Understanding the Role of Automated Response Actions to Improve AMI Resiliency

Ahmed Fawaz[1], Robin Berthier[1], Bill Sanders[1], Partha Pal[2]

April 24, 2012

[1]University of Illinois at Urbana Champaign

[2]BBN Technologies

TCIPG Mission

- Identify and address critical security and resiliency needs at the cyber-physical junction in the evolving power grid
  - Meet the challenge of rapid evolution and mixed legacy environment
  - Address the proliferation of devices, demand response, DG integration, HAN…
  - Emphasis on trust and resiliency
- Engage Industry (utility, control system vendors, technology providers)
  - Ensure relevance of research
  - Foster technology transfer
- Research Excellence
  - Balance long-range basic research with the need to develop practical solutions in the near term
  - Publications and conference presentations
  - TCIPG is the "go to" academic center
- Education
  - Develop university students who will be experts in the field
  - Outreach to K-12 students and the public

TCIPG Statistics

- Builds upon $7.5M NSF TCIP CyberTrust Center 2005-2010
- $18.8M over 5 years, starting Oct 1, 2009
- Funded by Department of Energy, Office of Electricity and Department of Homeland Security
- 5 Universities
  - University of Illinois at Urbana-Champaign
  - Washington State University
  - University of California at Davis
  - Dartmouth College
  - Cornell University
- 20 Faculty, 20 Senior Technical Staff, 37 Graduate Students, 5 Undergraduate Students, and 1 Admin

Industry Interaction: Vendors and Utilities that have participated in TCIPG Events

Industry Interaction: Other organizations that have participated in TCIPG Events

TCIPG Impacts all aspects of the *2011 Roadmap to Achieve Energy Delivery Systems Cybersecurity*

TCIPG Efforts

Build a Culture of Security	Assess and Monitor Risk	Protective Measures/Risk Reduction	Manage Incidents	Sustain Security Improvements
Conduct summer schools for industry	Analyze security of protocols (e.g. DNP3, Zigbee, ICCP, C12.22)	Build secure, real-time, & flexible communication mechanisms for WAMS	Build game-theoretic Response and recovery engine	Offer Testbed and Expertise as a Service to Industry
Develop K-12 power/cyber curriculum	Create tools for assessing security of devices, systems, & use cases	Design secure information layer for V2G	Develop forensic data analysis to support response	Anticipate/address issues of scale: PKI, data avalanche, PMU data compression
Develop public energy literacy	Create integrated scalable cyber/ physical modeling infrastructure	Provide malicious power system data detection and protection	Create effective Intrusion detection approach for AMI	Act as repository for cyber-security-related power system data
Directly interact with industry	Distribute NetAPT for use by utilities and auditors	Participate in industry-led CEDS projects		
Educate next-generation cyber-power aware workforce	Create fuzzing tools for SCADA protocols			

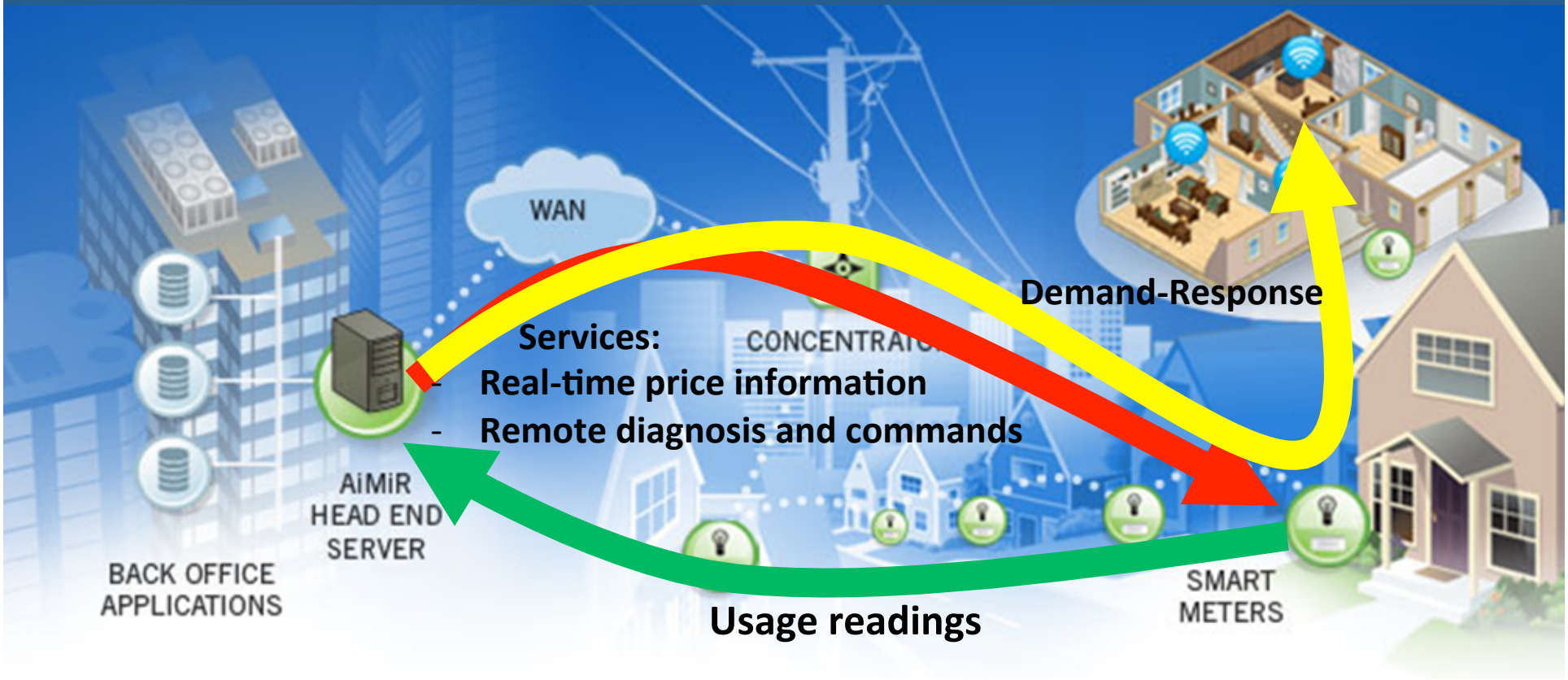
Agenda

- Background on AMI
  - System overview
  - Security aspects
- Towards Automated Response
  - Taxonomy
  - Cost model
  - Practical deployment
- Future Directions

Acknowledgements

- Core funding as part of TCIPG Center, Office of Electricity, Department of Energy
- Additional support for Development/Analysis/ Technology Transfer
  - BBN Technology
  - ITRON – Testbed provisioning

