Smart Grid Security

Team Ad Hawk

What is the smart grid?

- Smart grid is an umbrella term that encompasses the modernization of the transmission and distribution grids that exist within the current power grid.

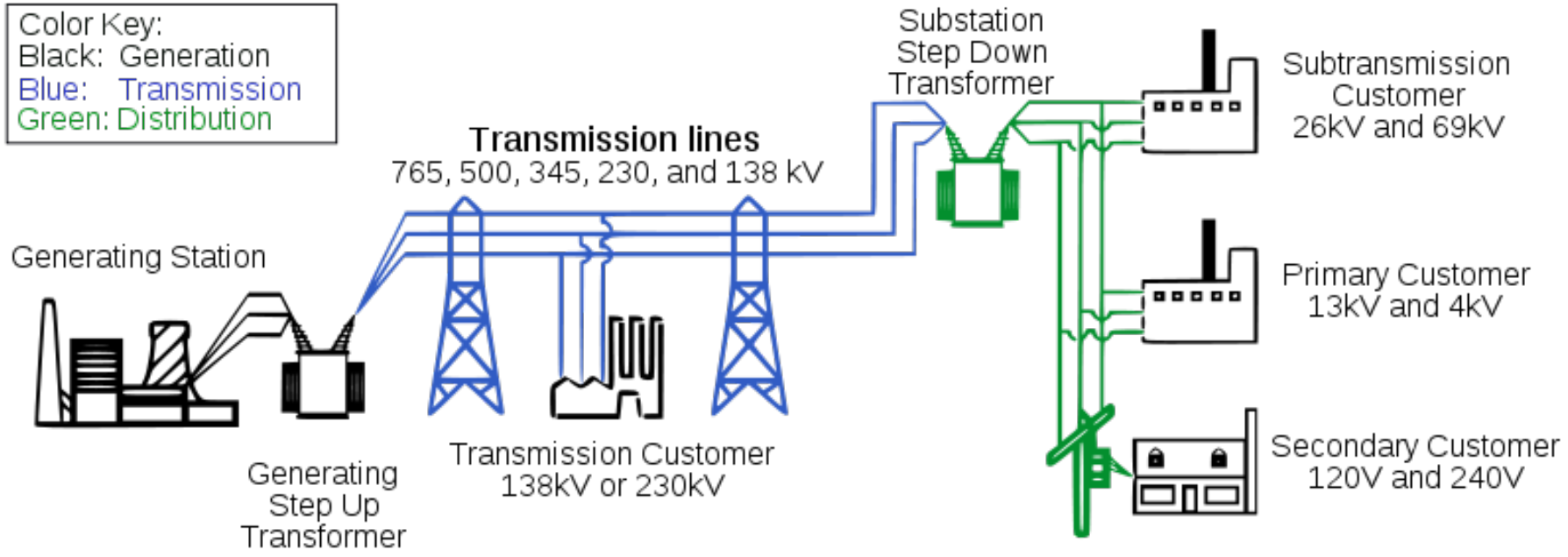
The Current Power Grid

- The electrical (power) grid is an interconnected network for delivering electricity from suppliers to consumers.

Components of Power Grid

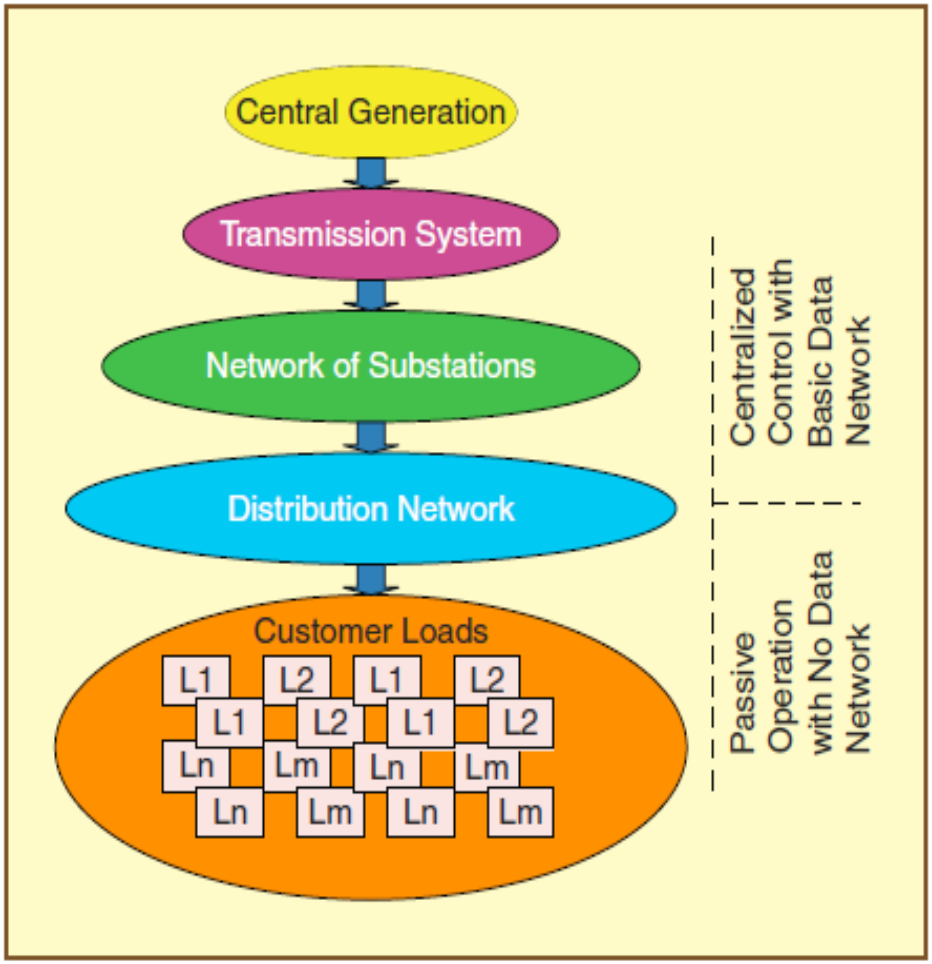
1. Generating Plants that produce electricity from combustible (coal, natural gas) fuels or non-combustible fuels (wind, solar)
2. Transmission lines that carry the electricity from the power plants to the power station
3. Transformers that reduce the voltage and then allow distribution lines to carry power to the customer

The Power Grid



Power Grid Hierarchy

The power plants at the top of the hierarchy ensure power delivery to the customer loads at the bottom of the chain



Issues in Power Grid

- Unidirectional
  - Doesn't allow for any kind of feedback
- Inefficient
  - It converts only 1/3 of fuel energy into electricity
- Failure can lead to domino effect

Fixing the Power Grid

- As mentioned before, the Smart Grid looks to update the current system and bring it into the 21st century

Functions of Smart Grid

1. Self healing
2. Motivate consumers to actively participate in operations of the grid
3. Resist attack
4. Provide higher quality power (wasted from outages)
5. Accommodate generation options
6. Enable electricity markets
7. Run more efficiently
8. Enable higher penetration of intermittent power generation sources

Self Healing & Resist Attack

- Using real time information from sensors and automated controls in order to anticipate, detect and respond to system problems.
  - Avoid or mitigate power outages and service disruptions
  - Automatically detect and isolate fault
  - Redirect power flows around damages facilities

Consumer Participation

- Consumers can change their behavior around variable electric rates or participate in pricing programs designed to ensure reliable electrical service during high-demand conditions.
- Incorporates consumer equipment and behavior in grid design, enabling consumers to better control “smart appliances” and “intelligent equipment” so that consumers can better manage energy use and reduce energy costs.

Accommodate Generation Options

- Ability to integrate small-scale power generation from residential or commercial customers who will now be able to sell excess power to the grid with minimal technical or regulatory barriers.

- With these additional generation options available we will now be able to have a market

Recap

Existing Grid	Intelligent Grid
Electromechanical	Digital
One-Way Communication	Two-Way Communication
Centralized Generation	Distributed Generation
Hierarchical	Network
Few Sensors	Sensors Throughout
Blind	Self-Monitoring
Manual Restoration	Self-Healing
Failures and Blackouts	Adaptive and Islanding
Manual Check/Test	Remote Check/Test
Limited Control	Pervasive Control
Few Customer Choices	Many Customer Choices

Wireless AMI Application and Security for Controlled Home Area Networks

Aravinthan, V., Namboodiri, V., Sunku, S. and Jewell, W.

