PSO TUNED UNSCENTED KALMAN FILTER FOR DETECTING DATA ATTACKS IN SMART POWER GRID

Kalaiselvi KANDASAMY[1], Renuga PERUMAL[2], Suresh Kumar VELU[3]

[1]Research Scholar and [2,3]Associate Professor
Department of Electrical and Electronics Engineering,
Thiagarajar College of Engineering, Madurai – 625 015, Anna University, Tamil Nadu, India
Email: kkseee@tce.edu, preee@tce.edu, vskeee@tce.edu

Abstract: *The conventional electric power grid is presently evolving into smart grid by providing new services based mainly on information and communication technology. Due to the new facilities and services, the strength of a smart grid communication network against data attack is one of the ultimate problems that affect the entire system. In this work, some of the most vulnerable data attacks such as random fault attack, denial of service (DoS) attack and false data injection attacks against the state estimation in electric power system are discussed. This article is dedicated to study these cyber security issues in smart grid enabled power system using Unscented Kalman filter (UKF) along with χ^2-detector and Euclidean detector. To obtain a reliable estimate of the system's state, the noise covariance of the Kalman filter has to be tuned before the operation. Therefore, tuning of the UKF using particle swarm optimization (PSO) technique for minimizing estimation error is presented in this work. The simulation results show the benefits of the PSO tuned UKF for solving the proposed problem.*

Keywords: *Smart grid, Data attack, χ2-detector, Euclidean detector, Unscented Kalman filter, State estimation.*

1. Introduction

The smart grid components are increasingly dependent on information technology in order to achieve maximum flexibility, adaptability and efficiency. Today it is possible due the development of more advanced sensing, communications and control devices. At the same time, security issues also arise as more complex information. For example, as shown in Figure 1, the combination of several physical and cyber components gives rise to cyber attack threats in smart grid, which can cause power outages and system blackouts, or huge economical losses [1]. A faulty sensor or actuator may cause process performance degradation, process shutdown, or a fatal accident. If actuator faults occur, analytical redundancy techniques should be used to determine if, where, and how the faults occurred. In power networks, state estimation estimates the power system operation state based on the real-time electric network and its results are necessary for the operators to make decisions in order to maintain security and performance of the system [2].

The presence of any bad measurements in the electric power grid affects the accuracy of the state estimation process. Bad data could be due to errors in the grid, measurement abnormalities caused by meter failures, and malicious attacks. Therefore, to achieve reliable and secure operation of power grid, it is essential for the system operator to detect and identify cyber attacks [3,4]. A smart grid is presented as complex interdependent networks and targeted attacks on smart grids are studied in the paper [5]. The importance of detection and identification of cyber security issues are presented in [6,7]. To detect and identify the false measurements and data in the power grid state, several techniques based on the statistical test on measurement residuals are developed and widely used. For example, false data detection in the power grid is analyzed in several articles [8,10].

One of the well-known approaches is using the Kalman Filter as an observer for the purpose of parameter estimation and fault detection [11-14]. In [11], a mathematical model of the smart gird and Kalman filter to estimate the variables of a wide range of state processes is given. The estimates from the Kalman Filter and the system readings are then fed into the χ^2-detector and Euclidean detector. But, for efficient tracking by any filter like Kalman filter, noise covariance must be optimized [15]. It is identified from the literature that the selection of the process noise and measurement noise covariance is a main parameter which decides the efficiency and accuracy of the Kalman filter. Therefore, the optimum selection of process noise and measurement noise covariance is studied in this paper to improve the accuracy of the Kalman filter. A generalized auto covariance least-squares method and neural network based tuning of Kalman filter is proposed in [16] and [17], respectively.

BUPT

In this work, the well known particle swarm optimization (PSO) technique [18-20] is proposed in this paper for tuning the Kalman filter. Also, Unscented Kalman filter (UKF) [21-22] is proposed instead of conventional Kalman filter for the estimation process, since it gives better solution with nonlinear parameters.

The organization of this paper is as follows. Section 2 illustrates problem formulation by considering a power system model. Section 3 discusses about details of proposed methodology. In section 4, test system and the analytical results are presented. The conclusions are given in section 5.

