Privacy- and Data-Aware Smart Grid Communication

by Vitaly Ford

Ph.D. Candidate

Cybersecurity Education Research and Outreach Center

Tennessee Tech University

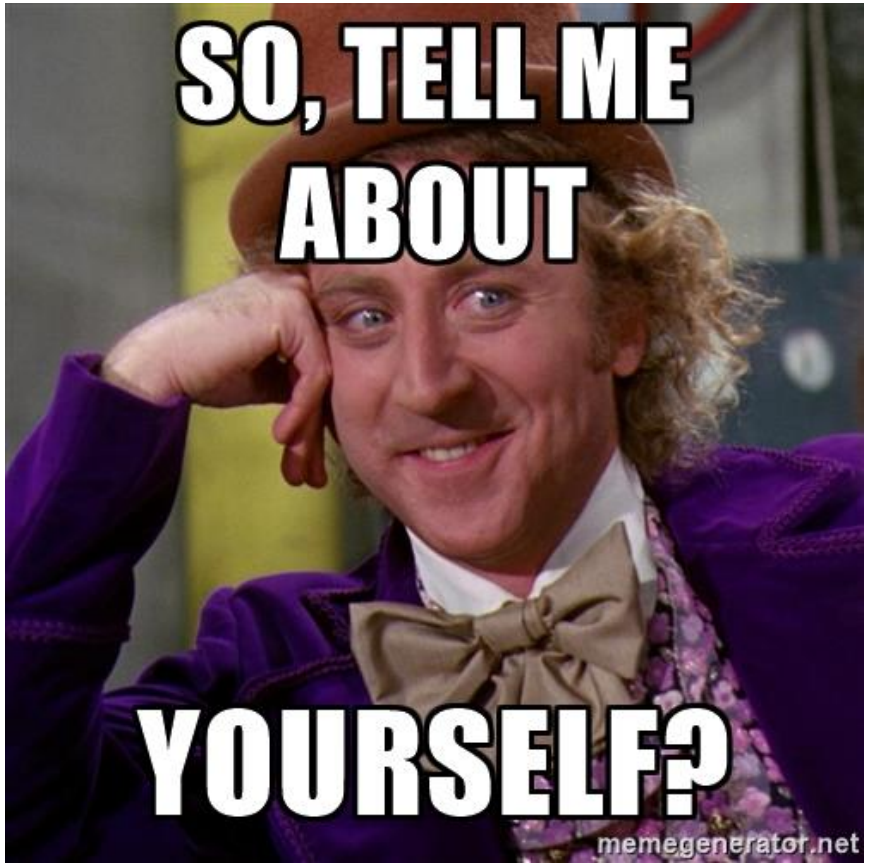
Advisor: Dr. Ambareen Siraj

Location: Rochester Institute of Technology

October 18, 2016

#whoami

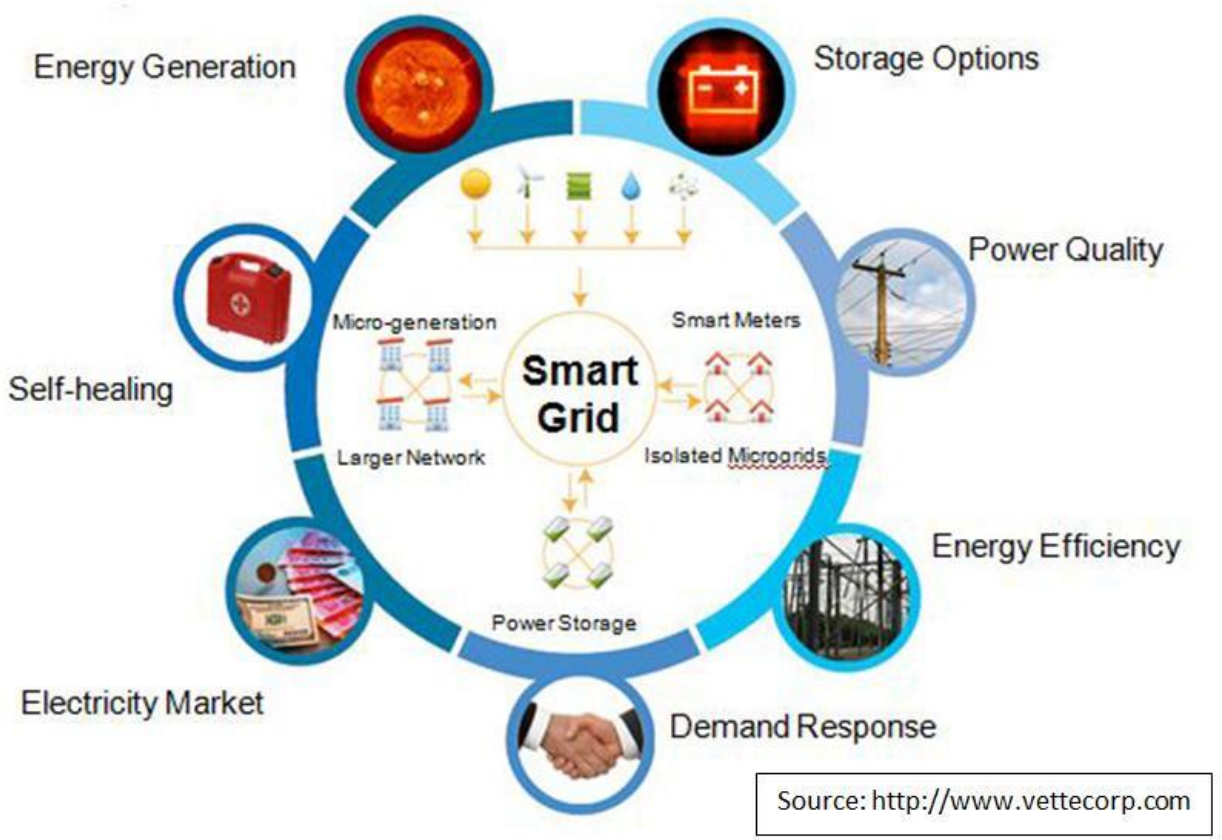
- Ph.D. Candidate at Tennessee Tech, Research Assistant, CEROC
- Smart Grid security and cybersecurity education researcher
- Instructor: Principles of Computing
- Coach Southeast Collegiate Cyber Defense Competition and Collegiate Penetration Testing Competition
  - SE CCDC participant: 2014, 2015
  - Capture the Flag participant since 2012
- CyberEagles Club founder
- Mentor for undergraduate/graduate students



55 32 46 35 49 45 4a 70 62 6d 64 76 49 51 3d 3d

Outline

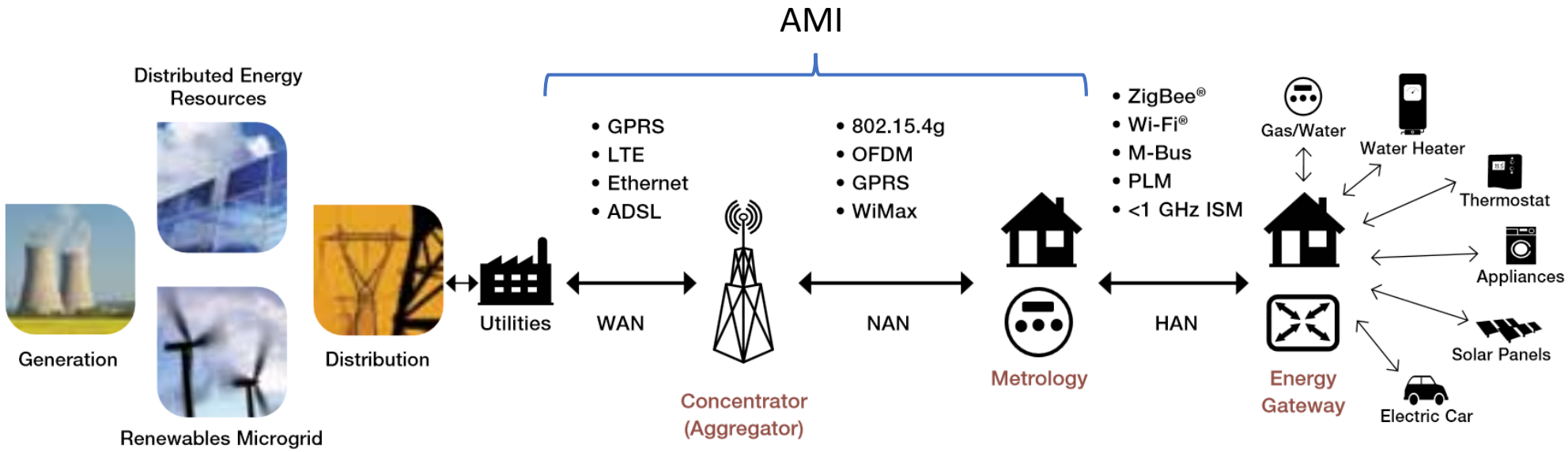
- Smart Grid
  - Advanced Metering Infrastructure (AMI)
  - Smart Meter
  - Characteristics
- Privacy and Security Issues
- Existing Solutions
- Privacy- and Data-Aware Scheme



Source: http://www.vettecorp.com

55 32 46 35 49 45 4a 70 62 6d 64 76 49 51 3d 3d

Smart Grid Network Model: Big Picture



- Smart meters receive info about appliances from the hub at the house
- Smart meters send data to the aggregator
- Aggregator forwards data to the utility company

55 32 46 35 49 45 4a 70 62 6d 64 76 49 51 3d 3d

Advanced Metering Infrastructure (AMI)

- Meters gather data every second
- Two network models:
  - One-hop
  - Multi-hop

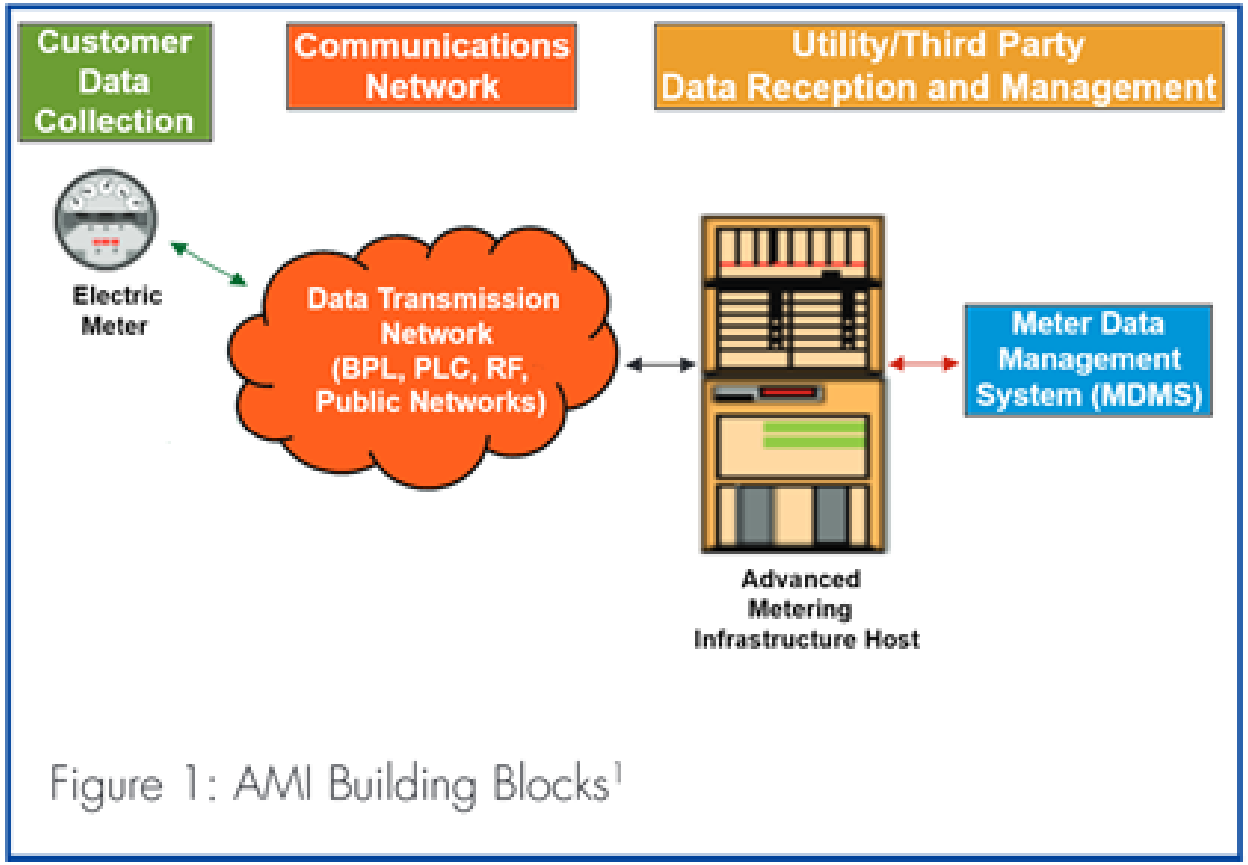
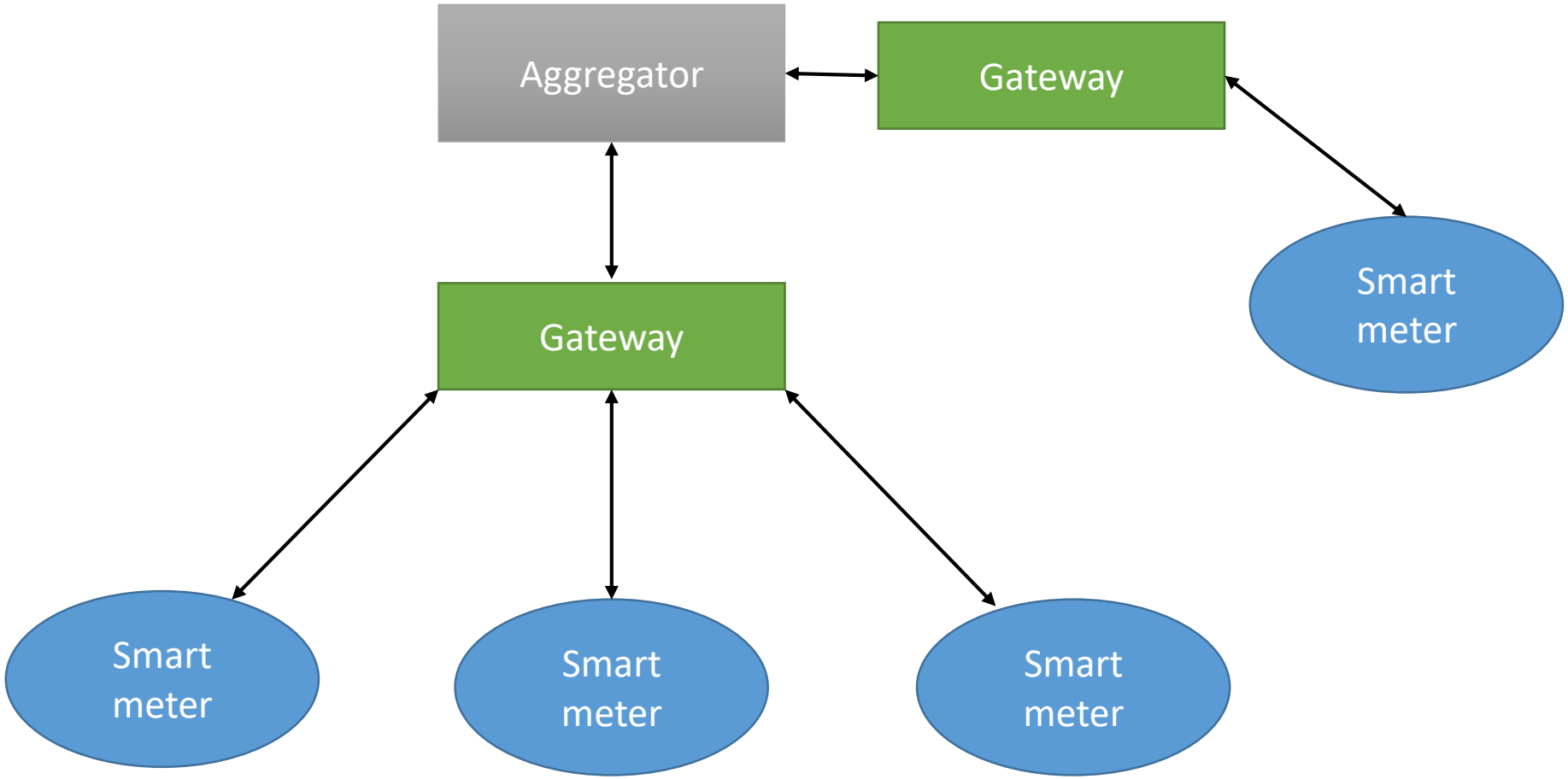


