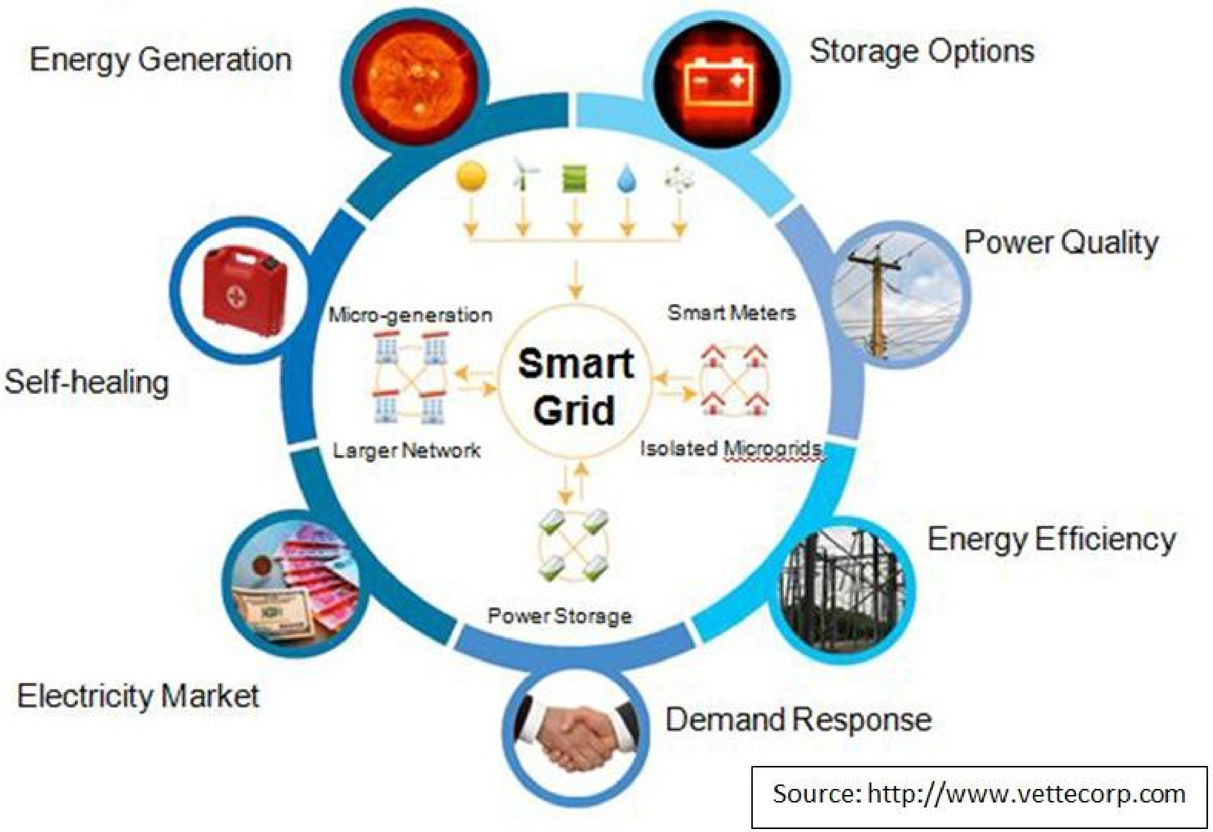
Consumer Privacy vs Data Mining: Issues with Smart Meter Data

Vitaly Ford
Assistant Professor
Computer Science and Math Department
Arcadia University, Glenside, PA

ARCADIA
UNIVERSITY
FOUNDED 1853

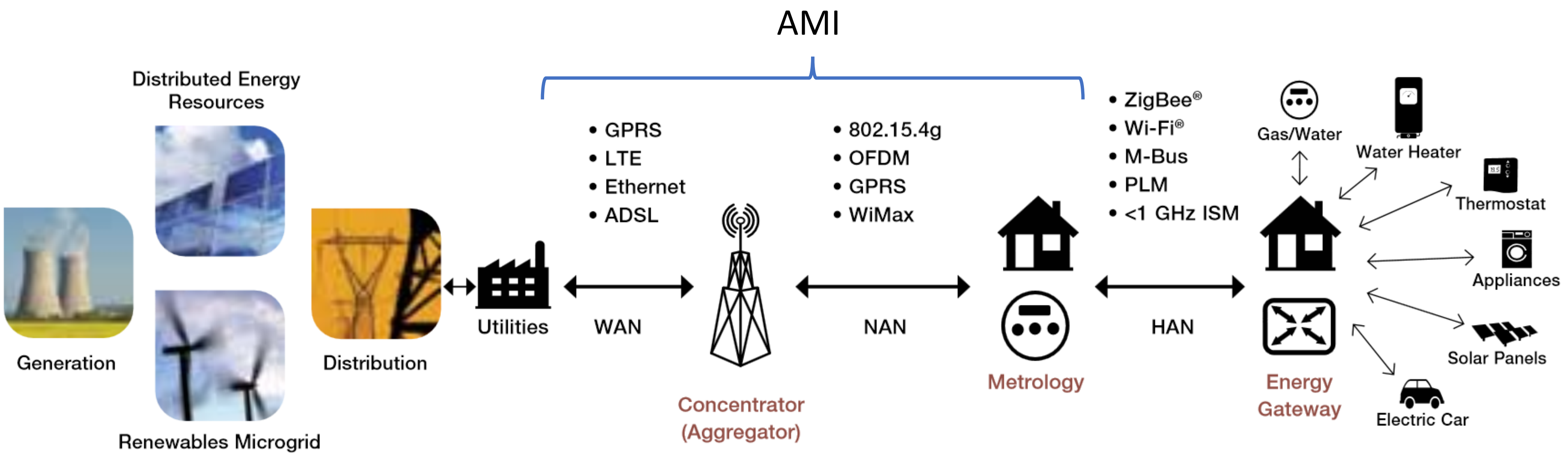
Outline

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



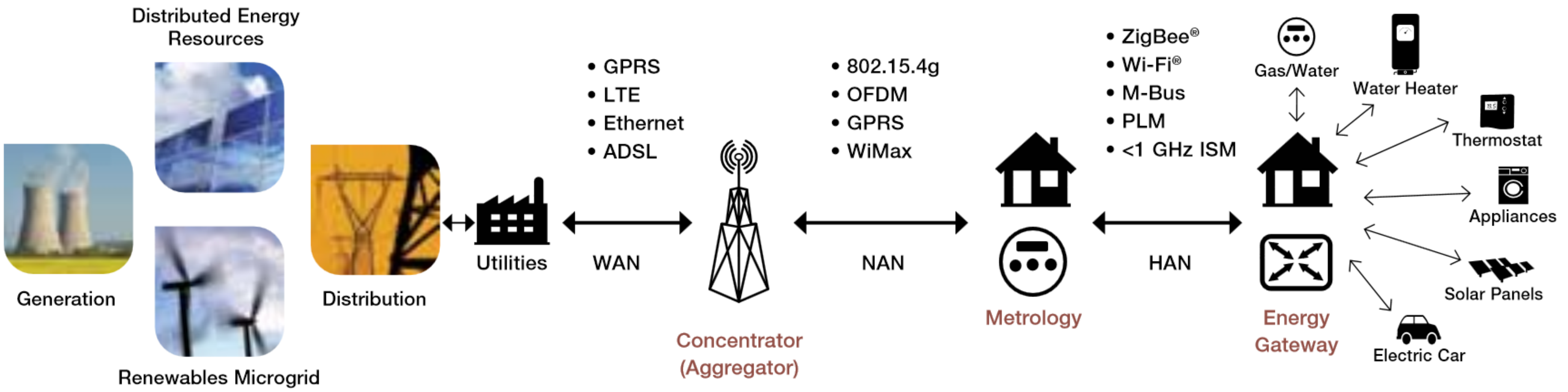
Source: http://www.vettecorp.com

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

https://cache.freescale.com/files/32bit/doc/brochure/PWRARBYNDBITSSES.pdf



Home Area Network (HAN)

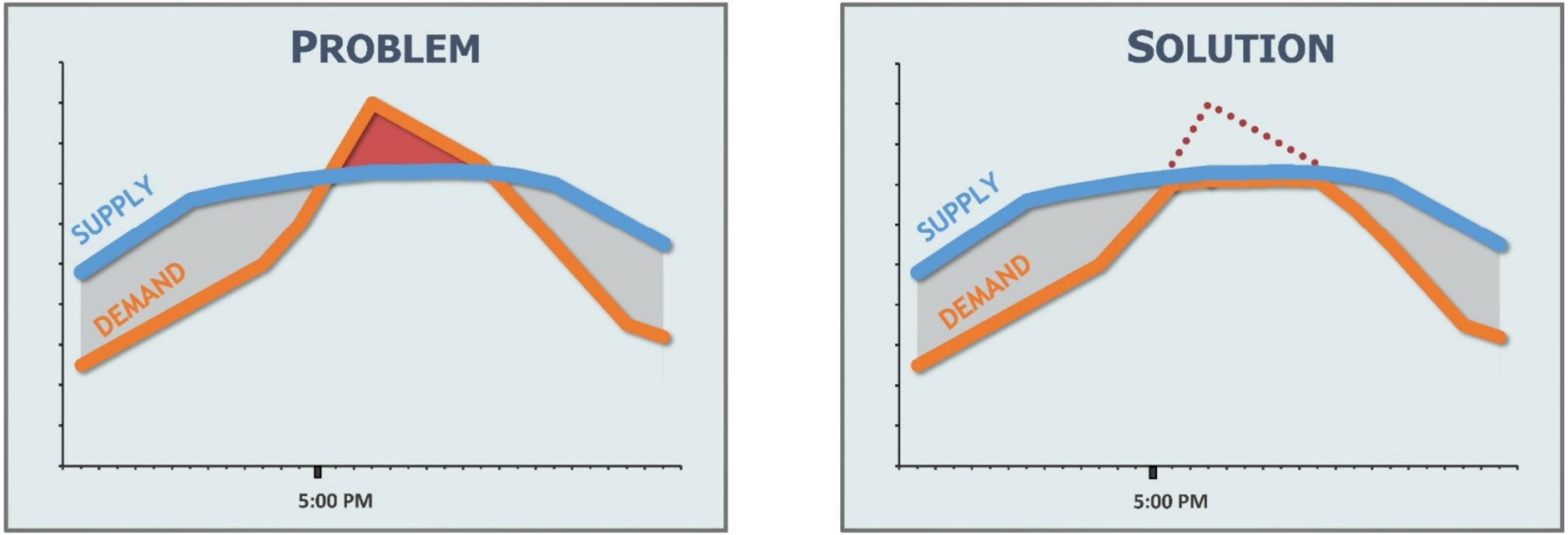
https://cache.freescale.com/files/32bit/doc/brochure/PWRARBYNDBITSSES.pdf

