Topic 7 : Smart Grid Privacy and Security

Department of Electrical & Computer Engineering
Texas Tech University

Spring 2012

Outline

- Smart Meter Privacy
  - Concerns
  - Possible Solutions
- Smart Grid Security
  - Load Altering Attacks
  - False Data Injection Attacks
- Impact on Electricity Market

Smart Meter

- Smart meter is the key element in:
  - Smart Grid
  - Advanced Metering Infrastructure

Smart Meter

- Enables two-way communications between users and utilities.
  - Pricing Information
  - Consumption Readings

Smart Meter

- Unlike traditional meters:
  - Manual Reading
  - Monthly Reading
- Smart meters:
  - Automated reading (wireless links e.g., in WMNs)
  - Once every 15 minutes (common rate)
  - Once every minute (can support)

Smart Meter

- Some of the applications of smart meters:
  - Utility: Collect, measure, and analyze consumption data for
    - Grid management
    - Outage notification
    - Billing purposes
  - Consumer: Better options to manage their load / bills.
    - Energy Detective®, Google Power meter®, …

Smart Meter Privacy Concerns

- Key Issue:
  - Data recorded by smart meters must be highly detailed
    - It may show what individual appliances a user is using.

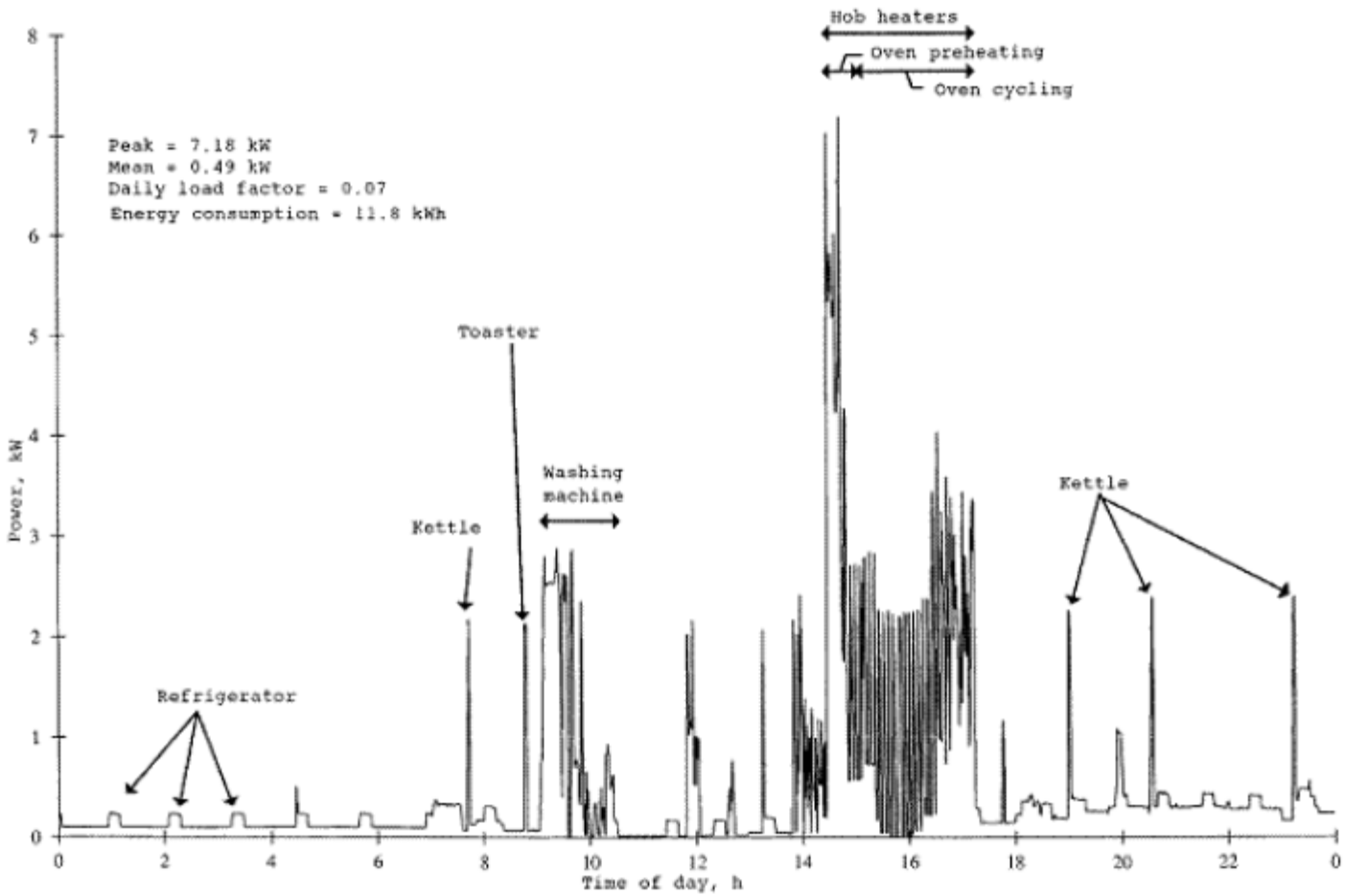
- Furthermore:
  - The readings are transmitted over wireless channels
    - Q: What if the transmissions is intercepted?

Smart Meter Privacy Concerns

- People have raised some concern about smart meters:
  - www.youtube.com/watch?v=8JNFr_j6kdI&feature=relmfu
  - www.youtube.com/watch?v=FLeCTaSG2-U
- Just Google "smart meter privacy concerns"!
- Q: How can smart meters reveal
  - What exact appliance you use at what exact time?

Smart Meter Privacy Concerns

- Each appliance has a "signature":



Power Usage to Personal Activity Mapping

Smart Meter Privacy Concerns

- Example 1: Criminals can use the data
  - To schedule burglary
    - They can figure out if you are not at home.
    - House alarm systems have their own signature
  - Pre-identify what items they want to steal.
    - Plasma TVs have their own signature.
    - Laptop computers have their own signature

Smart Meter Privacy Concerns

- Example 2: Privacy violation
  - Your living pattern can be revealed
    - When you wake up.
    - When you take shower
    - When you watch TV
  - You can even tell what TV program / movie is watched!
    - Fluctuations at brightness of movies → Load changes!

Smart Meter Privacy Concerns

- Example 3: Health Insurance Company can
  - Determine which medical devices you used.
    - Pre-existing conditions
    - Different insurance rate
- Example 4: Your landlord can tell
  - How many people live here.
  - When you have a party!

Smart Meter Privacy Solutions

- Q: How can we resolve these privacy concerns?

- Q: How can we assure that:
  - Appliance signatures cannot be identified.
  - It is not revealed that you have no power consumption

- Some solutions may involve privacy / performance tradeoffs.

Smart Meter Privacy Solutions: Reading Rate

- Smart meters can support minute-by-minute reporting.

- The current reading rate is once every 15 minutes
  - It may still reveal most appliance signatures.

- Q: Does it help to increase reading intervals?
  - What would be the problem?
  - Is there any trade-off?

Smart Meter Privacy Solutions: Renewable Generation

- Q: What if users have local renewable generation?

- In that case, we have

Meter reading = Load – Local Renewable Generation

Stochastic Nature

- It is just like we are adding noise to meter readings.
  - Q: Can we actually add intentional noise to reading?

Smart Meter Privacy Solutions: Storage

- Q: What if we have a battery at home?