Figure 1: AMI Building Blocks[1]

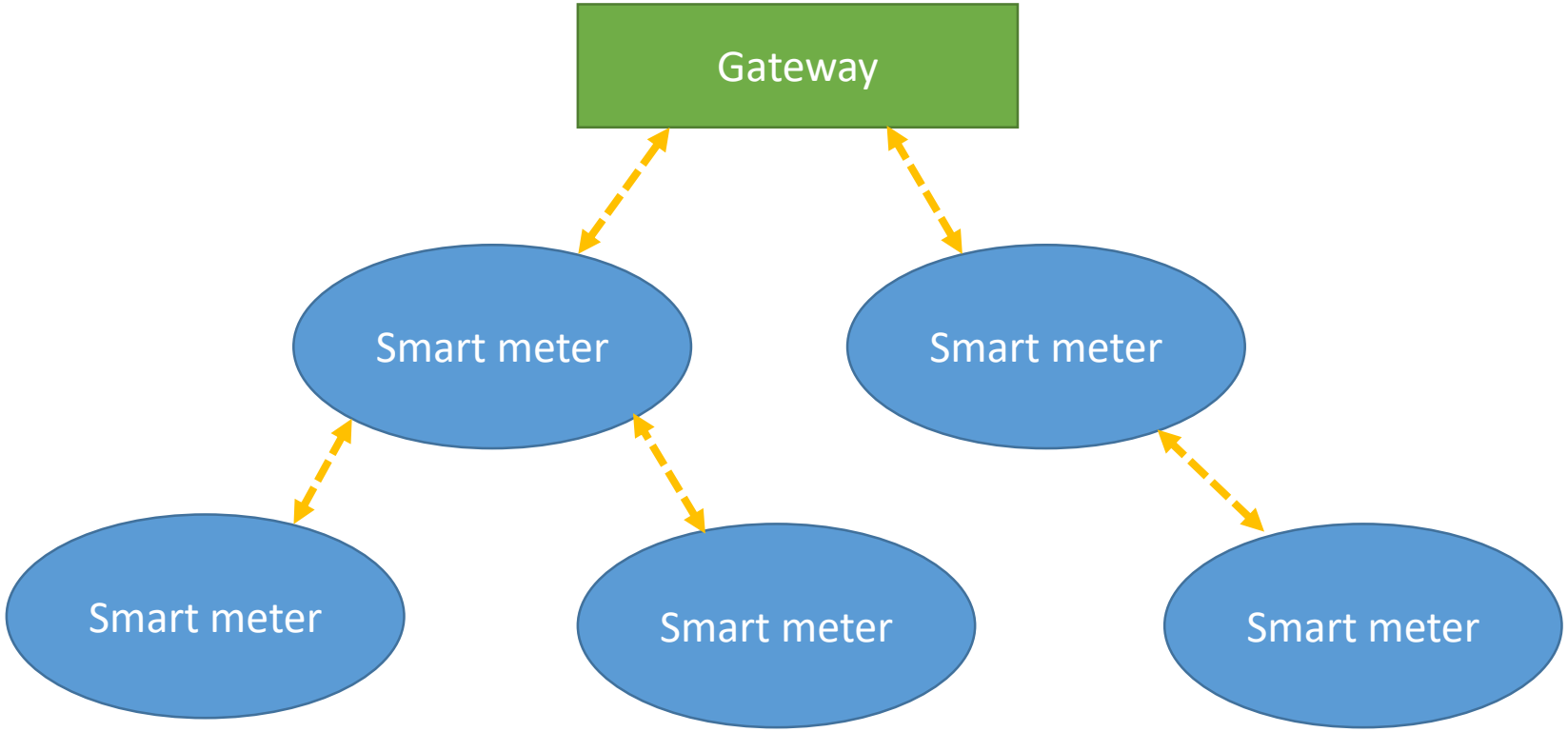
55 32 46 35 49 45 4a 70 62 6d 64 76 49 51 3d 3d

One-Hop AMI



55 32 46 35 49 45 4a 70 62 6d 64 76 49 51 3d 3d

Multi-Hop AMI



55 32 46 35 49 45 4a 70 62 6d 64 76 49 51 3d 3d

AMI Benefits

System Operation

Customer Service

Financial

55 32 46 35 49 45 4a 70 62 6d 64 76 49 51 3d 3d

AMI Benefits: System Operation

- Increased meter reading accuracy
- Easier energy theft detection due to real-time energy consumption data
  - Providing service to 3.3 million people, $65 million was lost to fraud, 2015

https://www.sas.com/content/dam/SAS/en_us/doc/solutionbrief/utilities-detect-reduce-energy-theft-106064.pdf

- Easier outage management

  due to two-way communication

55 32 46 35 49 45 4a 70 62 6d 64 76 49 51 3d 3d

AMI Benefits: Customer Service

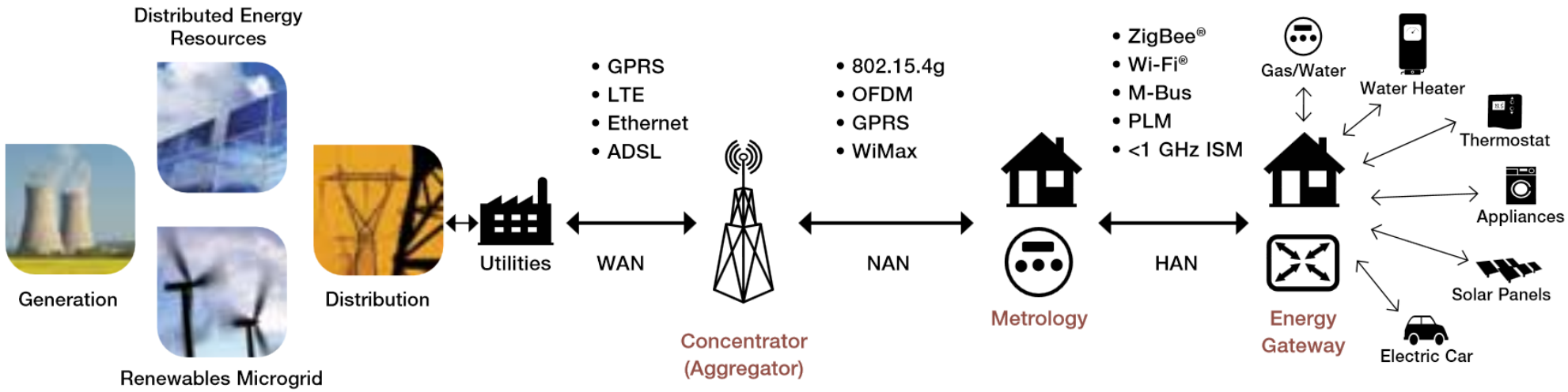
- Early detection of meter failures
  - Due to two-way communication, utilities can monitor the meter status
- Variety of time-based rate options
  - Utility companies can change electricity price in real-time
  - Consumers can decrease their bills by using appliances when the cost is less
- Customer energy profiles
  - Access to energy profiles to see how we can utilize appliances more efficiently
  - Industries can detect if their big machines consume more energy due to failure

55 32 46 35 49 45 4a 70 62 6d 64 76 49 51 3d 3d

AMI Benefits: Financial Benefits for Utilities

- Reduced equipment maintenance cost
  - Most maintenance can be done remotely
- Faster restoration and shorter outages
  - Meters and smart devices provide real-time status information and locality so that utilities can easily pinpoint the problem and resolve it

55 32 46 35 49 45 4a 70 62 6d 64 76 49 51 3d 3d

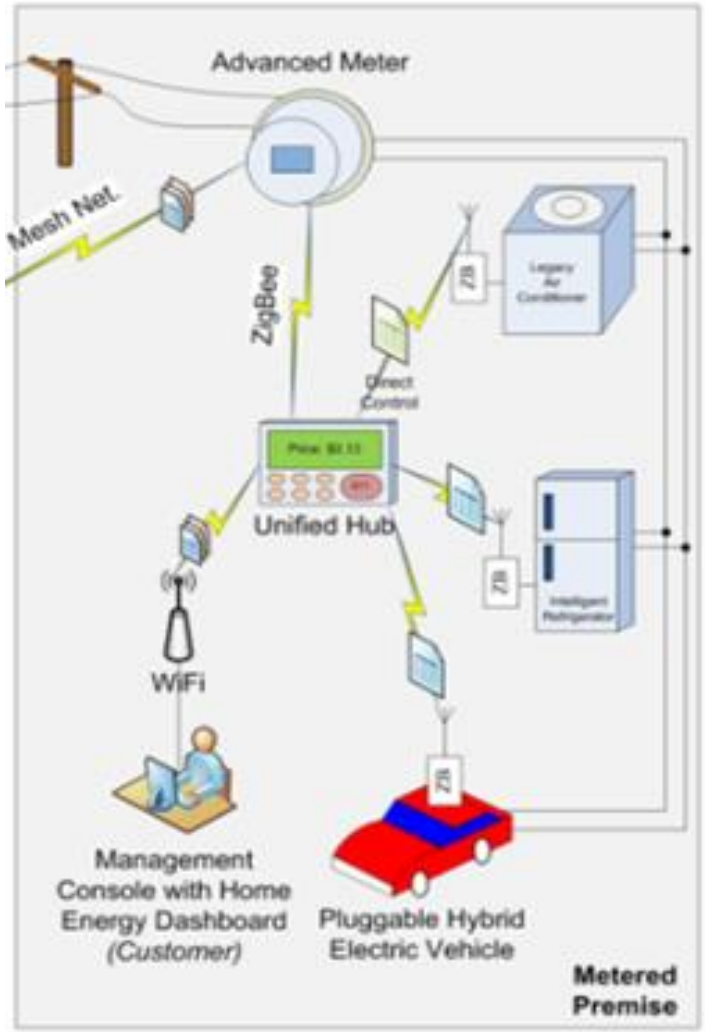


Home Area Network (HAN)

55 32 46 35 49 45 4a 70 62 6d 64 76 49 51 3d 3d

HAN Model

- A unified hub collects data from home appliances and sends to a smart meter
- Each meter reads energy consumption, connecting to a unified hub via ZigBee
- Smart meters are organized in a mesh network connected to the meter data management service
- **Example**: if utility can turn air conditioners in the whole neighborhood at the same time, then it can decrease electricity fluctuations



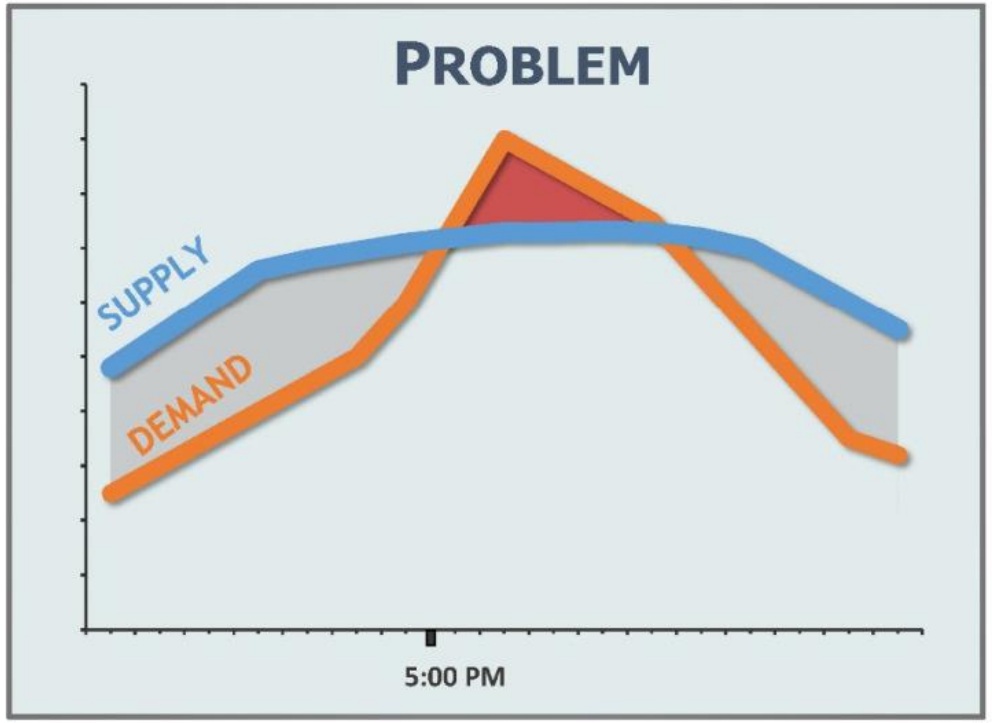
55 32 46 35 49 45 4a 70 62 6d 64 76 49 51 3d 3d

