Communication Capacity Requirement for Reliable and Secure State Estimation in Smart Grid

Authors: Husheng Li, Lifeng Lai, and Robert Qiu

Presenter: Mustafa El-Halabi

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

Main Objective

Establishing fundamentals limits (information-theoretic limits) for secure transmission of State Estimation in the Smart Grid

Outline

1. Confidentiality Techniques
2. Mathematical Background
3. Information-theoretic Security
4. Smart Grid Dynamic Model
5. Security Metric for Smart Grid Dynamic Model
6. Fundamental Limits for Secure Communications
7. Concluding Remarks

Smart Grid :

- Wireless links prone to eavesdropping attacks
  1. active eavesdropping
  2. passive eavesdropping

Smart Grid :

- Wireless links prone to eavesdropping attacks
  1. active eavesdropping
  2. passive eavesdropping
- Security issues:
  - Confidentiality
  - Integrity
  - Authentication
  - Nonrepudiation

Confidentiality techniques

- Cryptography: Private-key / Public-key cryptosystems

Confidentiality techniques

- Cryptography: Private-key / Public-key cryptosystems
- Information-theoretic security

Mathematical Background

- Entropy
  - A measure of uncertainty associated with a random variable
  - Entropy of a discrete r.v. X with values $\{x_1, ..., x_n\}$:

$$H(X) = -\sum_{i=1}^{n} p(x_i) \log p(x_i)$$

  - Entropy of a fair coin $= 1$ bit, entropy of a biased-$(1/3, 2/3)$ coin $= 0.81$ bits

Mathematical Background

- Entropy
  - A measure of uncertainty associated with a random variable
  - Entropy of a discrete r.v. X with values $\{x_1, ..., x_n\}$:

$$H(X) = -\sum_{i=1}^{n} p(x_i) \log p(x_i)$$

  - Entropy of a fair coin $= 1$ bit, entropy of a biased-$(1/3, 2/3)$ coin $= 0.81$ bits
- Conditional entropy (Equivocation)
  - A measure of the remaining uncertainty of a r.v. Y given that the value of X is known
  - Conditional entropy of Y given X:

$$H(Y|X) = -\sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} p(x, y) \log p(y|x)$$

Mathematical Background

- Mutual Information
  - A measure of how much knowing one r.v. reduces our uncertainty about another r.v.
  - $I(X;Y) = H(Y) - H(Y|X)$

Mathematical Background

- Mutual Information
  - A measure of how much knowing one r.v. reduces our uncertainty about another r.v.
  - $I(X;Y) = H(Y) - H(Y|X)$
- Channel Capacity

  - Rate (bits/s) of reliable transmission $= I(X;Y)$
  - Channel Capacity

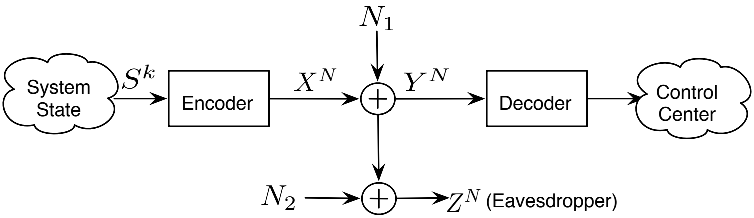
$$C = \max_{p(x)} I(X;Y)$$

Information-Theoretic Security for the Smart Grid

Goal:

Establish fundamental limits on the rate (bit/s) at which *secure* and *reliable* system state estimation in a smart grid could be communicated (Secrecy Capacity)

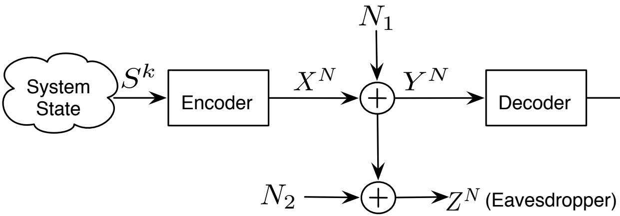
A Smart Grid System Model



$$
\begin{aligned}
Y &= X + N_1 \\
Z &= X + N_1 + N_2
\end{aligned}
$$

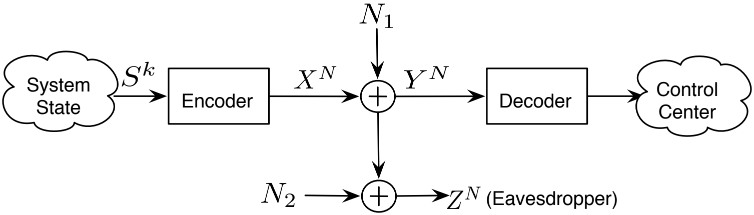
$$E[|X|^2] \leq P,\ N_1 \sim \mathcal{N}(0, \sigma_1^2),\ N_2 \sim \mathcal{N}(0, \sigma_2^2)$$

