Detection of False Data Injection Attacks in Smart Grid Communication Systems

Danda B. Rawat and Chandra Bajracharya

Department of Electrical Engineering

IEEE GlobalSIP 2015

December 14 - 16, 2015

Outline

- Overview
- System Model
- Problem Statement
- Proposed Approach
- Performance Evaluation
- Conclusions

Overview

A *smart grid* is a modernized electrical grid that uses information and communication technology to gather and act on information in an automated fashion to improve the overall performance of power system.

Source: The NIST conceptual model for smart grid

Motivation

- Communication networks in smart grid
  - Revolutionize the energy industry in terms of reliability. performance, and manageability.
  - Bring increased connectivity
    - Results in severe security vulnerabilities and challenges in the grid.
- According to *Ernest Orlando Lawrence Berkeley National Lab* report, power outages cost over $80 billion every year in the U.S. alone*.
- Thus, due to the critical nature of the smart grid services, smart grid become a prime target for *cyber attacks*.

*Source: http://certs.lbl.gov/pdf/55718.pdf

Motivation: Features of Smart Grid

- Low Latency Requirements (< 3 ms)
- Bi-directional Communications
- Auytomated Password/PIN update process
- Layered network architecture

Cyber attack detection and defense solution should be quick, resilient and reconfigurable so as to have uninterrupted power supply while complying CIA triad.

State Space Model

- The received SCADA measurements can be represented in a compact vector-matrix from as

$$\mathbf{z} = \mathbf{H}\mathbf{x} + \mathbf{n}$$

H : Measurement Jacobian matrix,
x : Vector containing state variables
n : Measurement noise

- State vector estimator can give us [8]

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

- After attack, SCADA measurement can be represented as

$$\mathbf{z} = \mathbf{H}\mathbf{x} + \mathbf{n} + \mathbf{a}$$

a : false data vector inserted by an attacker

Attack Model

- DoS attack
  - Attacker floods packets in the network to jam legitimate services.
- Random attack
  - Attacker simply manipulates the sensor readings by inserting a random attack vector.
- False data injection attack
  - Attacker is assumed to be familiar to the system and its parameters used in estimation and detection.

State Space Model

- Attack is detected if

$$\|\mathbf{z} - \mathbf{H}\hat{\mathbf{x}}\|_2^2 > \lambda$$

λ : Threshold

- This approach has problems as the Jacobian matrix **H** in smart grid is very sparse, and attackers can insert false data and by pass the above test to attack the smart grid when **a = Hz**.

Objectives and Proposed Approach

- Objectives
  - To detect false data injection attacks in smart grid systems.
  - To investigate Chi-square detector and cosine similarity matching approaches.
- Proposed Approach
  - Use Chi-square detector and cosine similarity matching approaches for attack detection in smart grid where Kalman filter estimation is used to measure any deviation from actual measurements.
  - Compare the performance of Chi-square detector and cosine similarity matching approaches.

Proposed Approach

- Error (difference between estimated value and the actual measurements) can be estimated as

$$\mathbf{e}_n = \check{\mathbf{x}}_n^+ - \mathbf{x}_n$$

Error

State estimation update (*a posteriori* estimate) using Kalman Filter

Actual measurement

Proposed Approach

- The deviation in expected/estimated value (by Kalman Filter) and measured value (by sensor measurements)

$$\mathbf{f}_n = \mathbf{z}_n - \check{\mathbf{z}}_n = \mathbf{z} - \mathbf{H}\mathbf{x}_n^+$$

Actual measurement

Expected/estimated value

Proposed Approach

- Residue can be calculated as

$$R_{Chi-square} = \mathbf{f}_n^T \mathbf{F}_n \mathbf{f}_n$$

- Compare $R_{Chi\text{-}square}$ against a given threshold.