Smart Meter

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

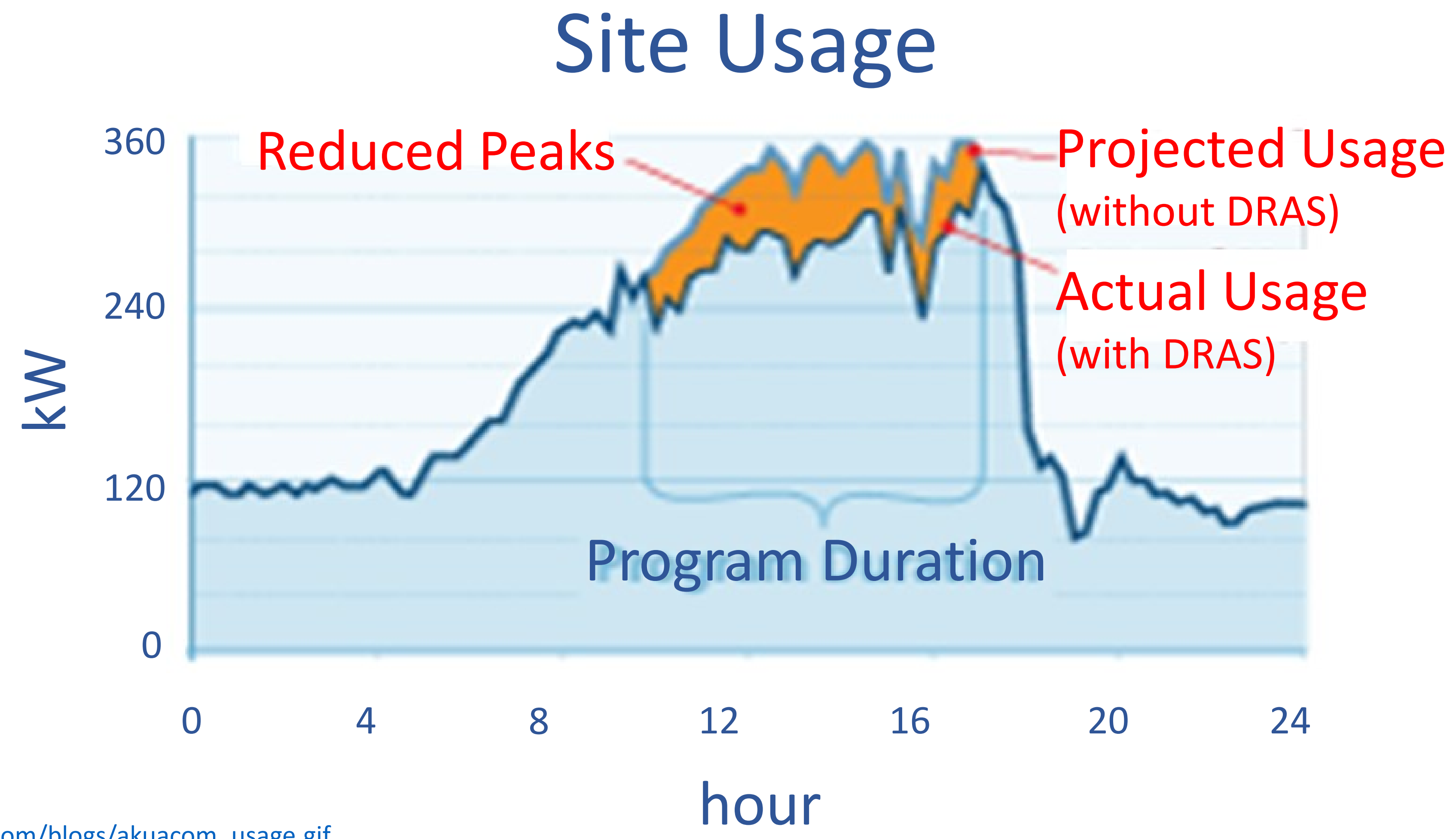
http://cdn.patchcdn.com/users/71520/2012/02/T800x600/d41acd900d6910fc2f7871441e13923.jpg