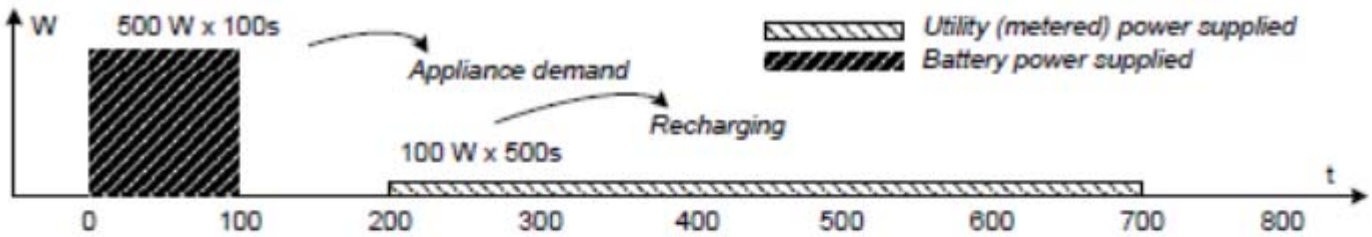
- By charging and discharging the battery we can
  - Have impact on the reported meter reading.

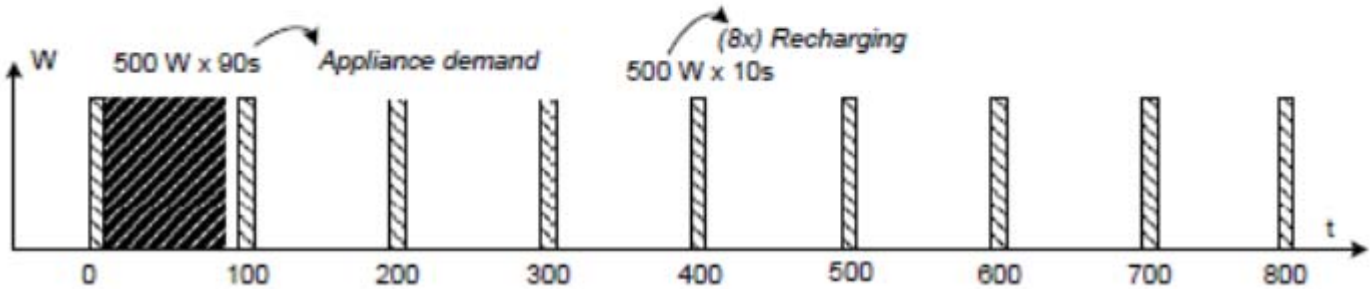
Meter Reading = Load – Discharge + Charge

- This is called "Load Signature Moderation".

Smart Meter Privacy Solutions: Storage

- Q: What if we have a battery at home?





Two approaches to moderate / hide the signature

Smart Meter Privacy Solutions: Encrypted Reading

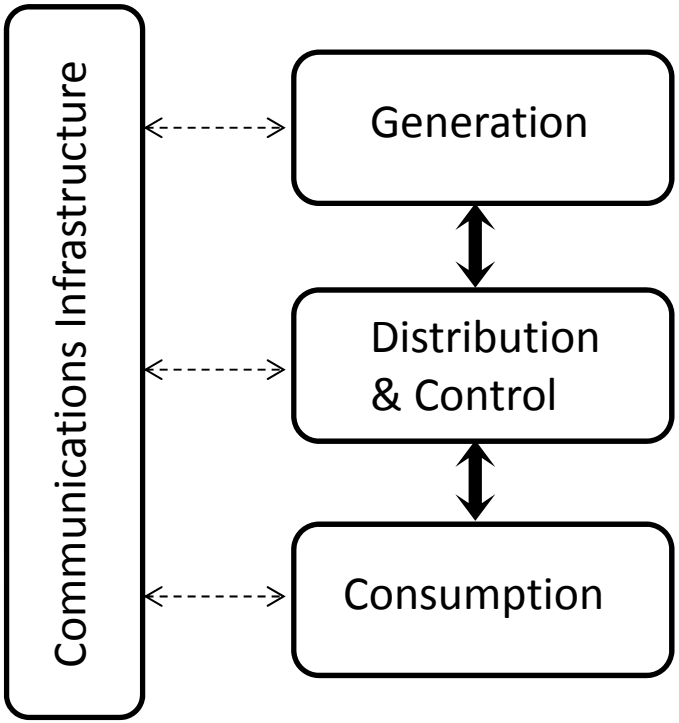
- So far, we have seen methods to hide the signatures.

- Q: What if we are on vacation?
  - Our meter readings indicate no/limited consumption.

- Some solutions:
  - Always report the load, even if the load is zero.
  - Encrypt the reported reading. (Q: What else can you do?)

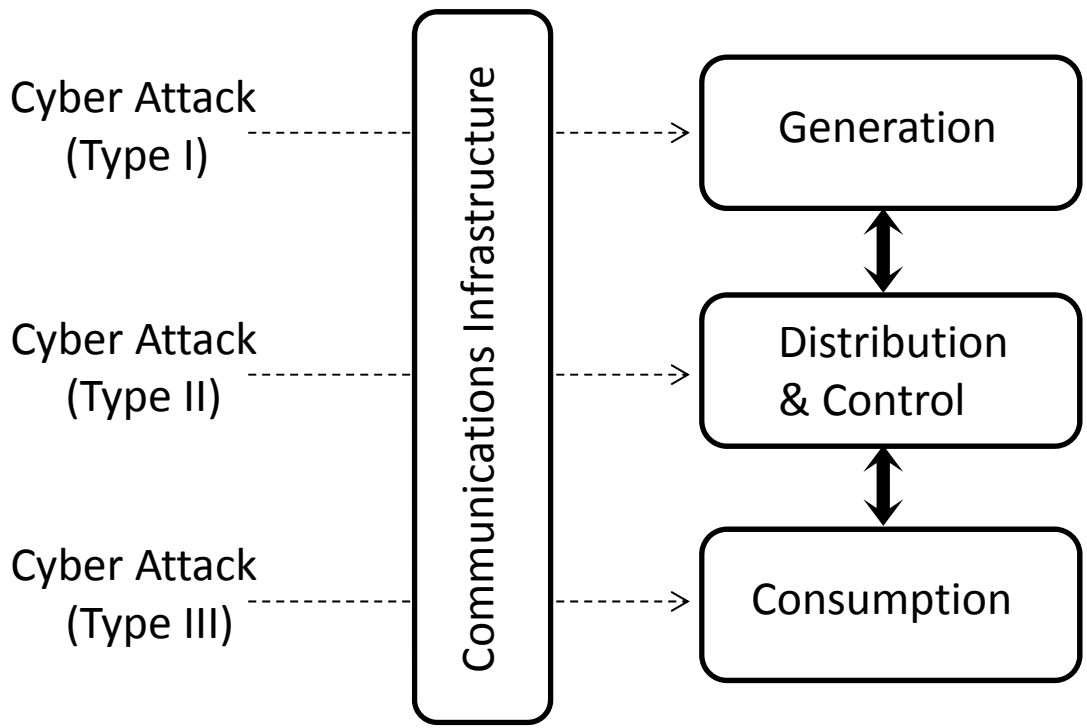
Smart Grid Security

- In Smart Grid all sectors interact via two-way communications:



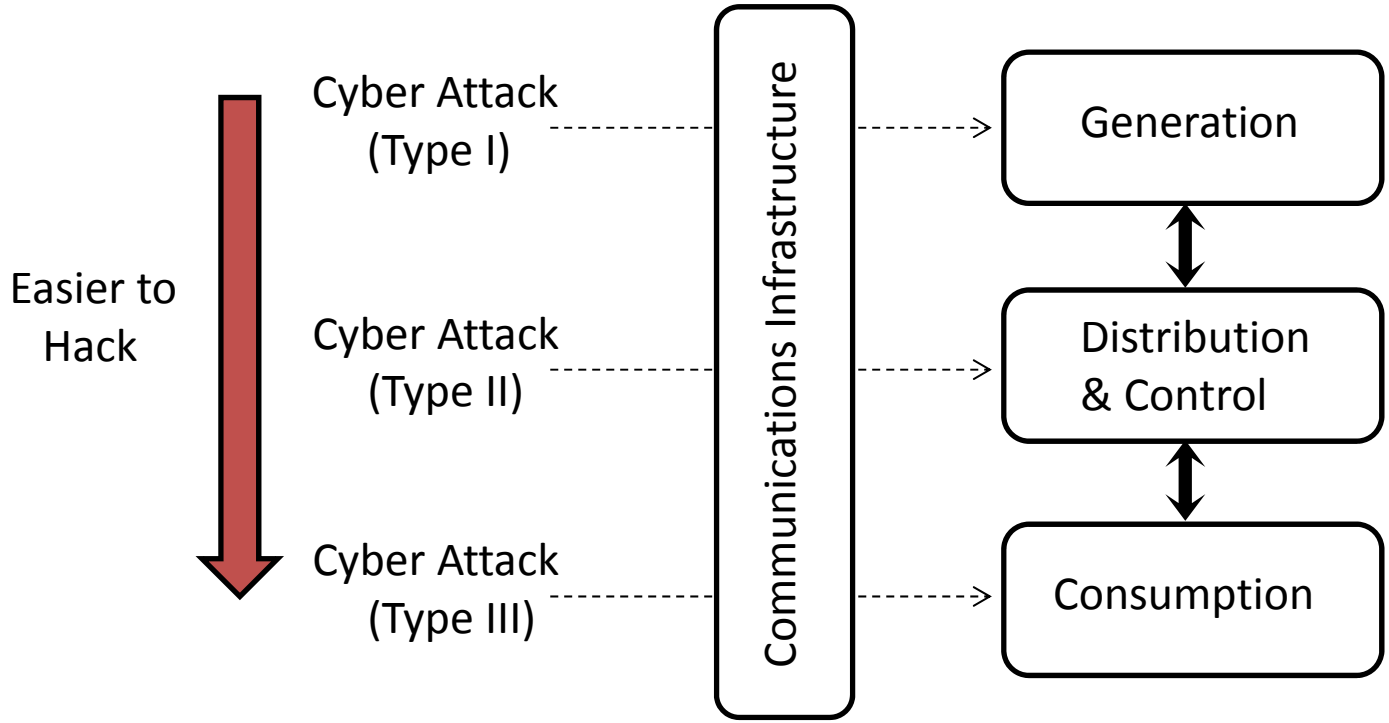
Smart Grid Security

- We can identify three types of cyber attacks against smart grid:



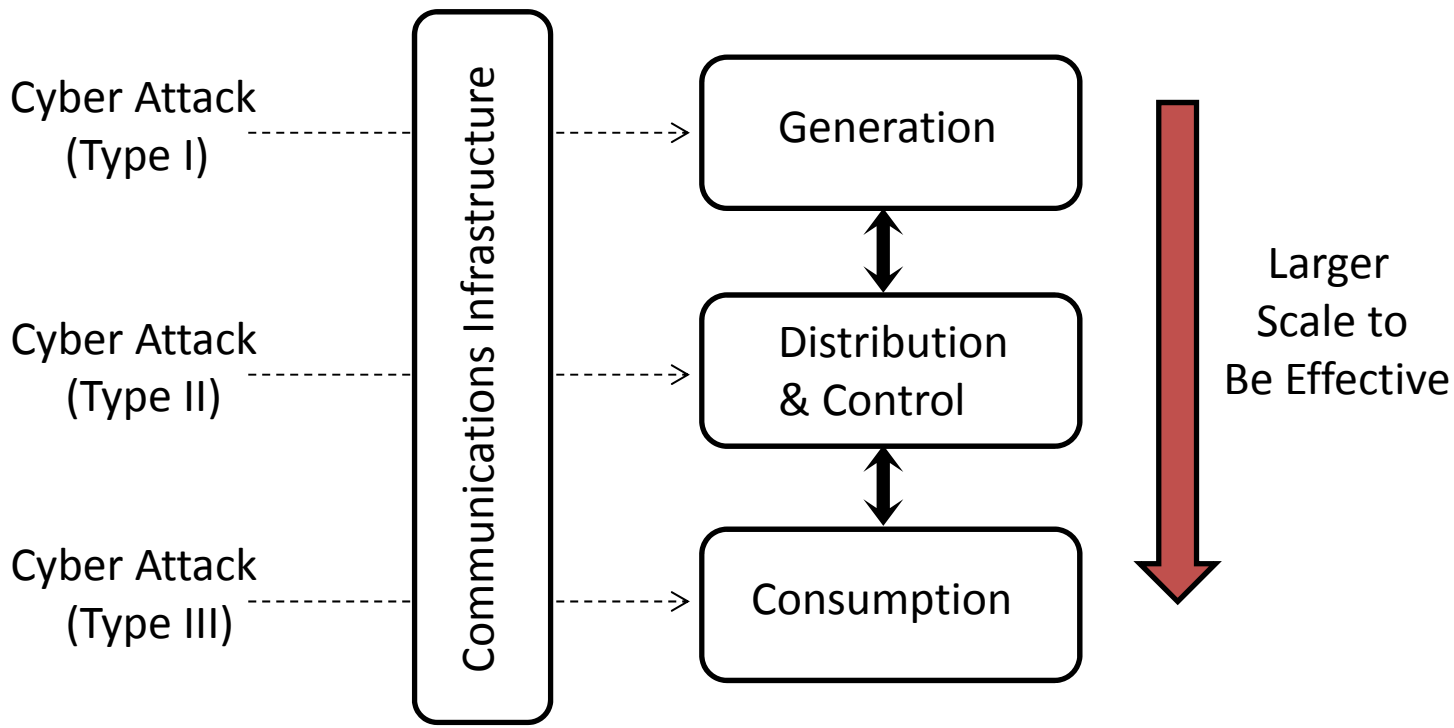
Smart Grid Security

- We can identify three types of cyber attacks against smart grid:



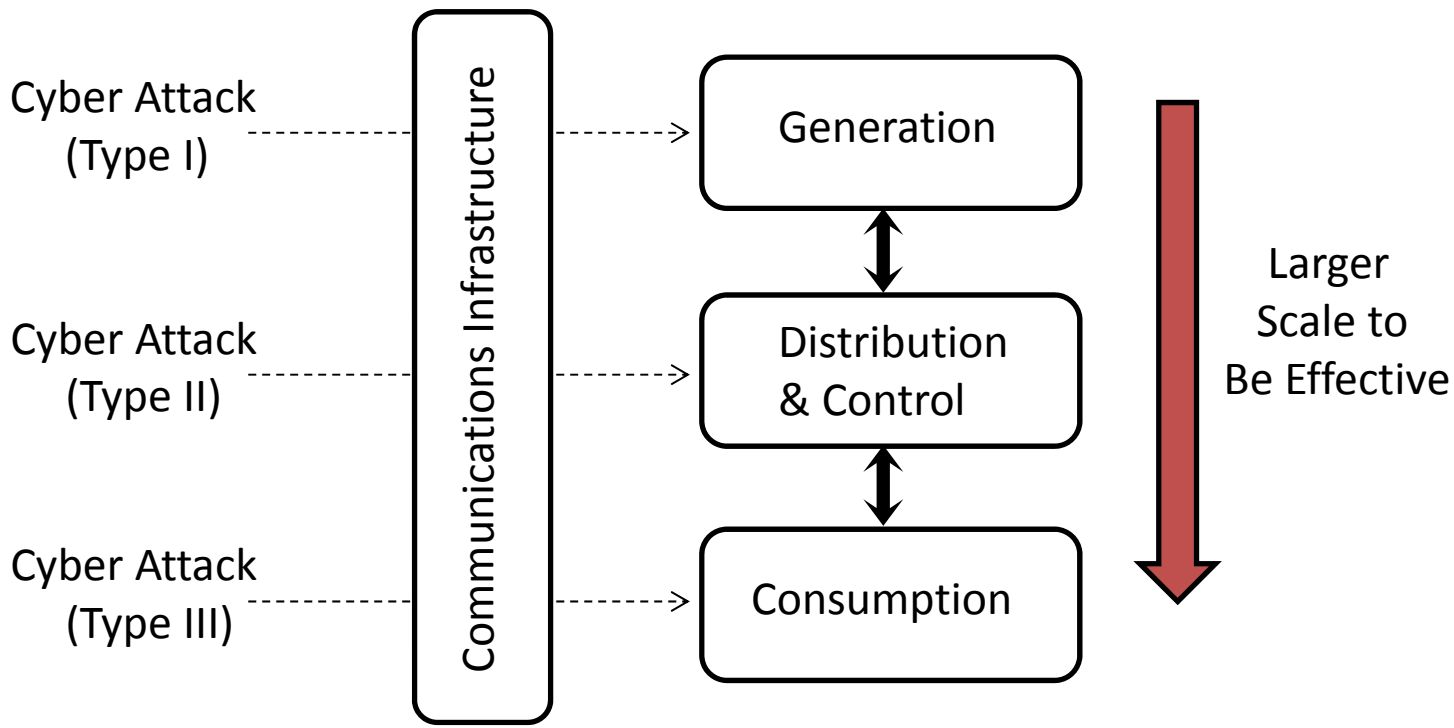
Smart Grid Security

- We can identify three types of cyber attacks against smart grid:



Smart Grid Security

- We can identify three types of cyber attacks against smart grid:



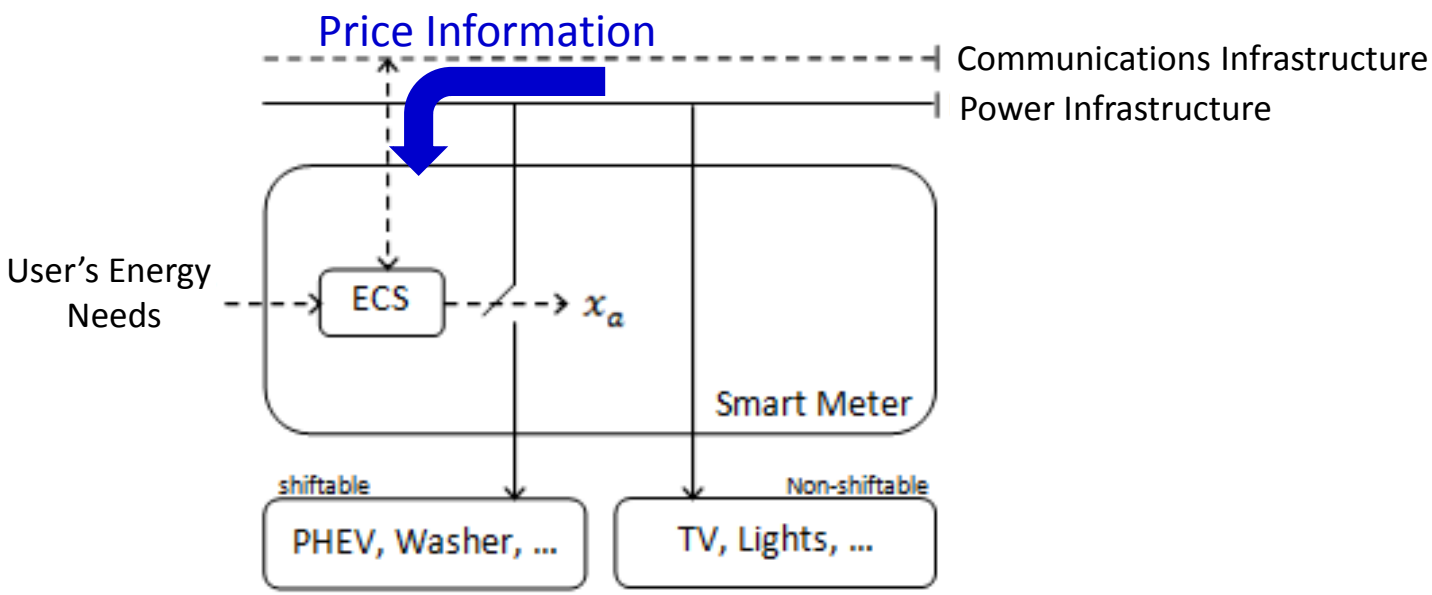
Hacking a Power Plant = Hacking Hundred of Thousands of Meters

Smart Grid Security

- We will discuss two types of cyber attacks:
  - Load Altering Attacks (Type III)
    - Targets Smart Meters and ECS Devices
    - Can affect Demand Response and System Stability
  - False Data Injection Attacks (Type II)
    - Targets PMUs and possibly Smart Meters
    - Can affect Situational Awareness and System Stability

Load Altering Attacks

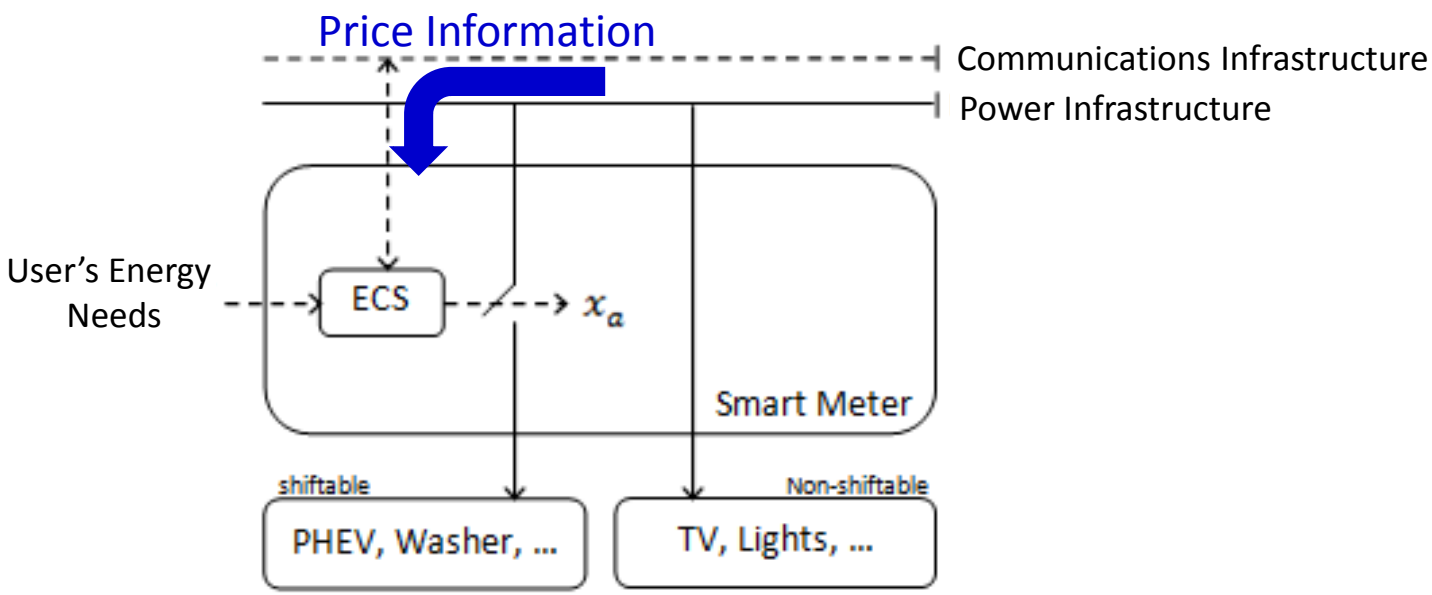
- Smart meter with an embedded ECS:



- x_a : Energy consumption schedule for appliance *a*.

