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

TEXAS A&M UNIVERSITY

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

Motivation

TEXAS A&M UNIVERSITY

- 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.

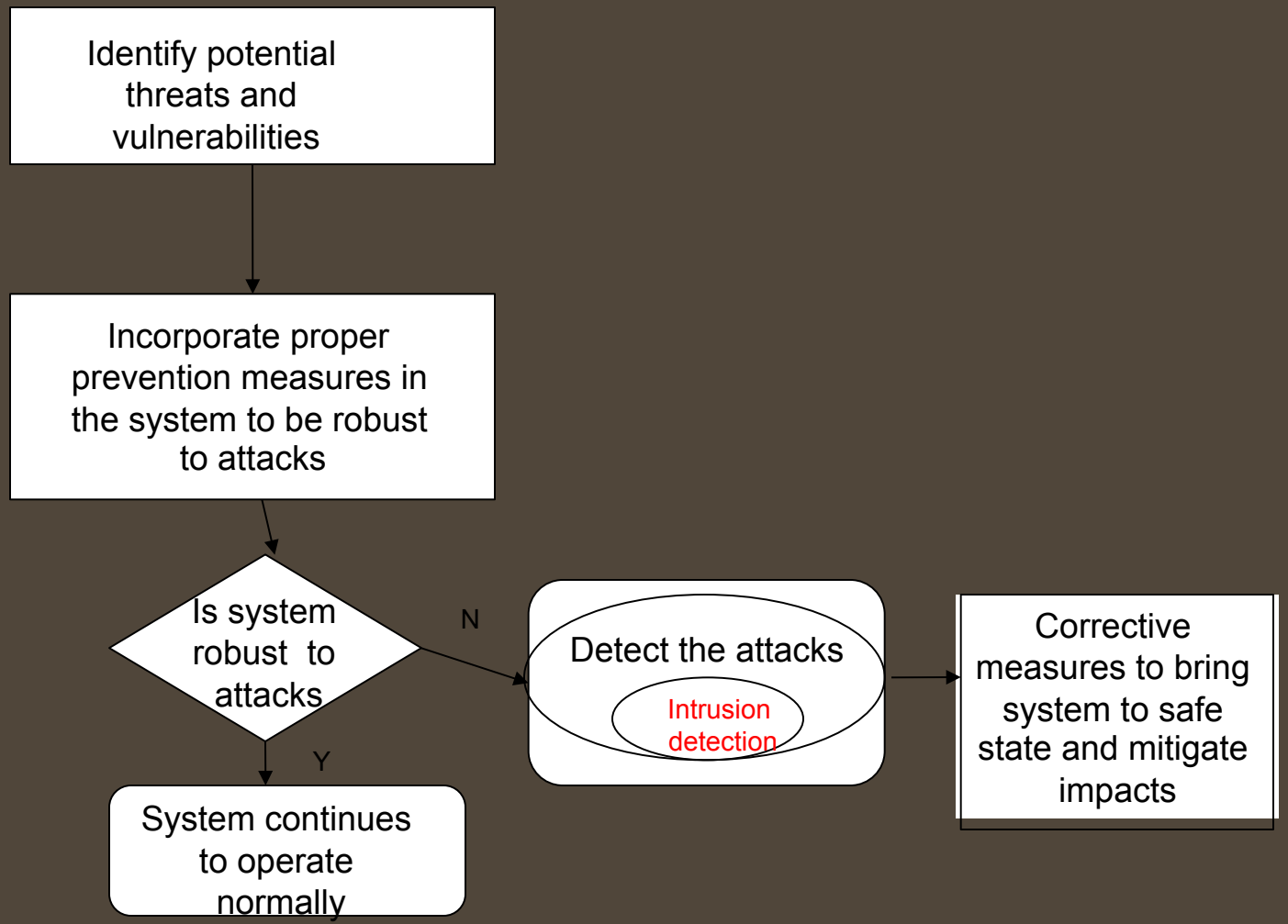
Wright said his firm found "egregious" errors, such as flaws in the meters and the technologies that utilities use to manage data from meters. "Even though these protocols were designed recently, they exhibit security failures we've known about for the past 10 years," Wright said.