Supply-Demand Problem



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

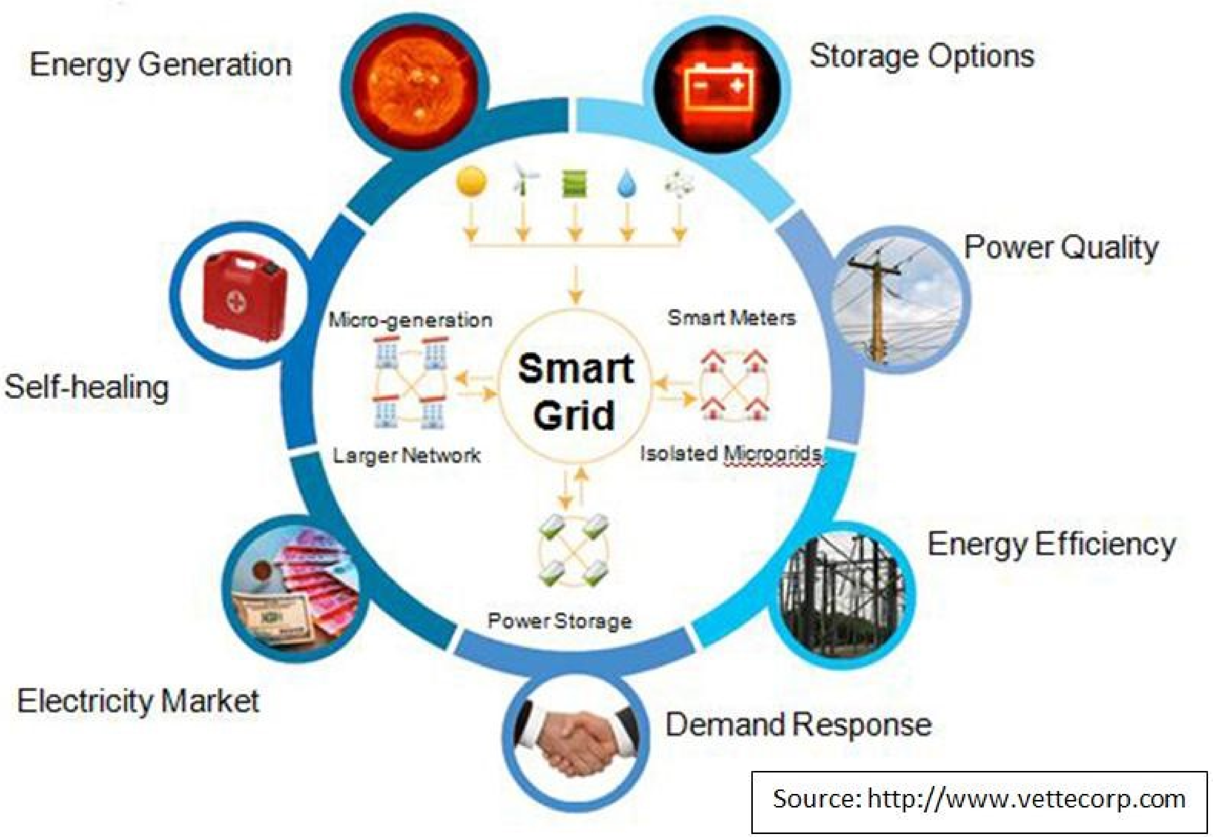
Demand-Response



http://i.bnet.com/blogs/akuacom_usage.gif

Outline

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



Source: http://www.vettecorp.com

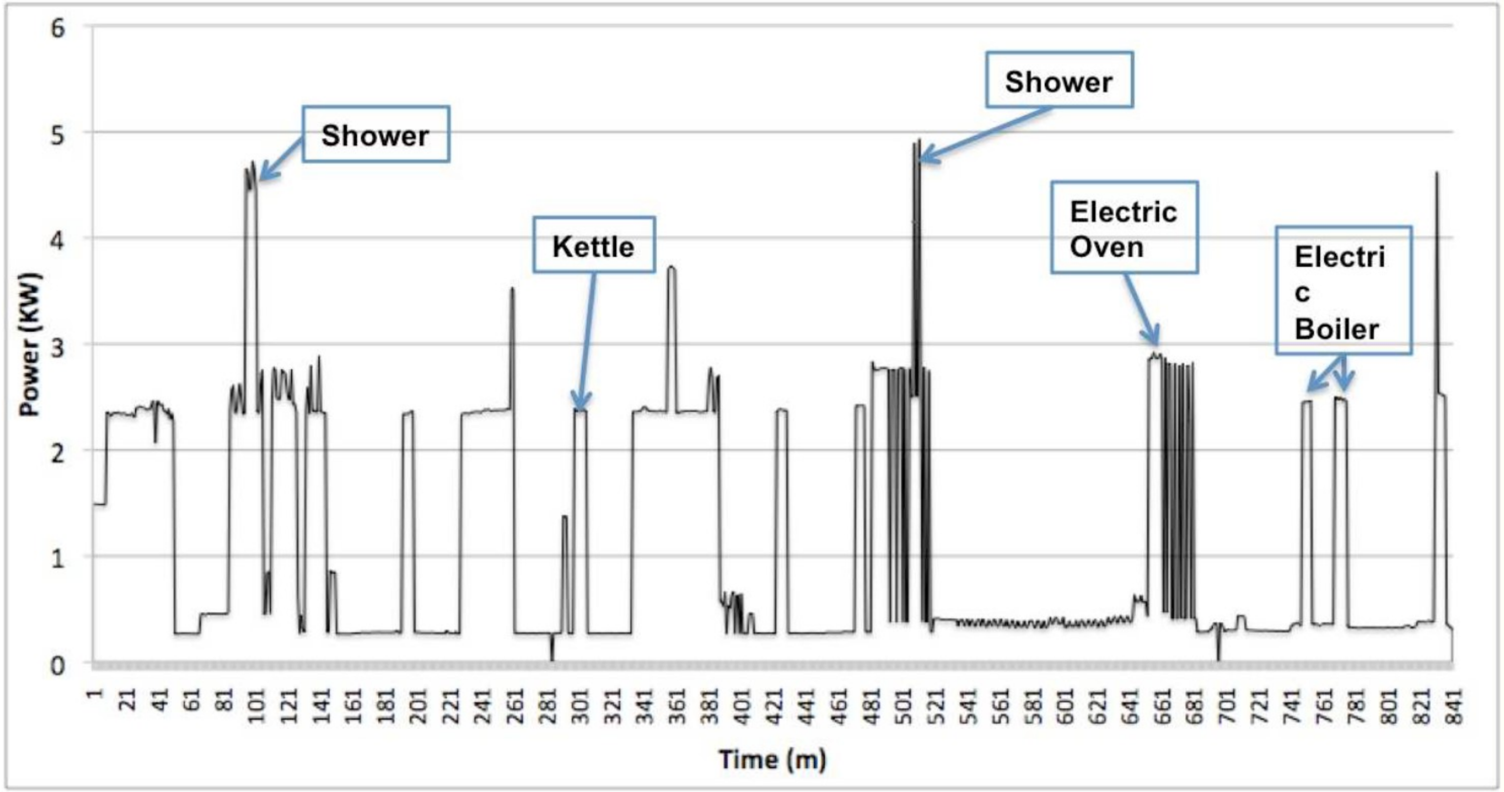
Security Issues

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

Consumer Privacy Violation

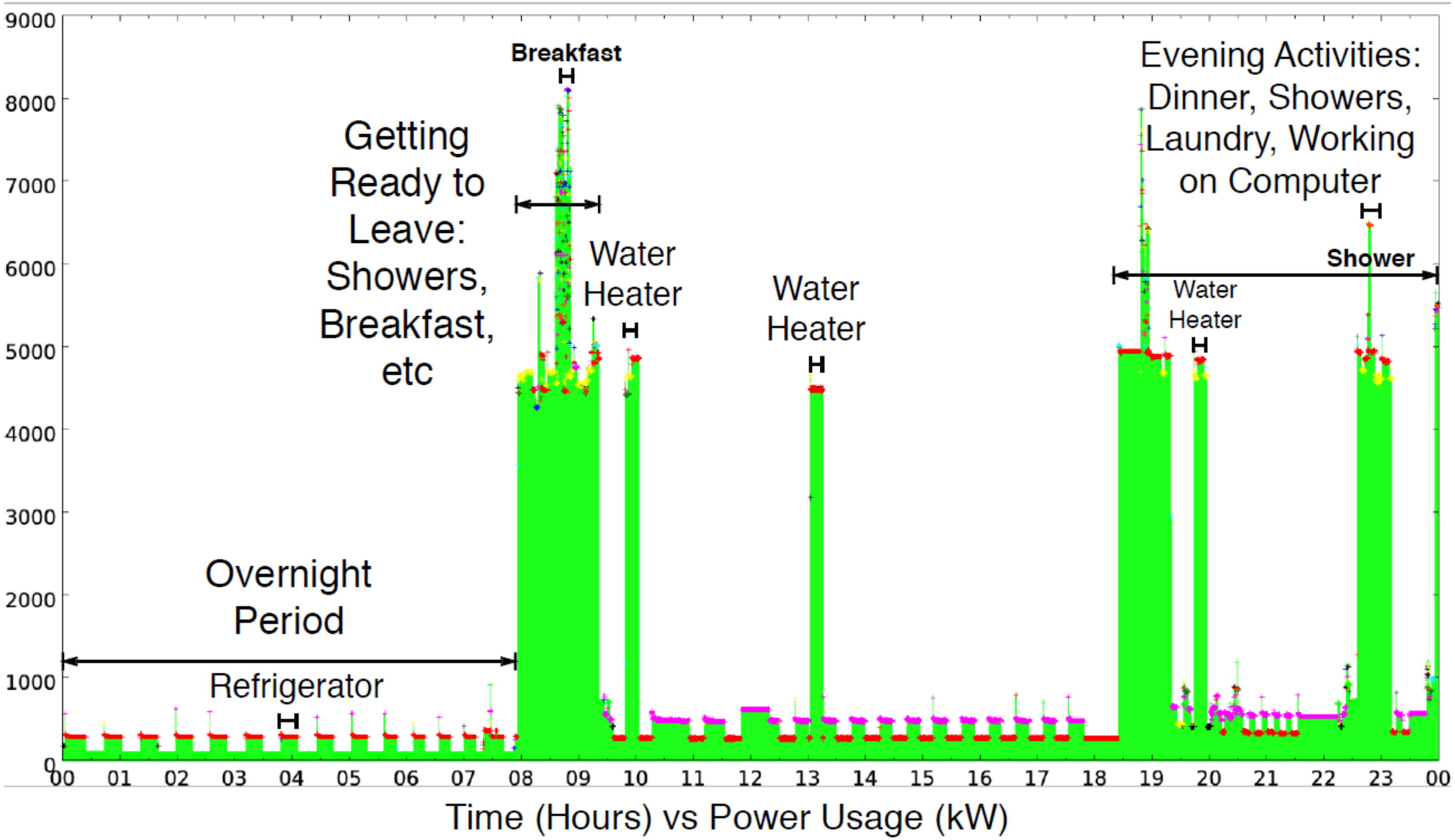
- Burglary preparation
- Targeted advertising
- Stalkers may exploit the data to discover victim’s home occupancy
- Risk assessment for insurance companies
- Parents “spying” on their children
- Landlords may determine if tenants violate the renting agreement
- Law enforcement agencies to discover illegal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

Profiling Consumer Energy Consumption



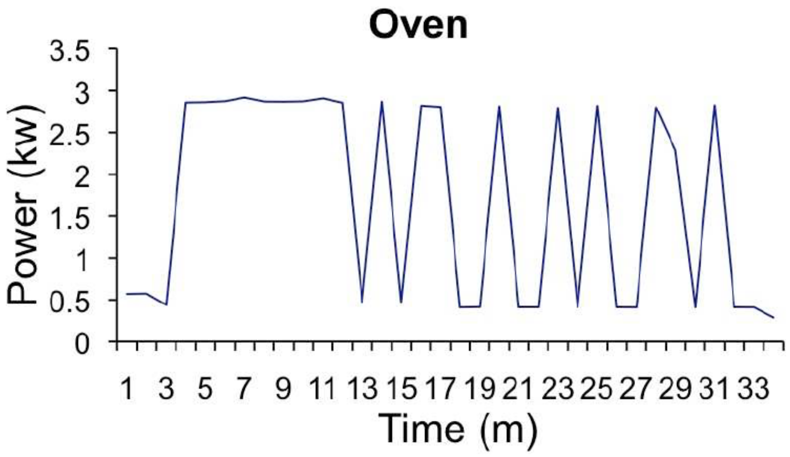
Ruzzelli, Antonio G., et al. "Real-time recognition and profiling of appliances through a single electricity sensor." *2010 7th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON)*. IEEE, 2010.

