TCIPG

Tamper Event Detection Using Distributed Infrastructure (T.E.D.D.I.)

Jason Reeves and Sean W. Smith

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 little 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.

Image from http://www.gwelec.com/images/products/sel-651r_control.jpg

- 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 effects.

RELATED TECHNIQUES

Prior efforts in distributed sensing did not solve the problem, because:

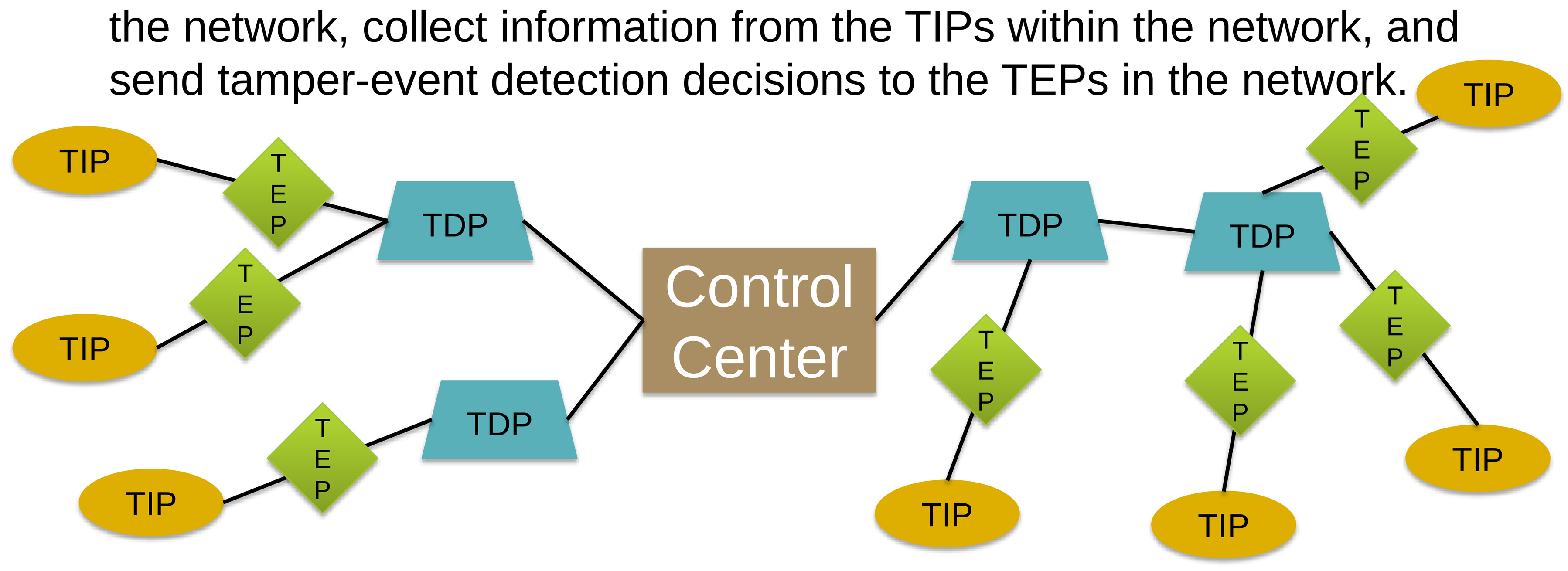
- They **do not consider the device's physical environment** in their risk assessment.
- They **do not consider user preferences** for certain events.
- They are focused only on **detecting** events rather than **responding** to them. Those that do respond are limited to a single course of action.
-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

Work	External Env. Status?	Responds to Events?	Includes User Preferences?	Data Fusion Approach
PQS [3]	No	No	Indirectly	Bayesian
Probabilistic Event Correlation [5]	No	No	Indirectly	Bayesian
SCPSE [8]	No	No	Indirectly	Attack Graph + HMM
SCADAHawk [4]	No	No	No	"Snapshots"
Evidence-Based Trust Assessment [6]	No	No	Yes	Bayesian
Amilyzer [1]	No	No	No	"Flow Matching"