Load Altering Attacks

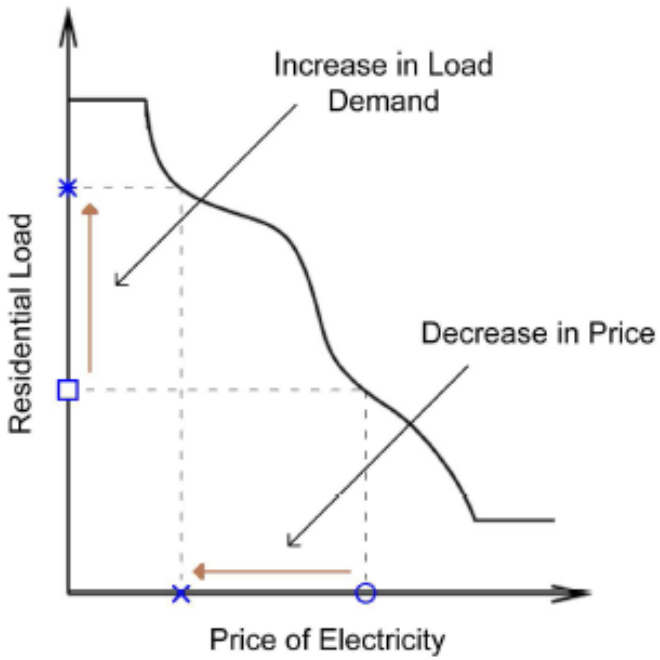
- Smart meter with an embedded ECS:



- Q: What if the price signal is compromised?

Load Altering Attacks

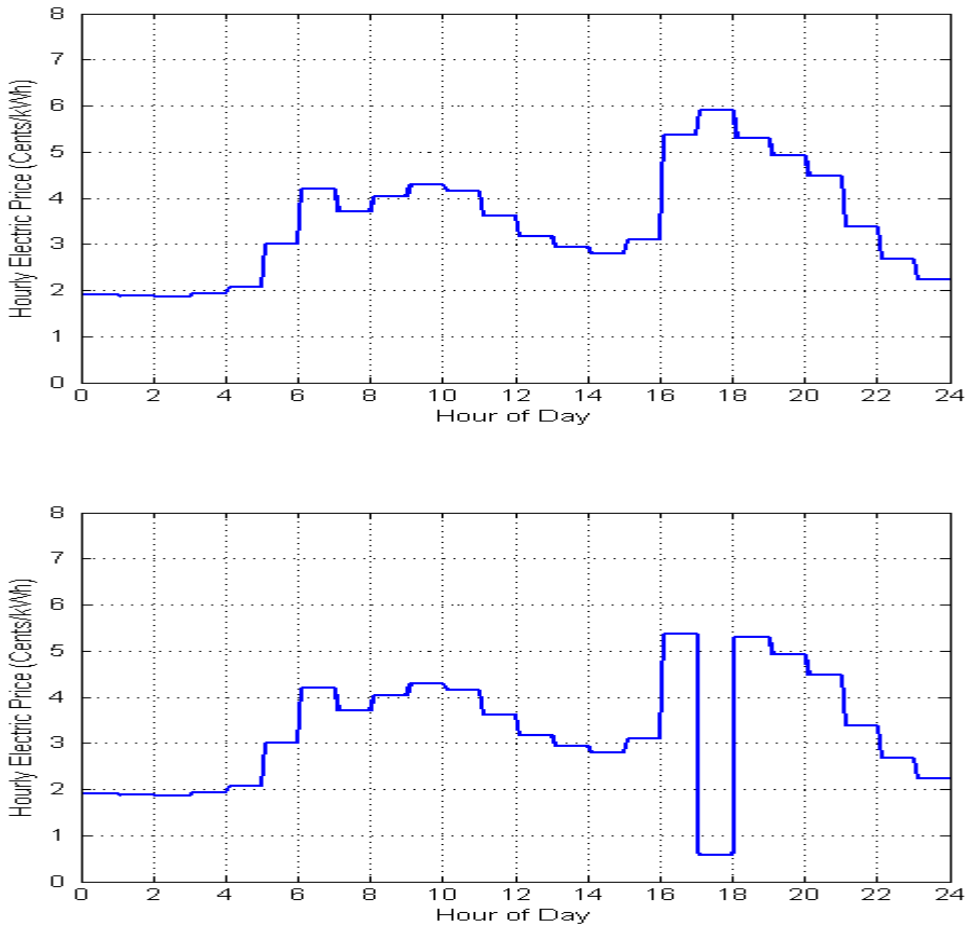
- Changes in price can change the load scheduled by ECS:



Reduced price will encourage increasing load at that hour.

Load Altering Attacks

- Changes in price can change the load scheduled by ECS:



Load Concentration

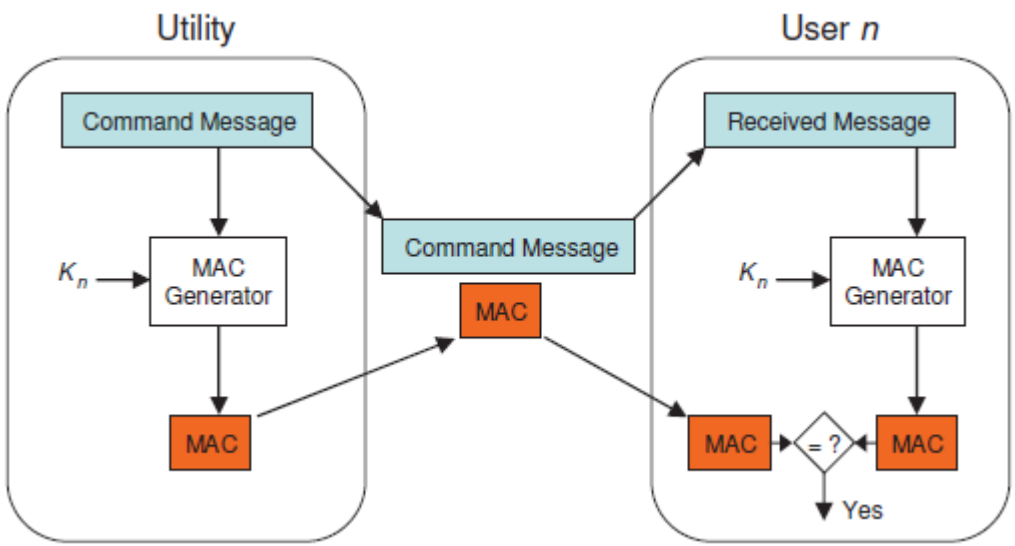
at 6:00 PM

Load Altering Attacks

- Assume that a hacker compromises the price data:
  - Sent to hundreds of thousands of ECS devices.
- A large number of users jump into the reduced price hour.
  - Q: Similar to load synchronization problem?
  - This can cause a load spike at an already peak hour.
  - Price signals have to be source authenticated.

Load Altering Attacks

- One option to authenticate received messages:

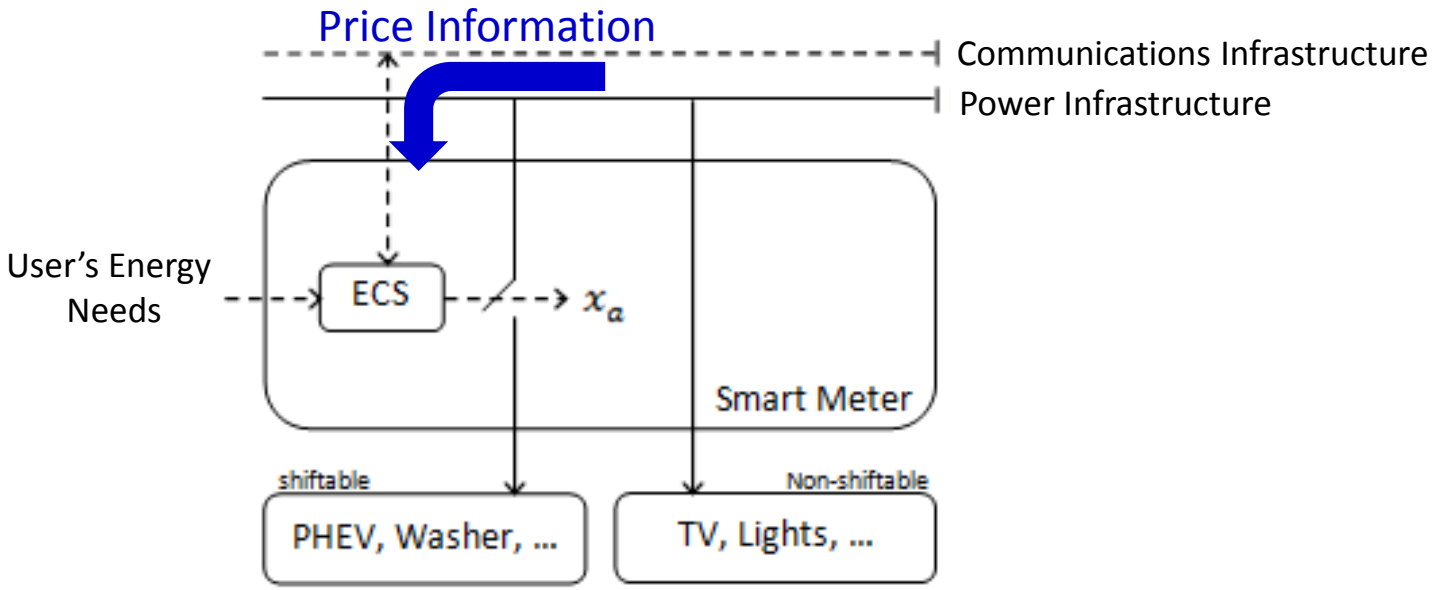


MAC: Message Authentication Code

- In general, source authentication is not very easy.

