

Analyzing Resiliency of Smart Grid Communication Architectures under Cyber Attacks

Anas Al Majali, Arun Viswanathan and Clifford Neuman

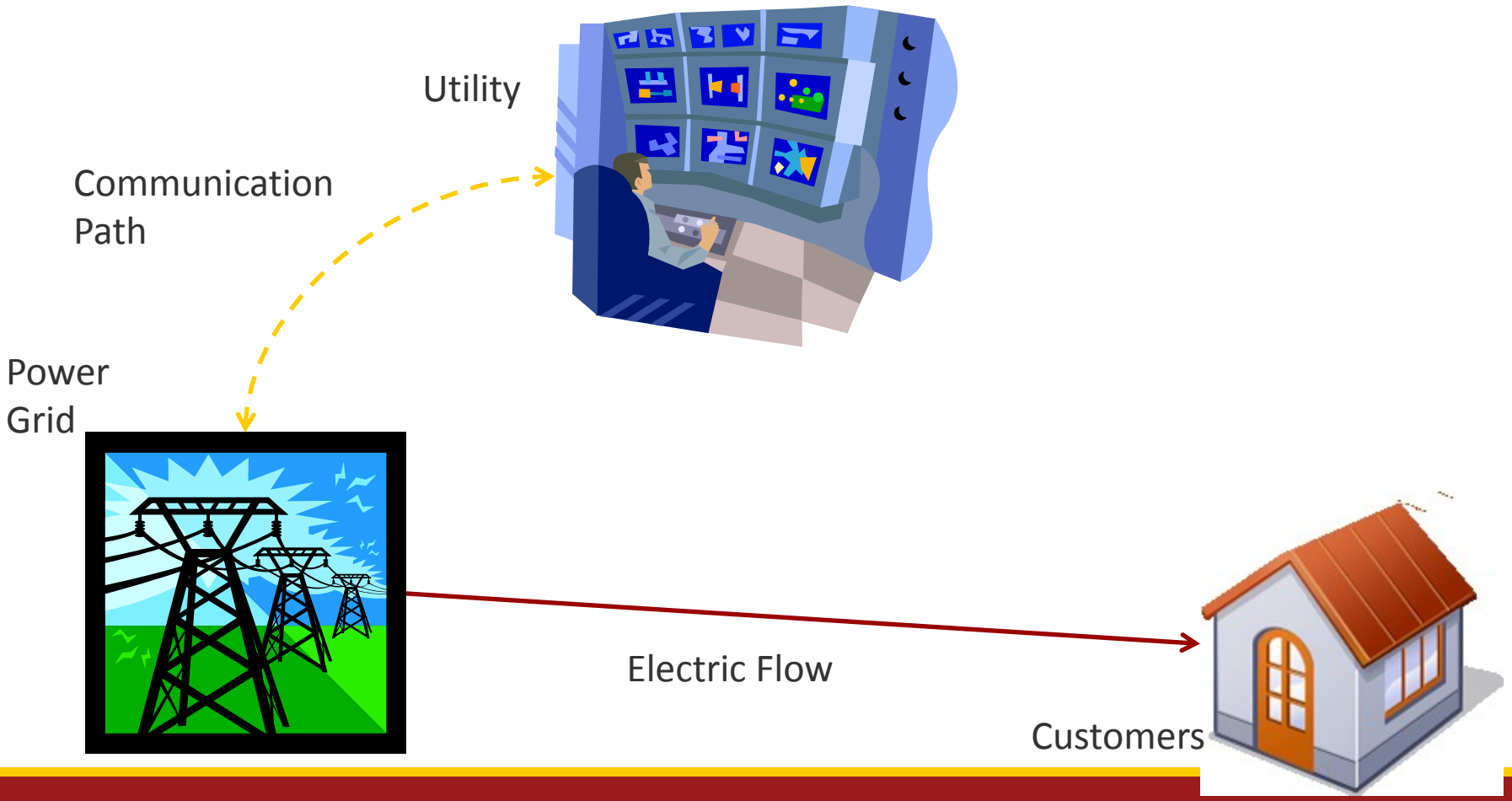
USC/Information Sciences Institute



Part I

Quick Overview

Power Grid


Utility
Communication Path
Power Grid
Electric Flow
Customers

Smart Grid



Utility

Communication Path

Bidirectional communication

AMI:
Advanced Metering Infrastructure

Power Grid



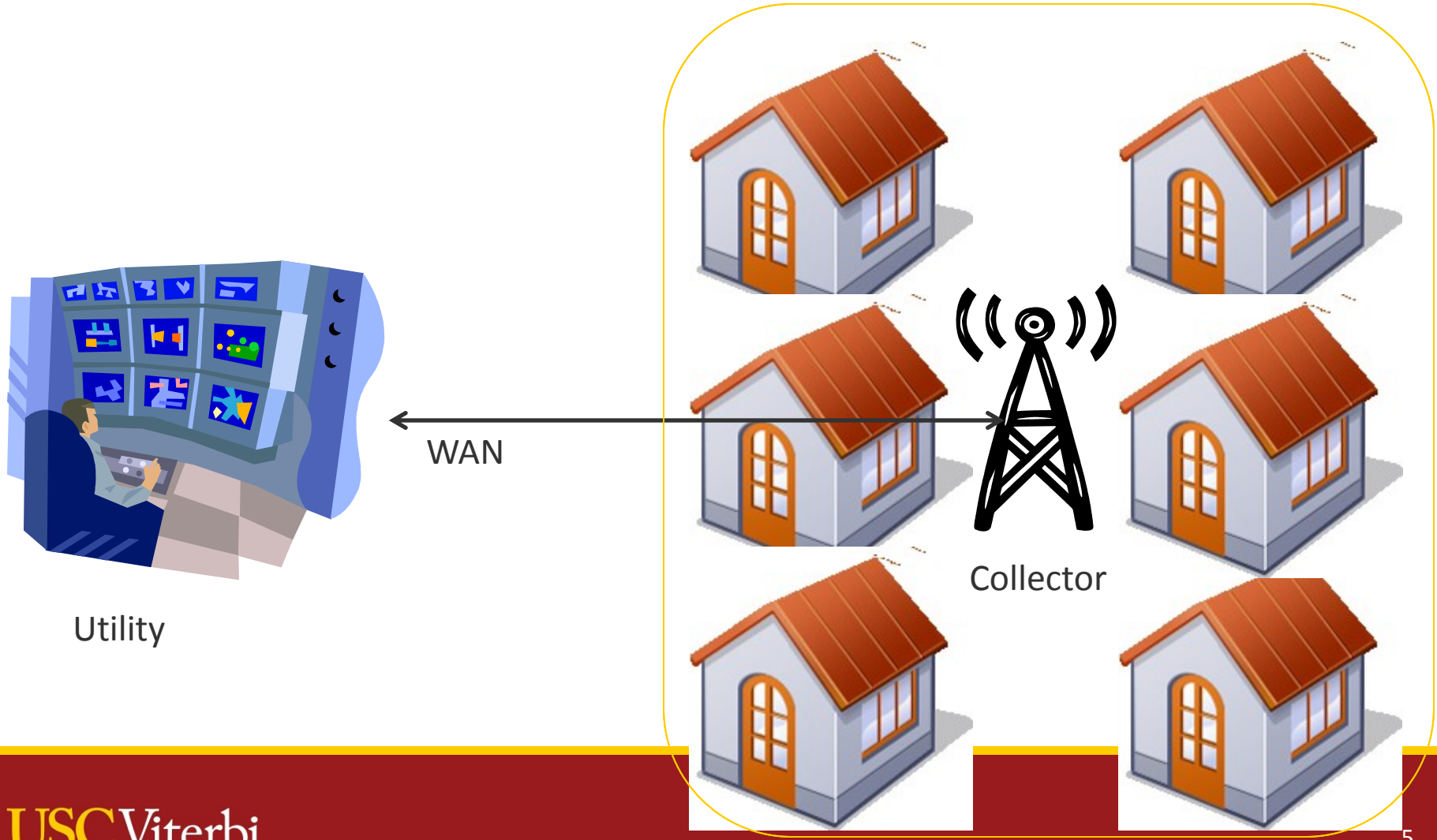
RF mesh:
Radio Frequency mesh

Electric Flow

Customers



RF Mesh



Objective

- Our objective is to experimentally evaluate the operational resiliency of the smart grid in terms of the higher level functions on which it depends and the communication architecture that underlies those higher level functions, under cyber attack on the communication architecture.

Resiliency

Our objective is to experimentally evaluate the operational resiliency of the smart grid in terms of the higher level functions on which it depends and the communication architecture that underlies those higher level functions, under cyber attack on the communication architecture.

- *Operational Resiliency is the capability of a system to fulfill its mission in a timely manner, even in the presence of attacks or failures.*

Methodology

Our approach consists of:

1. Modeling an RF mesh communication network deployed in a typical smart grid region using ns-2.
2. Simulating the behavior of higher-level smart grid functions.
3. Analyzing the performance of those functions under a DoS attack on the communication infrastructure.

Key Finding

It requires an attacker to compromise only a small fraction of the meters in a typical RF mesh region to disrupt the communication resilience within the region.



