TCIPG

Specification-based IDS for Smart Meters

Amilyzer: IDS Sensor for AMI

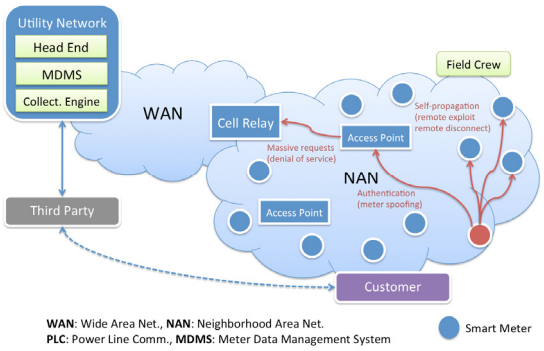
R. Berthier, A. Fawaz, E. Rogers, and W. H. Sanders

GOALS

- Design an efficient monitoring architecture to detect and potentially prevent intrusions targeting or originating from an advanced metering infrastructure (AMI).
- Implement a prototype of this monitoring solution and validate its accuracy and applicability.

FUNDAMENTAL QUESTIONS/CHALLENGES

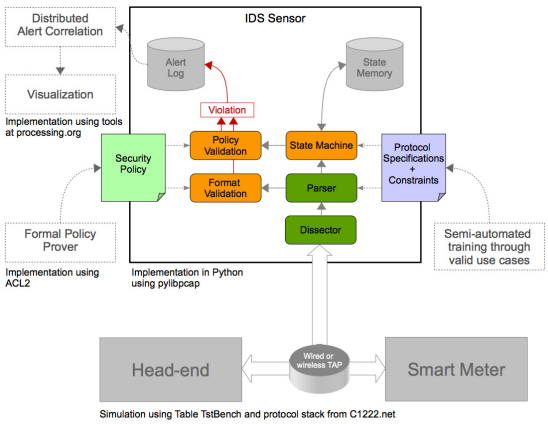
- What are the threats targeting an AMI?
- What detection technology should be developed to cover these threats?
- What monitoring architecture should be deployed?
- How should we automatically respond to security compromises?
- How should we provide large-scale situational awareness?



WAN: Wide Area Net., **NAN**: Neighborhood Area Net.
PLC: Power Line Comm., **MDMS**: Meter Data Management System

RESEARCH PLAN

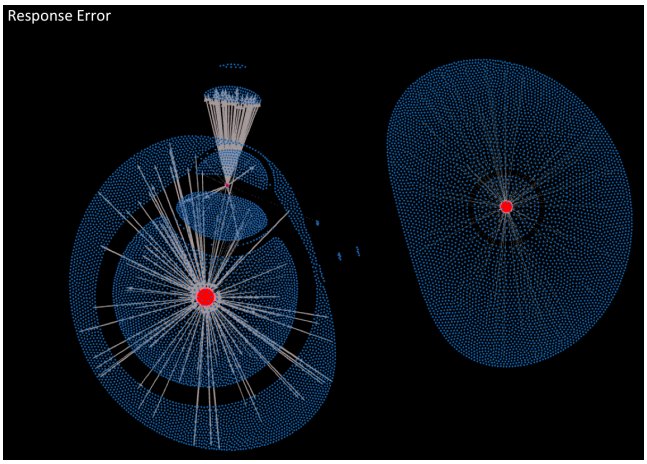
- Identify the characteristics of common smart meter communication use cases.
- Design a distributed monitoring framework and a security policy to ensure the detection of violations.
- Develop a C12.22 dissector and a C12.22 state machine to monitor meter traffic in real time.
- Implement a prototype in an embedded computer.
- Evaluate in a real AMI environment with hardware meters.
- Deploy at a utility site.
- Define a comprehensive security policy from known failure scenarios.
- Define an IDS test plan that can be implemented by utilities.



Simulation using Table TstBench and protocol stack from C1222.net

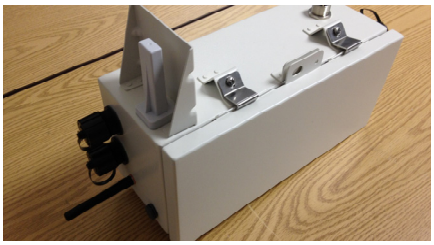
RESEARCH RESULTS

- Threat model reviewed.
- Dissector and parser for ANSI C12.22 and C12.19 implemented and tested.
- Comprehensive monitoring architecture implemented.
- Security policy defined based on NESCOR failure scenarios.
- Sensor prototype deployed to monitor 12,000 meters.



BROADER IMPACT

- Definition of a rigorous process utilities and vendors can use to design and develop an efficient monitoring architecture.
- Strong partnership with industry (EPRI, FirstEnergy, Itron, Fujitsu) to collaborate on development and evaluation, and to plan for technology transfer.
- Collaboration with other research partners (UT Dallas, Sandia National Labs).



INTERACTION WITH OTHER PROJECTS

- Alerts from Amilyzer have been integrated in a security event manager in collaboration with the Response and Recovery Engine project.
- Technology developed for Amilyzer has been leveraged to improve the ADEC-G project (IDS for control system protocols).
- Amilyzer has enabled the evaluation of a framework to detect energy theft detection, in collaboration with the University of Miami and Pennsylvania State University.

FUTURE EFFORTS

- Study solutions to enable Amilyzer to support encrypted traffic.
- Investigate approaches to allow multiple Amilyzer sensors to share state information and to coordinate a distributed detection strategy.
- Complete and validate the failure-driven security policy for AMI in collaboration with EPRI and multiple industry partners.

FUNDING SUPPORT PROVIDED BY DOE-OE AND DHS S&T