PSERC

WICHITA STATE UNIVERSITY

# Towards a Secure, Wireless-Based HAN for Metering in the Smart Grid

Vinod Namboodiri

Wichita State University

PSERC Webinar: March 1, 2011

# Context

- This is ongoing work part of PSERC **T39** Project:

  **Communication Requirements and Integration Options for Smart Grid Deployment**

  **Ward Jewell (Wichita State Univ.); Mladen Kezunovic (Texas A&M Univ.); Vinod Namboodiri (Wichita State Univ.)**

- Visvakumar Aravinthan, Vinod Namboodiri, Samshodh Sunku, Ward Jewell, *Wireless AMI Application and Security for Controlled Home Area Networks*, In Proc. of the IEEE PES General Meeting, July 2011.

# Smart Grid

Power network which has the ability to self heal from a disturbance, enables active participation by consumers in demand response, operating resiliently against physical and cyber attacks, accommodates all generation and storage options, provides power quality for the 21st century needs and optimizes assets and operating efficiency

- U.S Department of Energy

# Outline

- Introduction
- Wireless-based HANs
  - Why Wireless?
  - Communication Model
  - Selection of Technology
  - Challenges
- Towards a Secure Wireless HAN
  - Objectives
  - Threats and Solutions
  - SecureHAN Framework
- Future Work

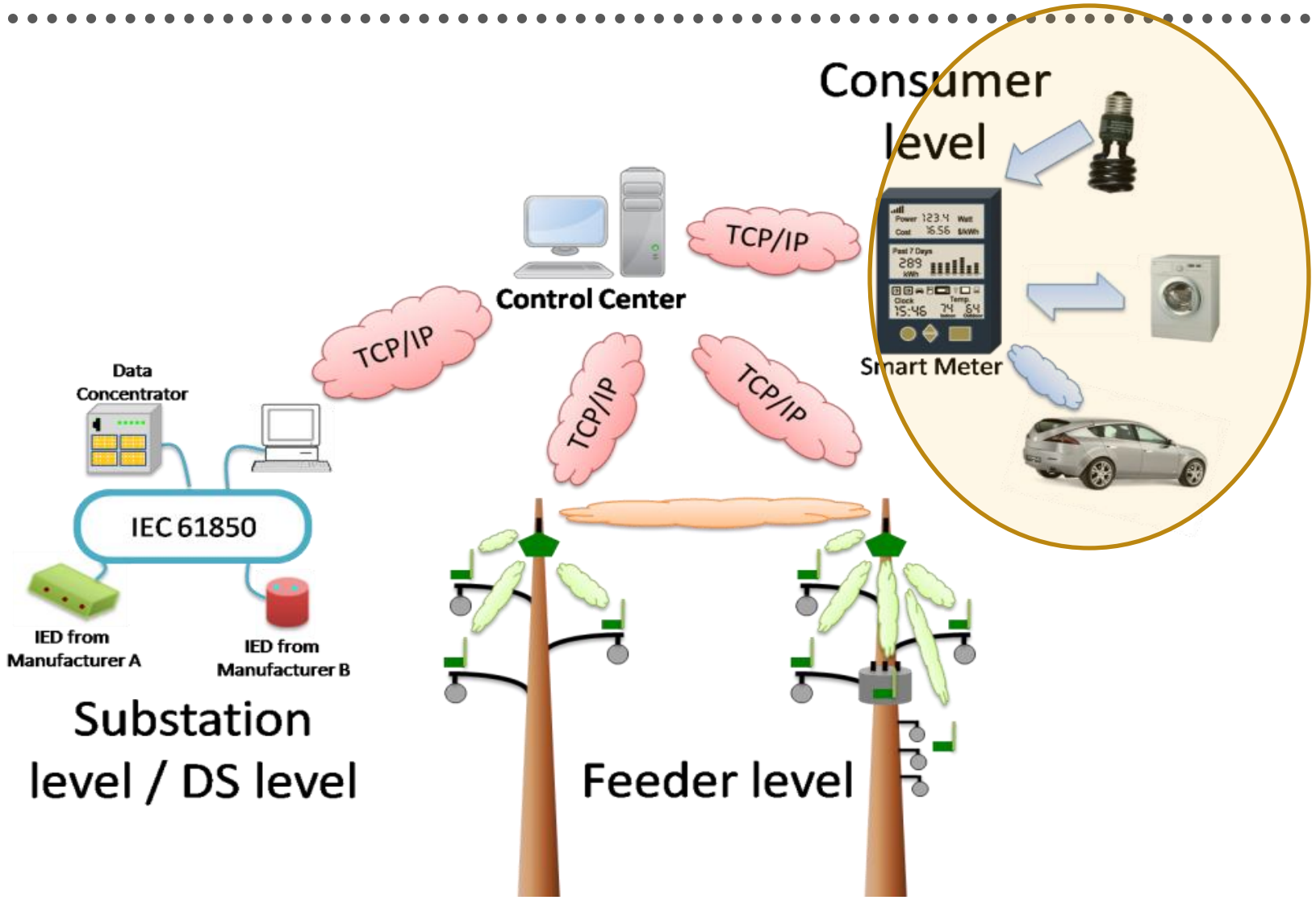
# Role of AMI

- Smart Grid involves customer participation
- Expected from the advanced metering infrastructure (AMI), commonly known as the smart meter.

