J. Mod. Power Syst. Clean Energy (2018) 6(5):847–859
https://doi.org/10.1007/s40565-018-0413-5

Detection of false data injection attacks using unscented Kalman filter

Nemanja ŽIVKOVIĆ[1], Andrija T. SARIĆ[2]

Abstract It has recently been shown that state estimation (SE), which is the most important real-time function in modern energy management systems (EMSs), is vulnerable to false data injection attacks, due to the undetectability of those attacks using standard bad data detection techniques, which are typically based on normalized measurement residuals. Therefore, it is of the utmost importance to develop novel and efficient methods that are capable of detecting such malicious attacks. In this paper, we propose using the unscented Kalman filter (UKF) in conjunction with a weighted least square (WLS) based SE algorithm in real-time, to detect discrepancies between SV estimates and, as a consequence, to identify false data attacks. After an attack is detected and an appropriate alarm is raised, an operator can take actions to prevent or minimize the potential consequences. The proposed algorithm was successfully tested on benchmark IEEE 14-bus and 300-bus test systems, making it suitable for implementation in commercial EMS software.

Keywords State estimation, False data injection attack, Bad data detection, Unscented Kalman filter

CrossCheck date: 12 March 2018

Received: 18 July 2017 / Accepted: 12 March 2018 / Published online: 7 May 2018

✉ Andrija T. SARIĆ
asaric@uns.ac.rs

Nemanja ŽIVKOVIĆ
nemanja.zivkovic@schneider-electric-dms.com

[1] Schneider Electric DMS NS, Novi Sad 21000, Serbia

[2] Department of Power, Electronic and Telecommunication Engineering, Faculty of Technical Sciences, University of Novi Sad, Novi Sad 21000, Serbia

1 Introduction

Due to the ever-increasing reliance on modern cyber infrastructures in power systems, cyber security has recently been considered to be among the most important issues in modern power systems. Supervisory control and data acquisition (SCADA) systems are vulnerable to attacks that are directed not only at data communication infrastructures but also to those directed at control centers and even remote terminal units (RTUs). The SCADA communication network is very diverse and consists of fiber optics, microwave and satellite connections, while the exchanged data is often unencrypted - leaving substantial space for potential attacks. Even though phasor measurement unit (PMU) based measurements are regarded as generally more secure than SCADA measurements, they are also susceptible to malicious attacks, as explained in [1]. For example, it was stated in [2] that among 245 reported incidents - the energy sector led all others with 79 (32%) incidents. A large number of those threats targeted SCADA devices with the intention of gaining unauthorized access. Earlier, an experimental attack was conducted by the researchers at the US Department of Energy's Idaho Lab, which resulted in the self-destruction of one generating unit, emphasizing the impact of cyber threats [3]. State estimation (SE), which is among the most important real-time applications of commercial energy management system (EMS) software, is thus indirectly vulnerable to cyber-attacks, which may result in severe system instability, suboptimal operation, financial losses, and even loss of human life.

To identify and remove bad measurements—so they cannot compromise the accuracy of estimated results, bad data detection (BDD) algorithms have been devised as an integral part of SE algorithms [4]. In the early BDD

algorithms, after the existence of bad measurements was confirmed, only the single measurement with the largest normalized residual was removed in one iteration of the SE algorithm. Multiple loops were needed until all bad measurements were eliminated and the detection test was passed. Later, a new approach was devised, in which multiple bad measurements were identified and removed at the same time, thus substantially reducing the SE execution time [4]. Both of these algorithms, which are presented in [4], rely on normalized residual techniques and show good results only in cases of independent and non-interacting bad measurements.

For correlated bad measurements, novel techniques have been developed, including hypothesis testing identification (HTI), which again relies on normalized residuals [5]. This and similar techniques are still among the most commonly used in commercial EMS software. However, the concept of "false data injection (FDI)" attacks was recently introduced in [6], proving that measurements can be manipulated in a way that does not trigger SE BDD modules. Given the knowledge of the system configuration and element parameters, an attacker can create undetectable malicious attacks. The development of techniques for identification and mitigation of such attacks is essential for the secure operation of large power grids.

The substantial amount of research carried out on FDI attacks can be classified into three categories.

1) Vulnerability of SE. The weaknesses of BDD algorithms have been explored from the perspective of an attacker as well as ways to construct malicious attacks with minimal resources and maximum impacts on power grids [6–18]. Although network topology and electric parameters are regarded as completely or partially known by the attacker, in some research [6, 10], they were not required, whereas others relied only on the measurement matrix [13–18].
2) Consequences of an FDI attack. FDI attacks on SE have been analyzed from the perspective of EMS applications such as contingency analysis, optimal power flow and automatic generation control [19–22].
3) Countermeasures development. These studies have focused on the detection of stealthy attacks and protection of the power system. New enhanced BDD algorithms have been proposed, optimal PMU placement strategies created, and discussions undertaken regarding ways to improve the protection of communication systems [12, 23–34].

In [30], Kullback-Leibler distance was proposed for tracking the dynamics of measurement variations to detect FDI attacks. The statistical behavior of the state estimation process, through cumulative sum based approach (CUSUM), was used for FDI attacks detection in [31]. Method based on the short-term state forecasting which considers temporal correlations between nodal states was proposed in [32]. Detection scheme using two physical system parameters and their behavior was proposed in [33]. In [34] to detect FDI attacks, a cosine similarity matching technique was used and tested in power systems for which estimated (expected) measurement values were obtained using a Kalman filter, by comparing them with actual measurements. The underlying SE observation model was regarded as linear, as was the state transition matrix (approximated by the identity matrix), enabling a Kalman filter to be used for SE.

However, in most commercial SE algorithms, the utilized measurement observation model is highly nonlinear, especially regarding the line current and transformer tap position measurements, implying the possible use of Kalman filter extensions intended for nonlinear systems - extended or unscented Kalman filters (EKF or UKF, respectively). Kalman filtering techniques were first proposed for use in dynamic state estimation in [35], and significant efforts have been subsequently undertaken to improve their performance [36–41]. In an EKF, which is probably the most widely used dynamic SE algorithm, the state distribution is approximated by Gaussian random variables (GRVs), which are propagated through a "first order" linearization of the nonlinear system, and EKF can therefore be seen as "first order" approximation of the optimal filter [36]. Enhancements to the EKF were proposed in [37, 38] to improve its performance and robustness by incorporating the high nonlinearity of measurement functions. Furthermore, an iterated EKF based on the generalized maximum likelihood approach was proposed in [39] to estimate dynamic states during disturbances. In [40], a UKF was introduced as a tool for dynamic state estimation, through a combination an unscented transformation and Kalman filter. In the UKF technique, the minimal set of selected sample points, which capture the true mean and covariance of the GRVs, is transferred through the complete nonlinear system, obtaining the posterior mean and covariance from the "third order" approximation of the optimal filter [41].

In this paper, we investigated the detection of FDI attacks by using a UKF to predict and update SVs starting from the previously known state and compared them with the results acquired from a typically used WLS-based SE algorithm. It should be noted that the UKF used in the proposed algorithm can be replaced by other nonlinear filters without any structural changes. We show that the SVs under attack significantly deviated between the UKF and WLS-based SE. The measurements influencing the suspicious SVs are those that may be under malicious attack.

The main contributions of the proposed method are as follows: ① a derivation of the time-variant transition function (necessary for the UKF prediction step) by a combination of power flow equations with load/generation

very short-term forecasts and generator schedules; ② false data detection using the normalized SV residuals obtained from WLS-based SE and UKF estimates, as well as the UKF state covariance matrix; ③ an analysis of the most critical scenario, where the attacker may gain access to the complete network model and set of measurements; ④ the efficient synergy of WLS-based SE and UKF algorithms for the real-time (online) detection of FDI attacks.

The paper is organized as follows. In Section 2, we formulate the problem of detecting FDI attacks, in which the advisory agent has an unlimited number of resources at its disposal. In Section 3, the proposed UKF based detection algorithm is explained, and the BDD process using UKF and SE results is covered in Section 4. The results of numerical simulations for benchmark power systems (with 14 and 300 buses), empowered with the data needed for forecast analysis, are provided in Section 5, and concluding remarks are presented in Section 6. The algorithmic details of the UKF are provided in Appendix A.

2 Problem formulation

We consider a scenario in which an attacker has gained access to an unlimited number of measurements by breaking into a SCADA system (Case 2 in Fig. 1), primary domain controller (PDC) (Case 5) and control center, or by directly tampering with the PMUs (Case 4), RTUs (Case 3) and communications network (Case 1).