Load Altering Attacks

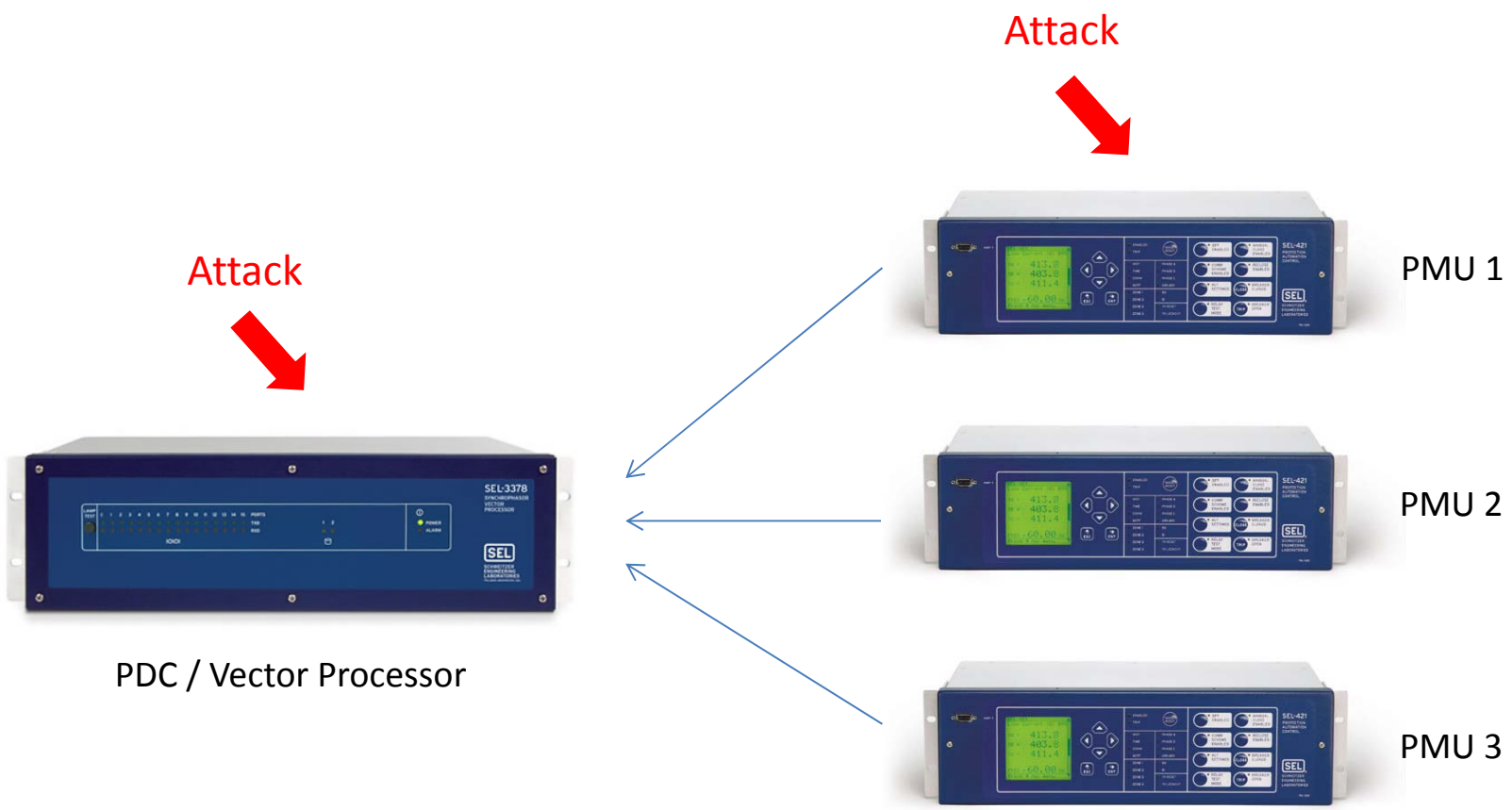
- Smart meter with an embedded ECS:



- Q: What if the DLC signal or the ECS itself are compromised?

False Data Injection Attacks

- They target PMUs and wide-area measurement systems:

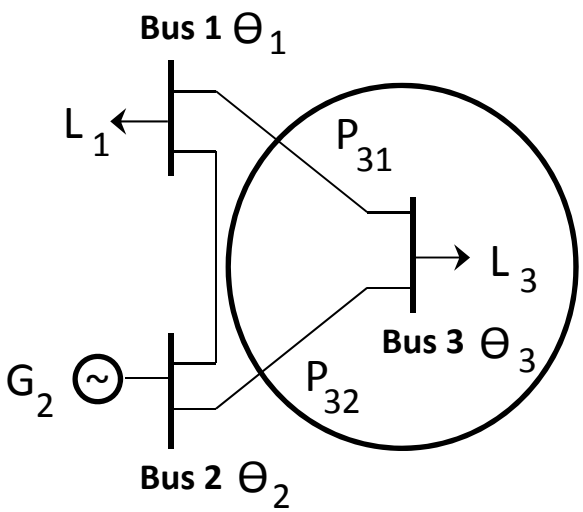


False Data Injection Attacks

- False data injection results in
  - Sending **incorrect data** to control centers.
- **Incorrect decisions** made by control center may lead to:
  - Inefficient Dispatch / Power Quality Degradation
  - Unnecessary Load Shedding
  - False Alarm / Erroneous Fault Detection
  - System Instability

False Data Injection Attacks

- A tempting target for an FDIA is state estimation.
  - **Northeast Blackout** initiated by error in state estimation



$$P_{31} + P_{32} - L_3 = 0$$

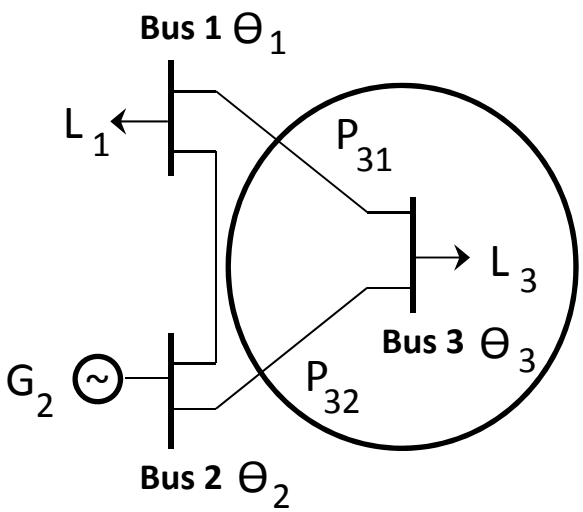
$$P_{31} = B_{31}(\theta_3 - \theta_1)$$

$$P_{32} = B_{32}(\theta_3 - \theta_2)$$

(B_{31} and B_{32} are obtained from Y - Bus Matrix)

