

Efficient detection of faults and false data injection attacks in smart grid using a reconfigurable Kalman filter

Prakyath Dayananda¹, Mallikarjunaswamy Srikantaswamy², Sharmila Nagaraju³, Rekha Velluri⁴,
Doddananjedevaru Mahesh Kumar⁵

¹Department of Electrical and Electronics Engineering, SJB Institute of Technology, Bangalore, India

²Department of Electronics and Communication Engineering, JSS Academy of Technical Education, Bangalore, India

³Department of Electrical and Electronics Engineering, Sri Jayachamarajendra College of Engineering, Mysore, India

⁴Department of Computer Science and Engineering, CHRIST (Deemed to be University), Bengaluru, India

⁵Department of Electronics and Instrumentation Engineering, JSS Academy of Technical Education, Bangalore, India

Article Info

Article history:

Received Mar 17, 2022

Revised Aug 28, 2022

Accepted Sep 19, 2022

Keywords:

False data injection attack

Kalman filter

Random attack

Reconfigurable Euclidean detector

Smart grid

ABSTRACT

The distribution denial of service (DDoS) attack, fault data injection attack (FDIA) and random attack is reduced. The monitoring and security of smart grid systems are improved using reconfigurable Kalman filter. Methods: A sinusoidal voltage signal with random Gaussian noise is applied to the Reconfigurable Euclidean detector (RED) evaluator. The MATLAB function randn() has been used to produce sequence distribution channel noise with mean value zero to analysed the amplitude variation with respect to evolution state variable. The detector noise rate is analysed with respect to threshold. The detection rate of various attacks such as DDOS, Random and false data injection attacks is also analysed. The proposed mathematical model is effectively reconstructed to frame the original sinusoidal signal from the evaluator state variable using reconfigurable Euclidean detectors.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Mallikarjunaswamy Srikantaswamy

Department of Electronics and Communication Engineering, JSS Academy of Technical Education

JSSATE-B Campus, Dr. Vishnuvardhan Road, Uttarahalli - Kengeri Main Road

Srinivasapura-Post Bengaluru – 560060 Karnataka, India

Email: mallikarjunaswamys@jssateb.ac.in

1. INTRODUCTION

The Power grid is considered to be a significant backbone of infrastructure, which has a profound effect on the economy and the day-to-day routines. Fiascos in the power grid normally have shattering effects. With the beginning of fresh skills, the out-of-the-way power grid is updated by a grid that is a distinctive smart cyber-physical system (CPS) that includes additional implanted smartness and networking competence. Sensors are furnished all over the system to observe different grid features, like the meter & voltage fluxes in such arrangements [1]–[3]. The gathered data by the sensors aids to give a reaction to the physical power grids. So, that kind of a CPS comprises two-approach messages among the controller scheme and the physical apparatuses as depicted in Figure 1. Numerous evolving attacks precisely aiming at the control and communication arrangements in smart grid are uncovered. A broad approach to detect physical altering is done by a process of installing an evaluator along with a corresponding detector in the given controller. A remarkable variance among the estimated and measured states indicates a likely attack on the structure. Here, we showcase a framework of security utilizing the Kalman filter (KF) for a given smart grid. The KF produces assessments for state variables by means of the mathematical prototype for the power grid & the information got by the system of sensors is installed so as to observe the power grid. Then we can also

use a χ^2 -detector which can further be used to identify the inconsistencies amid the assessed data & the experimental data and trigger alarms [4].

Nevertheless, the learning depicts that the χ^2 -detector can't identify the statistically resultant false data injection attack. We broadly examine this attack, along with the planned KF framework and project a supplementary detection method by means of the Euclidean distance metric [5], [6]. The main objectives include i) we plan a mathematical prototype along with the KF to identify likely attacks & errors on the system of smart grid, ii) then examine the functioning of the investigative technique χ^2 -detector, in recognizing errors & arbitrary attacks, and iii) we evaluate the restraint of the χ^2 detector in sensing the analytically resultant false data injection attack and consequently project a fresh detector of Euclidean to be joined with KF and d) then showcase the efficacy of the planned methods through widespread simulations & study on real-world systems. The remaining work is structured as below. Section 2 shows the motivation & the associated work on smart-grid security. Section 3 shows the planned structure, the measured prototype of the power grid & the KF estimator. Section 4 shows the two detectors employed in the structure so as to identify different attacks in the arrangement. In section 5, outcomes of the planned framework and the interpretations are detailed. Lastly, section 4 details the conclusion.

