Redundant Metering for Integrity with Information-Theoretic Confidentiality

D.P. Varodayan and G.X. Gao

Presenter: Abdallah Farraj

Submitted in Partial Fulfillment of the Course Requirements for
ECEN 689: Cyber Security of the Smart Grid
Instructor: Dr. Deepa Kundur

Paper Information

- Title: Redundant Metering for Integrity with Information-Theoretic Confidentiality
- Authors: David Varodayan (HP Labs) and Grace Xingxin Gao (Stanford University)
- Conference: IEEE International Conference on Smart Grid Communications, SGC 2010, Gaithersburg, Maryland, October 2010

Presentation Overview

- Introduction
- Historical Background
- Redundant Metering
- Proposed Solution
- Case Study
- Critical Review
- Summary

Introduction

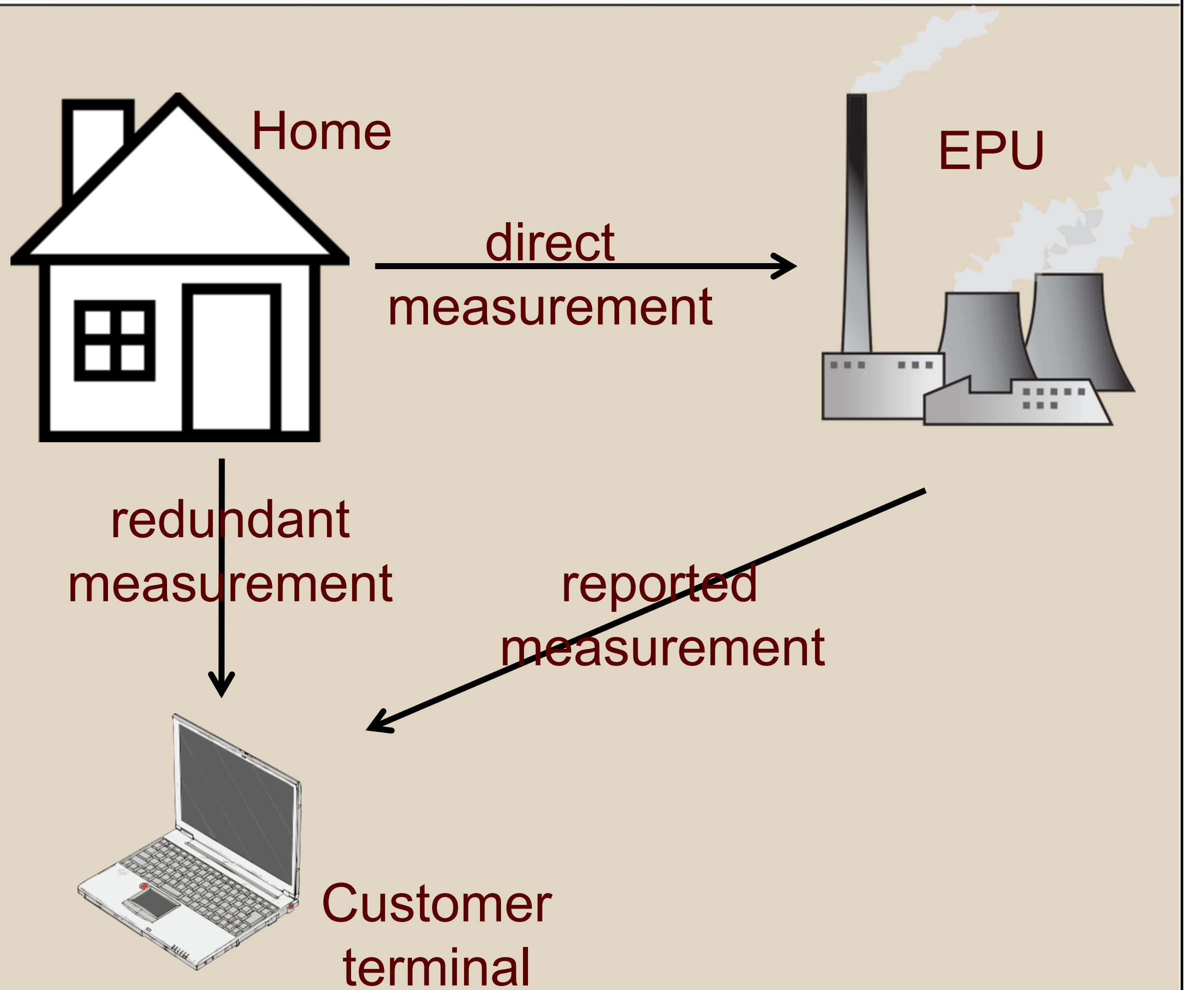
- Advanced Metering Infrastructure:
  - Time-of-use pricing
  - Demand response
- Billing challenges:
  - Integrity
  - Confidentiality

