an incomplete data set.
- A sequence specifier that will search for sequences of indicators that correspond to known attacks.
- A probability estimator that will let operators see how small changes in their numbers affect the entire system.

**WE NEED YOUR HELP!**

If your organization collects incident data on events affecting remotely deployed devices, or you are just generally interested in this project, we want to talk to you!

**WORKS CITED**