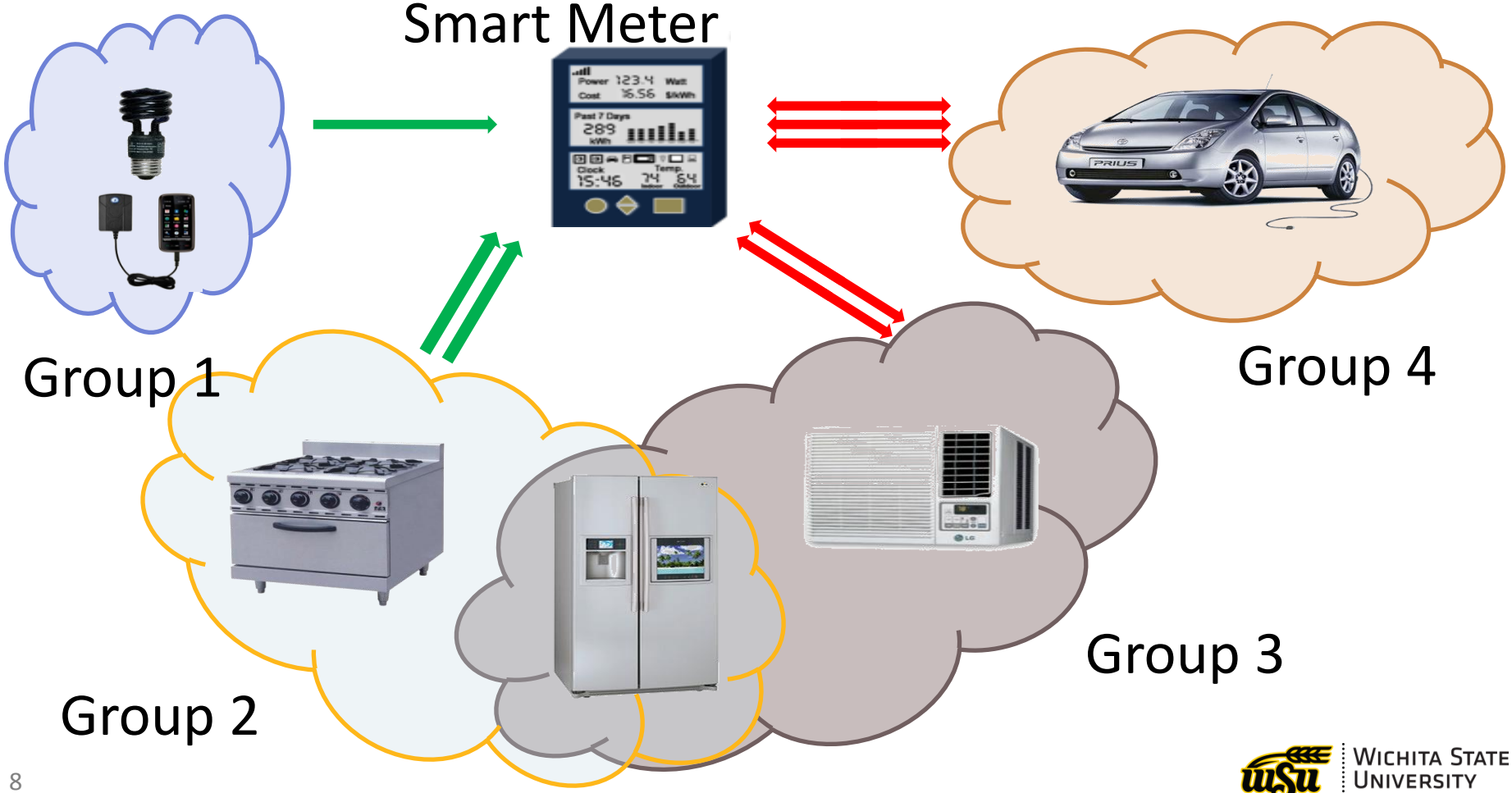
# Smart Meter Goals

- Allows utility to install a smart meter in every customer premise
- Allows a utility to look at aggregate load and possibly issue load handling instructions
  - Load control, demand response
- Typical Agreement
  - Customer allows control (typically high-load equipments)
  - Utility meets customer preferences, customer saves money

# Communication Network for DS



# Home Area Network (HAN)



# Outline

- Introduction
- Wireless-based HANs
  - Why Wireless?
  - Communication Model
  - Selection of Technology
  - Challenges
- Towards a Secure Wireless HAN
  - Objectives
  - Threats and Solutions
  - SecureHAN Framework
- Future Work

# Why Wireless Communication?

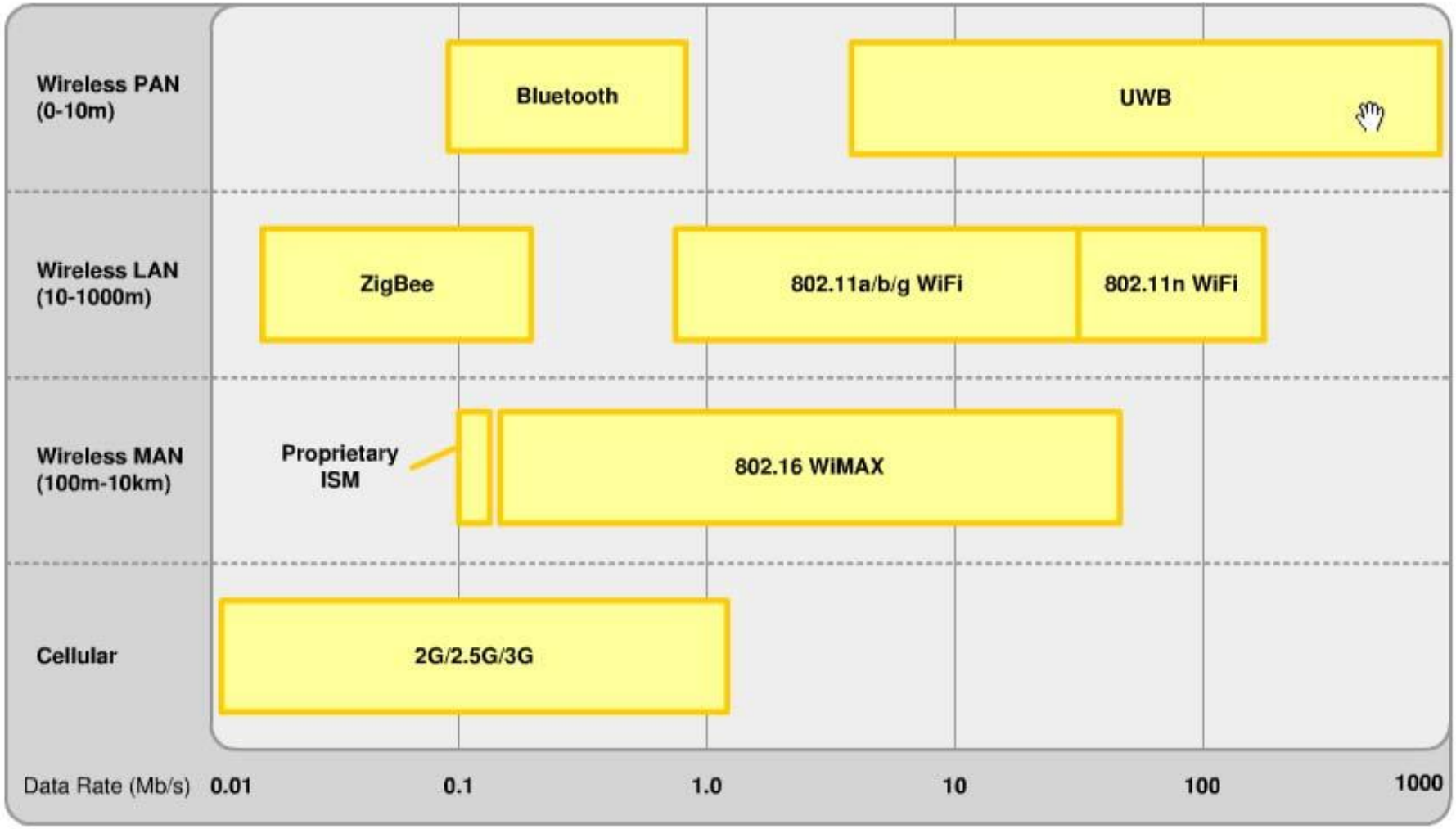
- Minimal Infrastructure Support
  - Cabling between equipment and smart meter
- Allows zero-configuration
  - Allows easy addition and removal of equipment
- Possible integration with existing residential wireless networks
  - Access networks
  - Security or Fire-Alarm networks