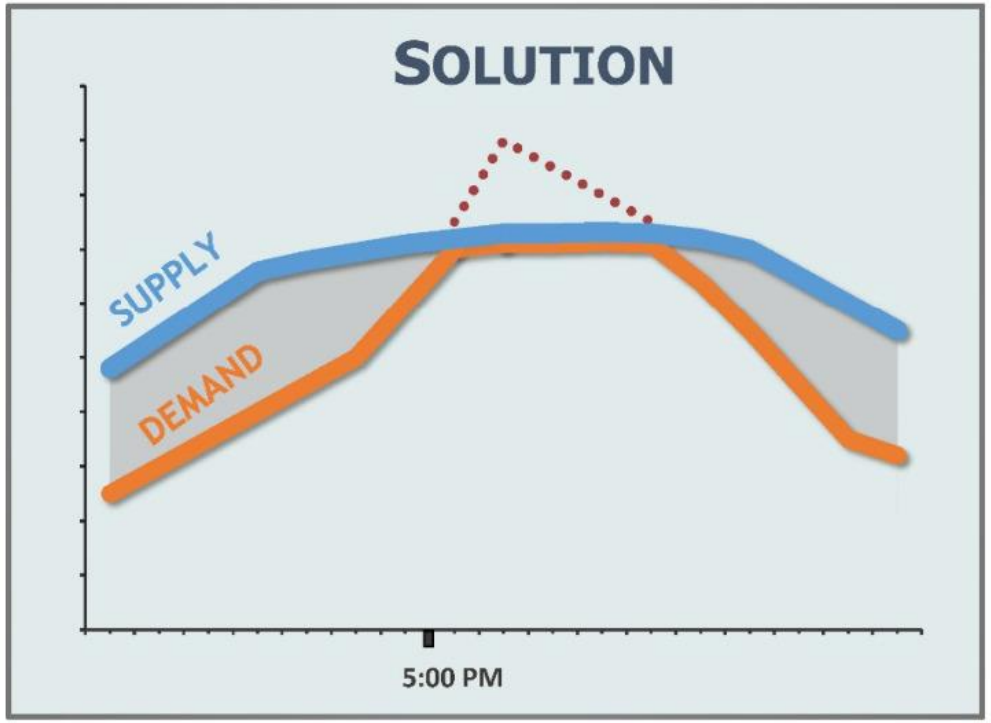
Smart Meter

- Energy monitoring device
- Wireless technologies
- Two-way communication
  - Send granular data in real-time
  - Remote maintenance
  - **Real-time pricing**

55 32 46 35 49 45 4a 70 62 6d 64 76 49 51 3d 3d

Supply-Demand Problem

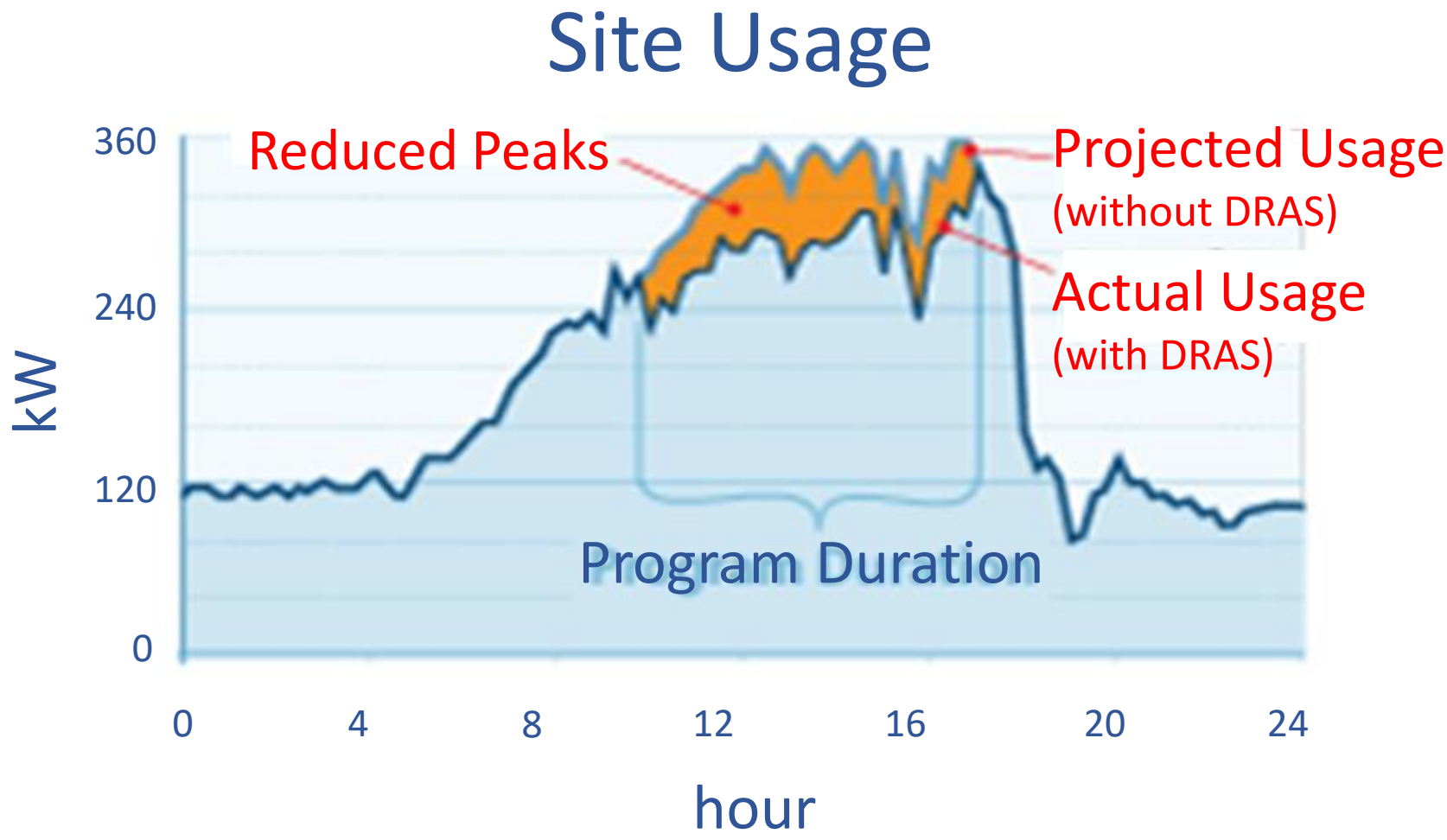




https://jasmasenergy.files.wordpress.com/2016/02/demand-response-graphic.jpg?w=1620

55 32 46 35 49 45 4a 70 62 6d 64 76 49 51 3d 3d

Demand-Response



55 32 46 35 49 45 4a 70 62 6d 64 76 49 51 3d 3d

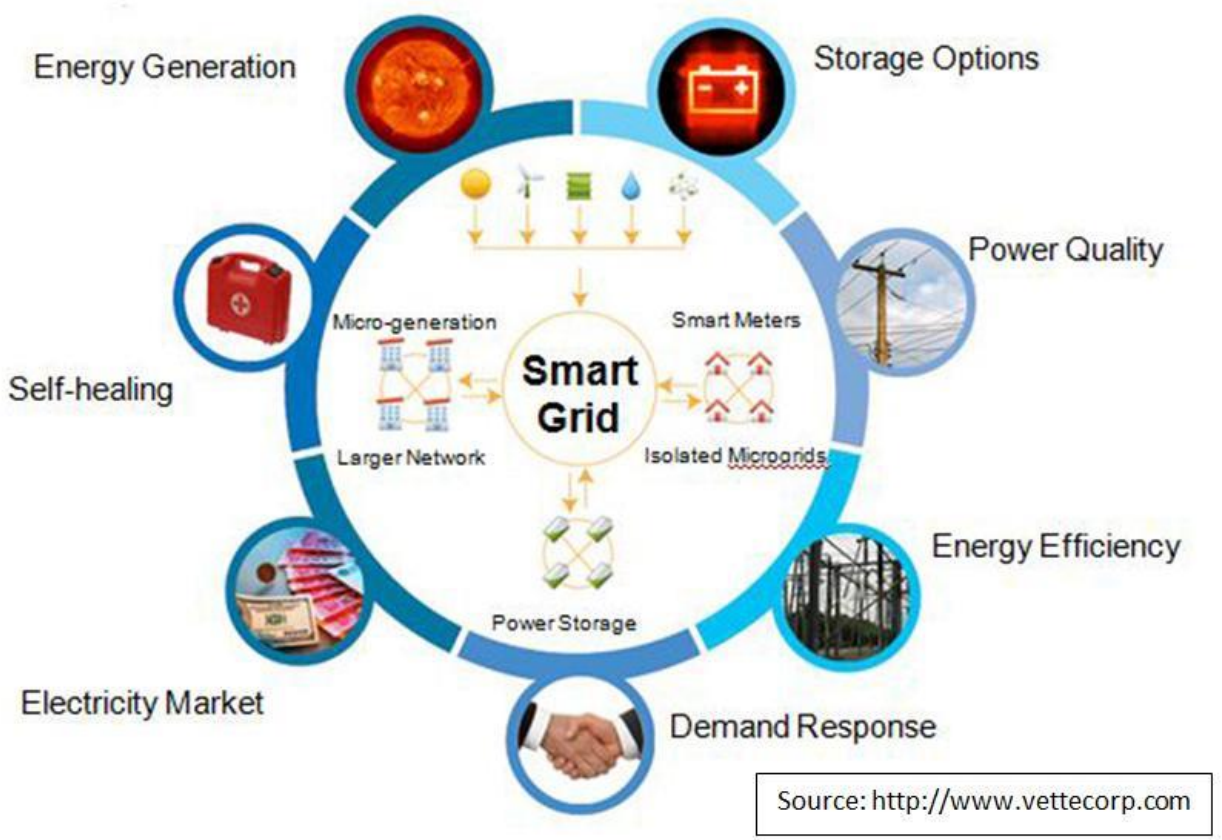
Demand-Response Outlook (cont.)

- Direct load control
  - Allows utilities to turn specific appliances on and off during peak demand periods and critical events
  - Load management saves money for both utilities and customers by reducing the need for the generation capacity and minimizing the amount of energy a utility must purchase on the open market at peak demand periods

55 32 46 35 49 45 4a 70 62 6d 64 76 49 51 3d 3d

Outline

- Smart Grid
  - Advanced Metering Infrastructure (AMI)
  - Smart Meter
  - Characteristics
- Privacy and Security Issues
- Existing Solutions
- Privacy- and Data-Aware Scheme



Source: http://www.vettecorp.com

55 32 46 35 49 45 4a 70 62 6d 64 76 49 51 3d 3d

Security Issues

- Denial of Service Attacks
- False-data Injections
- Man-in-the-middle Attacks
- Energy Fraud Attacks
- Authentication Attacks
- Disaggregation Attacks

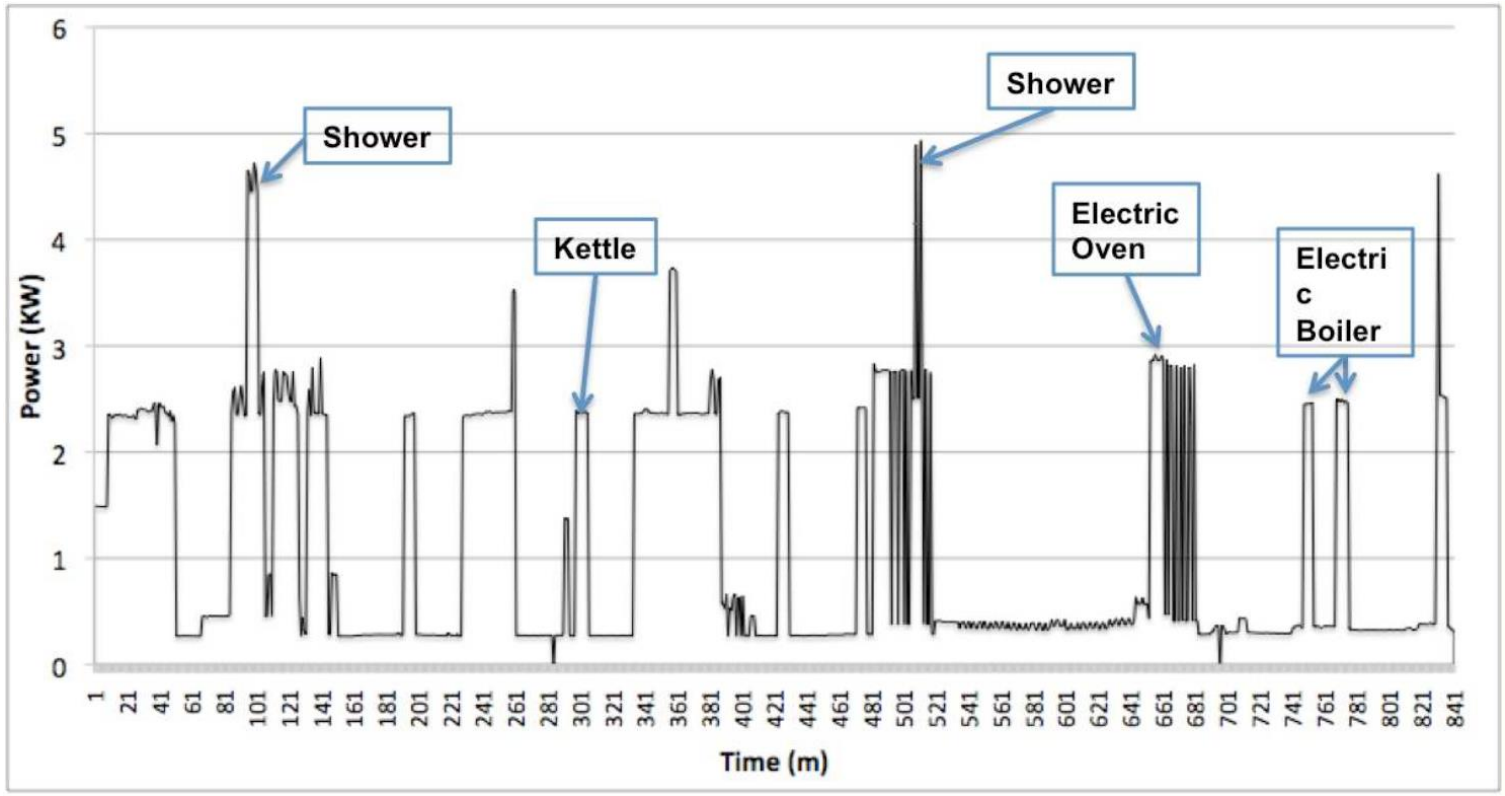
55 32 46 35 49 45 4a 70 62 6d 64 76 49 51 3d 3d