With the idea of analyzing the most critical scenario, which may not be the most typical and frequent in practice, we suppose that the attacker has sufficient knowledge of the power system (topology and physics) as described by a nonlinear SE measurements-SVs model

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

or by a linear SE model (assumed only for analysis in this section)

$$\boldsymbol{z} = \boldsymbol{H}\boldsymbol{x} + \boldsymbol{e} \tag{2}$$

where $\boldsymbol{z}$ and $\boldsymbol{x}$ are the M-dimensional measurement ($z_j \in \boldsymbol{R}^{M\times 1}$) and N-dimensional state vectors ($x_i \in \boldsymbol{R}^{N\times 1}$), M and N are the total number of measurements and SVs; $\boldsymbol{h}(\boldsymbol{x})$ is the vector of nonlinear functions of the system state vector $\boldsymbol{x}$ – observation model function; $\boldsymbol{e}$ is the measurement error vector (assumed to be zero mean multivariate Gaussian noise with covariance $\boldsymbol{R}$); $\boldsymbol{H}$ is the Jacobian matrix and $\boldsymbol{H} = \frac{\partial \boldsymbol{h}(\boldsymbol{x})}{\partial \boldsymbol{x}}$.

2.1 Analysis of compromised measurement cases

Typically, the goal of an attacker is to change either the SV(s) (x_i) to the desired value by δx_i or to change some particular measurement (probably power flow) to an arbitrary scalar value. To change specific measurements and remain undetected by the conventional bad data detection algorithms, the adversary would need to modify the corresponding SV (the one affecting the desired power flow measurement, and a minimum number of other measurements). Therefore, without loss of generality, we suppose that SV will be changed as a goal of the attack.

When we assume a realistic scenario where an attacker cannot obtain access to every measurement in the system (some can be regarded as secure), the measurements can be divided into two groups: ①fully protected measurements ($1, 2, \cdots, m$), denoted by '*'; ② unprotected measurements ($1, 2, \cdots, M-m$).

The measurement vector $\boldsymbol{z}$ can then be written as:

$$\boldsymbol{z} = \begin{bmatrix} z_1^* \\ \vdots \\ z_m^* \\ z_1 \\ \vdots \\ z_{M-m} \end{bmatrix} \tag{3}$$

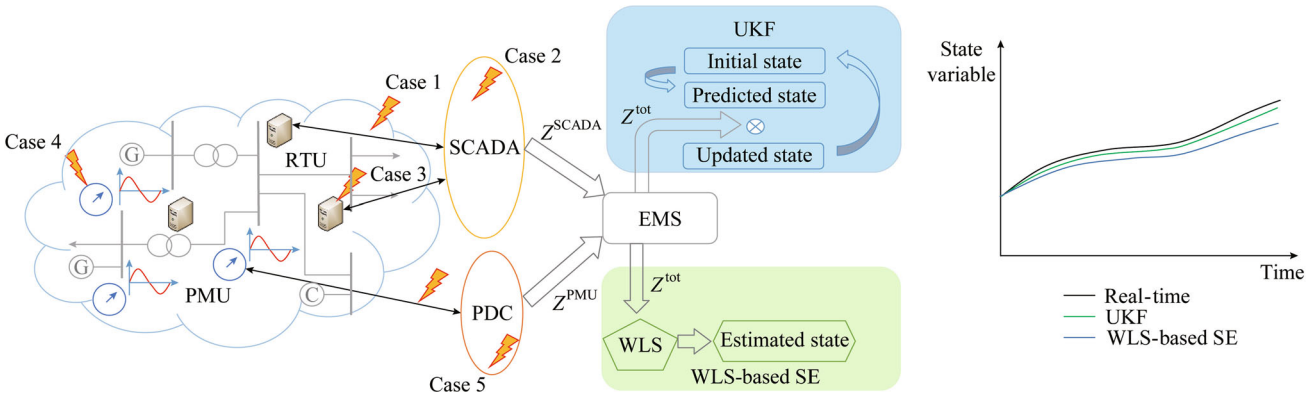


Fig. 1 FDI attack detection by comparing WLS-based SE and UKF results

Likewise, the state vector can be divided into the protected SVs that correspond to at least one of the secure measurements (x_k^*) and the unprotected ones (x_{N-k} is the total k SV which is fully protected – subvector x_k^* in (4)), where all the corresponding measurements may be compromised.

If the attacker plans to change the i^{th} SV (x_i) by δx_i while remaining undetected, then all the measurements corresponding to the rows with non-zero elements (total ℓ measurements) in the ith column of matrix $\boldsymbol{H}$ need to be changed ($z_\ell + \delta z_\ell$). The attacker can change only the unprotected SVs (x_{N-k}) without detection because all the corresponding measurements are those that can be tampered with z_{M-m} (the measurement error vector $\boldsymbol{e}$ in (2) is ignored).

$$\begin{bmatrix} z_1^* \\ \vdots \\ z_m^* \\ z_1 \\ \vdots \\ z_\ell + \delta z_\ell \\ \vdots \\ z_{M-m} \end{bmatrix} = \begin{bmatrix} \cdots & H_{1i} & \cdots \\ & \vdots & \\ \cdots & H_{ii} & \cdots \\ & \vdots & \\ \cdots & H_{Mi} & \cdots \end{bmatrix} \begin{bmatrix} x_1^* \\ \vdots \\ x_k^* \\ x_1 \\ \vdots \\ x_i + \delta x_i \\ \vdots \\ x_{N-k} \end{bmatrix} \tag{4}$$

The Jacobian matrix used by an adversary may be represented as a sum of the actual Jacobian $\boldsymbol{H}$ and some increment $\delta\boldsymbol{H}$ that is used to encapsulate all the uncertainties the attacker may have. The measurement-SVs model with multiple SVs under attack ($\boldsymbol{x}_{N-k}$) can now be written as:

$$\begin{aligned} \begin{bmatrix} \boldsymbol{z}_m^* \\ \boldsymbol{z}_{M-m} \end{bmatrix} &= \begin{bmatrix} \boldsymbol{H}_{m,k} & \boldsymbol{H}_{m,N-k} & \boldsymbol{0} \\ \boldsymbol{H}_{M-m,k} & \boldsymbol{H}_{M-m,N-k} & \boldsymbol{H}_{M-m,N-k} + \delta\boldsymbol{H}_{M-m,N-k} \end{bmatrix} \\ &\quad \times \begin{bmatrix} \boldsymbol{x}_k^* \\ \boldsymbol{x}_{N-k} \\ \delta\boldsymbol{x}_{N-k} \end{bmatrix} \\ &= \begin{bmatrix} \boldsymbol{H}_{m,k} & \boldsymbol{H}_{m,N-k} \\ \boldsymbol{H}_{M-m,k} & \boldsymbol{H}_{M-m,N-k} \end{bmatrix} \begin{bmatrix} \boldsymbol{x}_k^* \\ \boldsymbol{x}_{N-k} \end{bmatrix} \\ &\quad + \begin{bmatrix} \boldsymbol{0} \\ (\boldsymbol{H}_{M-m,N-k} + \delta\boldsymbol{H}_{M-m,N-k})\delta\boldsymbol{x}_{N-k} \end{bmatrix} \\ &= \begin{bmatrix} \boldsymbol{H}_{m,k} & \boldsymbol{H}_{m,N-k} \\ \boldsymbol{H}_{M-m,k} & \boldsymbol{H}_{M-m,N-k} \end{bmatrix} \begin{bmatrix} \boldsymbol{x}_k^* \\ \boldsymbol{x}_{N-k} \end{bmatrix} \\ &\quad + \begin{bmatrix} \boldsymbol{0} & \boldsymbol{0} \\ \boldsymbol{H}_{M-m,N-k} & \boldsymbol{1} \end{bmatrix} \begin{bmatrix} \delta\boldsymbol{x}_{N-k} \\ \delta\boldsymbol{H}_{M-m,N-k}\delta\boldsymbol{x}_{N-k} \end{bmatrix} \\ &= \begin{bmatrix} \boldsymbol{H}_{m,k} & \boldsymbol{H}_{m,N-k} & \boldsymbol{0} & \boldsymbol{0} \\ \boldsymbol{H}_{M-m,k} & \boldsymbol{H}_{M-m,N-k} & \boldsymbol{H}_{M-m,N-k} & \boldsymbol{1} \end{bmatrix} \begin{bmatrix} \boldsymbol{x}_k^* \\ \boldsymbol{x}_{N-k} \\ \delta\boldsymbol{x}_{N-k} \\ \delta\boldsymbol{z}_{M-m} \end{bmatrix} \end{aligned} \tag{5}$$

where $\delta\boldsymbol{z}_{M-m} = \delta\boldsymbol{H}_{M-m,N-k}\delta\boldsymbol{x}_{N-k}$ and $\boldsymbol{1}$ is an identity matrix.