AMI

- Advanced Metering Infrastructure
- Smart Meters
- Collects energy consumption data from appliances within the home
- Makes informed decisions about energy distribution within the home
- Gateway to the Neighborhood Area Network (NAN)

Possible Communication Mediums

- Wired
  - Ethernet
  - Power Line Carrier (PLC)
- Wireless
  - 802.11
  - Bluetooth
  - ZigBee

Appliances

- Broken up into groups based on energy consumption and availability needs

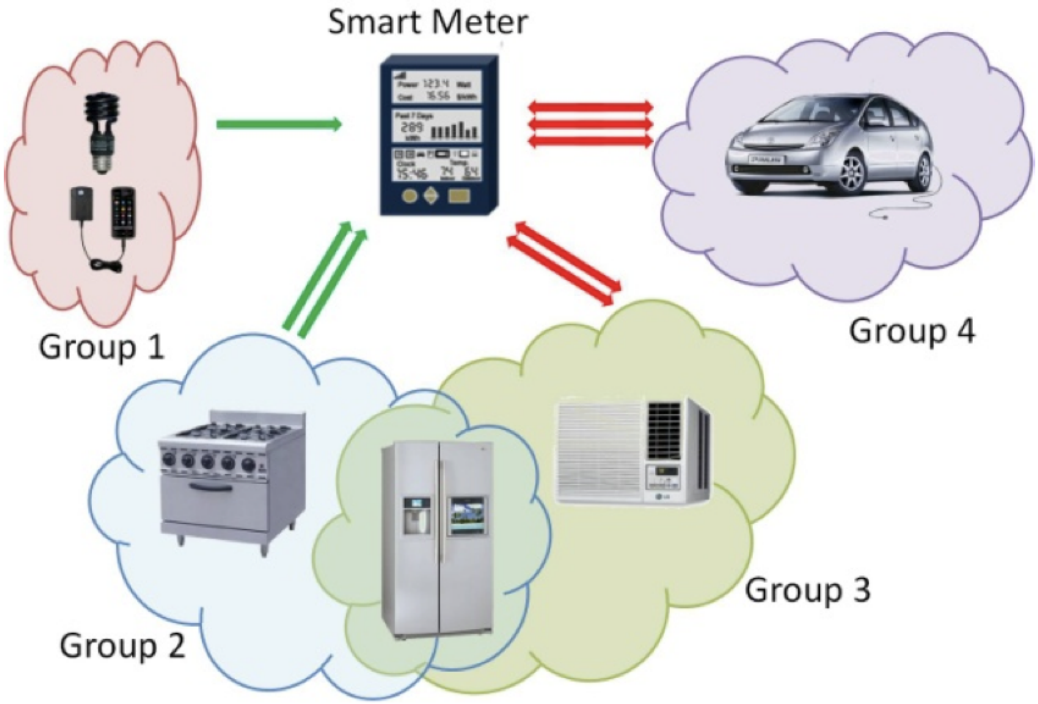


Figure 1: HAN Appliance Classification for AMI Application

Appliance Groups

- Group 1
  - Low energy consuming appliances
  - Lights, Laptop Chargers, Phone Charges, TV, etc.
- Group 2
  - High energy consuming appliances with a high need for availability
  - Stoves, Ovens, Refrigerators
- Group 3
  - High energy consuming appliances with a low need for availability
  - Air conditioners, clothes washers and dryers, dishwashers
- Group 4
  - Electric Vehicles

What Gets Sent to the AMI?

- Group 1
  - Only send a message when it is connected/disconnected from the outlet
- Group 2
  - Sends power usage and duration of usage when possible
- Group 3
  - Requests to use a specified amount of energy and for a specified time
  - Smart Meter will respond with a yes/no depending on electricity pricing and availability
- Group 4
  - Planned charging for a predetermined set of time

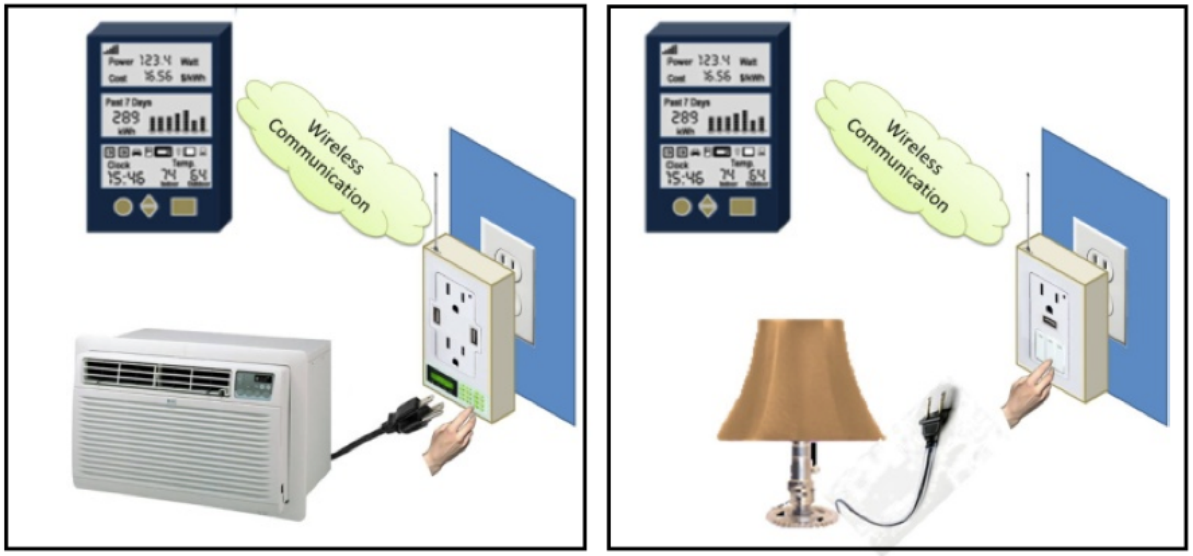
How Does the Appliance Interact with the AMI?

- Smart Appliances
  - Appliances have a built in interface that can communicate with the AMI

LG THINQ Washer and Dryers

How Does the Appliance Interact with the AMI?

- Smart Outlets
  - Two different types of outlets: one that is able to be controlled by the AMI (group 3) and one that only sends information to the AMI (groups 1 & 2)



(a) Controlled Outlet (b) Uncontrolled Outlet

Figure 2: Communication and Control Enabled Power Outlets

Security Objectives for Wireless AMI Networks

- Confidentiality
  - Only customers and the utility have access to the data collected
  - Users would prefer aggregate information
- Integrity
  - The appliances are not sending wrong information to the AMI
  - The customer does not alter the information from the AMI to the utility

Security Objectives for Wireless AMI Networks

- Availability
  - AMI network will remain available in the midst of an attack or failure
  - Does not worry about power concerns (tied into the power resources of the house)
- Time Sensitivity

  Allows room for delay, but not significant delay
- Authentication
  - The customer knows that his/her appliances are communicating with the right AMI
  - The AMI knows it is communicating with the customer's appliances

Possible Security Attacks on the AMI

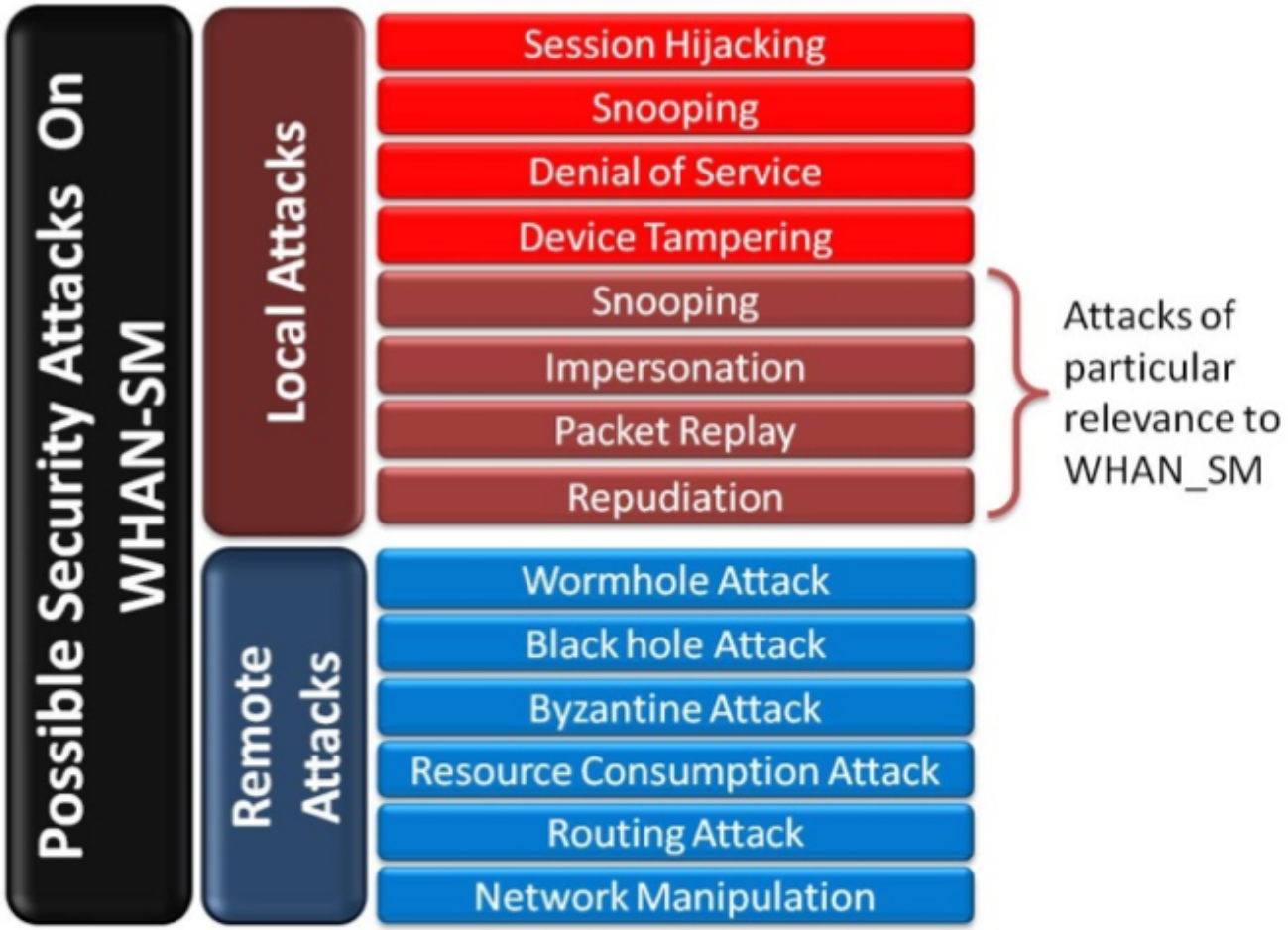


Figure 3: List of attacks on Wireless HAN scenario.