Consumer Privacy Violation

- Burglary preparation
- Targeted advertising
- Stalkers may exploit the data to discover victim’s home occupancy
- Risk assessment for insurance companies
- Parents “spying” on their children
- Landlords may determine if tenants violate the renting agreement
- Law enforcement agencies to discover illegal activities
- Businesses may analyze their competitors
- An employer can learn sleeping and eating habits of their employees

55 32 46 35 49 45 4a 70 62 6d 64 76 49 51 3d 3d

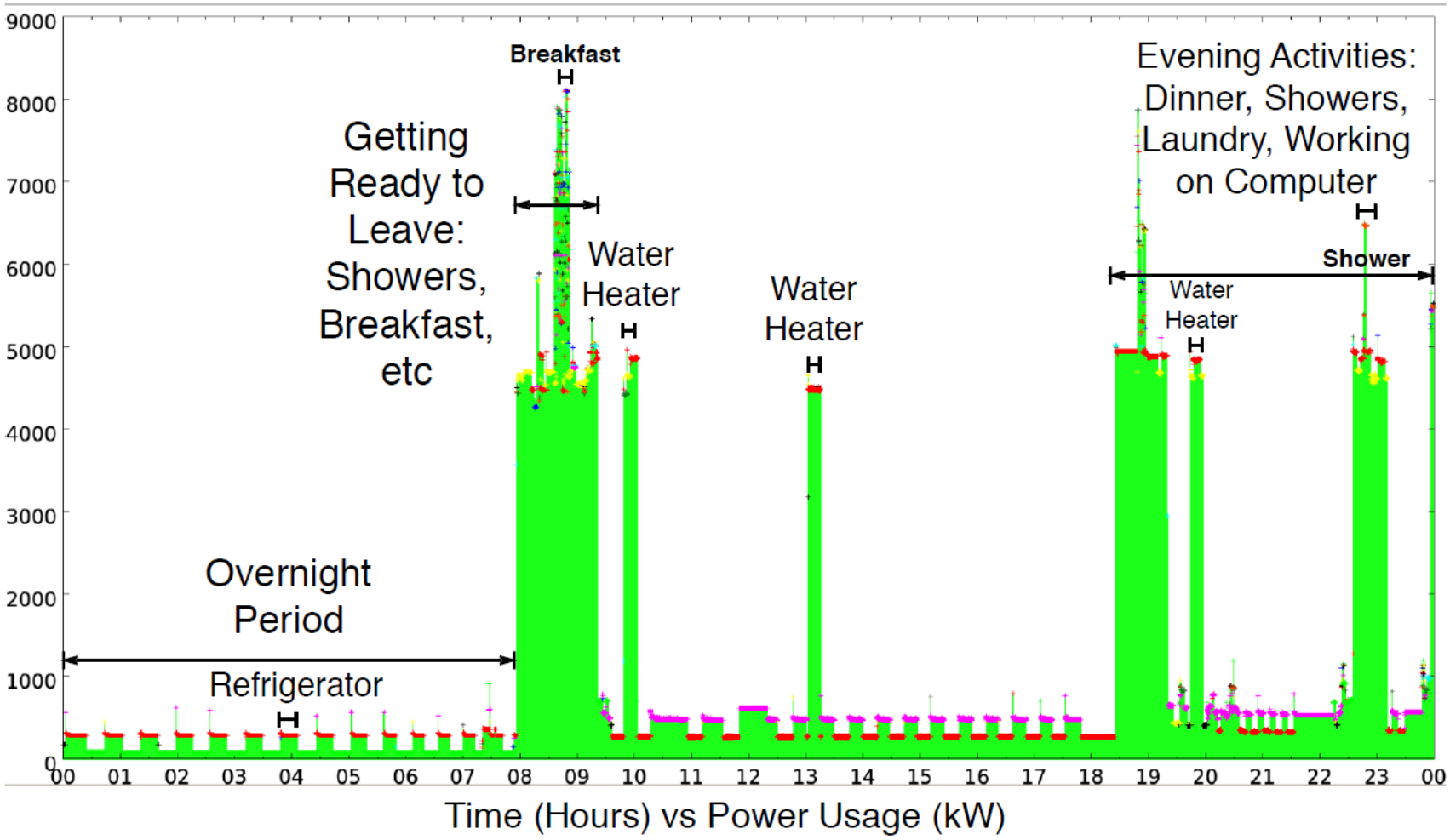
Profiling Consumer Energy Consumption



Ruzzelli, Antonio G., et al. "Real-time recognition and profiling of appliances through a single electricity sensor." *2010 7th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON)*. IEEE, 2010.

55 32 46 35 49 45 4a 70 62 6d 64 76 49 51 3d 3d

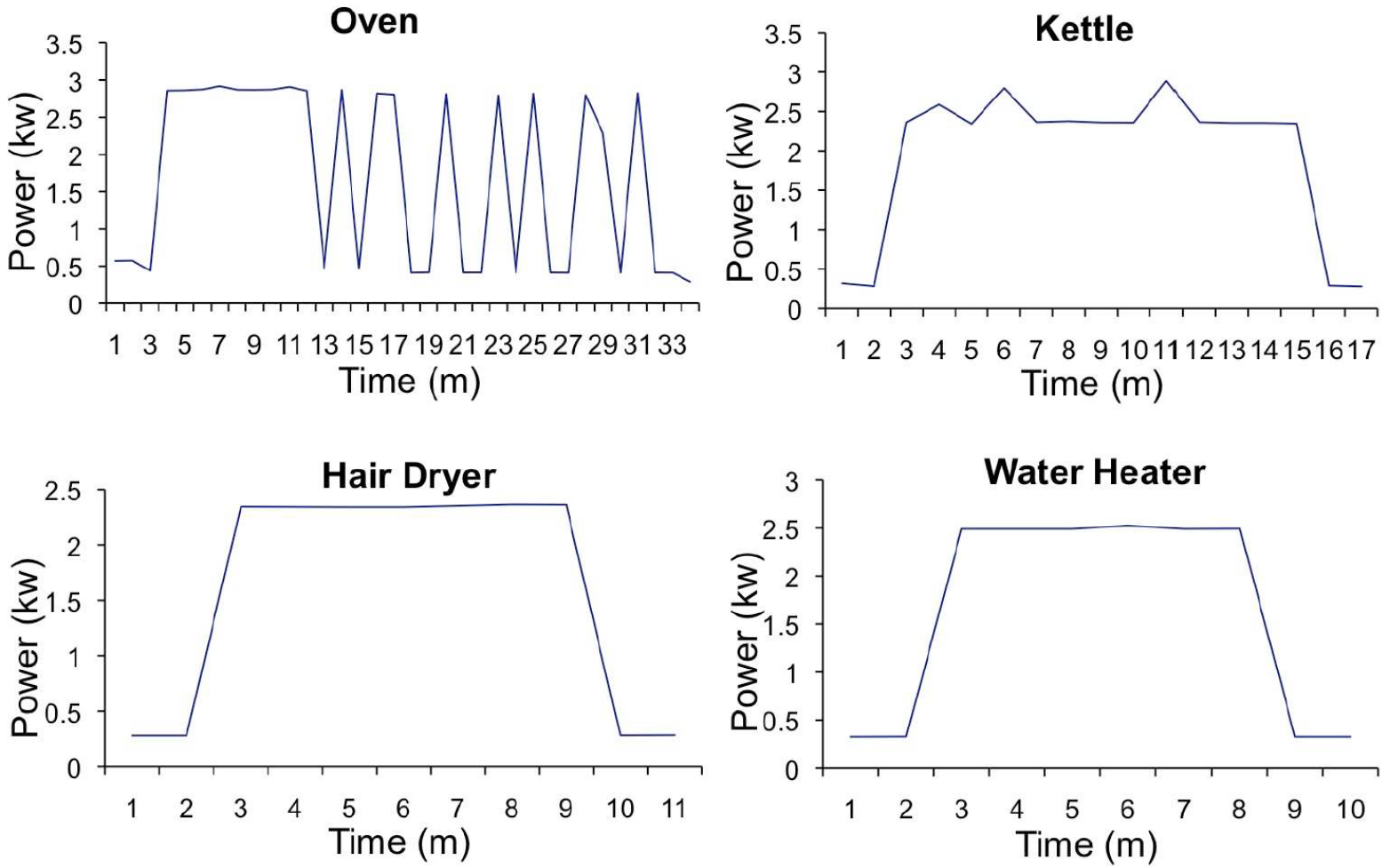
Granular Energy Consumption Data



Molina-Markham, Andrés, et al. "Private memoirs of a smart meter."*Proceedings of the 2nd ACM workshop on embedded sensing systems for energy-efficiency in building*. ACM, 2010.

55 32 46 35 49 45 4a 70 62 6d 64 76 49 51 3d 3d

Active Power Signatures for 4 Appliances

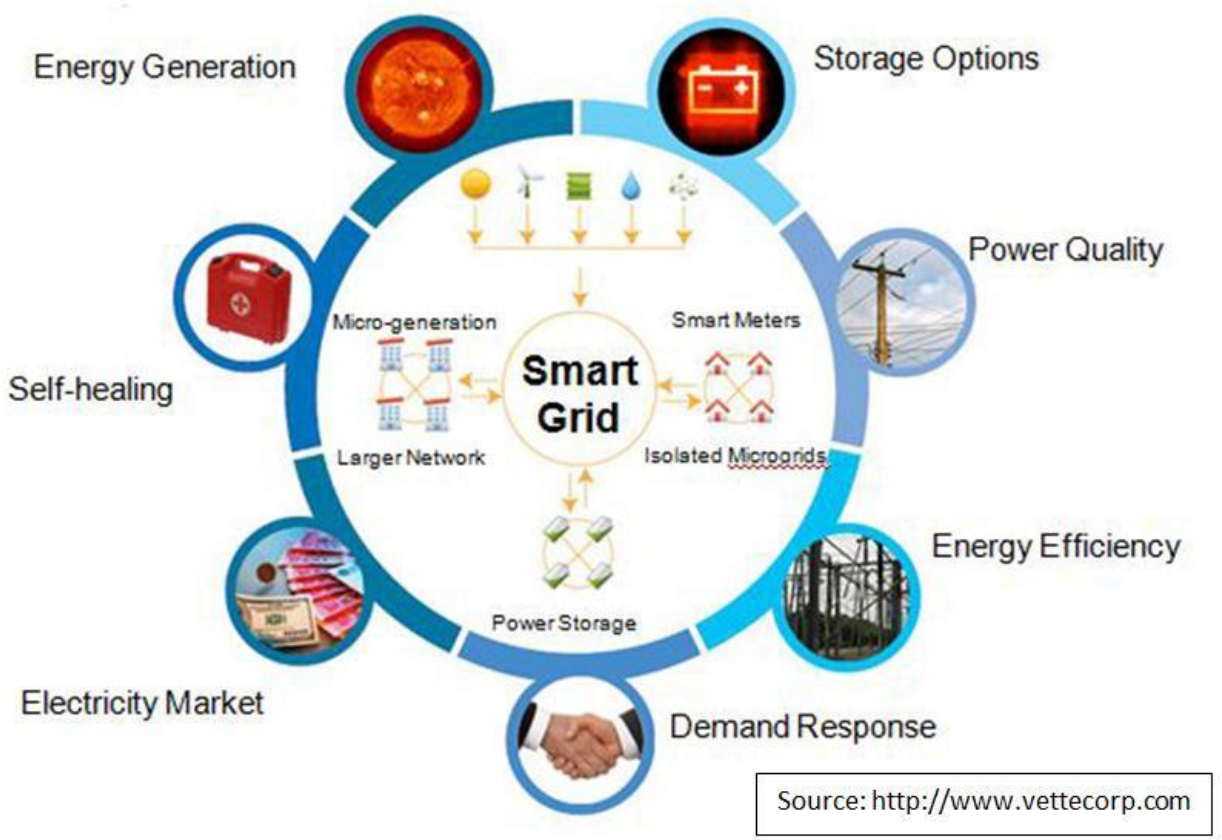


Ruzzelli, Antonio G., et al. "Real-time recognition and profiling of appliances through a single electricity sensor." *2010 7th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON)*. IEEE, 2010.

55 32 46 35 49 45 4a 70 62 6d 64 76 49 51 3d 3d

Outline

- Smart Grid
  - Advanced Metering Infrastructure (AMI)
  - Smart Meter
  - Characteristics
- Privacy and Security Issues
- Existing Solutions
- Privacy- and Data-Aware Scheme



55 32 46 35 49 45 4a 70 62 6d 64 76 49 51 3d 3d

Consumer's Wish List

- Reduce bill
- Better service
- Manage energy consumption
- Select utility company that best fits their energy needs
- Preserve privacy

55 32 46 35 49 45 4a 70 62 6d 64 76 49 51 3d 3d

Utility's Wish List

- Meet consumer needs
- Bill consumers correctly
- Employ load monitoring
- Process fine-grained data for further analysis
- Manage and control smart meters
- Minimize outages

55 32 46 35 49 45 4a 70 62 6d 64 76 49 51 3d 3d

AMI Challenges

- Fine-grained data: transfer, storage, and analysis
- Limited computational resources
- Consumer privacy preservation
- Scalability
- Multiple energy providers