Note that in (5), the state vector has been expanded with the additional sets of variables ($\delta\boldsymbol{x}_{N-k}$ and $\delta\boldsymbol{z}_{M-m}$) that, represent malicious SV changes and measurement changes (resulting as a consequence of the attacker's incomplete knowledge of Jacobian matrix $\boldsymbol{H}$), respectively.

Unfortunately, the resulting set of (5) is generally undetermined and cannot be solved even for the simplest scenario with the maximum measurement redundancy ($M > 3N$) and only one SV under attack (x_i) – irrespective of the size of $\boldsymbol{x}_k^*$. Therefore, a WLS-based SE cannot by itself be enhanced to detect FDI attacks but only in synergy with some other method. In consequence, a new algorithm that combines a WLS-based SE and forecast based UKF is proposed in Section 3.

2.2 Nonlinear problem formulation

Based on the analysis provided in Section 2.1, a critical case wherein all the measurements are susceptible to attacks ($m = 0$ and $k = 0$ in (4)) is considered. Let $\delta\boldsymbol{z}$ be the non-zero false data attack vector from (4) that is created by the adversary, who has a complete knowledge of the nonlinear observation model function $\boldsymbol{h}(\boldsymbol{x})$. The modified set of measurements can then be written as:

$$\boldsymbol{z}' = \boldsymbol{z} + \delta\boldsymbol{z} + \boldsymbol{e} = \boldsymbol{h}(\boldsymbol{x} + \delta\boldsymbol{x}) + \boldsymbol{e} = \boldsymbol{h}(\boldsymbol{x}') + \boldsymbol{e} \tag{6}$$

The typically used BDD techniques are based on a normalized residual approach, where the ℓ^2-norm of the measurement residual is compared against a threshold τ.

$$\|\boldsymbol{z}' - \boldsymbol{h}(\boldsymbol{x}')\| = \|\boldsymbol{h}(\boldsymbol{x} + \delta\boldsymbol{x}) + \boldsymbol{e} - \boldsymbol{h}(\boldsymbol{x} + \delta\boldsymbol{x})\| = \|\boldsymbol{e}\| < \tau \tag{7}$$

Therefore, malicious attacks created in this manner cannot be detected using standard BDD techniques [6].

3 Proposed algorithm

A flow-chart of the proposed algorithm for the detection of FDI attacks is shown in Fig. 2, wherein the different steps are described in sequence.

3.1 UKF-based states prediction and update

The prediction of the SVs from the $(k-1)^{\text{th}}$ time instant to the those at the k^{th} time instant

$$\boldsymbol{x}_{k|k-1} = \boldsymbol{f}(\boldsymbol{x}_{k-1}) + \boldsymbol{w}_k \tag{8}$$

is performed by the UKF prediction step (described briefly in Appendix A), where the linearized transition

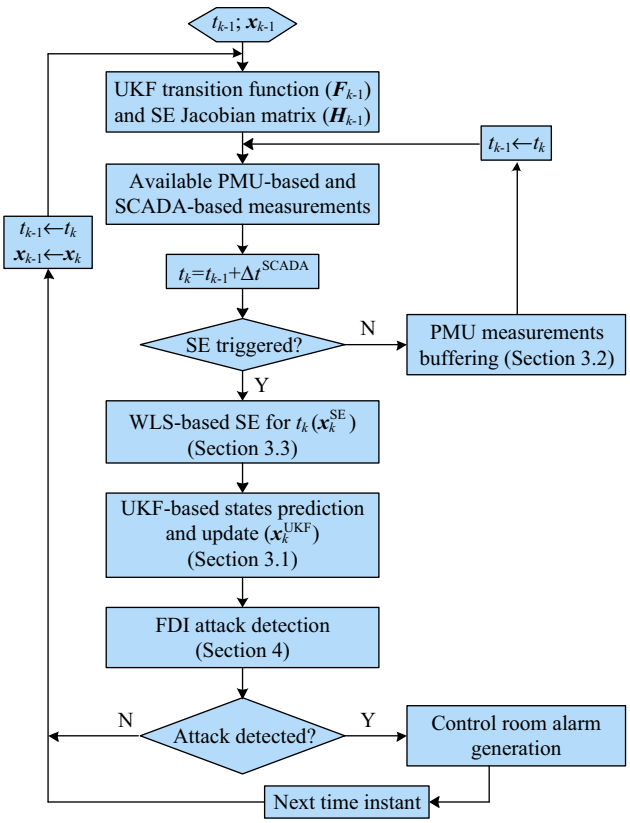


Fig. 2 Proposed algorithm for detection of FDI attack

model can be derived from increments to the power flow equations:

$$\begin{bmatrix} \Delta \boldsymbol{P} \\ \Delta \boldsymbol{Q} \end{bmatrix} = \begin{bmatrix} \Delta \boldsymbol{P}_g - \Delta \boldsymbol{P}_p \\ \Delta \boldsymbol{Q}_g - \Delta \boldsymbol{Q}_p \end{bmatrix} = \begin{bmatrix} \boldsymbol{E} & \boldsymbol{T} \\ \boldsymbol{K} & \boldsymbol{L} \end{bmatrix} \begin{bmatrix} \Delta \boldsymbol{\theta} \\ \Delta \boldsymbol{V} \end{bmatrix} = \boldsymbol{J} \Delta \boldsymbol{x} \tag{9}$$

where $\boldsymbol{E}$, $\boldsymbol{T}$, $\boldsymbol{K}$, $\boldsymbol{L}$ are corresponding submatrices of Jacobian matrix $\boldsymbol{J}$ for the power flow equations, with elements $E_{ij} = \frac{\partial P_i}{\partial \theta_j}\Big|_{\theta_0, V_0}$, $T_{ij} = \frac{\partial P_i}{\partial V_j}\Big|_{\theta_0, V_0}$, $K_{ij} = \frac{\partial Q_i}{\partial \theta_j}\Big|_{\theta_0, V_0}$ and $L_{ij} = \frac{\partial Q_i}{\partial V_j}\Big|_{\theta_0, V_0}$. Note that the only equation for active and reactive power in the Slack-bus is excluded ($i, j \neq Slack$), because $\theta_{Slack} = 0$.

For the assumed constant power factor ($\cos \varphi$), we have:

$$\begin{bmatrix} \Delta \boldsymbol{P} \\ \Delta \boldsymbol{Q} \end{bmatrix} = \begin{bmatrix} \Delta \boldsymbol{P} \\ \tan \varphi \Delta \boldsymbol{P} \end{bmatrix} \tag{10}$$

where

$$\Delta P_i = s_i P_{k-1,i} \tag{11}$$

and $P_{k-1,i}$ represents the per unit injection change (referenced to the base case values (1 p.u.) at time instant t_{k-1}) taken from the active power generation/load curve, whereas s_i represents the correlation coefficient between ΔP_i and $P_{k-1,i}$, which is also obtained from the generation/load curve. These curves are acquired as a result of the application of short-term forecasts and generator schedules.

Finally, we obtain the following time-variant transition model for UKF

$$\boldsymbol{x}_k = \boldsymbol{x}_{k-1} + \Delta \boldsymbol{x} = \boldsymbol{x}_{k-1} + \boldsymbol{J}_{k-1}^{\text{inv}} \begin{bmatrix} \Delta \boldsymbol{P} \\ \tan \varphi \Delta \boldsymbol{P} \end{bmatrix} \tag{12}$$

or

$$\boldsymbol{x}_k = \boldsymbol{F}_{k-1} \boldsymbol{x}_{k-1} \tag{13}$$

where $\boldsymbol{F}_{k-1} = \boldsymbol{1} + (\boldsymbol{J}_{k-1}^{\text{inv}})'$is the linearized UKF transition function. The elements of the $(\boldsymbol{J}_{k-1}^{\text{inv}})'$ matrix are defined as:

$$(\boldsymbol{J}_{k-1,ij}^{\text{inv}})' = J_{k-1,ij}^{\text{inv}} \frac{s_i P_{k-1,i}}{x_{k-1,i}} \tag{14}$$

The derived transition function is generally a full matrix, because changes in load and generation buses influence multiple SVs. Being time-varying, it captures sudden load/generation changes in power systems to a much higher degree than constant transition functions.

The update step of the UKF is then performed using a highly non-linear observation model $\boldsymbol{h}(\boldsymbol{x})$ acquired with the WLS-based SE algorithm, as explained in Appendix A.

