electronics

MDPI

Article

State Estimation within IED Based Smart Grid Using Kalman Estimates

Muhammad Rashed [1,*], Iqbal Gondal [2], Joarder Kamruzzaman [1] and Syed Islam [1]

[1] Internet Commerce Security Laboratory, School of Engineering, Federation University, Mt Helen, VIC 3350, Australia; joarder.kamruzzaman@federation.edu.au (J.K.); s.islam@federation.edu.au (S.I.)

[2] SCT, STEM College, RMIT University, Melbourne, VIC 3001, Australia; iqbal.gondal@rmit.edu.au

[*] Correspondence: muhammadrashed@students.federation.edu.au; Tel.: +61-401-362-726

Abstract: State Estimation is a traditional and reliable technique within power distribution and control systems. It is used for building a topology of the power grid network based on state measurements and current operational state of different nodes & buses. The protection of sensors and measurement units such as Intelligent Electronic Devices (IED) in Central Energy Management System (CEMS) against False Data Injection Attacks (FDIAs) is a big concern to grid operators. These are special kind of cyber-attacks that are directed towards the state & measurement data in such a way that mislead the CEMS into making incorrect decisions and create generation load imbalance. These are known to bypass the traditional bad data detection systems within central estimators. This paper presents the use of an additional novel state estimator based on Kalman filter along with traditional Distributed State Estimation (DSE) which is based on Weighted Least Square (WLS). Kalman filter is a feedback control mechanism that constantly updates itself based on state prediction and state correction technique and shows improvement in the estimates. The additional estimator output is compared with the results of DSE in order to identify anomalies and injection of false data. We evaluated our methodology by simulating proposed technique using MATPOWER over IEEE-14, IEEE-30, IEEE-118, IEEE-300 bus. The results clearly demonstrate the superiority of the proposed method over traditional state estimation.

Keywords: smart grid; state estimation; Kalman filter

Citation: Rashed, M.; Gondal, I.; Kamruzzaman, J.; Islam, S. State Estimation within IED Based Smart Grid Using Kalman Estimates. *Electronics* **2021**, *10*, 1783. https://doi.org/10.3390/electronics10151783

Academic Editor: Janaka Ekanayake

Received: 11 June 2021
Accepted: 21 July 2021
Published: 26 July 2021

1. Introduction

Smart grid is an IED-based distribution and generation facility where all the power facilities such as buses, nodes, control centres and meters use duplex communication and share useful data for operational efficiency [1]. The schematic view of the smart grid is shown in Figure 1. This intricate network includes customers ranging from single users, critical businesses, defence facilities, and airports. Since the smart grid is an Internet of Things (IoT) based network where every section of the network is interlinked, hence, cyber-attacks to a certain part of the network could take control of the complete grid [2]. The attackers could use it for further malicious motives such as shutdown, cascaded blackouts, or terrorism activities [3]. Therefore, the protection of smart grid from FDIAs and cyber-attacks require immediate attention. State estimation is a traditional technique that uses a limited number of measurements for determining the operational state of a system [4]. State estimation is used to build a grid topology at the supervisory control and management layer [5]. State estimation creates a matrix known as jacobian matrix by using the state data and covariance matrix that also helps with detection of errors [6].

It is also preferrable for an electrical grid because installation of metering devices at every bus is not practical. A bus refers to a part of transmission network within electrical grid where multiple transmission lines intersect. Cyber-attacks such as stealth and FDIAs have been known to target state estimation data and state measurements which are collected through IEDs such as phasor measurements units (PMUs) [7].