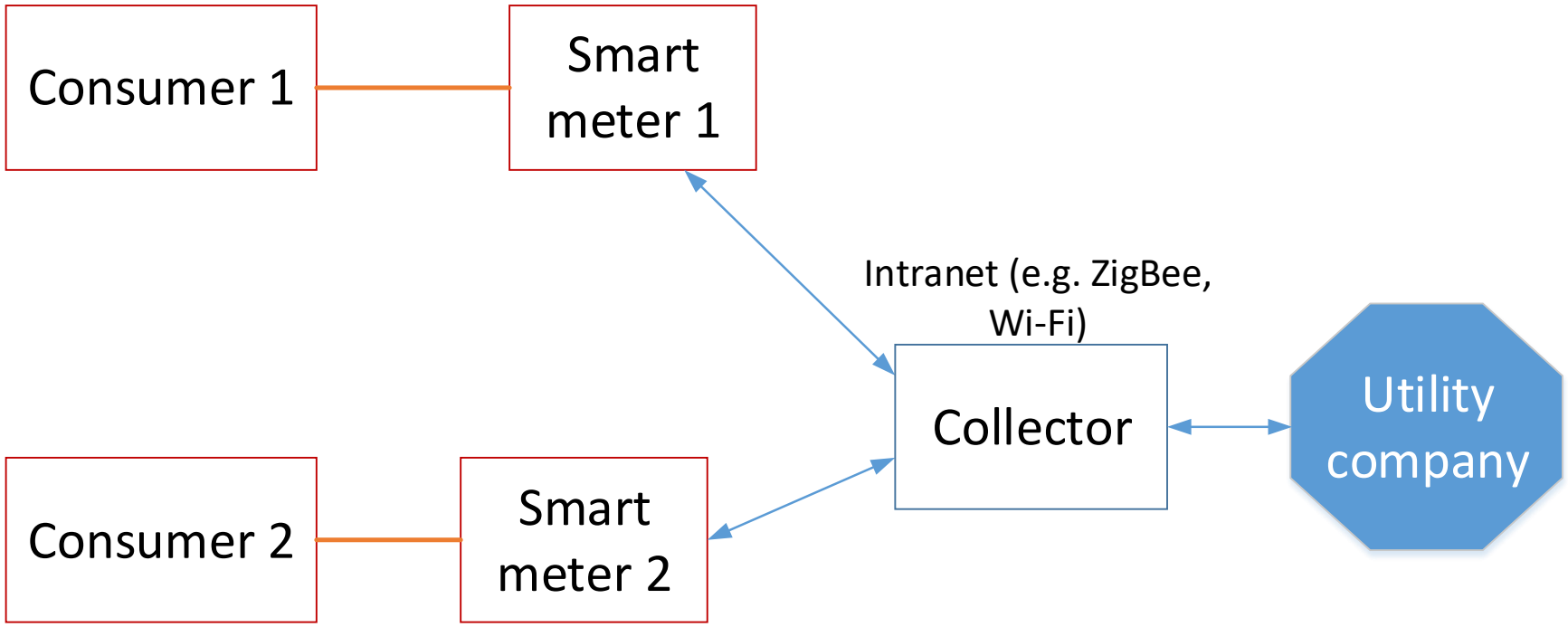
55 32 46 35 49 45 4a 70 62 6d 64 76 49 51 3d 3d

Existing Solutions

- Utility companies (UCs) utilize:
  - Collectors
  - Aggregators
  - Storage units
  - Trusted Third Party (TTP)

55 32 46 35 49 45 4a 70 62 6d 64 76 49 51 3d 3d

Standard Infrastructure



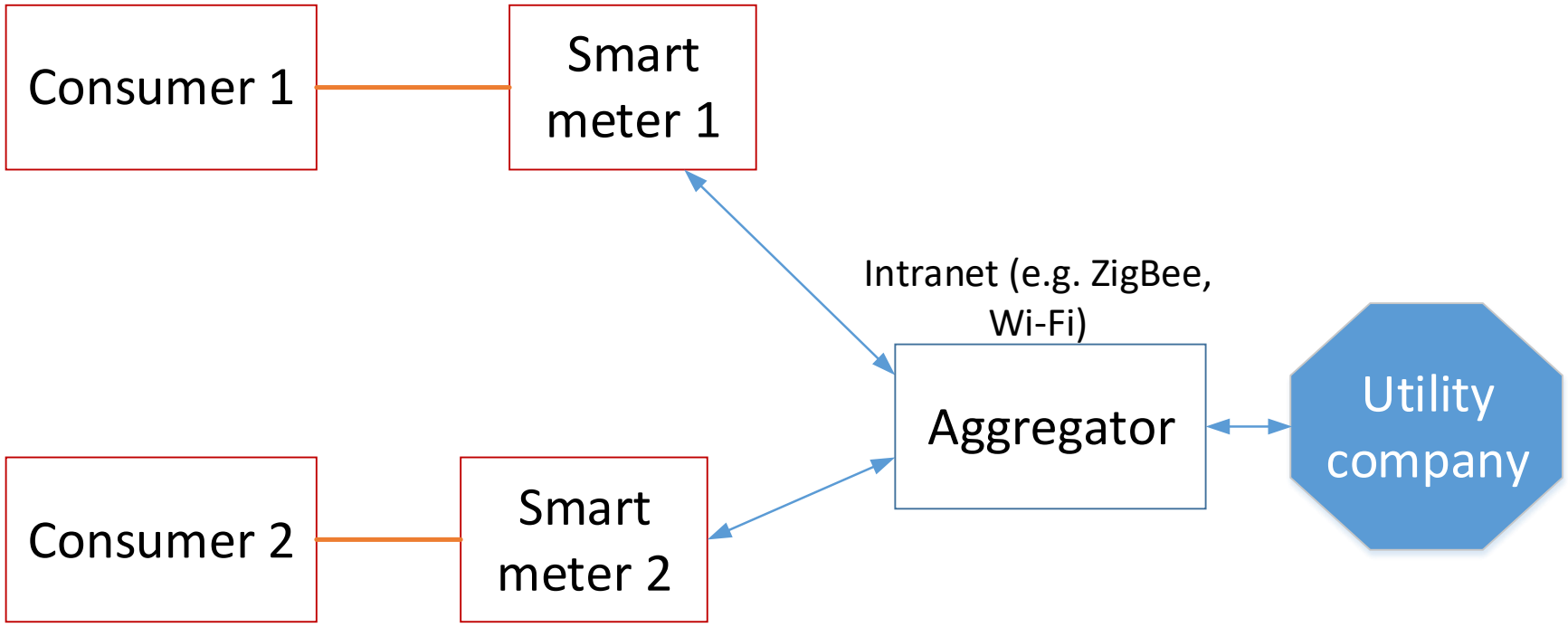
55 32 46 35 49 45 4a 70 62 6d 64 76 49 51 3d 3d

Disadvantages Associated with Standard Infrastructure

- Fine-grained data are directly stored at UC
- Privacy issues
- No scalability in case of several electricity providers (data will not be transferrable among providers)
- UC controls the data and can do whatever they want with them besides load monitoring, fraud detection, energy efficiency

55 32 46 35 49 45 4a 70 62 6d 64 76 49 51 3d 3d

Aggregation-based Infrastructure



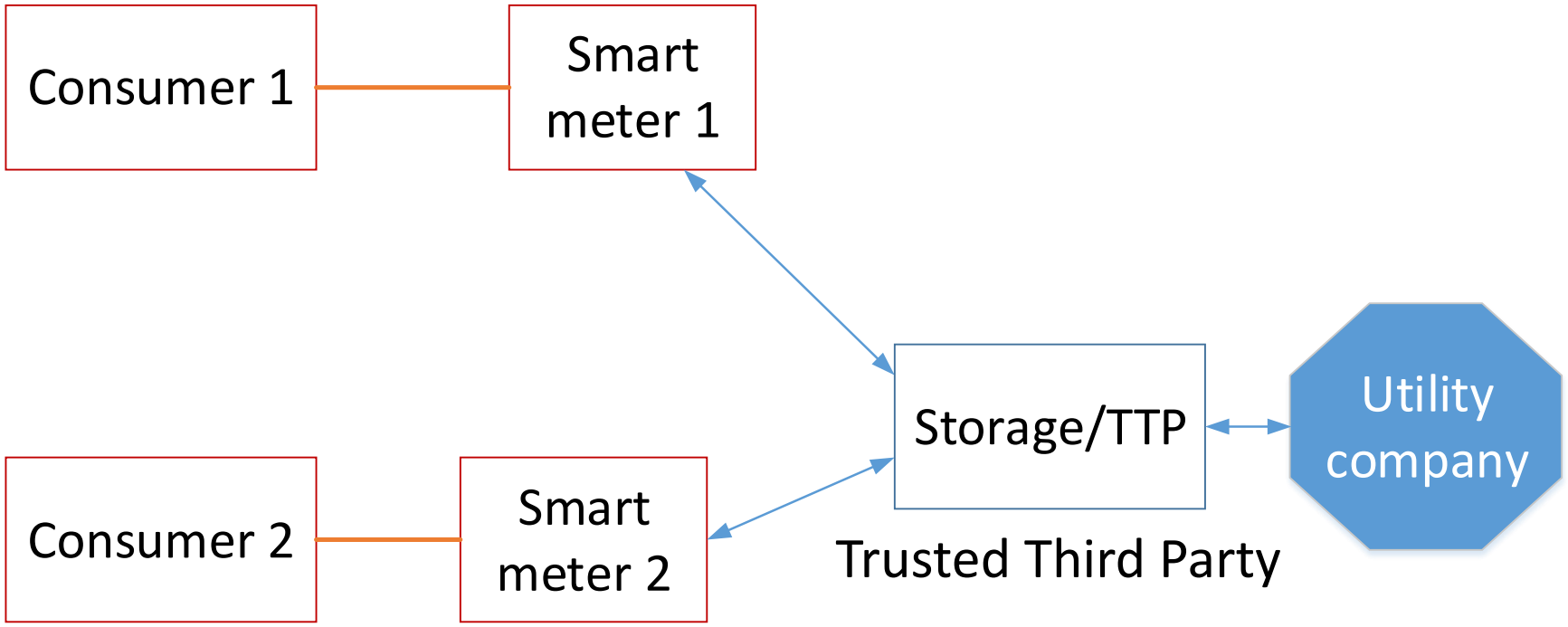
55 32 46 35 49 45 4a 70 62 6d 64 76 49 51 3d 3d

Disadvantages Associated with Aggregation-based Infrastructure

- No fine-grained data storage
- No fine-grained data applications
- No analysis of consumer energy consumption

55 32 46 35 49 45 4a 70 62 6d 64 76 49 51 3d 3d

Infrastructure with a Storage Unit



55 32 46 35 49 45 4a 70 62 6d 64 76 49 51 3d 3d

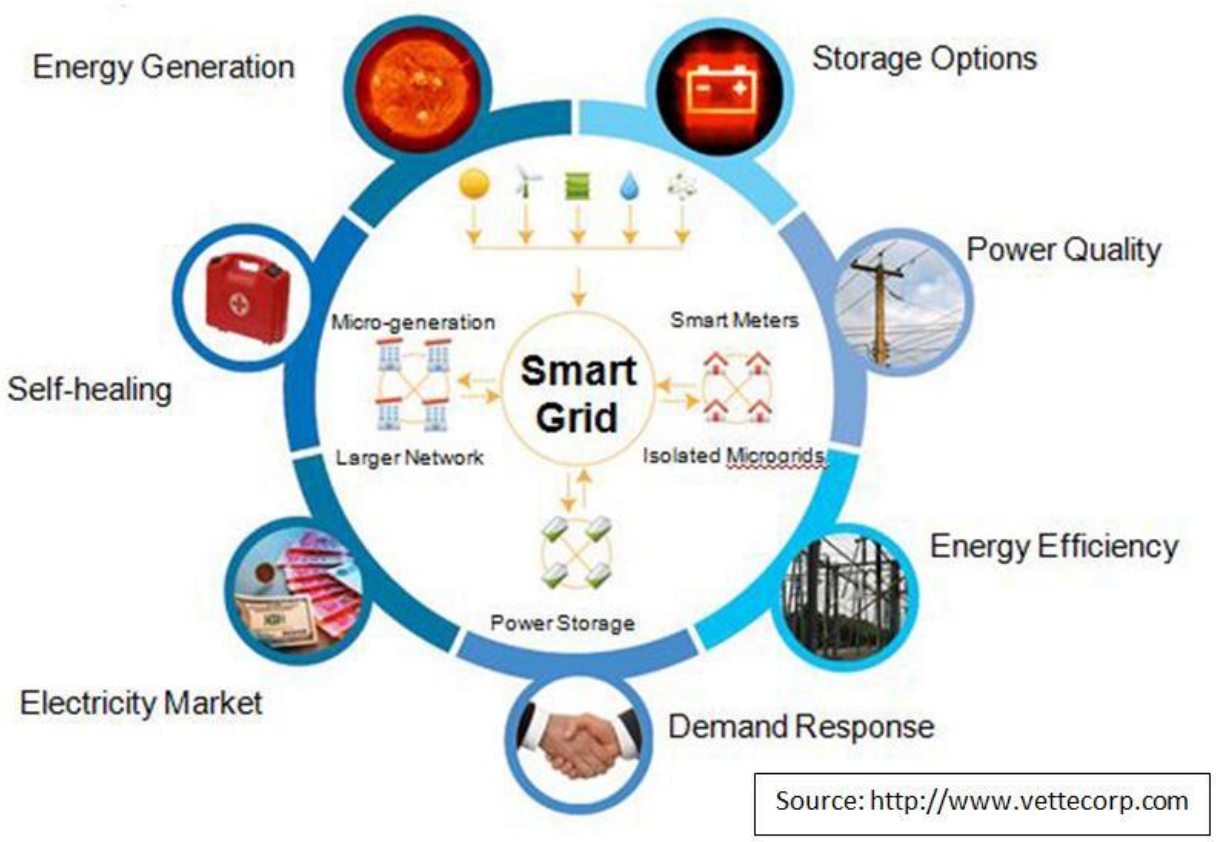
Disadvantages Associated with Infrastructure with a Storage Unit

- Two parties (Storage/TTP & UC) have direct access to Smart Meter (SM)s
- To support scalability, Storage/TTP has to use the same connection lines to SMs as UC, increasing network load
- Storage is deployed by UC
- Consumers cannot see their historical energy consumption
- Not scalable for multiple providers

55 32 46 35 49 45 4a 70 62 6d 64 76 49 51 3d 3d

Outline

- Smart Grid
  - Advanced Metering Infrastructure (AMI)
  - Smart Meter
  - Characteristics
- Privacy and Security Issues
- Existing Solutions
- Privacy- and Data-Aware Scheme



