Upgrading The Security of The Power Grid Against GPS Spoofing Attacks

Expert Professor: Dr. Maryam Dehghani
Shiraz University, Iran

Index

Introduction

- Many navigation systems and network synchronization equipment rely on GPS signals to determine their location and time.
- The structure of GPS signals is known to the public, so it is possible to build a system that produces fake GPS signals.
- Sending fake signals to GPS receivers can make them track the false signals and cause the receivers to find their location and time through the fake signals. This is called **GPS Spoofing Attack.**
- In power systems, PMUs depend on GPS for time synchronization. This dependency makes them vulnerable to GPS spoofing attacks.

Global Positioning System (GPS)

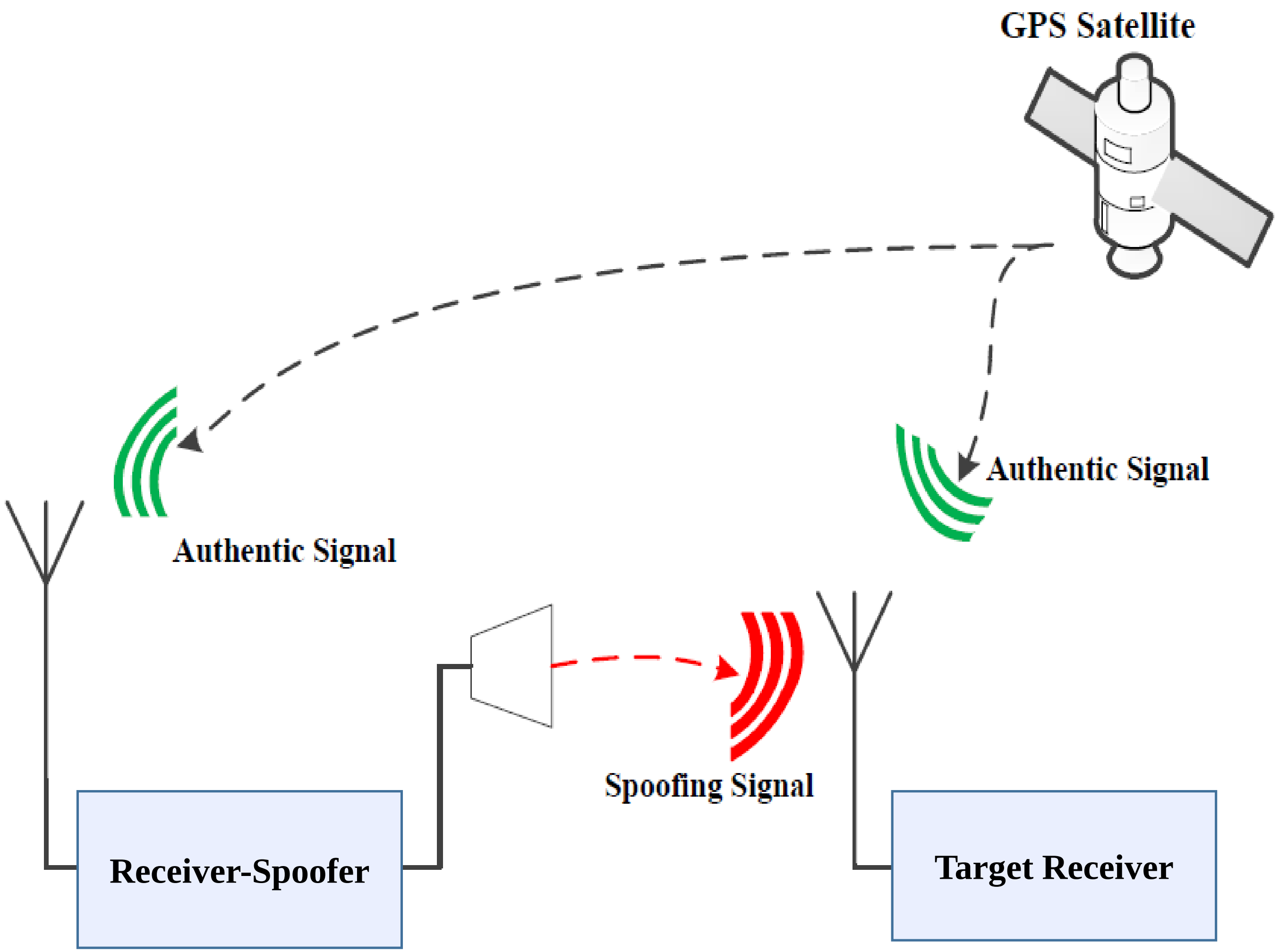
- The GPS signal contains location and time information
- The satellite clocks of GPS have no offset to universal time
- A GPS receiver cannot find its exact position simply by receiving GPS signals because the receiver has an uncertain offset relative to the universal time

GPS Spoofing Attack

Since GPS system use wireless communication, receivers are vulnerable to cyberattacks, including GPS spoofing attacks.

What a spoofer does:

- Simulating the actual GPS signal
- Causing excessive radio interference on the GPS frequency band by sending noise signals in the GPS frequency range
- Sending spoofing signals to the receiver to lock the receiver onto the fake signal (With power slightly above valid signals)


GPS Satellite
Authentic Signal
Authentic Signal
Spoofing Signal
Receiver-Spoofer
Target Receiver

Impact of GPS Spoofing Attack on PMU and Power Grid

For a signal with a frequency f, the phase measurement error $\in$ corresponding to the offset of the receiver is obtained by the following equation:

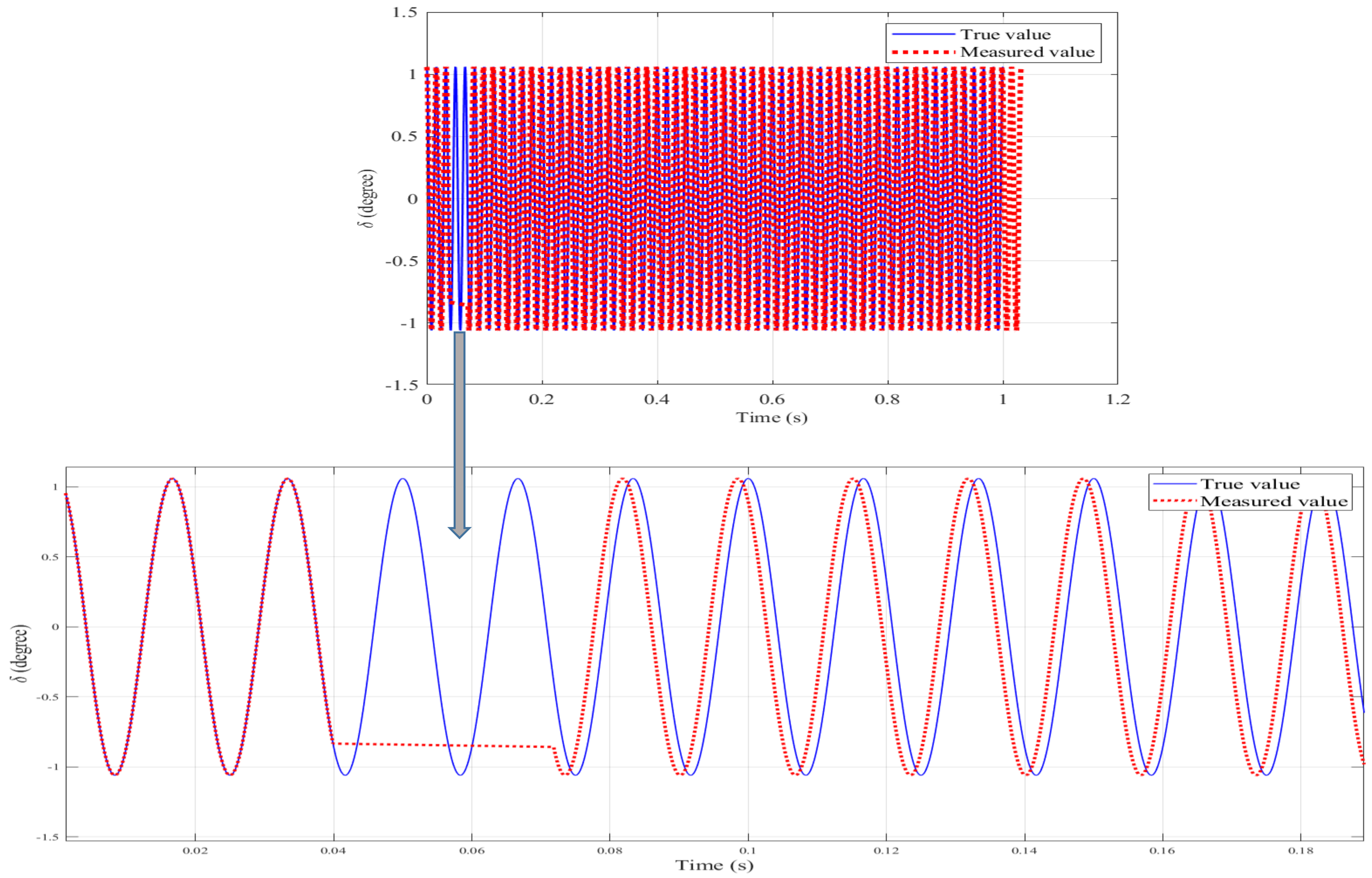
$$\varphi = 2\pi f t$$
$$\in = [2\pi f (t_u^* - t_u)]$$
$$\varphi^* = \varphi + \in$$

φ :signal phase before attack
φ^*: signal phase after attack

t_u : time offset before attack
t_u^* :time offset after attack

GPS spoofing attacks impact upon issues related to the synchronized phasors like:

Wide-area monitoring of power system, Protection and Control applications.


True value
Measured value
δ (degree)
Time (s)
True value
Measured value
δ (degree)
Time (s)

Effect of GPS Spoofing Attack on PMU Measurement

This attack only affects the phase angle of signals and the magnitude of signals remains unchanged.

The effect of GPS spoofing attack on current and voltage signals are:

$$i_n^{atk}(t) = \left|i_n^{atk}\right| \sin\left(\omega t + \theta_{I_n} + \theta_{spf}\right) = \ |i_n| \sin\left(\omega t + \theta_{I_n} + \theta_{spf}\right)$$
$$v^{atk}(t) = \left|v^{atk}\right| sin\left(\omega t + \theta_V + \theta_{spf}\right) = \ |v| \, sin\left(\omega t + \theta_V + \theta_{spf}\right)$$

The shift in voltage and current signals, which are measured by a PMU on the specified bus, are the same.

$$S_n \ = P_n + jQ_n = VI^*{}_n \ \ = |V||I_n| \angle\left(\theta_V - \theta_{I_n}\right)$$

$$S_n^{atk} = P_n^{atk} + jQ_n^{atk} = V^{atk} I_n^{atk^*} = |V||I_n| \angle\left(\theta_V - \theta_{spf} - \theta_{I_n} + \theta_{spf}\right) = S_n$$

$$S = \sum_{n=1}^{\mathbf{N}_b} v^{atk} I_n^{atk^*}$$

The complex power equation remains unchanged.

Literature Review

The detection methods of GPS spoofing attack can be divided into 2 general perspectives :

Navigation community

- Signal processing based method
- Cryptographic based method
- Radio spectrum and antenna based methods
- Diagnosis based on correlation analysis with other time sources

Power society

- Mainly state estimation approaches

Reviewing Some of The Works In Previous Researches

1997

Global Positioning System (GPS) time dissemination for real-time applications

Bring up idea of RAIM method (A signal processing based approach)

2007

Method and system for detecting GNSS spoofing signals

SINR analysis method (A signal processing based approach)

2009

A multi-antenna defense: Receiver-autonomous GPS spoofing detection.

Angle of arrival method (Radio spectrum and antenna based methods)

2011

An evaluation of the vestigial signal defense for civil GPS anti-spoofing

Evaluation of Correlation Peak Detection Method (correlation analysis with other time sources)

2015

A cross-layer defense mechanism against GPS spoofing attacks on PMUs in smart grids

Using the angle of arrival of GPS signals as an initial guess and then with the help of estimation of system states, it detects whether spoofing has occurred or not

2017

Synchrophasor data correction under gps spoofing attack: A state estimation based approach

An attack detection on one PMU in a power grid through a static state estimation **(SpM** algorithm**)**

2018

Vulnerability Analysis of Smart Grids to GPS Spoofing Analyzing the

vulnerability of smart grids to spoofing attack and providing an alternative minimization algorithm to reconstruct this attack **(AM** algorithm**)**

2018

Detection of PMU spoofing in power grid based on phasor measurement analysis

Providing a method based on power grid infrastructure using measured phase analysis, adding more PMUs and state estimation