2. Problem description

The proposed work considers some of the cyber security problems which are vulnerable in the modern smart grid. In this thesis, random fault attack, denial of service (DoS) attack and false data injection attacks against the state estimation in electric power system is presented. The measuring devices of the system includes the bus voltages, bus real and reactive power injections, and branch reactive power flow in each and every subsystem of a power grid. State estimation uses power flow models for the estimation process. The attack was designed to affect the state estimation of the SCADA system. By knowing the configuration information of a power system, an attacker can inject false measurements that will give the wrong information about the state estimation process which is not being detected by any of the existing techniques for bad measurement detection. Here, the attacker tries to find any attack vector and inject random fault into the SCADA centre as long as it can lead to a wrong estimation of state variables. If these bad measurements affect the result of state estimation, they can delude the power grid control algorithm, which probably ends with tragic consequences such as blackouts in large topographic areas. Consequently, this could result in major financial losses to the social welfare.

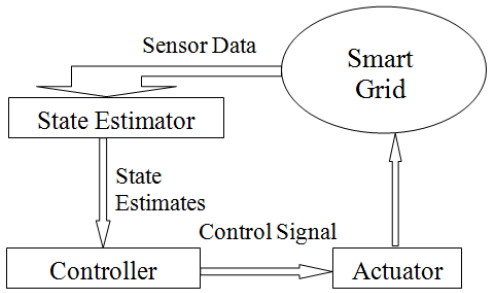


Figure 1 State estimation diagram

Figure 1 shows the block diagram of state estimation process in a smart grid system. The information from the generating stations were sensed by various sensors and fed to the state estimator which estimates the parameters of the system. The estimator detects the faults and fed the output to the controller system which gives the command to the generating stations.

2.1 Kalman filter state estimation

Valuable information about important variables in a physical process is provided by state estimator. The function of state estimator is shown in Figure 2. In the first step of state estimation process, the initial value of the predicted state estimate is set equal to this initial (zero) value. Then, the predicted measurement estimate from the predicted state estimate is calculated. Next, the measurement estimate error (variable) as the difference between the measurement and the predicted measurement is determined. Then, the corrected state estimate (posteriori estimate) by adding the corrective term to the predicted state estimate is calculated. Finally, the predicted state estimate for the next time step (k + 1), using the present state estimate and the known input in process model is calculated.

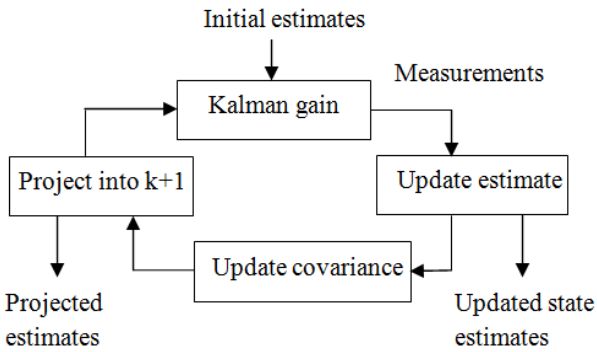


Figure 2 KF state estimation process

2.2 Power system state estimation and security

Before any security assessment can be made or control actions taken, a reliable estimate of the existing state of the system must be determined. For this purpose, the number of physical measurements cannot be restricted to only those quantities required to support conventional power-flow program are confined to the real power and reactive power injections at load buses and P, |V| values at voltage controlled buses.

If even one of these inputs is unavailable, the conventional power-flow solution cannot be obtained. Moreover, the gross error which is one or

BUPT

more of the input quantities can cause the power flow results to become useless. In practice, other conveniently measured quantities such as real power, reactive power line flow values are available, but they cannot be used in conventional power flow calculations. These limitations can be removed by the state estimation process. IEEE 9-bus system is considered in this work and Newton-Raphson method is used for load flow analysis. The problem and results are validated through simulation of IEEE 9 bus test system using MATLAB. In this research, it is shown that how the intruder can attack the vector quantities, for the cyber security attacks such as DOS attack, random fault attack and false data injection attack. Unscented Kalman filter (UKF) is used to detect and identify these cyber attacks.

3. Proposed methodology

The Kalman filter along with χ^2-detector and Euclidean detector is used for detection and identification of attacks. A state-space model of Unscented Kalman filter is developed for the three-phase sinusoidal voltage equations and the state variables are assumed using the voltage sensors measurements.

The UKF estimates the values for the state variables based on the system state and the data from numerous sensor readings. The estimated values generated by UKF and the observed values for the state variables are fed into the detector. The detector compares the two state vectors. If the two data differ from each other then there is a possible attack on the smart grid. The UKF generates estimates for state variables using the mathematical model for the power grid and the data obtained from the sensor network deployed to monitor the power grid.