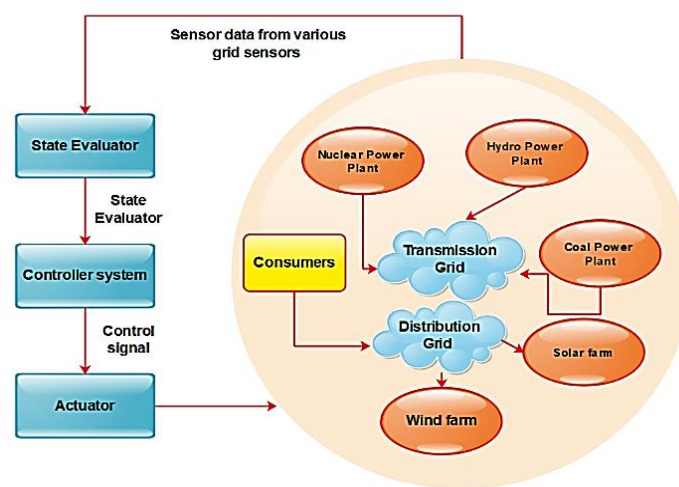


Figure 1. Fundamental block diagram of a smart grid system

2. MOTIVATION AND RELATED WORK

In this segment, we examine different security aspects deliberated in the literature. The modern studies on smart grid security could be largely classified into three sets. The research in the first group pacts with the wired or wireless security of networking between cyber constituents in the smart grid. The work inside second group would examine the early detection of abnormalities in the structure. The early anomaly detection methods can forehandedly safeguard the system. The research in the third group smears the control theories in the security procedure utilizing different state assessment & revealing methods.

A signature-dependent message validation system was projected, that works in the multicast authentication format in order to lessen the size of signature & bandwidth of communiqué at the price of augmented calculation. The projected method includes detecting, reacting, data recollecting & alarm supervision mechanisms. An error inside the smart grid scheme is constantly shown in the method of alteration in voltage, phase or current. Prevailing security methods are either i) not feasible, ii) mismatched with the smart grid, iii) not suitably scalable, or iv) not sufficient. Our research shows a structure, dependent on a state-space system obtained by the voltage stream reckonings, to secure various kinds of attacks & errors, corresponding to the Injection attack of the false data. We project an altered detector dependent on the metric of Euclidean distance to identify a complex Injection attack of the given false data over the power grid mechanism.

3. PROJECTED STRUCTURE FOR SMART GRID BY MEANS OF RED

In this segment, we showcase the complete report of the structure of the given security for the smart grid which is utilizing the KF. The structure is proficient in identifying different assaults, including short & long-term arbitrary attacks including the development of a state-space prototype by the three-phase

sinusoidal voltage reckonings [7]–[9]. Figure 2 depicts the projected structure of security, where we can see that KF assesses the figures for the given state parameters depending on state of the system and the statistics from various values of sensors. The KF produced projected values and the detected figures alongside variables of state are then given inside the detector. After this, the two-state vectors are equated by the detector. If the two vary from each other considerably and are above an assured pre-calculated threshold, an alarm to imply a likely smart grid attack is initiated by the detector.