False Data Injection Attacks

- A tempting target for an FDIA is state estimation.
  - **Northeast Blackout** initiated by error in state estimation



$$P_{31} + P_{32} - L_3 = 0$$

$$P_{31} = B_{31}(\theta_3 - \theta_1)$$

$$P_{32} = B_{32}(\theta_3 - \theta_2)$$

Several variables / states in the system

(B_{31} and B_{32} are obtained from Y - Bus Matrix)

False Data Injection Attacks

- State estimation problem:

Problem: An *n* x 1 vector of **unknown states** **x** is aimed to be estimated given an *m* x 1 vector of **measurements** **z**, where ***m* >> *n***. We know that

$$\mathbf{z} = \mathbf{H}\,\mathbf{x} + \mathbf{e}$$

Measurement

Measurement Errors / Noise

Topology + Kirchhoff's Circuit Laws

False Data Injection Attacks

- Example: States can be
  - States: Phase Angles at Each Bus
  - Measurements: Power Injection at Each Bus

    Power Flow on Each Link

- We can write down the power flow equations in form of:

$$\mathbf{z} = \mathbf{H}\,\mathbf{x} + \mathbf{e}$$

False Data Injection Attacks

- We would like to find a state estimation $\hat{x}$ such that

$$\min_{\hat{x}} \left\| z - H\,\hat{x} \right\|$$

- That is, we apply the least square error criterion.

- In most cases, we rather apply weighted least-square criterion:

$$\min_{\hat{x}} \sum_{i=1}^{m} \left(\frac{z_i - H_i \hat{x}}{\sigma_i} \right)^2$$

Q: What is the weight?

False Data Injection Attacks

- For regular least-square criterion, we have

$$\hat{x} = (H^T H)^{-1} H^T z$$

- For weighted least square criterion, we have

$$\hat{x} = (H^T W H)^{-1} H^T W z$$

where

$$W = diag\begin{bmatrix}\sigma_1^{-2} & \sigma_2^{-2} & \cdots & \sigma_m^{-2}\end{bmatrix}$$

False Data Injection Attacks

- If something goes wrong with measurements z:
  - Then, the state estimation solution will be incorrect!

- We can think of two scenarios:
  - Faulty Sensors / Bad Measurement (Natural Cause)
  - False Data Injection Attack (Intentional)

False Data Injection Attacks: Bad Data Detection

- Q: How can we detect a bad measurement?

- Key Idea: Measurements should reasonably match each other!

  - Bad data is detected if we see "inconsistency" in data.

- We define measurement residual as:

$$r = z - H\hat{x}$$

False Data Injection Attacks: Bad Data Detection

- Q: Do you expect low or high residual for accurate estimation?

- Residue Test:
  - Is $\|r\| = \|z - H\hat{x}\| \le \tau$? $\longrightarrow$ **Yes**: Pass

    $\longrightarrow$ **No**: Bad Data

- Here, norm is l_2 or l_∞ and τ is a design constant.

False Data Injection Attacks

- Q: How about FDIA and intentional error injection?

- Key Idea: Compromise the sensor reading:

$$z_a = z + a$$

Injected False Data

- The new state estimation solution becomes (Q: Why?):

$$\hat{x}_{bad} = (H^T W H)^{-1} H^T W z_a$$

False Data Injection Attacks

- Q: Can the attacker choose *a* such that
  - The attack is not detected?

- A: Yes, *a* should be a linear combination
  - Of the column vectors of matrix *H*. (Q: Why?)

False Data Injection Attacks

$$\hat{x}_{bad} =$$

$$r_a = z_a - H\,\hat{x}_{bad}$$

False Data Injection Attacks

- Q: Can we pick an arbitrarily large *c*?

- That is, can we have

$$\|c\| \to \infty \ ?$$

- Q: How does it affect $\hat{x}_{bad}$?

- Q: How does it affect r_a ?

False Data Injection Attacks

- Note that in general, the attacker is interested in

  - Maximizing State Estimation Error:

$$\underset{\mathrm{a}}{\text{maximize}} \ \left\| \hat{x}_{bad} - \hat{x} \right\|$$

  - Minimizing the Chance of Being Detected:

$$\underset{\mathrm{a}}{\text{minimize}} \ \left\| r_a - r \right\|$$

False Data Injection Attacks

- Next, we consider three scenarios:
  - Some sensors are protected:
    - For some $i \in \{1, \ldots, m\}$, it is required that $a_i = 0$.
  - Some state variables can be verified independently:
    - For some $j \in \{1, \ldots, n\}$, it is required that $c_i = 0$.
  - Both cases above happen simultaneously.

False Data Injection Attacks: Protected Sensors

- Q: What if some sensors are protected?
  - For some $i \in \{1, \ldots, m\}$, it is required that $a_i = 0$.

- Example: Sensor 2 is protected:

$$\begin{bmatrix} a_1 \\ 0 \\ a_3 \\ a_4 \end{bmatrix}_{4\times 1} = \begin{bmatrix} h_{11} & h_{12} \\ h_{21} & h_{22} \\ h_{31} & h_{32} \\ h_{41} & h_{42} \end{bmatrix}_{4\times 2} \begin{bmatrix} c_1 \\ c_2 \end{bmatrix}_{2\times 1}$$

False Data Injection Attacks: Protected Sensors

- Case 1: Targeted Attack
  - The attacker intends to inject particular c_1 and c_2 .

- Example: What if c_1 = 4 and c_2 = -1?

$$\begin{bmatrix} a_1 \\ 0 \\ a_3 \\ a_4 \end{bmatrix}_{4\times 1} = \begin{bmatrix} 3 & 2 \\ 1 & 4 \\ 2 & 1 \\ 5 & 3 \end{bmatrix}_{4\times 2} \begin{bmatrix} 4 \\ -1 \end{bmatrix}_{2\times 1}$$

False Data Injection Attacks: Protected Sensors

- Case 1: Targeted Attack
  - The attacker intends to inject particular c_1 and c_2 .

- Example: What if c_1 = 3 and c_2 = -1?

$$\begin{bmatrix} a_1 \\ 0 \\ a_3 \\ a_4 \end{bmatrix}_{4\times 1} = \begin{bmatrix} 3 & 2 \\ 1 & 4 \\ 2 & 1 \\ 5 & 3 \end{bmatrix}_{4\times 2} \begin{bmatrix} 3 \\ -1 \end{bmatrix}_{2\times 1}$$

False Data Injection Attacks: Protected Sensors

- Case 1: Targeted Attack
  - The attacker intends to inject particular c_1 and c_2 .

- General Approach:
  - Evaluate ***H c*** to see if the rows for protected sensors is zero.
    - If they are zero: simply use the resulted a_i values.
    - Otherwise, the attack is not possible!

False Data Injection Attacks: Protected Sensors

- Case 2: Random Attack
  - The attacker intends to inject any $c_1 \neq 0$ and $c_2 \neq 0$.
  - As long as the attack is not detected.

- Key Question:
  - Given $a_i = 0$ for all protected sensors:
    - Can we find any $c_1 \neq 0$ and $c_2 \neq 0$ such that $\boldsymbol{a} = \boldsymbol{H}\,\boldsymbol{c}$?

False Data Injection Attacks: Protected Sensors

- Case 2: Random Attack
  - The attacker intends to inject any $c_1 \neq 0$ and $c_2 \neq 0$.

- Example: Sensor 2 is protected:

$$\begin{bmatrix} a_1 \\ 0 \\ a_3 \\ a_4 \end{bmatrix}_{4\times 1} = \begin{bmatrix} 3 & 2 \\ 1 & 4 \\ 2 & 1 \\ 5 & 3 \end{bmatrix}_{4\times 2} \begin{bmatrix} c_1 \\ c_2 \end{bmatrix}_{2\times 1}$$

False Data Injection Attacks: Protected Sensors

- Case 2: Random Attack
  - The attacker intends to inject any $c_1 \neq 0$ and $c_2 \neq 0$.
- Example: Sensor 2 is protected:
  - Clearly any point (c_1, c_2) on line $c_1 + 4\,c_2 = 0$ would work.
  - Q: Can you show this on a c_1 / c_2 space?