Historical Background

- Integrity of smart meters is a concern
- Lack of confidence leads to clash
- Pacific Gas & Electricity (PG&E) case
  - Customers complained being overcharged
  - Some billing errors were found due to improper installations or faulty equipment
  - Ongoing lawsuits and political pressure
  - Customers verify billing independently

Redundant Metering

- Customer makes an Independent measurement
- Receives EPU reading
- Compares the two readings for integrity



Confidentiality Risk

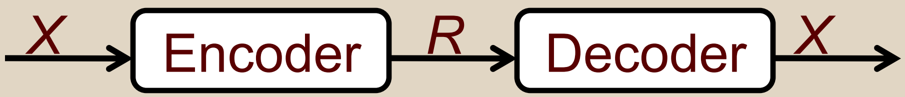
- Eavesdropper can hack the redundant measurement wireless link
- Can tell whether the house is occupied, and what appliances are in use
- Safety and theft consequences
- Need an information-theoretic solution
- Information is secure regardless of computational power of the eavesdropper

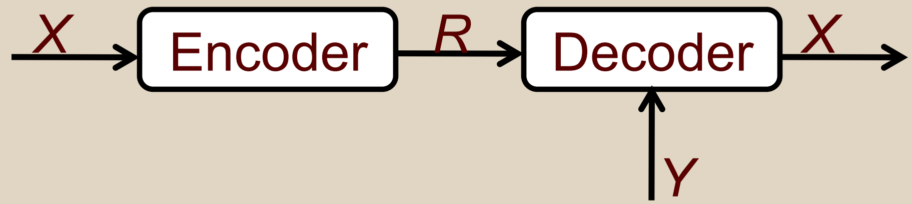
Information-Theoretic Confidentiality Solution

TEXAS A&M UNIVERSITY

- Compress redundant data to a rate below its entropy
- Eavesdropper cannot decode this data
- Using reported data, redundant data can be recovered at customer terminal
- Confidentiality guaranteed regardless of computational capability of eavesdropper

Information Theory Background





- Shannon Theorem:

$$R \geq H(X)$$

Lossless recovery at decoder is possible

$$R < H(X)$$

recovery at decoder is NOT possible

- Slepian & Wolf Thm.:

$$H(X) \geq R \geq H(X/Y)$$

Lossless recovery at decoder is possible

X: **Redundant Reading**
Y: **EPU Reported Reading**
H(X): **Entropy of X**
H(X/Y): **Conditional Entropy**
R: **Compression Rate**

Proposed Solution

- If X and Y are statistically dependent:
  - Encode X at rate R such that

$$H(X/Y) < R < H(X)$$

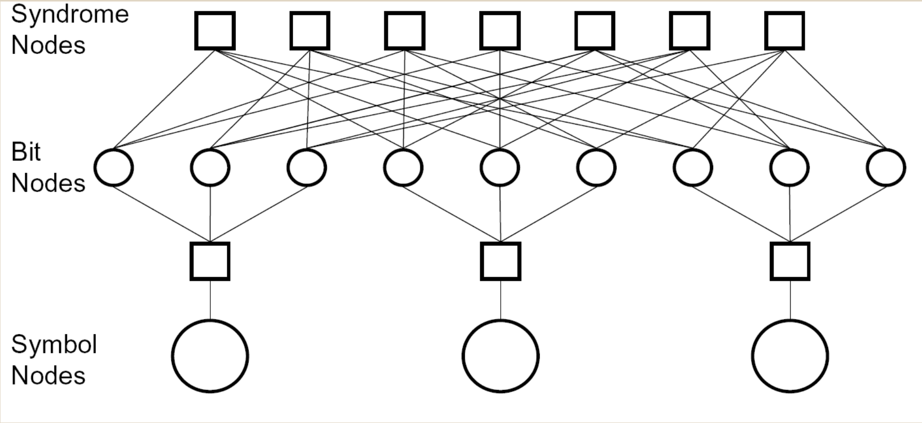
  - Eavesdropper receiving data at rate R cannot decode X
  - Customer terminal, with the presence of Y, can decode X