# Communication and Control Model

a) Controlled Operation

b) Uncontrolled Operation

# Selection of Technology




Source: DocStoc Wireless Technologies Comparison

# Pros and Cons

| | Wi-Fi | ZigBee | Bluetooth |
|---|---|---|---|
| Data Rate | High | Low | Medium |
| Power | High | Low | Medium |
| Cost | Medium | Low | Low |
| Communication Range | High | Medium | Low |

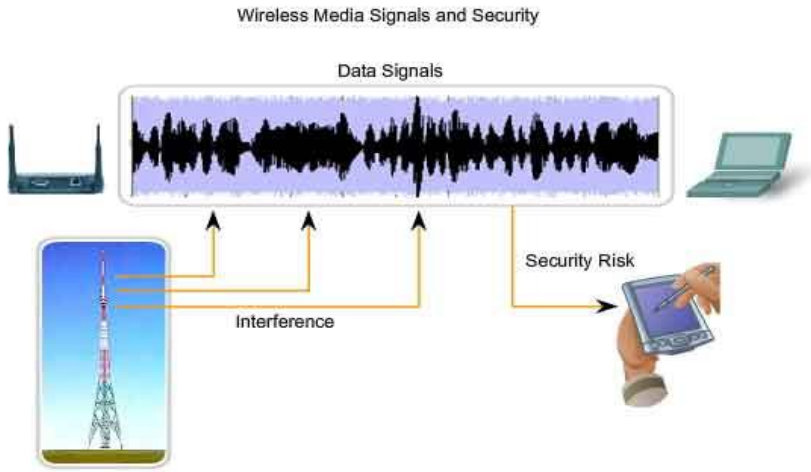
# Pros and Cons

| | Wi-Fi | ZigBee | Bluetooth |
|---|---|---|---|
| Data Rate | High | Low | Medium |
| Power | High | Low | Medium |
| Cost | Medium | Low | Low |
| Communication Range | High | Medium | Low |

Communication within HAN expected to be mainly control messages => low data rate

# Challenges

- Shared Wireless Medium



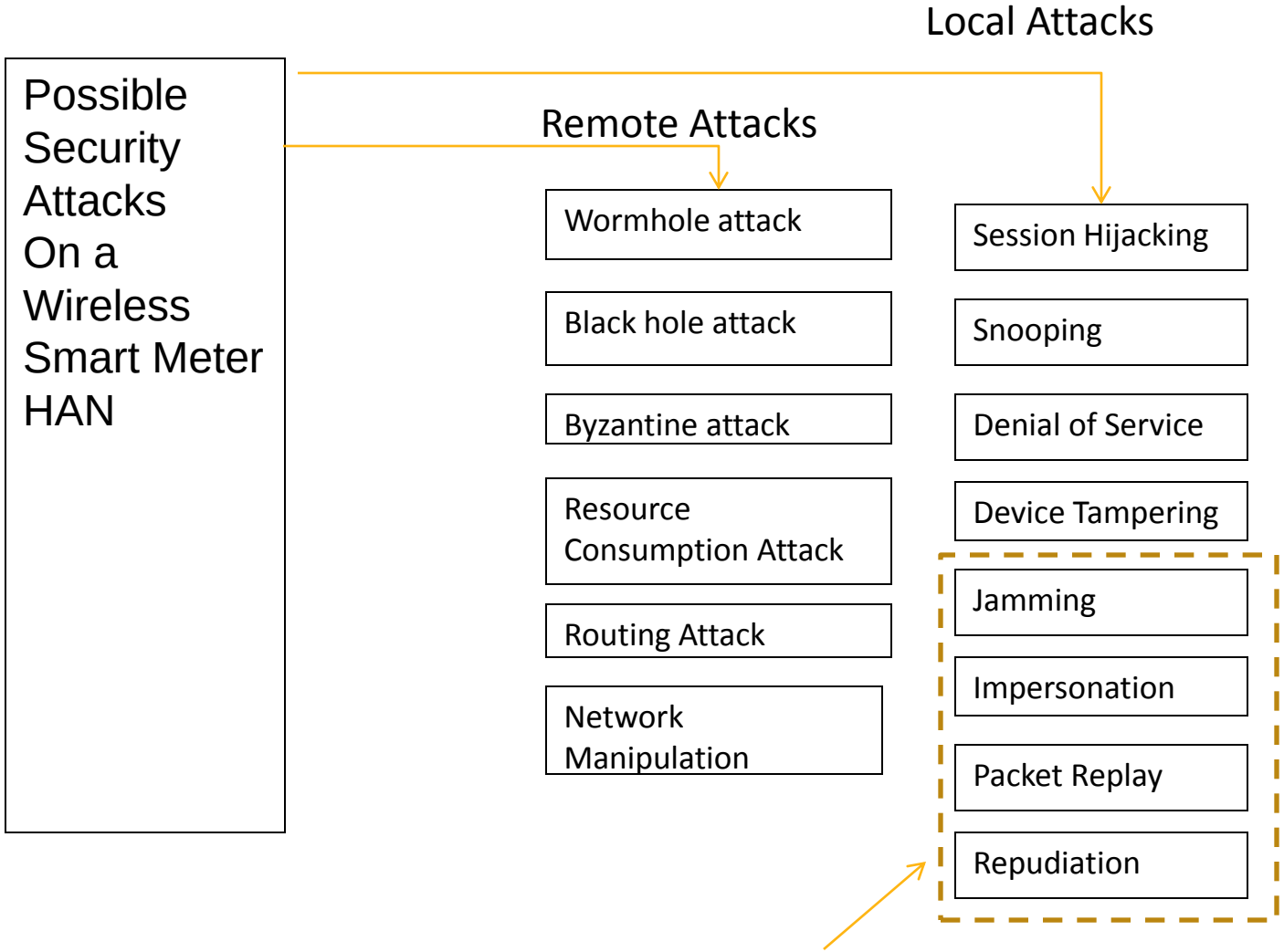

- Two-Party Dynamics
  - Traditional networks are single party networks
  - HAN scenario has customer and utility