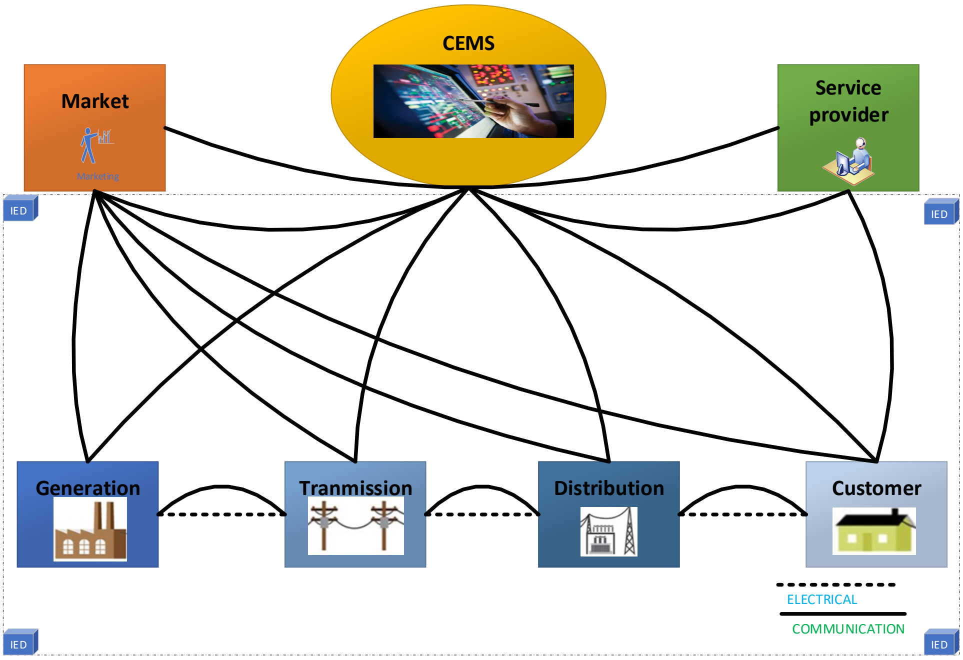


Figure 1. A schematic of an IED based smart grid.

A PMU like any other metering device is an IED that collects useful information and state data for monitoring the operational status of the sections of the grid [8]. For synchronisation purpose, a global positioning system signal is used with every PMU. This helps for correlation of state data from different sections & buses within multi-distributed gird [9]. FDIAs prepared based on the knowledge of the network configuration makes them more lethal and difficult to detect using traditional bad data detection approaches [10]. Furthermore, it is also desirous to have quick detection of FDIAs, however quick detection operations are computationally expensive.

In most state estimation algorithms, the measurement observation model is highly nonlinear which can be solved by the possible use of Kalman filter for nonlinear systems [11]. The Kalman filtering techniques have been improved significantly over the past few years with the variants such as extended Kalman filter, unscented Kalman filter and robust minimum variance unscented Kalman filter [12]. In this paper, we have investigated the detection of FDIA by using a minimum variance unscented Kalman filter (mv-UKF) to predict and update the state function starting from the previously known states [13]. These values were compared with the results acquired from a traditional weighted least square (WLS) based state estimation algorithm. The difference in the two deviates significantly when the system is under the influence of FDIA triggering the presence of an attack. As per author's knowledge, this technique has not been used in combination in distributed WLS.

Since WLS only collects a single set of measurements, it fails to estimate the state for a quasi-steady state load profile [14,15]. For this purpose, we proposed the use of distributed state estimation in that improves the result by performing state estimation and false data detection in a distributed fashion [16]. This also reduces the computational complexity of the central estimator. However, state estimation in a distributed fashion requires installation of PMUs at multiple locations hence there is a trade-off between number of PMUs versus detection accuracy [17]. Therefore, dynamic state estimation is useful and can help with identifying presence of bad data and topology errors.

The main motivation of this study is to develop a new data attack detection technique to overcome the problem that the traditional WLS cannot identify [18,19]. In the current literature, there is lot of emphasis being made on Kalman filter state estimation as well as distributed state estimation [20]. However, there is not much work available to cite where both of these techniques are combined together. Our proposed technique will find new vulnerabilities for power system design that can target detection methods for corresponding vulnerability in order to improve system detection and robustness. Considering the historical state estimates of the system without being attacked, a correct reference for state estimation with Kalman filtering is proposed by combing WLS and mv-UKF filter estimates.

The main contribution of this paper is:

- False data detection using measurement residual obtained from WLS based distributed state estimation
- Acquire estimates using mv-UKF and form a covariance matrix
- Observe the deviation in the output by performing two levels of state estimation using WLS and Kalman filter

The remainder of paper is organised as follows. The related work is explained in Section 2. The mathematical formulation is explained in Section 3. The case studies and simulations are discussed in Section 5. Finally, Section 6 concludes the paper.

2. Literature Review

In Ref. [2], Amin et al. Presented a fault discrimination approach based on machine learning algorithm (MLA) based cyber-attack. State of the art MLA classifiers were used to distinguish between faults and cyber-attacks within smart grid. They clarified that the precision in the detection of classifiers decreases when they are trained only with faults and data. The future scope includes the analysis of different types of cyber-attacks and the use of synthesized data for the early training of MLA in distinguishing between faults and cyber-attacks. The proposed techniques in this work have needs to be verified with IEEE-bus systems with distributed estimation.

J. Cao et al. [3] investigated a potential invasion pathway of the FDIA against a cyber physical system and designed a novel model to detect different types of FDIA. The problem of high false alarm rate of the model caused by imbalance data was addressed. They also proposed oversampling in order to obtain pseudo-data and stored into the database that assists in training and evaluating the model. An ensemble classifier was constructed to detect the FDIA which improved the accuracy of difficult-classification samples and precision of FDIA detection. The results show that this model can detect different types of FIDAs. However, the system needs to be tested on a number of different size bus systems.

Al-Eryani and Baroudi in [4] analysed distributed partitioning state estimation using chi-square tests using IEEE-39 Bus system. The system was divided into 3 subsystems and each partition was treated as a separate independent system. False data was injected in two different places. The results demonstrate that false data was detected using subsystem partition while not treating the whole grid as one system. The downside of this technique was that it was tested on a small system. The proposed methodology does not deal well with non-linearities in the load profile.