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.

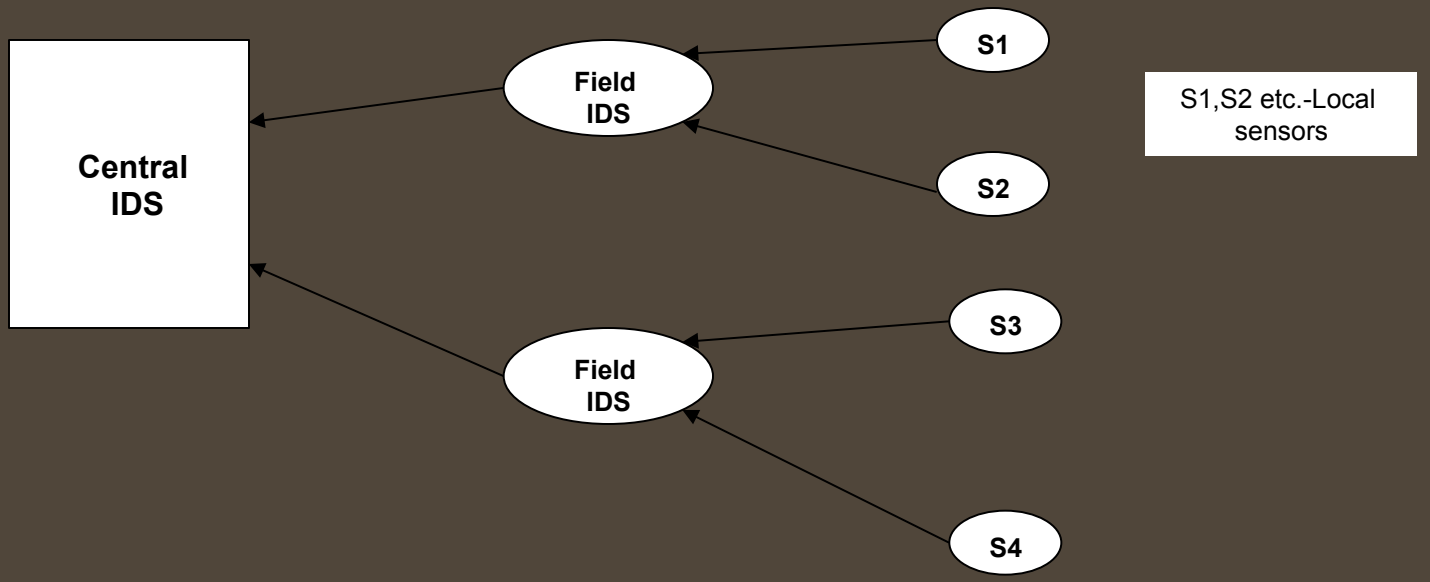
Wright found that hackers could exploit the weakness to break into meters remotely, which would be a key step for shutting down someone's power. Or someone could impersonate meters to the power company, to inflate victims' bills or lower his own. A criminal could even sneak into the utilities' computer 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
Y
Detect the attacks
Intrusion detection
Corrective measures to bring system to safe state and mitigate impacts
System continues to operate normally