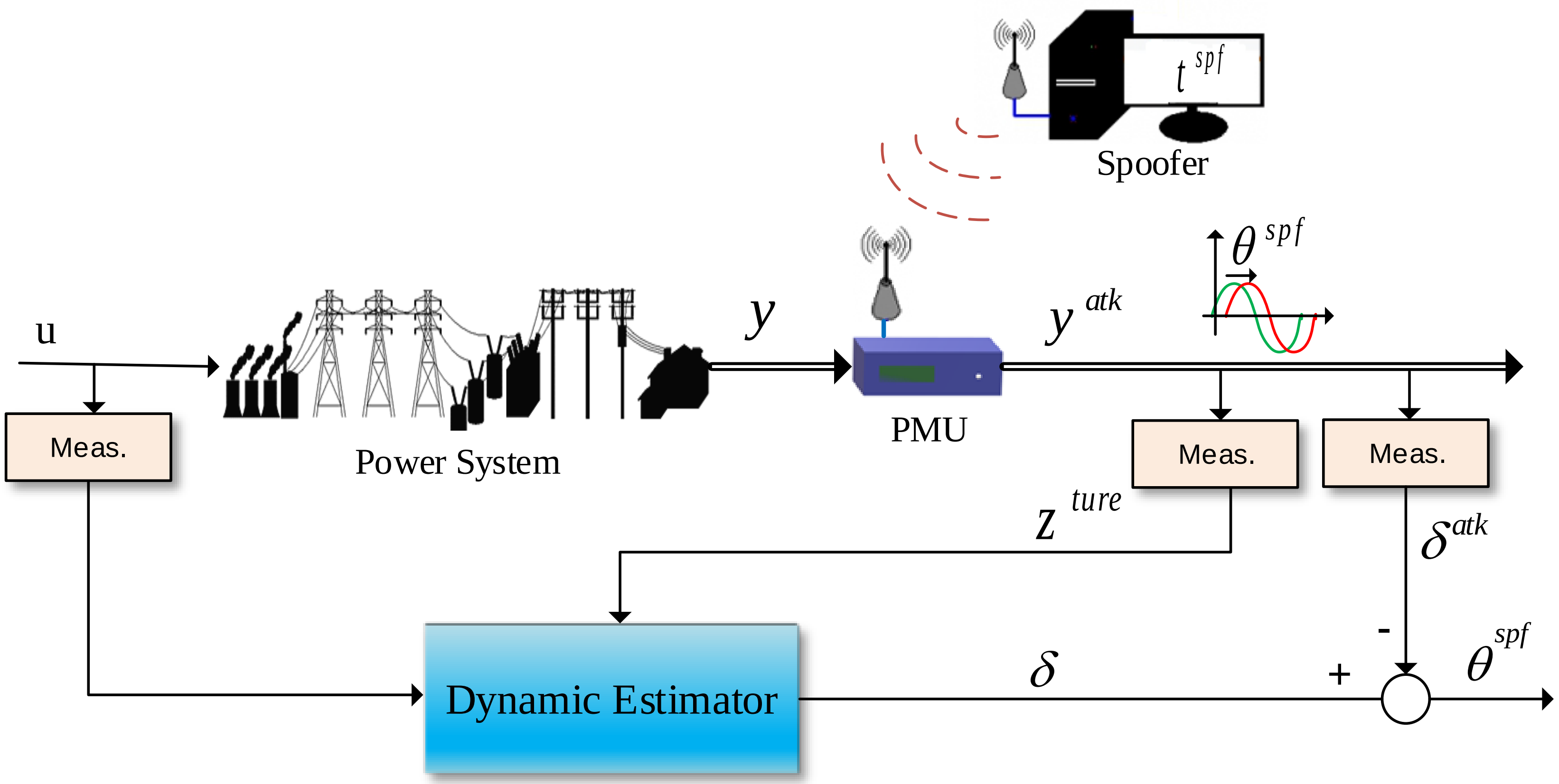
2019

Attack Identification and Correction for PMU GPS Spoofing in Unbalanced

A distribution system state estimation and minimization algorithm to detect multiple GPS spoofing attacks are presented in

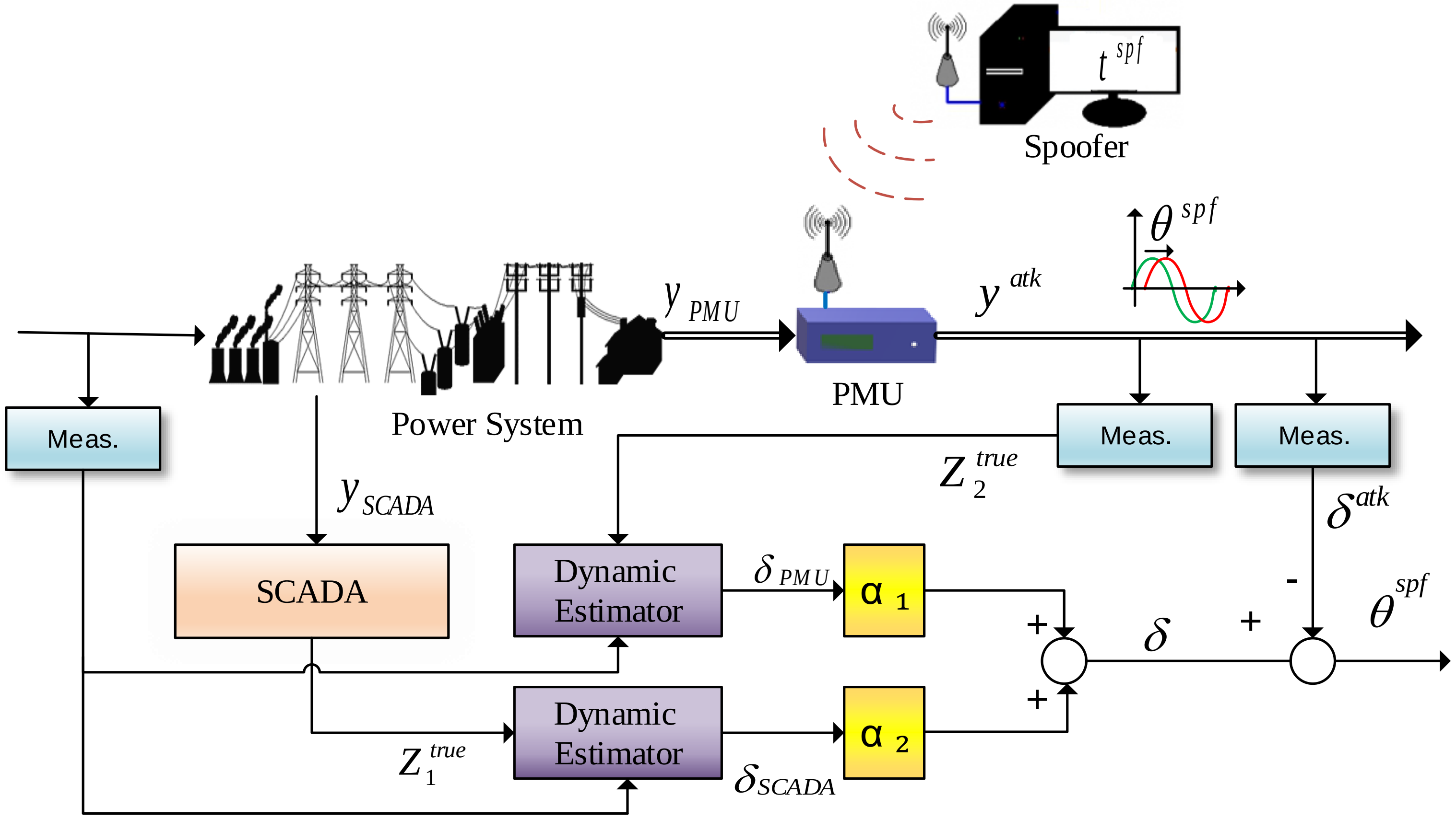
Proposed GPS Spoofing Attack Detection 1