3.2 PMU measurement buffering

The state estimation calculation is usually triggered either periodically at periods of 1-5 minutes or after a topological or significant analogue measurement change. Depending on the SCADA pooling time and measurement dynamics, the expected SE triggering period is usually 30 seconds to 1 minute – which is much longer than the refresh rates of PMU-based measurements. Due to these differences, measurement buffering was proposed in [42] For N^{PMU} measurements that arrive in the time interval between two WLS-based SE executions ($t_{k-1} \leq t_i \leq t_{k-1} + \Delta t^{\text{SE}}$) the mean and variance respectively, are

$$\mu_z = \frac{1}{N^{\text{PMU}}} \sum_{i=1}^{N^{\text{PMU}}} z(t_i) \tag{15}$$

$$\text{var}(\mu_z) = \frac{1}{(N^{\text{PMU}})^2} \sum_{i=1}^{N^{\text{PMU}}} \text{var}\{z(t_i)\} = \frac{\sigma^2}{N^{\text{PMU}}} \tag{16}$$

3.3 WLS-based SE

Because the SE model is nonlinear, the function $\boldsymbol{h}(\boldsymbol{x})$ is linearized and the resulting linearized SE is formulated as a WLS problem. The WLS estimator minimizes the objective function by satisfying the first-order optimality conditions.

$$\frac{\partial \boldsymbol{j}(\boldsymbol{x})}{\partial \boldsymbol{x}} = 0 \tag{17}$$

where $\boldsymbol{j}(\boldsymbol{x}) = \Delta \boldsymbol{z}^{\mathrm{T}} \boldsymbol{R}^{-1} \Delta \boldsymbol{z}$ is the objective function; $\Delta \boldsymbol{z} = \boldsymbol{z} - \boldsymbol{h}(\boldsymbol{x})$ is the vector of measurement residuals; $\boldsymbol{R}$ is the covariance matrix of measurement error vector.

The minimization problem can be solved using an iterative scheme, changing the point of linearization (for simplicity, the iteration index is removed).

$$(\boldsymbol{H}^{\mathrm{T}} \boldsymbol{R}^{-1} \boldsymbol{H}) \Delta \hat{\boldsymbol{x}} = \boldsymbol{H}^{\mathrm{T}} \boldsymbol{R}^{-1} \Delta \boldsymbol{z} \tag{18}$$

$$\boldsymbol{x} = \boldsymbol{x} + \Delta \hat{\boldsymbol{x}} \tag{19}$$

$$\hat{\boldsymbol{z}} = \boldsymbol{h}(\boldsymbol{x} + \Delta \hat{\boldsymbol{x}}) \tag{20}$$

where the Jacobian matrix $\boldsymbol{H}$ is assumed to be constant inside one SE cycle.

4 FDI attack detection using UKF

Knowing the initial network condition at time instant k-1 (vector of SVs $\boldsymbol{x}_{k-1}$) and assuming that the forecasted data are available for all the power consumers and generators for the following time instant k, a UKF can be used to determine the network condition on the basis of the transition matrix and available telemetered measurements. A transition matrix ($\boldsymbol{F}_{k-1}$) can be created using forecasted data, as part of load flow calculation for future time instant k using (10)-(14).

In a commercial EMS environment, an SE calculation is usually triggered in four ways: ① periodically, on user defined time intervals that are primarily in the range of 1–5 minutes; ② after significant analogue measurement(s) change(s); ③ after every topological or change in transformer tap position; ④ on the request of a user. Therefore, it can be expected that the period between time instants $k - 1$ and k is no longer than 5 minutes. For such short time periods, it can be assumed that the trust factor for the forecasted injections (generations minus loads) is high, resulting in small values of the process noise vector $\boldsymbol{w}_k$ in (A1).

When an FDI attack occurs, the maliciously changed group of measurements would swing the estimates of the SV(s) provided by the WLS-based SE algorithm in the desired direction. On the other hand, the estimates acquired from the UKF would only partially swing, due to the binding effect of the transition matrix ($\boldsymbol{F}_{k-1}$) and the small process noise vector ($\boldsymbol{w}_k$).

For the purpose of detecting FDI attacks and identifying false data, a normalized SV residuals based approach is proposed. A normalized SV residual (r_i) is calculated as the absolute value of a difference between a SV value estimated by the WLS-based SE (x_i^{SE}) and that calculated by the UKF (x_i^{UKF}) divided by the standard deviation acquired from the UKF covariance matrix $\boldsymbol{C}$ in (A4).

$$r_i = \frac{\left| x_i^{\mathrm{SE}} - x_i^{\mathrm{UKF}} \right|}{\sqrt{C_{i,i}}} \qquad i = 1,\ 2, \cdots, N \tag{21}$$

It should be noted that the traditional BDD algorithms, which are typically based on the normalized measurement residuals, are used to filter out bad measurements in both the WLS-based SE and UKF in the proposed algorithm. These filtered estimates are later used to calculate the residuals (21).

To determine whether the regarded SVs are under attack, the normalized SV residuals (r_i in (21)) are compared to a predefined threshold. When an FDI attack is confirmed, the proposed algorithm generates an alarm in the control room to warn a system operator.

Because the proposed method relies on forecast results, false positive detections may occur. Note that false positives are the cases where the proposed algorithm detects an attack although there is none, and false negatives are the cases when the algorithm fails to detect an existing attack. Detection depends on the specified threshold, which should provide the minimum number of false positives and false negatives. Threshold selection is very important because higher threshold values would tolerate larger forecast errors, while at the same time limiting the minimum attack intensity that could be detected. Lower threshold values would, on the other hand, increase the probability of false positive detections. Being system oriented and forecast quality dependent, the following steps are proposed for threshold definition:

1) Generation of daily-based load curves obtained from the application of very short-term load forecasts for multiple day types (week day, weekend, and holiday) and seasons (spring, summer, autumn, and winter).
2) Iterative adjustment (decrease/increase) of the threshold value, starting from the initial one.
3) Application of FDI attacks of different intensities.
4) Attack detection using the proposed algorithm.

Only sudden changes in generation/load, that are not captured in a very short-term forecast as well as unplanned system events such as equipment outages (for example, overhead line outages), could produce differences between UKF and WLS-based SE estimates that are not the consequence of a malicious attack and would therefore lead to false positive detections. However, such detections could easily be disregarded after the system operator becomes aware of them. Orchestrating FDI attacks during such unplanned events to evade detections is regarded as highly unlikely. An attacker would need to have access to all the measurements in the region over a long period and then

attack one of the SVs affected by the outage during a short time frame (inside a 5 minute' interval, before the next execution of a very short-term forecast).

5 Application

To evaluate the proposed algorithm, simulations were conducted on the modified 14-bus test system [43] shown on Fig. 3, and on an IEEE 300-bus test system [44]. The SVs calculated using the WLS-based SE and UKF were compared in cases with and without a malicious attack on the smaller 14-bus test system. On the same system, the sensitivity of the algorithm to different transition process noise values was tested. The ability of the proposed method to detect attacks of different intensities and its sensitivity to forecast accuracy was demonstrated on the 300-bus test case.

5.1 Modified 14-bus test system

A single-line diagram of the modified 14-bus test system is shown in Fig. 3. Compared to the original model in [43], generation was removed from buses 3 and 6 and added to buses 5, 11 and 13. The types of all the generating units and utilized daily load curves are specified in Fig. 3. The initial voltage phasors and nodal active and reactive power injections were also slightly changed from their original values to compensate for the addition/removal of generating units shown in Table 1.

High measurement redundancy was assumed (with active and reactive power flow measurements on all branches, shunt power injection measurements, and voltages at every bus). PMU-based voltage measurements were placed on the generator (generation, PV and slack) buses. Forecasted generation curves for solar and wind units, and schedules for thermal and hydro units were used in Fig. 4 in conjunction with forecasted load curves in Fig. 5 to estimate near-term network condition.

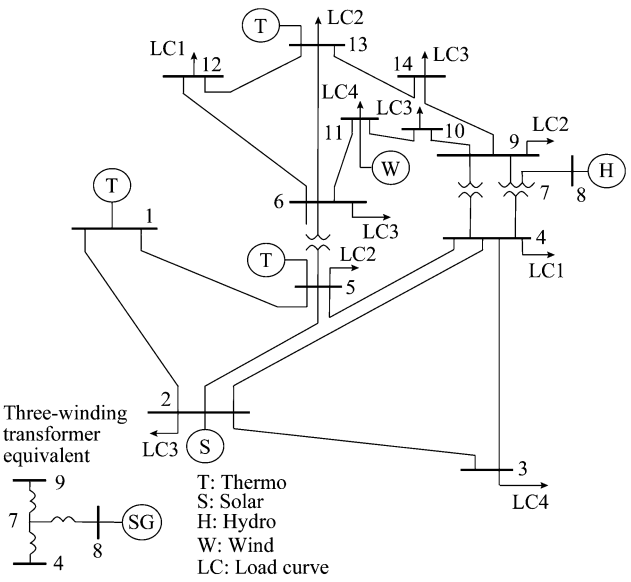


Fig. 3 Single-line diagram of modified 14-bus test system

In Fig. 6, the WLS-based SE and UKF estimated voltage magnitudes at bus 12 (load, PQ bus) were plotted for the analyzed 6-hour period when no attack was introduced. Estimation calculations were conducted every 30 seconds, which is an expected average SE sampling period for utilities with modern EMSs. The maximum normalized residuals for all the voltage magnitudes are shown on the figure as well. It can be easily concluded that as the UKF estimates followed the WLS-based SE estimates, the normalized residuals were below the predefined threshold, and no FDI attack was detected.