Jamming Attacks

- Easily achieved by an attacker
- Sends a constant signal or intermittent signal on the shared medium
- Appliances will not be able to communicate with the AMI
- Group 3 appliances will not be able to request for power consumption
- AMI will not have complete data on Group 1 and 2 appliances using power

Impersonation Attacks

- Customer may want pass off a Group 3 appliance as Group 1 or 2 so it is not delayed power

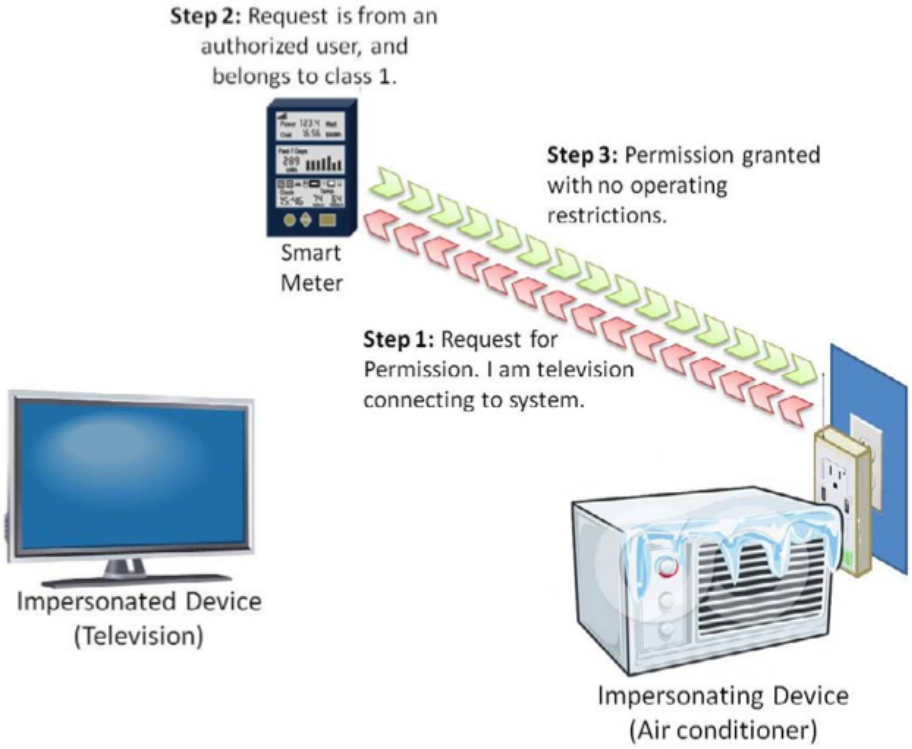


Figure 4: Example of an Appliance Impersonation Attack

Replay Attacks

Replay a request made by an appliance, when really no request is made

- Ex) Angry neighbor wants to get back at the customer for not returning their lawn mower so they do a replay attack to raise the customer's electric bill

- Overloads the AMI and could hurt the whole grid

Non-Repudiation Attacks

- Customer refutes having received control messages
- AMI refutes it controlled a customer’s compliance.

Solutions – Jamming

- Use multiple alternate frequency channels
- If current channel has noise above a threshold, switch to the next channel in a common random sequence of channels
- This random sequence is established during appliance authentication
- AMI could also be equipped with spread spectrum capabilities that could monitor and apply manual interventions
- Requires time synchronization or control messages to be able to get through

Solutions – Jamming

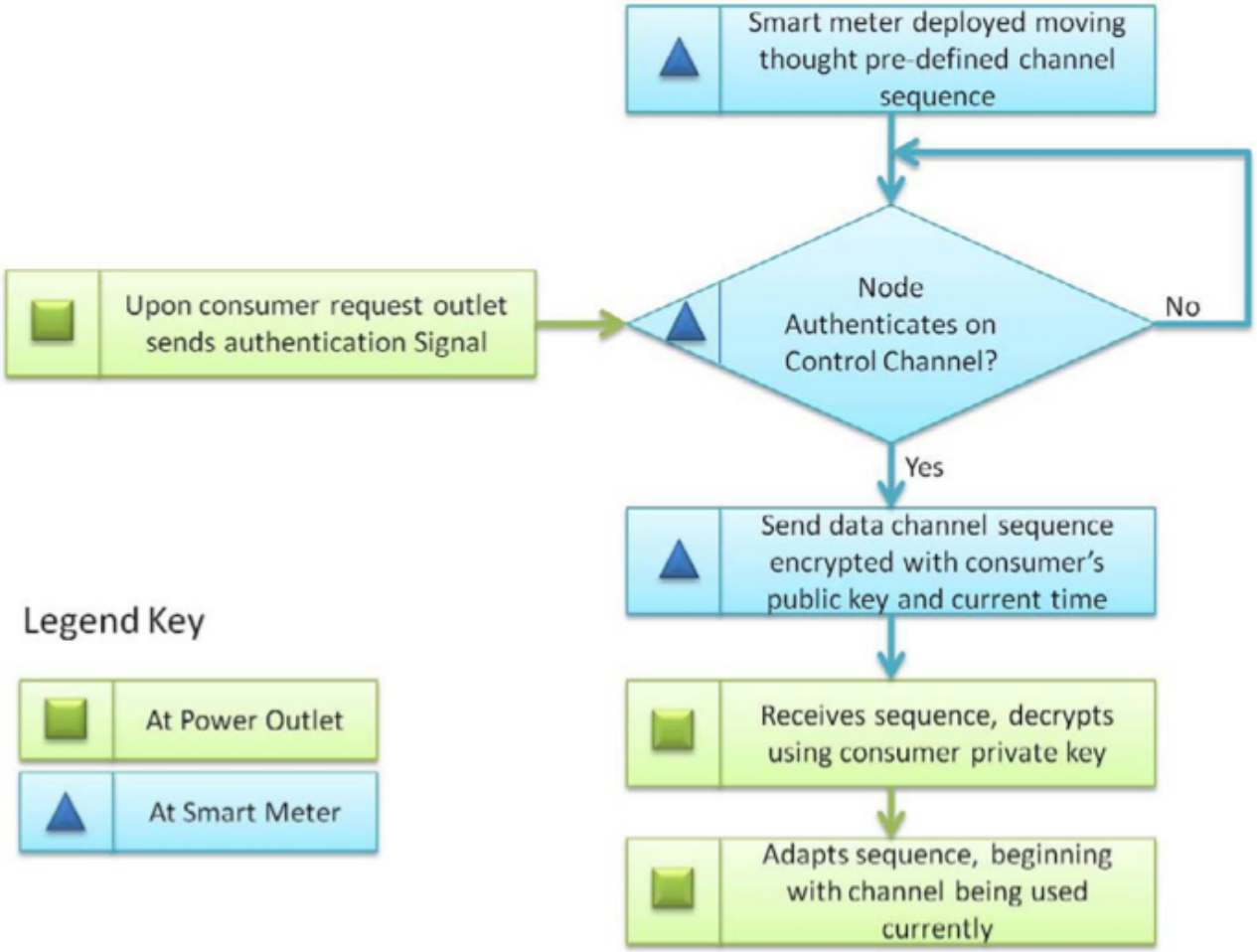


Figure 5: Channel Switching Algorithm

Solutions – Impersonation

- Compare metrics between current device and what metrics are expected
- Metrics either pre-stored based on manufacturer's data, or verified against prior device operation history