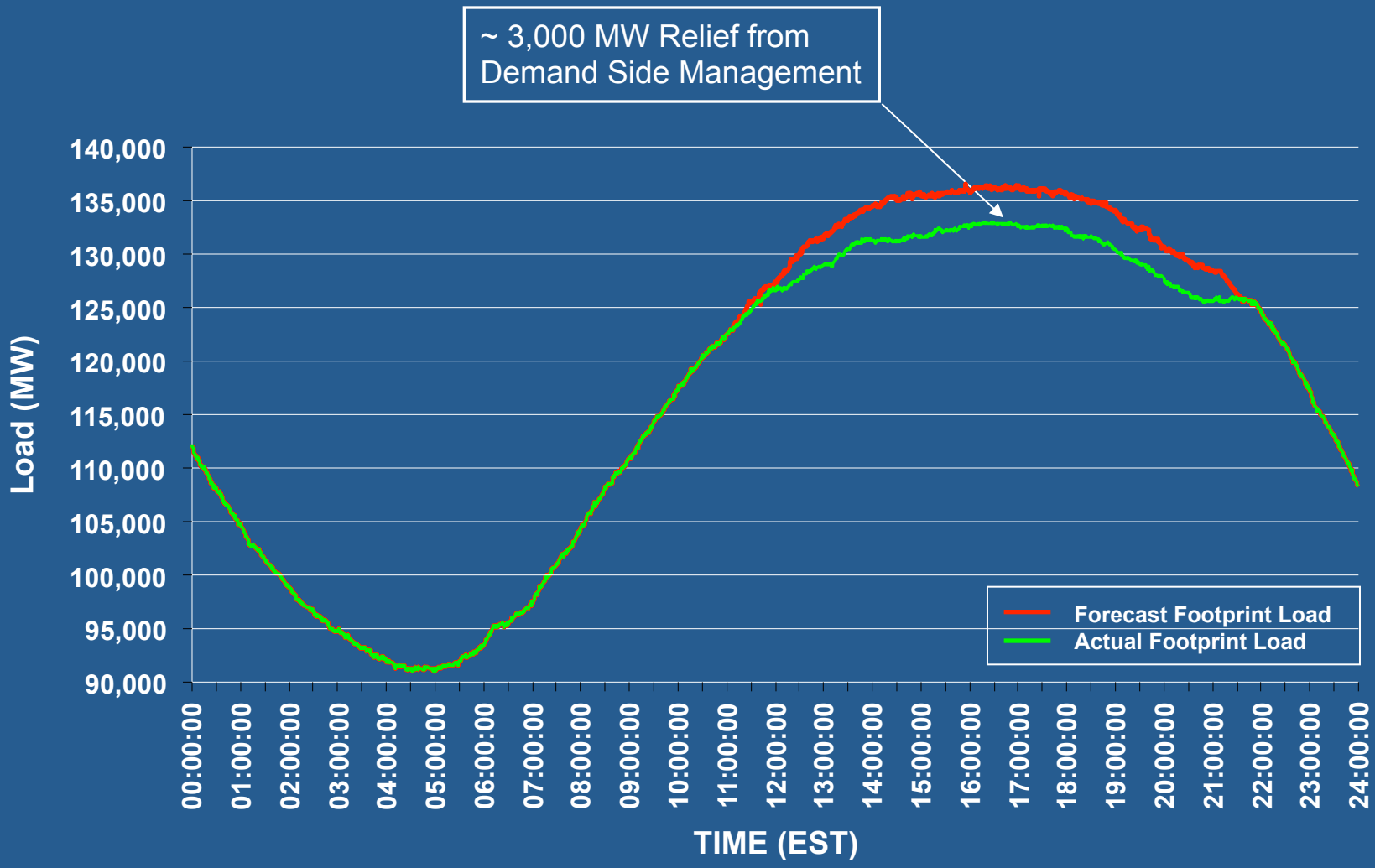
Advanced Metering Infrastructure



Utility Data Center	Neighborhood Area Network (NAN)	Home Area Network (HAN)

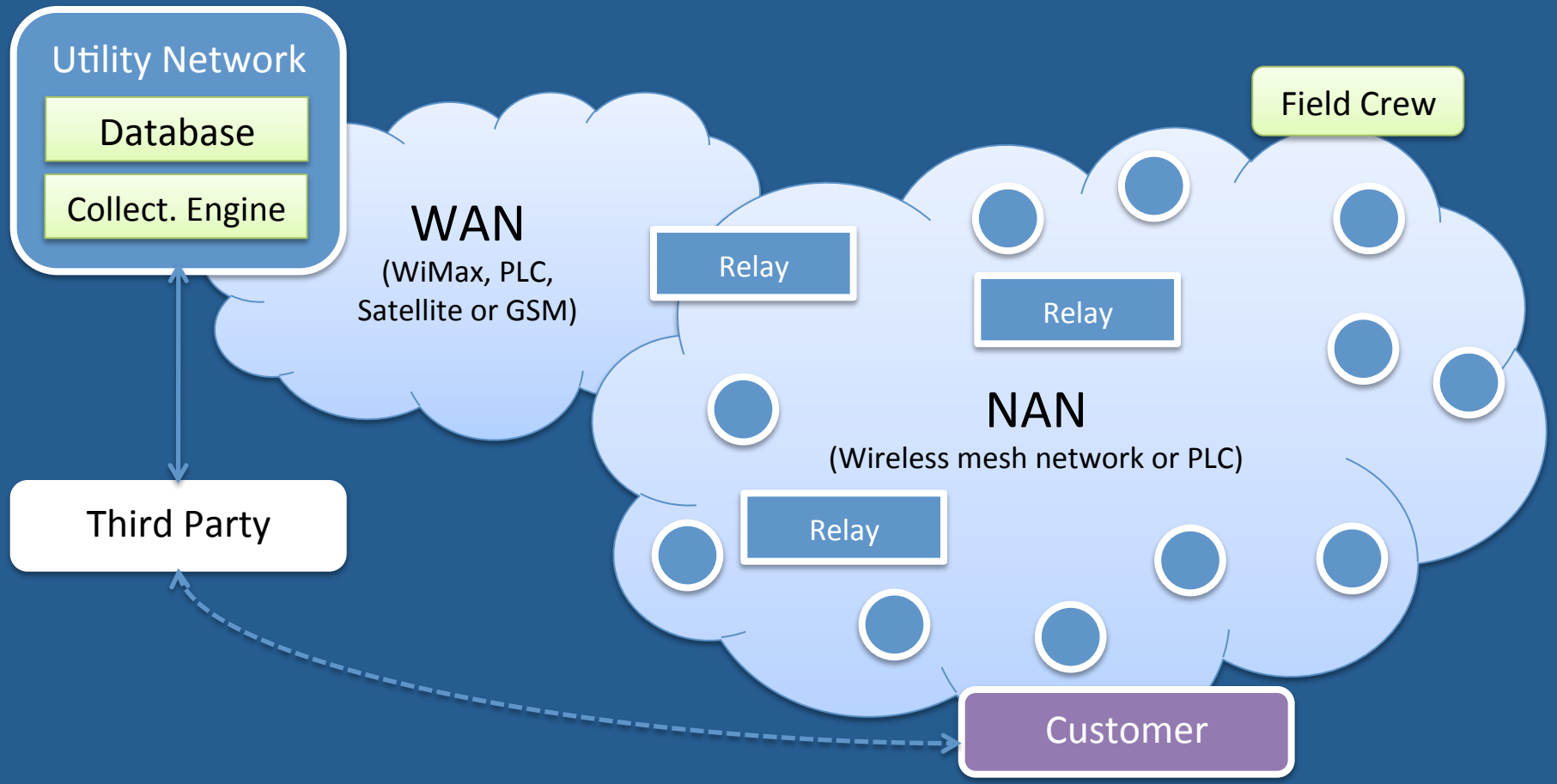
http://www.nuritelecom.com/solutions/advanced-metering-infrastructure.html

Demand Response in MISO Markets



http://www.narucmeetings.org/Presentations/Doying%20Midwest%20ISO%20Demand%20Response.ppt

AMI Architecture



WAN: Wide Area Net., **NAN**: Neighborhood Area Net.
PLC: Power Line Comm.