Part II

Detailed Discussion

Outline

- **Part II**
  - Objective
  - Resiliency
  - Methodology
  - Results
  - Lessons Learned
  - Conclusion

Outline

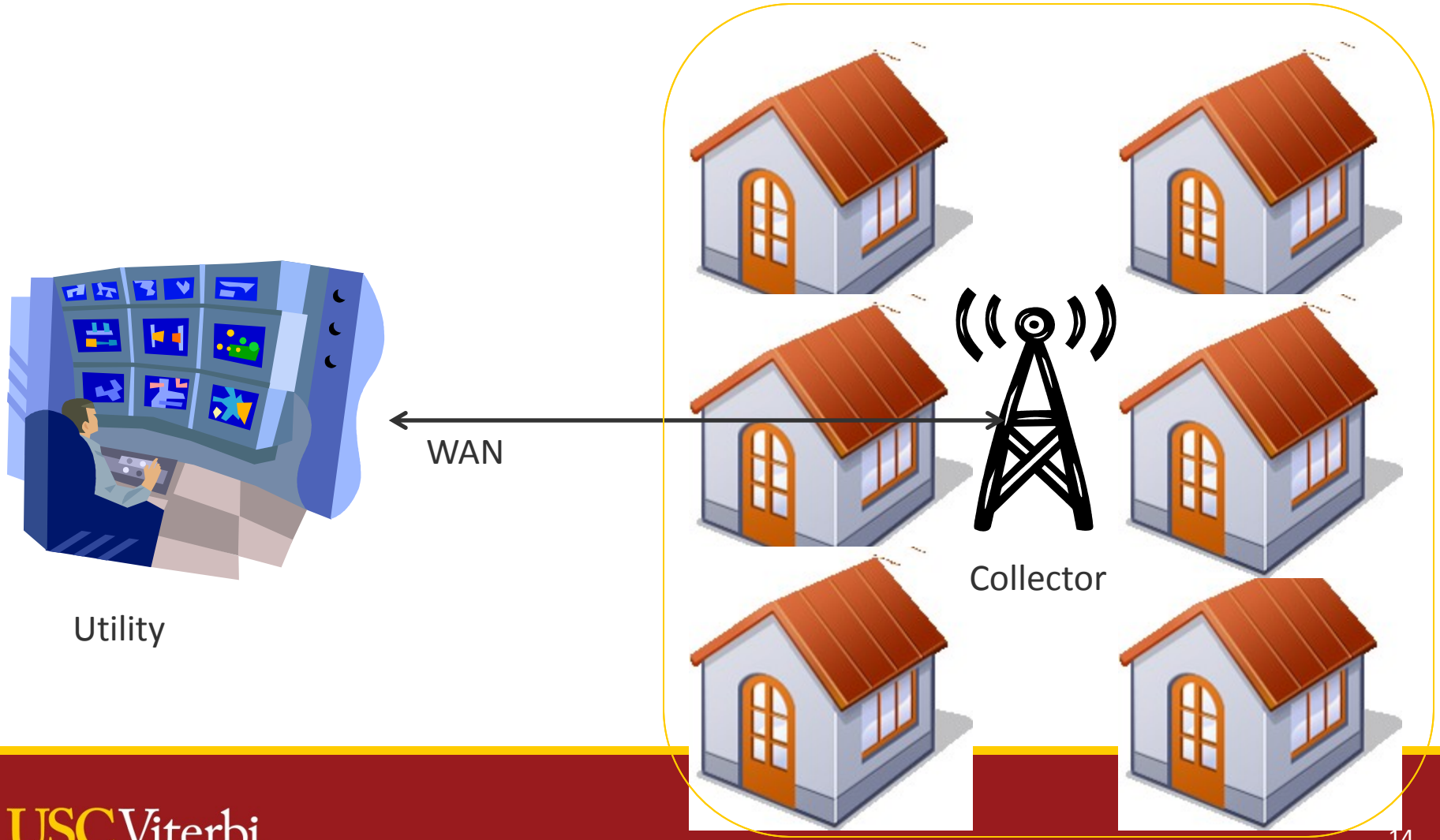
- **Part II**
  - Objective
  - Resiliency
  - Methodology
  - Results
  - Lessons Learned
  - Conclusion

Resiliency (revisited)

- Our objective is to experimentally evaluate the operational resiliency of the smart grid in terms of the higher level functions on which it depends and the communication architecture that underlies those higher level functions, under cyber attack on the communication architecture.

- *Operational Resiliency is the capability of a system to fulfill its mission in a timely manner, even in the presence of attacks or failures.*

RF Mesh (revisited)



Higher-level Functions

- Our objective is to experimentally evaluate the operational resiliency of the smart grid in terms of the higher level functions on which it depends and the communication architecture that underlies those higher level functions, under cyber attack on the communication architecture.

Functional View of the Smart Grid Layers

Smart Metering

Automated readings and remote meter management

Demand Response

Dynamic load Management

Outage Management

Automated outage detection

Electric Vehicles

Automated (dis)charging based on dynamic pricing signals

Cyber Security

Protects the smart grid against cyber threats and failures

AMI Communication Layer

Combination of wireless, cellular and wired Networks providing communication services between utilities and consumers

Physical Power Grid

Delivers power to the end consumers

Resiliency of Smart Grid Functions

- Remote Metering is resilient if:
  - Data from some percentage of the meters is always delivered to the utility within a bounded time.
- Demand Response is resilient if:
  - Required kWh of load is always curtailed within a bounded time.
- Cyber Security component is resilient if:
  - It always detects and responds to security threats before performance and security requirements of other functions are violated.

