Understanding Resilience of Large-Scale and Long-Lived Energy Delivery Infrastructure

TEDDI: Tamper Event Detection on Distributed Infrastructure

Jason Reeves, Christopher Frangieh, and Sean W. Smith

GOALS

- To prevent attackers from accessing a utility's control network by tampering with its remotely deployed embedded devices.
- To build a fast, accurate, easy-to-use tamper protection system that can defend a utility's network effectively while minimizing false positives.

THE PROBLEM

- As part of the smart grid rollout, utilities are installing a large number of low-powered embedded devices at the very edges of their networks (for example, smart meters). These devices pose a security risk for utilities, as they are easy to find and access, have little physical security, and may have a connection directly to a utility's SCADA network. Thus, an attacker could use these devices to attack higher-value targets on the network.

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

- Grid defenders want to keep attackers from accessing their networks, but they are hindered by *the grid defender's dilemma.*

Clipart from Microsoft Corporation.

WHAT IS THE GRID DEFENDER'S DILEMMA?

- At its core, the dilemma is the tension between network *security* and network *availability*, and how they are prioritized. Unlike traditional IT networks, the power grid prioritizes availability, which introduces several challenges for grid operators:
  - Rather than lump all events together under the label of "tampering," operators must now identify exactly what event is currently affecting the grid. That means being aware of "benign" events, such as technician visits or natural disasters.
  - Once an event is identified, operators need the ability to execute the proper response, as the cost of choosing the wrong response could be substantial.
  - Finally, operators have limited time and resources, and thus need to be able to easily use and configure any system they install.
- To solve this dilemma, grid defenders need an easy-to-use tool that requires minimal prior knowledge about important events, but also has the power and flexibility to differentiate between events and choose an appropriate response for each one.

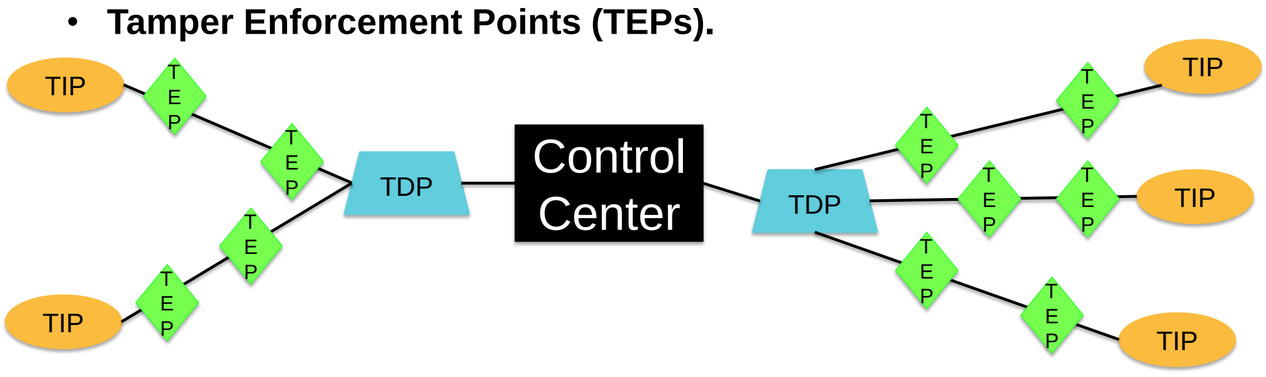
RELATED WORK

- While a large corpus of tamper protection work exists, current tamper/intrusion solutions suffer from several flaws that make them sub-optimal for grid networks.