Proposed Approach

- Cosine similarity matching between expected/estimated value (by Kalman Filter) and measured value (by sensor measurements) can be used as

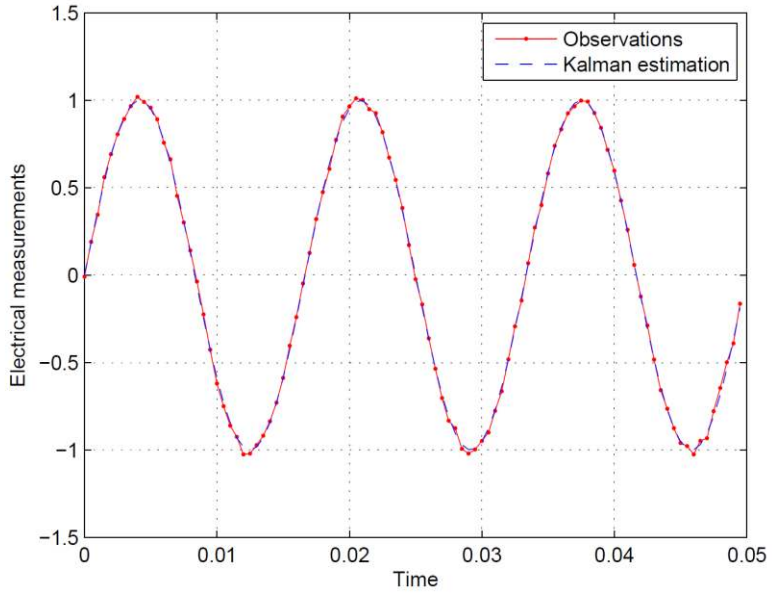
$$R_{cos-sim} = 1 - sim(\check{\mathbf{x}}, \hat{\mathbf{x}}) = 1 - \frac{\overrightarrow{v}(\check{\mathbf{x}}).\overrightarrow{v}(\hat{\mathbf{x}})}{||\overrightarrow{v}(\check{\mathbf{x}})|| \times ||\overrightarrow{v}(\hat{\mathbf{x}})||}$$

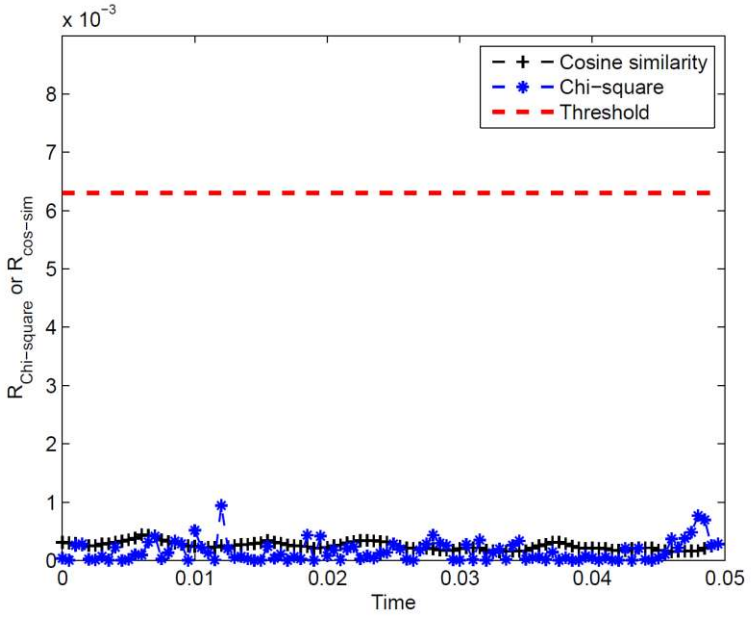
- Compare $R_{cos\text{-}sim}$ against a given threshold.

Simulation Scenario

- Sinusoidal signal with
  - frequency 60 Hz.
  - amplitude 1 Volt.
  - Sampling frequency 2000 Hz.
  - initial covariance matrix $\mathbf{P}_{n-1}^{+} = \mathbf{I}$.
- Additive Gaussian white noise with zero mean.