Pei et al. in [5] proposed a deviation based false data detection method based on an additional Kalman filter for the purpose of dynamic state estimation. The exponential weighting functions were used to detect FDIA effectively. The measurements were collected using the PMUs synchronised using Global position system signals. However, due to continuous variation and non-linearities in the load profile, a time variant method needs to be looked into to improve the detection.

In Ref. [6], an online parametric estimate based on software defined controller was used with GPU enabled robust estimator. The graphical processing unit with deep learning algorithm, short-term memory, and an extended Kalman filter was used to solve the issue of massive connections. However, the implementation requires 6G enabled network in order to achieve minimum latency countering the transients in order to minimise the chances of cascading failures, therefore, it is not going to take place in coming years before trials and practical tests can take place.

In Ref. [7], chen et al. presented a false data detection model based on particle swarm optimization. The system was tested against false data attack with minimum attack residual increment. Two kinds of estimates were proposed for conducting chi-square tests. However, the system was not analysed for multiple cyber-attacks as this will lead to a much more complex residual model and hence it will be difficult to solve the false data attack vector. The proposed methodology needs to be verified for distributed state estimation.

In Ref. [9], a parallel dynamic state estimator using graphical processing units and markov model was proposed due to stochastic nature of the power system. The history of the system's behaviour was used to improve the accuracy of the results obtained through Euclidean distance metric. However, the detection accuracy needs to be improved by increasing the number of processing units which will lead to increased computational complexity. The use of parallel graphical processing units for state estimation may increase computational complexity.

3. State Estimation Using Weighted Least Squares

The state estimation within power grid uses an internal bad data detection system known as chi-square test based on a normalized residual of collected phasor measurements [20]. Based on these phasor measurements, a threshold limit is created that defines the normal operating conditions of the grid. The estimates will always stay below this threshold limit created by the system, under normal operating conditions, unless there is bad data present. A residual superseding the threshold limit triggers the presence of bad data alarm, hence the estimator will not accept the measurement as an authentic. In order to formulate the objective function for chi-square test, the non-linear model for a state estimation can be represented as follows [21]:

$$z = h(x) + e \tag{1}$$

where z is the meter measurement, $h(x)$ is the function of state variable x represents a Jacobian matrix depending on the network topology, and e is the noise that follows a Gaussian distribution.

In order to solve the WLS estimation problem, the objective function can be defined as follows [22]:

$$J(\hat{x}) = \sum_{i=1}^{m} \frac{(z_i - h_i(x))^2}{\sigma_i^2} \tag{2}$$

where $J(\hat{x})$ is the weighted-sum square residual that follows chi-square distribution, $\hat{x}$ is an estimate of x solved by WLS, $\mathcal{X}^2_{(m-n)}$ is the detection threshold corresponding to p, where p is the detection confidence which is taken as 95%, and n is the number of state variables. We examine the function $J(\hat{x}) \geq \mathcal{X}^2_{(m-n)}$, if the resulting value is greater, then bad data is detected, otherwise no bad data.

3.1. *False Data Injection Attack*

Mathematical Formulation

In order to inject false attack, the measurements at each bus are falsified by adding an attack vector a. The state estimates can be represented as follows [23,24]:

$$z_a = Hx + a + e \tag{3}$$

$$a = Hc \tag{4}$$

$$\mathrm{a} = [\mathrm{a}_1, \mathrm{a}_2, \ldots, \mathrm{a}_\mathrm{m}]^\mathrm{T} \tag{5}$$

$$z_a = Hx + Hc + e \tag{6}$$

$$z_a = H(x + c) + e \tag{7}$$

where a = [a_1, a_2, . . . , a_m]^T represents the attack at corresponding bus, H is the Jacobian matrix representing the topology of the network, c = (c_1, c_2, . . . , c_n)^T is an arbitrary vector, e is the system noise [25]. This attack is not detected since the state (x + c) is treated as the real value in the estimator. The hypothesis tests fail to detect the FDIA as this will not change the measurement. For this purpose, the use of dynamic state estimator based on Kalman filter is used.

3.2. Kalman Filter as an Estimator

The Kalman filter is better suited for dealing with non-linearities in the load profile which WLS cannot estimate [26]. It takes a set of data and estimates the trend of data by using a distribution function of these variables. As shown in Algorithm 1, the additional estimator is mv-UKF where kalman estimates are acquired based on a priori knowledge of the previous estimates. These estimates are used to measure the deviation between the WLS estimate and mv-UKF estimates. Collection of sigma point is necessary in order to form the mean and covariance matrix of the kalman estimates.

A Kalman filter contains feedback loops and can be used for time series prediction with historical data [11]. The non- linear equations in kalman are not linearized as with other gradients methods [12]. Instead, a statistical distribution of the state is represented through sigma points which provides estimates of the actual state and the posterior covariance matrix [11–13].