# Outline

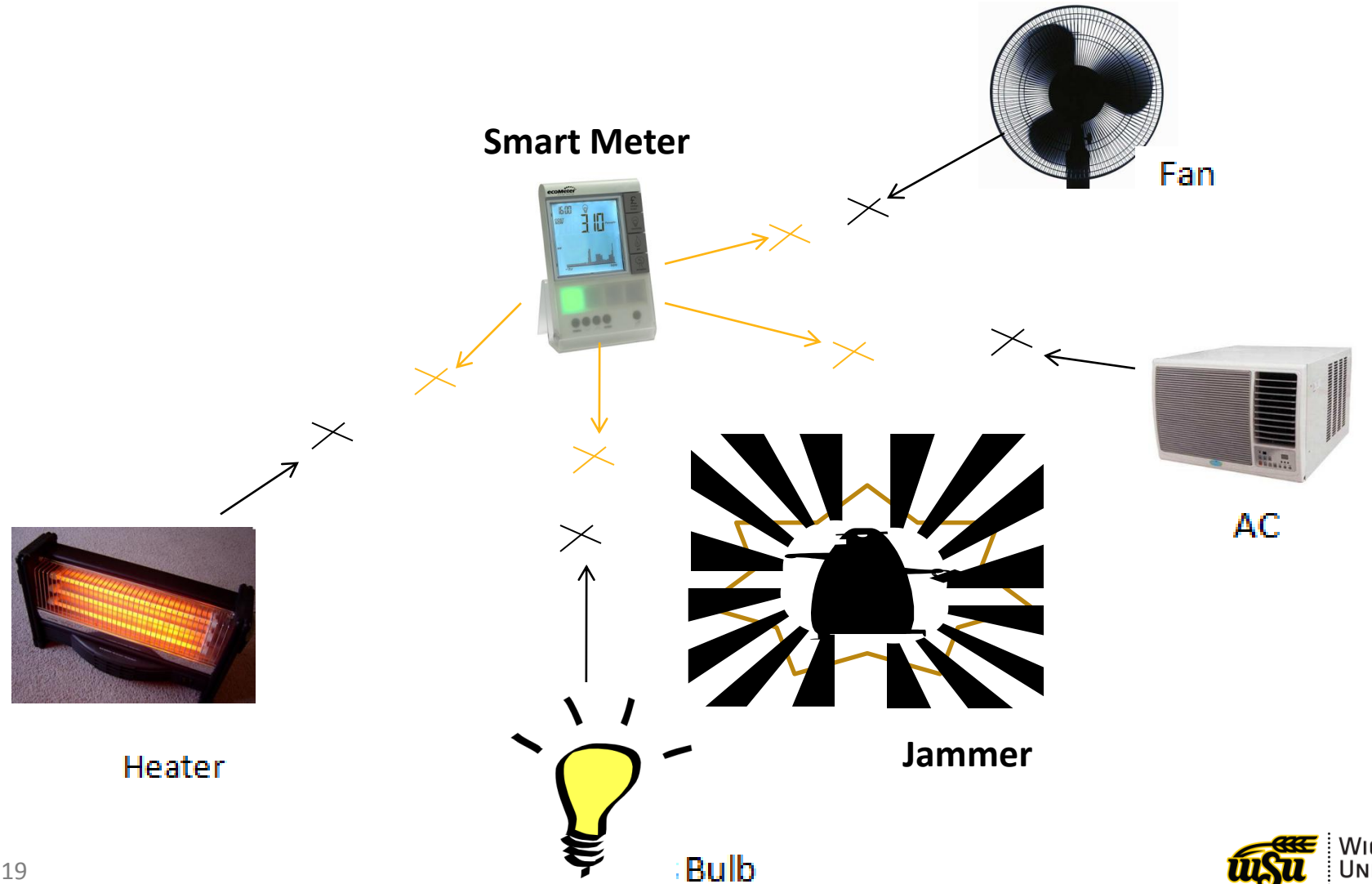
- Introduction
- Wireless-based HANs
  - Why Wireless?
  - Communication Model
  - Selection of Technology
  - Challenges
- Towards a Secure Wireless HAN
  - Objectives
  - Threats and Solutions
  - SecureHAN Framework
- Future Work

# Security Objectives

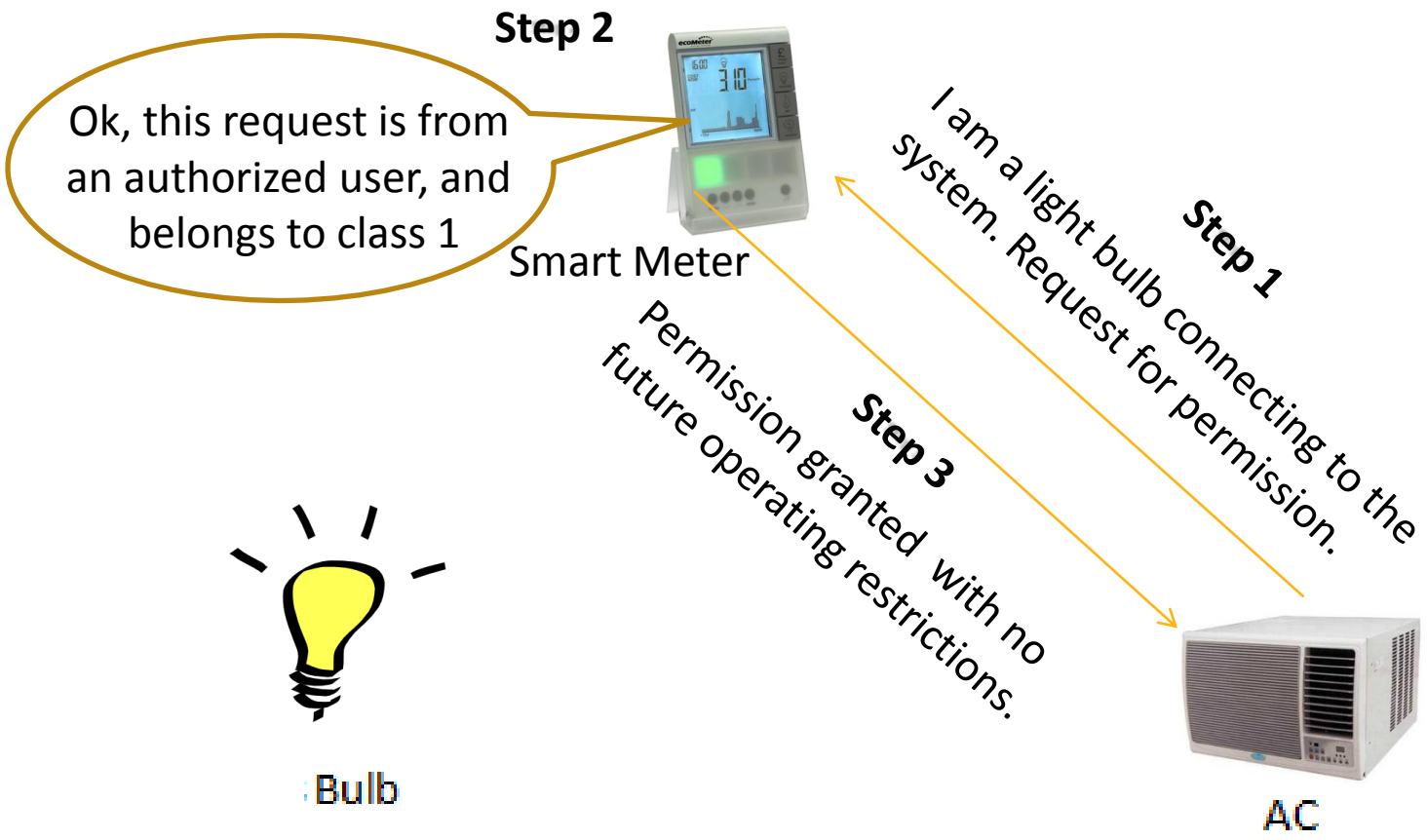
- Confidentiality
- Integrity
- Authentication
- Availability
- Time Sensitivity
  - Traditional wireless networking objectives like fairness not applicable