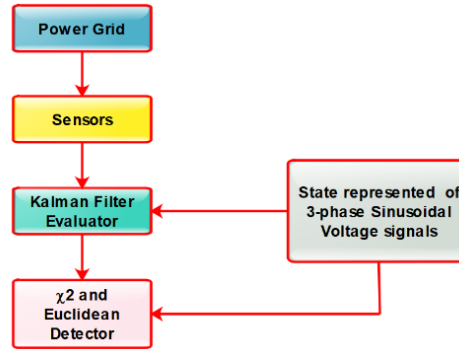


Figure 2. Security execution protocols of the smart grid system

3.1. Prototype of state space

The power structure installs sensors, like phasor units of measurement, so as to assess the system state at different places and stint to make sure of the even operation of the power scheme. the sinusoidal voltage mathematical model is given in (1). the three phases voltage signals are given in (2) and (3) respectively [10], [11].

$$S_1(t) = A_f \cos(\omega t + \varphi) \quad (1)$$

$$S_2(t) = A_f \cos(\omega t + \varphi - \frac{2\pi}{3}) \quad (2)$$

$$S_2(t) = A_f \cos(\omega t + \varphi - \frac{4\pi}{3}) \quad (3)$$

Extension of (1) as shown in (4).

$$S_1(t) = A_f * \cos \omega t * \cos \varphi - A_f * \sin \omega t * \sin \varphi \quad (4)$$

Where A_f is described the amplitude function, ωt is represented as the angular frequency and φ is identified as phase angle with respect to time. When the angular frequency is constant with respect to the time then amplitude and phase can be represented in state-space model is given in (5).

$$S_1(t) = g_1 * \cos \omega t - g_2 * \sin \omega t \quad (5)$$

Where $g_1 = A_f^8 \cos \varphi$ and $g_2 = A_f^2 \sin \varphi$ is the state variables at no delay condition in the model. The tiny noise is applied to the system and this condition is given in (6).

$$\begin{bmatrix} g_1(t+1) \\ g_2(t+2) \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} g_1(t) \\ g_2(t) \end{bmatrix} + w(t) \quad (6)$$

In (6) can be represented in simplest form and it is given in (7).

$$g(t+1) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} g(t) + w(t) \quad (7)$$

Where $g(t) = \begin{bmatrix} g_1(t) \\ g_2(t) \end{bmatrix}$ and $w(t)$ is described as process noise. At nonstationary deterministic condition the actual voltage signal is given in (8). Where $h(t)$ is describes the actual voltage signal with respect to time and $F(t)$ is represents the measurement noise.

$$h(t) = [\cos wt - \sin wt] \begin{bmatrix} g_1(t) \\ g_2(t) \end{bmatrix} + \Gamma(t) \quad (8)$$

3.2. Reconfigurable Kalman filter (RKF)

Figure 3 depicts the control system alongside the KF entrenched on the approximation of the vector of state & detector in order to do the identification of errors [12], [13]. The (9) represents the KF technique where $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, from in (8) it can be represented in simplest form and it is given in (10).

$$g(t+1) = Ag(t) + w(t) \quad (9)$$

$$h(t) = V_c(t)x(t) + s(t) \quad (10)$$

Where $h(t)$ is identified as sensor measurement vector, $V_c(t)$ is represents the $[\cos wt - \sin wt]$ and $s(t)$ is described as a white gaussian noise at mean is zero and standard deviation 'ρ' it is not depend on process noise and initial condition [14], [15]. The KF mean and covariance of the evaluator is defined by (11)-(14).

$$\hat{s}(t|t) = E_{st}[g(t), h(t), \dots \dots h(t)] \quad (11)$$

$$\hat{s}(t|t-1) = E_{st}[g(t), h(t), \dots \dots h(t-1)] \quad (12)$$

$$P_t(t|t) = \Sigma(t|t-1) \quad (13)$$

$$P_t(t|t-1) = \Sigma(t|t-1) \quad (14)$$

Where, $\hat{s}(t|t)$ is represents the signal evaluator with respect to 't', $\hat{s}(t|t-1)$ is describes the signal evaluator with respect to time 't-1', $P_t(t|t)$ is identified as covariance of the Evaluator with respect to the 't' and $P_t(t|t-1)$ is represents the covariance of the Evaluator with respect to the 't-1'. The KF Iteration process is represented by (15) and (16).