Algorithm 1 Additional estimator using mv-UKF

```
Result: Collect meter readings using sensors
Initialization;
while forecast kalman estmiates do
    calculate sigma points;
Create mean and covriance matrix as per Equations (10)–(18)
Calculate kalman gain per Equations (19) and (20)
    if WLS estimate and kalman esitmates deviation exceeds objective function threshold in
Equation (2)
then
        Claculate new sigma points and increase weights per Equations (10) and (11)
    else
        No bad data detected, update state function
    end
end
```

The test results in [1] were completed using DSE only and was limited to IEEE-14 and IEEE-30 Bus without the use of Kalman filter. In this work, we have expanded the research work in [1] by using the similar methodology, however, included the IEEE-118 and IEEE-300 bus and an additional Kalman filter has also been incorporated.

4. Mathematical Formulation Based on Kalman Estimates

Kalman filter estimator can be represented as follows:

$$x_t = f(x_{t-1}, t-1) + q_{t-1} \tag{8}$$

$$z_t = h(x_t, t) + r_t \tag{9}$$

where x is the state vector, q_{t-1} is the system noise, r_t is the measurement Gaussian noise with zero mean, and z is the measurement vector. The function f and h are non-linear equations representing the system and measurements model in terms of the state variables [13]. The Kalman filter implementation consists of the prediction and correction steps. First, it obtains the state and matrix covariance prediction, in the second step it calculates the Kalman gain and the state and matrix covariance update steps [11,12]:

The sets of $2n + 1$ point is created in (8) for the state vector x at time $t - 1$ as follows:

$$X_{t+1} = x_t + \sqrt{c}\left[\sqrt{nP_{t-1}}\right] \tag{10}$$

The initial state vector and the initial covariance matrix is defined based on a priori knowledge of the historical estimates [13]. The sets of sigma points are estimated by the state update function [14].

Step I: *State prediction*

$$\hat{X}_t^i = f\left(X_{t-1}^i, t-1\right) \tag{11}$$

where $i = 0, 1, \ldots, 2n$, X_{t-1}^i is the $(i + 1)$th column of matrix X_{t-1} and the resulting X_t is an $n \times (2n + 1)$ matrix propagated by points. The predicted state mean vector x_t^- and covariance matrix P_t^- are defined as follows:

$$x_t^- = \sum_{i=0}^{2n} W_i^m \hat{X}_k^i \tag{12}$$

$$P_k^- = \sum_{i=0}^{2n} W_i^c [(\hat{X}_k^i - x_k^-)\left(\hat{X}_k^i - x_k^-\right)^T] + Q_{t-1} \tag{13}$$

where W_i^m refers to weights of the Kalman filter and $\hat{X}_k^i$ are sigma points [11]. Q_{t-1} is the covariance matrix of the process noise [12]. A minimal set of sampling points known as sigma points are selected and transformed using the nonlinear function, whereas the new mean and the covariance are formed out of those transformed points [13]. The idea is that it is easier to approximate a Gaussian distribution than it is to approximate an arbitrary nonlinear function [14].

Step II: *State Correction*

The points around the predicted state mean vector and the covariance matrix are defined as:

$$X_t^- = \left[x_t^- \ \ldots \ x_t^-] + \sqrt{c}[0 \ \sqrt{P_t^-} - \sqrt{P_t^-}\right] \tag{14}$$

Derive points from the measurement update function as,

$$Y_t^- = h(X_t^-, t) \tag{15}$$

The mean is calculated as:

$$\mu_t = \sum_{i=0}^{2n} W_i^m Y_t^{-i} \tag{16}$$

where W_i^m is the weights and Y_t^{-i} is the measurement update function for the corrected state estimate [11].

The covariance S_k and the cross-covariance C_t matrix of the state and measurements are given as:

$$S_k = \sum_{i=0}^{2n} W_i^c \left[\left(Y_t^{-i} - \mu_t\right)\left(Y_t^{-i} - \mu_t\right)^T\right] + R_t \tag{17}$$

$$C_t = \sum_{i=0}^{2n} W_i^c [\left(X_t^{-i} - x_t^-\right)\left(Y_t^{-i} - \mu_t\right)^T] \tag{18}$$

where R_t is the covariance matrix of the observation noise vector [12–14].