False Data Injection Attacks: Protected Sensors

- Case 2: Random Attack
  - The attacker intends to inject any $c_1 \neq 0$ and $c_2 \neq 0$.

- Example: Sensors 2 and 4 are protected:

$$\begin{bmatrix} a_1 \\ 0 \\ a_3 \\ 0 \end{bmatrix}_{4\times 1} = \begin{bmatrix} 3 & 2 \\ 1 & 4 \\ 2 & 1 \\ 5 & 3 \end{bmatrix}_{4\times 2} \begin{bmatrix} c_1 \\ c_2 \end{bmatrix}_{2\times 1}$$

False Data Injection Attacks: Protected Sensors

- Case 2: Random Attack
  - The attacker intends to inject any $c_1 \neq 0$ and $c_2 \neq 0$.
- Example: Sensors 2 and 4 are protected:
  - Q: Can you show this on a c_1 / c_2 space?
  - Q: Is the attack even possible? What is the problem?

False Data Injection Attacks: Protected Sensors

- Case 2: Random Attack
  - The attacker intends to inject any $c_1 \neq 0$ and $c_2 \neq 0$.

- **Theorem [Liu, et al.]**:

> If the attacker can compromise k specific meters, where $k \geq m - n + 1$, there always exist attack vectors $\boldsymbol{a} = \boldsymbol{H}\,\boldsymbol{c}$ such that $\boldsymbol{c} \neq \boldsymbol{0}$, $\boldsymbol{a} \neq \boldsymbol{0}$, and for all protected sensors, we have $a_i = 0$.

Q: Can this explain the results in the previous example?

False Data Injection Attacks: Verifiable States

- Q: What if some state variables can be verified independently?
  - For some $j \in \{1, \ldots, n\}$, it is required that $c_j = 0$.
  - Otherwise, operator will detect the attack! (Q: Why?)
    - The detection will be different from residue test.

- Q: How can the operator independently verify some states?

False Data Injection Attacks: Verifiable States

- Q: What if some state variables can be verified independently?
  - For some $j \in \{1, \ldots, n\}$, it is required that $c_j = 0$.

- Example: State 1 can be verified independently:

$$\begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \end{bmatrix}_{4\times 1} = \begin{bmatrix} h_{11} & h_{12} \\ h_{21} & h_{22} \\ h_{31} & h_{32} \\ h_{41} & h_{42} \end{bmatrix}_{4\times 2} \begin{bmatrix} 0 \\ c_2 \end{bmatrix}_{2\times 1}$$

False Data Injection Attacks: Verifiable States

- Q: What if some state variables can be verified independently?
  - For some $j \in \{1, \ldots, n\}$, it is required that $c_j = 0$.
- Example: State 1 can be verified independently:
  - It is very similar to a targeted attack: $c_1 = 0$.
  - The attack is always feasible if no sensor is protected.
    - Q: Why?

False Data Injection Attacks: Combined Scenario

- Q: What if both cases happen at the same time:
  - For some $i \in \{1, \ldots, m\}$, it is required that $a_i = 0$.
  - For some $j \in \{1, \ldots, n\}$, it is required that $c_i = 0$.
- Example: State 1 can be verified and sensor 2 is protected:

$$\begin{bmatrix} a_1 \\ 0 \\ a_3 \\ a_4 \end{bmatrix}_{4\times 1} = \begin{bmatrix} h_{11} & h_{12} \\ h_{21} & h_{22} \\ h_{31} & h_{32} \\ h_{41} & h_{42} \end{bmatrix}_{4\times 2} \begin{bmatrix} 0 \\ c_2 \end{bmatrix}_{2\times 1}$$

False Data Injection Attacks: Combined Scenario

- Again, it will be a feasibility problem.
  - We can always analyze and see if the attack is feasible.

- Q: What if the attack is not feasible the way that we discussed?
  - Would the attacker give up?
  - What can the attacker do if "perfect" attack is not feasible?

False Data Injection Attacks: Combined Scenario

- Recall that in general, the attacker is interested in

  - Maximizing State Estimation Error:

$$\underset{\mathrm{a}}{\text{maximize}} \ \left\| \hat{x}_{bad} - \hat{x} \right\|$$

  - Minimizing the Chance of Being Detected:

$$\underset{\mathrm{a}}{\text{minimize}} \ \left\| r_a - r \right\|$$

False Data Injection Attacks: Combined Scenario

- For perfect attack:
  - State estimation error will be infinity.
  - The difference between new and old residue will be zero.
    - Minimum expected chance of attack being detected.

- Q: Can you formulate these problems for “imperfect” attacks?

- The attacker may also look at the “damage level” of the attack.

Impact on Electricity Market

- Q: Is it possible for an electricity market participant
  - To financially benefit from implementing an FDIA?

- Key idea:
  - State estimation results have impact on LMP:
    - LMP: Locational Marginal Price
    - LMP is used in various electricity market transactions.

Impact on Electricity Market

- LMP: Cost to serve the next MW of load (i.e., increasing the load) at a specific location, using the lowest production cost of all available generators, while observing all transmission limits.

- The line congestion information particularly affects LMP.
  - State estimation is used to evaluate congestion.
    - Phase angle difference between two sides of link.

- An FDIA can increase or decrease LMP($[\Theta_1,\ldots, \Theta_n]$).

Impact on Electricity Market

- Generators sell electricity at LMP.
  - They rather change $[\Theta_1,\ldots, \Theta_n]$ to increase LMP($[\Theta_1,\ldots, \Theta_n]$).
- Loads/utilities buy electricity at LMP.
  - They rather change $[\Theta_1,\ldots, \Theta_n]$ to decrease LMP($[\Theta_1,\ldots, \Theta_n]$).
- You can find more details about this problem in Xie, et al.

References

- B. J. Murrill, E. C. Liu, R. M. Thompson, “Smart Meter Data: Privacy and Cybersecurity”, Congressional Research Service, CRS Report for Congress, 7-5700, R42338, February 2012.

- National Institute of Standards and Technology, "Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid", The Smart Grid Interoperability Panel – Cyber Security Working Group, NISTIR 7628, August 2010.

- G. Kalogridis, C. Efthymiou, S.Z. Denic, T.A. Lewis, and R. Cepeda, "Privacy for Smart Meters: Towards Undetectable Appliance Load Signatures", in Proc. of the IEEE International Conference on Smart Grid Communications, Gaithersburg, MD, Oct. 2010.

References

- H. Mohsenian-Rad and A. Leon-Garcia, “Distributed Internet-based Load Altering Attacks against Smart Power Grids,” *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 667-674, Dec 2011.

- Y. Liu, P. Ning, M. K. Reiter, “False Data Injection Attacks against State Estimation on Electric Power Grids,” *ACM Conference on Computer and Communications Security* (CCS '09) , Chicago, IL, November 2009.

- R. B. Bobba, K. M. Rogers, Q. Wang, H. Khurana, K. Nahrstedt, T.J. Overbye, “Detecting False Data Injection Attacks on DC State Estimation,” in *Proc. First Workshop on Secure Control Systems*, (CPSWeek), Stockholm Sweden, April, 2010.

References

- O. Kosut, J. Liyan, R. J. Thomas, L. Tong, "Malicious Data Attacks on Smart Grid State Estimation: Attack Strategies and Countermeasures," in *Proc. IEEE International Conference on Smart Grid Communications*, Gaithersburg, MD, October 2010.

- G. Dàn and H. Sandberg, "Stealth Attacks and Protection Schemes for State Estimators in Power Systems," in *Proc. IEEE International Conference on Smart Grid Communications*, Gaithersburg, MD, October 2010.

- L. Xie, Y. Mo, and B. Sinopoli, "False Data Injection Attacks in Electricity Markets,“ in *Proc. IEEE International Conference on Smart Grid Communications*, Gaithersburg, MD, October 2010.