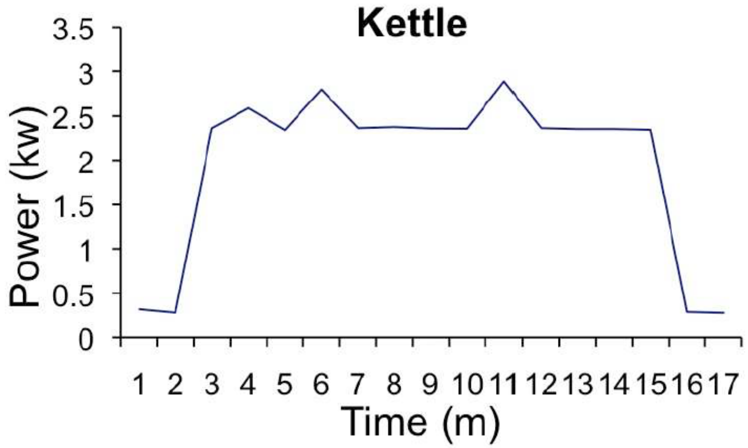
Granular Energy Consumption Data

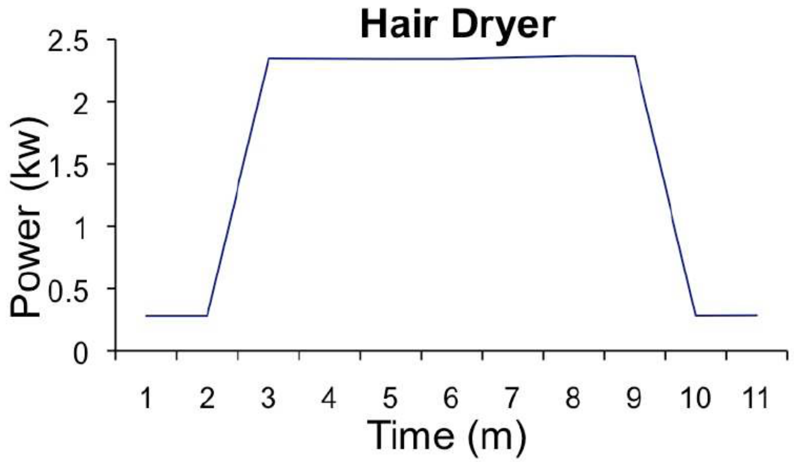


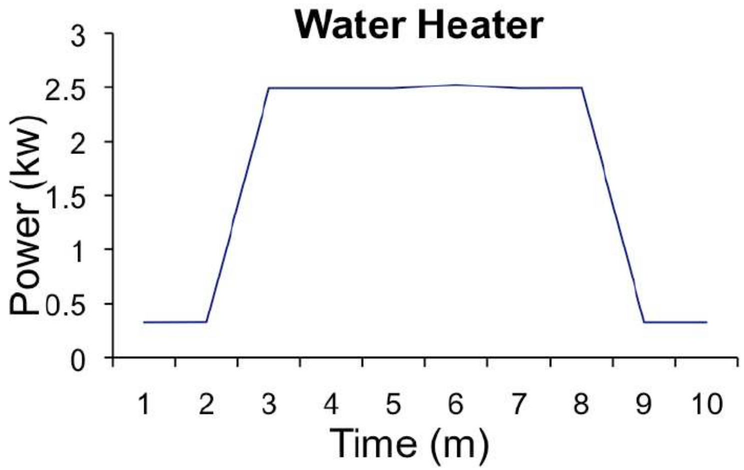
Molina-Markham, Andrés, et al. "Private memoirs of a smart meter."*Proceedings of the 2nd ACM workshop on embedded sensing systems for energy-efficiency in building*. ACM, 2010.

Active Power Signatures for 4 Appliances


Oven


Kettle


Hair Dryer


Water Heater

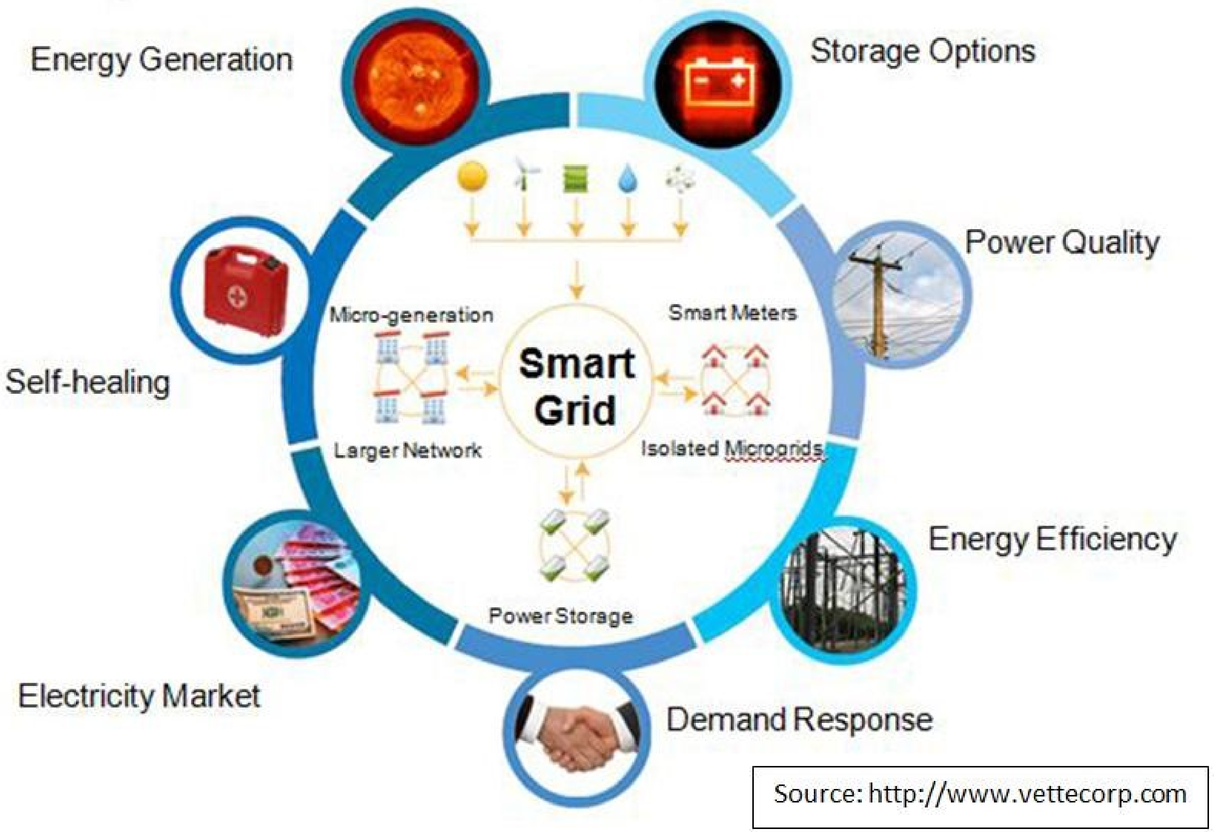
Ruzzelli, Antonio G., et al. "Real-time recognition and profiling of appliances through a single electricity sensor." *2010 7th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON)*. IEEE, 2010.

Motivation

- Need for consumer privacy preservation
- Need for fine-grained data analysis
- Need for securing the communication
- Consumers need to access their own data without revealing their real identity
- Minimal changes to the current grid infrastructure

