Tamper Event Detection Using Distributed SCADA Hardware

Overview and Problem Statement

Utilities collect and monitor data from a number of devices, such as recloser controls, that are distributed across their service areas. The devices are often mounted on utility poles in both remote and densely populated areas, and have little physical security other than the cabinets in which they are placed. However, the devices require a connection to the utility's SCADA network, which means that an attacker could gain access to the network and begin injecting traffic just by defeating the physical security of the cabinet.

While a utility would like to detect tampering with one of its devices, several issues complicate this goal:

- The utility requires its devices—and therefore its tamper detection equipment—to operate in extreme environments without generating false positives.
- The utility must also allow for "legitimate" tamper events, such as servicing by a technician.
- The utility may also want to leave the connection open in the event of a natural disaster, to simplify and expedite recovery effects.

Prior efforts in distributed sensing and tamper detection/physical security do not solve the problem, because:

- They **do not consider the device's physical environment** in their risk assessments, or **cannot operate in all of the environments** that power devices live in.
- They **do not consider user preferences** with respect to certain event types.
- 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 we are concerned about.

Research Objectives

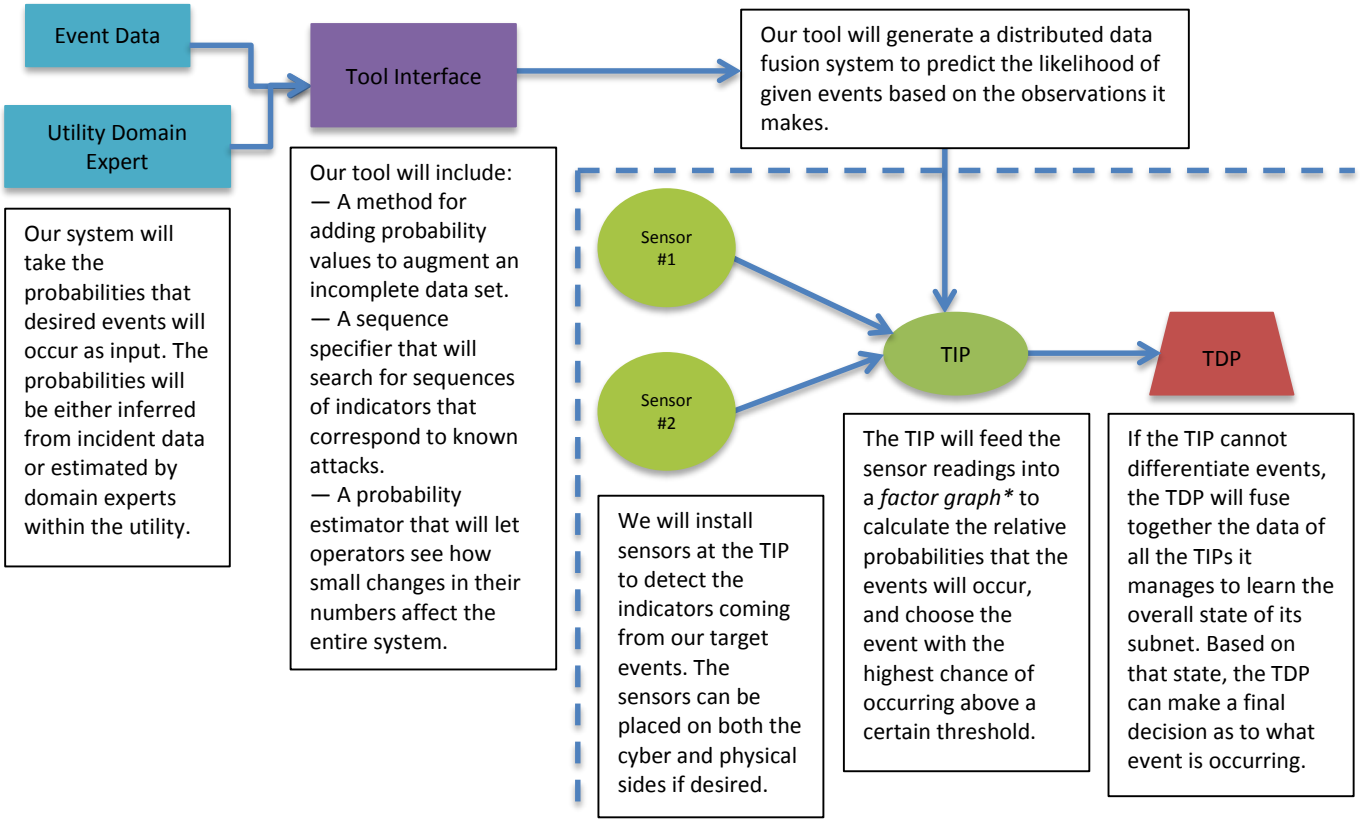
- To prevent attackers from accessing a utility's control network by tampering with its remotely deployed embedded devices.
- To determine whether a tamper signal sent from a device is malicious, is benign (e.g., a technician is servicing the device), or represents an emergency situation, such as a natural 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.
- **Smart Grid Application Area:** Electricity distribution systems, specifically the embedded devices that are spread throughout a utility's service area.

Technical Description and Solution Approach

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

- **Tamper Information Points (TIPs)**, which 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.
- **Tamper Enforcement Points (TEPs)**, which act on tamper decisions that are made. For example, the TEP could destroy secret data on a device.
- **Tamper Decision Points (TDPs)**, which reside in a higher-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.

Our plan is to build a tool that utility operators can use to build customized tamper detection systems for their specific networks.



Project Status

- We are currently constructing a prototype TIP/TDP setup for a sample power network. We can evaluate the system for speed and accuracy, and use it to inform our tool design.
- This problem was first proposed to us by Schweitzer Engineering Laboratories, and we are continuing to work with them as we develop our product.

Researchers

- Jason Reeves, reeves@cs.dartmouth.edu
- Sean Smith, sws@cs.dartmouth.edu

Industry Collaborators

- Schweitzer Engineering Laboratories
- IBM
- Aruba Networks

* See "Extending Factor Graphs so as to Unify Directed and Undirected Graphical Models" by Brendan Frey (*Proceedings of the Nineteenth Conference on Uncertainty in Artificial Intelligence*, 2003).

funded by the U.S. Department of Energy and the U.S. Department of Homeland Security