Possible Security Attacks On a Wireless Smart Meter HAN
Remote Attacks
Local Attacks
Wormhole attack
Black hole attack
Byzantine attack
Resource Consumption Attack
Routing Attack
Network Manipulation
Session Hijacking
Snooping
Denial of Service
Device Tampering
Jamming
Impersonation
Packet Replay
Repudiation
Attacks of particular relevance to Smart Meter HAN scenario

# Jamming Scenario



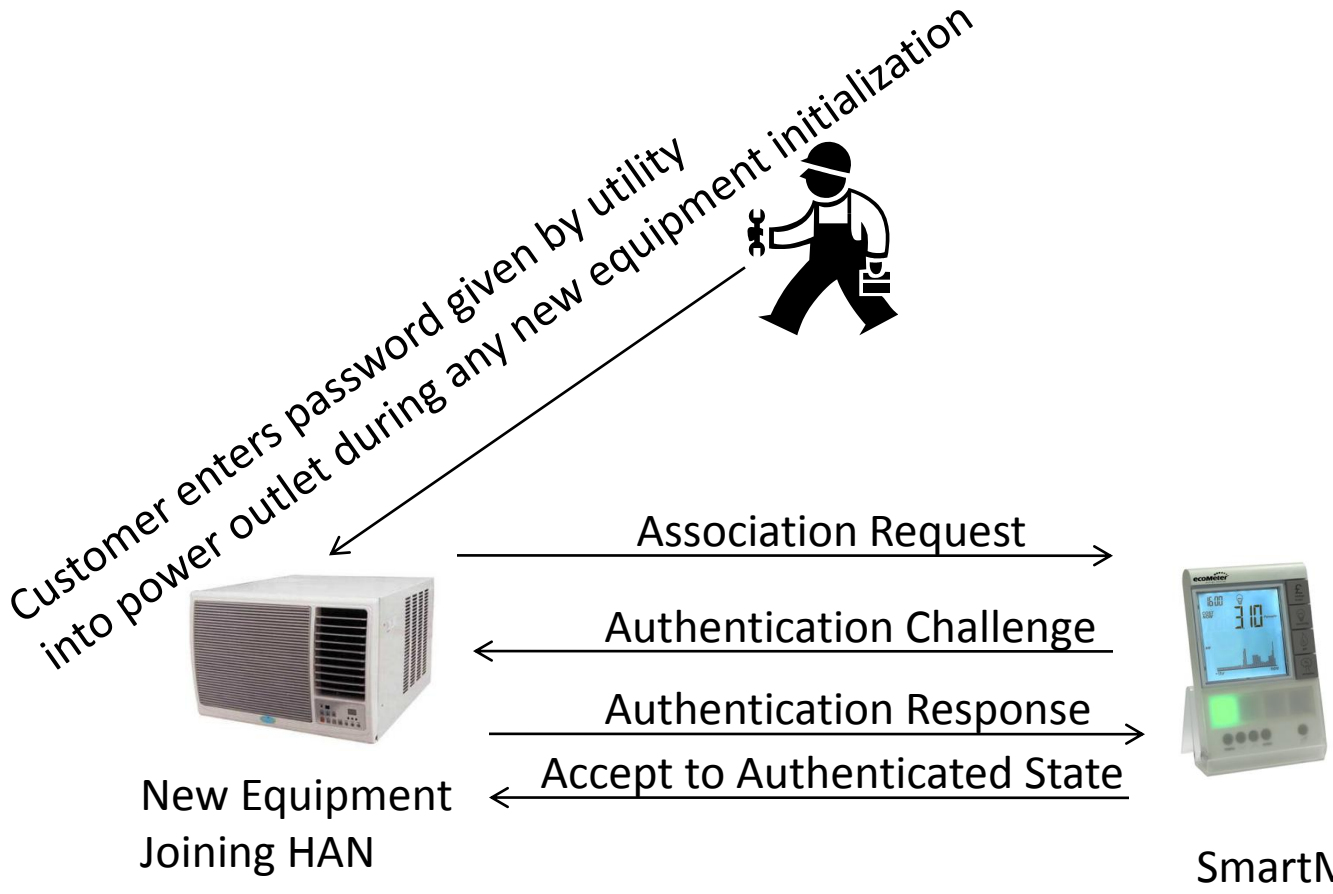
# Impersonation



# Other Vulnerabilities

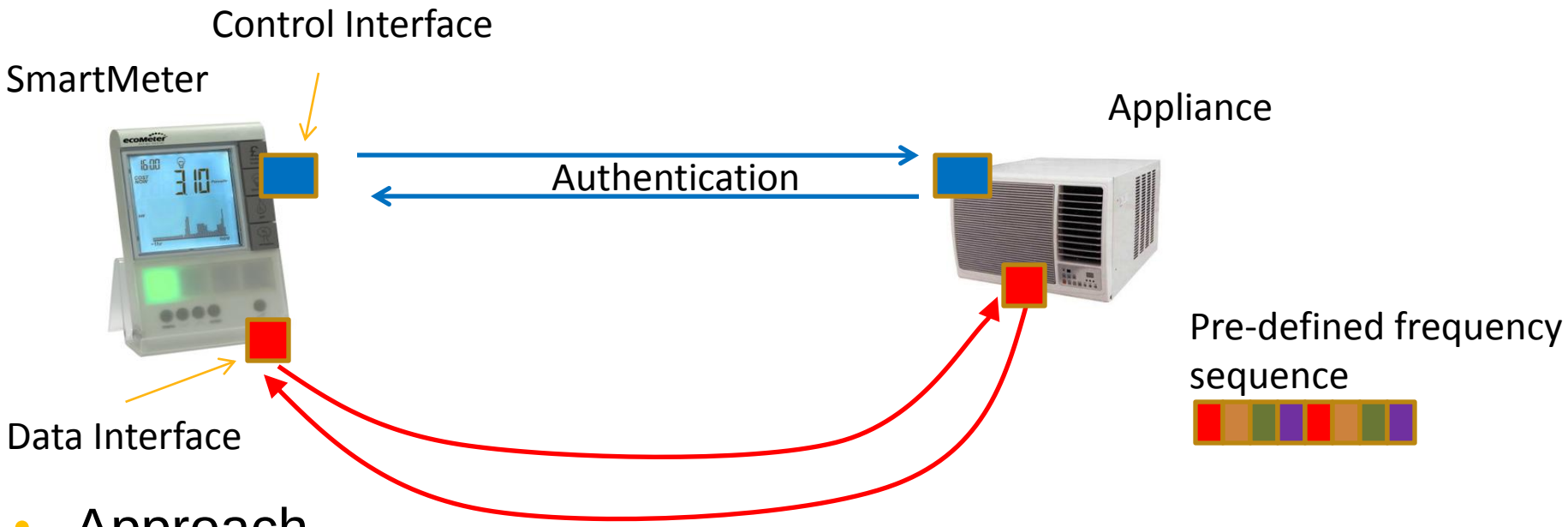
- Replay Attack
  - Neighbor captures packets sent to smart meter and re-sends at a later time
  - Can interfere with equipment scheduling operation at the smart meter
  - Does not need to break encryption
- Repudiation
  - Traceability to what happened in network important