The χ^2-detector is a typical choice for the UKF estimators. Here, the residue of the UKF compares the estimated value with the threshold obtained from the standard χ^2-table. Attacks such as the DoS attack and random attack are readily detected by the UKF and χ^2-detector combination. However, the false data injection attack can bypass such detectors and may remain undetected. Hence, Euclidean distance detector which exactly calculates the difference between the estimated and observed voltage signal is proposed to detect false data injection attack.

3.1 Unscented Kalman Filter

The Kalman filter (KF) is well known for signal estimation applications while the system model is linear. When, predict and update functions are highly non-linear, the KF cannot give up good performance because the linearization of the underlying non-linear model. Therefore, when the system model and measurement is non linear, UKF provides accurate estimation. UKF determines a minimal set of sample (sigma) points around the mean. Then the non-linear functions are used to propagate these sigma points, from which the mean and covariance of the estimate are then recovered. This results in a filter which more accurately captures the true mean and covariance. This technique move out the requirement to explicitly calculate Jacobians, which is a bottleneck task for complex functions.

The sensor readings or the observations are forwarded to the estimator at regular interval of time. At each time step, the estimator of the system generates estimated readings based on the previous time step and the real time sensor readings.

In the UKF prediction state, the update is done independently in co-ordination with a linear update. The mean and covariance of the process noise is used in increasing the estimated state and covariance as given in Equations (1- 2)

$$X^{a}_{k-1|k-1} = \begin{bmatrix} \hat{X}^{T}_{k-1|k-1} & E\left[W^{T}_{k}\right] \end{bmatrix}^{T} \tag{1}$$

$$P^{a}_{k-1|k-1} = \begin{bmatrix} P_{k-1|k-1} & \mathbf{O} \\ \mathbf{O} & Q_k \end{bmatrix} \tag{2}$$

The predicted state and covariance are produced by recombination of the weighted sigma points as given in Equations (3 - 4).

$$\hat{X}_{k|k-1} = \sum_{i=0}^{2L} W_s^i X^{i}_{k|k-1} \tag{3}$$

$$P_{k|k-1} = \sum_{i=0}^{2L} W_c^i \left[X^{i}_{k|k-1} - \hat{X}_{k|k-1} \right] \left[X^{i}_{k|k-1} - \hat{X}_{k|k-1} \right]^{T} \tag{4}$$

Next, the same augmentation of the predicted state and covariance is done with the mean and covariance of the measurement noise as given in Equations (5 - 6).

$$X^{a}_{k|k-1} = \begin{bmatrix} \hat{X}^{T}_{k|k-1} & E\left[V^{T}_{k}\right] \end{bmatrix}^{T} \tag{5}$$

$$P^{a}_{k|k-1} = \begin{bmatrix} P_{k|k-1} & \mathbf{O} \\ \mathbf{O} & R_k \end{bmatrix} \tag{6}$$

BUPT

The predicted measurement and predicted measurement covariance are generated recombining the weighted sigma points as given in Equations (7 - 8).

$$\hat{z}_k = \sum_{i=0}^{2L} W_s^i \lambda_k^i \tag{7}$$

$$P_{\approx k \approx k} = \sum_{i=0}^{2L} W_c^i \left[\lambda_k^i - \hat{z}_k \right] \left[\lambda_k^i - \hat{z}_k \right]^T \tag{8}$$

The state–measurement cross covariance matrix is obtained as given in Equation (9).

$$P_{xk \approx k} = \sum_{i=0}^{2L} W_c^i \left[X_{k|k-1}^i - \hat{X}_{k|k-1} \right] \left[\lambda_k^i - \hat{z}_k \right]^T \tag{9}$$

3.2 χ^2-detector and Euclidean detector

The χ^2-detector is a conventional detector used with Kalman filter. The chi-square goodness-of-fit test is used to find and compare the observed sample distribution with the expected probability distribution. The χ^2-detector, constructs χ^2 test statistics from the Kalman filter and compares them with the threshold value g(t). The χ^2-detector compares g(t) with previously computed threshold value using the χ^2 –detector table to identify a failure or attack. The χ^2 test is long-term test because, at each detection step, all integrated effects since system start time are considered. This property makes it very useful for the fault detection in smart grid which consists of sensors that are subject to soft failures like instrument bias shift. Another advantage of χ^2 - detector is its computational complexity.