An FDI attack aimed at the voltage at bus 12 was started after 1 hour, as shown in Fig. 7. The intensity of the voltage magnitude change targeted by the attacker was 0.1 p.u. It can be observed that although the WLS-based SE calculated voltage immediately reached the targeted voltage, the voltage calculated by the UKF only reached the targeted value after more than one hour, thus enabling the FDI attack to be detected, which can be seen by analysing the maximum normalized residuals over time.

The influence of the process noise vector, $\boldsymbol{w}_k$ in (A1), was also analysed, and was determined to be critical to the FDI detection process. In Fig. 8, the UKF estimated voltages for three different process noise values were plotted;

Table 1 Active and reactive power injections into system buses

Bus number	Load		Generation	
	Active (MW)	Reactive (Mvar)	Active (MW)	Reactive (Mvar)
1	0.0	0.0	232.4	1.2
2	21.7	12.7	40.0	29.5
3	94.2	19.0	0.0	0.0
4	47.8	− 3.9	0.0	0.0
5	7.6	1.6	30.0	3.9
6	11.2	7.5	0.0	0.0
7	0.0	0.0	0.0	0.0
8	0.0	0.0	40.0	38.8
9	29.6	16.6	0.0	0.0
10	9.0	5.8	0.0	0.0
11	3.5	1.8	35.0	4.4
12	6.1	1.6	0.0	0.0
13	13.5	5.8	20.0	25.9
14	14.9	5.0	0.0	0.0

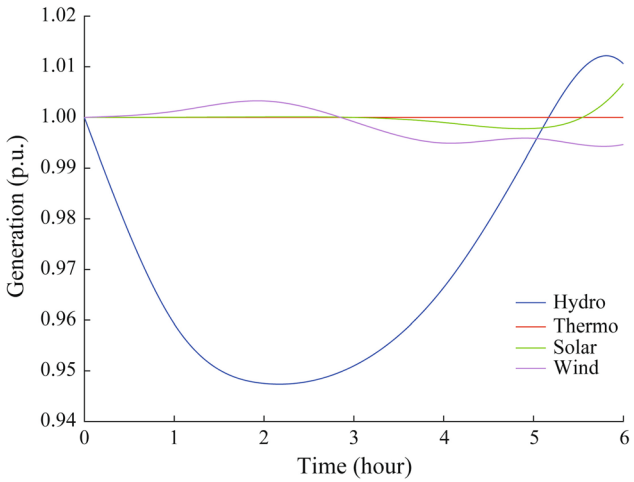


Fig. 4 Forecasted generation curves

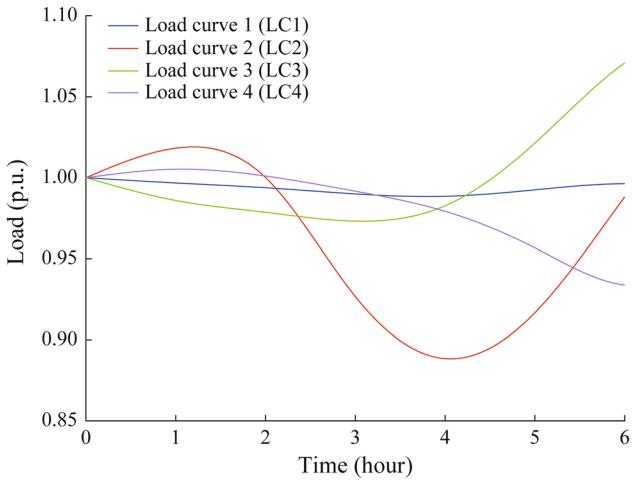


Fig. 5 Forecasted daily load curves

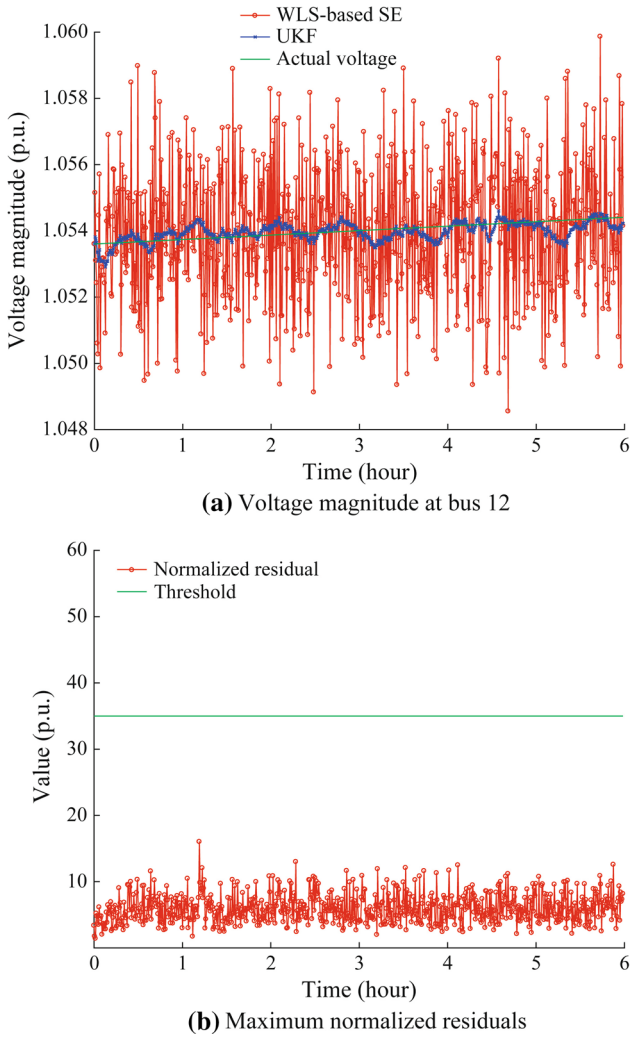


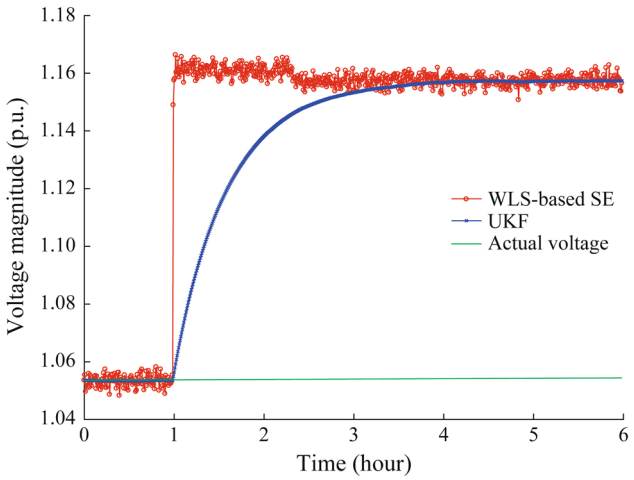
Fig. 6 Obtained results for modified 14-bus test system without FDI attack

the smallest process noise was 10 times smaller than the medium process noise and 100 times smaller than the largest process noise.

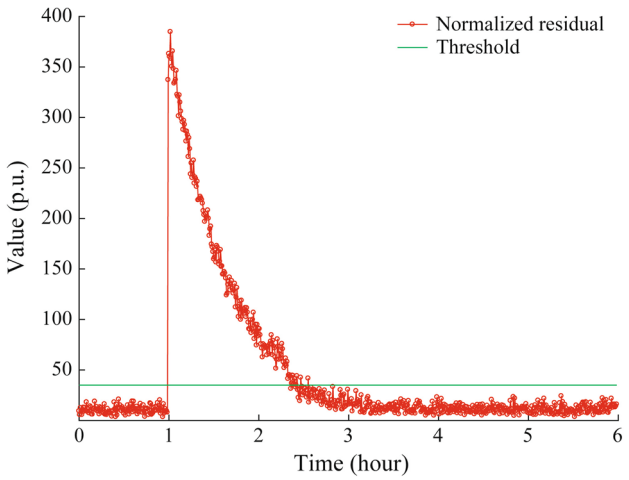
From the presented results, it was concluded that for large process noise, the UKF results closely followed the WLS-based SE estimates, thus reducing the time available for FDI attack detection, whereas for lower process noise, the differences between the WLS-based SE and UKF results were much more significant and remained so for longer periods of time. This conclusion emphasizes the necessity for high-quality generation and load forecasts, and for short SE execution periods.