The filter gain K_t, the mean x_t and the covariance P_t are estimated as:

$$K_t = C_t S_t^{-1} \tag{19}$$

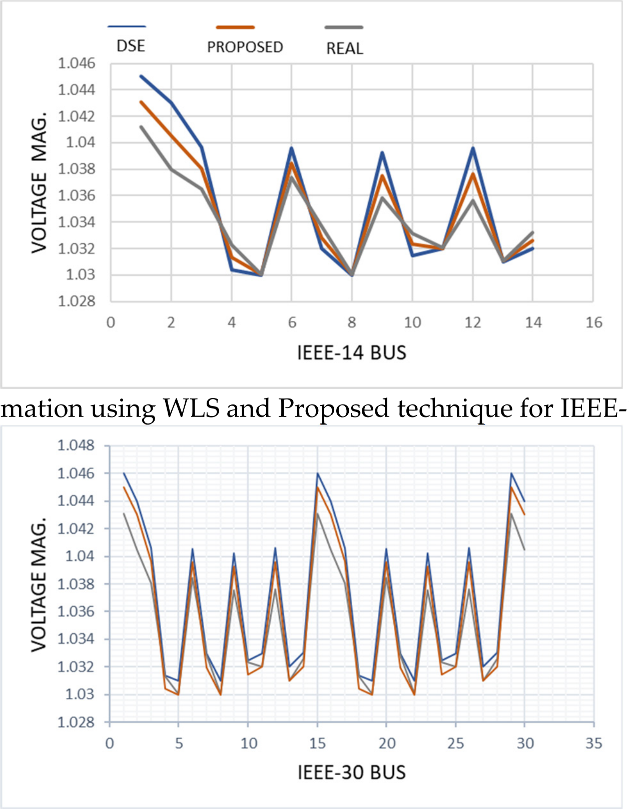
$$x_t = x_t^- + K_t[y_t - \mu_t] \tag{20}$$

With the help of additional online estimator, state variables can be forecasted based on prior knowledge of historic measurement.

5. Results & Discussion

In order to evaluate the performance of the proposed algorithm, the simulations were conducted on IEEE-14, IEEE-30, IEEE-118 and IEEE-300 bus systems using MATLAB & MATPOWER. The state variables were estimated using WLS based state estimation and mv-UKF techniques. The system was subjected to FDIA on various bus and the deviation in the output of the two results was measured. As shown in Figure 2, the WLS based distributed state estimates DSE were plotted against real input and proposed methodology, when there was no FDIA introduced. The normalized residual for all the voltage magnitudes were found to be below the predefined threshold level set to trigger the presence of FDIA.

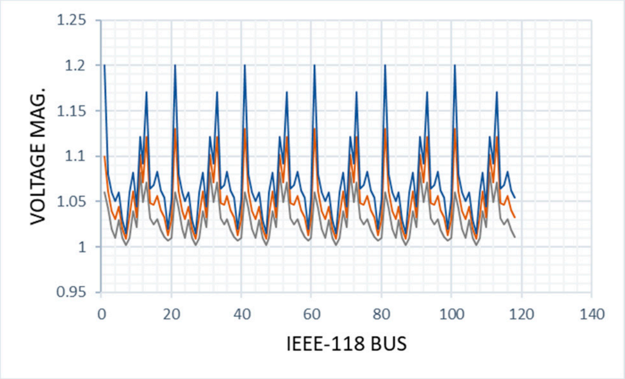
Table 1 shows the estimates obtained through DSE and an additional estimator based on mv-UKF. This clearly shows that the size of the subsystem plays an effective role in improving the results. The tests were carried out with different subsystems. Table 2 demonstrates the attack cases, number of measurements and the value of objective function obtained using Equation (2). It is clear from the readings that the values obtained using DSE stays below threshold limit hence presence of bad data is not detected. The proposed estimator gives a value higher than the threshold limit hence indicating the presence of bad data.



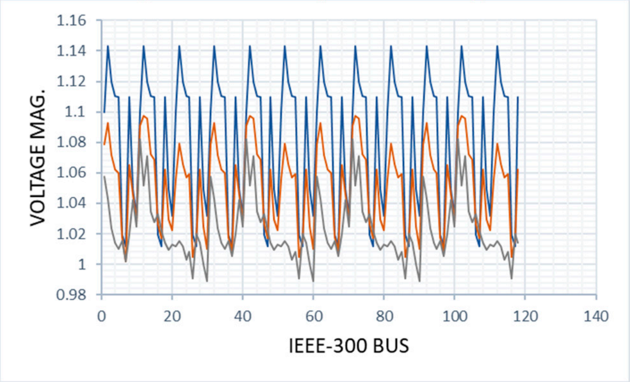
(**a**) Estimation using WLS and Proposed technique for IEEE-14 Bus

(**b**) Estimation using WLS and Proposed technique for IEEE-30 Bus

Figure 2. *Cont.*



(**c**) Estimation using WLS and Proposed technique for IEEE-118 Bus



(**d**) Estimation using WLS and Proposed technique for IEEE-300 Bus

Figure 2. Estimate data collected using DSE WLS and Proposed technique.

Table 1. Compromised Bus numbers with Error.