The parameters required to perform the test are already generated by the Kalman filter making it compatible with the Kalman filter. Furthermore, the threshold for the detector can be easily obtained from the χ^2 table making the threshold computation relatively easy. In the most of works done earlier, the threshold value is randomly chosen such that error rate will be less than 5%. If it is optimized, then the error will be reduced below 5% and then the accuracy of Kalman filter will get improved.

Though χ^2-detector has a high noise tolerance and work in most of the cases but attacks such as false data injection attack fails to get detect. The false data injection attack is crafted such that it can bypass the statistical detector, such as χ^2 -detector. Therefore, to detect false data injection attack Euclidean detector, which calculates the deviation of the observed data from the estimated data is proposed [11]. Here, the sinusoidal signals from the state estimates are reconstructed and then, correlated them with the measurements obtained from the sensors.

3.3 Tuning of the filter

The basic filter operations are the state evaluation, Kalman gain evaluation, and the state and covariance updates. Most of the previous works, it is assumed that the estimation of Kalman gain can converge within few steps and operate in steady state. The filter tuning searches for every variant of the Kalman filter which can be minimized but not completely ignored in order to get near optimal solutions. It should have the ability to estimate all the variables from the observables and should be self consistent in estimating all the unknowns.

Most of the earlier research work, have concentrated their effort in using simulated data to tune the filter off line and these values will be used later for online and real time applications. There is no proper conventional technique to find measurement noise covariance (R) and process noise covariance (Q). Here, we propose artificial intelligent method to reduce further computational time and improve accuracy of the Kalman gain estimation by optimal estimation of noise covariances. Tuning of the filter is mainly done for the estimation of the noise covariance matrices. The performance of a Kalman filter mainly depends largely on the accuracy of R and Q. Incorrect priori knowledge of noise covariance may lead to performance degradation. Sometimes, even it can leads to practical divergence. Therefore, an intelligent method of estimation of these matrices becomes very important for online operation. Measurements can be executed during the operation of the filter under various noise conditions and measurement noise covariance.

The filter tuning is a process of obtaining parameters such as process noise covariance matrices and measurement noise covariance matrix that give the best filter performance. Each time during optimization procedure we have to run the Kalman filter on all available data. Proper initialization of this is very essential as it is necessary to minimize the error. Therefore, the tuning of the filter performed using the well known particle swarm optimization algorithm.

3.4 Applying PSO in filter tuning

PSO is used in this work to tune the filter covariances. Measurement noise covariance and process noise covariance of UKF are optimized that give the best filter performance in mean square error sense. Typically, this kind of problems of designing a filter with optimal tuning parameters was left up to engineering intuition and trial and error method that

BUPT

do not guarantee best filter performance due to large number of parameters to be tuned. This requires a significant computational time since for example in order to find a global minimum of a smooth function of parameters. Therefore, PSO is proposed in this article to optimize the gain value of the filter. The explanation of PSO technique is avoided here, since it is a well known optimization technique.

4. Results and discussion

The input of the proposed system is verified using MATLAB simulation. The random attack and DoS attack are detected using χ^2-detector and false data injection attack is identified using Euclidean detector. The estimated values obtained in each case are compared with the input signal. The χ^2-detector compares the threshold value, g(t) with the predetermined threshold value from the χ^2 table.

4.1 χ^2- detector test

The χ^2 distribution method helps to find the best-fit value. In the simplest case, a linear fit is needed for the data so a range of slopes are tested. The program is written does the chi-squared calculation for a given slope, puts the value in a vector, and then repeats for the next slope. In the end, a series of chi-squared values corresponding to the slopes are obtained. In the assumption, uncertainty in y-direction is much larger than the uncertainty in the x-direction.

Figure 3 shows the graph of chi-square versus slope. The slope is the best method to know the minimum chi-squared value for the set. Also to find the best fit, the best chi-squared value is compared with the number of data points; if the best chi-squared is less than our number of data points then our model is good. For this data set, the minimum chi squared is greater than the number of data points which means it's not a great fit, but it's not terrible either. The fact that the minimum χ^2 is less than twice the number of data points means that each point was an average less than two sigma from the line. From this plot, we can see that the minimum χ^2 is a little more than 1500, and the slope is nearly 2. Information we can get from the chi-squared analysis is whether or not this best-fit line agrees with our theoretical prediction. The graph is used to find the range of slopes within $\chi^2_{min}\pm$ 1. If the theoretical prediction falls in that range, then obtained best fit line agrees with the theoretical model.