Performance Evaluation



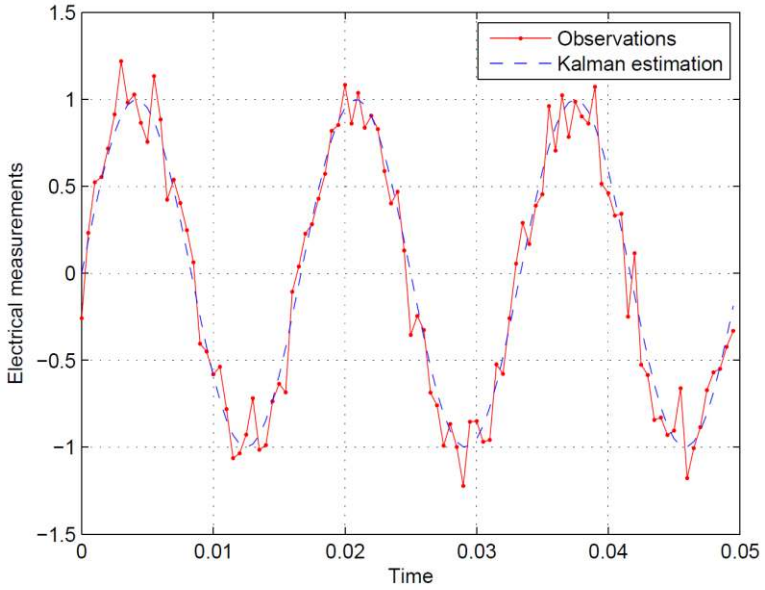


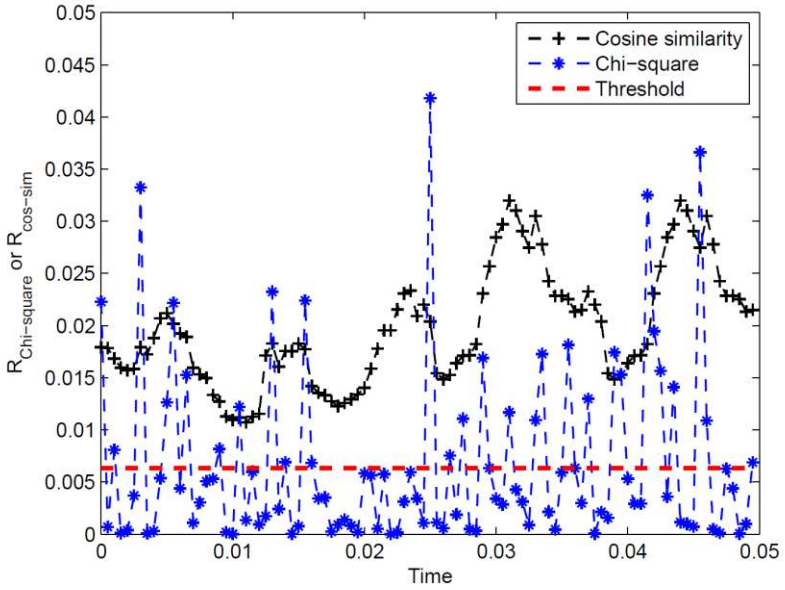
(a) Measured voltage signal and Kalman Filter estimation.

(b) Detectors' outputs along with threshold.

Variation of electrical measurements and Kalman filter estimations vs. the time when there were no attacks.