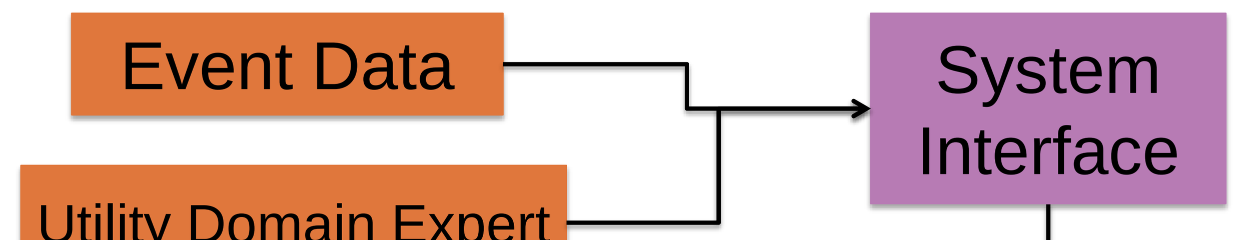
OUR PROPOSAL: T.E.D.D.I.

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



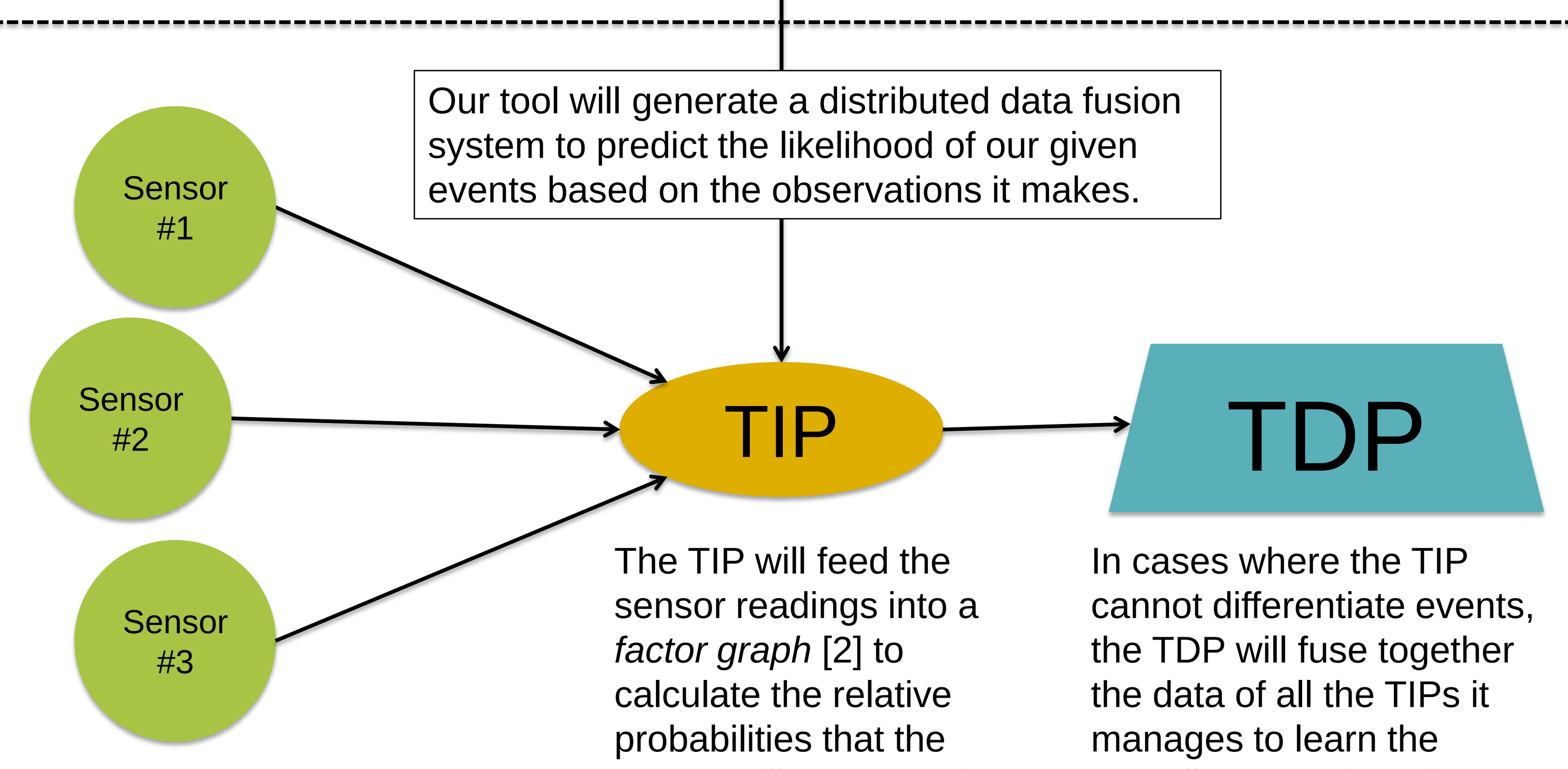
RESEARCH PLAN AND CHALLENGES



Our system will take as input the probabilities that desired events will occur. The probabilities will be either inferred from incident data or estimated by domain experts within the utility.