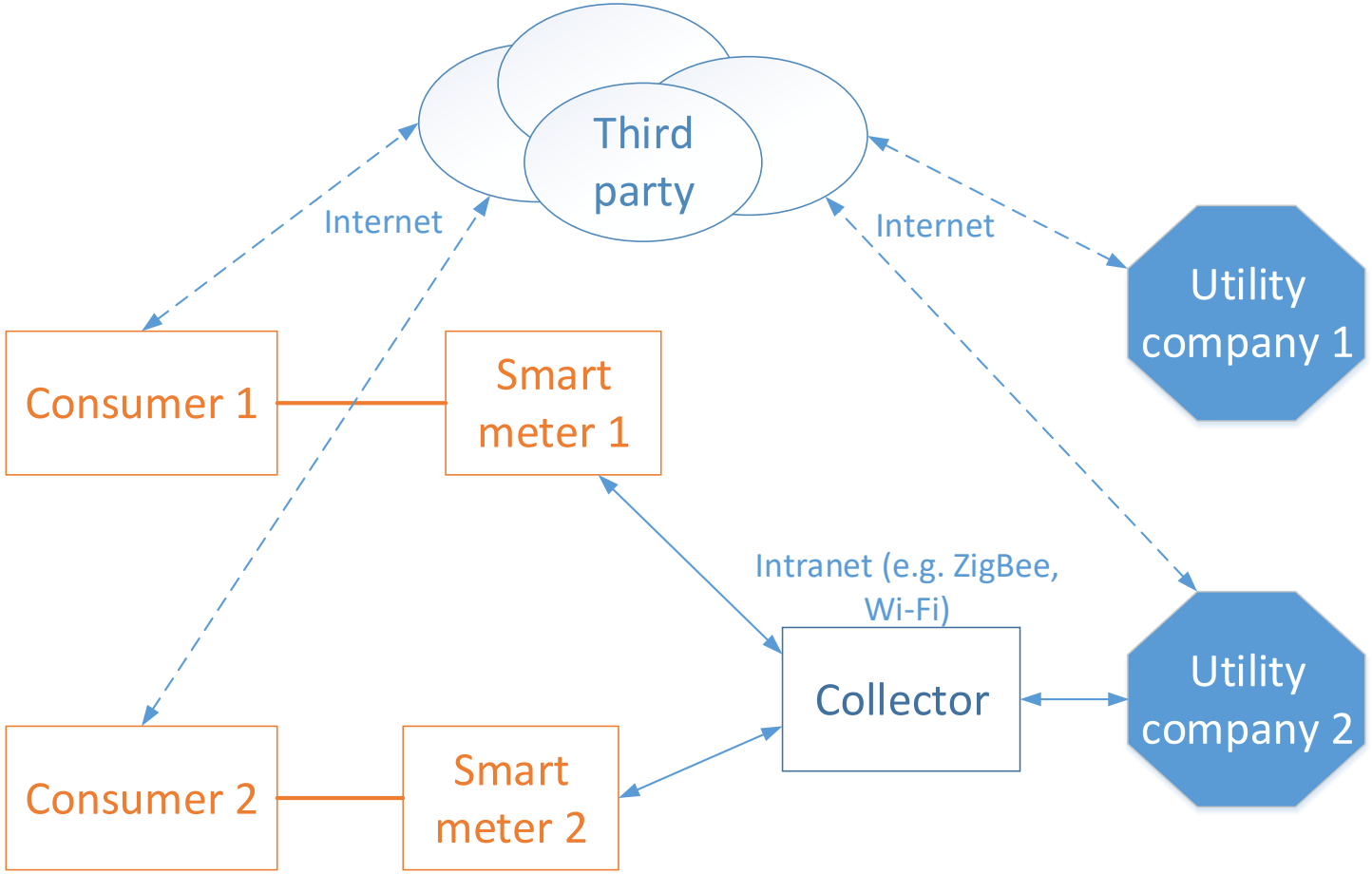
55 32 46 35 49 45 4a 70 62 6d 64 76 49 51 3d 3d

Proposed Solution

- Apart from use of lightweight cryptography and consumer privacy preservation, other unique features
  - Scalability, no significant changes to the current grid
  - Fine-grained data analysis
  - Network load reduction
  - Only UC has a direct access to smart meters
  - Different consumer-oriented applications
    - Comparison of energy providers' prices
    - Variable price rates for energy, reducing smart meter computational load
  - Aggregation is made out of AMI

55 32 46 35 49 45 4a 70 62 6d 64 76 49 51 3d 3d

Proposed Infrastructure



55 32 46 35 49 45 4a 70 62 6d 64 76 49 51 3d 3d

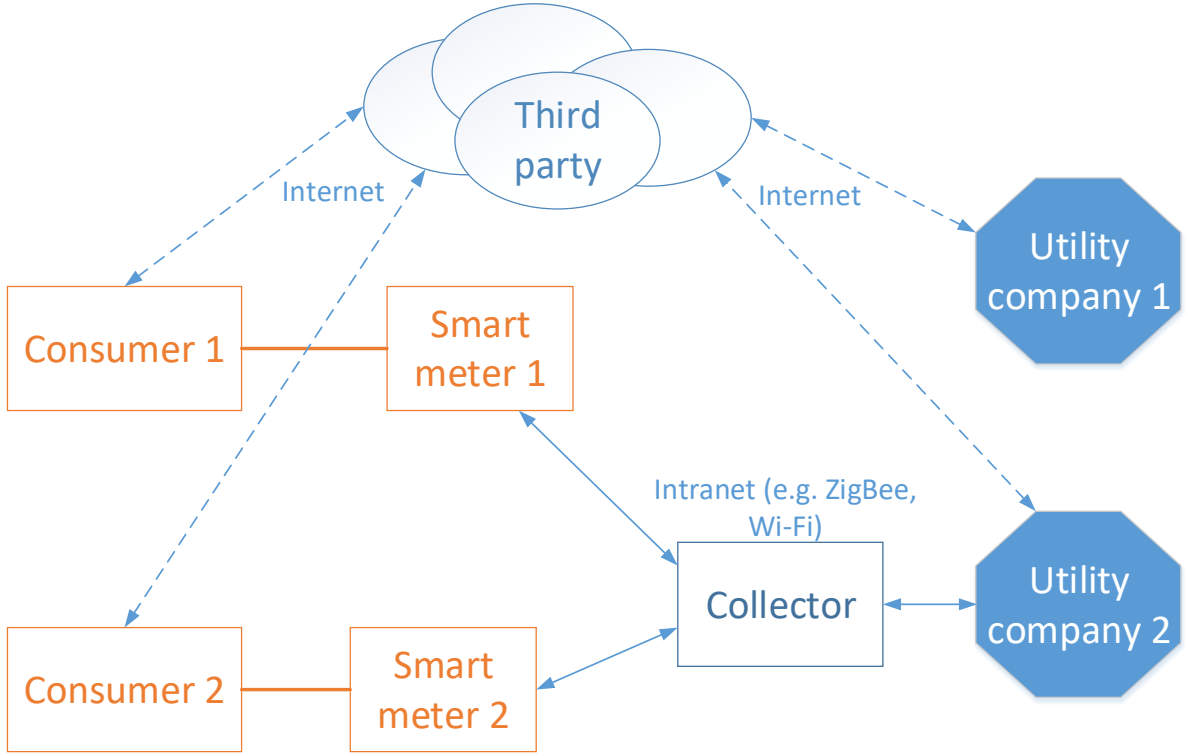
Role of Trusted Third Party

- Independent commercial cloud-based organization
- Responsibility
  - Store and analyze fine-grained data
  - Calculate the bill
  - Provide detailed analysis to consumers
  - Provide privacy-preserving analysis for utilities

55 32 46 35 49 45 4a 70 62 6d 64 76 49 51 3d 3d

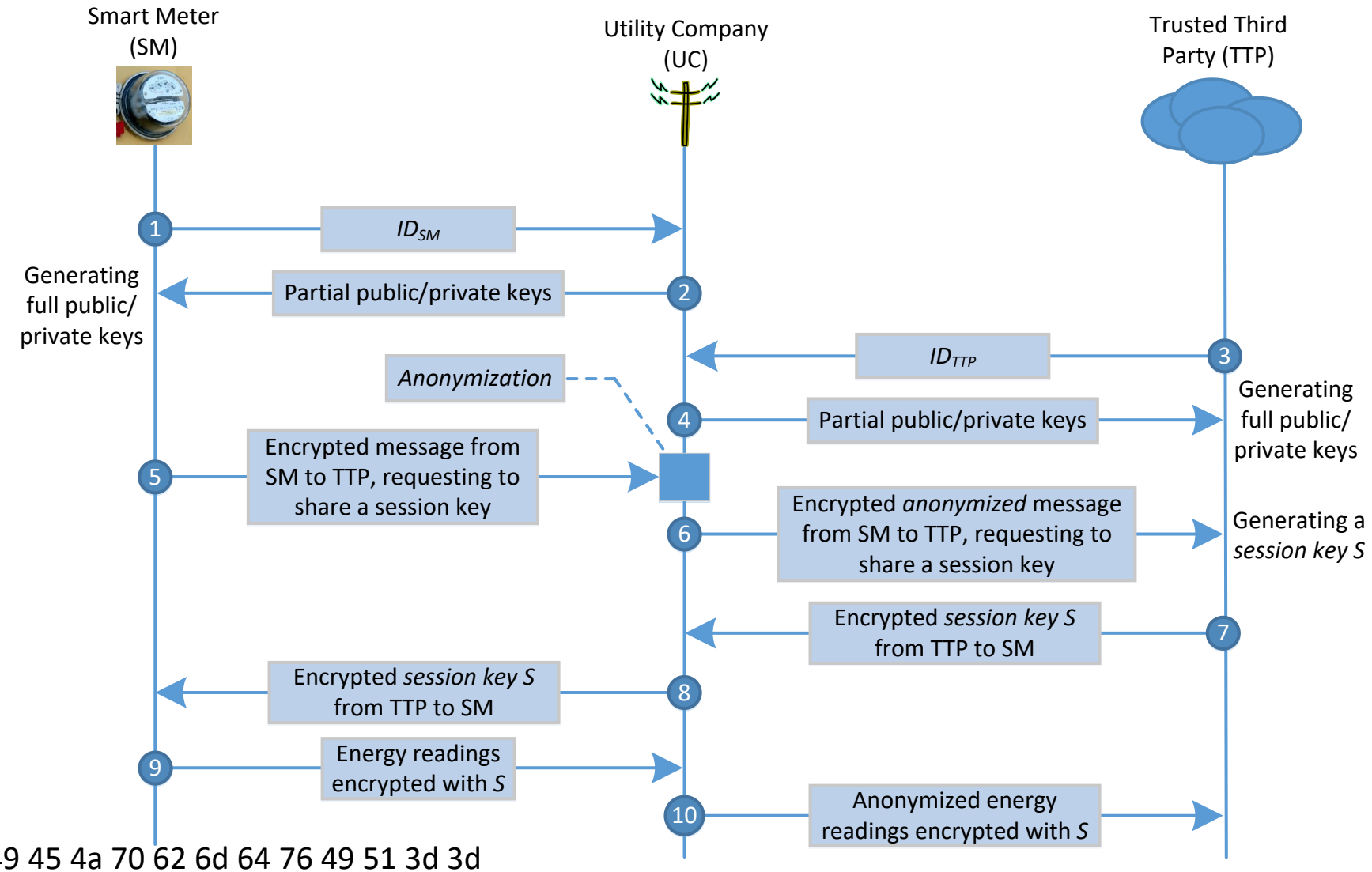
UC-TTP and Consumer-TTP Interaction

- Utility company
  - Billing
  - Load monitoring
  - Support of different price ranges
  - Fraud detection
- Consumers
  - Consumption analysis
  - Comparison of UC’s



55 32 46 35 49 45 4a 70 62 6d 64 76 49 51 3d 3d

Proposed Protocol



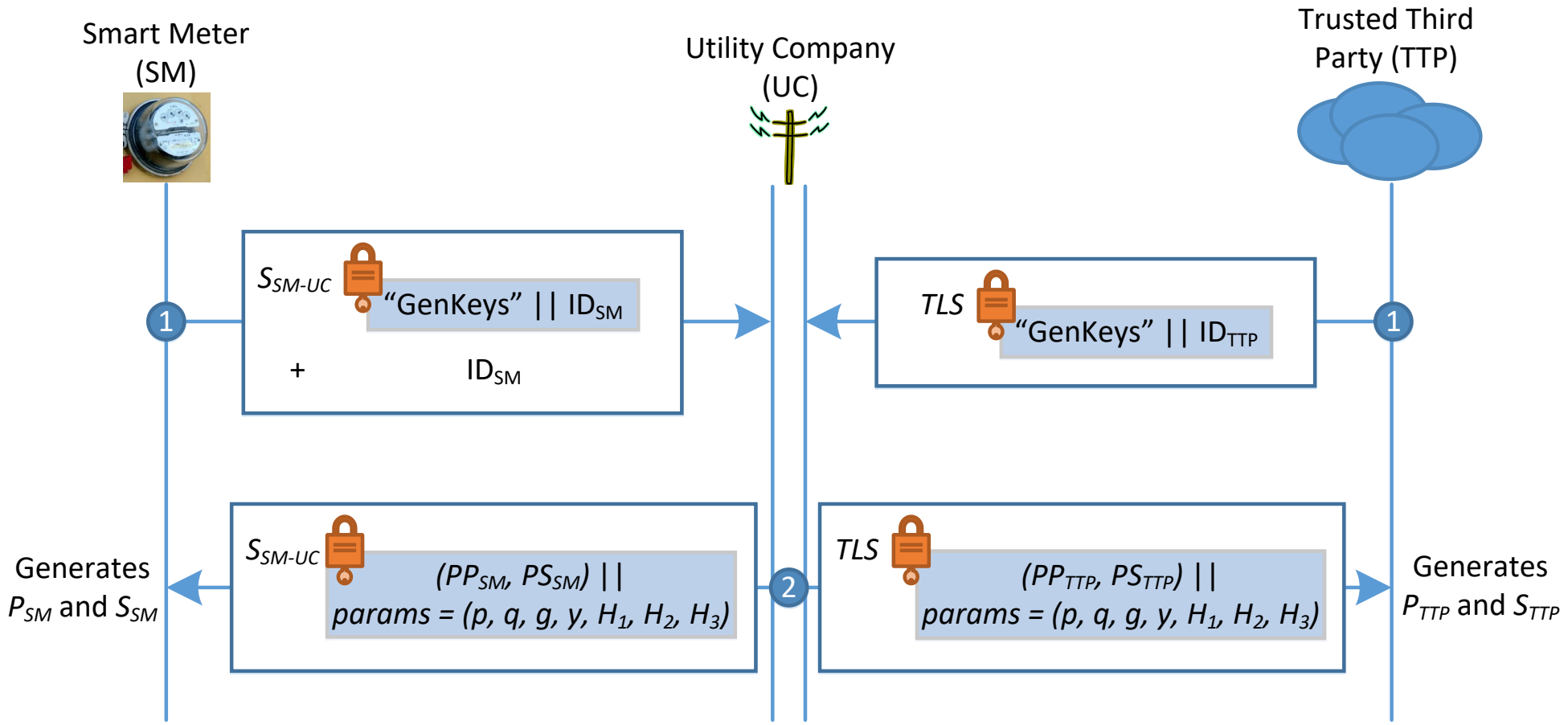
55 32 46 35 49 45 4a 70 62 6d 64 76 49 51 3d 3d

Communication Phases

- Registration phase
  - Utility Company (UC) serves as a key generation center
  - Smart meters and the Trusted Third Party (TTP) communicate to the utility company to obtain partial public/private keys
- Session key exchange phase
  - Smart meters and TTP exchange a session key
- Data transmission phase
  - Smart meters send encrypted energy readings to TTP via UC