Smart Meter

Requirements

- Large-scale
  - Managing few millions nodes
- Resilient
  - Energy delivery mission is critical
- Privacy-preserving
  - Protect sensitive customer information

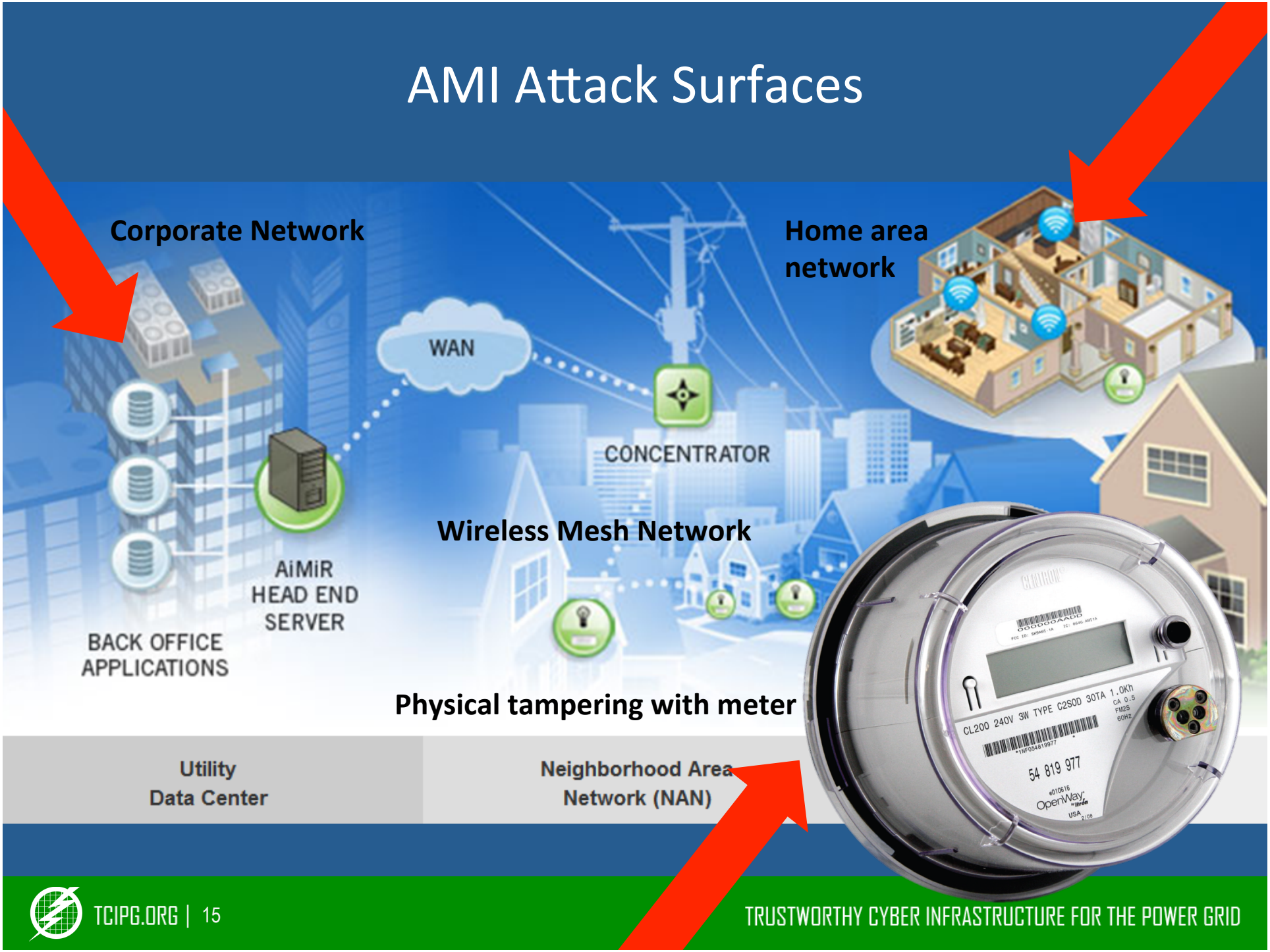
Constraints

- Long term deployment
  - Life cycle of 5 to 15 years (vs. 2-3 years in IT)
- Meters have low-computational power
- Limited network bandwidth
- Limited information about attacks
- Security solutions should be:
  - Non-intrusive
  - Low maintenance

Cyber Security Threats

- Motivations:
  - Energy fraud
  - Denial of service
    - Extortion
  - Power Disruption
    - Targeted remote disconnect
    - Large-scale outages and instability
  - Stealing personal information
  - Abuse of communication infrastructure
  - Loss of customer trust and adoption

AMI Attack Surfaces



Smart Meter Vulnerabilities

- Communication protocol vulnerabilities
  - Routing
  - Configuration
  - Name service
- Software and firmware vulnerabilities
- Hardware vulnerabilities
- Read and write access to data storage
- Access to encryption keys
- Weak random generator
- Lack of replay protection