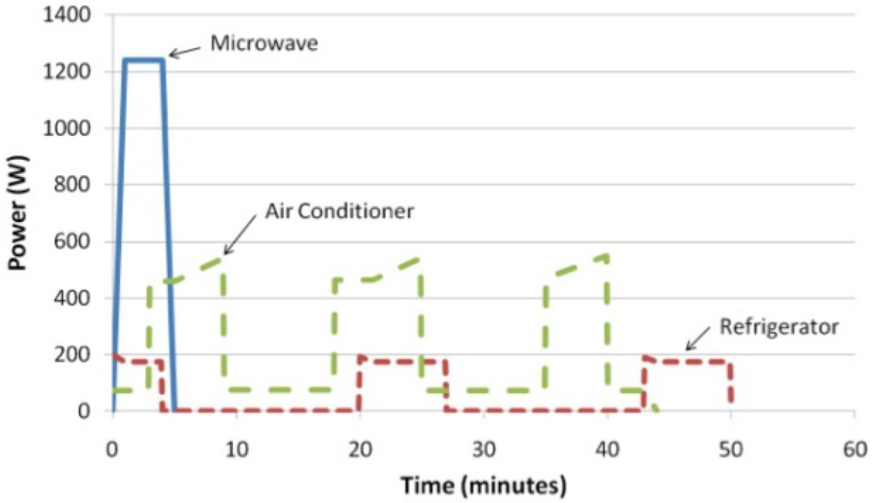


Figure 6: Appliance Loading Patterns

Solutions – Impersonation

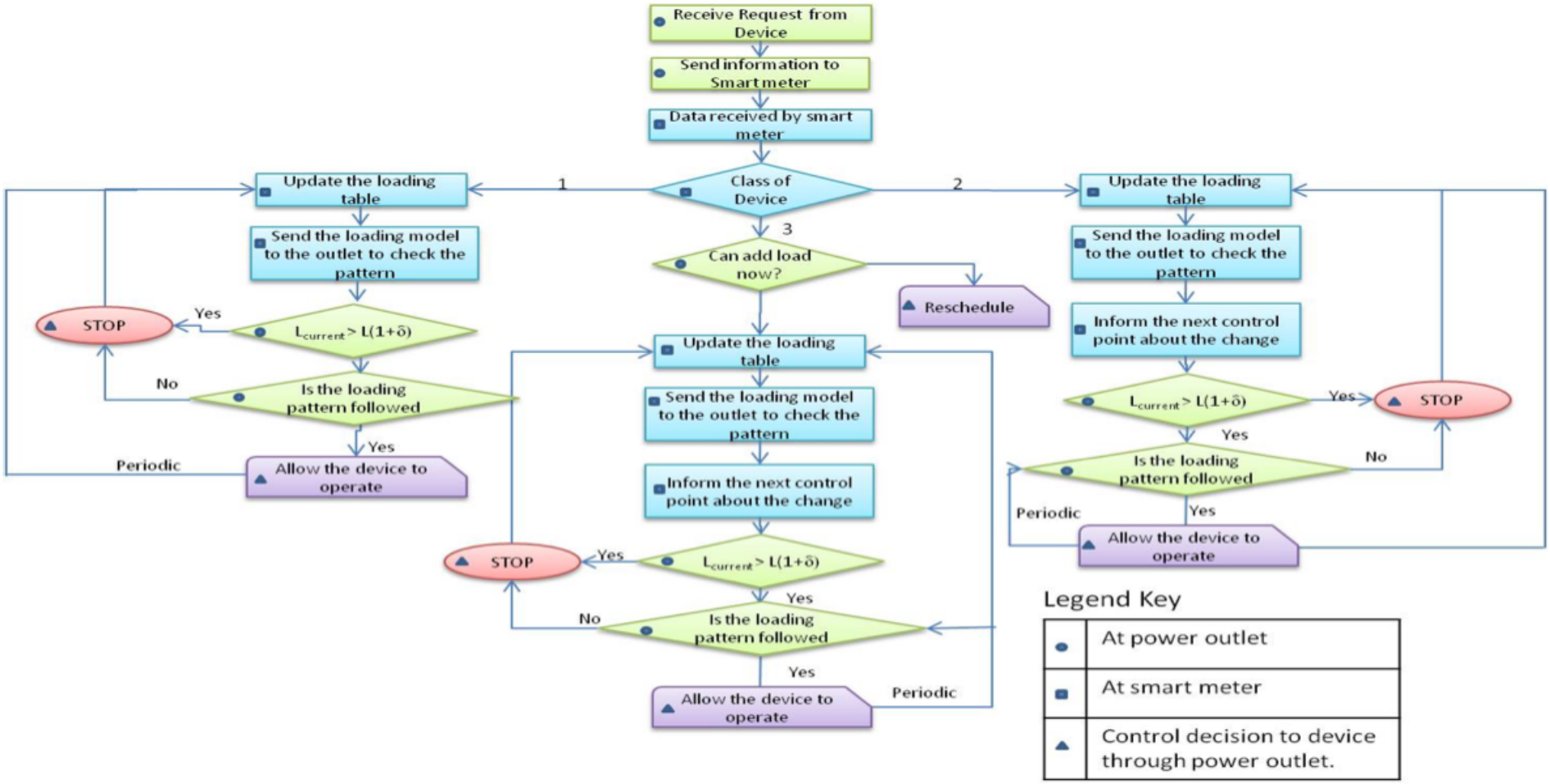


Figure 7: Load profiling algorithm to counter the possibility of device impersonation.

Solutions – Replay

- Sequence Numbers
- Timestamps
- If a packet arrives out of sequence or with significant delay, ignore the request

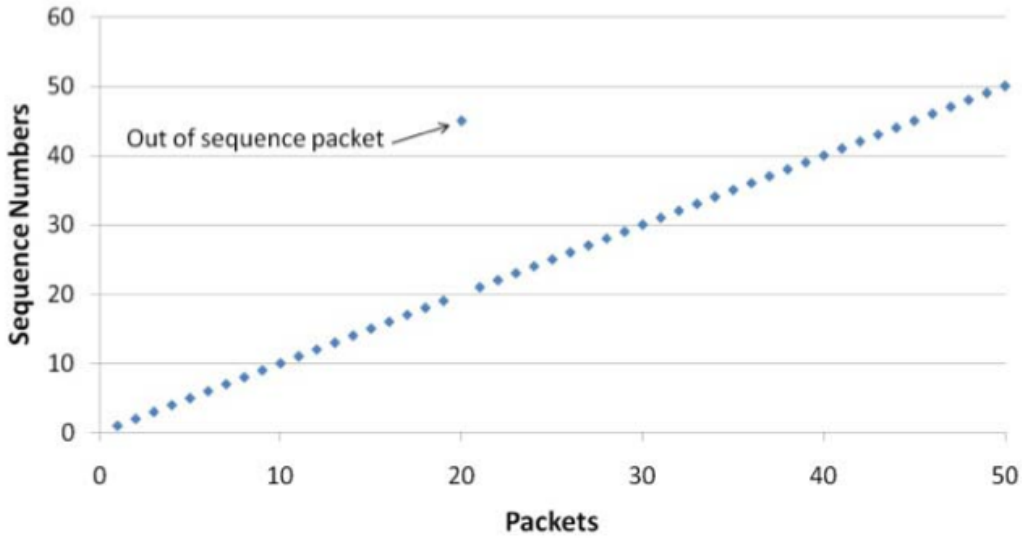


Figure 8: The sequence number technique to detect packet reply attacks

Solutions – Non-Repudiation

- Sign packets with private key
- AMI keep logs for a specified time
  - Requires regulations and enforcement for utilities to keep these logs tamper-free
  - Third party audits

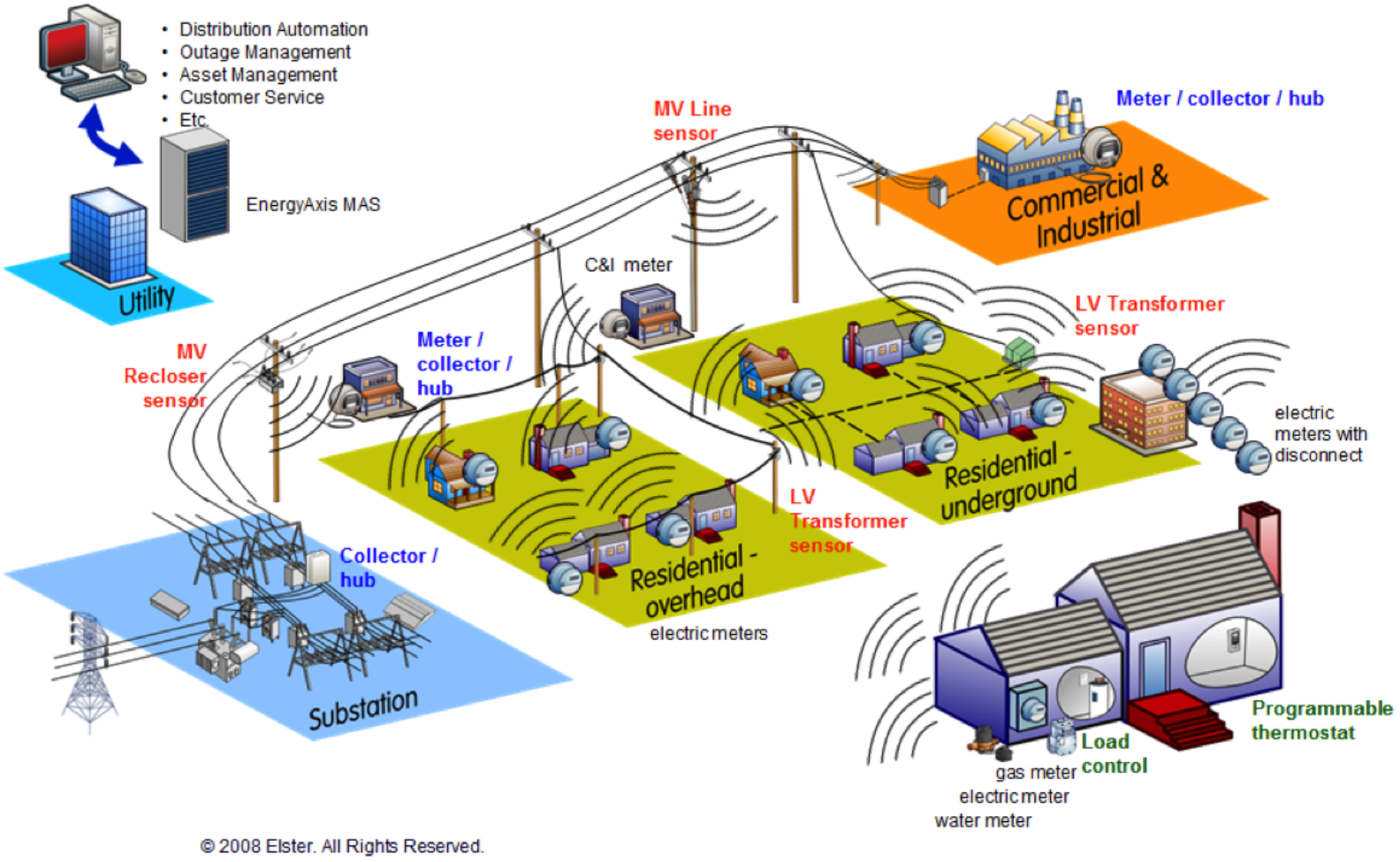
NAN & Backbone

- NAN - Neighborhood Area Network
  - Network connecting each smart meter (or other control system endpoint device) in a local area
  - Assumed to be a wireless mesh network
  - Could be others:
    - cellular, WiMAX, power line communication (PLC)
- Backbone (aka "backhaul")
  - Connection from NAN <--> Utility / Substation
  - Variety of communication technologies:
    - wired (fiber links)
    - wireless (microwave, satellite, low freq RF, etc)