Compromised Bus	Real (p.u.)	Estimate DSE (p.u.)	Estimate Proposed (p.u.)	Error Estimate in DSE	Error in Proposed
20	1.0094	0.9732	1.0126	0.0355	0.0041
40	1.0214	0.9860	1.0248	0.0358	0.0039
60	0.9828	0.9469	0.9887	0.0359	0.0059
80	1.0094	0.9732	1.0126	0.0353	0.0048
100	1.0214	0.9860	1.0248	0.0358	0.0039

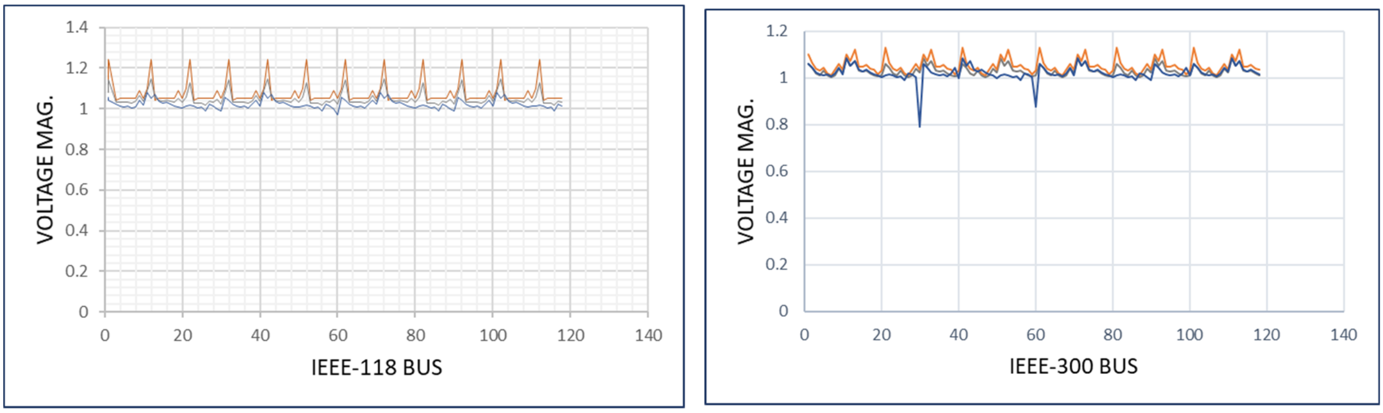
Table 2. Objective function for different Attack scenarios.

Area	Bus	States (n)	Measurements (m)	(m-n)	Proposed	J(x)	WLS
1	Attack case 1	7	60	53	0.7005	0.68	0.675
2	Attack case 2	7	60	53	0.6755	0.64	0.63
3	Attack case 3	7	60	53	0.6505	0.63	0.62
4	Attack case 4	7	60	53	0.634	0.61	0.58
5	Attack case 5	7	60	53	0.345	0.33	0.3
6	Attack case 6	7	60	53	0.3308	0.325	0.31
7	Attack case 7	7	60	53	0.36	0.34	0.33
8	Attack case 8	7	60	53	0.4013	0.4	0.4
9	Attack case 9	7	60	53	0.435	0.43	0.42
10	Attack case 10	7	60	53	0.435	0.43	0.48
11	Attack case 11	7	60	53	0.485	0.48	0.48
12	Attack case 12	7	60	53	0.47	0.465	0.463

After the FDIA at bus 20, 40, 60, 80, 100 as shown in Table 1, the intensity of the voltage magnitude was changed. It can be observed that the WLS based state estimates remain below the threshold limit, hence the presence of FDIA was not detected. With the proposed methodology, the voltage magnate exceeds the threshold level defined by the objective function, hence triggering the FDIA attack. Table 2 shows different attack scenarios and the value of estimates against J(x). It is clear that by using the proposed technique, the magnitude exceeds the J(x) hence indicative of FDIA, whereas the traditional WLS estimates stay below the threshold, hence no FDIA can be detected.

The test spanned over 4 h, samples collected every 30 s, which is an expected sampling period within SCADA. The results show that the estimated values with our method are improving in the case of large-sized grids. All meter readings are contaminated by gaussian noise with covariance of 10^{-1}. In order to simulate Equations (4) and (5), the voltage magnitudes were falsified at corresponding bus to emulate the injection of false data attack. In the Figure 2, the estimates obtained through proposed estimator were plotted along with the results obtained through DSE and actual input in per unit scale against each bus number, when there is no FDIA.

The estimates obtained using mv-UKF estimator were plotted against each bus along with real values and DSE in case of an FDIA. It can be easily seen that the Kalman filter estimates based on priori information are closer to the actual values in case of FDIA. For example, in Figure 3, at Bus no. 10 for IEEE-300 Bus, the estimates through Kalman filter are improved compared with WLS method where the measurements are recorded at 0.90 per unit which is below the threshold limit 1.



(**a**) (**b**)

Figure 3. Estimate Data after false data injection attack (**a**) IEEE-118 Bus; (**b**) IEEE-300 Bus.