Password sent clear over optical port
Usage data not integrity protected

Replaced anti-tampering seal

Password stored in clear in EEPROM

Encryption key derived from password

Replayed authentication and spoofed meter

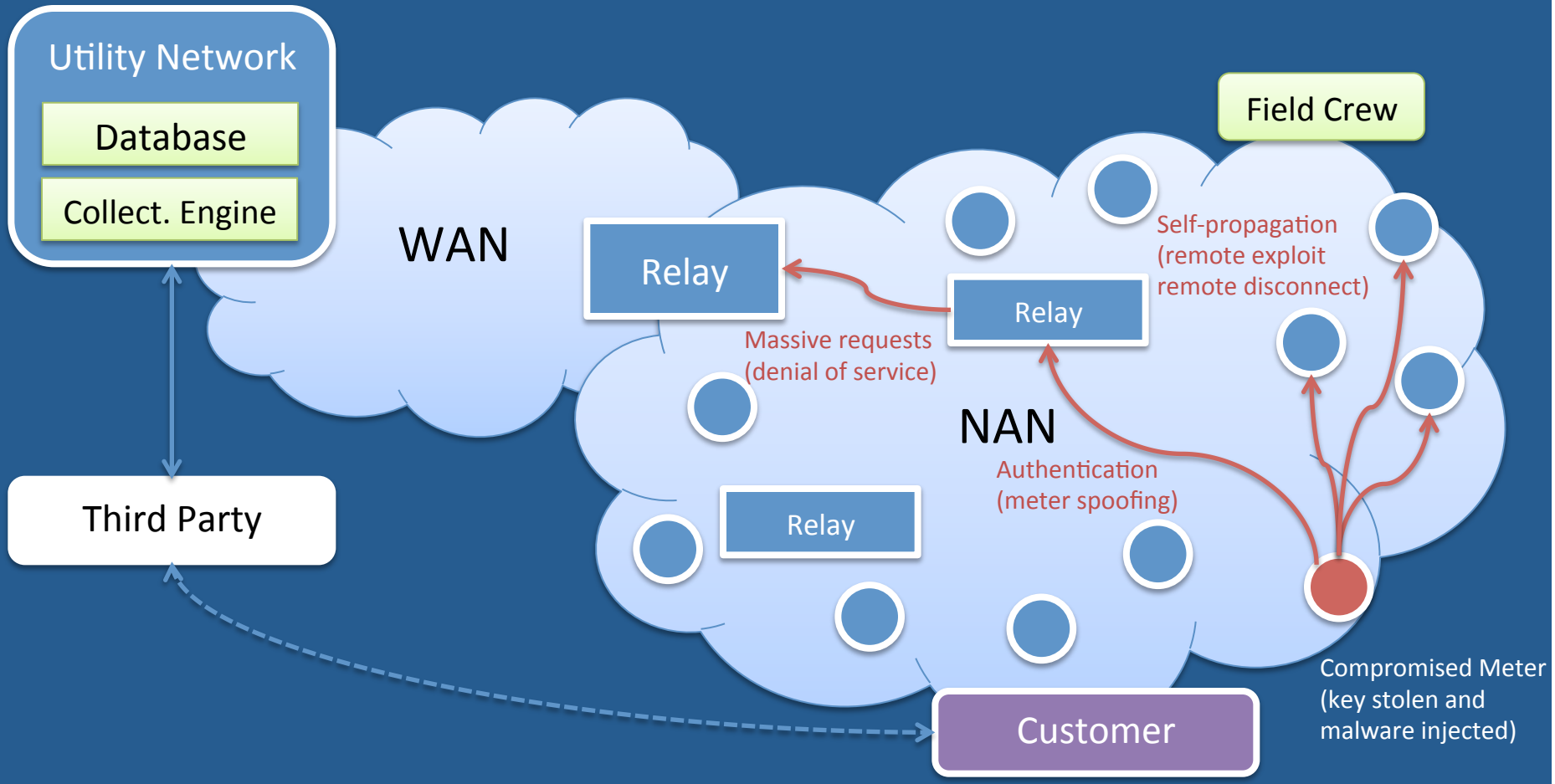
Multi-vendor Penetration Testing in the Advanced Metering Infrastructure (2010), and *Energy Theft in the Advanced Metering Infrastructure* (2009) by S. McLaughlin et al.

Smart Meter Vulnerabilities (cont.)

- Communication protocol vulnerabilities
  - Routing
  - Configuration
  - Name service
- Software and firmware vulnerabilities — Local variables promoted to global; Vulnerable to buffer overflow
- Hardware vulnerabilities — Very small stack space, no memory protection; Vulnerable to timing attacks
- Read and write access to data storage — "r/w" flag often disabled
- Access to encryption keys
- Weak random generator
- Lack of replay protection

Smart meter worm developed and tested by IOActive (BlackHat 2009)
Self-replicating and self-propagating code

Cyber Security Threats to AMI



WAN: Wide Area Net., **NAN**: Neighborhood Area Net.
PLC: Power Line Comm.

Smart Meter

Multi-layered Security Approach

- Prevention
  - Authentication
  - Encryption
- Detection
  - Meter alarms/logs
  - Intrusion detection
- Response
  - Access control lists
  - Credentials/keys update
  - Firmware update

*Building a **resilient** architecture requires to implement all three*

Multi-layered Security Approach

- Prevention
  - Authentication
  - Encryption
- Detection
  - Meter alarms/logs
  - Intrusion detection
- Response
  - Access control lists
  - Credentials/keys update
  - Firmware update

Multi-layered Security Approach

- Prevention
  - Authentication
  - Encryption
- Detection
  - Meter alarms/logs
  - Intrusion detection
- Response
  - Access control lists
  - Credentials/keys update
  - Firmware update

Critical need for smart automated response

- *Complexity of large-scale distributed systems*
- *Efficiency of automated attacks*
- *Reduction of response cost and time*

Work Plan

1. Understand possible response actions
   → Identify a taxonomy of AMI-specific actions

2. Understand safety/cost/benefit tradeoffs of actions
   → Define a cost model

3. Test and study practical deployment
   → Implement automated responses in TCIPG testbed

RESPONSE ACTION TAXONOMY

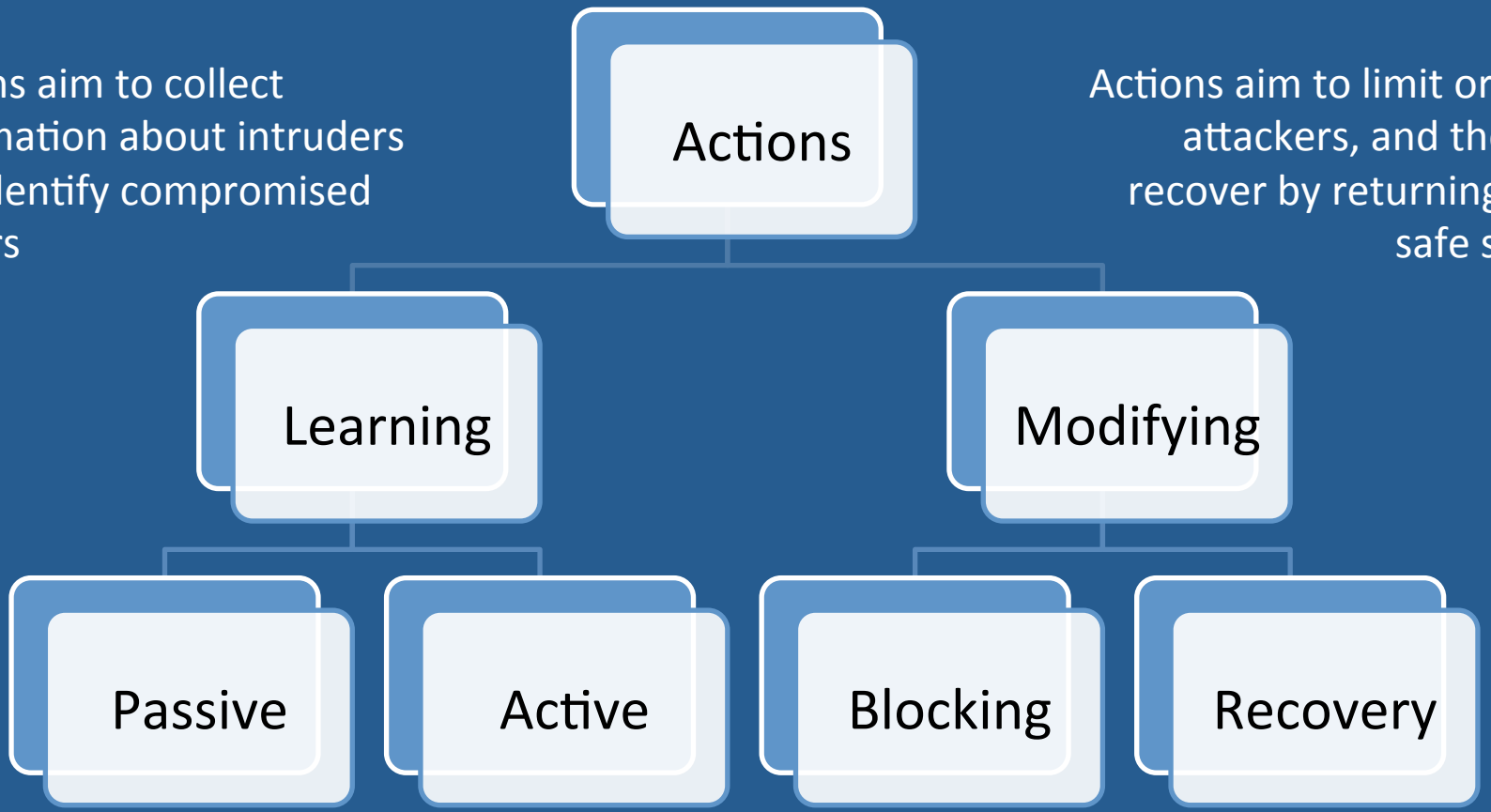
Response Action Taxonomy

- Comprehensive response classification
  - Ensures coverage and completeness
- Customized for AMI
  - Cooperative actions among meters
  - Tunable response intensity
  - Special AMI recovery actions
- Understand characteristics of actions
  - Important for cost computation

Response Actions Taxonomy

Actions aim to collect information about intruders and identify compromised meters

Actions aim to limit or stop attackers, and then to recover by returning to a safe state.