Proposed Solution

- If *X* and *Y* are significantly different:
  - Coding rate *R* is insufficient for the decoder to recover *X*
  - Decoding failure
  - Integrity of EPU measurement is suspect
- Solution checks for meter measurement integrity while saving data confidentiality

Practical Coding Scheme

- Using Gray code, map symbols into bits *X*
- Compute syndrome bits *S*
- Transmit *S* instead of *X*
- Compression rate *R* is ratio of numb. of syndrome nodes to numb. of bit nodes



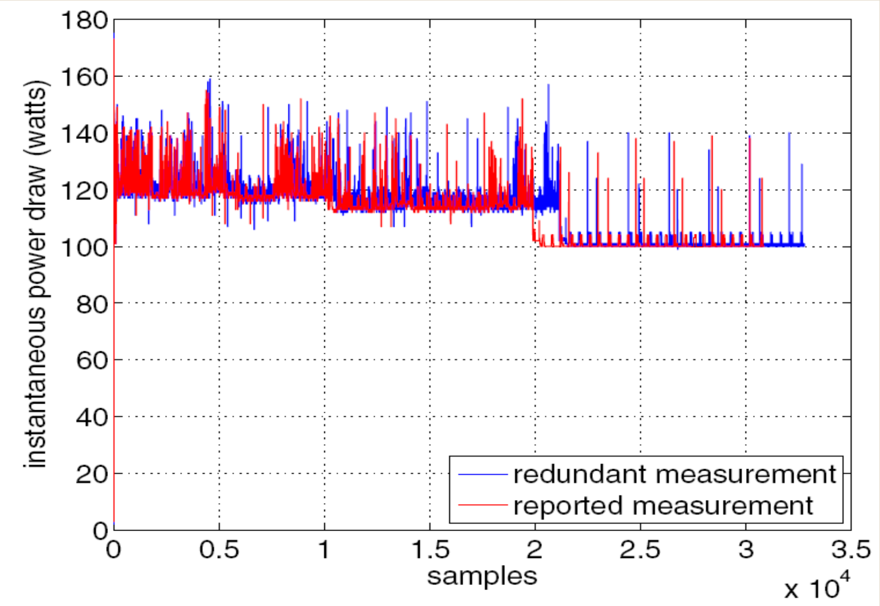
from D. Varodayan and G. Gao, “Redundant Metering for Integrity with Information-Theoretic Confidentiality”

Practical Coding Scheme

- Decoder seeks to recover X from S
- With the presence of Y, the decoder:
  - Seeds the symbol nodes with probability mass function (PMF) of X given Y
  - Runs an iterative sum-product algorithm until convergence is achieved
  - Estimates the corresponding symbol values

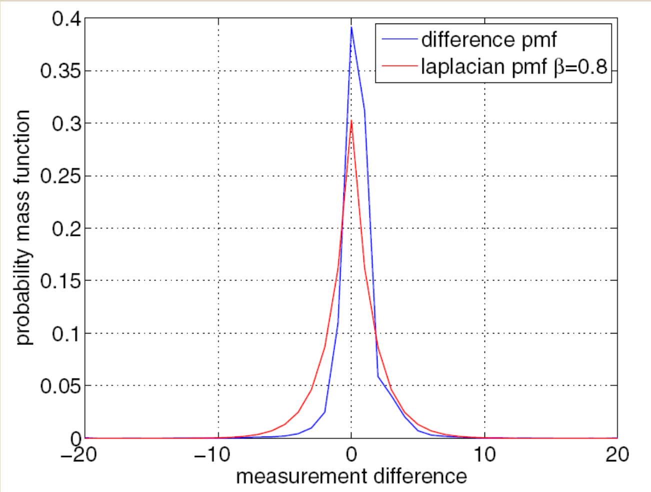
Stanford PowerNet Case Study

- Two asynchronous meters readings
- 30872 reported (32768 redundant) samples
- Resample the readings to synchronize
- Find the difference PMF
- Divide data into blocks
- Use variable-rate LDPC to encode the blocks