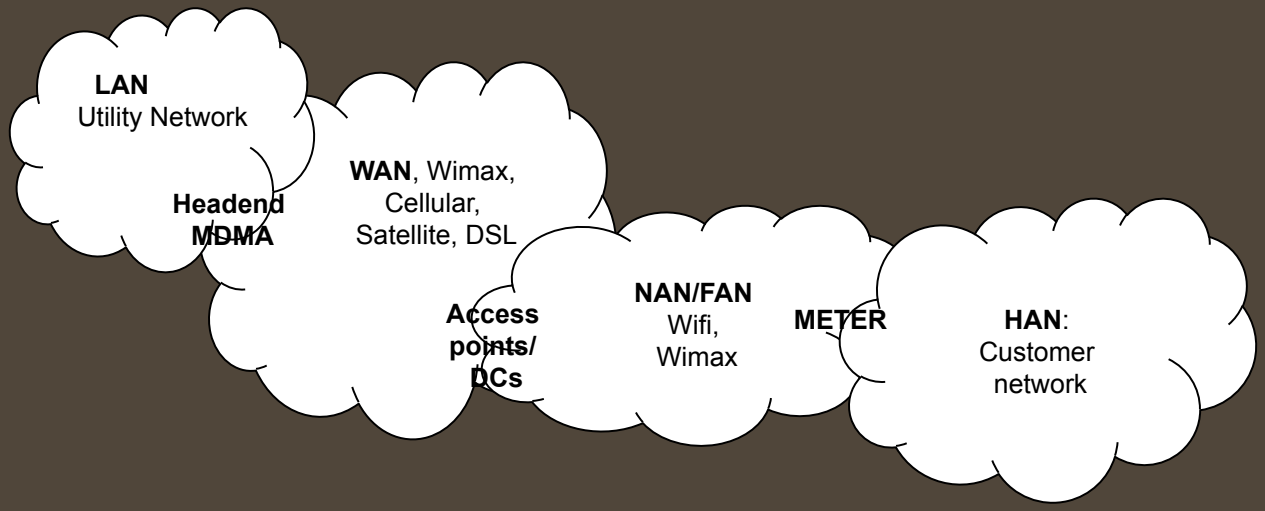
Past related work

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



AMI Communication

Overview of AMI networks: WAN, FAN, HAN
Heterogeneous



Threat Model

TEXAS A&M UNIVERSITY

- 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.

IDS: Overview

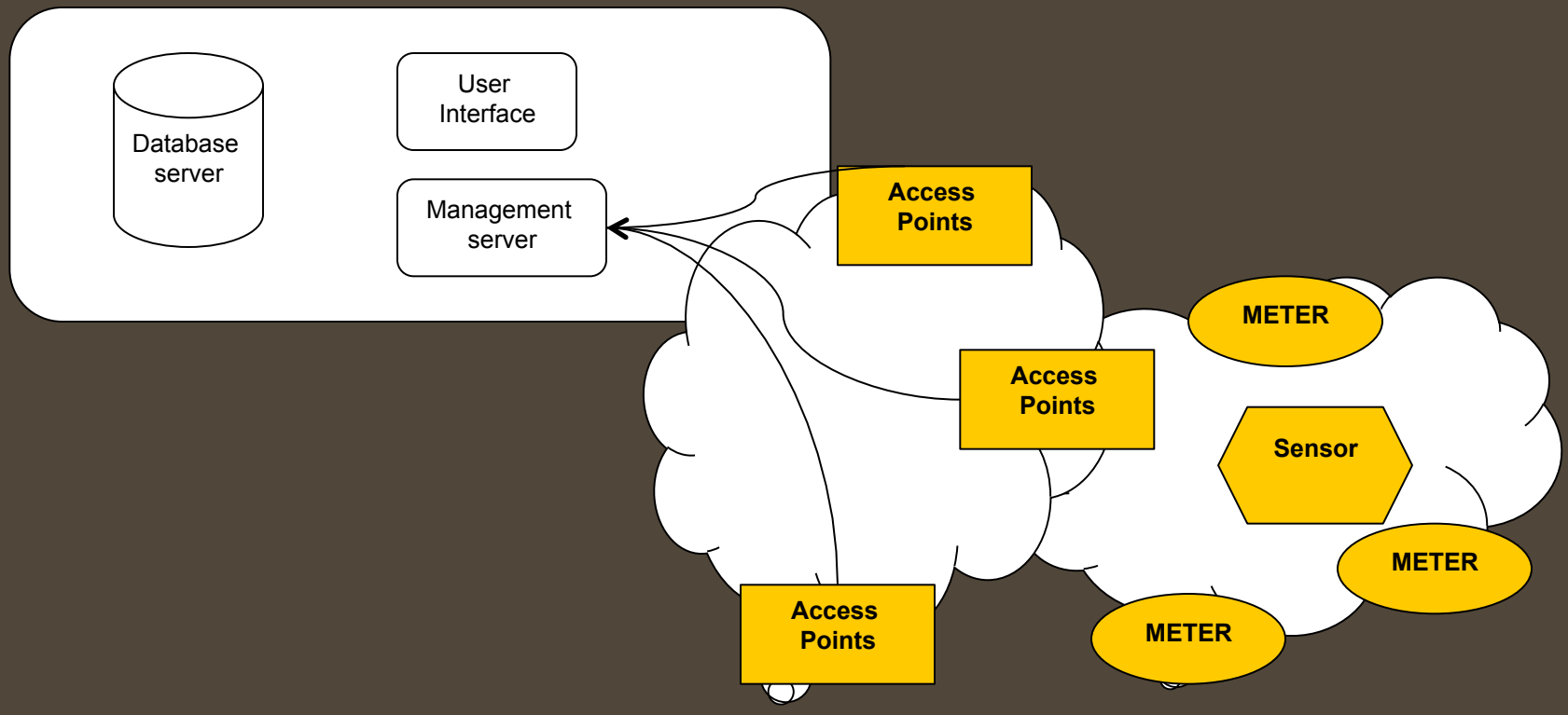
Intrusion Detection:

Monitoring events in a system and analyzing them for any signs of unwanted/malicious activity.

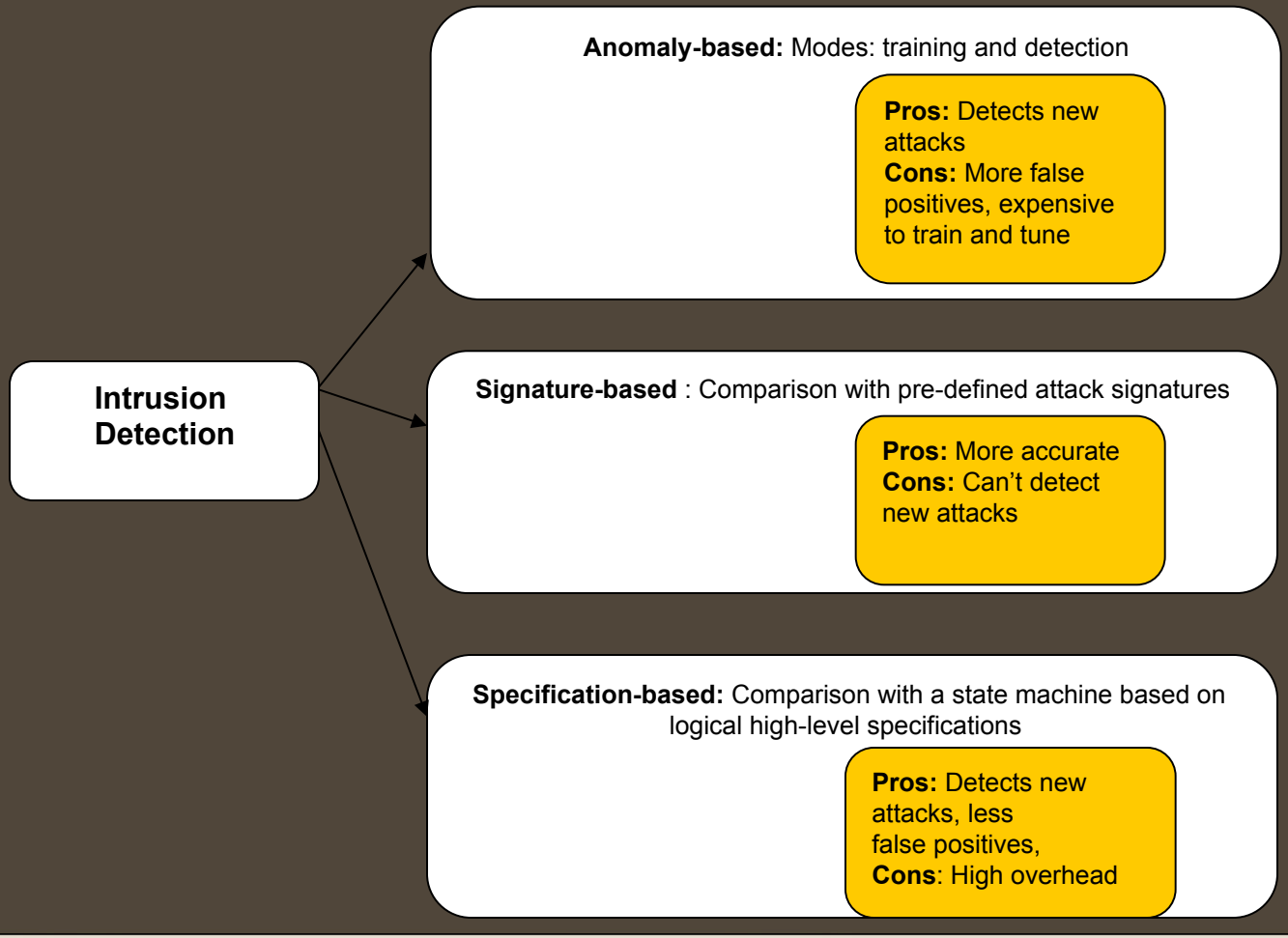
Components in a traditional IDS:

- 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.

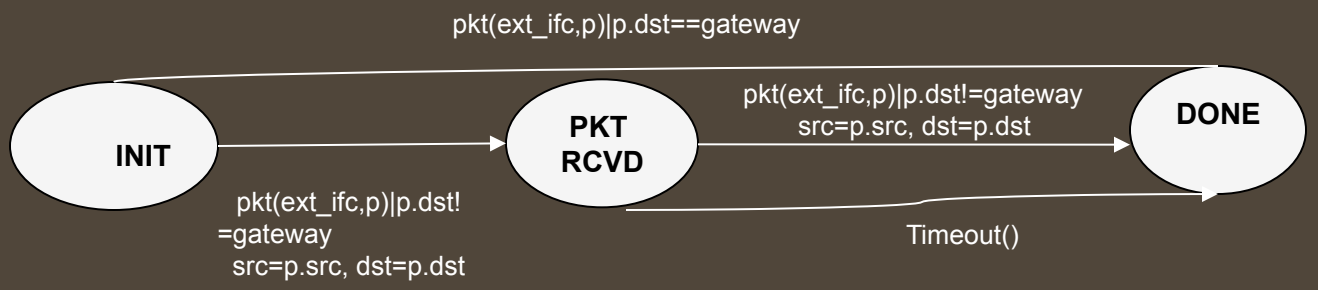
IDS components:



Detection Technologies:



- 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



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

TEXAS A&M UNIVERSITY

- 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:

Attack Consequences	Detection goal and operation	Type and location of sensors
Illegitimate network operations	**Stateful** checking of protocol operations against security policy and application configurations	Behavioral monitor centralized on access points
Illegitimate use of credentials	Checking system logs against security policy	Authentication log monitor, centralized on access points or distributed on network nodes
Integrity of node software or hardware	Operating system, application and file integrity checking	Remote attestation and virtualization distributed on network nodes

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

TEXAS A&M UNIVERSITY

- 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!

Personal Assessment

TEXAS A&M UNIVERSITY

- 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

1. Robin Berthier, William H.Sanders, and Himanshu Khurana, “Intrusion Detection System for Advanced Metering Infrastructures: Requirements and Architectural Directions”, Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on Smart Grid

2. “Smart Meters Have Security Holes,” http://www.msnbc.msn.com/id/36055667, 2010

3. T. Roosta, D. K. Nilsson, U. Lindqvist, and A. Valdes, “An Intrusion Detection System for Wireless Process Control Systems,” Proceedings of the 5th IEEE International Conference on Mobile Ad Hoc and Sensor Systems (MASS), pp. 866–872, 2008

4. R. Sekar, A. Gupta, J. Frullo, T. Shanbhag, A. Tiwari, H. Yang and S. Zhou, “Specification-based Anomaly Detection: A New Approach for Detecting Network Intrusions”

TEXAS A&M UNIVERSITY

QUESTIONS?