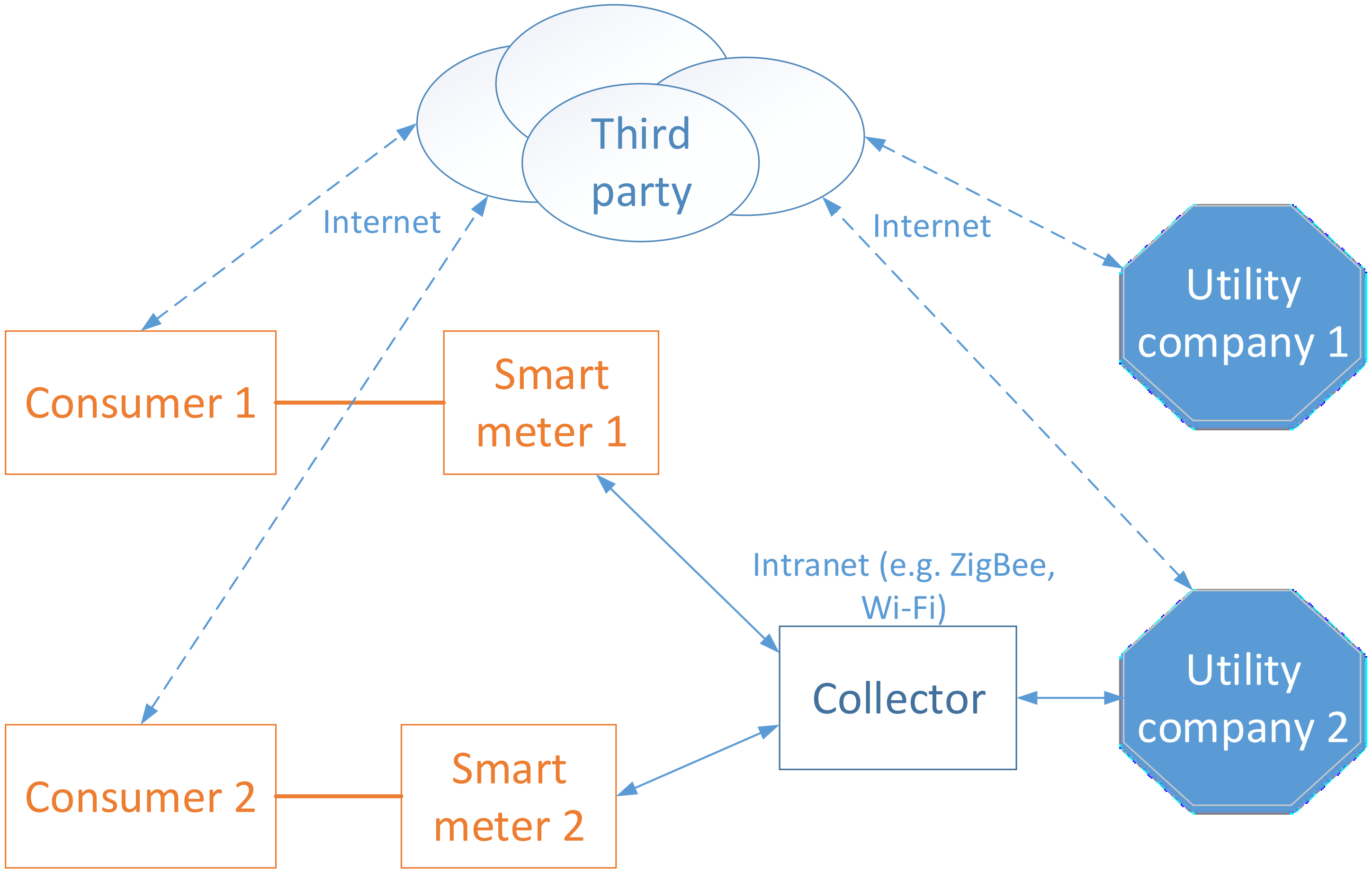
Outline

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



Source: http://www.vettecorp.com

Proposed Infrastructure

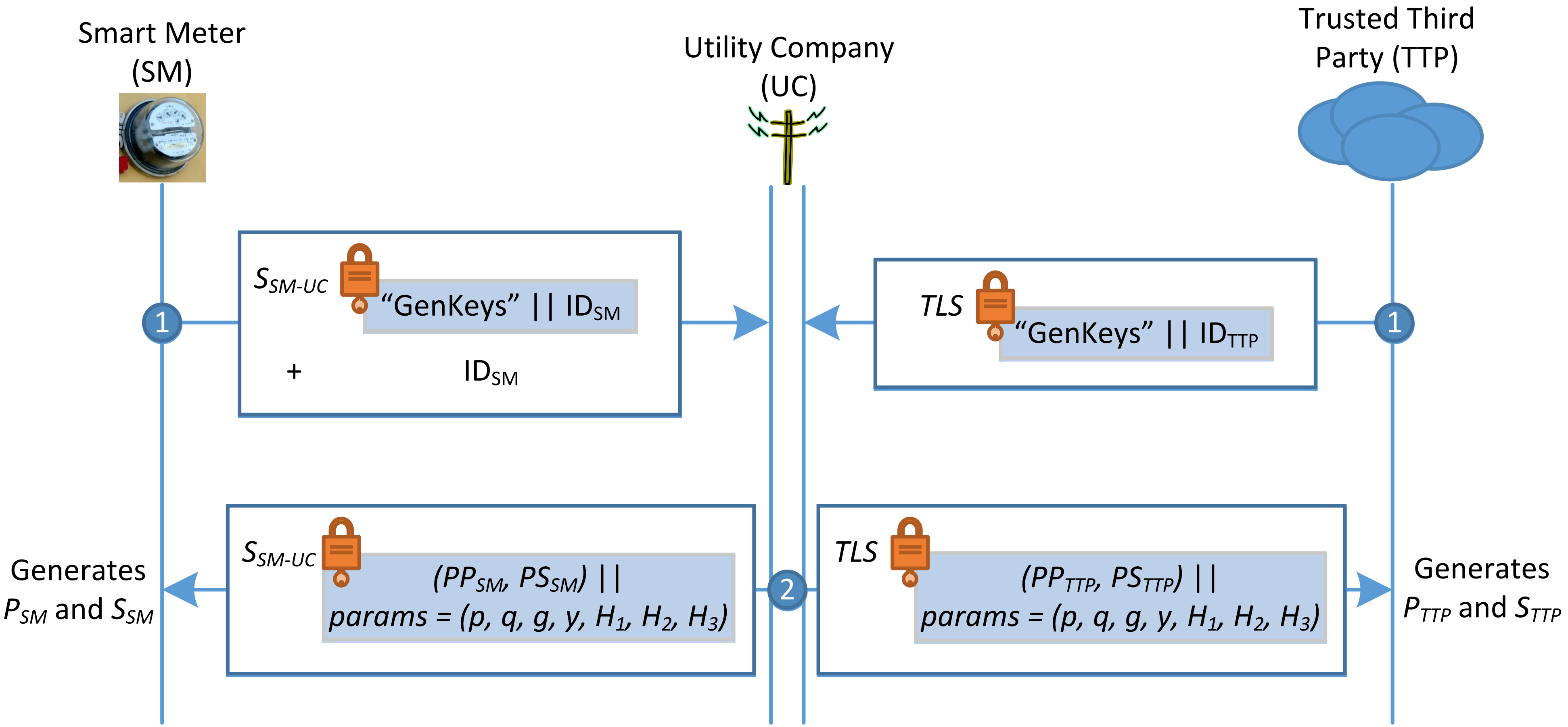


Communication Phases

- Registration phase
  - Certificateless Public Key Encryption [*]
  - Utility Company (UC) serves as a key generation center
  - Smart Meters (SMs) 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

[*] Sun, Yinxia, Zhang, Futai, and Baek, Joonsang. “Strongly Secure Certicateless Public Key Encryption Without Pairing.” In Feng Bao, San Ling, Tatsuaki Okamoto, Huaxiong Wang, and Chaoping Xing, editors, Cryptology and Network Security, volume 4856 of Lecture Notes in Computer Science, pages 194-208. Springer Berlin Heidelberg, 2007.

Registration Phase



Smart Meter (SM)
Utility Company (UC)
Trusted Third Party (TTP)
1
$S_{SM\text{-}UC}$
"GenKeys" || ID_{SM}
+
ID_{SM}
TLS
"GenKeys" || ID_{TTP}
1
Generates P_{SM} and S_{SM}
$S_{SM\text{-}UC}$
(PP_{SM}, PS_{SM}) ||
$params = (p, q, g, y, H_1, H_2, H_3)$
2
TLS
(PP_{TTP}, PS_{TTP}) ||
$params = (p, q, g, y, H_1, H_2, H_3)$
Generates P_{TTP} and S_{TTP}

Registration Phase at Utility Company

- Generate two primes p and q: $q \mid p - 1$
- Pick generator g of $\mathbb{Z}_p^*$ of order q
- Set its private key as a random $x \in \mathbb{Z}_q^*$
- Set its public key as $y = g^x \; mod \; p$

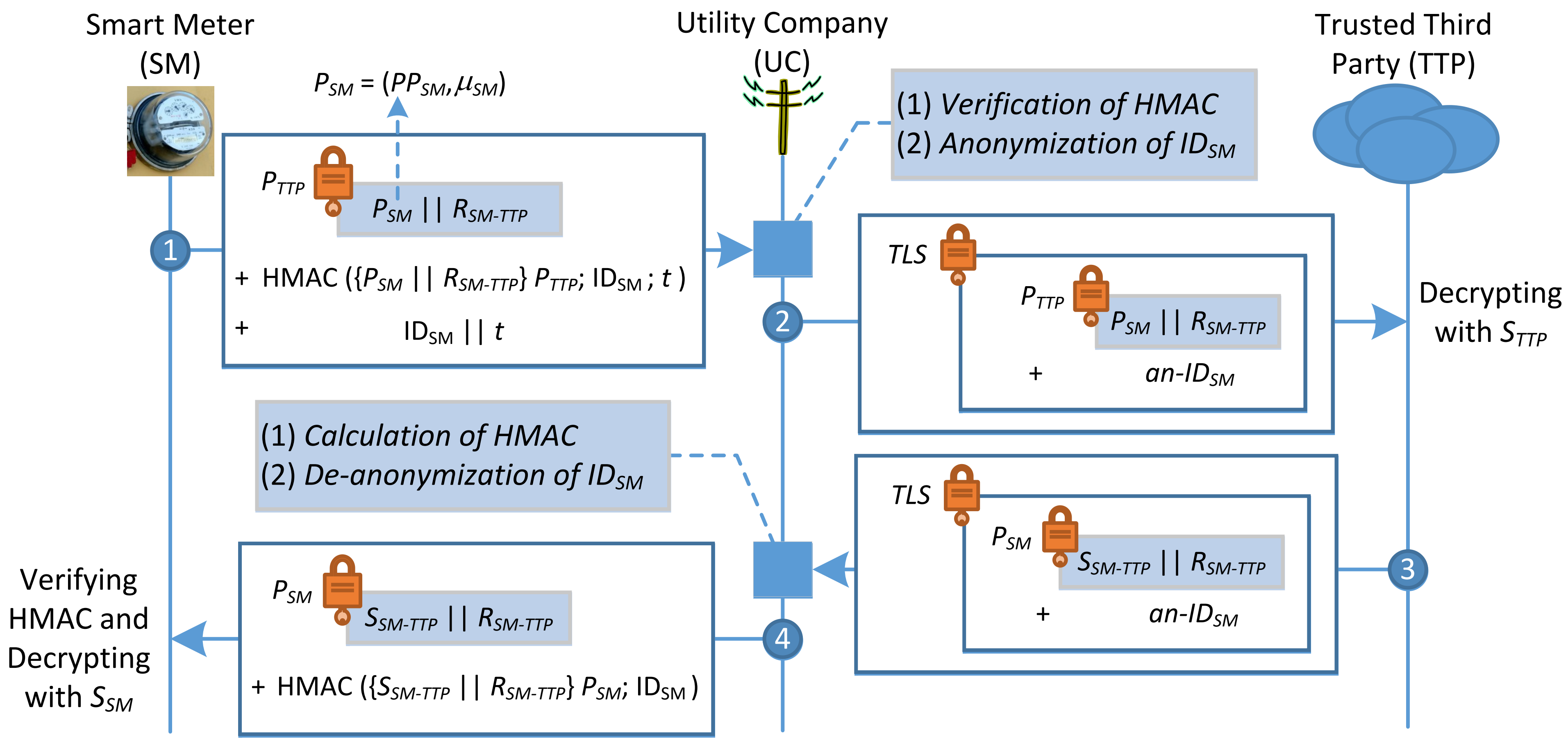
Registration Phase at Utility Company

- Given an *ID*$_R$ from the requester, generate *partial* public/private keys
- Picks $s \in \mathbb{Z}_q^*$ at random
- Computes partial public key $PP_R = g^s \, mod \, p$
- Computes partial private key $PS_R = s + xH_1(ID_R, PP_R) \, mod \, q$
- Partial public and private keys are returned to the requester