$$\hat{s}(t+1|t) = A\hat{s}(t) \quad (15)$$

$$P_t(t|t-1) = AP_t(t-1)A^T + Z \quad (16)$$

Where $\hat{s}(t+1|t)$ is represents the state and covariance of the evaluator with respect to t to t+1-time steps, $P_t(t|t-1)$ is describes the covariance of the evaluator with respect to t-1 to t and 'Z' is represents the covariance matrix process noise [16], [17]. The RKF measuring updates are represented by (17)-(19).

$$K_A(t) = P_t(t|t-1)V_c(t)^T(V_c(t)P_t(t|t-1)V_c(t)^T + R)^{-1} \quad (17)$$

$$P_t(t|t) = P_t(t|t-1) - K_A(t)V_c(t)P_t(t|t-1) \quad (18)$$

$$\hat{s}(t) = \hat{s}(t|t-1) + K_A(t)(h(t) - V_c(t)\hat{s}(t|t-1)) \quad (19)$$

Where $K_A(t)$ is described the reconfigurable Kalman gain and R represents the covariance matrix noise analysis. The Kalman Gain before the evaluation is represented by (20), (21) and enhancement of (19) is given in (22). The evaluation error $\delta(t)$ is represented in (23).

$$P \triangleq \lim_{k \rightarrow \infty} P_t(t|t-1) \quad (20)$$

$$K_A = P_t V_c^T (V_c P_t - 1)^{-1} \quad (21)$$

$$\hat{s}(t+1) = A\hat{s}(t) + K_A[(h(t+1) - V_c A\hat{s}(t) + \beta u(t))] \quad (22)$$

$$\delta(t) \triangleq \hat{s}(t) - s(t) \quad (23)$$

3.3. Model generalization

The state-space model is detailed in section 3. It could be widespread for power grid dimensions. The voltage monitored at every bus could stay in the method of a sinusoidal [18], [19]. Let us study the three-phase bus structure as shown in Figure 4.

$$\zeta_x = \sum_{i=1}^n |S_x| |S_i| Z_{xi} \sin(\varphi_x - \varphi_i) - \cos(\varphi_x - \varphi_i) \quad (24)$$

$$\rho_x = \sum_{i=1}^n |S_x| |S_i| Z_{xi} \sin(\varphi_x - \varphi_i) - \cos(\varphi_x - \varphi_i) \quad (25)$$

Where $|S_x|$ is represented the voltage amplitude, $|S_i|$ has described the phase, Z_{xi} is identified as gain, ζ_x is represented the active power, ρ_x has described reactive power and x is the number of system buses [20], [21]. To determine unknown variables in each system buses by (24) and (25).

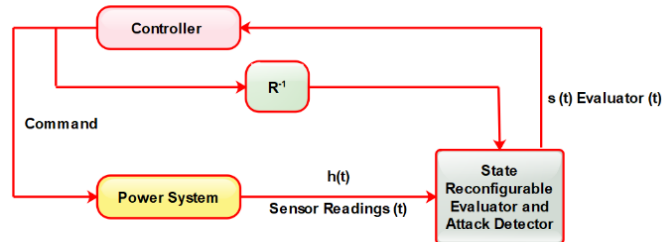


Figure 3. Proposed power grid

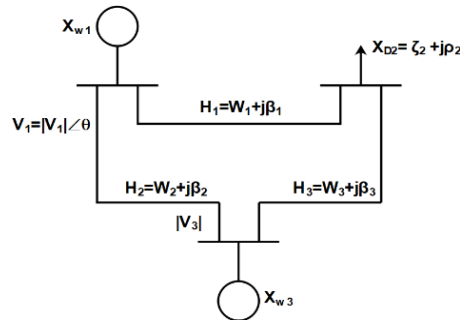


Figure 4. Fundamental three bus structure

3.4. Model of attack

The model attack occurs when FDIA gets introduced to the smart grid system. It is able to control a sub set of the sensor readings in the system. It is presumed that the invader is capable of controlling a subdivision of the sensor evaluations in the structure. there are three types of attacks namely: i) DDoS, ii) random, and iii) false data injection [22], [23].

3.5. DDoS attack

The DDoS attack is jamming the communication channel, compromising devices and flooding packets in networks to avoid data transfer. This kind of assault is such that wherein an opponent extracts few or every constituent of an unreachable control system. The bout of DDoS could be on control, sensor, or on both data.