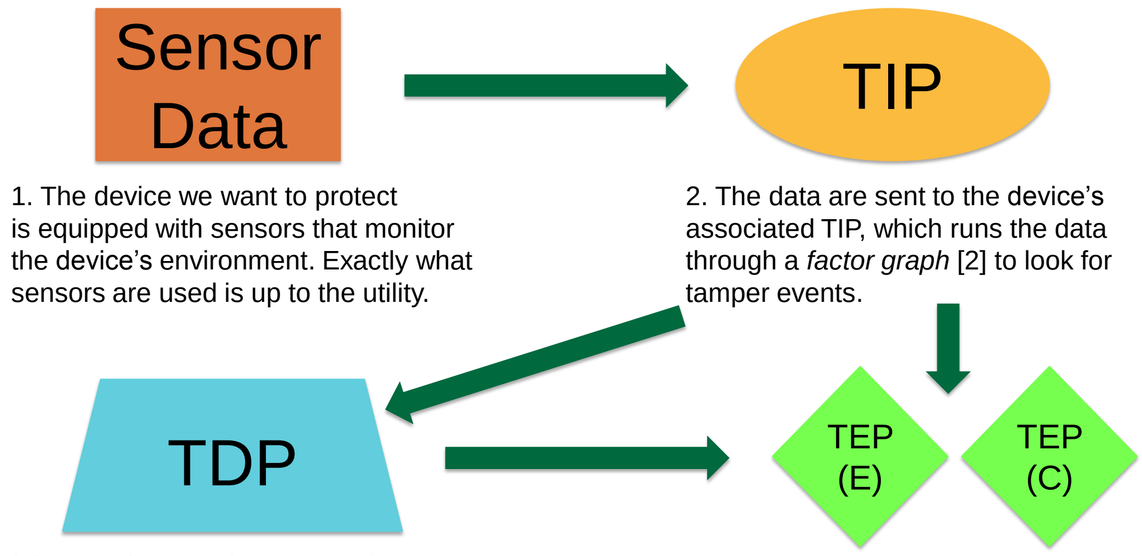
Tamper/Intrusion Protection Solution	Detects Physical Tampering?	Able to Detect Distributed Events?	Multiple Responses?	Long/Complex Setup?
IBM 4758 [5]	Yes	No	No	No
RRE [10]	No	Yes	Yes	Yes
SCADAHawk [6]	No	Yes	No	Yes
PQS [4]	No	No	No	Yes
PAC [7]	No	Yes	No	Yes
Amilyzer [1]	No	No	No	Yes
Evidence-Based Trust Assessment [8]	No	No	No	Yes

OUR PROPOSAL: TEDDI [3]

- We propose a *distributed* approach to tamper detection, consisting of three components:
  - **Tamper Information Points (TIPs)**.
  - **Tamper Decision Points (TDPs)**.
  - **Tamper Enforcement Points (TEPs).**



HOW TEDDI WORKS



1. The device we want to protect is equipped with sensors that monitor the device's environment. Exactly what sensors are used is up to the utility.

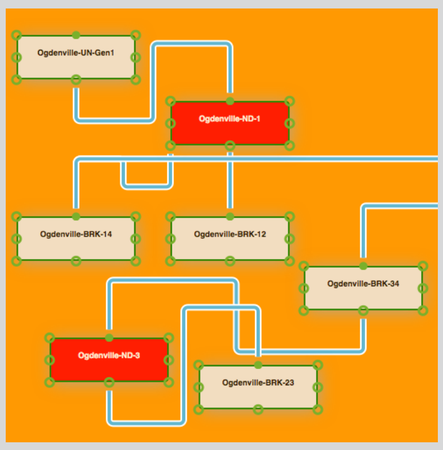
2. The data are sent to the device's associated TIP, which runs the data through a *factor graph* [2] to look for tamper events.

3. If the TIP does not have enough information to make a decision, it sends a request to its associated TDP, which uses data from all of the TIPs it manages to make an authoritative decision.

4. Once either the TIP or TDP detects that an event is occurring, the decision is sent to the appropriate *edge* (E) and *central* (C) enforcement points, which coordinate and execute the proper response.

NEW! THE TEDDI GENERATION TOOL

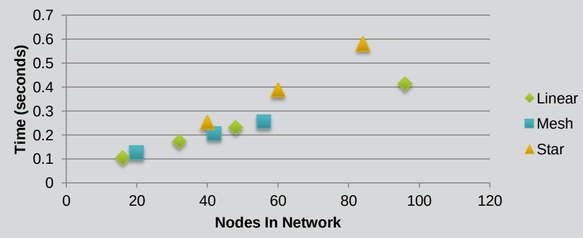
- We built the *TEDDI Generation Tool* to generate the TIP, TDP, and TEPs needed for an arbitrary SCADA network. The tool simplifies the configuration process, and contains:
  - A *Response Suggestion Engine*, to help the user decide how best to respond to tamper decisions.
  - A *Network Topology Uploader*, to allow users to define the network they want to protect using CPTL [9].
  - A *TDP Placement Tool*, to assist the user in determining the optimal locations to place decision points.