Measuring Communication Resiliency



- **Packet Delivery Ratio (PDR)**
  - Defined as the number of packets successfully received by a receiver over the expected number of packets.
- **Average End-to-end Delay**
  - Defined as the average time taken for packets to be transmitted from the sending application to the receiving application.
- **Average Packet Hop Count**
  - Defined as the average number of intermediate nodes through which the packets sent by a sender are routed. In the case of an RF mesh-based network, the average hop count measures the number of meters traversed by a packet before it reaches the receiver.
- **Successful DR Requests Ratio**
  - Defined as the number of DR requests that successfully receive a reply over the total DR requests that were issued.

Outline

- **Part II**
  - Objective
  - Resiliency
  - Methodology
  - Results
  - Lessons Learned
  - Conclusion

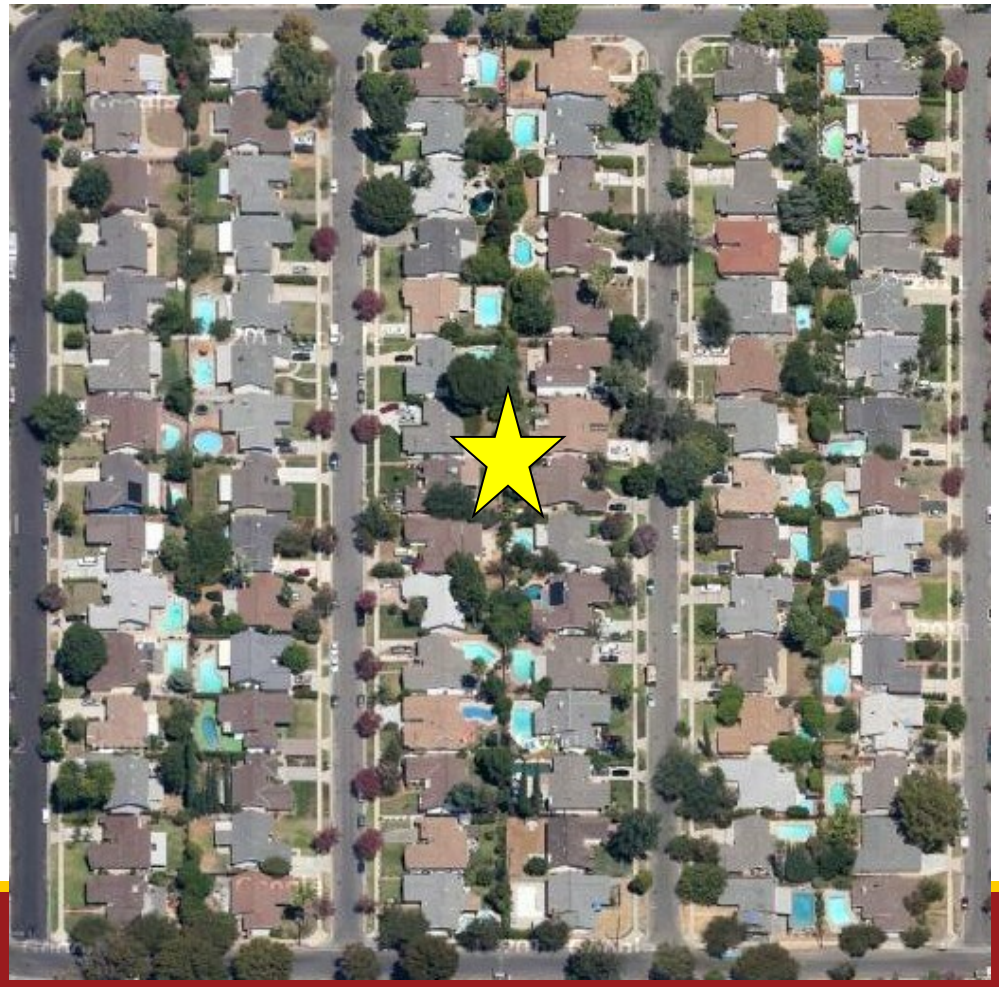
Methodology (revisited)



