TCIPG

Specification-based IDS for Smart Meters

Amilyzer: IDS Sensor for AMI

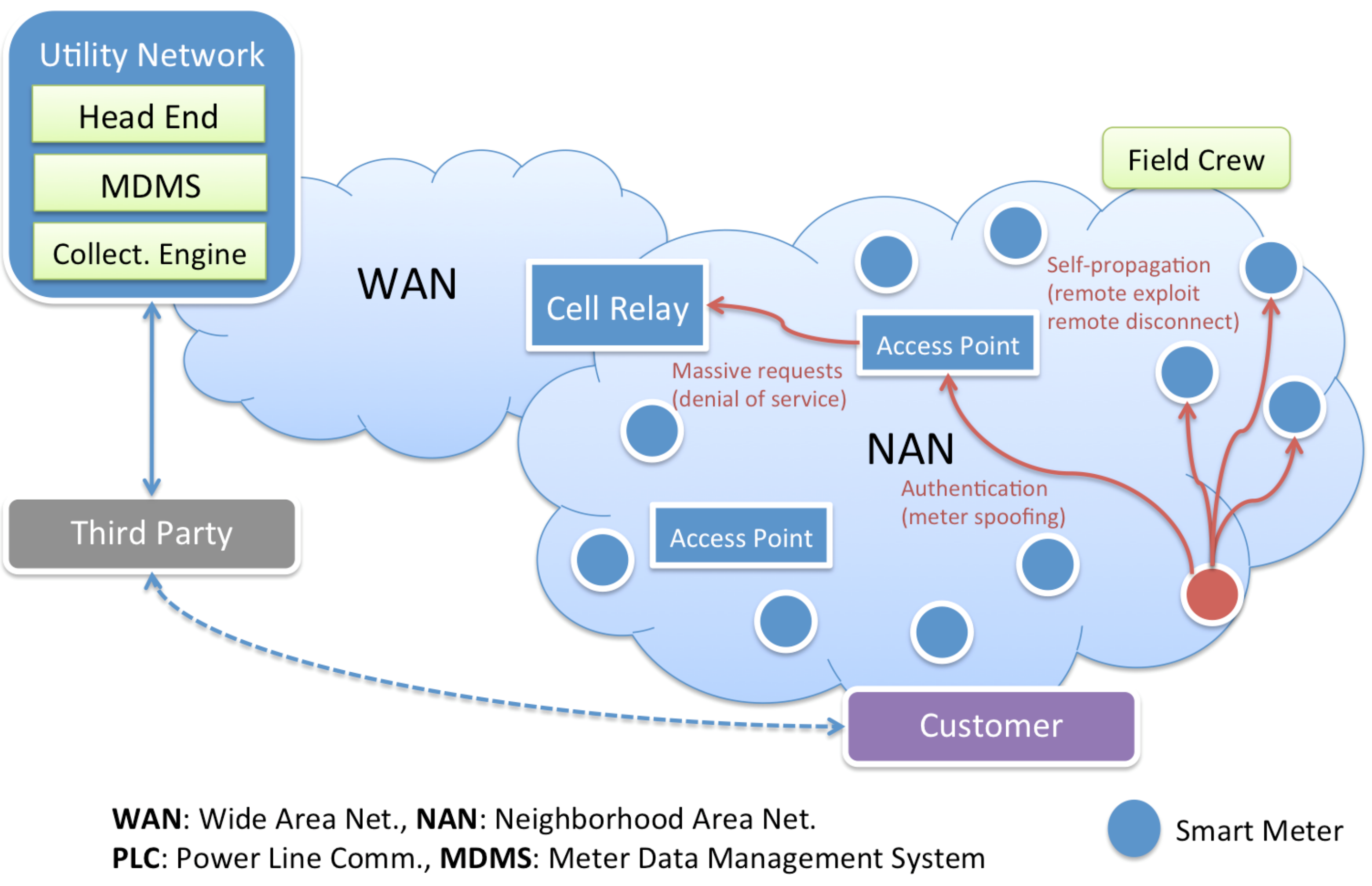
R. Berthier, A. Fawaz, E. Rogers, and W. H. Sanders

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.