The block diagram of proposed detection method based on PMU data is:



Proposed GPS Spoofing Attack Detection 2

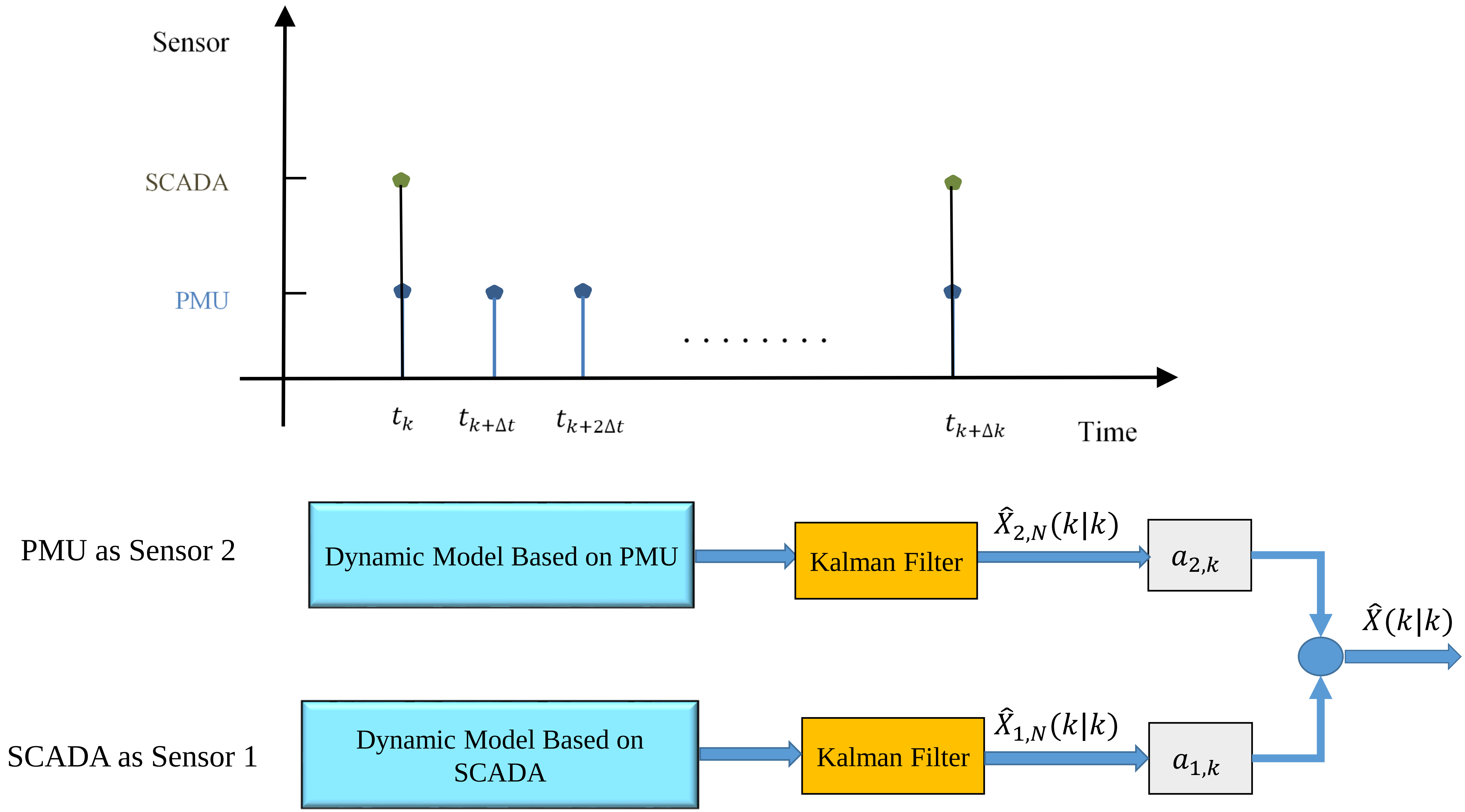
The block diagram of proposed detection method based on PMU and SCADA data is:



Algorithm of Proposed Method

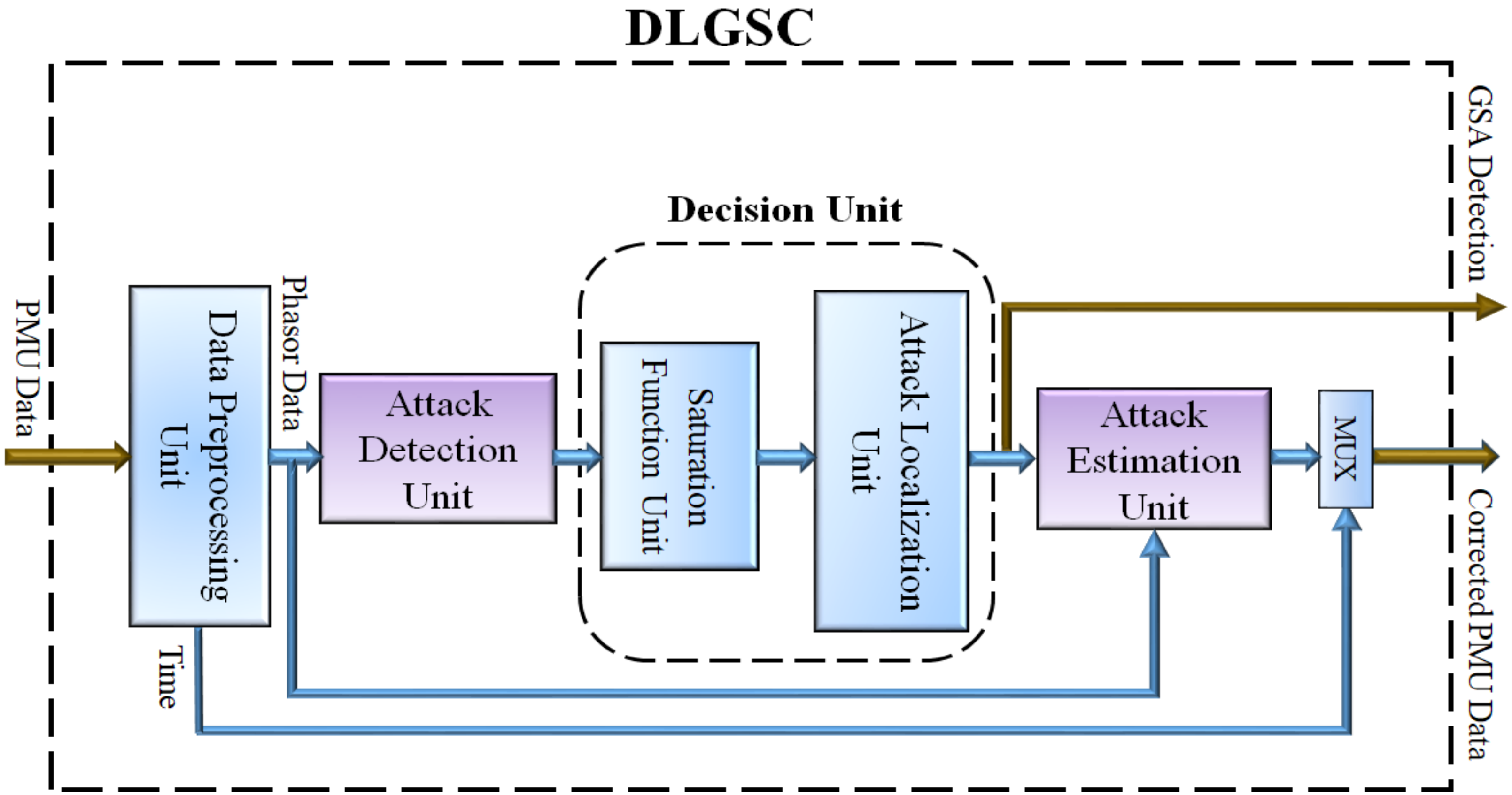
The detection scheme is based on dynamic estimation of the states in a power system model and can be summarized as follows:

- 1- Obtain the power system model based on the system configuration. The unmodeled dynamics could be modeled as a bounded noise.
- 2- Gather all measured data from PMUs and SCADA.
- 3- Use the dynamic fusion estimator and estimate the states of the power system.
- 4- Compare the measured and estimated rotor angles and calculate the phase shifts caused by spoofing attacks and detect the presence of attacks.

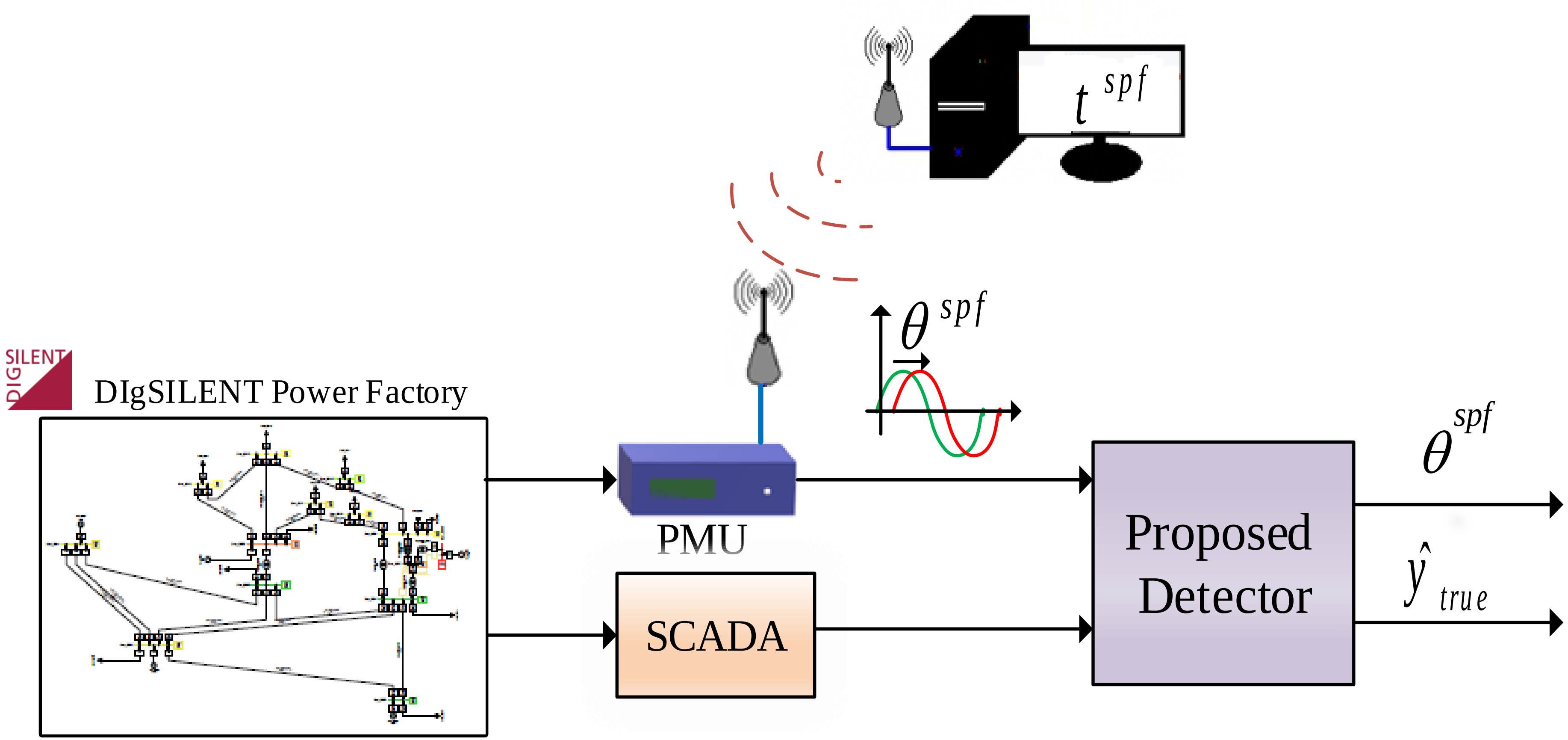

Sensor
SCADA
PMU
t_k
$t_{k+\Delta t}$
$t_{k+2\Delta t}$
$t_{k+\Delta k}$
Time
PMU as Sensor 2
Dynamic Model Based on PMU
Kalman Filter
$\hat{X}_{2,N}(k|k)$
$a_{2,k}$
$\hat{X}(k|k)$
SCADA as Sensor 1
Dynamic Model Based on SCADA
Kalman Filter
$\hat{X}_{1,N}(k|k)$
$a_{1,k}$