Registration Phase at Requester

- Verify partial keys $g^{PS_R} = PP_R \cdot y^{H_1(ID_R, PP_R)}\ mod\ p$
- Pick $z_R \in \mathbb{Z}_q^*$ at random
- Generate full private key $S_R = (z_R, PS_R)$
- Compute $\mu_R = g^{z_R}\ mod\ p$
- Generate full public key $P_R = (PP_R, \mu_R)$

Session Key Exchange Phase



Smart Meter (SM)

Utility Company (UC)

Trusted Third Party (TTP)

$P_{SM} = (PP_{SM}, \mu_{SM})$

1

P_{TTP} $P_{SM} \,||\, R_{SM\text{-}TTP}$

+ HMAC ($\{P_{SM} \,||\, R_{SM\text{-}TTP}\}\ P_{TTP}$; ID_{SM} ; t)

+ $\mathrm{ID}_{SM} \,||\, t$

(1) *Verification of HMAC*

(2) *Anonymization of* ID_{SM}

2

TLS

P_{TTP} $P_{SM} \,||\, R_{SM\text{-}TTP}$

+ $an\text{-}ID_{SM}$

Decrypting with S_{TTP}

3

TLS

P_{SM} $S_{SM\text{-}TTP} \,||\, R_{SM\text{-}TTP}$

+ $an\text{-}ID_{SM}$

(1) *Calculation of HMAC*

(2) *De-anonymization of* ID_{SM}

4

P_{SM} $S_{SM\text{-}TTP} \,||\, R_{SM\text{-}TTP}$

+ HMAC ($\{S_{SM\text{-}TTP} \,||\, R_{SM\text{-}TTP}\}\ P_{SM}$; ID_{SM})

Verifying HMAC and Decrypting with S_{SM}

Session Key Exchange Phase at Smart Meter

- Compute $\gamma_T = PP_T \cdot y^{H_1(ID_T, PP_T)} \; mod \; p$
- Pick $\sigma \in \{0, 1\}^{l_1}$ at random
- Compute $r = H_2(M, \sigma)$, where M is a message with length l_0
- Compute $C = (c_1, c_2)$
    - $c_1 = g^r \; mod \; p$
    - $c_2 = H_3(\mu_T^r \; mod \; p, \gamma_T^r \; mod \; p) \oplus (M_i || \sigma)$

Session Key Exchange Phase at Trusted Party

- Use private key $S_T = (z_T, PS_T)$
- Compute $(M_i||\sigma) = H_3\left(c_1^{z_T} \ mod \ p, c_1^{PS_T} \ mod \ p\right) \oplus c_2$

$$H_3(c_1^z, c_1^w) \bigoplus c_2 = H_3(g^{rz}, g^{rw}) \bigoplus H_3(\mu^r_{TTP}, \gamma^r_{TTP}) \bigoplus (M_i||\sigma) =$$

$$H_3(g^{rz}, g^{rw}) \bigoplus H_3(g^{rz}, (g^s g^{xH_1(ID_{TTP}, PP_{TTP})})^r) \bigoplus (M_i||\sigma) =$$

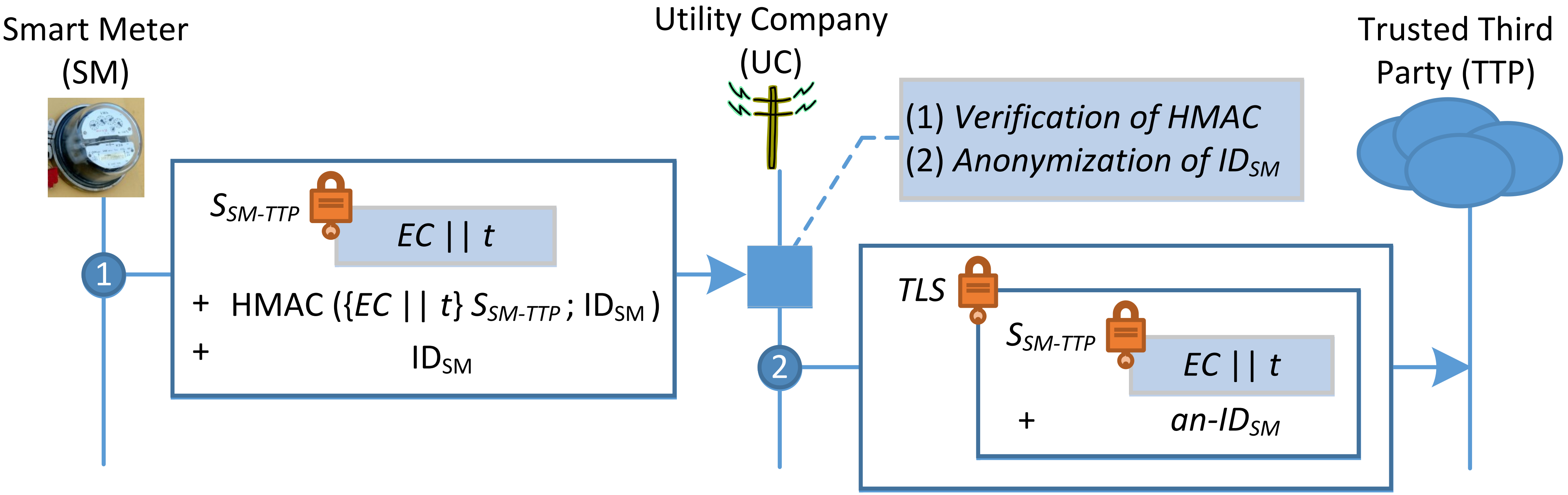
$$H_3(g^{rz}, g^{rw}) \bigoplus H_3(g^{rz}, (g^{s+xH_1(ID_{TTP}, PP_{TTP})})^r) \bigoplus (M_i||\sigma) =$$

$$H_3(g^{rz}, g^{rw}) \bigoplus H_3(g^{rz}, (g^w)^r) \bigoplus (M_i||\sigma) = (M_i||\sigma).$$

Session Key Exchange Phase at Trusted Party

- Verify $g^{H_2(M,\sigma)}\ mod\ p = c_1$
- Retrieve M from $(M_i||\sigma)$

Data Transmission Phase



Smart Meter (SM)

Utility Company (UC)

Trusted Third Party (TTP)

1

$S_{SM\text{-}TTP}$ *EC || t*

+ HMAC ({*EC || t*} $S_{SM\text{-}TTP}$; $\mathrm{ID}_{\mathrm{SM}}$)

+ $\mathrm{ID}_{\mathrm{SM}}$

(1) *Verification of HMAC*

(2) *Anonymization of* ID_{SM}

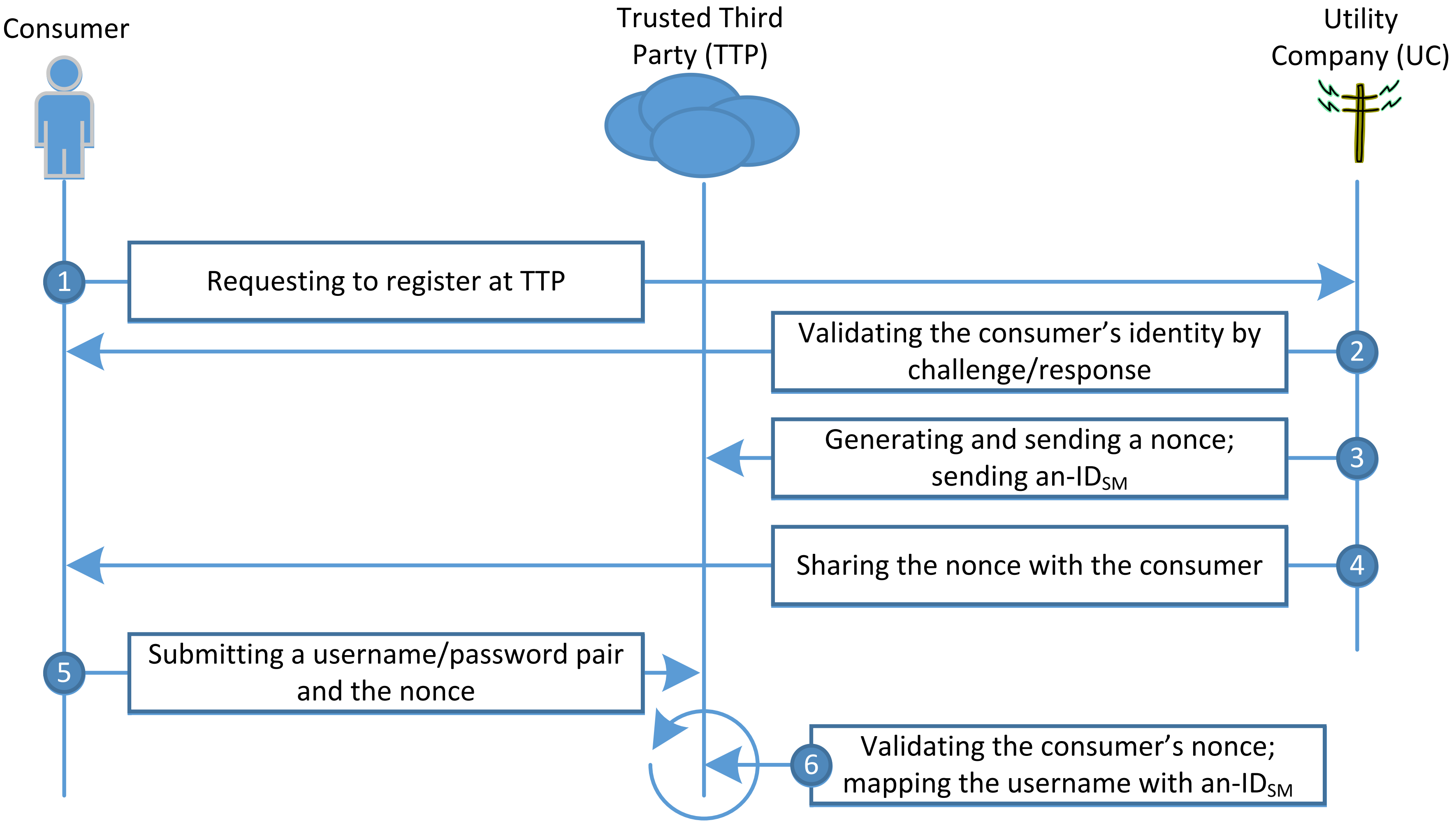
2

TLS

$S_{SM\text{-}TTP}$ *EC || t*

+ *an-*ID_{SM}

Consumer Authentication



Consumer

Trusted Third Party (TTP)