Response Action Tags

- Response rollback
  - Reversible
  - Irreversible with removable effects
  - Irreversible
- Operation Layer
  - System-wide
  - Network Layer
  - MAC Layer

Response Action Tags

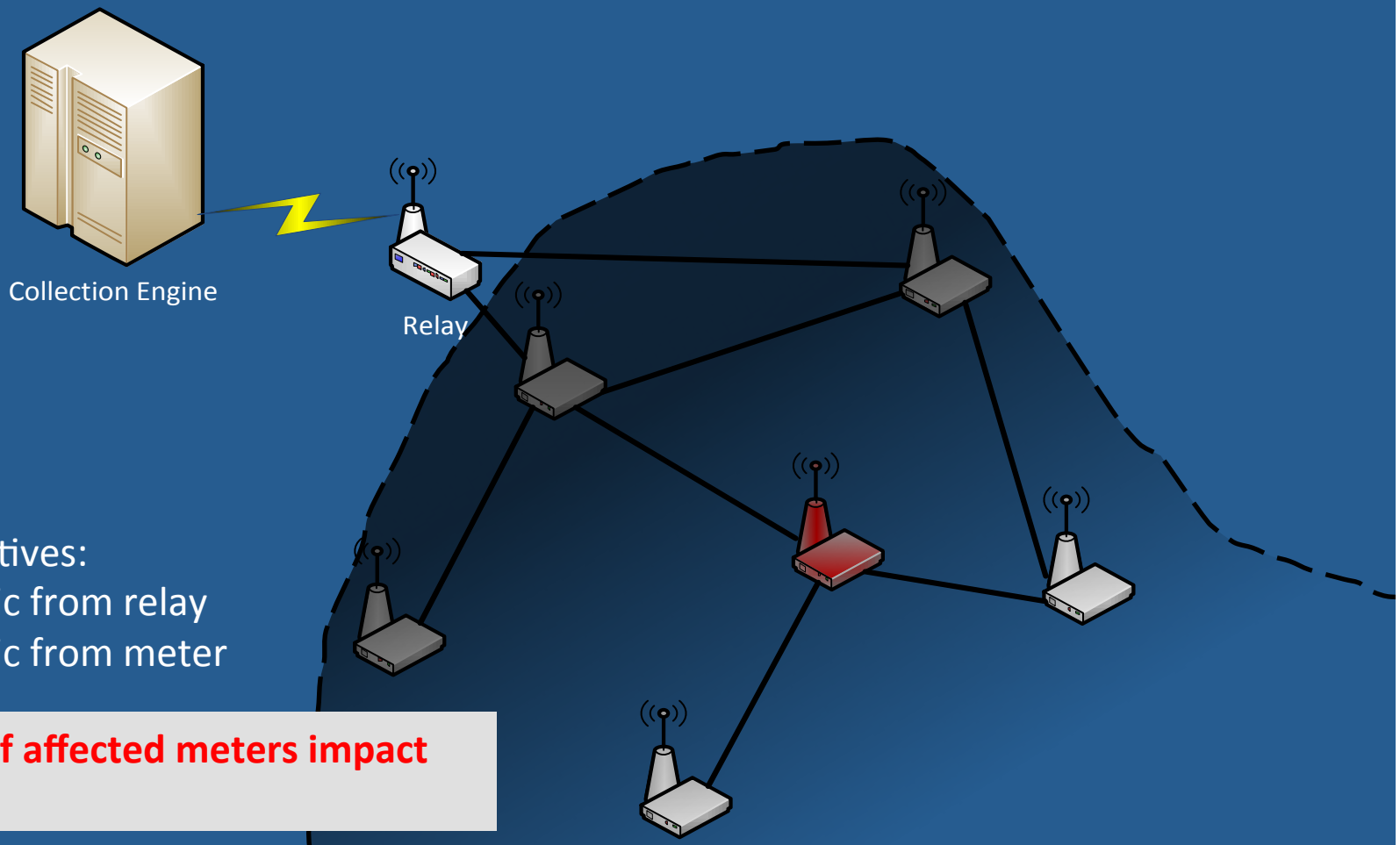
- Resources Involvement
  - Multiple meters
  - Single meter
  - Cooperative
- Admin Involvement
  - Fully automated
  - Requires admin input
- Response flexibility

(Subset of the) Taxonomy

		Action	Rollback	Layer	Resources	Admin Involvement
Learning	Passive	Generate reports	N/A	System	Multiple	Automated
		Alarm	N/A	System		Automated
		Profile customers' power usage to detect anomalies	N/A	System	Multiple	Automated
	Active	Start analysis tools	N/A	Network	Multiple	Automated
		Verify ARP table entries (MAC-device mappings)	N/A	Network	Multiple	Automated
		Detect duplicates by probing the network	N/A	Network	Cooperative	Automated
		Send probe packets to test routes	N/A	Network	Cooperative	Automated
		Add decoy nodes	R	System		Automated
Modifying	Limiting	Isolate neighborhood	R	System	Multiple	Semi-automated
		Firewall rule at collector	R	Network	Single	Automated
		Blocking connections	IR	Network	Single	Automated
		Limiting network access	R	Network	Single	Automated
		Rate limiting network traffic	R	Network	Single	Automated
		Enabling quarantine / jail environment	R	System	Multiple	Automated
	Recovery	Merge neighborhood network temporarily	R	System	Multiple	Semi-automated
		Distribute attack signature	IR	System	Cooperative	Automated
		Verify C12.22 routing tables	N/A	Network	Cooperative	Automated
		Apply patch	IR	System	Multiple	Semi-automated
		Replace meter (physically)	IR	N/A	Single	Semi-automated
		Recover meter readings	N/A	N/A	Multiple	Automated
		Turn on/off service (recover attack)	R	N/A	Multiple	Automated

COST MODELING OF RESPONSE ACTIONS

Why does it matter?