5.2 IEEE 300-bus test system

Furthermore, FDI attacks of different intensities were aimed at bus 4 (load, PQ type), which affected all the necessary measurements to change the SE results without being detected by the typically used BDD algorithms. The voltages estimated using the WLS-based SE method in the first execution after the attack commenced were compared with those acquired from the UKF, as shown in Table 2. It was concluded that for attacks of greater strength (targeted malicious voltage magnitude changes in p.u.), the differences between the WLS-based SE and UKF estimates were significant, as was the normalized residual, which overtopped the defined threshold by almost 20 times. The maximum normalized residuals decreased with decreasing attack intensity - the 0.01 p.u. attack was the last to be successfully detected (last row in Table 2). Depending on the accuracy of measurement equipment in the power system, voltage magnitudes may be estimated using the WLS-based SE algorithm alone, with errors exceeding 1% (even in the absence of a malicious attack). The consequences of such errors are minor, which leads to the conclusion that the proposed method is instantly capable of



(a) Voltage magnitude at bus 12



(b) Maximum normalized residuals

Fig. 7 Obtained results for modified 14-bus test system with an FDI attack starting after one hour

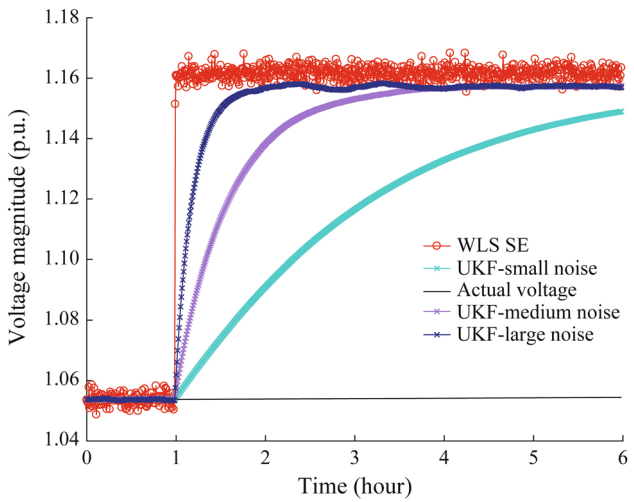


Fig. 8 UKF estimated voltages at bus 12 using three different process noise values

Table 2 Detection of FDI attacks of different strengths

Attack strength	WLS-based SE	UKF	Actual voltage	Maximum normalized residual
0.200	1.1831	1.0907	1.0254	957.32
0.150	1.1487	1.0722	1.0254	775.87
0.100	1.1129	1.0548	1.0254	577.26
0.050	1.0718	1.0389	1.0254	319.65
0.025	1.0495	1.0319	1.0254	169.32
0.010	1.0347	1.0278	1.0254	65.81

Table 3 Detection of FDI attacks for different forecast accuracies

MAPE (%)	Maximum normalized residual (p.u.)	Minimum attack strength (p.u.)
0	17.4	0.010
0.2	22.7	0.010
0.4	36.1	0.010
0.6	68.4	0.020
0.8	140.3	0.025
1.0	234.8	0.040

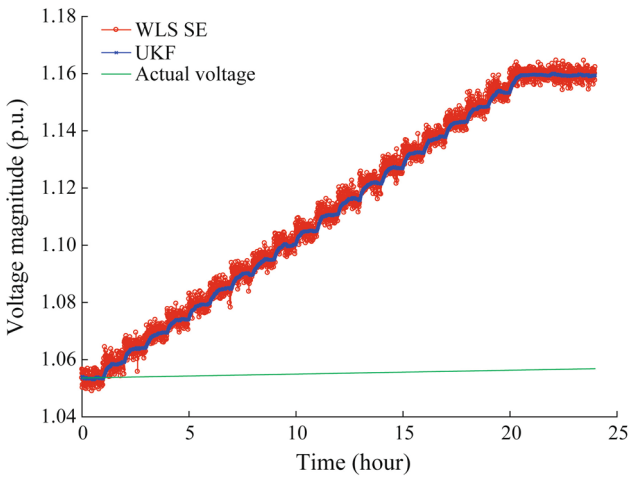
detecting any FDI attack that may create significant consequences to the network operation.

In addition, the sensitivity of the proposed method was tested against different very short-term forecast accuracies. The expected mean absolute percentage error (MAPE) for very short-term forecast (5-minute in advance) in the modern EMS systems is significantly lower than 1%. Therefore, the maximum normalized SV residuals in the absence of an FDI attack were obtained for forecast accuracies ranging from 0% to 1% MAPE, as shown in Table 3. The minimum strengths of the FDI attacks that were successfully detected without triggering any false positive detections (see in Table 3) expectedly increased with the increase of forecast MAPE. However, even for the higher forecast errors the proposed method proved capable of detecting FDI attacks of significant strengths. The range of the FDI attack strengths that could be detected would further increase with the less strict selection of the detection threshold (allowing false positive detections).

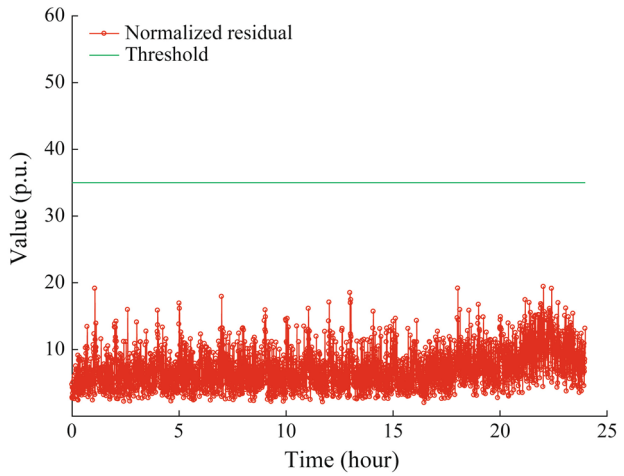
One potential drawback of the proposed approach occurs in cases when the malicious attack is comprised of multiple low strength attacks aimed at the same SV, driving its value towards the targeted value in small increments over a substantial period of time. For attacks constructed in that manner, the differences between WLS-based SE and

UKF calculated values could be below the threshold in the time instant of the incremental attack. In addition, the UKF estimation would reach the WLS-based SE after a limited number of iterations but before the following incremental attack - allowing the attack to be continuously undetected, as shown in Fig. 9.

On the other hand, constructing this type of FDI attack is much more difficult because a prolonged period of time is needed for the attack to attain the desired strength necessary to produce any significant consequences. Furthermore, multiple meaningful changes to all the affected measurements are needed. Such practical complications make this type of an attack an unlikely scenario. Nevertheless, our subsequent research will focus on these slow, incremental FDI attacks.



(a) Voltage magnitude at bus 12



(b) Maximum normalized residuals

Fig. 9 Obtained results for IEEE 300 bus test system under an incremental FDI attack over a 24-hour time period

6 Conclusion

In this paper, the synergy between a traditional WLS-based SE and UKF was used for detection of FDI attacks in power systems. An unlimited number of compromised measurements was supposed, and a more realistic nonlinear observation model was used. To implement the UKF prediction step, a transition function was derived using a power flow model in combination with load/generation short-term forecasts and generator schedules.

The proposed method was tested on benchmark IEEE 14-bus and 300-bus test systems, and all FDI attacks of significant strength were successfully identified for reasonable forecast quality. The only possible failure cases which have been identified are as follows: ① detection of lower strength FDI attacks in systems with bad forecast quality; ② false positive detections in cases of sudden changes in generation/load, that are not captured within a very short-term forecast and unplanned system events (such as equipment outages); ③ detection of attacks consisting of multiple small intensity attacks executed over a long time period. While the third case is highly unlikely and impractical, the second one could easily be disregarded by the system operator.

By relying on a more realistic and accurate nonlinear measurement observation model, and a fast, easily implemented and robust UKF, the proposed solution can be successfully deployed as part of an SE package in commercial EMS software.

Acknowledgements This work was supported by the Ministry of Education, Science and Technological Development of the Republic of Serbia and Schneider Electric DMS NS, Serbia (No. III-42004).

Appendix A

The transition of a system state vector from the $(k\text{-}1)^{\text{th}}$ to k^{th} time instant can be described as:

$$\boldsymbol{x}_k = \boldsymbol{f}(\boldsymbol{x}_{k-1}) + \boldsymbol{w}_k \tag{A1}$$

where $\boldsymbol{x}_k$ is the N-dimensional state estimation vector at k^{th} time instant; $\boldsymbol{f}(\cdot)$ is the N-dimensional nonlinear set of state transition functions; $\boldsymbol{w}_k$ is the N-dimensional process noise vector, assumed to be zero mean multivariate Gaussian

noise with covariance $\boldsymbol{Q}_k$, at k^{th} time instant; N is the number of unknown system SVs (the same as in (1)).