Proposed GPS Spoofing Attack Detection 3

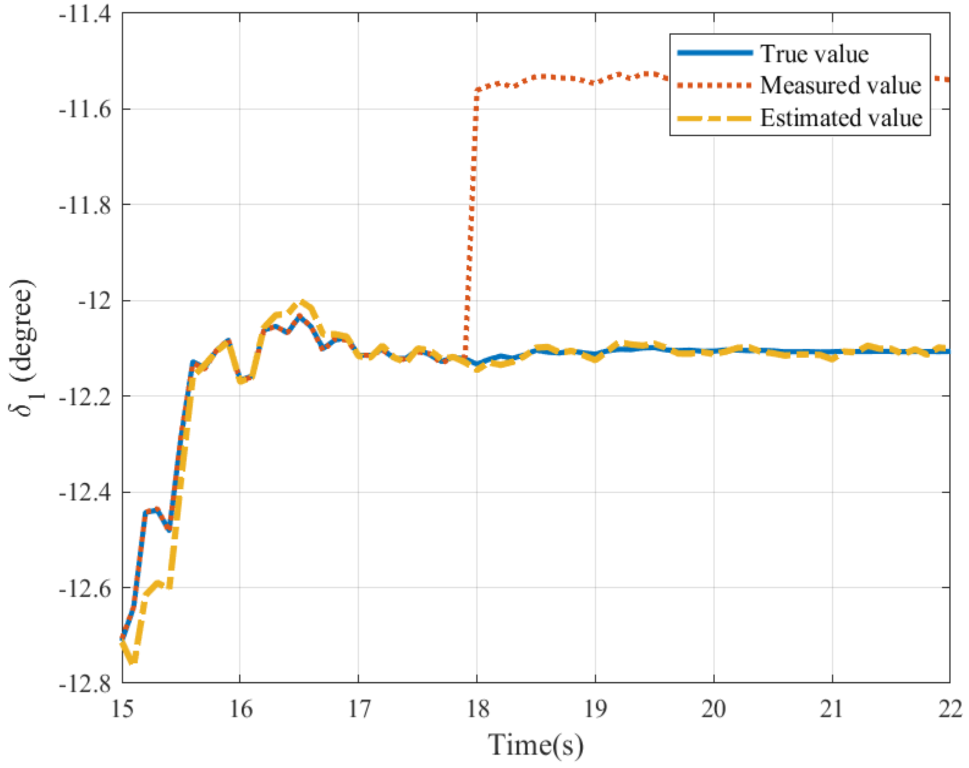
The proposed Deep Learning GPS Spoofing Counteract (DLGSC) structure is:



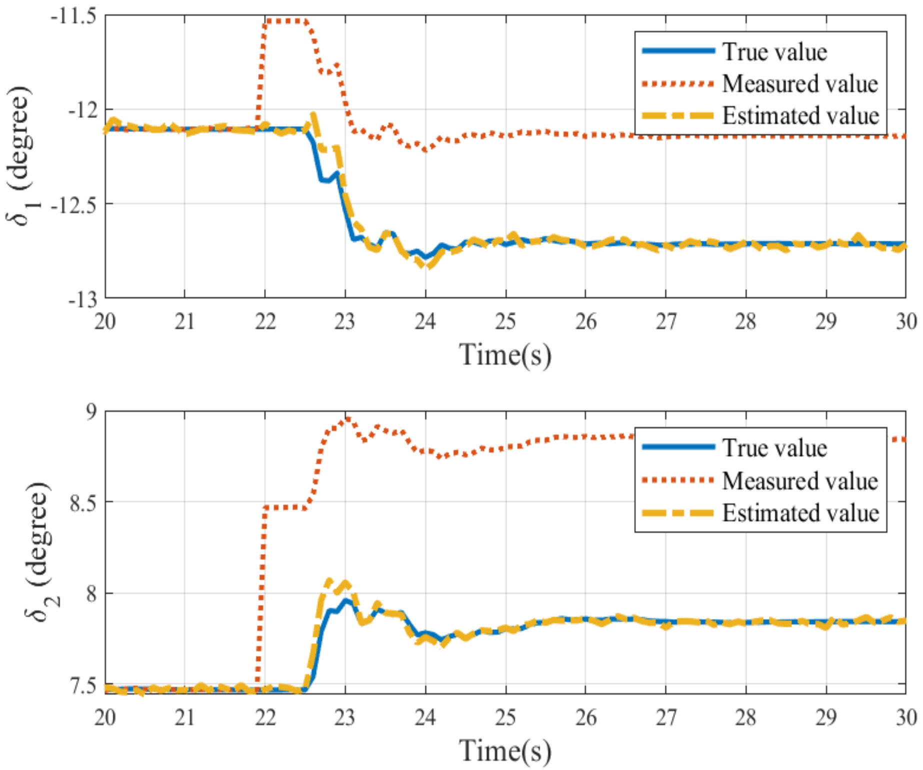
GPS Spoofing Detection in The Simulation Results



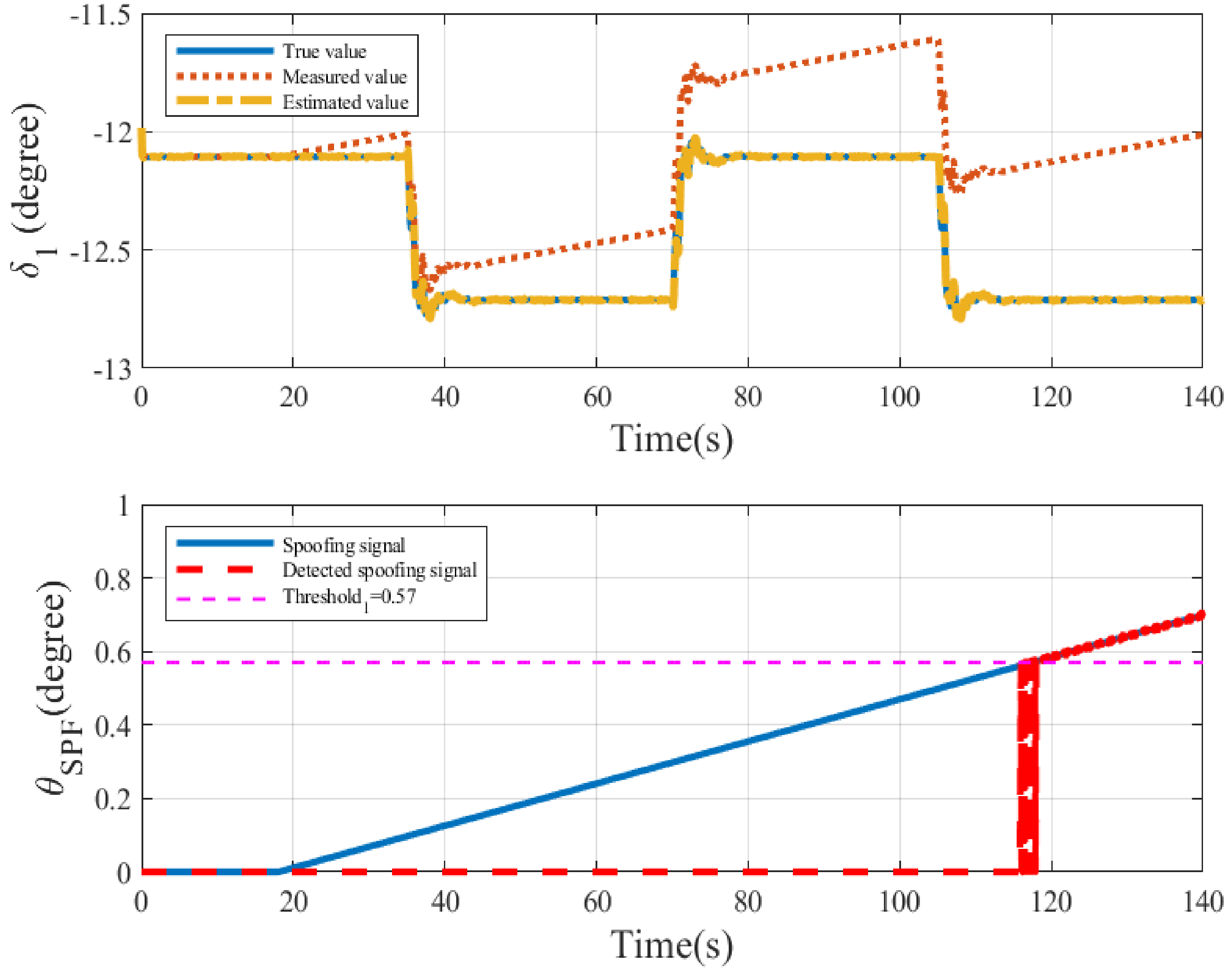
Block diagram of GPS spoofing detection scheme by DIgSILENT data