Advanced Metering Infrastructure

- AMI is a "tack on" solution to obtain realtime meter data
- First step in smart grid implementation
  - no narrow control at this point, mostly one way meter data collection (AMR)
- AMI designs mostly concentrated to the NAN scope

Advanced Metering Infrastructure



Advanced Metering Infrastructure

- Current designs utilize:
  - proprietary RF devices on ISM bands
  - PLC (powerline)
  - WiMAX
  - ZigBee
  - EVDO, GPRS, CDMA, other cellular
  - WiFi
- Mostly built on protocols that can be hacked
  - "SCADAoIP"

Security in NANs

- MaxStream (now Digi Corp) 900MHz radios
  - extremely popular serial <--> RF device
  - offers FHSS, but...
  - hop sequences, modulation, etc are published
- Open radios to look at PCB board
  - find IC datasheet to narrow down freq band
- GnuRadio
  - open source signal processing algorithms

http://media.digikey.com/photos/Digi%20Int'l%20Photos/X09-009NSC.jpg

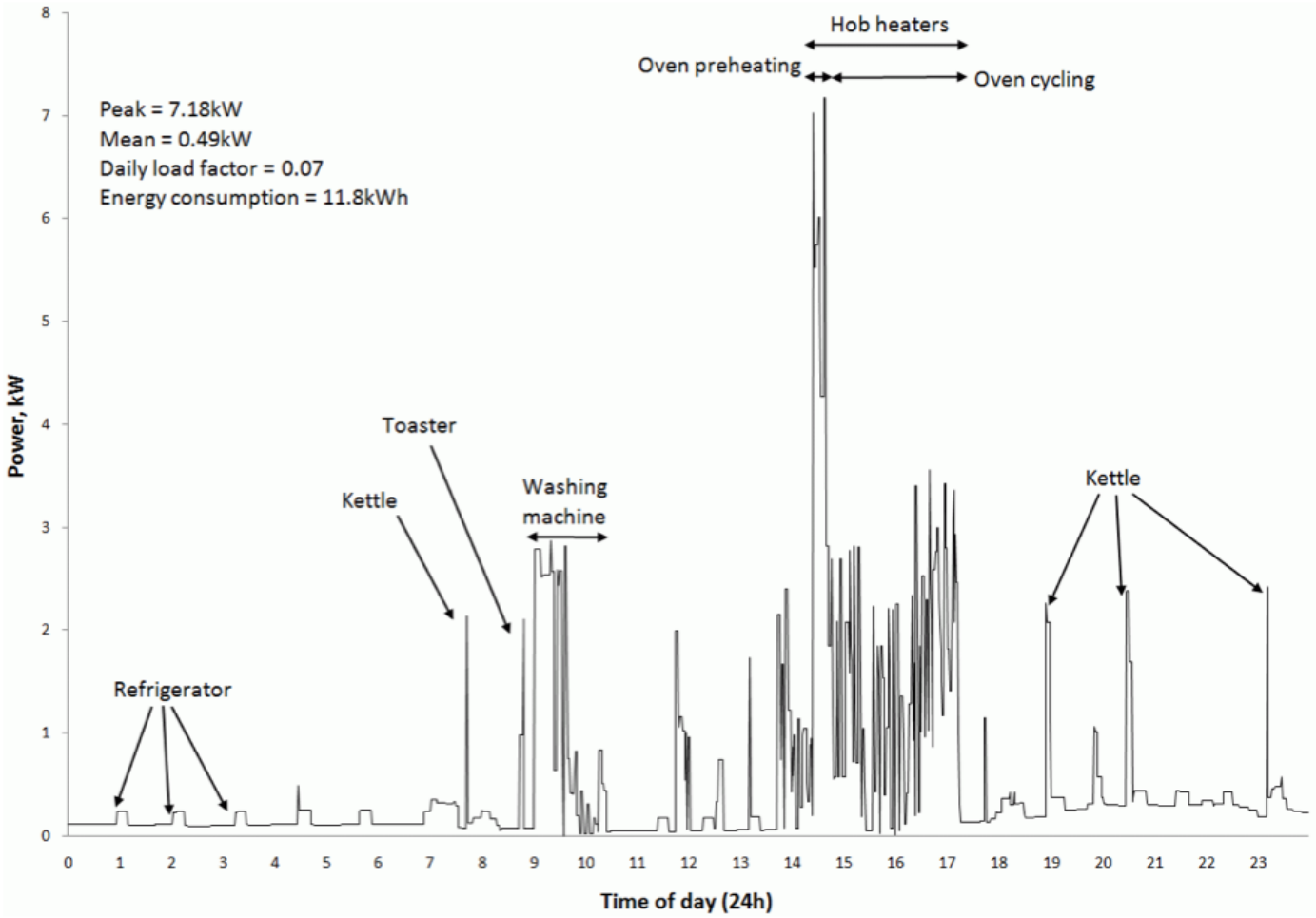
Security Pushback

- Many wireless technology hacks presented against AMI systems in Black Hat 2010 talk "Wardriving the Smart Grid"
- Research paper nowhere to be found
- Official link has a note stating that they have been redacted heavily
- Most likely pushback by big Smart Grid development companies (large IT firms)

Smart Meter Data Anonymizing System

- Paper: *Smart Grid Privacy via anonymization of Smart Metering Data (Efthymiou; Kalogridis)*
- Data collected by smart meters sent to utility in high frequency intervals
  - high frequency required for prompt electricity routing decisions

Smart Meter Data Anonymizing System



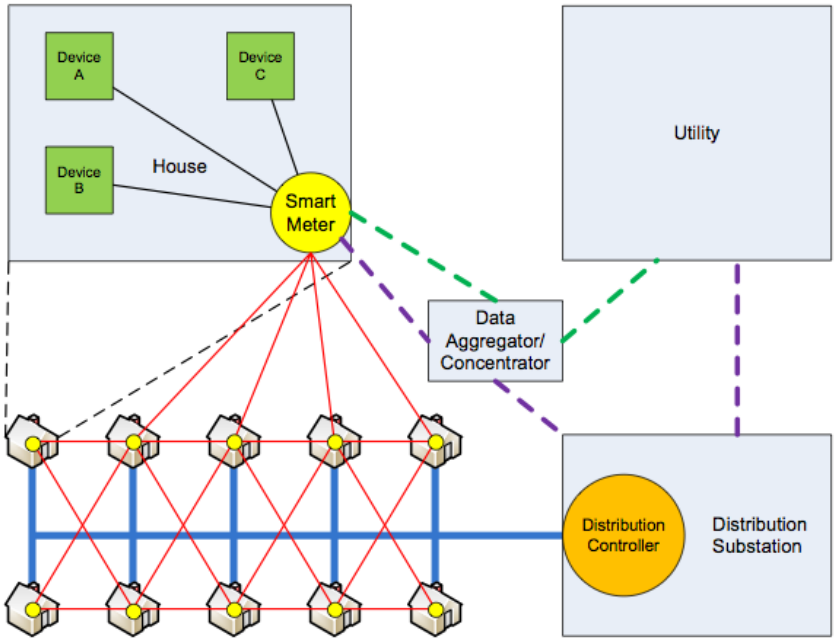
Smart Meter Data Anonymizing System

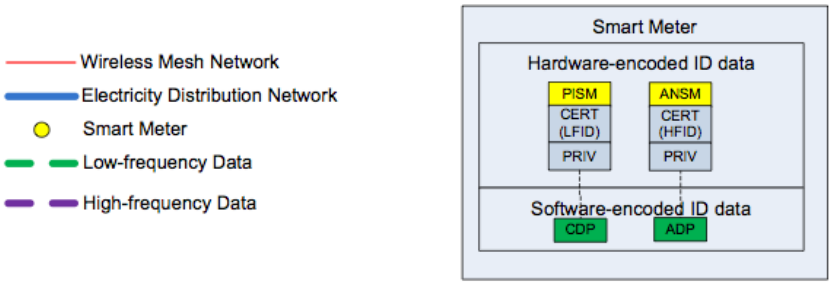
- Design basis: split data into two types
  - low frequency - for billing purposes
    - weekly / monthly aggregations
  - high frequency - for electric routing decisions / issue detection
    - seconds / minutes
- Concentrate on protecting high frequency data by anonymizing data within NAN