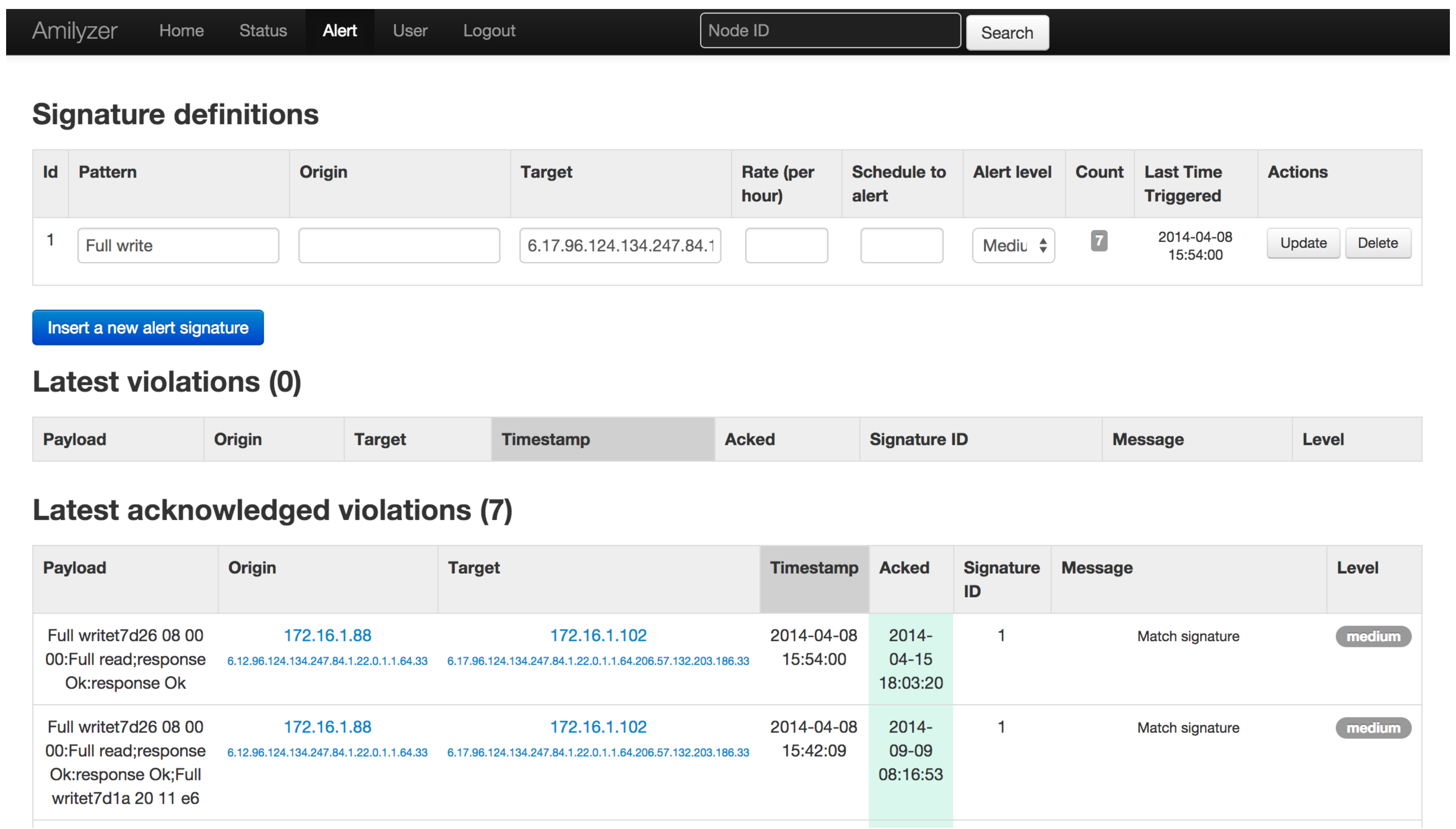
FUNDAMENTAL QUESTIONS/CHALLENGES

- 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?


Utility Network
Head End
MDMS
Collect. Engine
WAN
Cell Relay
Field Crew
Self-propagation (remote exploit remote disconnect)
Access Point
Massive requests (denial of service)
NAN
Authentication (meter spoofing)
Access Point
Third Party
Customer
WAN: Wide Area Net., NAN: Neighborhood Area Net.
PLC: Power Line Comm., MDMS: Meter Data Management System
Smart Meter

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.