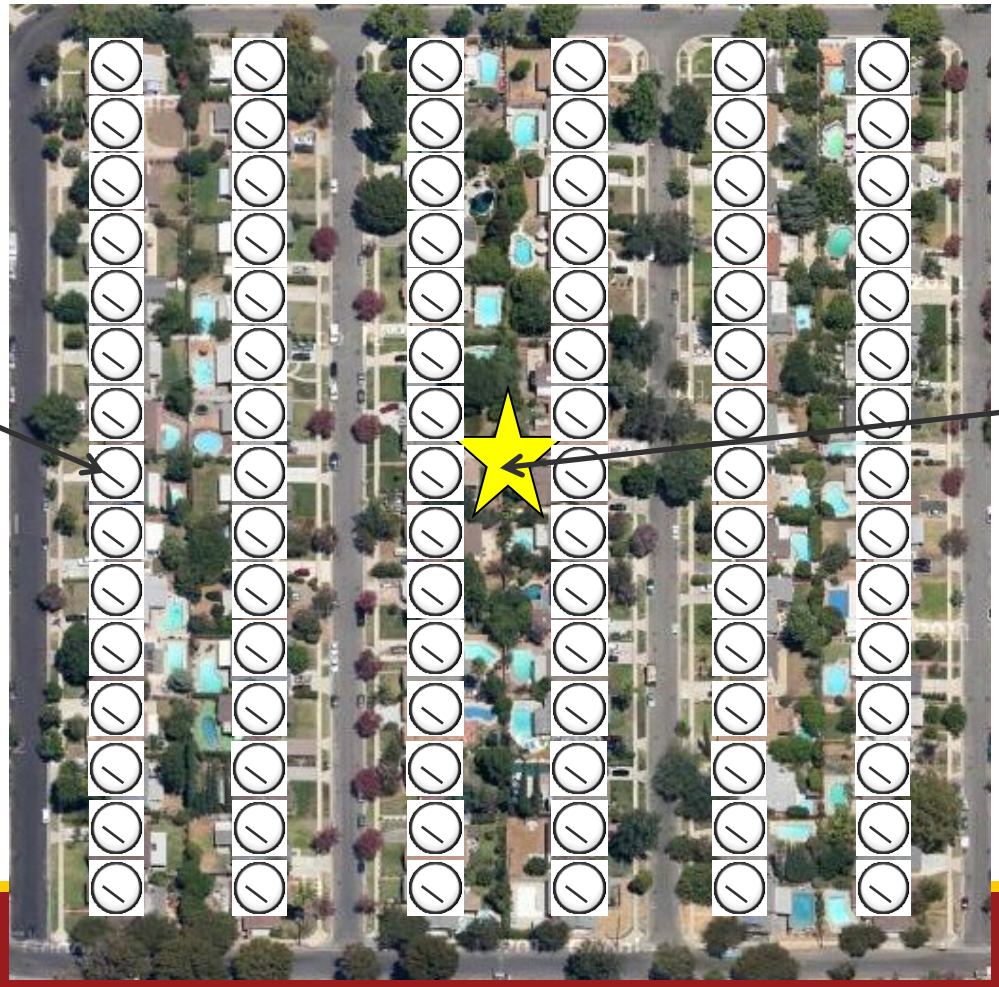
Our approach consists of:

1. Modeling an RF mesh communication network deployed in a typical smart grid region using ns-2.
2. Simulating the behavior of higher-level smart grid functions.
3. Analyzing the performance of those functions under a DoS attack on the communication infrastructure.

Experiment Topology (Meter Distribution)



Experiment Topology (Meter Distribution)



Experiment Configuration



- **Meter Configuration**: using ns-2 we configured meter nodes with parameters derived from specification of a real smart meter.

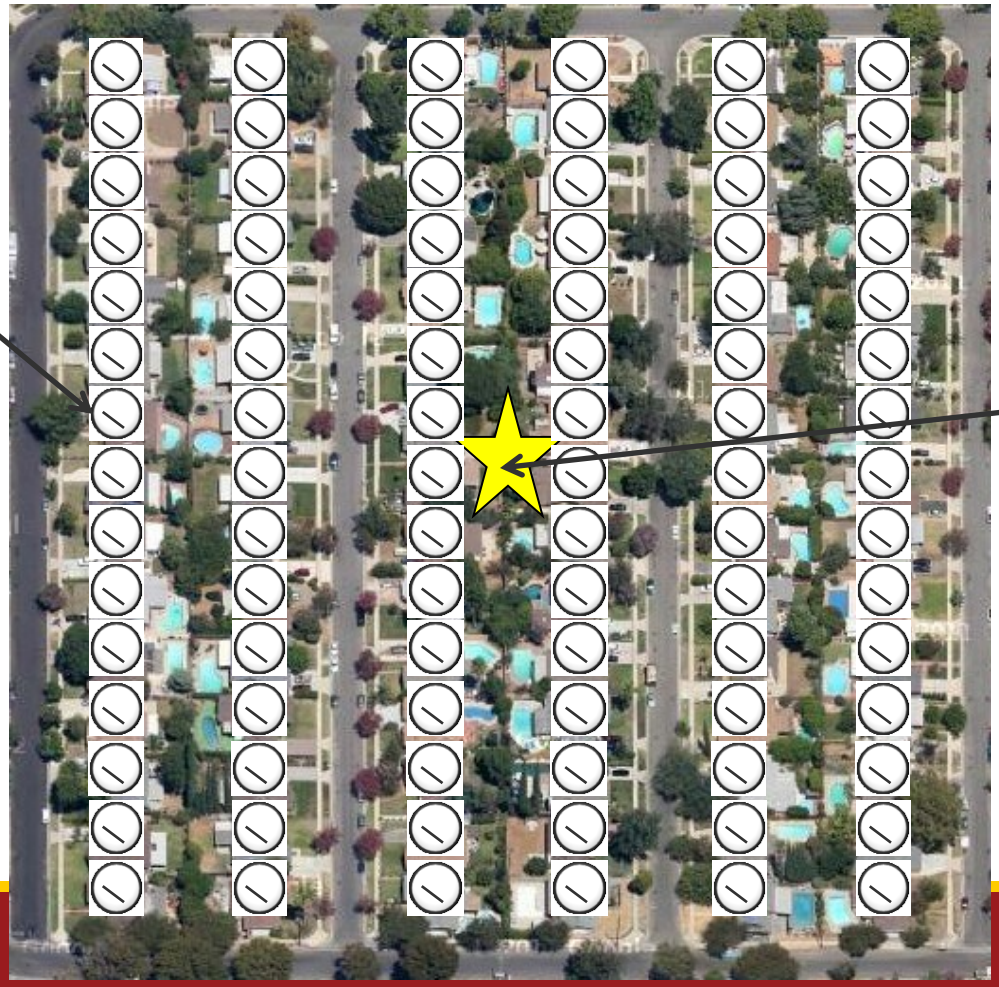
- **Propagation Model**: used the shadowing propagation model to simulate an outdoor shadowed urban area.