Utility Company (UC)

1 Requesting to register at TTP

2 Validating the consumer’s identity by challenge/response

3 Generating and sending a nonce; sending an-ID$_{SM}$

4 Sharing the nonce with the consumer

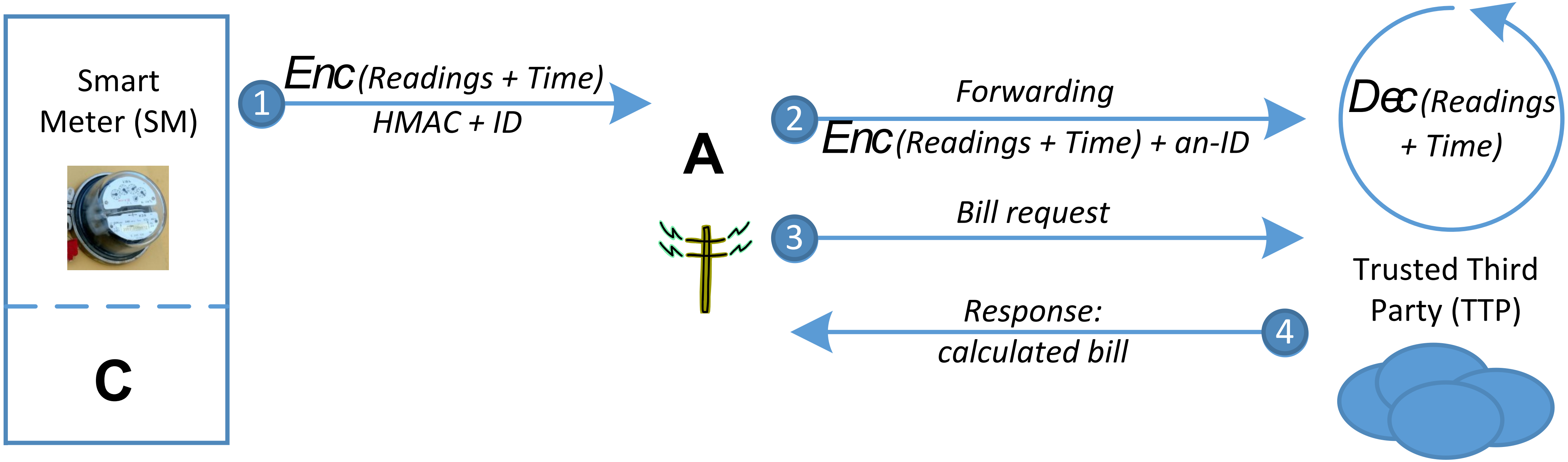
5 Submitting a username/password pair and the nonce