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 will install sensors at the TIP to detect the indicators coming from our target events. These sensors can be placed both on the cyber side (function probes, network monitors, etc.) and on the physical side (accelerometers, voltage monitors, etc.).

The TIP will feed the sensor readings into a *factor graph* [2] to calculate the relative probabilities that the events will occur, and choose the event with the highest chance of occurring above a certain threshold.

In cases where the TIP cannot differentiate events, the TDP will fuse together the data of all the TIPs it manages to learn the overall state of its subnet. Based on that state, the TDP can make a final decision as to what event is occurring.

If the TDP cannot come to a conclusion based on the sensor data, it will pass the decision up to a higher-level TDP that can make a more informed decision.

RESEARCH QUESTIONS

- This system requires a lot of data from utilities to function properly. What kinds of data are being tracked by utilities? What other kinds of data could feasibly be collected?
- How can we ease the data-gathering burden on utilities? Can we put together a library of known events and probabilities for use?
- How do we calculate the utility of a response? Which of the responses in our set should be applied? In what order should they be applied?
- Can we serve as a data source for a larger system, such as CPTL [7]?

ACTION PLAN

- Construct a prototype TIP and TDP, and use them to inform our automated TIP/TDP system.
- Construct our event prediction tool, and evaluate its sensitivity to probability changes in any of the nodes.
- Investigate the idea of using TEPs to calculate an optimal response strategy based on the TDP's decision.
- Implement our system inside the TCIPG testbed, and evaluate both its speed and accuracy in detecting various events.
- Run a user study with utility personnel to see if they can use our system to predict and respond to events, and collect feedback to see how our tool can be improved.

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

1. Robin Berthier and William H. Sanders. "Monitoring Advanced Metering Infrastructures with Amilyzer." In *Proceedings of C&ESAR: The Computer & Electronics Security Applications Rendez-vous (C&ESAR)*, 2013.
2. Brendan Frey. "Extending Factor Graphs so as to Unify Directed and Undirected Graphical Models." In *Proceedings of the 19th Conference on Uncertainty in Artificial Intelligence*, 2003.
3. Christopher Roblee, Vincent Berk, and George Cybenko. "Large-Scale Autonomic Server Monitoring Using Process Query Systems." In *Proceedings of the IEEE International Conference on Autonomic Computing*, 2005.
4. William Sousan, Qiuming Zhu, Robin Gandhi, and William Mahoney. "Smart Grid Tamper Detection Using Learned Event Patterns." In Vijay Pappu, Marco Carvalho, and Panos Pardalos, editors, *Optimization and Security Challenges in Smart Power Grids*, Energy Systems, pp. 99-115. Springer: Berlin Heidelberg, 2013.
5. Alfonso Valdes and Keith Skinner. "Probabilistic Alert Correlation." In *Recent Advances in Intrusion Detection*, 2001.
6. Yujue Wang and Carl Hauser. "An Evidence-Based Trust Assessment Framework for Critical Infrastructure Decision Making." In *5th Annual IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection*, 2011.
7. Gabriel A. Weaver, Carmen Cheh, Edmond J. Rogers, William H. Sanders, and Dennis Gammel. "Toward A Cyber-Physical Topology Language: Applications to NERC CIP Audit." In *ACM Workshop on Smart Energy Grid Security (SEGS '13)*, 2013.
8. Saman Zonouz, Katherine M. Rogers, Robin Berthier, Rakesh B. Bobba, William H. Sanders, and Thomas J. Overbye. "SCPSE: Security-Oriented Cyber-Physical State Estimation for Power Grid Critical Infrastructures." In *IEEE Transactions on Smart Grid*, vol. 3, no. 4, pp. 1790-1799, 2012.

TRUSTWORTHY CYBER INFRASTRUCTURE FOR THE POWER GRID | TCIPG.ORG
UNIVERSITY OF ILLINOIS | DARTMOUTH COLLEGE | UC DAVIS | WASHINGTON STATE UNIVERSITY
FUNDING SUPPORT PROVIDED BY DOE-OE AND DHS S&T