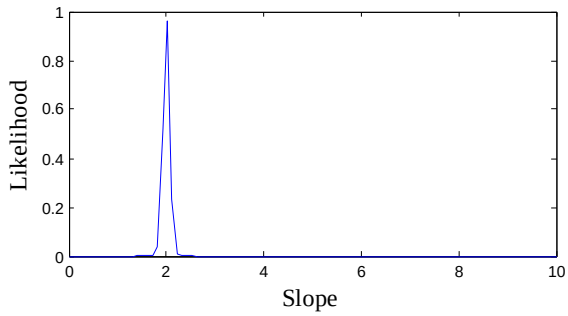


Figure 3 χ^2 versus slope

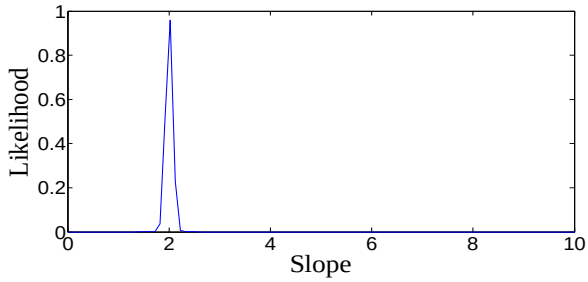


Figure 4 Likelihood versus slope

Figure 4 shows the graph between the likelihood versus slope. The likelihood is the probability that this best-fit line could have generated the data collected. The likelihood is a Gaussian that peaks at the slope corresponding to the min chi-squared. The width (sigma) of the Gaussian is determined by finding the slopes corresponding to $\chi^2_{min}\pm$ 1. From this plot, we can see that the maximum point is 2.

4.2 No fault condition

The input data are obtained from load flow analysis of the IEEE 9 bus system using Newton-Raphson method and the voltages are taken as the base case. These data are used as the state parameter for the Kalman filter estimator. The estimated values obtained from the Kalman filter estimator overlap with the input signal which is a sinusoidal signal, denoting there is no difference between the estimated and the observed value. Hence, there is no fault in the system and there won't be any changes in the system parameters. Therefore, the output from the power plant will be similar to that of the input signal.

Figure 5 shows the graph of the fitness function value versus generation. Here, the error is taken as the internal absolute error. The error value of the system is optimized by the PSO to get the g_{best} value. The graph shows that the error is minimized to zero. This helps to improve the filter performance by varying the Kalman gain (k).

BUPT

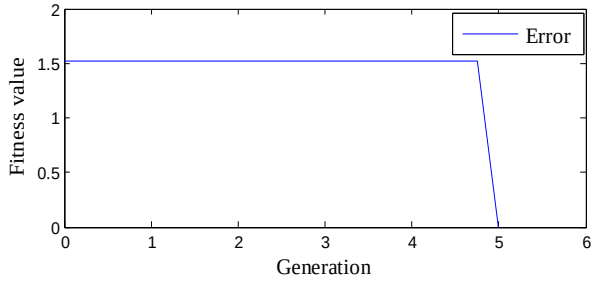


Figure 5 Fitness value versus generation

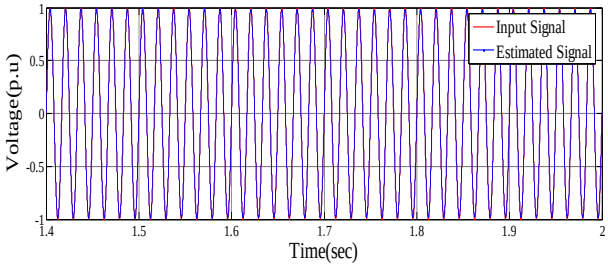


Figure 6 Voltage estimation during no fault condition

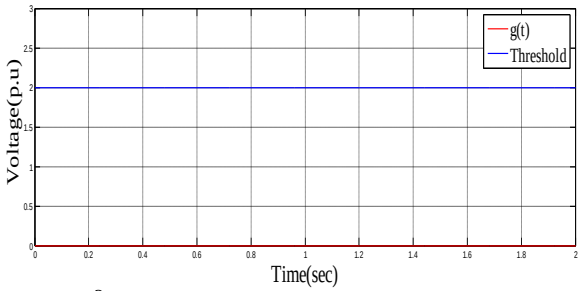


Figure 7 χ^2 – detector under no fault condition

Figure 6 shows the output waveform of the estimated value of the system when there is no fault. Here, the estimated value will be equal to the input signal due to the absence of the fault. Figure 7 shows the output waveform of a smart grid system when there is no fault. Here, g(t) which is calculated using the χ^2–detector will also be equal to the threshold value.