Security Metric: Normalized Equivocation



$$\begin{aligned}\Delta &= \frac{H(S^k|Z^N)}{H(S^k)} \\ &= \textit{residual uncertainty about the message at the eavesdropper} \\ &= \begin{cases} 0 & \textit{no secrecy} \\ 1 & \textit{perfect secrecy} \end{cases}\end{aligned}$$

Secrecy Capacity of the Gaussian Wiretap Channel



- Information source S is ergodic and belongs to finite-length alphabet:
  Secrecy Capacity

$$C_s = \frac{1}{2}\log\left(1+\frac{P}{\sigma_1^2}\right) - \frac{1}{2}\log\left(1+\frac{P}{\sigma_2^2+\sigma_1^2}\right)$$

Smart Grid Security Meter

Normalized equivocation Δ needs to be modified:

1. SG is a dynamic system, information might not be ergodic
2. Source alphabet in SG is continuous

Fundamental limits need to be revisited in the context of SG !

Dynamics of a SG

$$\mathbf{x}(t+1) = F\left(\mathbf{x}(t), w(t)\right)$$

$$\begin{aligned} \mathbf{x}(t) &= \textit{state vector at time slot } t \\ w(t) &= \textit{random factor} \\ F &= \textit{map previous state to next state} \end{aligned}$$

Redefining "Equivocation" for the SG

$$\Delta = \frac{H(S^k|Z^N)}{H(S^k)} = \frac{?}{?}$$

Tools:

1. Topological Entropy
2. Spanning Set

Topological Entropy

$$\mathbf{x}(t+1) = F\left(\mathbf{x}(t), w(t)\right)$$

Definition: Topological Entropy

$$H(F, \mathcal{X}) = \lim_{\epsilon \to 0} \lim_{k \to \infty} \frac{1}{k} \log q(k, \epsilon)$$

$H(F, \mathcal{X})$ is the uncertainty of the dynamic system
$\log q(k, \epsilon)$ is the number of bits to describe an approximation (ϵ) of system's dynamic behavior during time slot k.

Spanning Set

$$\mathbf{x}(t+1) = F\left(\mathbf{x}(t), w(t)\right)$$

Let $\mathcal{X}_k$ = set of all possible $\{\mathbf{x}_1, ..., \mathbf{x}_k\}$

Definition: (k, ϵ)-Spanning Set

For $k > 0, \epsilon > 0$, a finite set $Q \subset \mathcal{X}_k$ is (k, ϵ)-spanning set if, for any $\mathbf{x} \in \mathcal{X}_k$, we can always find an $\hat{\mathbf{x}} \in Q$, s.t.
$\| \mathbf{x}(t) - \hat{\mathbf{x}}(t) \|_\infty < \epsilon$, $t = 1, ..., k$.

Revisiting Equivocation Δ

- For ergodic finite-length alphabet source: $\Delta = \frac{H(S^k|Z^N)}{H(S^k)}$
- Using topological entropy: $H(S^k) \to H(F, \mathcal{X})$
- Using (k, ϵ)-Spanning Set: $H(S^k|Z^N) \to H(F, \mathcal{X}|Z)$

For a SG dynamic system: $\Delta = \frac{H(F,\mathcal{X}|Z)}{H(F,\mathcal{X})}$

Reliable & Secure Communication: Definitions

Secure System

If communication between sensor and controller satisfies $\Delta = 1$, the communication is secure.

Secure Communication Requirement for the Smart Grid

Main results:

- If $H(F, \mathcal{X}) \leq C_1 - C_2$, reliable and secure communication is guaranteed.
- If $C_1 - C_2 < H(F, \mathcal{X}) \leq C_1$, only reliable communication is guaranteed.
- If $H(F, \mathcal{X}) > C_1$, neither reliable communication nor security is guaranteed.

where, $C_1 = \frac{1}{2} \log \left(1 + \frac{P}{\sigma_1^2}\right)$, $C_2 = \frac{1}{2} \log \left(1 + \frac{P}{\sigma_2^2 + \sigma_1^2}\right)$

Assessment

- First Information-theoretic approach to smart grid security
- The Fundamental limits for secure communication in a smart grid environment build foundation for more precise problems, with answers that could provide important insights into the nature of secret communication
- The insights may be used to shape development of practical systems for encryption in complex settings
- The model considered is far simpler than the practical case
- A multiuser setting needs to be investigated

References

- Y. Liang, S. K. Yan-Cheong, and M. Hellman, "The Gaussian Wiretap Channel," *IEEE Trans. Inform. Theory*, vol. 24, pp. 451–456, July 1978.
- Y. Liang, A. S. Matveev, and A. V. Savkin, "Estimation and Control Over Communication Networks," Birkhauser, 2009.
- C. E. Shannon, "Communication theory of secrecy systems," *Bell Systems Technical Journal*, vol. 28, pp. 656–715, Oct. 1949.
- Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Information Theoretic Security," *Foundations and Trends in Communications and Information Theory*, vol. 5, nos. 4-5, pp. 355–580, Now Publishers, Hanover, MA, USA, 2008.