Experiment Procedure

- What parameters need to be configured?
  - Ad-hoc routing protocol
    - AODV: Ad-hoc On-Demand Distance Vector.
    - DSR: Dynamic Source Routing.
    - DSDV: Destination Sequenced Distance Vector.
  - Number of meters
    - 150 – 350.
  - Sending interval of the meters
    - 60, 420, 900, 1800 seconds.

Simulation of Smart Grid Functions

Meter



Smart Metering: Automated, periodic meter reads -1000 bytes every X s.

Demand Response: DR load curtailment signals. Collector-meter-collector

Collector: Responsible for conveying messages between the RF mesh and the Utility through the WAN

DoS Attack

- There are many types of attacks that can be performed on the RF mesh
  - Spoofing meter reads.
  - Manipulating meter reads.
  - DoS attack.

DoS Attack

DoS attack parameters:

1. Percentage of compromised meters.
2. Sending interval of the compromised meters



Compromised meters generate DoS attack by simultaneously sending low bit rate traffic to the collector

Compromised meter

Outline

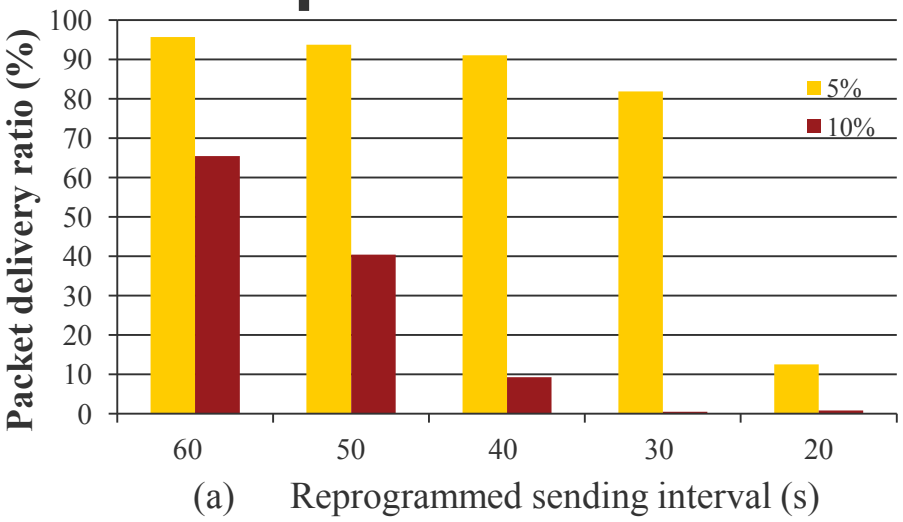
- **Part II**
  - Objective
  - Resiliency
  - Methodology
  - Results
  - Lessons Learned
  - Conclusion

Baseline Configuration

- We identify an acceptable configuration with:
  - Routing Protocol AODV
  - Number of meters 250
  - Sending interval 900 s