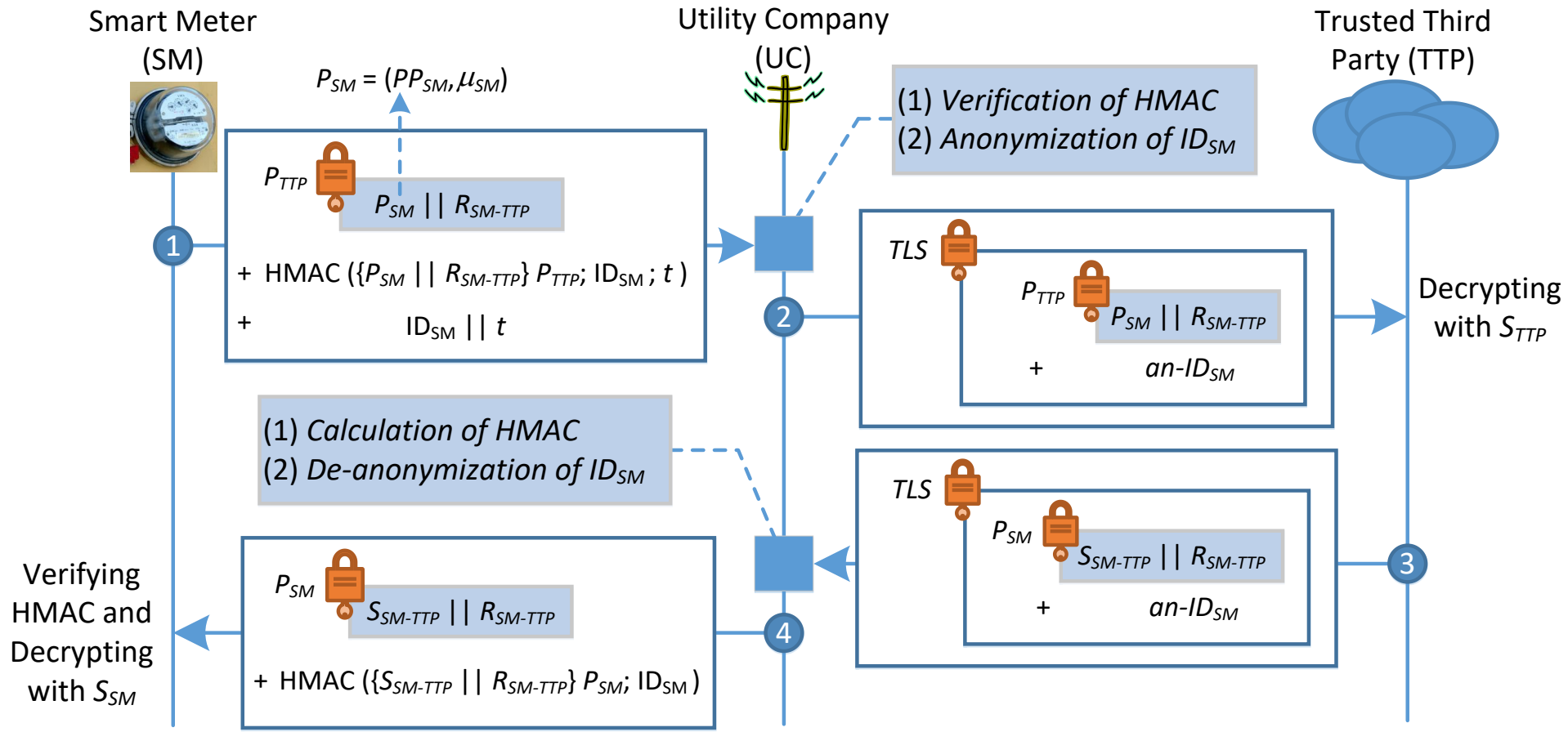
55 32 46 35 49 45 4a 70 62 6d 64 76 49 51 3d 3d

Registration Phase



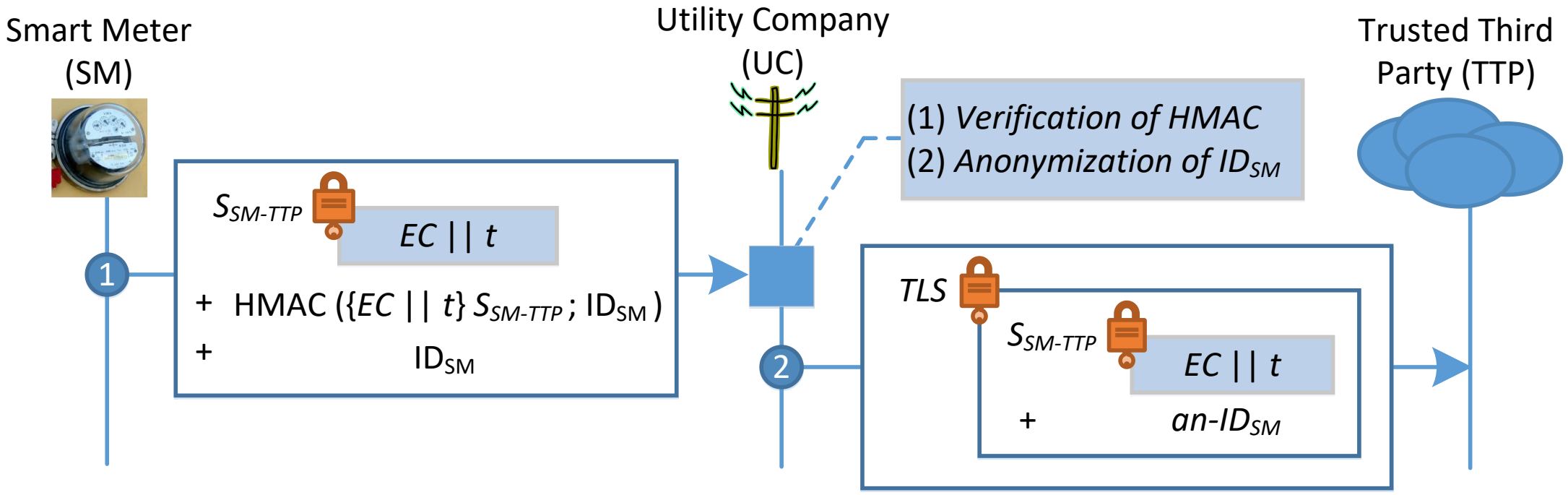
55 32 46 35 49 45 4a 70 62 6d 64 76 49 51 3d 3d

Session Key Exchange Phase



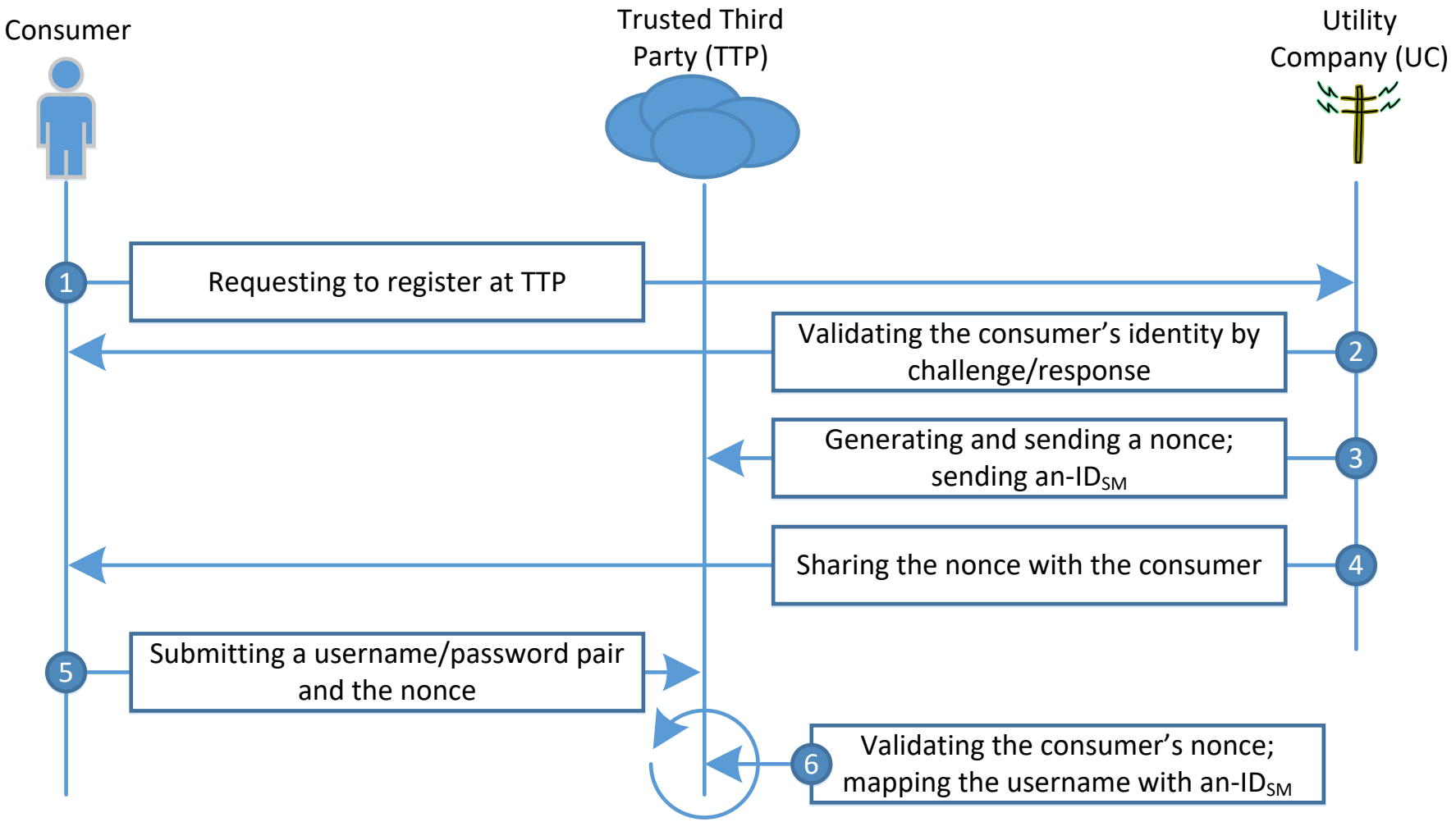
55 32 46 35 49 45 4a 70 62 6d 64 76 49 51 3d 3d

Data Transmission Phase



55 32 46 35 49 45 4a 70 62 6d 64 76 49 51 3d 3d

Consumer Authentication



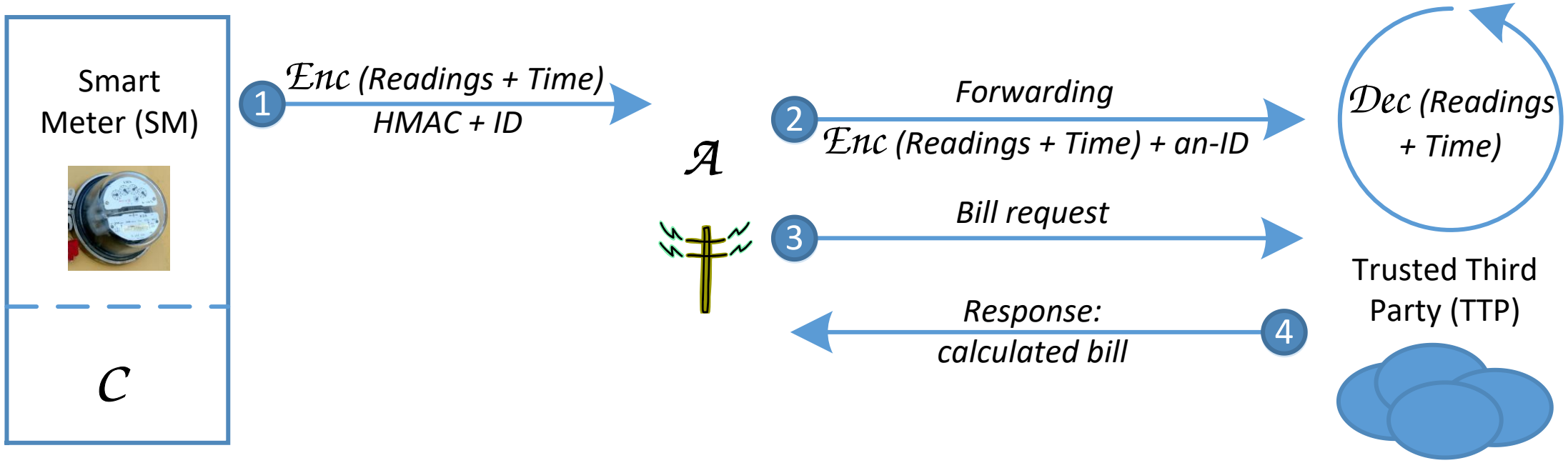
55 32 46 35 49 45 4a 70 62 6d 64 76 49 51 3d 3d

Attack Vectors

- Utility company as an *honest-but-curious* adversary
- Wait-for-response attack by a utility company
- Trusted third party as an *honest-but-curious* adversary
- Man-in-the-middle attacks