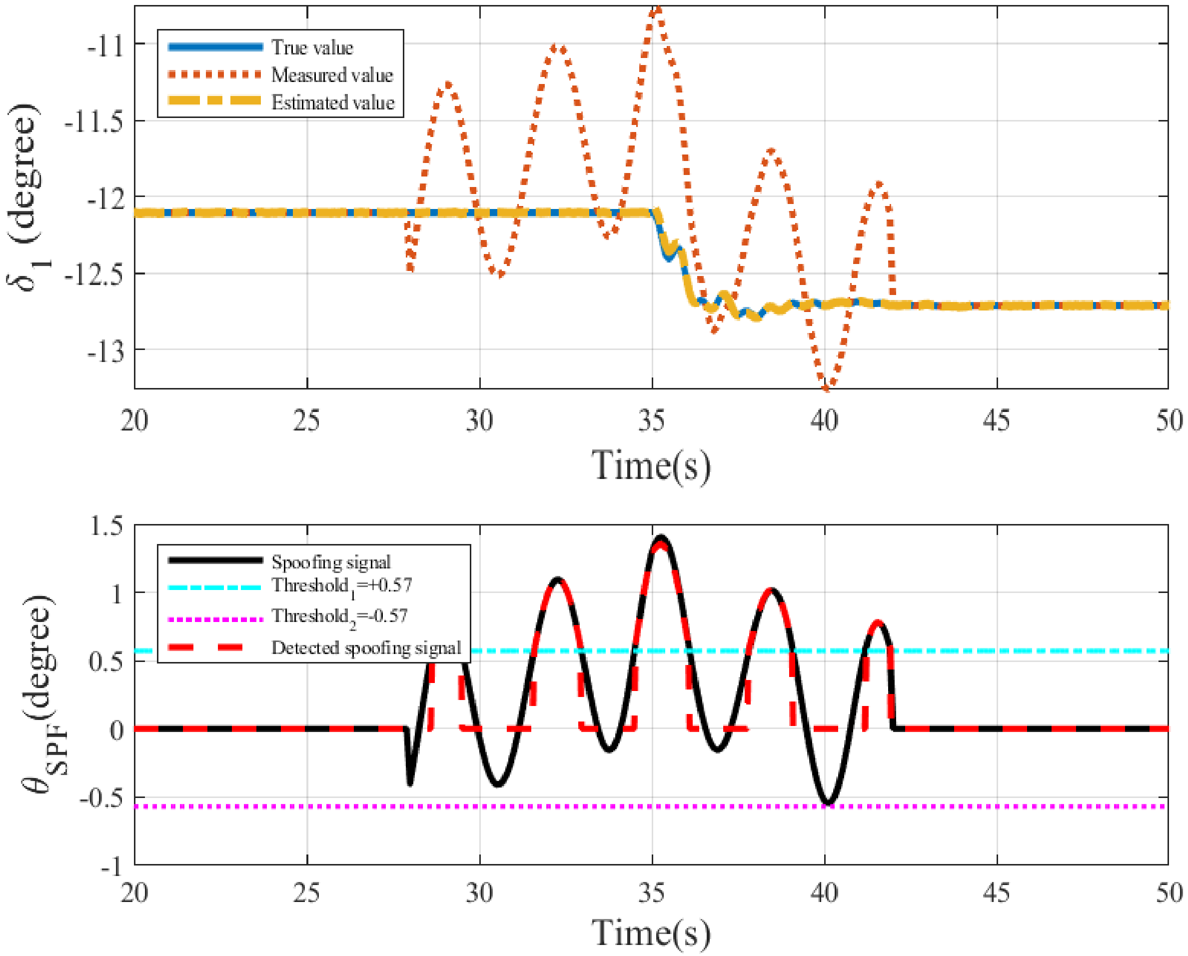
Result of attack detection on 1 PMU



Results of attack detection on 2 PMUs



Effect of gradual-increase spoofing attack on PMU 1. a) Effect on δ_1. b) Detection of the ramp attack.

