Specification-based IDS for Smart Meters

Overview and Problem Statement

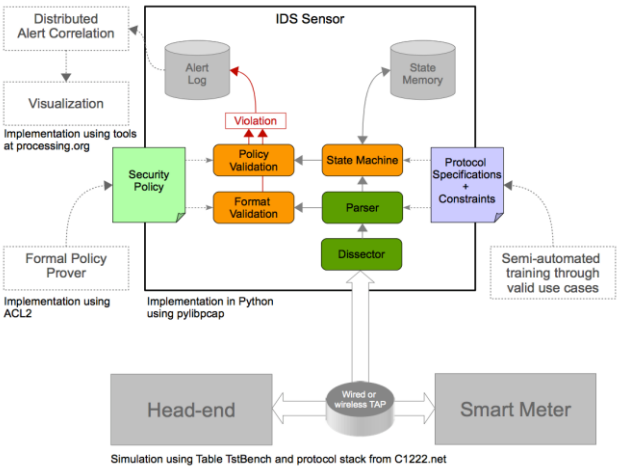
To ensure the security and reliability of a modernized power grid, the current deployment of millions of smart meters requires the development of innovative situational awareness solutions to prevent compromised devices from impacting the stability of the grid and the reliability of the energy distribution infrastructure. To address that issue, we introduce a specification-based intrusion detection sensor called **Amilyzer** that can be deployed in the field to identify security threats in real time. Amilyzer monitors the traffic among meters and access points at the network, transport, and application layers to ensure that devices are running in a secure state and that their operations respect a specified security policy. It does so by implementing a set of constraints on transmissions made using the C12.22 AMI protocol that ensure that all violations of the specified security policy will be detected. The soundness of those constraints was verified using a formal framework, and the security policy was defined based on the set of failure scenarios for AMI identified by the NESCOR group. Amilyzer has been successfully deployed by a utility partner since December 2012 and is currently monitoring a 30,000-meter AMI.

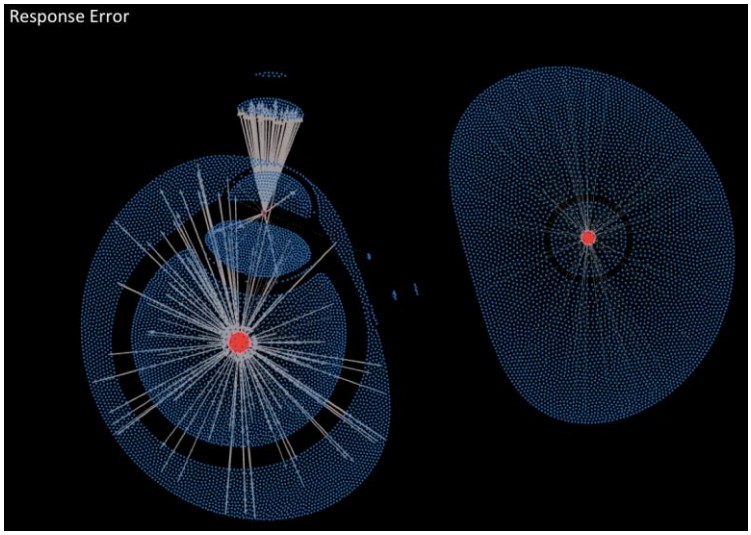
Research Objectives

- Identify potential AMI failure scenarios and translate them into a sound security policy.
- Develop detection technologies to run on low-computation hardware with limited memory.
- Design a comprehensive but cost-efficient monitoring architecture.
- Provide large-scale situational awareness.
- **Smart Grid Application Area:** AMI security.

Technical Description and Solution Approach

- Identification of the characteristics of common smart meter communication use cases.
- Design of a distributed monitoring framework and a security policy to ensure the detection of violations.
- Development of a C12.22 dissector and a C12.22 state machine to monitor meter traffic in real time.
- Implementation of a prototype in an embedded computer.
- Evaluation in a real AMI environment with hardware meters.