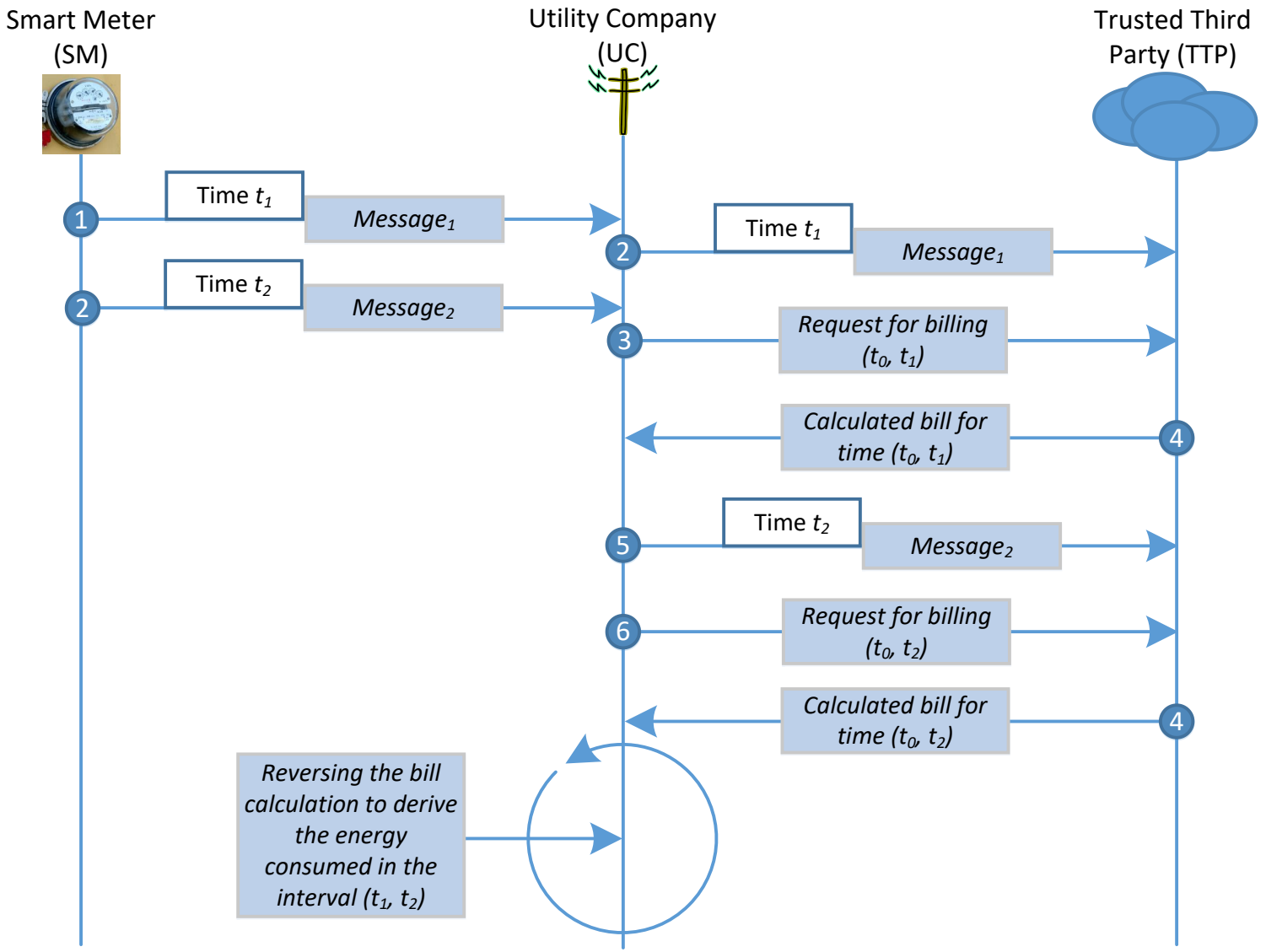
55 32 46 35 49 45 4a 70 62 6d 64 76 49 51 3d 3d

Attacker: Utility Company



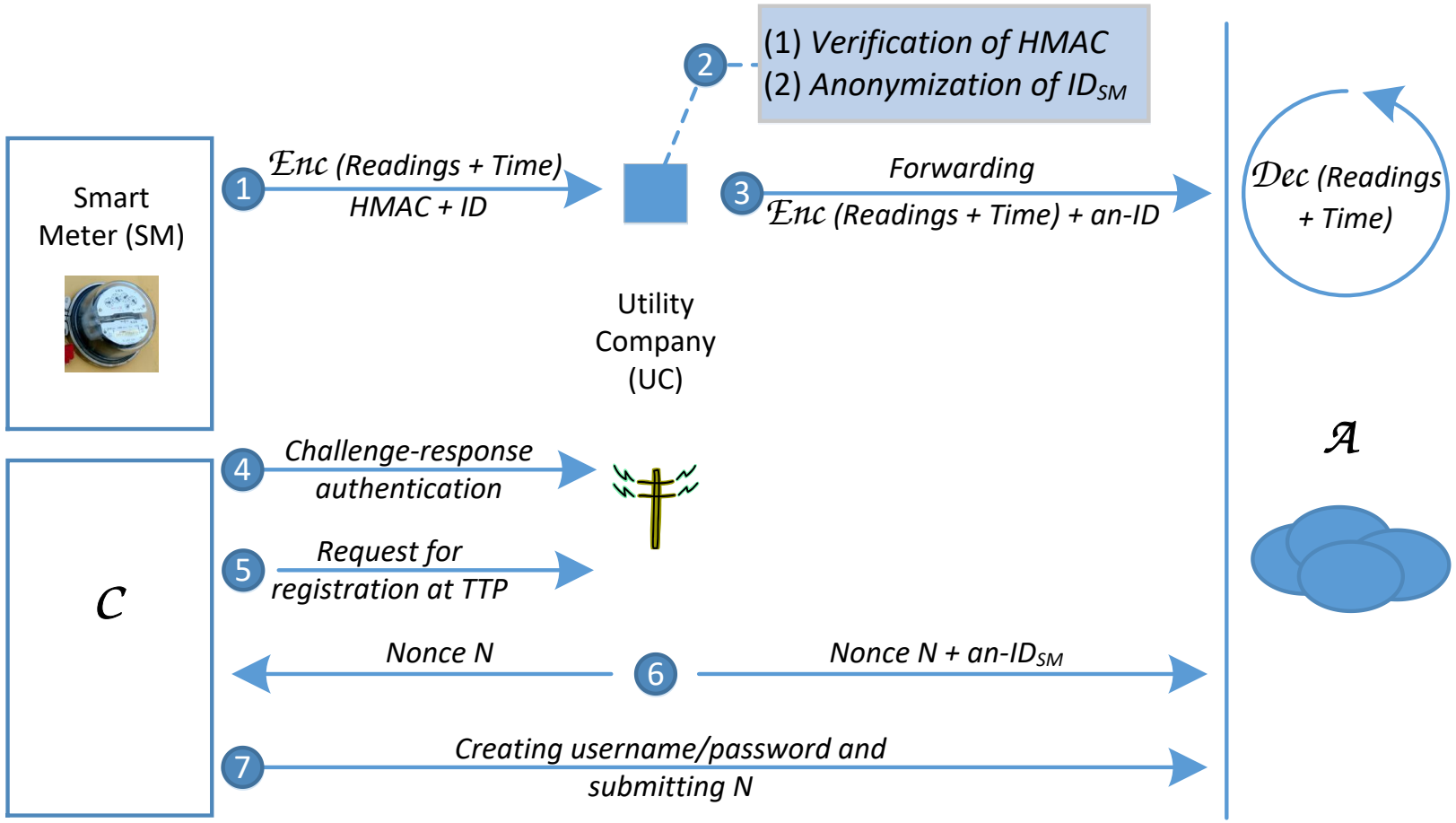
55 32 46 35 49 45 4a 70 62 6d 64 76 49 51 3d 3d

Wait-for-Response Attack



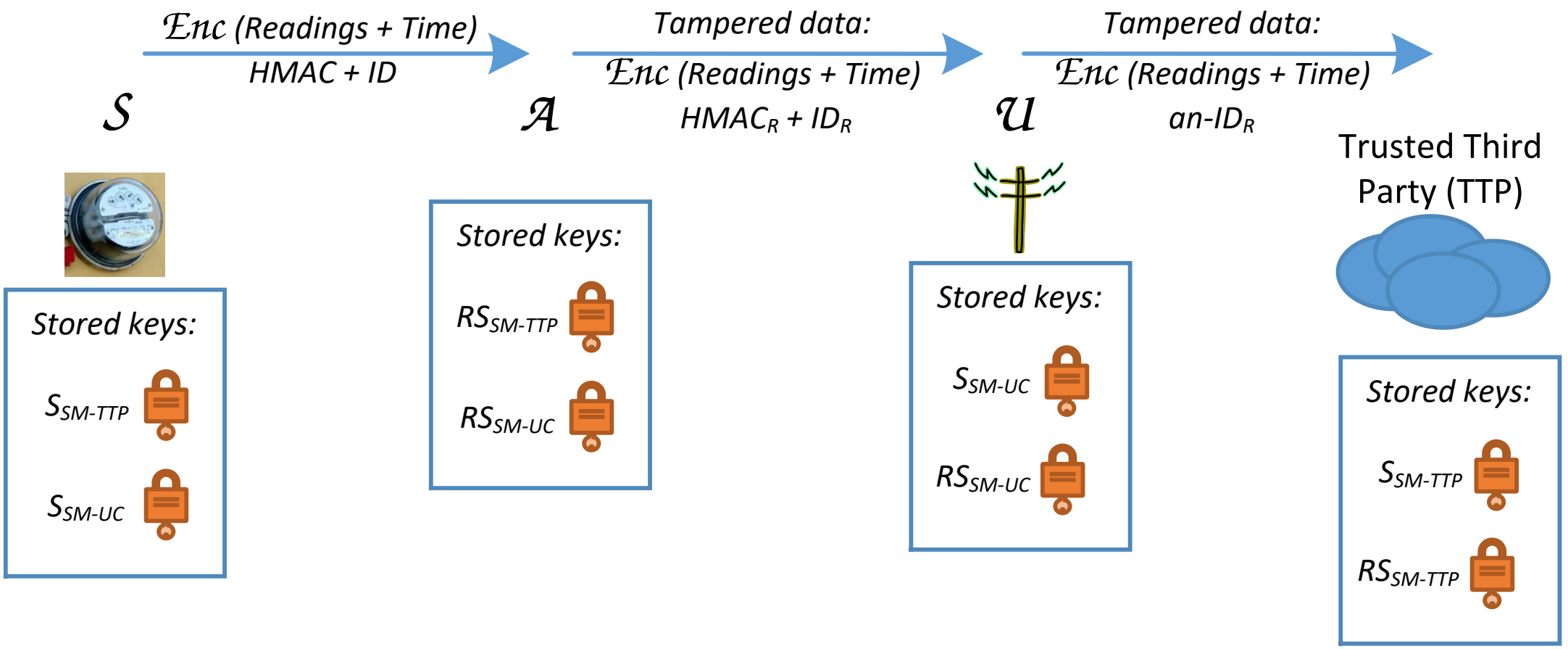
55 32 46 35 49 45 4a 70 62 6d 64 76 49 51 3d 3d

Attacker: Trusted Third Party



55 32 46 35 49 45 4a 70 62 6d 64 76 49 51 3d 3d

Attacker: MITM



55 32 46 35 49 45 4a 70 62 6d 64 76 49 51 3d 3d

Conclusion and Future Research

- Cyber-Physical Systems research: security, privacy, data mining
- Unified AMI Simulation Framework
- Vehicular Network Integration
- Relax the assumption that the utility company and TTP do not collude

55 32 46 35 49 45 4a 70 62 6d 64 76 49 51 3d 3d

Education: CTF Unplugged

- Mission 000: Background
- Mission 001: Reconnaissance
- Mission 010: Forensics
- Mission 011: Cryptography
- Mission 100: Reverse Engineering
- Mission 101: Steganography
- Mission 110: Web

V. Ford, A. Siraj, A. Haynes, and E. L. Brown, “Capture the Flag Unplugged: An Offline Cyber Competition”, accepted at ACM SIGCSE 2017.

55 32 46 35 49 45 4a 70 62 6d 64 76 49 51 3d 3d

CyberEagles

- Cybersecurity Club at Tennessee Tech
- Seminars, speakers, competitions, conferences
- http://blogs.cae.tntech.edu/cybereagles/
- https://forum.cybereagles.club/

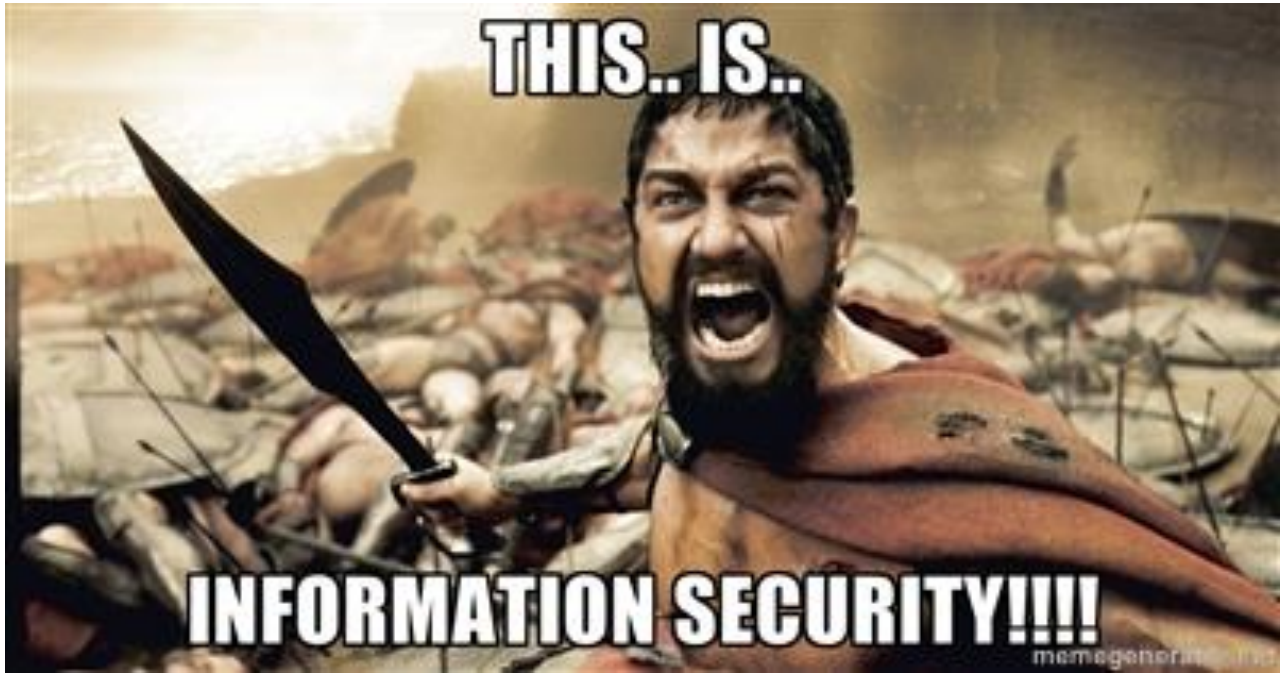
55 32 46 35 49 45 4a 70 62 6d 64 76 49 51 3d 3d

References

1. V. Ford, A. Siraj, and M. A. Rahman, “Secure and Efficient Protection of Consumer Privacy in Advanced Metering Infrastructure Supporting Fine-grained Data Analysis,” *Journal of Computer and System Sciences* 83.1 (2017): 84-100.
2. V. Ford, A. Siraj, and W. Eberle, “Smart Grid Energy Fraud Detection Using Artificial Neural Networks,” in *Proceedings of the 2014 IEEE Symposium Series on Computational Intelligence*, December 9-12, 2014.
3. V. Ford and A. Siraj, “Clustering of smart meter data for disaggregation,” in *Proceedings of IEEE Global Conference on Signal and Information Processing*, December 3-5, 2013.
4. V. Ford, A. Siraj, A. Haynes, and E. L. Brown, “Capture the Flag Unplugged: An Offline Cyber Competition”, accepted at ACM SIGCSE 2017.

55 32 46 35 49 45 4a 70 62 6d 64 76 49 51 3d 3d

Thank you!



http://i1-news.softpedia-static.com/images/news2/IT-Security-Memes-6.jpg?1373973589

http://vford.me

vford@tntech.edu

55 32 46 35 49 45 4a 70 62 6d 64 76 49 51 3d 3d