# Authentication



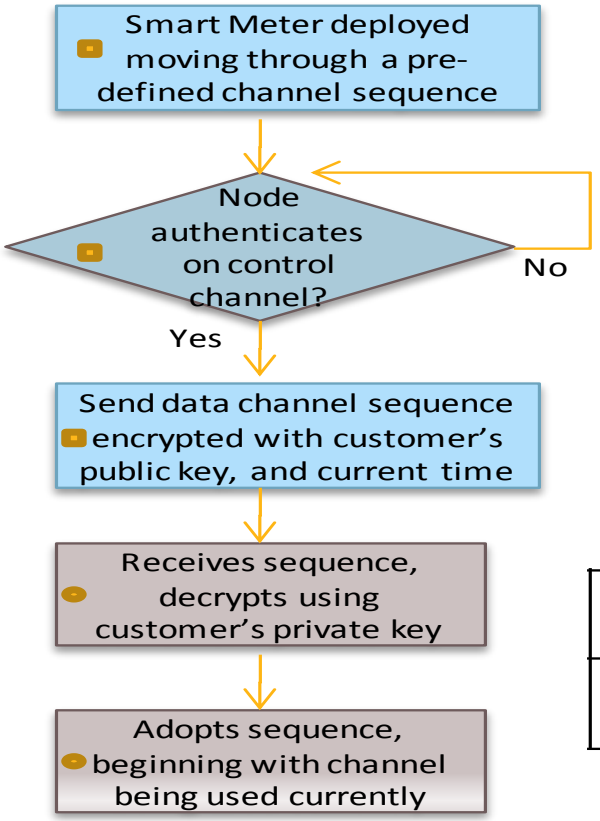

Assumed that customer can be trusted with password !

# Jamming Defense




- Approach
  - Data interface moves through a pre-defined sequence of channels
  - Jammer can impact only for a small amount of time
    - Retransmissions can be used
    - Low data rate requirement helps