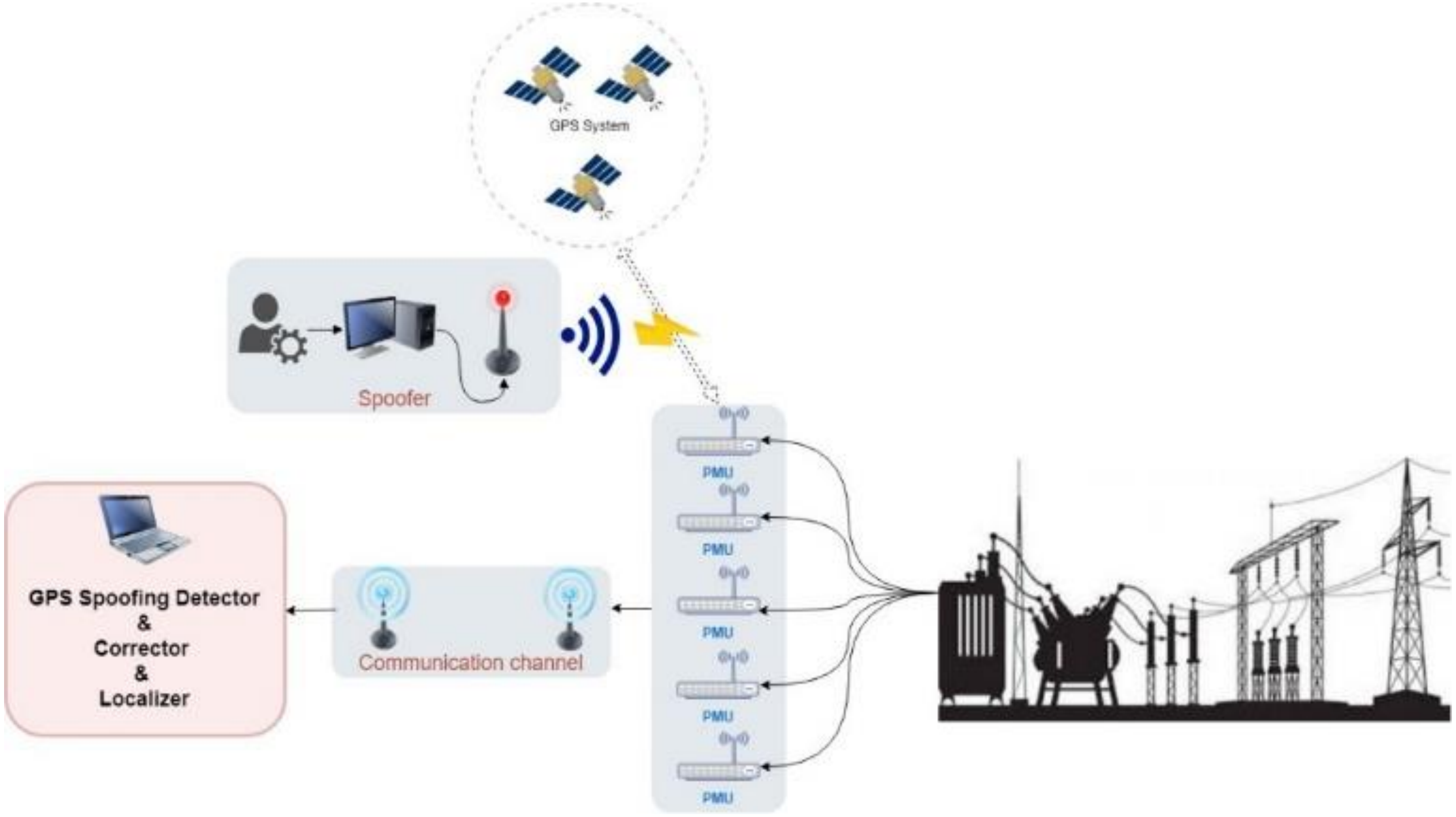


Effect of oscillatory spoofing attack on PMU 1. a) Effect on δ_1. b) Detection of the attack.

Comparison of proposed method with recent static methods

Phase Shift	Comparative Items	Proposed Algorithm	AM Algorithm (2018)	SpM Algorithm (2018)
ε_1	Computation Time (seconds)	0.0648	1.361	0.985
ε_2		0.0628	1.384	1.017
ε_3		0.0570	1.398	1.012
$\varepsilon_1 = 0.57^\circ$	Estimated Value of Phase Shift (degrees)	0.57220	0.3927	0.9053
$\varepsilon_2 = 30^\circ$		30.0008	30.6778	30.6996
$\varepsilon_3 = 90^\circ$		90.0008	90.3160	91.3448
$\varepsilon_1 = 0.57^\circ$	Relative Error (percentage)	0.3860	31.11	58.82
$\varepsilon_2 = 30^\circ$		0.0027	2.26	2.33
$\varepsilon_3 = 90^\circ$		8×10^{-4}	0.35	1.49

Practical setup of GPS Spoofing Attack Detection



Components Needed to Setting up a PMU

Raspberry Pi board

GPS module

Equipment Required for Network

Access point

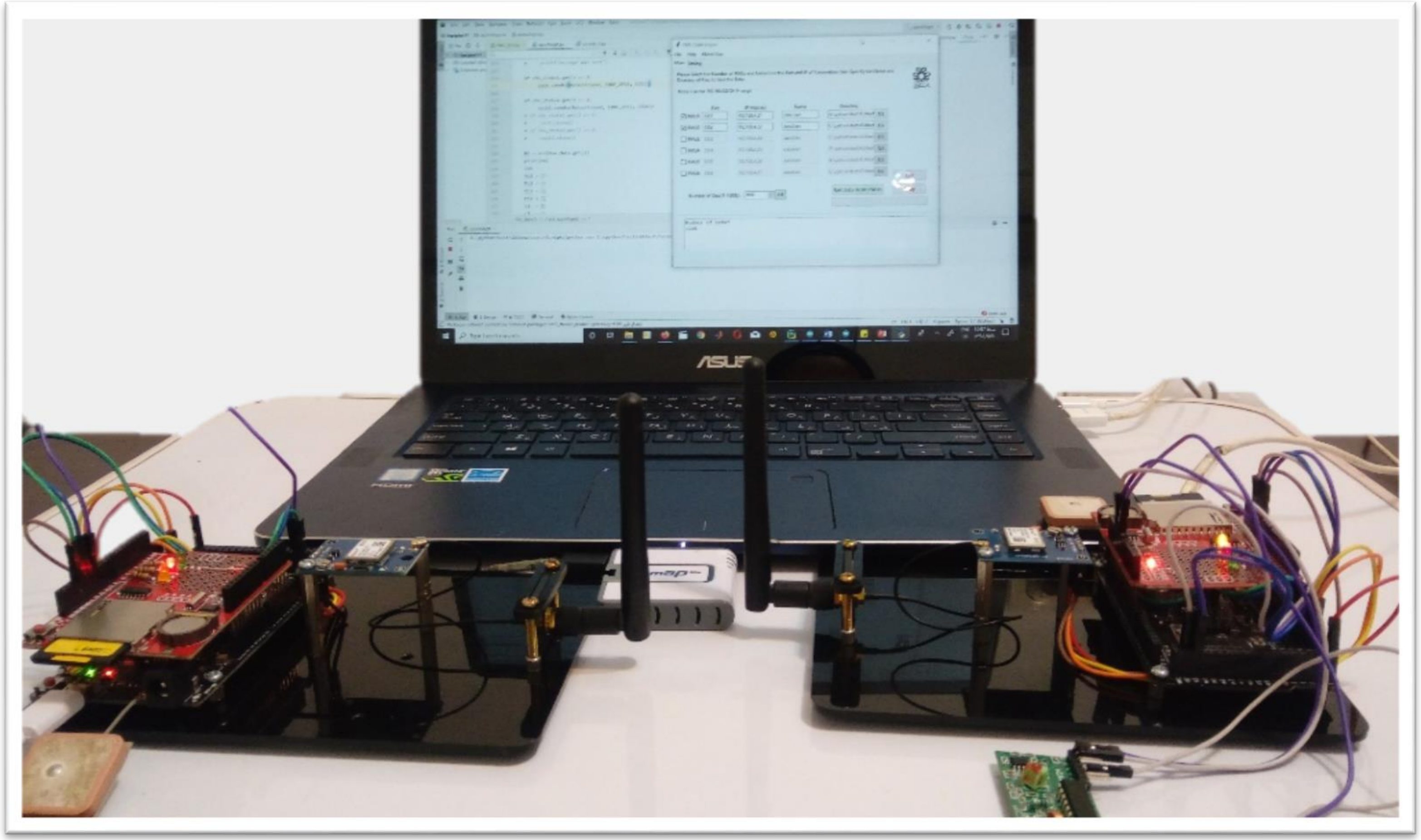
Switch Hub

Equipment Needed to Simulate The Attack

HackRF One-SDR Module

HackRF One is a Software Defined Radio peripheral capable of transmission or reception of radio signals

Simple Laboratory Network Tested



Thank you for your attention