The DSE alone fails to detect this kind of attack. At Bus no. 58, Figure 3, in IEEE-300 Bus, the estimates obtained through WLS is 0.93 which is below the threshold limit 1 per unit. This implies the residual will stay below the threshold limit hence false data will not be detected. The results from the proposed online detector based on Kalman filter gives an improvement and a value that exceeds the threshold; hence the presence of false data will be triggered. The simulation results confirm the improvement in state estimation and false data detection. It is concluded that in the case of FDIA, the deviation in the results of WLS and Kalman filter was larger in the case of FDIA.

6. Conclusions

Paper propose the use of online Kalman filter estimator based on prior knowledge of the state estimates in addition to traditional WLS state estimator within DSE. The proposed estimator improves the state estimation results and detect FDIA which is not detected using DSE alone. The measurements collected through metering devices are compared with the estimates produced by online estimator and the difference of two identifies the presence of bad data. The effectiveness of the proposed estimator was proven by the tests conducted over IEEE-14 bus, IEEE-30 bus, IEEE-118 bus, and IEEE-300 bus using MATLAB. The false data is injected at different buses and the output of the WLS was recorded. The results are plotted along with actual measurements and from online estimator. The results prove that the estimates generated by additional estimator have improved in the case of FDIA. The difference in the reading of two estimators identifies the false data. The simulation results prove the superiority of the proposed method over WLS under false data injection attack.

Author Contributions: Conceptualization, M.R., I.G., J.K. and S.I.; methodology, M.R., I.G., J.K. and S.I.; software, M.R., I.G., J.K. and S.I.; validation, M.R., I.G., J.K. and S.I.; formal analysis, M.R., I.G., J.K. and S.I.; investigation, M.R., I.G., J.K. and S.I.; resources, M.R., I.G., J.K. and S.I.; data curation, M.R., I.G., J.K. and S.I.; writing-original draft preparation, M.R.; writing-review and editing, I.G., J.K. and S.I.; visualization, M.R., I.G., J.K. and S.I.; supervision, I.G., J.K. and S.I.; project administration, M.R., I.G., J.K. and S.I. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

Abbreviation	**Meaning**
IED	intelligent electronic devices
CEMS	central energy management system
FDIA	false data injection attack
DSE	distributed state estimation
WLS	weighted least squares
IoT	internet of things
PMU	phasor measurement unit
SCADA	supervisory control and data acquisition
MLA	machine learning algorithm
GPU	graphical processing unit
6G	6 generation
Nomenclature	
z	meter measurement
h(x)	function of state variable
e	noise follows gaussian distribution
j(x)	objective function that follows chi-square distribution
σ_i^2	variance
a	attack vector
za	measurement with attack vector
$\mathrm{x_t}$	state variable
$\hat{x}$	state estimate
q_{t-1}	system noise
r_t	measurement gaussian noise
X_{t+1}	sigma points
W	sigma points weights
Q_{t-1}	covariance of the system noise
R_t	observation noise
μ_t	mean of the corrected state

References

1. Rashed, M.; Gondal, I.; Kamruzzuman, J.; Islam, S. State Estimation in the Presence of Cyber Attacks Using Distributed Partition Technique. In Proceedings of the 2020 Australasian Universities Power Engineering Conference (AUPEC), Hobart, Australia, 29 November–3 December 2020; pp. 1–6.
2. Ruhul, A.B.M.; Hossain, M.J.; Anwar, A.; Zaman, S. Cyber Attacks and Faults Discrimination in Intelligent Electronic Device-Based Energy Management Systems. *Electronics* **2021**, *10*, 650. [CrossRef]
3. Cao, J.; Wang, D.; Qu, Z.Y.; Cui, M.S.; Xu, P.C.; Xue, K.; Hu, K.W. A Novel False Data Injection Attack Detection Model of the Cyber-Physical Power System. *IEEE Access* **2020**, *8*, 95109–95125. [CrossRef]