In this paper, a linearized form of the transition model function $\boldsymbol{f}(\cdot)$ is proposed ($\boldsymbol{F}$ in (13)).

The observation model function (in our case, the SE model) is represented by the following equation (which is the same as (1) for the k^{th} time instant).

$$\boldsymbol{z}_k = \boldsymbol{h}(\boldsymbol{x}_k) + \boldsymbol{e}_k \tag{A2}$$

The UKF uses the unscented transformation sampling technique to perform a nonlinear transformation. A minimal set of sampling points (known as sigma points) is selected and transformed using the nonlinear function, whereas the new mean and covariance are formed out of those transformed points. The basic underlying idea is that it is easier to approximate a Gaussian distribution, than it is to approximate an arbitrary nonlinear function.

The state estimation vector at the (k - 1)th time instant ($\boldsymbol{x}_{k-1}$) and its covariance matrix ($\boldsymbol{C}_{k-1}$) are augmented with the mean ($\boldsymbol{0}$) and covariance matrix $\boldsymbol{Q}_k$ of the process noise vector $\boldsymbol{w}_k$, respectively.

$$\boldsymbol{x}^a_{k-1} = \left[\boldsymbol{x}^{\mathrm{T}}_{k-1}\ \boldsymbol{0}\right]^{\mathrm{T}} \tag{A3}$$

$$\boldsymbol{C}^a_{k-1} = \begin{bmatrix} \boldsymbol{C}_{k-1} & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{Q}_k \end{bmatrix} \tag{A4}$$

$$n^a = 2N \tag{A5}$$

where n^a represents the dimension of the augmented state vector ($\boldsymbol{x}^a_{k-1}$), and $\boldsymbol{C}^a_{k-1}$ represents the augmented state covariance matrix.

The $2n^a + 1$ sigma points ($\boldsymbol{\chi}_{k-1|k-1}$) and weight are, respectively, defined as:

$$\boldsymbol{\chi}^i_{k-1|k-1} = \begin{cases} \boldsymbol{x}^a_{k-1} & i = 0 \\ \boldsymbol{x}^a_{k-1} + \boldsymbol{B}_i & i = 1, 2, \ldots, n^a \\ \boldsymbol{x}^a_{k-1} - \boldsymbol{B}_{i-n^a} & i = n^a + 1, n^a + 2, \ldots, 2n^a \end{cases} \tag{A6}$$

$$W^s_i = \begin{cases} \dfrac{\kappa}{n^a + \kappa} & i = 0 \\ \dfrac{1}{2(n^a + \kappa)} & i = 1, 2, \ldots, 2n^a \end{cases} \tag{A7}$$

$$W^c_i = \begin{cases} \dfrac{\kappa}{n^a + \kappa} + (1 - \alpha^2 + \beta) & i = 0 \\ \dfrac{1}{2(n^a + \kappa)} & i = 1, 2, \ldots, 2n^a \end{cases} \tag{A8}$$

where $\boldsymbol{B}_i$ is the ith column of the matrix and $\boldsymbol{B} = \sqrt{(n^a + \kappa)\boldsymbol{C}^a_{k-1}}$; α is the constant that determines the spread of the sigma points around the $\boldsymbol{x}^a_{k-1}$ (usually set to a small number, e.g., 0.001); β is the constant used to incorporate the prior knowledge of the distribution of state vector ($\beta = 2$ for Gaussian distributions); κ is the scaling parameter, usually calculated as $\kappa = n^a(\alpha^2 - 1)$; W^s_i (W^c_i) is the weight associated with the ith sigma point and used to calculate the predicted state vector (covariance matrix).

The predicted sigma points ($\boldsymbol{\chi}^i_{k|k-1}$) are acquired by propagating the previously calculated sigma points using the state transition function $\boldsymbol{f}(\cdot)$, to obtain the predicted state vector with mean ($\boldsymbol{x}_{k|k-1}$) and covariance ($\boldsymbol{C}_{k|k-1}$), respectively

$$\boldsymbol{\chi}^i_{k|k-1} = \boldsymbol{f}(\boldsymbol{\chi}^i_{k-1|k-1}) \tag{A9}$$

$$\boldsymbol{x}_{k|k-1} = \sum_{i=0}^{2n^a} W^s_i \boldsymbol{\chi}^i_{k|k-1} \tag{A10}$$

$$\boldsymbol{C}_{k|k-1} = \sum_{i=0}^{2n^a} W^c_i \left(\boldsymbol{\chi}^i_{k|k-1} - \boldsymbol{x}_{k|k-1}\right)\left(\boldsymbol{\chi}^i_{k|k-1} - \boldsymbol{x}_{k|k-1}\right)^{\mathrm{T}} \tag{A11}$$

Afterwards, the obtained predicted state vector and state covariance matrix should be augmented with the mean ($\boldsymbol{0}$) and covariance matrix ($\boldsymbol{R}_k$) of the observation noise vector, respectively.

$$\boldsymbol{x}^a_{k|k-1} = \left[\boldsymbol{x}^{\mathrm{T}}_{k|k-1}\ \boldsymbol{0}\right]^{\mathrm{T}} \tag{A12}$$

$$\boldsymbol{C}^a_{k|k-1} = \begin{bmatrix} \boldsymbol{C}_{k|k-1} & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{R}_k \end{bmatrix} \tag{A13}$$

$$n^a = 2N + N = 3N \tag{A14}$$

After a new set of sigma points ($\boldsymbol{\chi}^i_{k|k-1}$) are defined using (A6)–(A8), they are propagated through the observation model ($\boldsymbol{h}$) to determine the predicted measurement vector and the predicted measurement covariance matrix, respectively.

$$\hat{z}_k = \sum_{i=0}^{2n^a} W^s_i \bar{z}^i_k \tag{A15}$$

$$\boldsymbol{C}_{z_k,z_k} = \sum_{i=0}^{2n^a} W^c_i \left(\bar{z}^i_k - \hat{z}_k\right)\left(\bar{z}^i_k - \hat{z}_k\right)^{\mathrm{T}} \tag{A16}$$

where

$$\bar{z}^i_k = \boldsymbol{h}(\boldsymbol{\chi}^i_{k|k-1}) \tag{A17}$$

The state-measurement cross-covariance matrix is determined as:

$$\boldsymbol{C}_{x_k,z_k} = \sum_{i=0}^{2n^a} W^c_i \left(\boldsymbol{\chi}^i_{k|k-1} - \boldsymbol{x}_{k|k-1}\right)\left(\bar{z}^i_k - \hat{z}_k\right)^{\mathrm{T}} \tag{A18}$$

and is used to calculate the Kalman gain

$$\boldsymbol{K}_k = \boldsymbol{C}_{\boldsymbol{x}_k,\boldsymbol{z}_k}\boldsymbol{C}^{-1}_{\boldsymbol{x}_k,\boldsymbol{z}_k} \tag{A19}$$

The state vector is updated by adding the innovation $(\boldsymbol{z}_k - \hat{\boldsymbol{z}}_k)$ weighted by the Kalman gain to the predicted state

$$\boldsymbol{x}_{k|k} = \boldsymbol{x}_{k|k-1} + \boldsymbol{K}_k(\boldsymbol{z}_k - \hat{z}_k) \tag{A20}$$

The updated covariance matrix is determined using

$$\boldsymbol{C}_{k|k} = \boldsymbol{C}_{k|k-1} - \boldsymbol{K}_k\boldsymbol{C}_{z_k z_k}\boldsymbol{K}_k^{\mathrm{T}} \tag{A21}$$

References

[1] Zhang Z, Gong S, Dimitrovski AD et al (2013) Time synchronization attack in smart grid: impact and analysis. IEEE Trans Smart Grid 4(1):87–98

[2] Incident response activity (2015) In: NCCIC/ICS-CERT monitor September 2014–February 2015. https://ics-cert.us-cert.gov/monitors/ICS-MM201502. Accessed 2 April 2017

[3] Meserve J (2007) Sources: staged cyber attack reveals vulnerability in power grid. http://edition.cnn.com/2007/US/09/26/power.at.risk/. Accessed 2 April 2017

[4] Abur A, Exposito A (2004) Power system state estimation: theory and implementation. CRC Press, New York

[5] Mili L, Cutsem TV, Ribbens-Pavella M (1984) Hypothesis testing identification: a new method for bad data analysis in power system state estimation. IEEE Trans Power Appar Syst 103(11):3239–3252