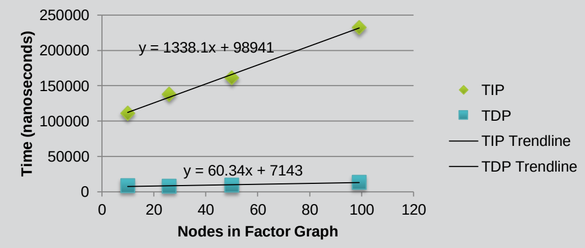
NEW! RESULTS

- **Accuracy results:**
  - We fuzz-tested the TIP by feeding it rounds of random sensor data. **The TIP made the correct event decision in 99 of 100 rounds.**
  - We connected 11 TIPs to a single TDP, and fuzz-tested the TIPs such that they continuously asked the TDP to calculate the regional tamper state. **Across over 50 rounds of testing, the TDP properly calculated the regional tamper state every time it was asked.**
- **Performance results:**
  - We tested the generation tool to see how long it would take to calculate the optimum TDP placements on various networks with between 16 and 96 nodes. **On average, the tool calculated the optimal TDP layout in under .6 seconds for every network** (Graph 1)**.**
    - We also tested the tool using a 441-node graph based partially on the EM network at Dartmouth. **The tool calculated the best TDP placement strategy in under 2.85 seconds.**
- We calculated the average time to process 10, 26, 50, and 99-node factor graphs on both TIPs (Raspberry Pis) and TDPs (standard servers). **The TIP took less than 235 microseconds (on average) to go through the 99-node graph and make a decision, while the TDP did so in under 15 microseconds** (Graph 2)**.**

Graph 1: TDP Placement Tool Processing Time



Graph 2: Factor Graph Processing Time



WORKS CITED

1. Robin Berthier and William Sanders. "Monitoring Advanced Metering Infrastructures with Amilyzer." In *Cybersecurity of SCADA and Industrial Control Systems (C&ESAR)*, 2013.
2. Brendan Frey. "Extending Factor Graphs so as to Unify Directed and Undirected Graphical Models." In *Proceedings of the Nineteenth Conference on Uncertainty in Artificial Intelligence*, 2003.
3. J. Reeves and S. W. Smith. "Solving the Grid Defender's Dilemma: Tamper Protection for Distrubuted Cyber-Physical Systems." In *The 12th International Conference on Security and Cryptography (SECRYPT 2015)*, July 2015. URL: http://www.cs.dartmouth.edu/~reeves/secrypt2015paper.pdf
4. 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.
5. Sean W. Smith, Elaine Palmer, and Steve Weingart. "Using a High-Performance, Programmable Secure Coprocessor." In *Second International Conference on Financial Cryptography*, 1998.
6. 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.
7. Alfonso Valdes and Keith Skinner. "Probabilistic Alert Correlation." In *Recent Advances in Intrusion Detection*, 2001.
8. Yujue Wang and Carl Hauser. "An Evidence-Based Trust Assessment Framework for Critical Infrastructure Decision Making." In *Fifth Annual IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection*, 2011.
9. Gabriel Weaver, Carmen Cheh, Edmond Rogers, William Sanders, and Dennis Gammel. "Towards a Cyber-Physical Topology Language: Applications to NERC CIP Audit." In *The ACM Workshop on Smart Energy Grid Security (SEGS '13)*, 2013.
10. Saman Zonouz, Himanshu Khurana, William Sanders, and Timothy Yardley. "RRE: A Game-Theoretic Intrusion Response and Recovery Engine." *IEEE Transactions on Parallel and Distributed Systems*, 25(2):395–406, 2014.

CYBER RESILIENT ENERGY DELIVERY CONSORTIUM | CRED-C.ORG

FUNDING SUPPORT PROVIDED BY THE DEPARTMENT OF ENERGY, OFFICE OF ELECTRICITY DELIVERY & ENERGY RELIABILITY