4. Eryani, Y.A.; Baroudi, U. An Investigation on Detecting Bad Dat Injection Attack in Smart Grid. In Proceedings of the 2019 International Conference on Computer and Information Sciences (ICCIS), Sakaka, Saudi Arabia, 3–4 April 2019; pp. 1–4. [CrossRef]
5. Pei, C.; Xiao, Y.; Liang, W.; Han, X.J. A Deviation-Based Detection Method Against False Data Injection Attacks in Smart Grid. *IEEE Access* **2021**, *9*, 15499–15509. [CrossRef]
6. Tariq, M.; Ali, F.; Naeem, F.; Poor, H.V. Vulnerability Assessment of 6G-enabled Smart Grid Cyber-physical Systems. *IEEE Internet Things J.* **2020**, *7*, 5468–5475.
7. Chen, R.; Li, X.; Zhong, H.; Fei, M. A novel online detection method of data injection attack against dynamic state estimation in smart grid. *Neurocomputing* **2019**, *344*, 73–81. [CrossRef]
8. Karimipour, H.; Dinavahi, V. Robust Massively Parallel Dynamic State Estimation of Power Systems Against Cyber-Attack. *IEEE Access* **2018**, *6*, 2984–2995. [CrossRef]
9. Valverde, G.; Terzija, V. Unscented Kalman filter for power system dynamic state estimation. *IET Gener. Transm. Distrib.* **2011**, *5*, 29–37. [CrossRef]
10. Ganjkhani, M.; Badakhshan, S.; Shamshirband, S.; Kwok-Wing, C. A Novel Detection Algorithm to Identify False Data Injection Attacks on Power System State Estimation. *Energies* **2019**, *12*, 2209. [CrossRef]
11. Dang, L.; Chen, B.; Wang, S.; Ma, W.; Ren, P. Robust Power System State Estimation With Minimum Error Entropy Unscented Kalman Filter. *IEEE Trans. Instrum. Meas.* **2020**, *69*, 8797–8808. [CrossRef]
12. Zhao, J.; Mili, L. Robust Unscented Kalman Filter for Power System Dynamic State Estimation With Unknown Noise Statistics. *IEEE Trans. Smart Grid* **2019**, *10*, 1215–1224. [CrossRef]
13. Zheng, Z.; Zhao, J.; Mili, L.; Liu, Z. Robust Unscented Unbiased Minimum-Variance Estimator for Nonlinear System Dynamic State Estimation With Unknown Inputs. *IEEE Signal. Process. Lett.* **2020**, *27*, 376–380. [CrossRef]
14. ŽIvkoviĆ, N.; SariĆ, A. Detection of false data injection attacks using unscented Kalman filter. *J. Mod. Power Syst. Clean Energy* **2018**, *6*, 847–859. [CrossRef]
15. Attia, M.; Senouci, S.; Sedjelmaci, H.; Aglzim, E.H.; Chrenko, D. An efficient Intrusion Detection System against cyber-physical attacks in the smart grid. *Comput. Electr. Eng.* **2018**, *68*, 499–512. [CrossRef]
16. Gomez-Exposito, A.; Abur, A.; Jaen, A.d.; Gomez-Quiles, C. A Multilevel State Estimation Paradigm for Smart Grids. In Proceedings of the IEEE, Detroit, MI, USA, 24–28 July 2011; Volume 99, pp. 952–976. [CrossRef]
17. Anwar, A.; Mahmood, A.N. Vulnerabilities of Smart Grid State Estimation against False Data Injection Attack. *Renew. Energy Integr.* **2014**, *4*, 411–428.
18. Kimani, K.; Oduol, V.; Langat, K. Cyber security challenges for IoT-based smart grid networks. *Int. J. Crit. Infrastruct. Prot.* **2019**, *25*, 36–49. [CrossRef]
19. Jinping, H.; Piechocki, R.J.; Kaleshi, D.; Hau, C.W.; Zhong, F. Sparse Malicious False Data Injection Attacks and Defense Mechanisms in Smart Grids. *IEEE Trans. Ind. Inform.* **2015**, *11*, 1–12. [CrossRef]
20. Li, S.; Yilmaz, Y.; Wang, X. Quickest Detection of False Data Injection Attack in Wide-Area Smart Grids. *IEEE Trans. Smart Grid* **2015**, *6*, 2725–2735. [CrossRef]
21. Monticelli, A. Electric power system state estimation. In Proceedings of the IEEE, Salt Lake City, UT, USA, 8–13 October 2000; Volume 88, pp. 262–282. [CrossRef]
22. Ahmad, F.; Rasool, A.; Ozsoy, E.; Sekar, R.; Sabanovic, A.; Elitaş, M. Distribution system state estimation-A step towards smart grid. *Renew. Sustain. Energy Rev.* **2018**, *81*, 2659–2671. [CrossRef]
23. Ahmadi, N.; Chakhchoukh, Y.; Ishii, H. Power Systems Decomposition for Robustifying State Estimation under Cyber Attacks. *IEEE Trans. Power Syst.* **2020**, *3*, 1922–1933. [CrossRef]
24. Anagnostou, G.; Pal, B.C. Derivative-Free Kalman Filtering Based Approaches to Dynamic State Estimation for Power Systems With Unknown Inputs. *IEEE Trans. Power Syst.* **2018**, *33*, 116–130. [CrossRef]
25. Ashok, A.; Govindarasu, M.; Ajjarapu, V. Online Detection of Stealthy False Data Injection Attacks in Power System State Estimation. *IEEE Trans. Smart Grid* **2018**, *9*, 1636–1646. [CrossRef]
26. Brumback, B.; Srinath, M. A Chi-square test for fault-detection in Kalman filters. *IEEE Trans. Autom. Control.* **1987**, *32*, 552–554. [CrossRef]