6 Validating the consumer’s nonce; mapping the username with an-ID$_{SM}$

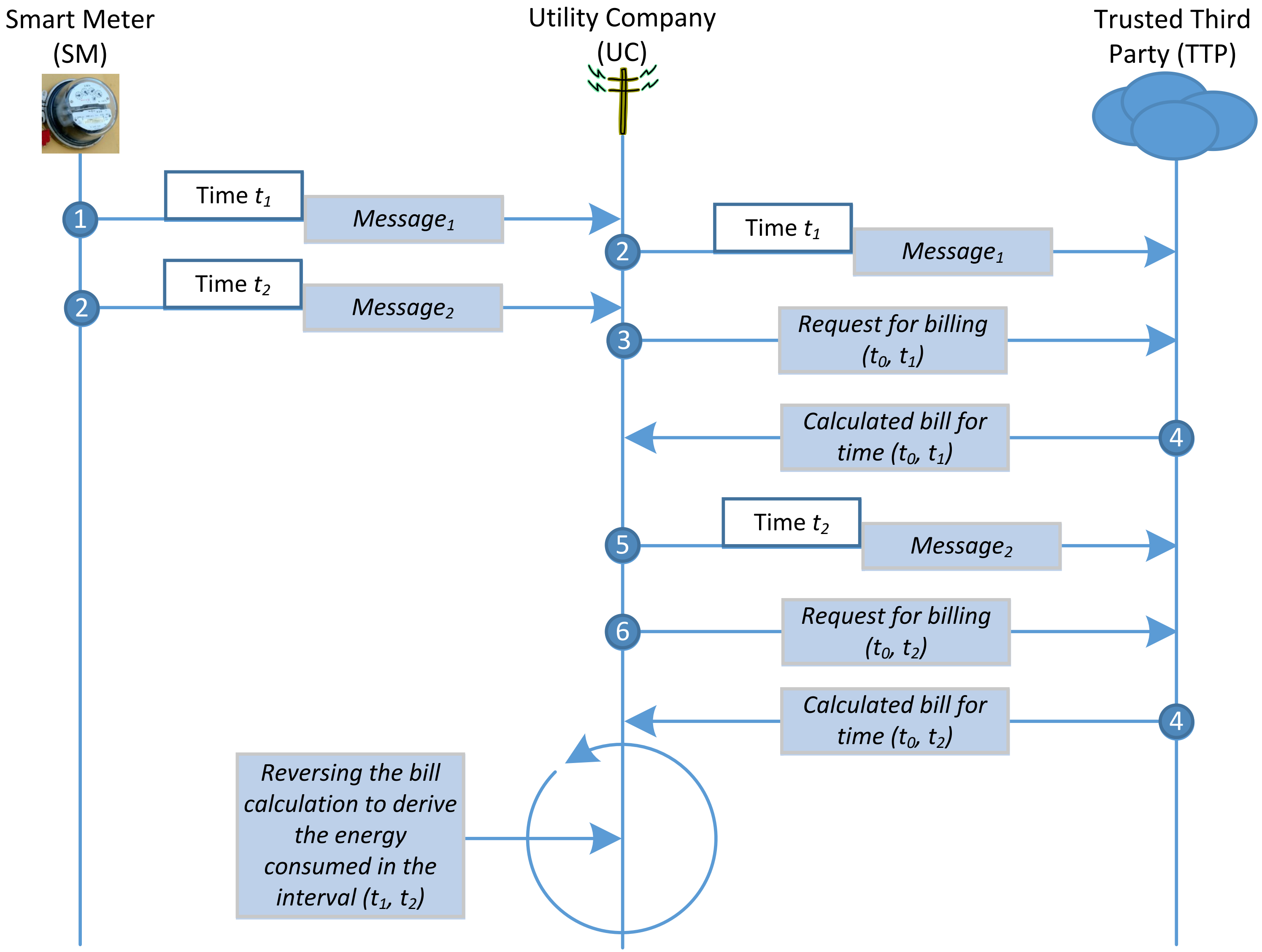
Attack Vectors

- 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

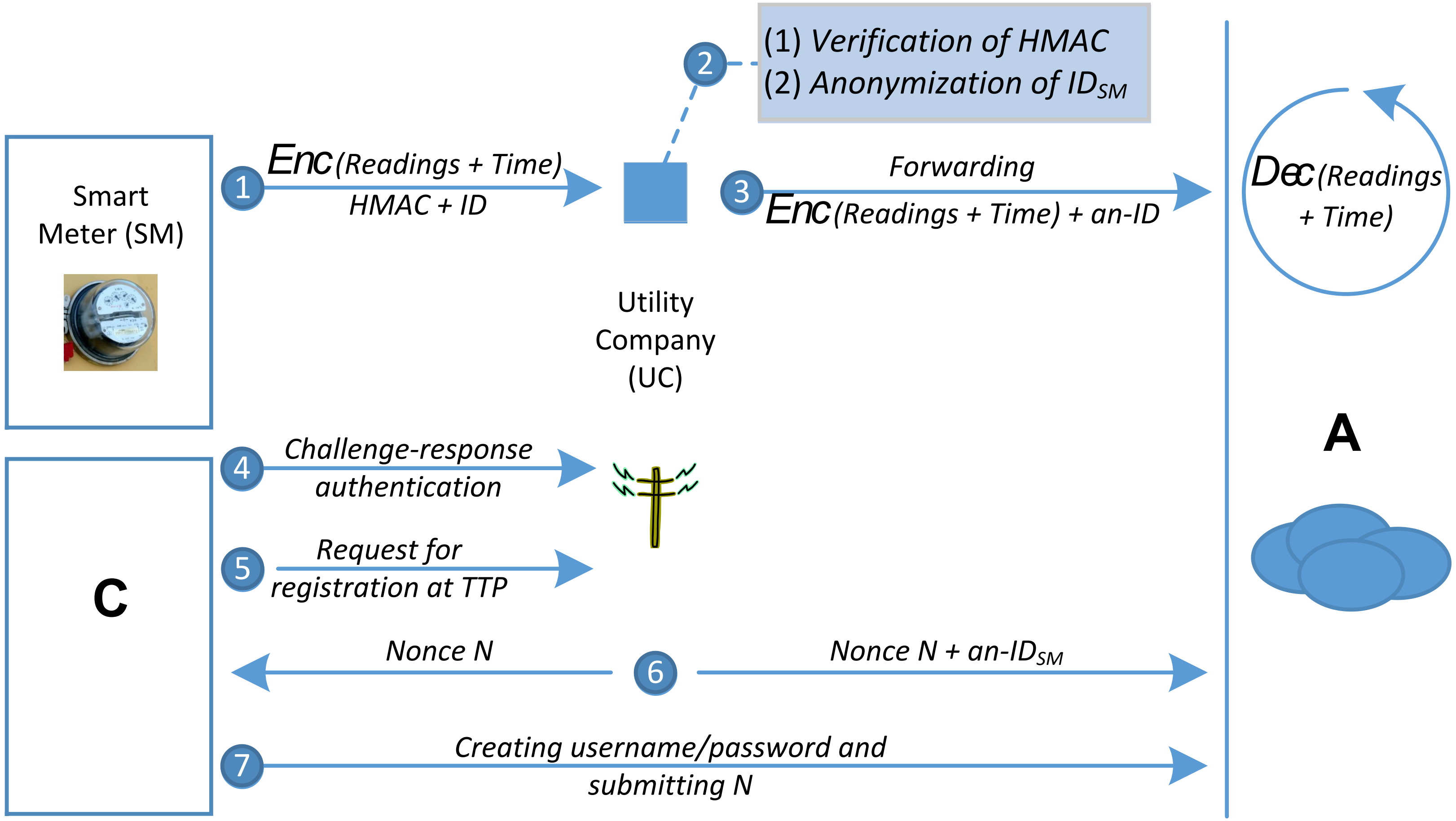
Attacker: Utility Company



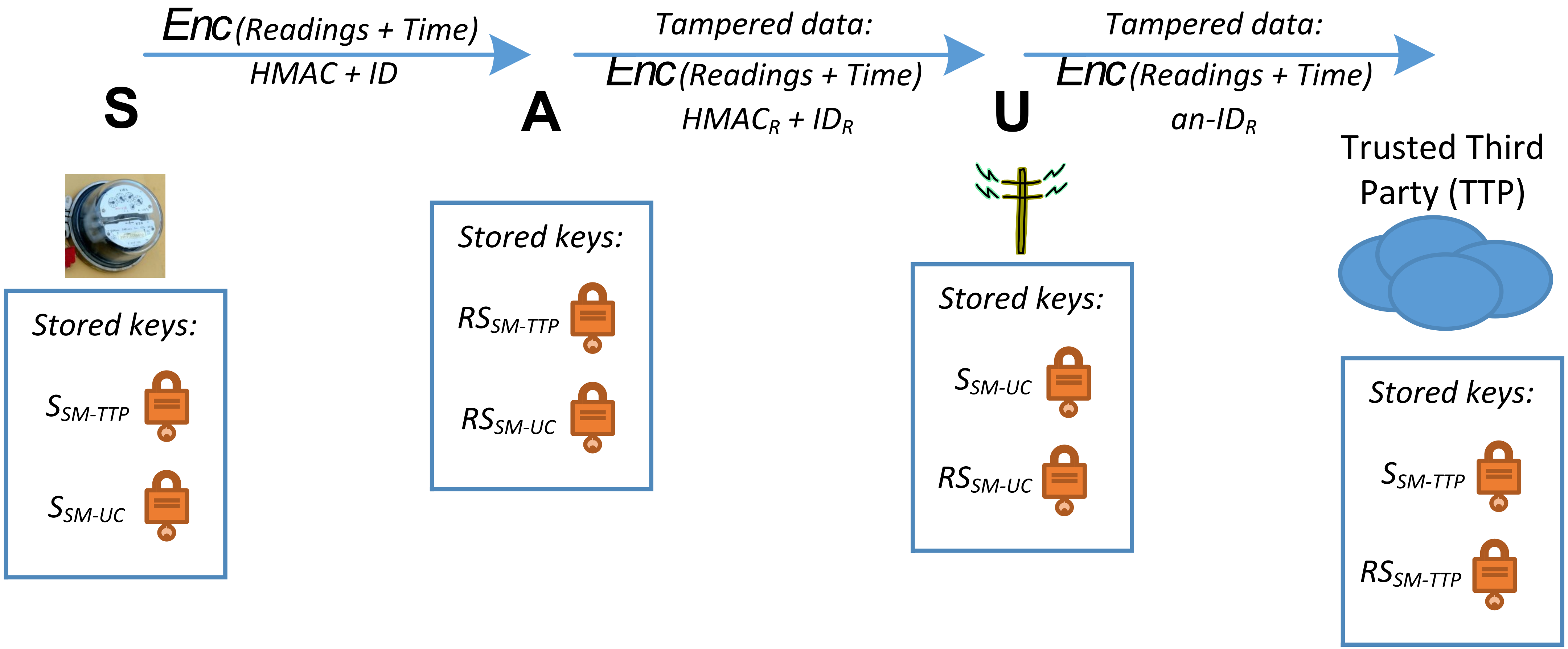
Wait-for-Response Differential Attack


Smart Meter (SM)
Utility Company (UC)
Trusted Third Party (TTP)
1
Time t_1
Message$_1$
2
Time t_1
Message$_1$
2
Time t_2
Message$_2$
3
Request for billing (t_0, t_1)
4
Calculated bill for time (t_0, t_1)
5
Time t_2
Message$_2$
6
Request for billing (t_0, t_2)
4
Calculated bill for time (t_0, t_2)
Reversing the bill calculation to derive the energy consumed in the interval (t_1, t_2)

Attacker: Trusted Third Party



Attacker: MITM



Enc(Readings + Time)

HMAC + ID

S

Stored keys:

$S_{SM\text{-}TTP}$

$S_{SM\text{-}UC}$

A

Tampered data:

Enc(Readings + Time)

$HMAC_R + ID_R$

Stored keys:

$RS_{SM\text{-}TTP}$

$RS_{SM\text{-}UC}$

U

Tampered data:

Enc(Readings + Time)

an-ID_R

Stored keys:

$S_{SM\text{-}UC}$

$RS_{SM\text{-}UC}$

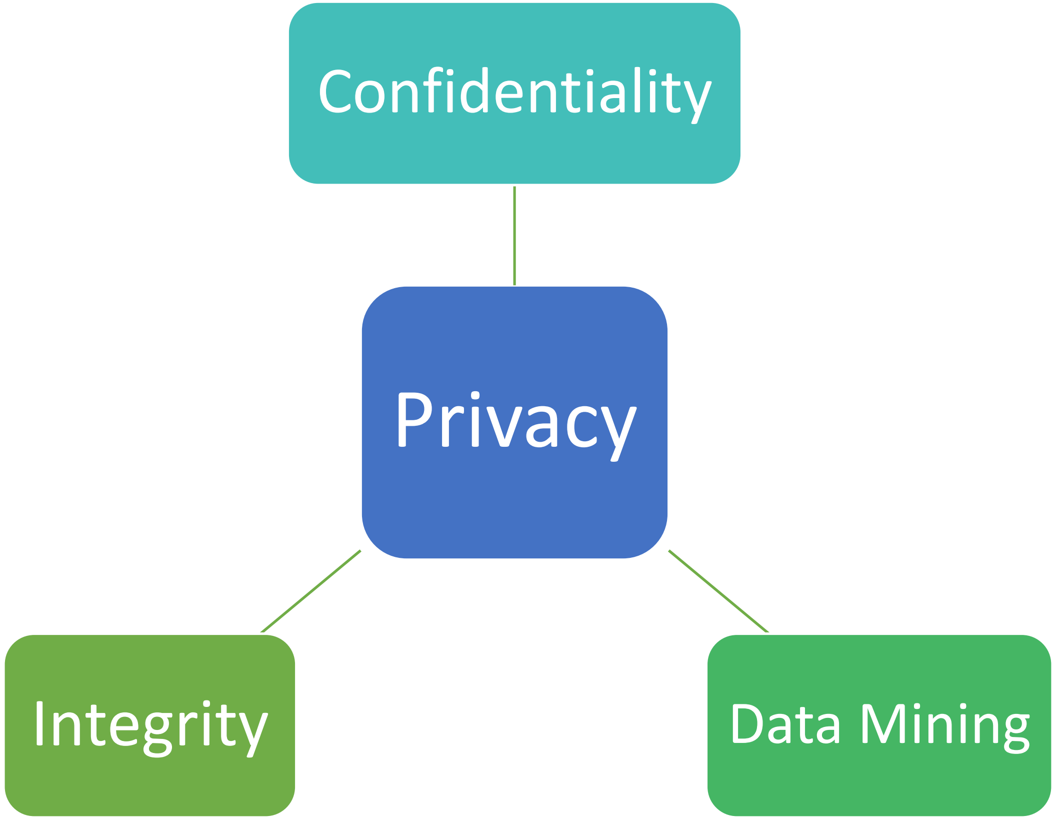
Trusted Third Party (TTP)

Stored keys:

$S_{SM\text{-}TTP}$

$RS_{SM\text{-}TTP}$

Results



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

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.

Thank you!

https://vford.me

fordv@arcadia.edu