Smart Meter Data Anonymizing System

- Two IDs assigned to meter by manufacturer:
  - HFID (high-freq), "anonymous"
  - LFID (low-freq), public
- HFID known to manufacturer and trusted 3rd party
  - may be one in the same
- Meter sends HF data to a data collector assigned to its respective NAN

Smart Meter Data Anonymizing System

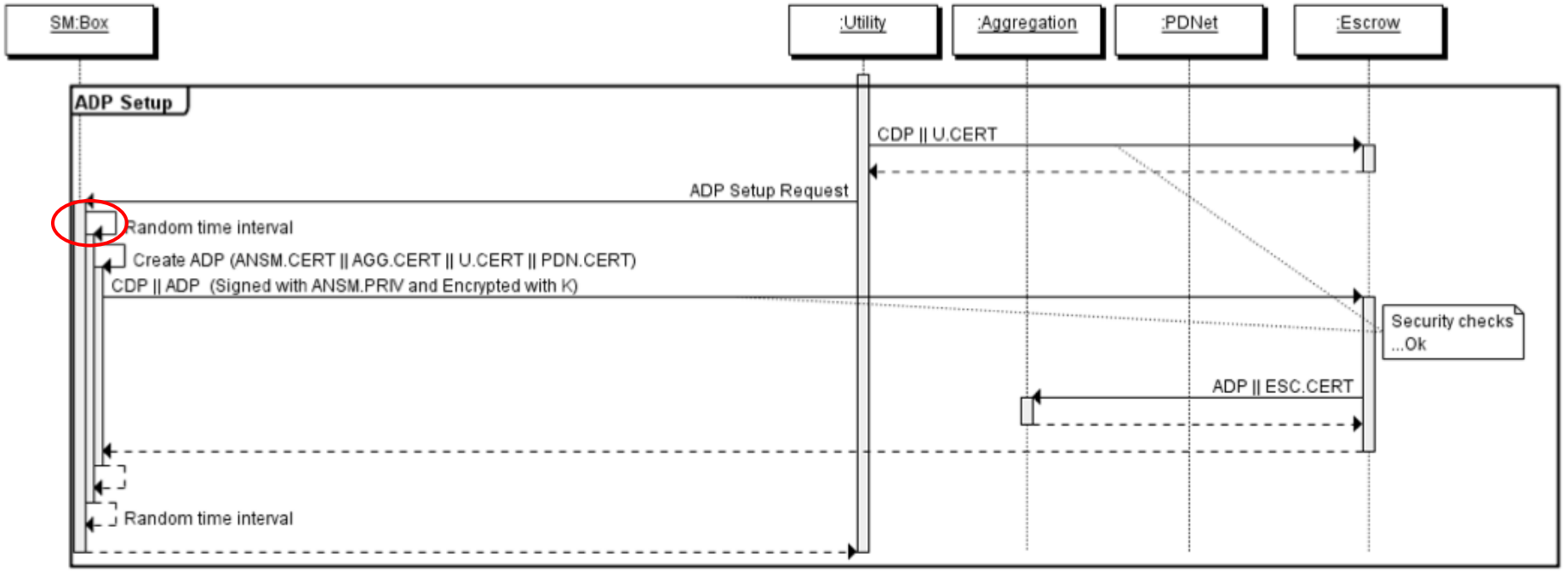




Smart Meter Data Anonymizing System

- Utility company is able to separate by individual meters, but cannot provide authentication
- This is where the trusted 3rd party comes in
  - third party "escrow" can facilitate authentication by checking against white-list of known HFIDs
  - utility sends IDs to escrow for verification
- What if the utility wants to send commands to the meter?
  - send to the aggregator; aggregator will forward to meter

Smart Meter Data Anonymizing System



Sequence diagram for ADP setup

Smart Meter Data Anonymizing System

- Some issues / open questions with this paper:
  - Who is the aggregator?
    - Very important question because aggregator holds the anonymous identities of each meter and their location
  - What if a meter fails the authentication?
    - In order to track down this meter, must ask the aggregator which location the meter is at
    - ...could potentially be abused to remove privacy

So far we've seen...

- Overview of Smart Grid
- Local Security
- Regional Security

To tie it all together...

Fault-Tolerant and Scalable Key Management for Smart Grid

Dapeng Wu, Chi Zhou

Problem

No existing authentication scheme meets Smart Grid's needs.

Existing solutions

- Consumer off-the-shelf
- Rely on existing security infrastructure of the Internet

New System?

- Better defend against DoS attacks
- Better fail-safe mechanisms

How to secure Smart Grid?

Interconnected Trust Realms

Trust Realms

Require 4 Principles

1. Trust Anchor
2. Data Aggregator
3. Data Collector
4. Sensors

Trust Anchor

Manage the realm's key distribution

Each TA has:

- One Private Key
- One Public Key

Data Aggregator

Able to perform complex data processing tasks

For data communications, each Data Aggregator has:

- A certified public key
- A certified private key

Data Collector

Data sensing and collecting agents

For communicating with other principals in its realm, each data collector has

- A certified public key
- A certified private key

Sensors

Low power devices for gathering data

To facilitate communications to other principals

- Smart card
- Two certificates for trust delegation
  - Issued by trust anchors

Public and Symmetric key

Public Key

- Elliptic Curve Cryptography

Symmetric Key

- Based on Needham-Schroeder auth. (think Kerberos)

Elliptic Curve Crypto

- Basis for public key scheme
  - high efficiency
    - Based on discrete logs
    - Equal difficulty to RSA at shorter length

But wait: there's more!

Elliptic Curve Crypto

- Basis for public key scheme
  - high efficiency
    - Based on discrete logs
    - Equal difficulty to RSA at shorter length

Bonus!

- Generated on-the-fly
  - No static symmetric key needed btw aggregators and collectors
  - Avoids
    - threat of compromised symmetric keys
    - reduced management overhead

Needham-Schroeder

1. A → T: A, B, N_A
2. T → A: $\{N_A, B, K_{AB}, \{K_{AB}, A\}K_{BT}\}K_{AT}$
3. A → B: $\{K_{AB}, A\}K_{BT}$
4. B → A: $\{N_B\}K_{AB}$
5. A → B: $\{N_B+1\}K_{AB}$

A and B: Alice and Bob
T: Trusted Server
K: symmetric key

Problems with N-S protocol?

1. A → T: A, B, N_A
2. T → A: $\{N_A, B, K_{AB}, \{K_{AB}, A\}K_{BT}\}K_{AT}$
3. A → B: $\{K_{AB}, A\}K_{BT}$
4. B → A: $\{N_B\}K_{AB}$
5. A → B: $\{N_B+1\}K_{AB}$

Any Ideas?

Problems with N-S protocol?

Replay attack using old $\{K_{AB}, A\}K_{BT}$

Kerberos fix:

- timestamps
- nonces

Would this work in Smart Grid, too?

Time Trickiness in WSN

- Small sensors, small resources
  - real-time clocks have intrinsic drift
  - can't reliably handle authentication-grade accuracy
    - If times overlap
      - nonces not necessarily one-time
      - Messages not necessarily fresh
- Transmission times
  - The higher the bandwidth
    - more messages
    - tighter time requirements
    - more vulnerability to replay

Fixing N-S in WSN

- Hardware implementation
- Ensure
  - Timestamp - details in paper
  - Once-only nonce

Once-Only Nonce: Ideal solution

Just use a random bit generator!

Once-Only Nonce: Practical Implementation

timestamp
\+ nonce
pseudorandom bit seq

Practical Solution

Smart Grid
Key Management

Needham Schroeder + Elliptic Curve Crypto

Smart Grid PKI

- Trust Delegation
  - Trust Anchor
    - Establish symmetric keys with agents
    - Sensors access local grid via agents