[6] Liu Y, Ning P, Reiter M (2009) False data injection attacks against state estimation in electric power grids. In: Proceedings of 16th ACM conference on computer and communications security, Chicago, USA, 9–13 November 2009, 12 pp

[7] Dan G, Sandberg H (2010) Stealth attacks and protection schemes for state estimators in power systems. In: Proceedings of 1st IEEE international conference on smart grid communications, Gaithersburg, USA, 4–6 October 2010, 6 pp

[8] Teixeira A, Amin S, Sandberg H et al (2010) Cyber security analysis of state estimators in electric power systems. In: Proceedings of 49th IEEE conference on decision control (CDC), Atlanta, USA, 15–17 December 2010, 8 pp

[9] Sandberg H, Teixeira A, Johansson KH (2010) On security indices for state estimators in power networks. In: Proceedings of 1st workshop on secure control systems, Stockholm, Sweden, 12 April 2010, 6 pp

[10] Hug G, Giampapa JA (2012) Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks. IEEE Trans Smart Grid 3(3):1362–1370

[11] Anwar A, Mahmood AN, Tari Z (2015) Identification of vulnerable node clusters against false data injection attack in an AMI based smart grid. Inf Syst 53(C):201–212

[12] Kosut O, Jia L, Thomas R et al (2010) Malicious data attacks on smart grid state estimation: attack strategies and countermeasures. In: Proceedings of 1st IEEE international conference on smart grid communications, Gaithersburg, USA, 4–6 October 2010, 6 pp

[13] Kim J, Tong L, Thomas R (2014) Data framing attack on state estimation. IEEE Jr Sel Areas Commun 32(7):1460–1470

[14] Ozay M, Esnaola I, Vural F et al (2013) Sparse attack construction and state estimation in the smart grid: centralized and distributed models. IEEE Jr Sel Areas Commun 31(7):1306–1318

[15] Esmalifalak M, Nguyen H, Zheng R et al (2011) Stealth false data injection using independent component analysis in smart grid. In: Proceedings of 2nd IEEE international conference on smart grid communications, Brussels, Belgium, 17–20 October 2011, 5 pp

[16] Kim J, Tong L, Thomas R (2015) Subspace methods for data attack on state estimation: a data driven approach. IEEE Trans Signal Process 63(5):1102–1114

[17] Yu ZH, Chin WL (2015) Blind false data injection attack using PCA approximation method in smart grid. IEEE Trans Smart Grid 6(3):1219–1226

[18] Anwar A, Mahmood AN (2016) Stealthy and blind false injection attacks on SCADA EMS in the presence of gross errors. In: Proceedings of power energy society general meeting, Boston, USA, 17–21 July 2016, 5 pp

[19] Esfahani PM, Vrakopoulou M, Margellos K et al (2010) Cyber attack in a two-area power system: impact identification using reachability. In: Proceedings of American control conference, Baltimore, USA, 30 June–2 July 2010, 6 pp

[20] Esfahani PM, Vrakopoulou M, Margellos K et al (2010) A robust policy for automatic generation control cyber attack in two area power network. In: Proceedings of 49th IEEE conference on decision control, Atlanta, USA, 15–17 December 2010, 6 pp

[21] Sridhar S, Manimaran G (2010) Data integrity attacks and their impacts on SCADA control system. In: Proceedings of power energy society general meeting, Minneapolis, USA, 25–29 July 2010, 6 pp

[22] Xie L, Mo Y, Sinopoli B (2010) False data injection attacks in electricity markets. In: Proceedings of 1st IEEE International conference on smart grid communications, Gaithersburg, USA, 4–6 October 2010, 6 pp

[23] Bobba RB, Rogers KM, Wang Q et al (2010) Detecting false data injection attacks on DC state estimation. In: Proceedings of 1st workshop on secure control systems, Stockholm, Sweden, 12 April 2010, 9 pp

[24] Kim TT, Poor HV (2011) Strategic protection against data injection attacks on power grids. IEEE Trans Smart Grid 2(2):326–333

[25] Vukovic O, Sou KC, Dan G et al (2012) Network – aware mitigation of data integrity attacks power system state estimation. IEEE Jr Selected Areas Comm 30(6):1108–1118

[26] Bi S, Zhang YJ (2014) Graphical methods for defense against false-data injection attacks on power system state estimation. IEEE Trans Smart Grid 5(3):1216–1227

[27] Anwar A, Mahmood A (2014) Vulnerabilities of smart grid state estimation against false data injection attack. In: Johangir H, Apel M (eds) Renewable energy integration. Springer, Singapore

[28] Jokar P, Arianpoo N, Leung V (2013) Intrusion detection in advanced metering infrastructure based on consumption pattern. In: Proceedings of IEEE international conference on communications, Budapest, Hungary, 9–13 June 2013, 5 pp

[29] Rana M, Li L, Su SW (2016) Cyber attack protection and control in microgrids using channel code and semidefinite programming. In: Proceedings of power energy society general meeting, Boston, USA, 17–21 July 2016, 5 pp

[30] Chaojun G, Jirutitijaroen P, Motani M (2015) Detecting false data injection attacks in AC state estimation. IEEE Trans Smart Grid 6(5):2476–2483

[31] Huang Y, Tang J, Cheng Y et al (2016) Real-time detection of false data injection in smart grid networks: an adaptive CUSUM method and analysis. IEEE Systems Journal 10(2):532–543

[32] Zhao J, Zhang G, La Scala M et al (2017) Short-term state forecasting-aided method for detection of smart grid general

STATE GRID
STATE GRID ELECTRIC POWER RESEARCH INSTITUTE

false data injection attacks. IEEE Trans Smart Grid 8(4):1580–1590
[33] Xu R, Wang R, Guan Z et al (2017) Achieving efficient detection against false data injection attacks in smart grid. IEEE Access 5:13787–13798
[34] Rawat DB, Bajracharya C (2015) Detection of false data injection attacks in smart grid communication systems. IEEE Signal Processing Letters 22(10):1652–1656
[35] Debs AS, Larson RE (1970) A dynamic estimator for tracking the state of a power system. IEEE Trans Power Apparatus Systems 89(7):1670–1678
[36] Wan EA, Van Der Merwe R (2000) The unscented Kalman filter for nonlinear estimation. In: Proceedings of IEEE 2000 adaptive systems for signal processing, communications, and control symposium, Lake Louise, Canada, 4 October 2000, 6 pp
[37] Mandal JK, Sinha AK, Roy L (1995) Incorporating nonlinearities of measurement function in power system dynamic state estimation. IEE Generation, Transmission and Distribution 142(3):289–296
[38] Shih KR, Huang SJ (2002) Application of a robust algorithm for dynamic state estimation of a power system. IEEE Trans Power Systems 17(1):141–147
[39] Zhao J, Netto M, Mili L (2017) A robust iterated extended Kalman filter for power system dynamic state estimation. IEEE Trans Power Systems 32(4):3205–3216
[40] Valverde G, Terzija V (2011) Unscented Kalman filter for power system dynamic state estimation. IET Generation, Transmission and Distribution 5(1):29–37
[41] Julier SJ, Uhlmann JK (1997) A new extension of the Kalman filter to nonlinear systems. In: Proceedings of 11th international symposium on aerospace/defence sensing, simulation and controls, Orlando, USA, 20–25 April 1997, 12 pp
[42] Zhang Q, Chakhchoukh Y, Vittal V et al (2013) Impact of PMU measurement buffer length on state estimation and its optimization. IEEE Trans Power Syst 28(2):1657–1665
[43] Bus power flow test case (1993) In: Power systems test case archive. University of Washington. http://www2.ee.washington.edu/research/pstca/pf14/pg_tca14bus.htm. Accessed 6 April 2017
[44] Bus power flow test case (1993) In: Power systems test case archive. University of Washington. http://www2.ee.washington.edu/research/pstca/pf300/pg_tca300bus.htm. Accessed 6 April 2017

Nemanja ŽIVKOVIĆ received the B.Sc. and M.Sc. degrees in power engineering from the University of Novi Sad, Serbia, in 2009 and 2010, respectively. He works at Schneider Electric DMS NS company as head of EMS product management and is currently engaged in multiple projects worldwide on delivery of Schneider's solution for power system analysis and optimization of (sub)transmission networks. His main areas of interest are (sub)transmission power system analysis and optimization applications, as well as cyber security, with special focus on applicability on large networks.

Andrija T. SARIĆ received the B.Sc., M.Sc., and Ph.D. degrees in electrical engineering from the University of Belgrade, Serbia, in 1988, 1992, and 1997, respectively. He is a Full Professor of electrical engineering at the University of Novi Sad, Faculty of Technical Sciences, Serbia. His main areas of interest are power system analysis, optimization and planning, as well as application of artificial intelligence methods in these areas.