Signature definitions

Id	Pattern	Origin	Target	Rate (per hour)	Schedule to alert	Alert level	Count	Last Time Triggered	Actions
1	Full write		6.17.96.124.134.247.84.1			Mediu	7	2014-04-08 15:54:00	Update Delete

Insert a new alert signature

Latest violations (0)

Payload	Origin	Target	Timestamp	Acked	Signature ID	Message	Level

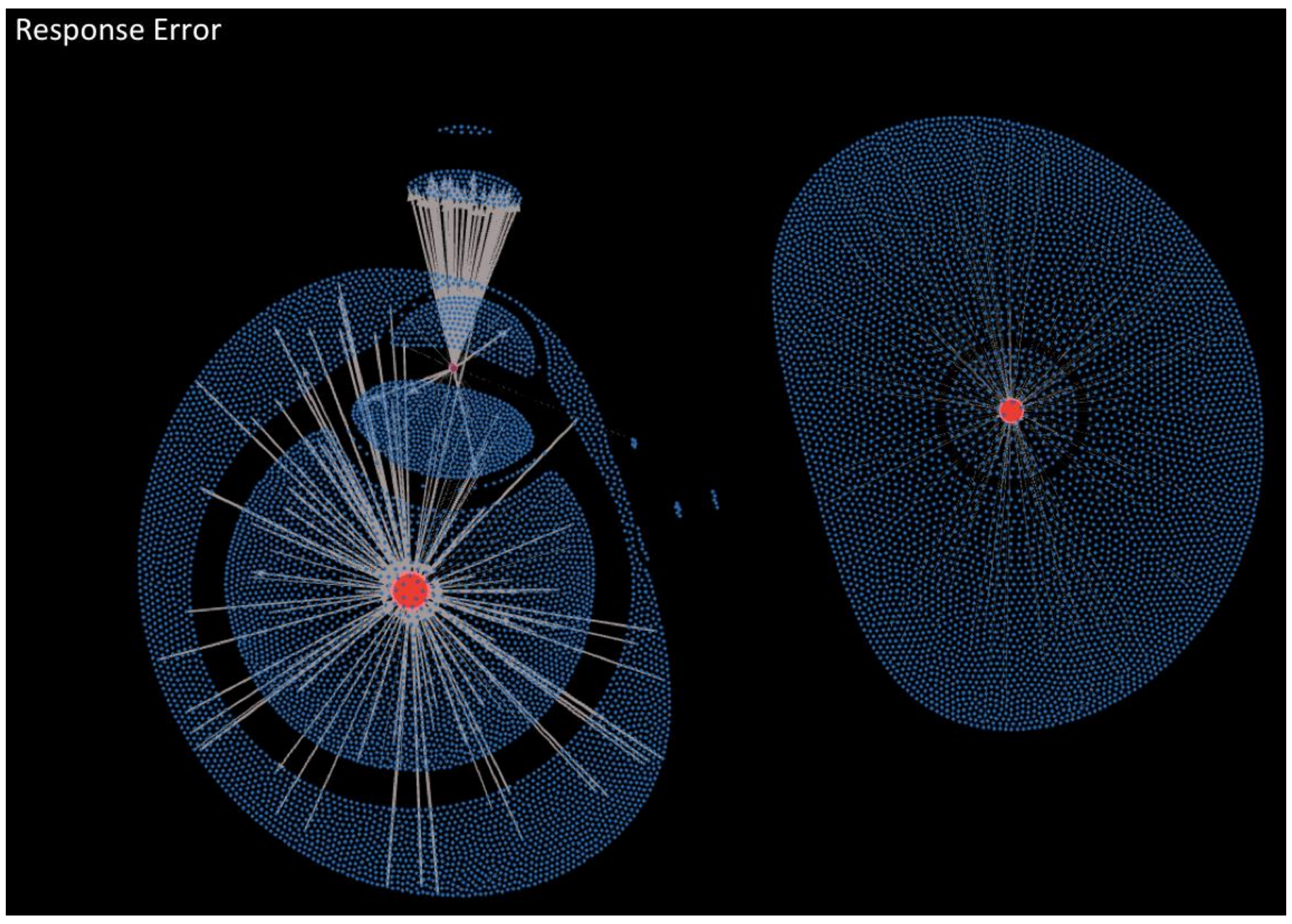
Latest acknowledged violations (7)