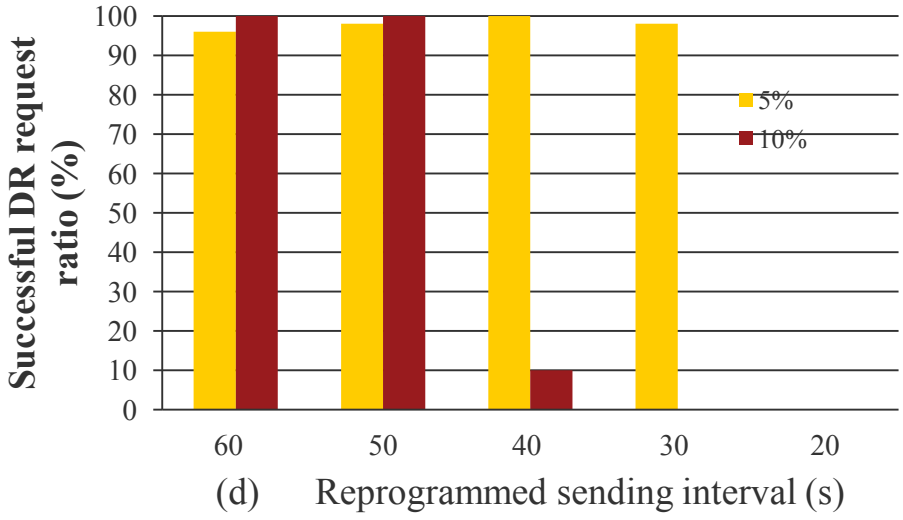
- Metrics values for this configuration:
  - PDR: 97.07%
  - Average packet end-to-end delay: 2.86 s
  - Average hop count: 2.28
  - Successful DR Requests Ratio: 100%