3.6. Random attack

Here, the assaults aren't constructed to bypass the discovery procedure executed by the central system. Such arbitrary attacks can be produced at any point in time.

$$h'(t) = V_c(t)g'(t) + s(t) + h_a(t) \quad (26)$$

Where $h_a(t)$ is represented the random attack vector, $h'(t)$ is described as model observation and $g'(t)$ is identified as system process states [24].

3.7. False data-injection attack

It is alleged so as to know that the attacker is aware of the model of a given system, having variables ρ , R , A , β , V_c and gain K_A . The attacker could as well regulate a subdivision of sensors (Sbad). Where τ is represented the sensor selection matrix $\tau = \text{diag}(\gamma_1 + \gamma_1 + \gamma_2 + \gamma_3 + \gamma_4 + \dots \dots \dots + \gamma_m)$ and $x \in S_{bad}$.

$$h'(t) = V_c(t)g'(t) + s(t) + \tau h_a(t) \quad (27)$$

4. ATTACK DETECTOR

The RKF predictor computes the system state by means of the reckonings detailed in section 3.2. As the readings of a given meter are evident for that state, the planned assessments and the authentic meter evaluations are paralleled by the detector. In case the variance among the two is over an earlier calculated threshold, an alarm is generated to inform a likely attack [25], [26].

4.1. χ^2 -detector

The χ^2 -detector is a traditional one which castoff with RKF. The χ^2 -detector constructs χ^2 -test measurements from the RKF and parallels those with the threshold got from the customary χ^2 -Table 1 [27]. Let the residue $R(t+1)$ at $k+1$ sec be determined by (28) and a simplified (30) is presented by (29). The scalar test statistics of χ^2 -detector is given in (30).

$$R(t+1) \triangleq h(t+1) - \hat{h}(t+1|t) \quad (28)$$

$$R(t+1) \triangleq h(t+1) - V_c(A\hat{s}(t)) \quad (29)$$

$$w(t) = R(t)^{TB}(t)R(t)$$

Where $w(t)$ is represented as the precomputed threshold and $B(t)$ is described as the covariance matrix of $R(t)$. The reconstructed sinusoidal signals from evaluator of the reconfigurable Euclidean detector. The comparison analysis has been done with conventional methods by (30). Where ζ is represented the amplitude and ρ is described the evaluated voltage signal amplitude. Table 1 shows the experimental setup of χ^2 -detector used PKF.

$$d(\zeta, \rho) = \sqrt{(\zeta_1 - \rho_1)^2 + (\zeta_1 - \rho_1)^2 + (\zeta_1 - \rho_1)^3 + \dots \dots \dots + (\zeta_n - \rho_n)^2} \quad (30)$$

Table 1. Reconfigurable Kalman filter experimental setup

Particular	Quantity
Initial covariance matrix $\zeta(0 0)$	Identified matrix
Frequency	65 Hz
The initial value for $s_1(0)$	0
The initial value for $s_2(0)$	0
Amplitude	1 Volt
Sampling frequencies	2.5 Hz

4.2. Detector executing the distance metric of Euclidean

The false data injection assault is sensibly made to avoid the numerical detector, like the χ^2 -detectors. So, to identify such kinds of assaults, we acclaim a reconfigurable euclidean-based detector, that computes the aberration of the experiential figures compared to the assessed figures. To implement the reconfigurable euclidean detector, initially, sinusoidal signals are built from the state assessments and then equated with the quantities got from the sensors as depicted. If the variance among the two is more than the threshold ' 3α ' where α is represented the standard deviation, as in the situation of the χ^2 -detector, an alarm is produced. To reduce to 99.85% of false positives obtained because of noise, we fix the threshold.

5. IMPLEMENTATION AND EVALUATION OF PERFORMANCE

We executed the RKF Evaluator, Euclidean detector, and χ^2 -detector making use of MATLAB. The research setup and the preliminary figures are depicted in Table 1. A 65Hz signal of the sinusoidal voltage having arbitrary Gaussian noise is produced and given to the RKF estimator by way of the input. The input & the consequent sinusoidal signal got utilizing the state assessments are shown in Figures 5 to 9.