Payload	Origin	Target	Timestamp	Acked	Signature ID	Message	Level
Full writet7d26 08 00 00:Full read;response Ok:response Ok	172.16.1.88 6.12.96.124.134.247.84.1.22.0.1.1.64.33	172.16.1.102 6.17.96.124.134.247.84.1.22.0.1.1.64.206.57.132.203.186.33	2014-04-08 15:54:00	2014-04-15 18:03:20	1	Match signature	medium
Full writet7d26 08 00 00:Full read;response Ok:response Ok;Full writet7d1a 20 11 e6	172.16.1.88 6.12.96.124.134.247.84.1.22.0.1.1.64.33	172.16.1.102 6.17.96.124.134.247.84.1.22.0.1.1.64.206.57.132.203.186.33	2014-04-08 15:42:09	2014-09-09 08:16:53	1	Match signature	medium

User interface to define signatures and review intrusion detection alerts

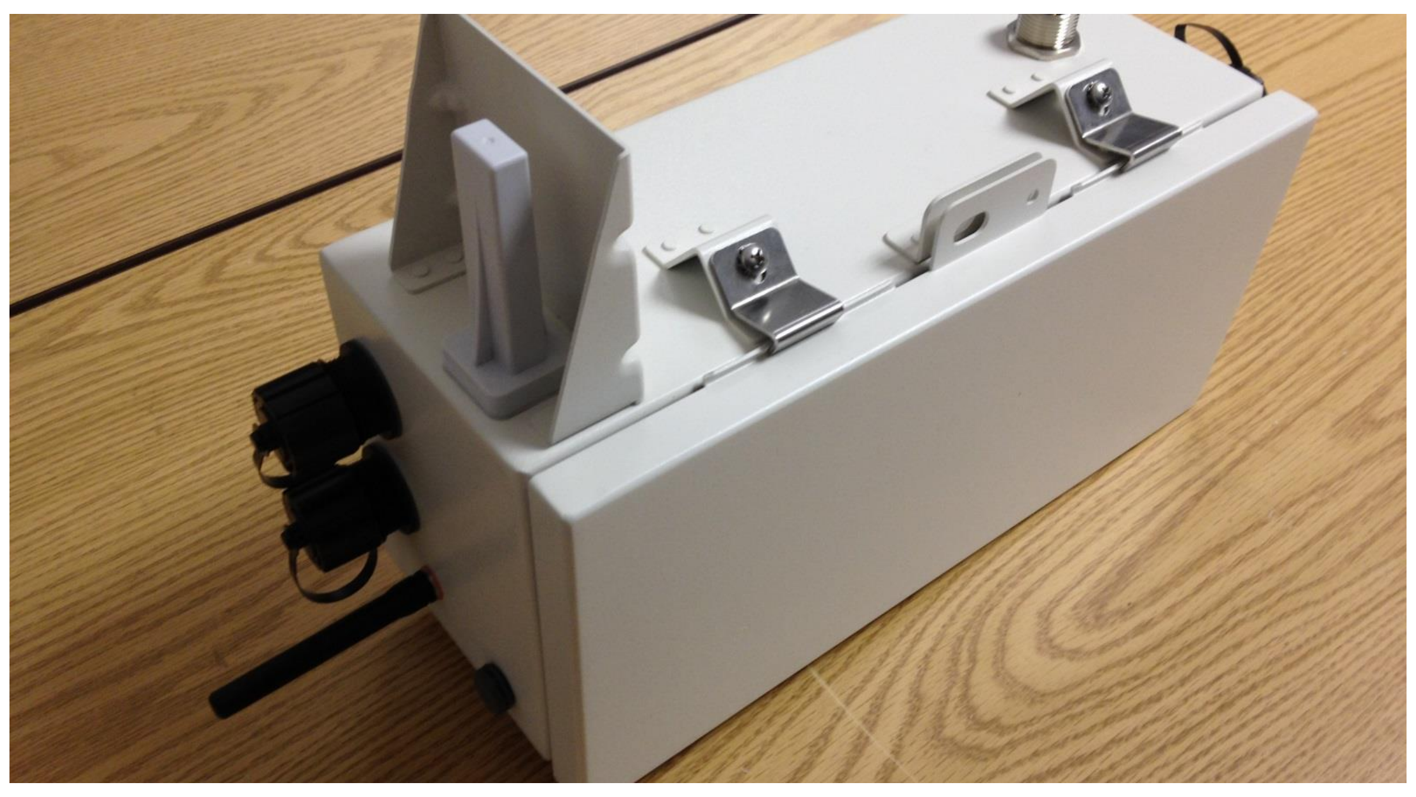
RESEARCH RESULTS

- 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 30,000+ 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, Honeywell, 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, 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.

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