# Channel Switching Algorithm

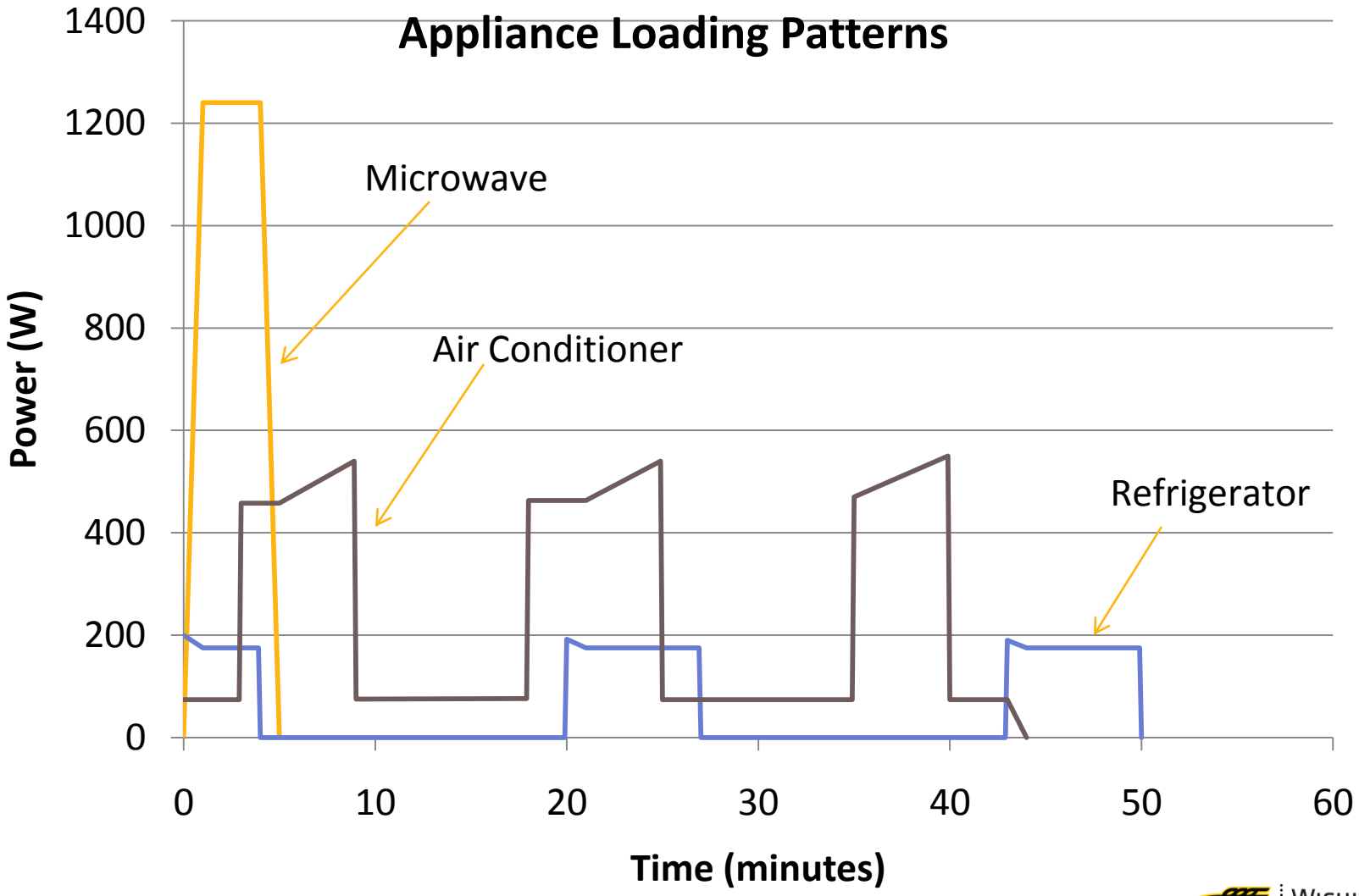


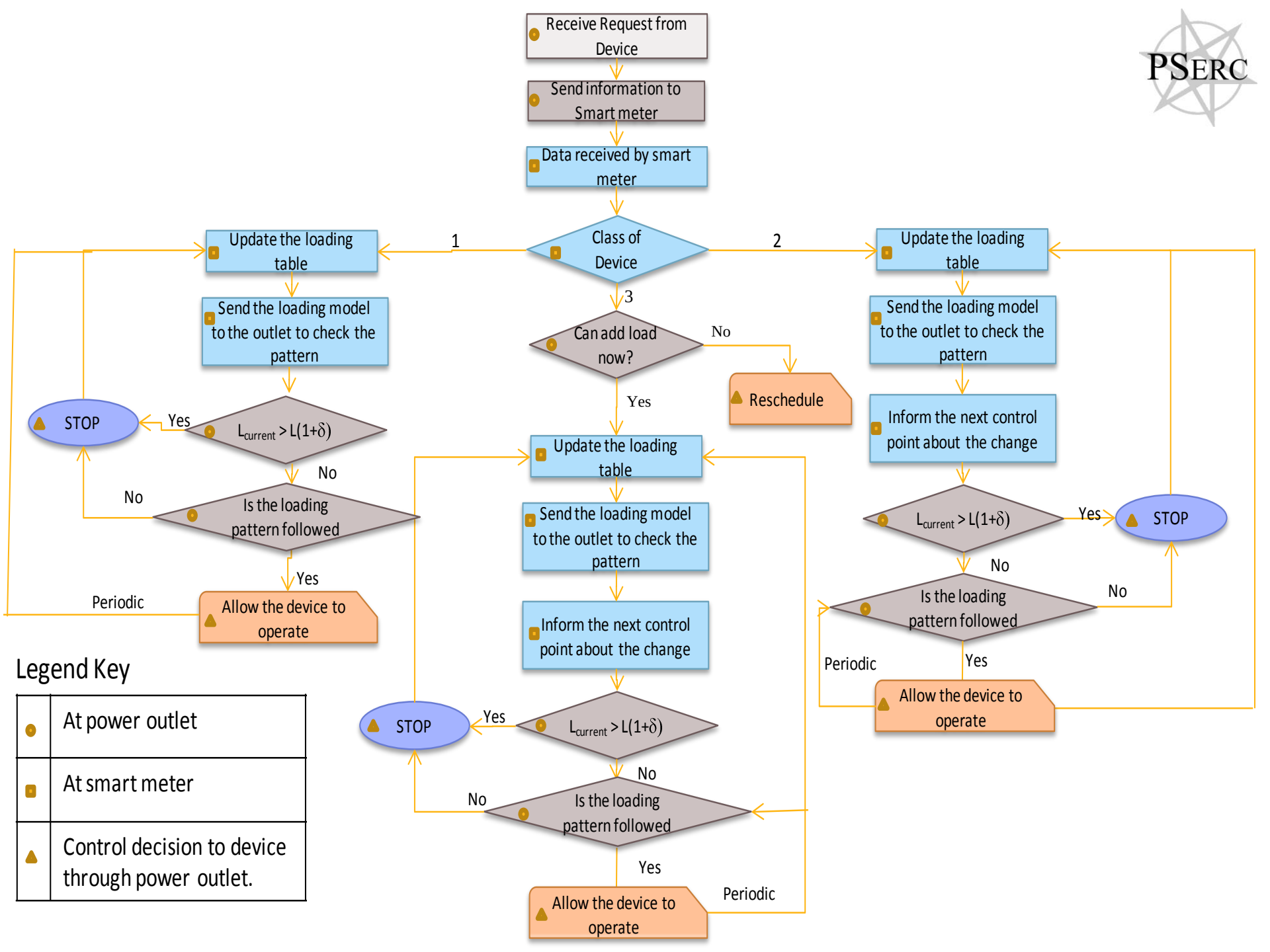

Legend Key

| | |
|---|---|
| | At power outlet |
| | At smart meter |

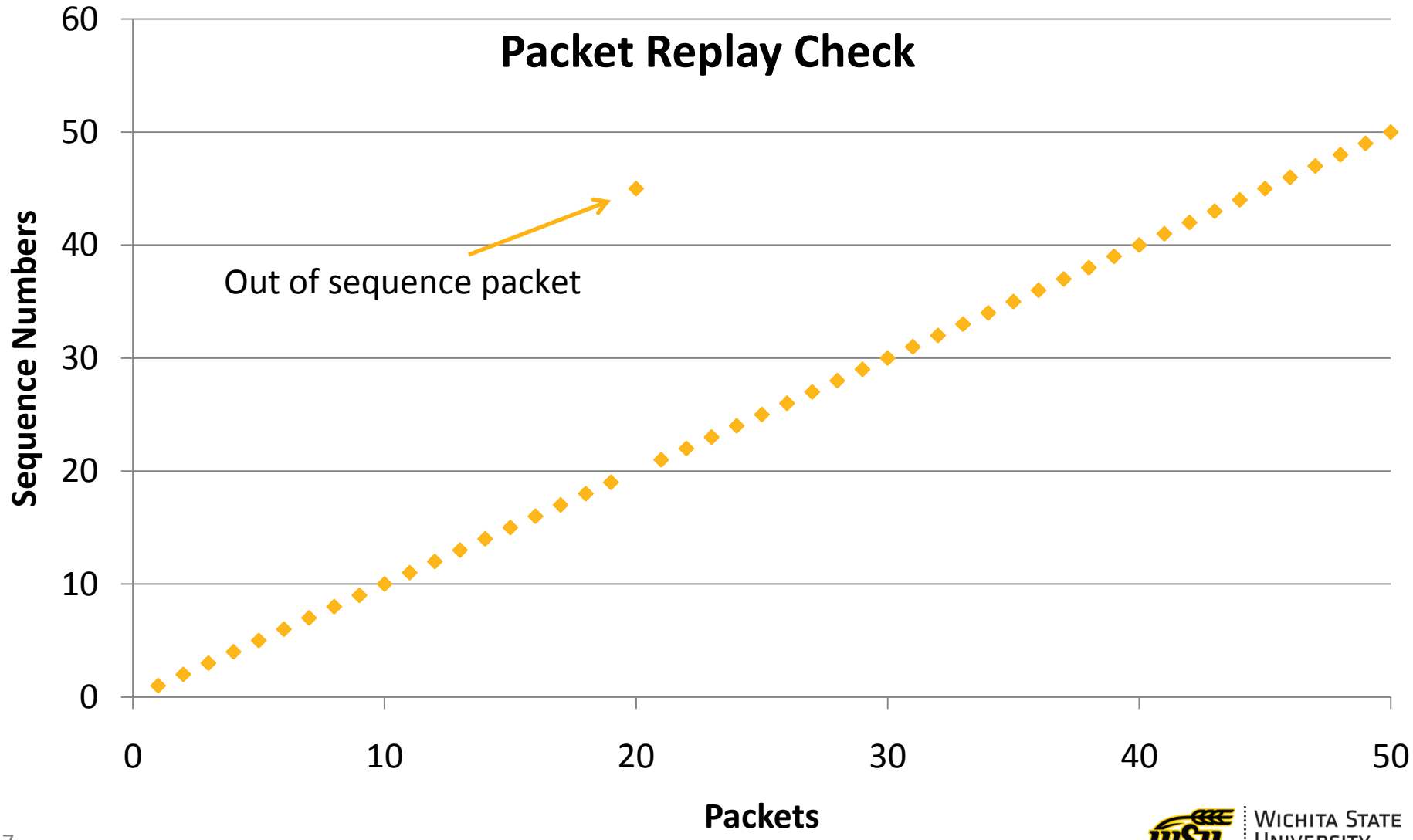
Can additionally employ directional reception at smart meter

