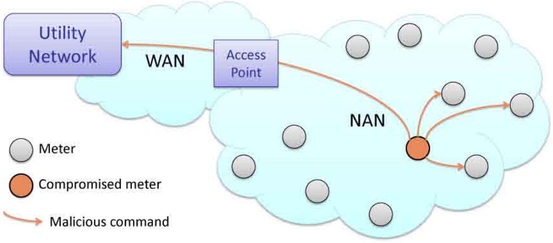
TCIPG

# Specification-based IDS for Smart Meters

R. Berthier 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.



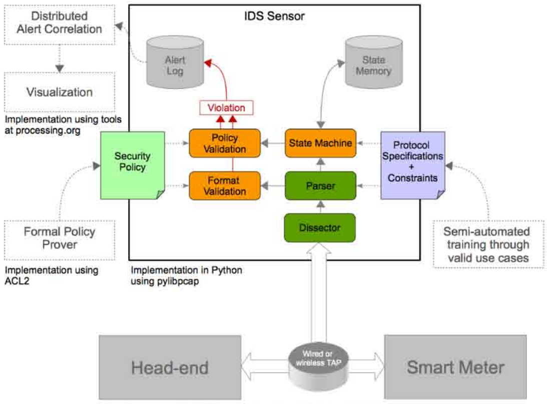
## Fundamental Questions

- What are the threats targeting the AMI?
- Which detection technology to develop to cover these threats?
- What monitoring architecture to deploy?
- How to automatically respond to security compromises?
- How to provide large-scale situational awareness?

## Challenges

- Large-scale environment.
- Real-time and cost efficiency requirements.
- Sensors to run on low-computation hardware with limited memory.

## Prototype in Development



Implementation using tools at processing.org

Implementation using ACL2

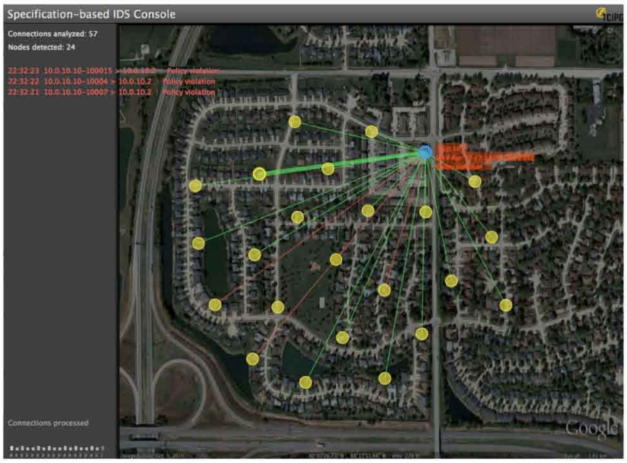
Implementation in Python using pylibpcap

Simulation using Table TstBench and protocol stack from C1222.net

## Broader Impact

- Definition of a **rigorous process** for utilities and vendors to design and develop an efficient monitoring architecture.
- Discussion with **industry partners** (Fujitsu, EPRI, and Itron) to collaborate on development and evaluation, and to plan for future technology transfer.

## Situational Awareness Solution


Specification-based IDS Console

Connections analyzed: 57

Nodes detected: 24

```
22:32:23  10.0.10.10-100015 > 10.0.10.2    Policy violation
22:32:22  10.0.10.10-10004 > 10.0.10.2    Policy violation
22:32:21  10.0.10.10-10007 > 10.0.10.2    Policy violation
```

Connections processed

## Research Results

- Threat model reviewed:

Cross-disciplinary documents & standards: NIST IR 7628, OpenSG

Industry Research: InGuardians, IBM, Itron Industrial Defender and others

Academic Research: AMI and SCADA threat models, IDS solution

| Attack Techniques | Attack Consequences |
|---|---|
| *Network Compromise* | |
| Communication interception and traffic analysis | Integrity of configuration and routing operations<br>Inconsistent traffic origin or destination |
| Traffic modification, injection, and replay | Integrity of communication traffic<br>Illegitimate system or network operations<br>Inconsistent traffic origin or destination |
| *System Compromise* | |
| Authorization or authentication violation | Illegitimate system or network operations<br>Inconsistent traffic origin or destination<br>Illegitimate use of credentials |
| Spoofing of utility system | Illegitimate system or network operations<br>Inconsistent traffic origin or destination |
| Node compromise, spoofing of metering device | Integrity of node software or hardware<br>Illegitimate system or network operations<br>Inconsistent traffic origin or destination |
| *Denial of Service* | |
| Resource exhaustion | Unresponsive nodes, high bandwidth usage |
| Signal jamming | Unresponsive nodes, high signal power level |
| Packet dropping | Integrity of communication traffic |

- Comprehensive monitoring architecture defined:

| Monitoring Operations | Agent Location | OSI Layers |
|---|---|---|
| Checking of configuration protocol | AP, Sensor | 3, 4, 5-7 |
| Checking of routing protocol | AP, Sensor | 3 |
| Checking of application operations | AP, Sensor | 5-7 |
| Checking of packet headers (firewall) | AP, Sensor | 3, 4 |
| Integrity checking of packets | AP, Sensor | 3, 4, 5-7 |
| Checking of node's health reports | AP | 5-7 |
| Checking of system logs | Meter | 5-7 |
| Integrity checking of software/hardware | Meter | |
| Monitoring of traffic characteristics | AP, Sensor | 3, 4 |
| Monitoring of wireless signal | Sensor, Meter | 1, 2 |

Stateful specification-based

Stateless specification-based

Anomaly-based

Trustworthy Cyber Infrastructure for the Power Grid • www.tcipg.org

University of Illinois • Dartmouth College • Cornell University • UC Davis • Washington State University