Experiment under DoS Attack

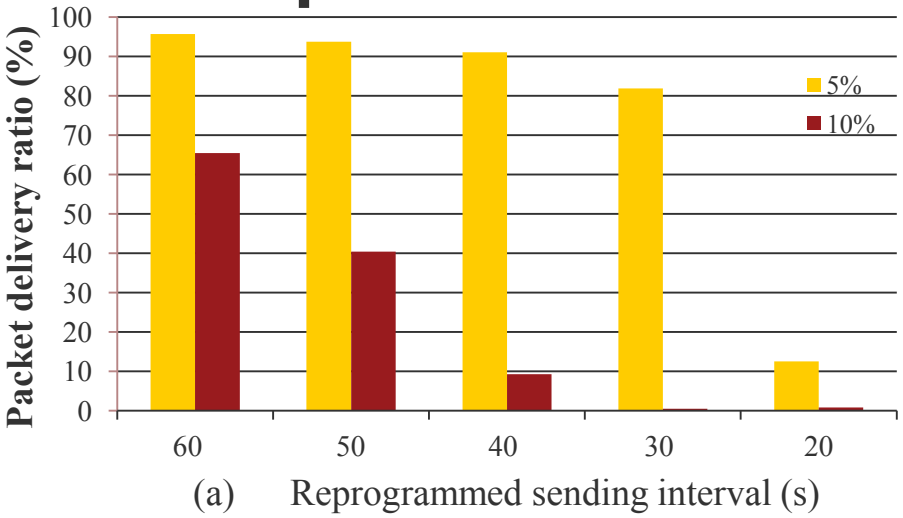


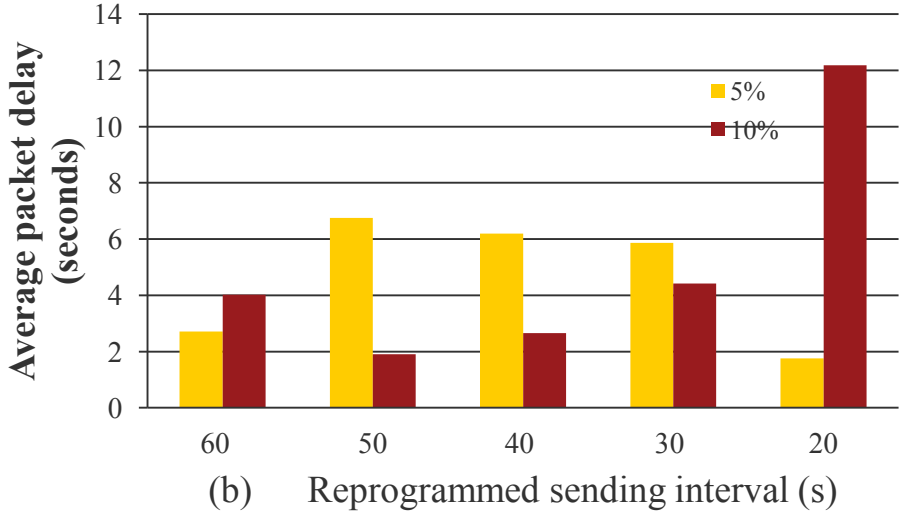
Demand Response: missing DR signals

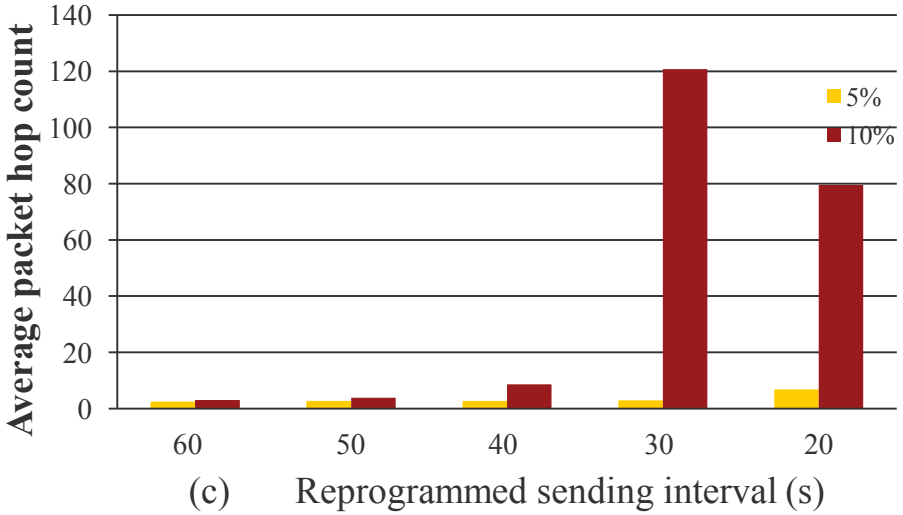
Smart Metering: missing meter reads

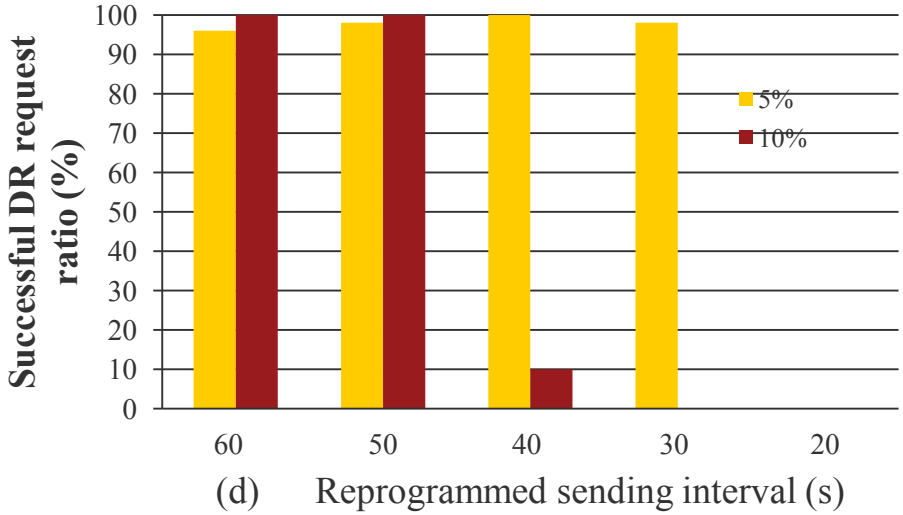


Experiment under DoS Attack









Key Finding

It requires an attacker to compromise only a small fraction of the meters in a typical RF mesh region to disrupt the communication resilience within the region.

Outline

- **Part II**
  - Objective
  - Resiliency
  - Methodology
  - Results
  - Lessons Learned
  - Conclusion

Lessons Learned

Cyber Security

Need to compromise small fraction of meters to generate DoS attack.

Function	Lessons Learned	Consequences
Smart Metering	Missing meter reads	• Billing • Load monitoring and forecasting
Demand Response	Reduced and delayed (request-response) pairs	Disrupting load management

Overall Operational Resiliency

- Consequences on the overall operational resiliency of the smart grid.
  - Utilities loose money if billing is disrupted for long time.
  - Inability to control end devices reduces “reserves”.

Recommendation:

Need to focus on the resiliency of the smart grid communication architecture



Further Discussion

What wasn't addressed?

- Other communication architectures like cellular.

- Other functions can be studied if there is enough information to model them like outage management.

Experimentation Platform

	ns-2 (Simulation)	DETER (Emulation)
Support for Wireless	✓	✓ (SWOON*: Wireless Emulation)
Scale (hundreds of nodes)	✓	✗ (for SWOON not DETER)
Real nodes (for future work)	✗	✓ (Real hardware and software)

**SWOON (Secure Wireless Overlay Observation Network)*

What new directions does this paper open?



- Simulations can help us generate traffic traces for emulating aggregate behavior of an RF mesh network on a testbed like DETER.

- This is important in a nascent domain like smart grid where there is a lack of real world traces.

What new directions does this paper open? (Cont.)



- This type of analysis can be used to evaluate the resiliency of critical smart grid functions like DR.

- The resiliency of those functions can have an important effect on the future architecture of the smart grid.

What could have been done differently?



- The RF mesh model.
  - Routing protocols.
  - Collectors and routers.

Conclusion

- We evaluated the operational resiliency of the smart grid in terms of the higher level functions on which it depends and the communication architecture that underlies those higher level functions, under cyber attack on the communication architecture.

- We quantitatively demonstrated that it requires an attacker to compromise only a small fraction of meters to violate the resiliency of the communication architecture and consequently the overall resiliency of the smart grid.