Performance Evaluation



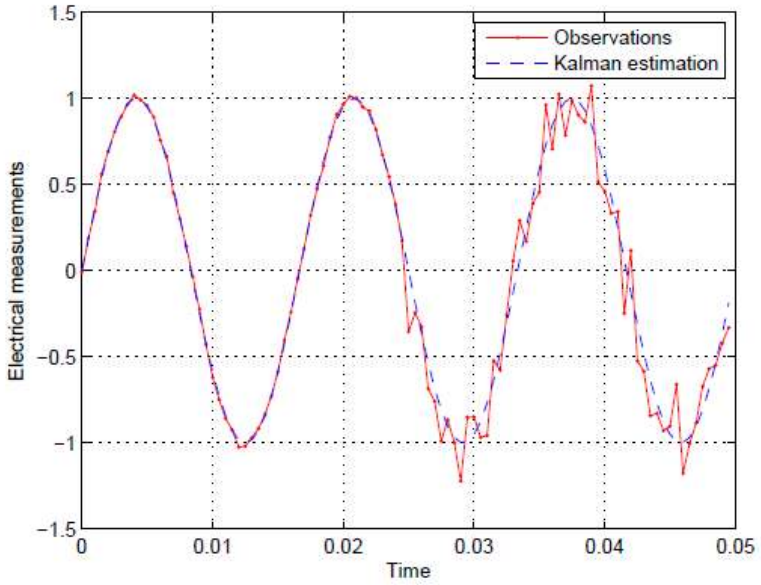


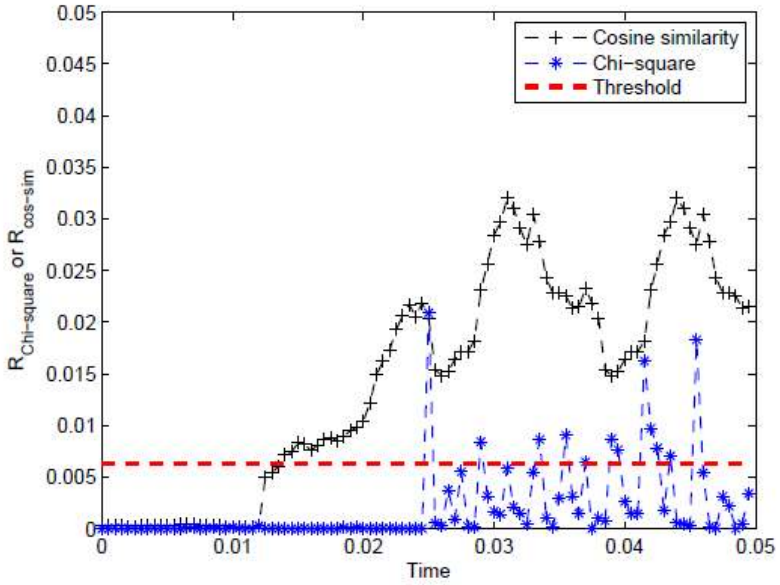
(a) Measured voltage signal and Kalman Filter estimation.

(b) Detectors' outputs along with threshold.

Variation of electrical measurements and Kalman filter estimations vs. the time when there were random attacks.

Performance Evaluation



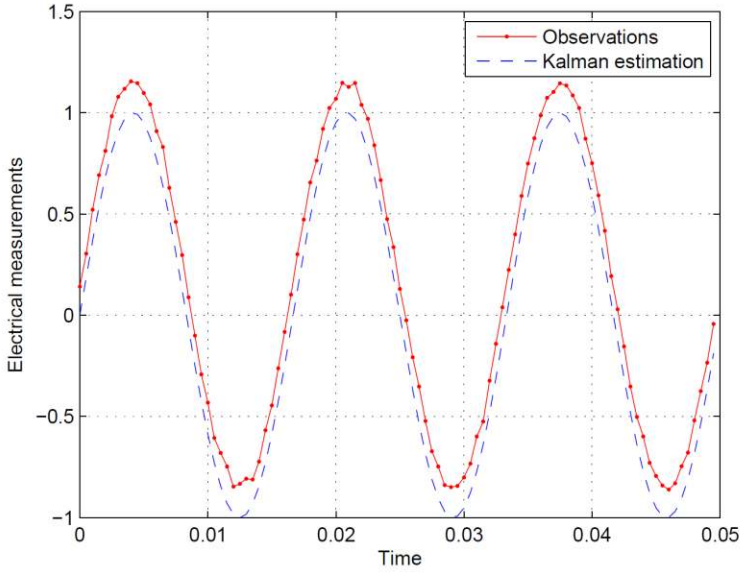


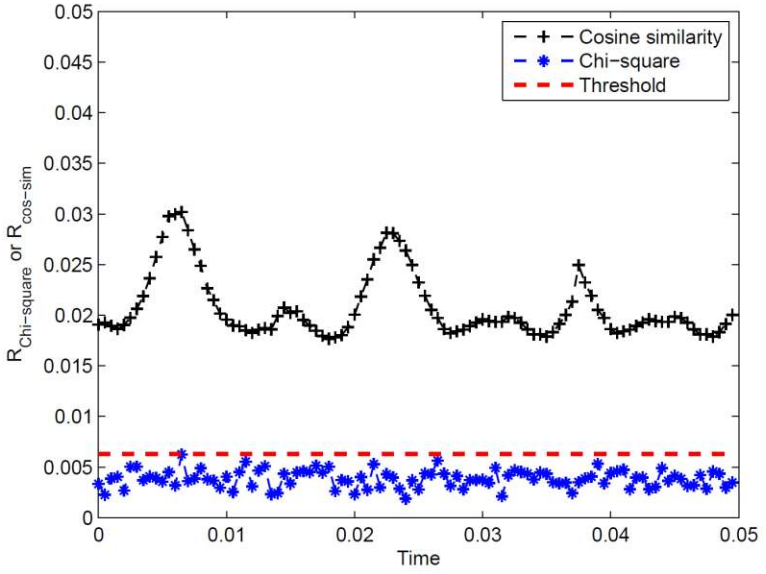
(a) Measured voltage signal and Kalman Filter estimation.