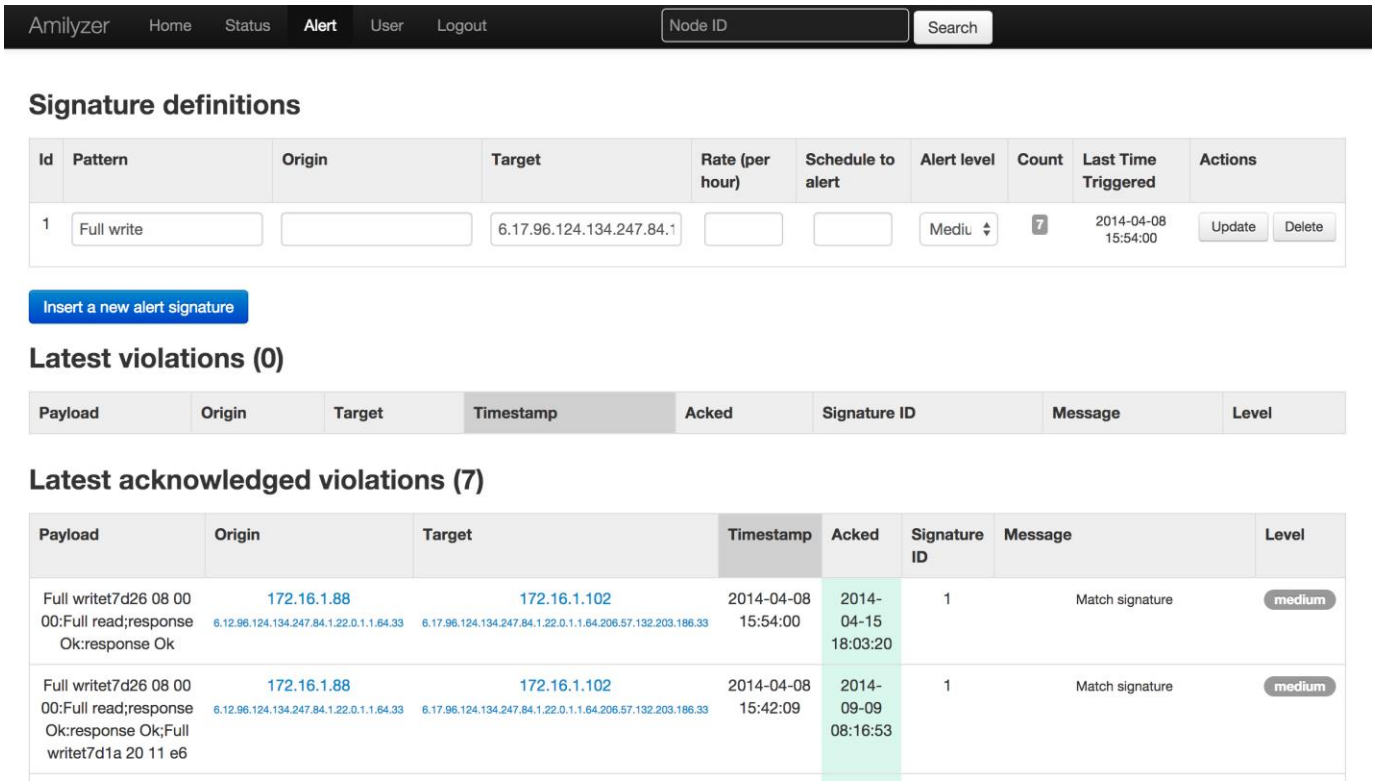




Software modules inside Amilyzer (left). Visual representation of 12,000 meters and their communications (right).

Results and Benefits

- Definition of a rigorous process that utilities and vendors can use to develop a comprehensive monitoring architecture.
- Integration of formal methods in a practical framework to offer strong security guarantees.
- Deployment of an Amilyzer sensor in collaboration with FirstEnergy to monitor 30,000+ meters.
- **Partnerships and External Interactions**: In collaboration with EPRI, FirstEnergy, and Itron.
- **Technology Readiness Level**: Prototype.



User interface to define signatures and review intrusion detection alerts.

Researchers

- Dr. Robin Berthier, rgb@illinois.edu
- Ahmed M. Fawaz, afawaz2@illinois.edu
- Edmond Rogers, ejrogers@illinois.edu
- Prof. William H. Sanders, whs@illinois.edu

Industry Collaborators

- EPRI: Galen Rasche and Annabelle Lee
- Itron: Ido Dubrawsky
- FirstEnergy: Don Miller, Nathaniel Maier, Marcus Noel, and Nathan Sterrett
- Fujitsu: Jorjeta Jetcheva, Daisuke Mashima, and Ulrich Herberg
- UT Dallas: Alvaro Cardenas, David Urbina, Michael Guerrero
- Honeywell: Jun Ho Huh

funded by the U.S. Department of Energy and the U.S. Department of Homeland Security