4.3 Random attack

In this case, the intruder can easily manipulate the sensor readings by including random attack vector model. An unknown data which may be due to the malfunctioning of the switching devices is injected into the system. By giving a random value after a period of time as expressed in Equation (10), the estimated value gets varied from the input signal.

$$y'(t) = C(t)x'(t) + v(t) + y(t) \qquad (10)$$

Where,

y(t) = random attack generated in the system,

$y'(t)$ = system observations during attack.

$x'(t)$ = System states during attack and

$C(t)$ = [cos*wt* – sinwt]

These random attacks could be generated at any point in time and could be a long-term continuous attack or a short attack. The random attack is modelled in the system by introducing random value after the period of time. Therefore, the estimated value gets varied from the input signal. If there is a slight difference between the estimates and the input signal, the filter works iteratively by correcting its estimates using the state space model and the measurements are obtained.

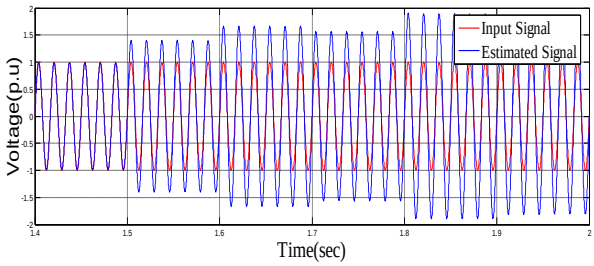


Figure 8 Voltage estimation during random attack

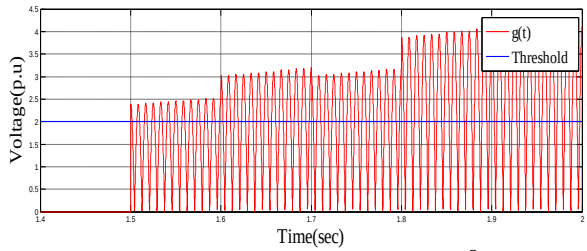


Figure 9 Random attack detection using χ^2–detector

Here, the random attack is injected into the system after a particular period of time. Therefore, the input from the generating plant gets varied after a period a time due to fault in the switching devices. The change in the input signal affects the system and causes random changes in the system parameters. The Figure 8 and 9 show the output waveforms for the continuous random attack system using the χ^2-detector. Difference between the input signal and the estimated value is clearly noticed, when the random noise is introduced into the system.

4.4 Denial of service attack

Denial of service attack means, the attacker will flood packets in the network for compromising devices to prevent data transfer and for jamming the communication system. Since, one of the primary security objectives of the smart grid operation is availability, DoS attacks which have an immediate impact on the availability of communication systems and control systems become the primary network security threats in the smart grid. Most of the DoS attacks come under passive detection method that keeps monitoring the network status, such as system

BUPT

voltage, phase angle etc. The detector raises an attack alarm once there is an evident mismatch between new samples and threshold values.