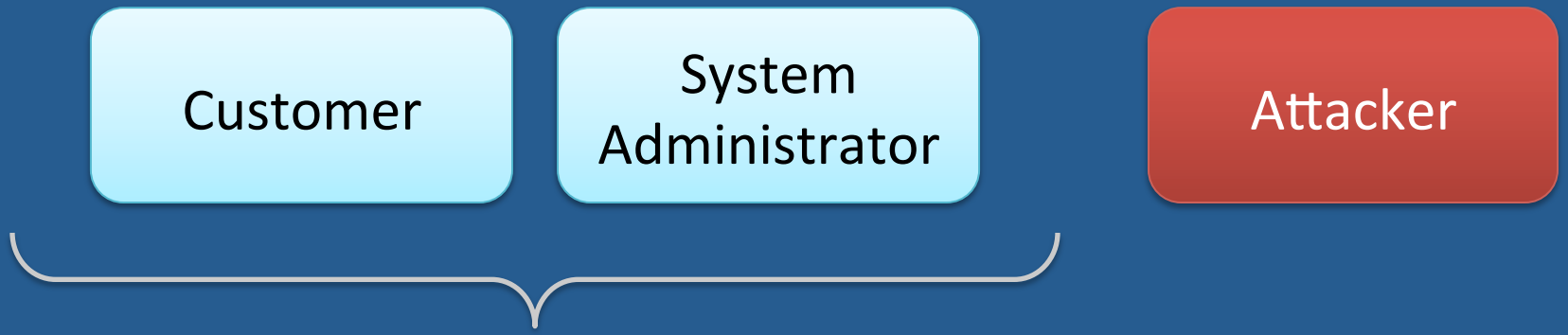
Action alternatives:

a. Block traffic from relay
b. Block traffic from meter

The number of affected meters impact the cost

Effect of an Action

- Three entities involved



Goal is to compute the *cost* of a response action using system model, taxonomy, action tags and attack tree

Cost for Legitimate Entities

Cost Parameters

- Operation Cost
- Impact on Services (CIA)
- Effectiveness
  - Cost of Attack
  - Benefits
- Recovery time
- Response deployment period (TTL)
- Action parameters (flexible actions)
- Computation time/cost (real-time deadlines)

Current Approaches

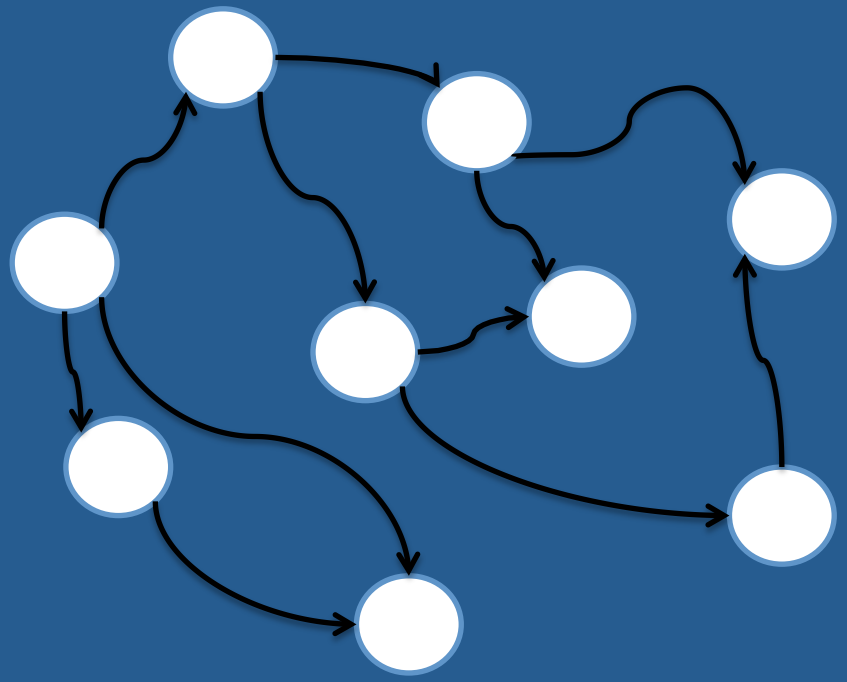
Current approaches capture a partial image

- Static costs mapped to actions
  - Systems dynamics alter the effect of an action
- Parameterized cost
  - Operation cost, damage cost, response goodness and impact (static parameters)
  - Ensures better coverage but does not capture system dynamics
- Resource dependency model
  - Capture dynamics but leads to an incomplete cost value

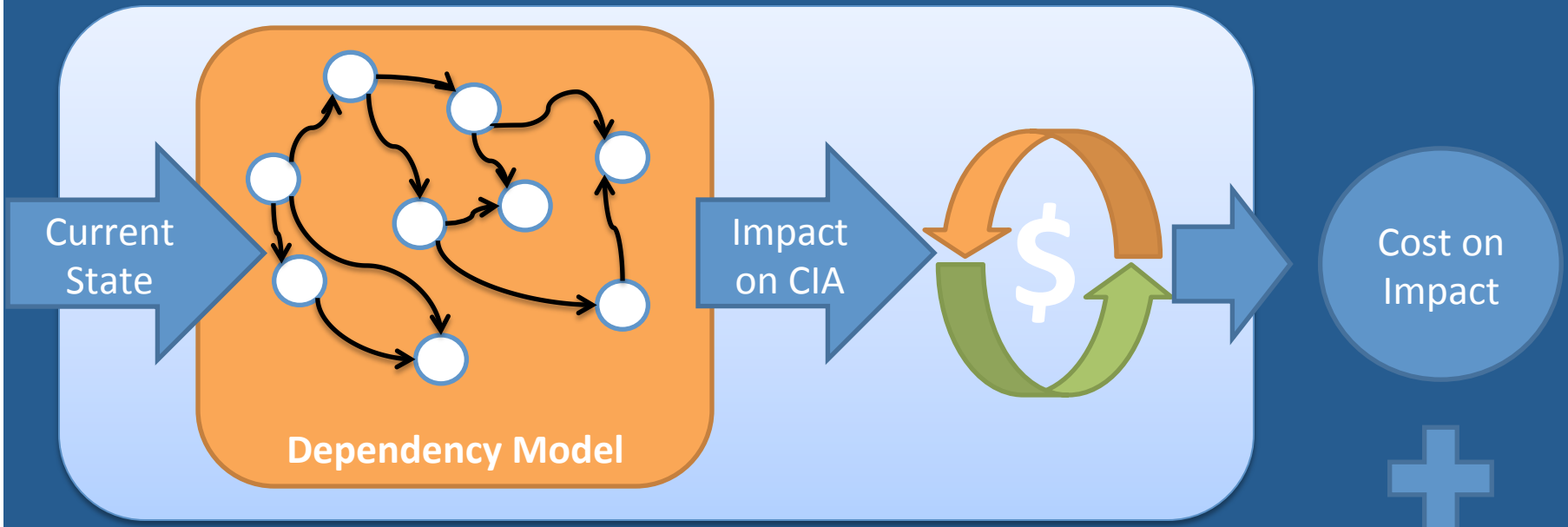
Computing Effect on CIA

- System modeled using *Dependency graph G=(V,E)*
  - V set of resources
  - E set of edges (*r, s*) representing relation
- Resources labeled with dysfunction rate vector

  Vr[C,I,A]
- Each edge labeled with a degree matrix $W_{r_i r_j} = (w_{r_i r_j}(1,1) \; w_{r_i r_j}(1,2) \; w_{r_i r_j}$



Comprehensive Cost Approach



Response Cost = Recovery Cost + Labor Cost + Operation Cost

Cost Effectiveness

Taxonomy characterizes two high level type

- *Learning*: leaves attack running
- *Modifying*: activity tackles attack

Impact of attack on system

- Model attacker (Möbius ADVISE model)
  - Objectively simulates multiple adversary models
- Probabilistic attack costs
  - Tag attack trees with costs
- Historic data
  - Not enough for complete cost model