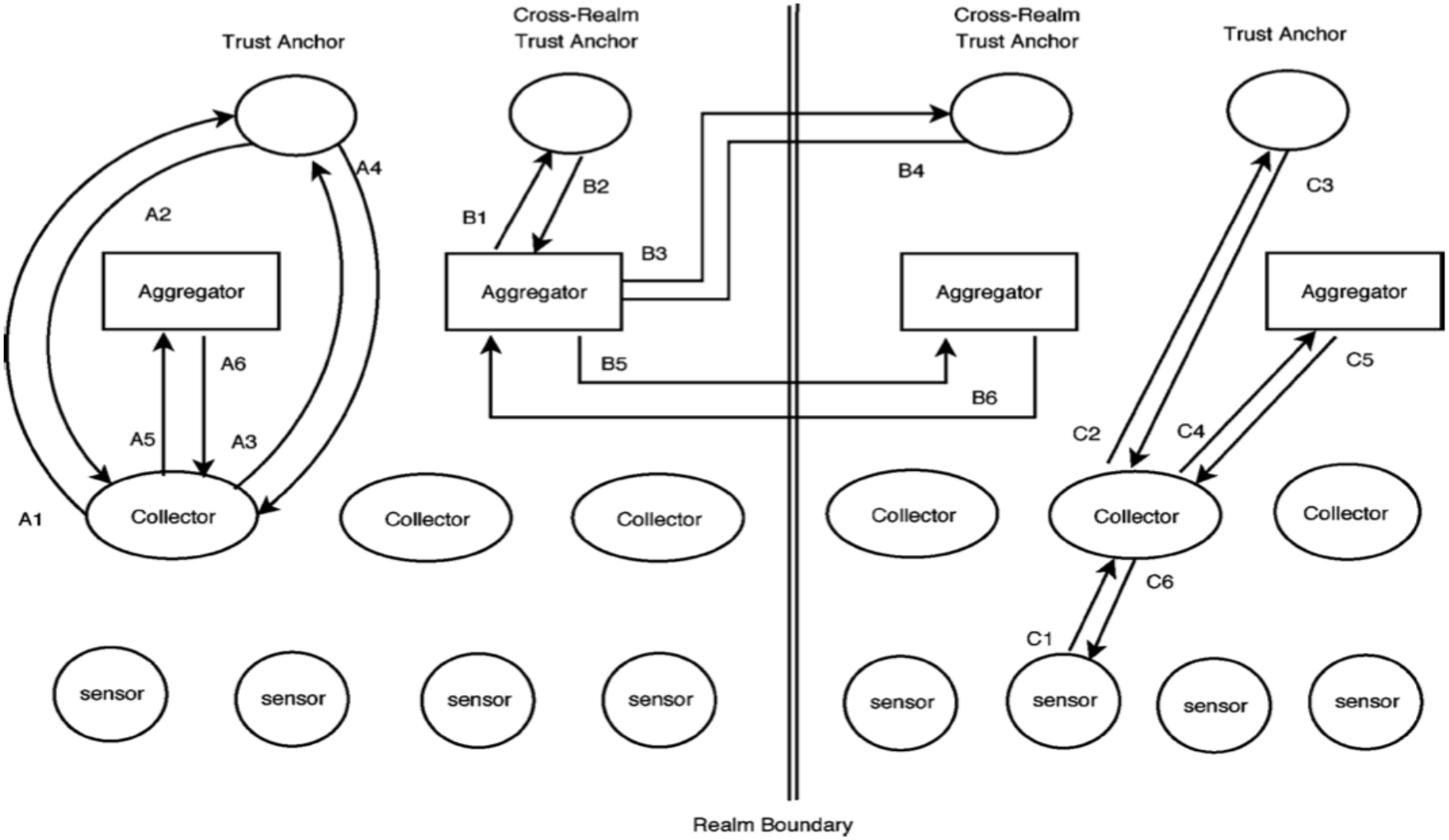
- Sensors and all agents issued
  - Private key
  - Certificate of a public key

Symmetric Keys

- Generated on the fly
- Used in the successive Needham-Schroeder authentication

Putting it all together...

How it works


Trust Anchor
Cross-Realm
Trust Anchor
Cross-Realm
Trust Anchor
Trust Anchor
A1
A2
A3
A4
A5
A6
B1
B2
B3
B4
B5
B6
C1
C2
C3
C4
C5
C6
Aggregator
Aggregator
Aggregator
Aggregator
Collector
Collector
Collector
Collector
Collector
Collector
sensor
sensor
sensor
sensor
sensor
sensor
sensor
sensor
Realm Boundary

Mutual Authentication

- Collector and Aggregator
- Aggregators between Realms
- Sensor and Collector

Mutual Authentication: Collector and Aggregator

Collector initiates the authentication process by sending Message A1 to a trust anchor.

Trust anchor sends Message A2 (containing a symmetric key) to the collector.

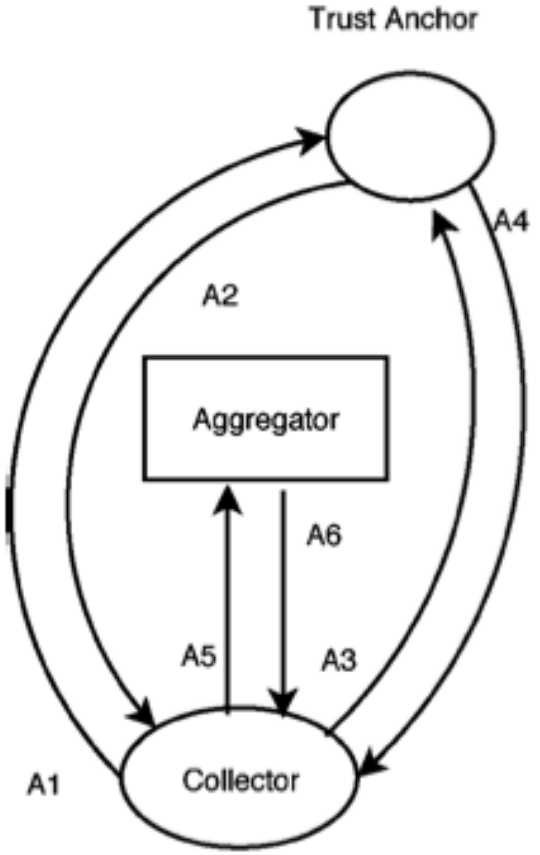
To obtain a session key, the same procedure as that in the Needham- Schroeder protocol is used:

The collector sends Message A3 to the trust anchor

Trust anchor replies the collector by Message A4

Collector sends Message A5 to an aggregator

Aggregator replies the collector by Message A6



Mutual Authentication: Aggregators btw Realms

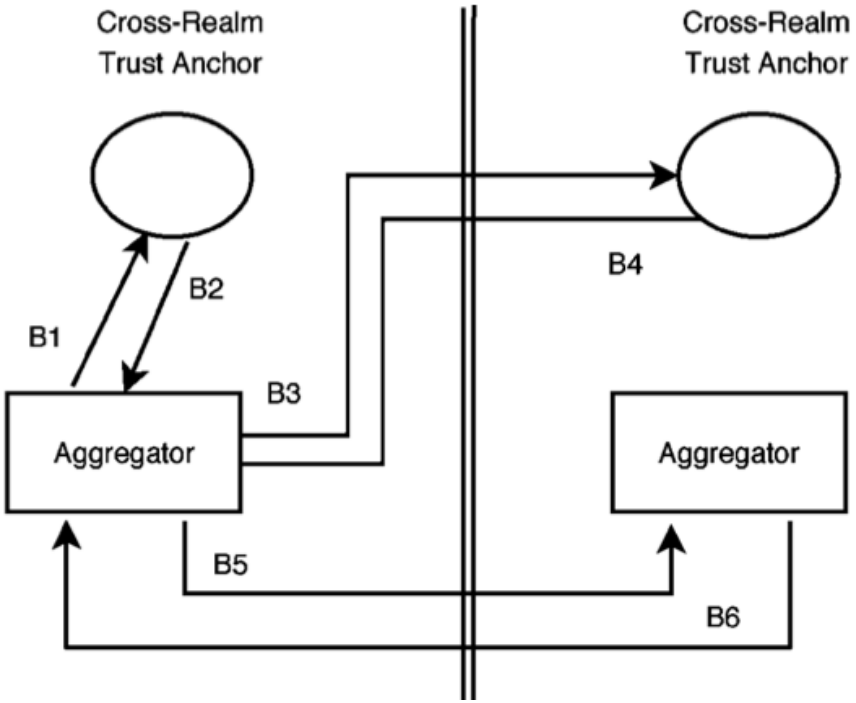
Aggregator initiates authentication process

- sends Message B1 to a trust anchor in the same realm.

Trust anchor sends Message B2 (containing a symmetric key) to the aggregator.

To obtain a session key, the same procedure as that in the Needham-Schroeder protocol is used:

- Aggregator sends Message B3 to a trust anchor in another realm
- Trust anchor replies the aggregator by Message B4
- Aggregator sends Message B5 to an aggregator in another realm
- Aggregator in another realm replies the originating aggregator by Message B6

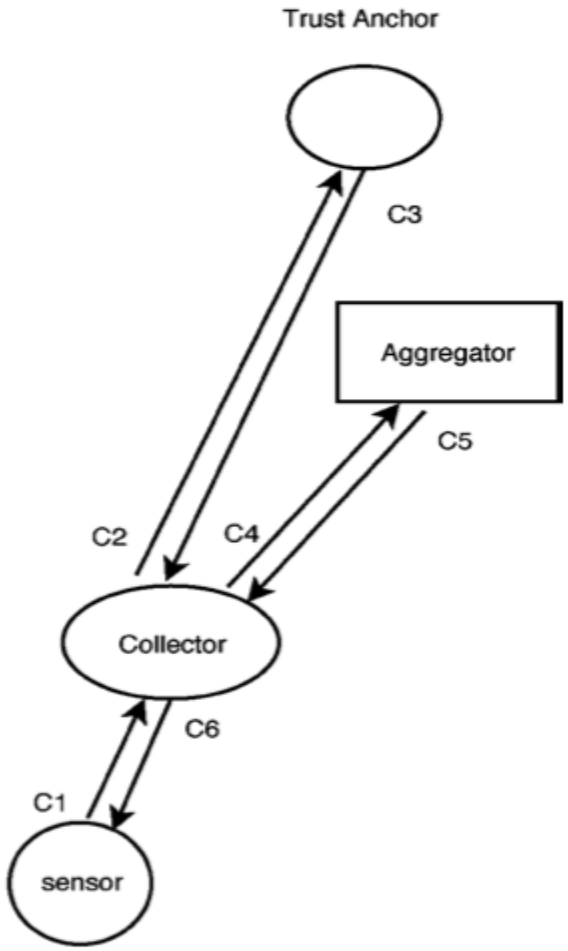


Mutual Authentication: Sensor and Collector

Messages C1 and C6 are used for trust delegation request and verification.

