Intrusion Detection for Advanced Metering Infrastructures: Requirements and Architectural Directions
by Robin Berthier, William H. Sanders, and Himanshu Khurana

Presenter: Saranya Parthasarathy

Submitted in Partial Fulfillment of the Course Requirements for
ECEN 689: Cyber Security of the Smart Grid
Instructor: Dr. Deepa Kundur
Agenda

• Motivation
• Past related work
• AMI Communication
• Threat Model
• IDS: Overview
• Design Considerations
• Proposed Architecture
• Open Issues
• Personal assessment
• References
Motivation

- AMI (Advanced Metering Infrastructures) widely deployed as part of smart grid initiatives
- Collection of systems used to record and evaluate data associated with the use of utility resources
- Why AMI?
  - Real-time pricing and greater visibility to end users' about electricity usage
  - Remote load shed.
  - Provide better control of energy use to reduce demand, electricity costs and carbon footprint
Recent Stats: 3 million smart meters to be deployed in Texas between now and end of 2012
These meters lack security testing (Source: Ref [2])

More testing needed, some say
But many security researchers say the technology is being deployed without enough security probing.

Wright said his firm found "egregious" errors, such as flaws in the meters and the technologies that utilities use to manage data from meters. "Even though these protocols were designed recently, they exhibit security failures we've known about for the past 10 years," Wright said.

He said InGuardians found vulnerabilities in products from all five of the meter makers the firm studied. He would not disclose those manufacturers.

One of the most alarming findings involved a weakness in a communications standard used by the new meters to talk to utilities' computers.

Wright found that hackers could exploit the weakness to break into meters remotely, which would be a key step for shutting down someone's power. Or someone could impersonate meters to the power company, to inflate victims' bills or lower his own. A criminal could even sneak into the utilities' computer networks to steal data or stage bigger attacks on the grid.
• 3 classes of solutions for handling the potential vulnerabilities
  
  ❖ Prevention (like better cryptographic techniques and authentication mechanisms)
  ❖ Detection
  ❖ Mitigation/resilience

• This paper focuses on the DETECTION part
Identify potential threats and vulnerabilities

Incorporate proper prevention measures in the system to be robust to attacks

Is system robust to attacks

N

Detect the attacks

Corrective measures to bring system to safe state and mitigate impacts

Y

System continues to operate normally
Past related work

- Mostly focusing on a particular component
- [3]-Proposes an architecture for a model-based multi-layer IDS for sensor networks used for PCS

![Diagram showing central IDS and field IDS connections with sensors]

S1, S2 etc.-Local sensors
Overview of AMI networks: WAN, FAN, HAN
Heterogeneous
Threat Model

- Classification based on
  - Type of attacker
  - Motivation
  - Attack technique
- Attackers and motivation:
  - Curious eavesdroppers
  - Motivated eavesdroppers
  - Unethical customers
  - Active attackers
  - Publicity seekers
  - Overly intrusive meter data management agencies
• Attack techniques:

  ❖ **Network Compromise**
  Interception, Modification, Injection, Replay

  ❖ **System Compromise**
  Authorization, Authentication violation, Compromise of meter, Spoofing of meter

  ❖ **Denial of Service**
  Signal jamming, Dropping packets.
Intrusion Detection:
Monitoring events in a system and analyzing them for any signs of unwanted/malicious activity.

Components in a traditional IDS:
- **Sensors** to monitor activity
- **Management server**: Centralized information collection from sensors
- **Database server**: Store all data produced by an IDS
- **User interface**: Check status of system monitored.
IDS components:

- Database server
- User Interface
- Management server

Access Points

METERS

Sensor
Detection Technologies:

- **Anomaly-based**: Modes: training and detection
  - **Pros**: Detects new attacks
  - **Cons**: More false positives, expensive to train and tune

- **Signature-based**: Comparison with pre-defined attack signatures
  - **Pros**: More accurate
  - **Cons**: Can’t detect new attacks

- **Specification-based**: Comparison with a state machine based on logical high-level specifications
  - **Pros**: Detects new attacks, less false positives
  - **Cons**: High overhead
• Specification-based –
  ❖ High-level representation in terms of a state diagram
  ❖ Build a state machine and define boundaries
  ❖ Monitor data flows across these boundaries to determine anomalous behavior
  ❖ Eg of a simplified IP state machine

```
INIT
pkt(ext_ifc,p)|p.dst==gateway

PKT RCVD
pkt(ext_ifc,p)|p.dst! =gateway
src=p.src, dst=p.dst

DONE
pkp(ext_ifc,p)|p.dst! =gateway
src=p.src, dst=p.dst

Timeout()
```

From: Ref[4]
Design considerations

- Anomaly or Signature or specification based?
- Centralized or distributed?
  - **Centralized**: light weight sensors communicating with a centralized server with IDS capability.
    - Limitation: Scalability with millions of nodes
  - **Distributed**: Data processing at sensors
    - Server: Co-ordinates sensors and collects high-level alerts
    - Problem: Volume of alerts generated
Proposed Architecture

- Specification-based

**Reasons:**
- Lack of empirical data in smart grid
- Less false positives compared to anomaly-based
- Limited number of protocols reduces development cost of specification-based
Distributed

Reasons:
- Reliability improves; system operates even if a subset of meters are compromised
- Scalable
- Alerts managed by grouping and alert correlation
Suggested sensor locations:

<table>
<thead>
<tr>
<th>Attack Consequences</th>
<th>Detection goal and operation</th>
<th>Type and location of sensors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Illegitimate network operations</td>
<td><strong>Stateful</strong> checking of protocol operations against security policy and application configurations</td>
<td>Behavioral monitor centralized on access points</td>
</tr>
<tr>
<td>Illegitimate use of credentials</td>
<td>Checking system logs against security policy</td>
<td>Authentication log monitor, centralized on access points or distributed on network nodes</td>
</tr>
<tr>
<td>Integrity of node software or hardware</td>
<td>Operating system, application and file integrity checking</td>
<td>Remote attestation and virtualization distributed on network nodes</td>
</tr>
</tbody>
</table>
Resources needed for such monitoring:

- A network configuration to provide information about topology (NAN, WAN etc).
- Protocol specifications, like the example shown before for simplified IP state machine.
- Statistical profiles of normal behavior obtained through a training phase.
Open Issues

- Overhead due to IDS if it uses the same network to communicate as the AMI
- Computational power and memory requirements
- Development of specifications from the protocols available needs manual efforts as of now.
- Tuning the system to reduce false positives and avoid false negatives!

All these provide great scope for further exploration!
Formulates threats well

Very high-level architecture

Specific details regarding the states, state variables, transitions needed for intrusion detection are not explained.

Further work needed to study its applicability - by trying to develop a state-based model for a test system with AMIs.

Deals with smart meters and the communication infrastructure in smart grid - Mainly on the distribution side of the grid.
References


QUESTIONS?