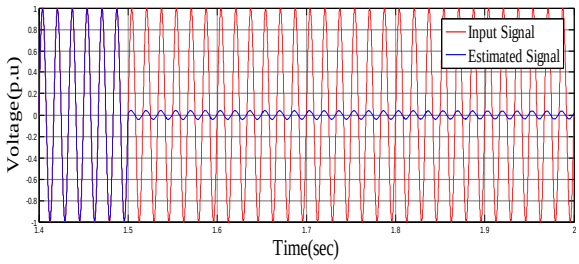


Figure 10 Voltage estimation during DoS attack

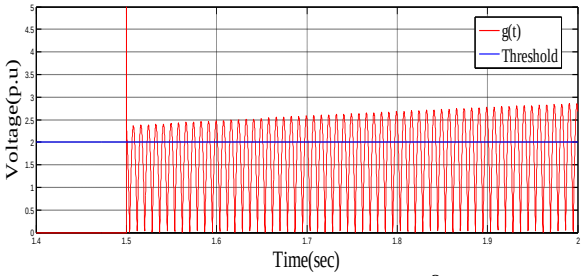


Figure 11 DoS attack detection using χ^2–detector

Here, the lack of sensor information is considered as the denial of service attack and therefore after a particular interval of time, the amplitude of the input signal is minimised. Due to the lack of the input signal, the estimated signal will also be reduced after a particular period of time. Figure 10 shows the output waveform of estimated voltage value during DoS attack. The DoS attack is performed after a particular period of time. Therefore, after the particular time (ie.1.5sec), the estimated value gets changed from the input signal. The estimator output during DoS attack is shown in Figure 11. After a particular period of time, there will a lack of sensor data and therefore the input data value decreases which may be nearly zero. Due to this, the g(t) may gets varied from the threshold value as shown in Figure 11.

4.5 False data injection attack

It is assumed that the false data that injected into the power system by a hacker who knows the system model parameters. Therefore, false data are injected into the power plant subsystem after a period of time. So, we can expect variation in the estimated value. As discussed in section 3.2, the Euclidean detector is used instead of χ^2- detector to identify the false data injection attack.

The output waveform of the estimated value during false data injection attack in the smart grid is shown in Figure 12. Because of the false data injection, the estimated value does not match with the input signal. Detection of false data injection attack using Euclidean-detector is shown in Figure 13. It is observed that the estimated value changes from the input signal when false data are injected into the system.

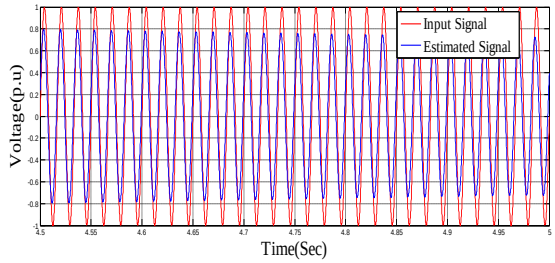


Figure 12 Voltage estimation during false data injection attack

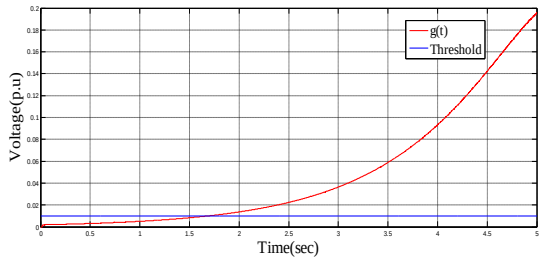


Figure 13 Detection of false data injection attack

The computational performance of PSO tuned UKF is compared with conventional UKF as given in Table 1. In the case of PSO tuned UKF, the measurement noise deviation is almost zero and hence the estimation error is zero.

Table 1
Performance analysis

Parameter	UKF	PSO-UKF
Measurement noise deviation	0.08	1×10^{-6}
Estimation error	0.28	0.00001
Tuning time (sec)	-	0.2

5. Conclusions

Some of the major cyber security issues such as random fault attack, denial of service attack and false data injection attacks are analyzed in this work. These cyber attacks are detected using Unscented Kalman filter together with the χ^2–detector and Euclidean detector. The process noise covariances and the measurement noise covariances of the

BUPT

Kalman filter are tuned using the PSO technique which helps to improve the Unscented Kalman filter performance by finding the proper estimation value. To exhibit the validity of the proposed techniques, simulations are carried out on IEEE 9 bus test system.

Acknowledgement

The authors thank University Grants Commission (UGC), New Delhi, India for financially supporting to carry out this research under the grant: F1-17.1/3157/SA-III.