Converting Impact for AMI Services

Block meter

- Stops all services between user and utility
- Temporarily interruption as routes are generated

Verify route integrity

- Delays "service packets" due to extra traffic

Attack/Response Action Cost Breakdown

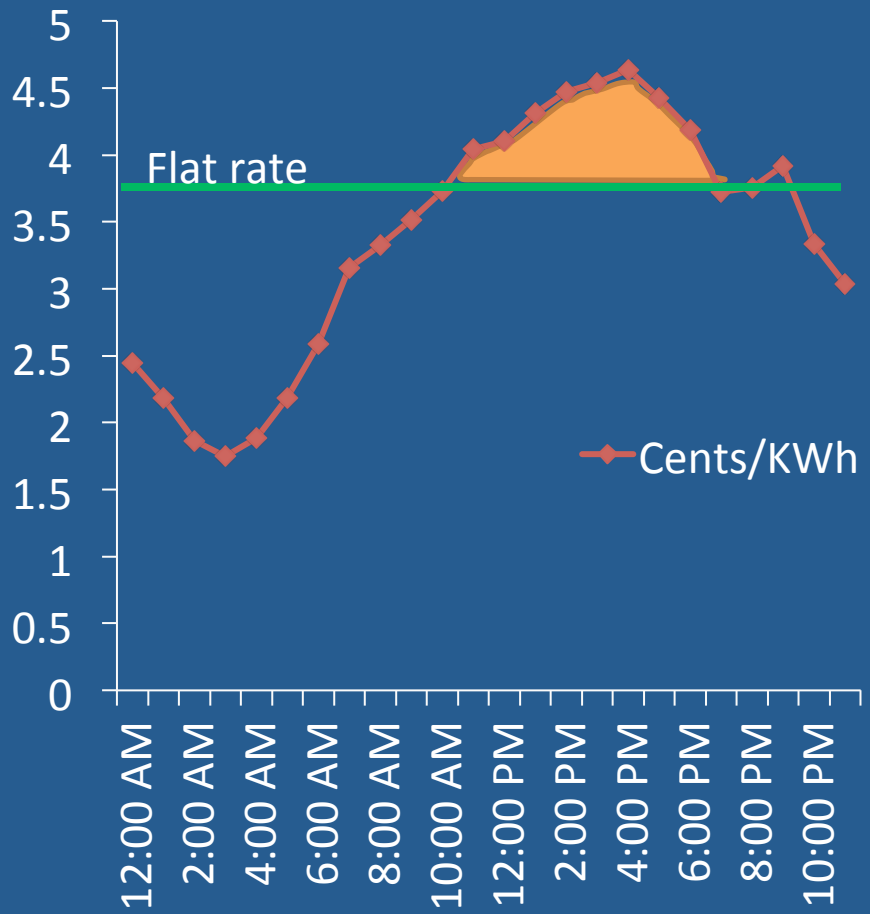
For each element in the grid the cost is computed for both the *administrator* and *customer*

Availability for Pricing Information

- Customer uses flat rate in case of unavailable pricing information

- *Flat rate<Market rate*
  - Utility loses revenue
- *Flat rate>Market rate*
  - Customer overcharged

$$Cost = \Delta(price) \times Usage$$



Integrity of Pricing Information

- Action increases rate
  - Customer dissatisfaction
- Action lowers rate
  - Customer over billed (legal action)
  - Increase demand for power
    - Rate increase
    - Generation perturbations

Impact on Meter Readings

- Availability
  - SLA penalty
  - Delay in EMS usage profiles
- Integrity
  - Energy theft or overbilling customer
  - Misleading usage profiles

Impact on Service Commands

- Availability
  - SLA penalty
  - Customer dissatisfaction due to delays in utility services (turning on power, blackouts detection,…)
- Integrity
  - Extra labor and operation costs due to false positives
  - Cost increase for the customer

Cost of Confidentiality

- Compromised confidentiality
  - Leads to invasion to privacy through load profiling
- Legal action and lost confidence
- Current surveyed SLAs *do not* contain provisions for confidentiality

Provisions for Service Level Agreements

- Availability

  Guarantee that usage data, commands and pricing arrive in a timely manner within regular load

- Integrity

  Guarantee that X% of usage data, commands and pricing are not tampered

- Confidentiality

  Guarantee that X% of usage data privacy is not compromised

Cost for Attacker

- Stop attack
  - Block compromised entities
- Slow down attack
  - Rate limiting of compromised entities
- Facilitate attack
  - Misdiagnosis or misconfigured response
  - Collect information on the attacker and the strategies used