Messages C2 and C3 are used to acquire a symmetric key.

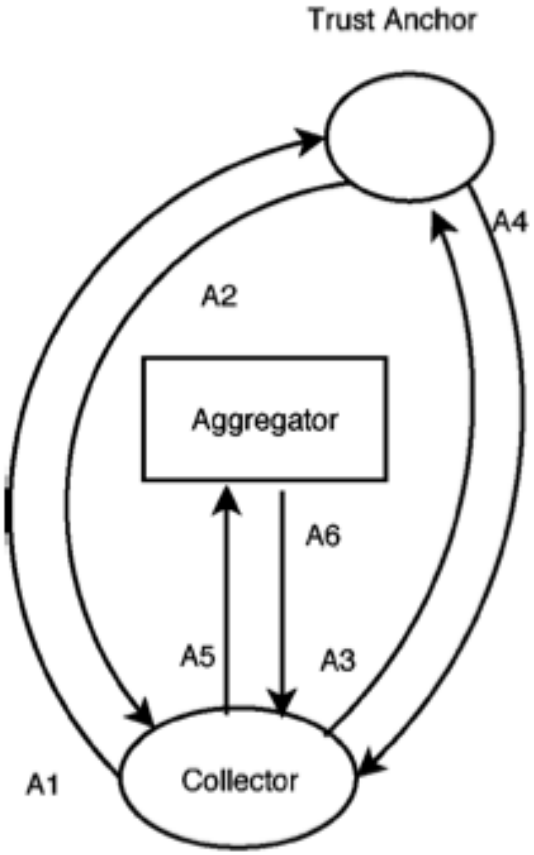
Messages C4 and C5 are used for the session key delivery



More details on session key delivery here:

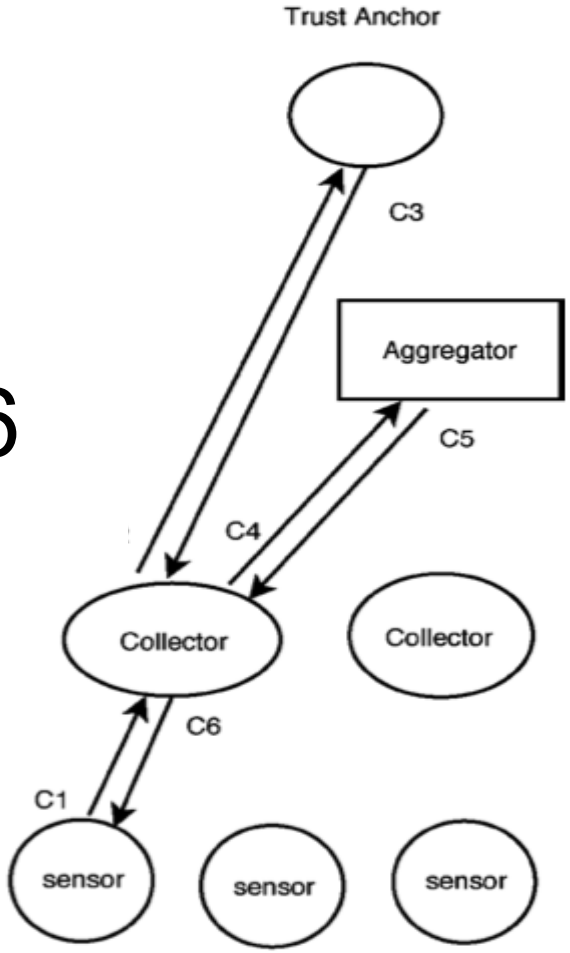
[C. Tang and D. O. Wu, "An efficient mobile authentication scheme for wireless networks," IEEE Trans. Wireless Commun., vol. 7, no. 4, pp.1408–1416, Apr. 2008.]

Session keys through Needham-Schroeder

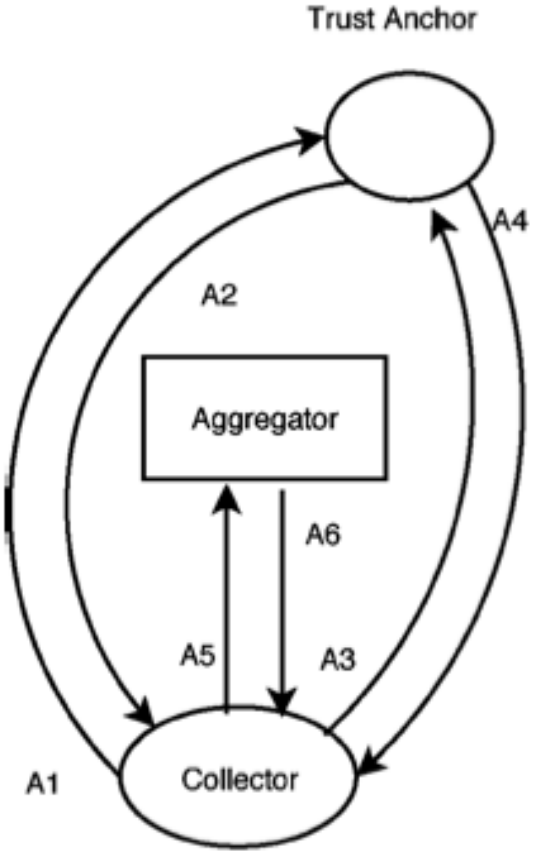


Messages 3-6

More on the specific application of the protocol is in the paper

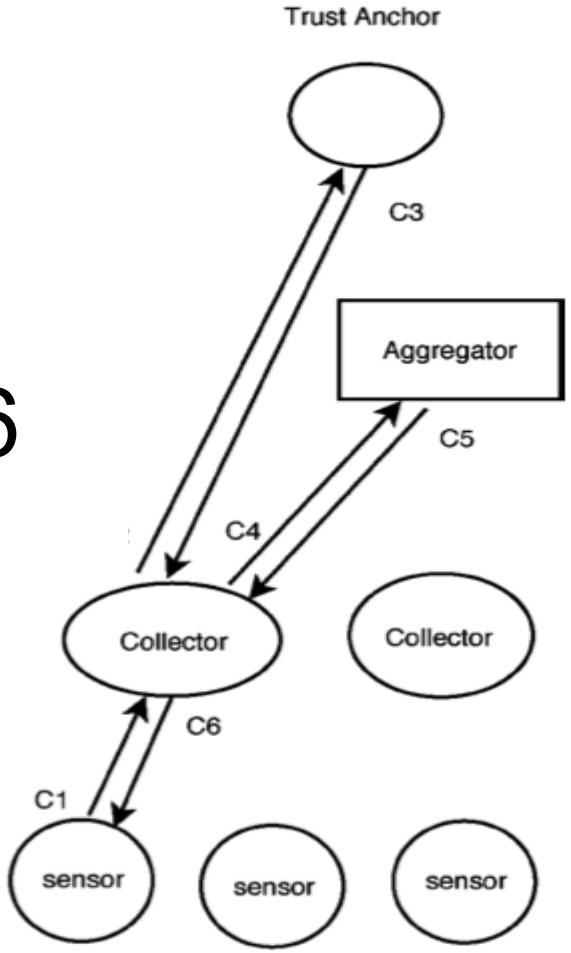


Comm. keys through Needham-Schroeder



Messages 3-6

Straight implementation of Needham-Schroeder



Benefits of System

- Simple TA key management
  - on-the-fly key generation: don't have to maintain shared symmetric keys
- Key generation speed
  - TAs can assign another TA with a lighter load to issue a session key
- Fault Tolerance
  - If one TA fails, just designate another one

Other Benefits

- Elliptic Key Cryptography helps keep message size small (around 100 bytes)
- Easy to manage system
  - Ex: Add new aggregator?
    - +1 certificate
    - +1 private key
  - Remove?
    - Just disqualify certificate
- Very scalable system

Well then...

So then why hasn't the smart grid been implemented yet?

The Path of the Smart Grid

Hassan Farangi

Business Logic

- The power grid is a business and like every business there must be ROI
  - What strategies will allow for maximization of ROI?
- Already invested in the Advanced Metering Infrastructure (AMI)
  - Smart Grid must be built on top of current infrastructure so as to not waste investment
- Can't convert the system all in one day and therefore it must be done in increments

Other Reasons

- Trying to integrate disparate systems as we all know is hard

- Lack of Standards
  - NIST is working to create some standards
    - NIST Framework and Roadmap for Smart Grid Interoperability Standards (Release 1.0, Sept 2009)

Questions?

image: http://rlv.zcache.com/question_mark_hat-p148553218496209654enxqz_400.jpg

References

- Aravinthan, V.; Namboodiri, V.; Sunku, S.; Jewell, W.; , "Wireless AMI application and security for controlled home area networks," *Power and Energy Society General Meeting, 2011 IEEE* , vol., no., pp.1-8, 24-29 July 2011
- Dapeng Wu; Chi Zhou; , "Fault-Tolerant and Scalable Key Management for Smart Grid," *Smart Grid, IEEE Transactions on* , vol.2, no.2, pp.375-381, June 2011
- Efthymiou, C.; Kalogridis, G.; , "Smart Grid Privacy via Anonymization of Smart Metering Data," *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on* , vol., no., pp.238-243, 4-6 Oct. 2010
- Farhangi, H.; , "The path of the smart grid," *Power and Energy Magazine, IEEE* , vol.8, no.1, pp.18-28, January-February 2010