References

1. Li .H., Lai .L and Zhang .W., *Communication requirement for reliable and secure state estimation and control in smart grid* , IEEE Trans. Smart Grid, vol. 2, no. 3, pp. 476–486, Sep. 2011.
2. Eric Knapp, Raj Samani, *Applied Cyber Security and the Smart Grid*, Elsevier Inc, First Edition, 2013.
3. Khadija Tazi; Farid Abdi; Mohamed Fouad Abbou, *Review on cyber-physical security of the smart grid: Attacks and defense mechanisms*, 2015 3rd International Renewable and Sustainable Energy Conference (IRSEC),Year: 2015, pp. 1 – 6.
4. Divyadeep Vermaa, *Efficient Method for Smart Grid Fault Observation with Minimum PMUs*, Journal of Electrical Engineering, vol.17, no.2, 2017, pp.355-362.
5. Sushmita Rujy and Arindam Pal, *Analyzing Cascading Failures in Smart Grids under Random and Targeted Attacks*, 2014 IEEE 28th International Conference on Advanced Information Networking and Applications, pp. 226-233.
6. Y. Liu, P. Ning, and M. K. Reiter, *False data injection attacks against state estimation in electric power grids*, ACM Transactions on Information and System Security, vol. 14, no. 1, 2011, pp. 13:1–13:33.
7. Y. Mo and B. Sinopoli, *False data injection attacks in control systems*, in Preprints of the 1st Workshop on Secure Control Systems, 2010, pp.1–6.
8. Danda B. Rawat, and Chandra Bajracharya, *Detection of False Data Injection Attacks in Smart Grid Communication Systems*, IEEE Signal Processing Letters, vol. 22, no. 10, pp. 1652 – 1656, 2015.
9. Liu .L., Esmalifalak .M and Han .Z, *Detection of false data injection in power grid exploiting low rank and sparsity*, IEEE International Conference on Communications, Budapest, Hungary, June 2013, pp. 4461-4665.
10. Bo Tang; Jun Yan; Steven Kay; Haibo He, *Detection of false data injection attacks in smart grid under colored Gaussian noise*, 2016 IEEE Conference on Communications and Network Security (CNS),Year: 2016, pp. 172 – 179.
11. Kebina Manandhar Xiaojun Cao, and Yao Liu, *Detection of faults and attacks including false data injection attack in smart grid using Kalman filter*, IEEE Transactions of control of network systems. vol.1, no.4, December 2014.
12. Zeeshan Hameed Mir; Fethi Filali, *An adaptive Kalman filter based traffic prediction algorithm for urban road network*, 2016 12th International Conference on Innovations in Information Technology (IIT), 2016, pp. 1 – 6.
13. Yanyan Li; Yonghong Tan; Ruili Dong; Haifen Li, *State Estimation of Macromotion Positioning Tables Based on Switching Kalman Filter* , IEEE Transactions on Control Systems Technology, 2017, vol. 25, no. 3, pp. 1076 – 1083.
14. Mohamed Ahmeid; Matthew Armstrong; Shady Gadoue; Maher Al-Greer; Petros Missailidis, *Real-Time Parameter Estimation of DC–DC Converters Using a Self-Tuned Kalman Filter* , IEEE Transactions on Power Electronics, 2017, vol. 32, no. 7, pp. 5666 – 5674.
15. B.R.J.Haverkamp, M.verhaegen, C.T.chou, R.johasson, *Tuning of the continuos-time Kalman Filter from sampled data*, proceedings of American control conference California, 1999, vol. 6, pp. 3895 – 3899.
16. Bernt M.A Kesson, John Bagterp Jorgenson, Niels Kjolstad Poulsen, *A generalized auto covariance least-squares method for Kalman filter tuning*, Journal of process control, Elsevier 2007, vol. 18, no. 7-8, pp. 769-779.
17. Oleksiy V.Korniyenko, Mohammad S.Sharawi, Oklahand University, *Neural Network based approach for tuning Kalman filter*, 2005 IEEE International Conference on Electro Information Technology, pp. 1 - 5.
18. Yamille del Valle, Ganesh Kumar Venayagamoorthy, Salman Mohagheghi, Jean-Carlos Hernandez, and RonaldG.Harley, *Particle Swarm Optimization: Basic Concepts, Variants and Applications in Power System*, IEEE Transactions on Evolutionary Computation, vol. 12, no. 2, 2008, pp. 171-195.
19. J.Kennedy and R.C.Eberhart, *Particle Swarm optimization*, in proceedings of IEEE International conference on Neural Networks,1995, pp. 39-43.
20. Jyoti Ohri, *PSO-RBNN based control Design for Trajectory Tracking*, Journal of Electrical Engineering, vol.17, no.3, 2017, pp.10-16.
21. Wei He, Nicholas Williard, Chaochao Chen, Michael Pecht, *State of charge estimation for electric vehicle batteries using unscented Kalman filtering*, Elsevier Microelectronics Reliability, vol. 53, no. 6, January 2013, pp. 840-847.
22. Bingbing Wang; Jinping Sun; Xuwang Zhang; Xiuwei Yang, *A waveform-agile unscented Kalman filter for radar target tracking* , 2016 9th International Congress on Image and Signal Processing, Bio Medical Engineering and Informatics (CISP-BMEI), 2016, pp. 1153 – 1157.

BUPT