IMPLEMENTATION & DEPLOYMENT

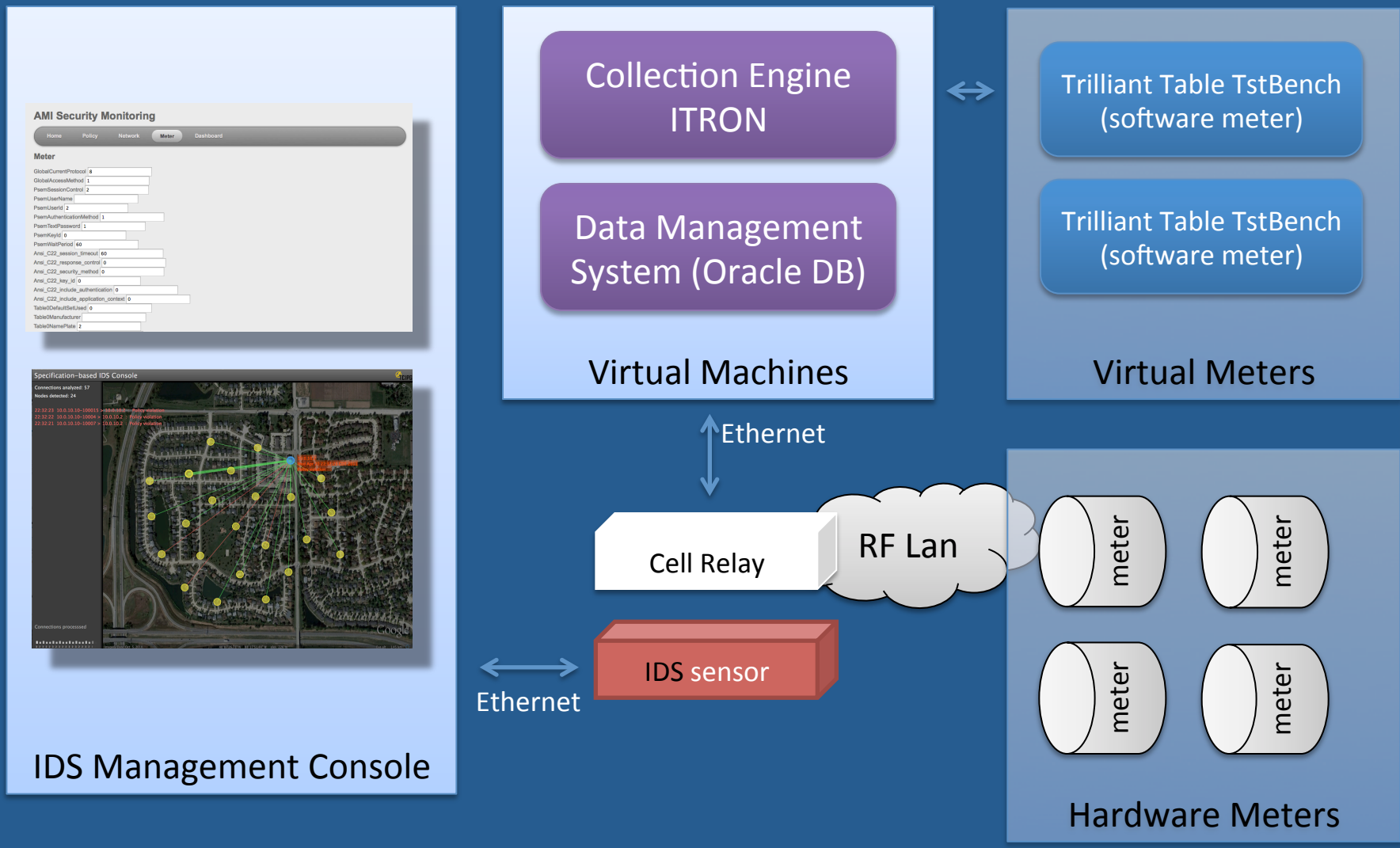
Framework

- Intrusion response systems can be based on:
  - Heuristics
  - Machine learning
  - Game theory

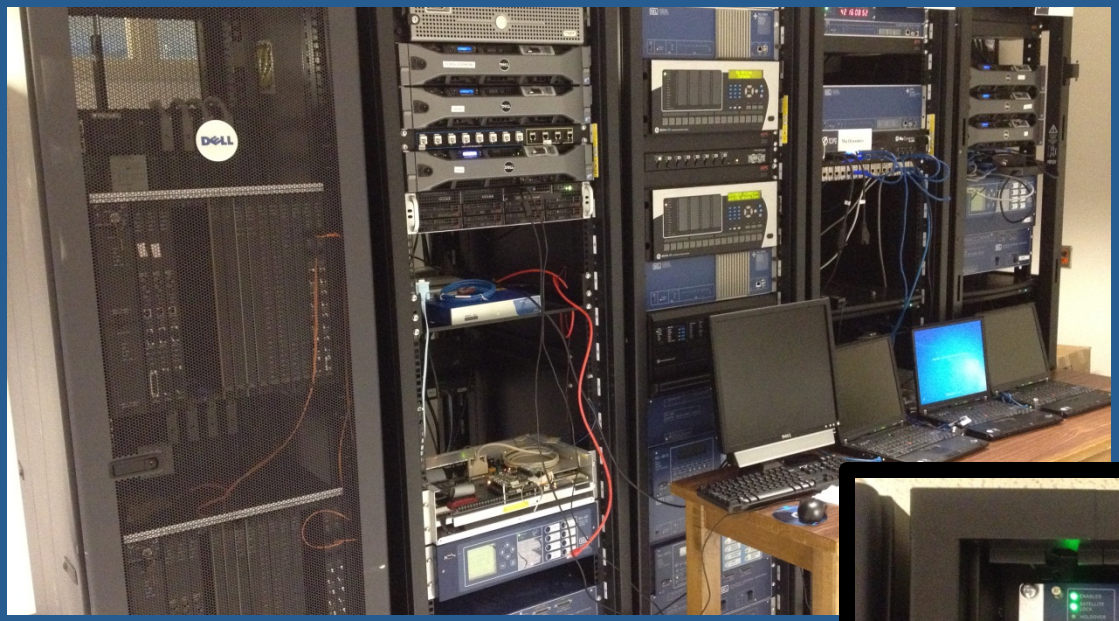
Recovery and Response Engine (RRE)

- Assumes security game between attacker and defender
- Uses an Attack-Response tree to model system
- Computes the optimal response strategy that minimizes the cost for an administrator
- $r(s,a,s') = (\delta_g(s) - \delta_g(s'))^{\tau_1} \; C(a)^{\tau_2}$
  - **C(a)** is the cost function introduced by our cost model

AMI Testbed Architecture

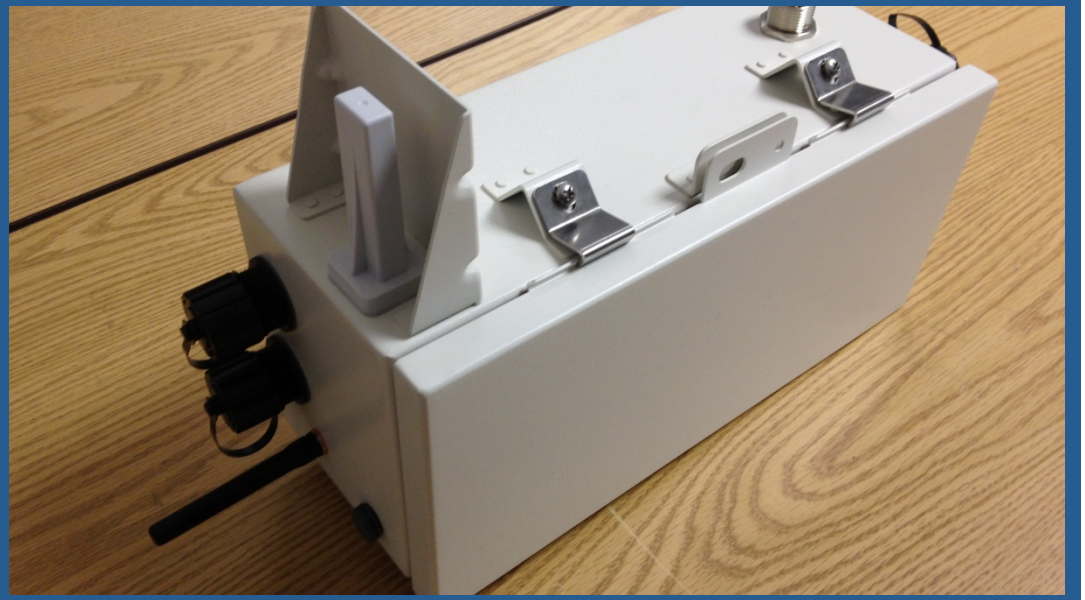


Testbed



Testbed


CL200 240V 3W TYPE C2S0D 30TA 1.0K
MARKETING SAMPLE
306 382 308
PELIGRO



FUTURE WORK AND RESEARCH QUESTIONS

Future Work

- Automate the assignment of weights in dependency model using minimum administrator input
- Automate the generation of relations between CIA
- Complete case study by defining models for the different security implications
- Design a “security inspired” metering SLA
- Complete implementation in RRE framework
- Initiate testing within testbed using realistic AMI
- Optimize performance

Safety

- Attackers can drive automated responses by triggering IDS sensors
- A separate unit to include the admin to the loop in the case for some specified actions
- Actions with safety issues should be semi-automated
  - Provide a choice for the admin with alternatives
- Define a safety criterion for AMI

Research Questions

- Design modular response actions and cost model
  - Ensures compatibility with different technologies and implementations
- Automate generation of response actions
- Propose Performance metrics for automated responses

Conclusion

- Formed a response action taxonomy with learning and modifying categories
- Current cost models rely on subjective administrator parameters or static values
- Defined response cost model to include parameters from the taxonomy
- Map response parameters to monetary values using SLAs and other cost factors
- Plan to implement automated response for AMI testbed

Questions?

Robin Berthier rgb@illinois.edu

Ahmed Fawaz afawaz2@illinois.edu

William H. Sanders whs@illinois.edu