# Impersonation – Load Profiling




Receive Request from Device
Send information to Smart meter
Data received by smart meter
Class of Device
1
2
3
Update the loading table
Send the loading model to the outlet to check the pattern
Lcurrent > L(1+δ)
Yes
No
STOP
Is the loading pattern followed
No
Yes
Periodic
Allow the device to operate
Can add load now?
No
Yes
Reschedule
Update the loading table
Send the loading model to the outlet to check the pattern
Inform the next control point about the change
Lcurrent > L(1+δ)
Yes
No
STOP
Is the loading pattern followed
No
Yes
Periodic
Allow the device to operate
Update the loading table
Send the loading model to the outlet to check the pattern
Inform the next control point about the change
Lcurrent > L(1+δ)
Yes
No
STOP
Is the loading pattern followed
No
Yes
Periodic
Allow the device to operate
Legend Key
At power outlet
At smart meter
Control decision to device through power outlet.

# Packet Replay



# Non-Repudiation

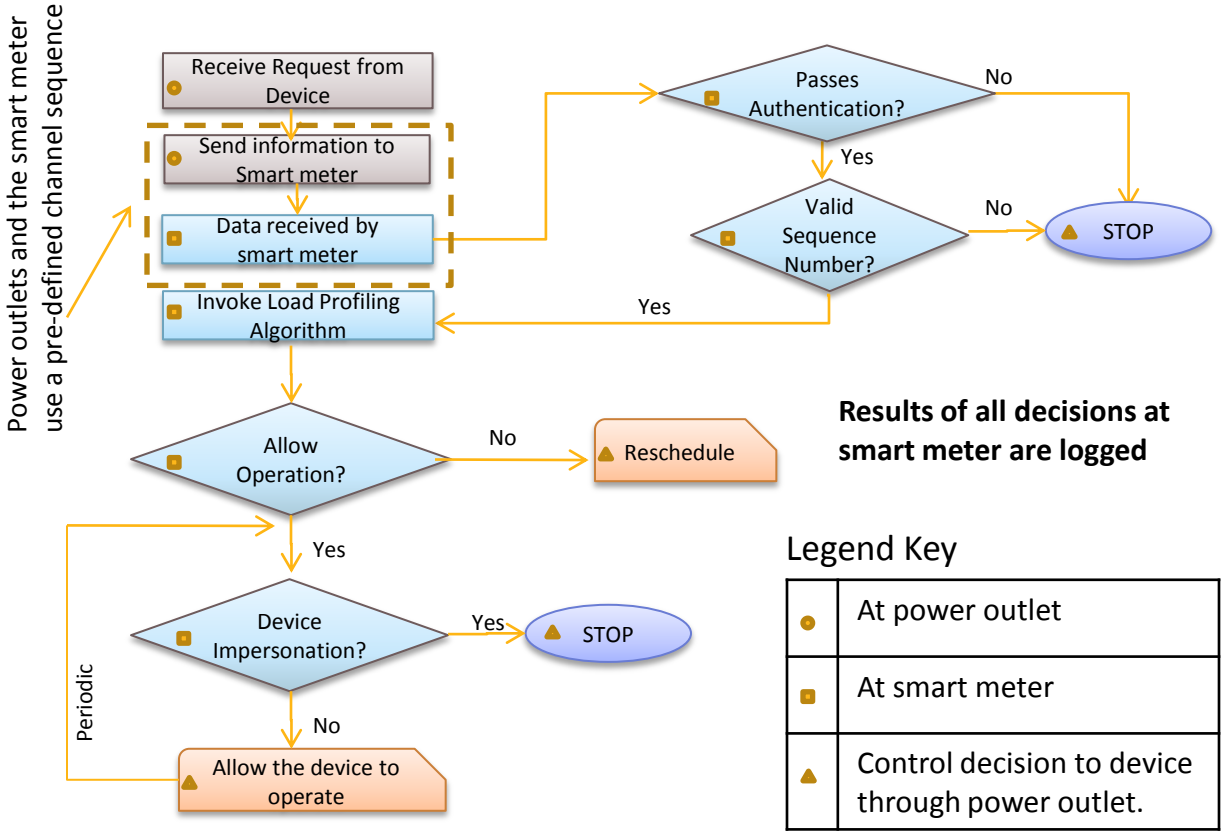
- Keep a log of all communication for specified number of days
  - On dispute, logs used to trace back events
  - Regulations needed to ensure utility does not tamper with logs
  - Available for third-party investigations

# Need a Common Secure Framework

- To integrate responses and defenses to vulnerabilities
- To clearly demarcate role of smart meter, power outlets, and appliances/devices

- Evaluate by how security objectives are met

# SecureHAN Framework



# Progress Towards Security Objectives

- Integrity and Authentication
- Confidentiality
- Availability and delays

# Outline

- Introduction
- Wireless-based HANs
  - Why Wireless?
  - Communication Model
  - Selection of Technology
  - Challenges
- Towards a Secure Wireless HAN
  - Security Objectives
  - Threats and Solutions
  - SecureHAN Framework
- Future Work

# Future Work

- Build a testbed to study HAN control and communications and interactions with utility, and evaluate SecureHAN practically.
- Examine communication path from smart meter to utility control center
  - Consider remote attacks
- Standardization activities to enable control and communication capabilities in appliances
- Include EVs and meet related challenges