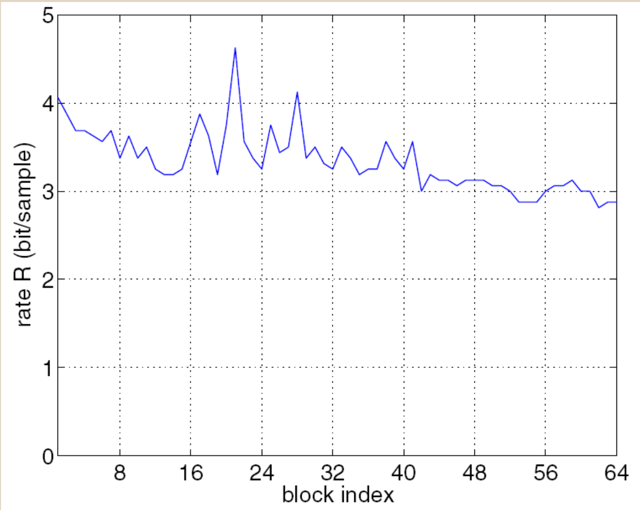


from D. Varodayan and G. Gao, “Redundant Metering for Integrity with Information-Theoretic Confidentiality”

Stanford PowerNet Case Study



from D. Varodayan and G. Gao, "Redundant Metering for Integrity with Information-Theoretic Confidentiality"



- Feed the decoder with a Laplace PMF ($\beta = 0.8$)
- Run the iterative sum-product algorithm
- Estimate the symbols

- Variable compression rate is below the raw bit rate (8 bits/sample)
- Eavesdropper cannot decode data

Critical Review

- Effect of memory in the redundant measurement is ignored
  - Lower coding rate *R*
- If X and Y are significantly uncalibrated, proposed algorithm may not work well
  - – Need calibration data at decoder
- Both *X* and *Y* need to be synchronous (or have time stamp)

Critical Review

- Eavesdropper ability to access the Y signal might change the whole game
- PMF estimation (and adaptive rate R) might be practically challenging
- Channel noise and imperfections were not considered

Summary

- Customers use redundant meters to check the integrity of EPU smart meters
- Redundant and reported readings are relayed to a customer terminal
- Eavesdropper might access the signal of the redundant meter
- Information-theoretic solution is proposed

TEXAS A&M UNIVERSITY

Summary

- Compress the redundant reading below its entropy
- Redundant data cannot be recovered from just its encoded bits (data secured)
- With the presence of EPU reading, the redundant reading can be recovered
- Secure solution regardless of the eavesdropper computation power

References

- D. Varodayan and G. X. Gao, Redundant Metering for Integrity with Information-Theoretic Confidentiality, *IEEE International Conference on Smart Grid Communications,* Gaithersburg, Maryland, October 2010
- Greentech Media, "PG&E Sued Over Smart Meters, Slows Down Bakersfield Deployment," GreenTechMedia Nov11, 2009 http://www.greentechmedia.com/articles/read/pge-sued-over-smart-meters-slows-down-bakersfield-deployment
- A. Liveris, Z. Xiong, and C. Georghiades, "Compression of binary sources with side information at the decoder using LDPC codes," *IEEE Commun. Lett., vol. 6, no. 10, pp. 440–442, Oct. 2002*
- D. Varodayan, D. Chen, M. Flierl, and B. Girod, "Wyner-Ziv coding of video with unsupervised motion vector learning," *EURASIP Signal Process.: Image Commun. J, vol. 23, no. 5, pp. 369–378, Jun.* 2008