(b) Detectors' outputs along with threshold.

Variation of electrical measurements and Kalman filter estimations vs. the time when there was random attack in the second half of the observation period.

Performance Evaluation



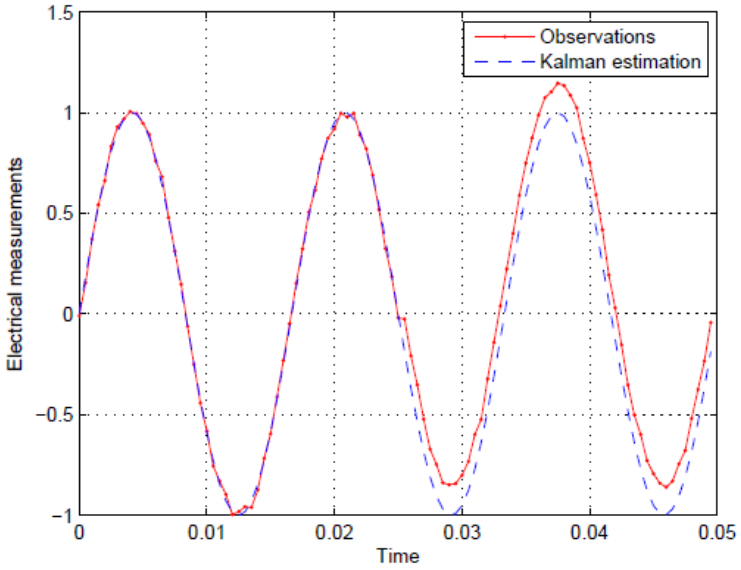


(a) Measured voltage signal and Kalman Filter estimation.

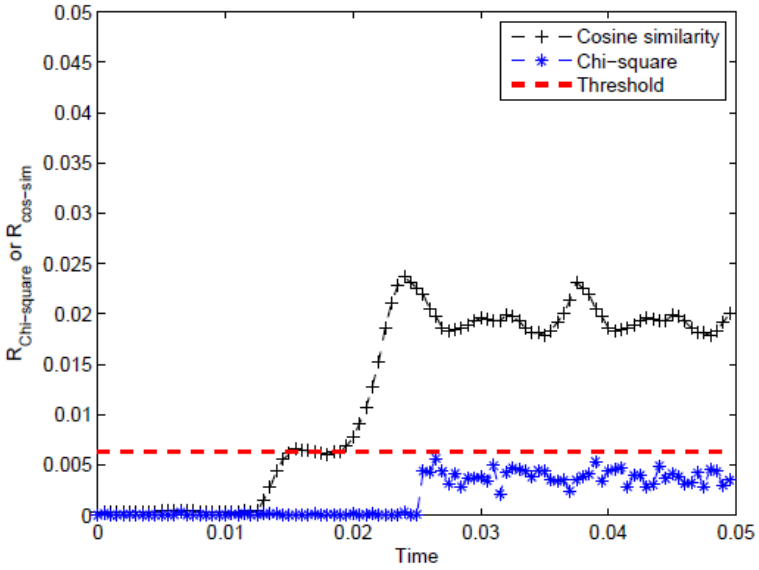
(b) Detectors' outputs along with threshold.

Variation of electrical measurements and Kalman filter estimations vs. the time when there were false data injection attacks.

Performance Evaluation



(a) Measured voltage signal and Kalman Filter estimation.



(b) Cosine similarity and Chi-square detector outputs using Kalman Filter against threshold.

Variation of electrical measurements and Kalman filter estimations vs. the time when there were false data injection attacks after about half observation period.

Conclusions

- We have presented Chi-square detector and cosine similarity matching approaches to detect false data injection attacks in smart grids
- We have used Kalman filter estimation to find expected measurements which are used to measure any deviation between actual measurements and estimated values to detect attacks.
- Chi-square detector and cosine similarity matching are capable of detecting random attacks
- Chi-square detector is incapable of detecting false data injection attacks, however, the cosine similarity matching approach is capable of detecting false data injection attacks

References

Danda B. Rawat and Chandra Bajracharya, "Detection of False Data Injection Attacks in Smart Grid Communication Systems," *IEEE Signal Processing Letters*, pp. 1652 - 1656, Vol. 22, No. 10, 2015.