5.1. Attack/error detection utilizing the χ^2 -detector

Figure 5 depicts the simulation consequences utilizing the χ^2 -detector in the lack of attacks for some amount of duration. We can see that the assessed figures got from the KF estimator overlay with the input signal showing there is no change amongst the projected and the experimental figures. The RKF functions iteratively by amending its assessments utilizing the state-space model and the values got & the

assessments slowly congregate through the input signal. In the time of assaults, the projected assessments will not agree with the experiential analysis and $w(t)$ surpasses the threshold as depicted in Figure 6 depicts a short-duration attack being identified by the structure. Figure 7 depicts the discovery of the attack of the DDoS.

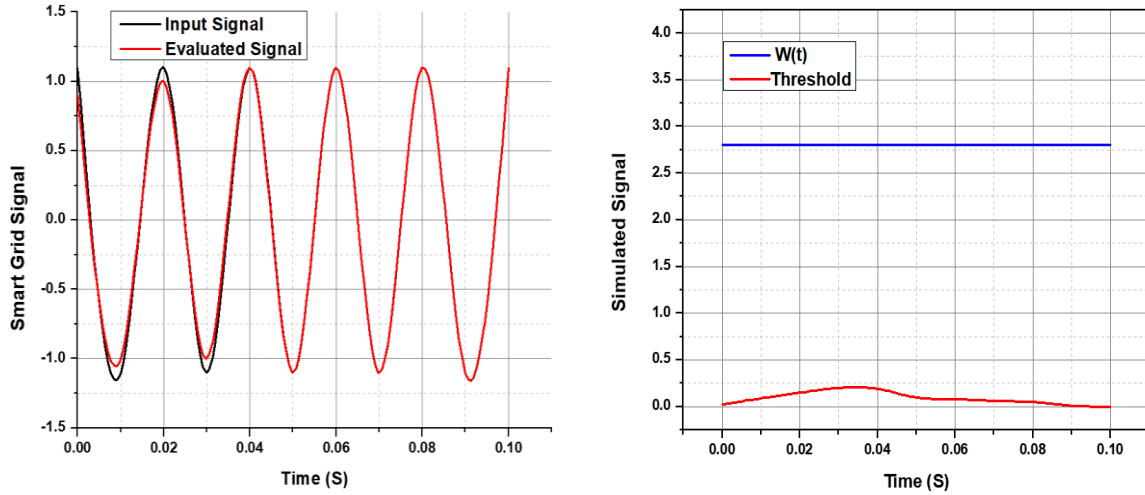


Figure 5. No attack/fault signal transfer response using χ^2 -detector

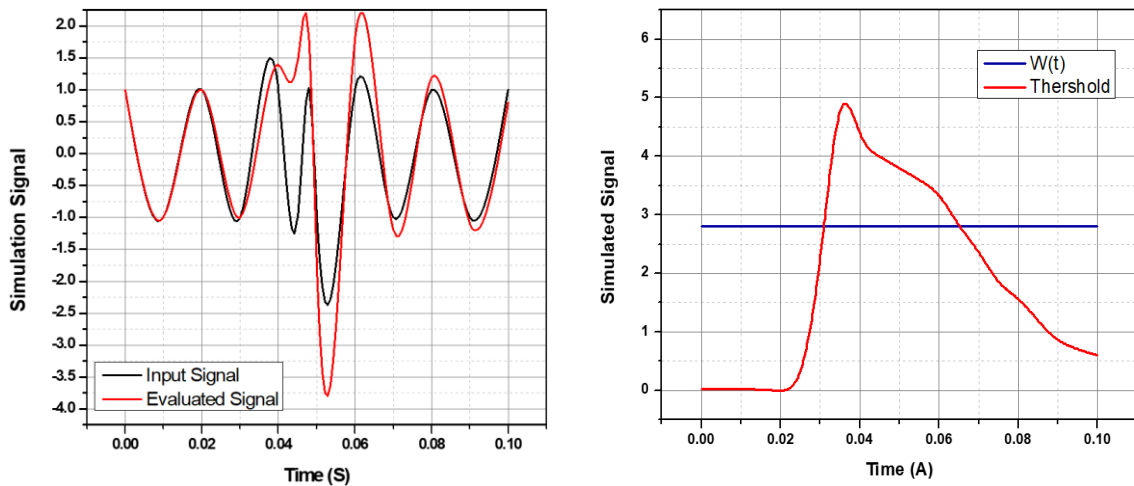


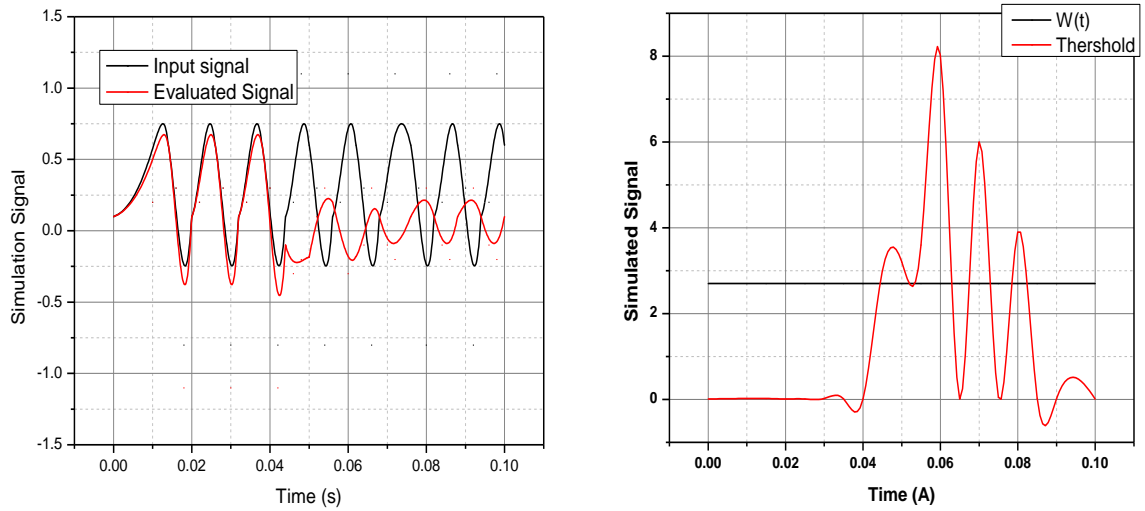
Figure 6. random attack for a short period transfer response using χ^2 -detector

5.2. False data injection attack detection using RKF

Here, it so happens that it injects forged sensor measurements which can mislead the system by executing the RKF estimator with the χ^2 -detector. The attack sequence can be obtained from in (31). Where 'n' is the represents the measurement of state space, $h^* = V_c s$, $M = \max_{i=1,2,3,4,\dots,n-1}$,

$$h_a(n+t) = h_a(t) - \frac{\lambda^{(x+1)}}{M} h^* \quad (31)$$

The source of the assault arrangement confirms that it overcomes the detector and upsurges the fault in the assessment of the state. The second subgraph in Figure 7 depicts the behavior of the χ^2 -detector beneath the injection attack of the false data. We observe the approximations don't match with the experimented figures in the top subgraph in Figure 7 Nevertheless, $w(t)$ never surpasses the threshold. We talk about this disadvantage in the subsequent phase by utilizing the Euclidean detector that could detect such attacks by continually observing the variation amongst the estimated and the experimented values.

Figure 7. DDoS attack for a short period transfer response using χ^2 -detector

5.3. False data injection attack discovery utilizing the Euclidean detector

This detector equates the alteration among the data experimented and the assessed data depending on the metric of the Euclidean distance. Nevertheless, to evade fake alarms due to dimension faults, we set the threshold to 3α as detailed in section IVB. Figure 8 shows the graph of the metric of the Euclidean distance while an attack is not there in the structure and the below subgraph in Figure 8 shows the plot when false data injection assault is there inside the structure.

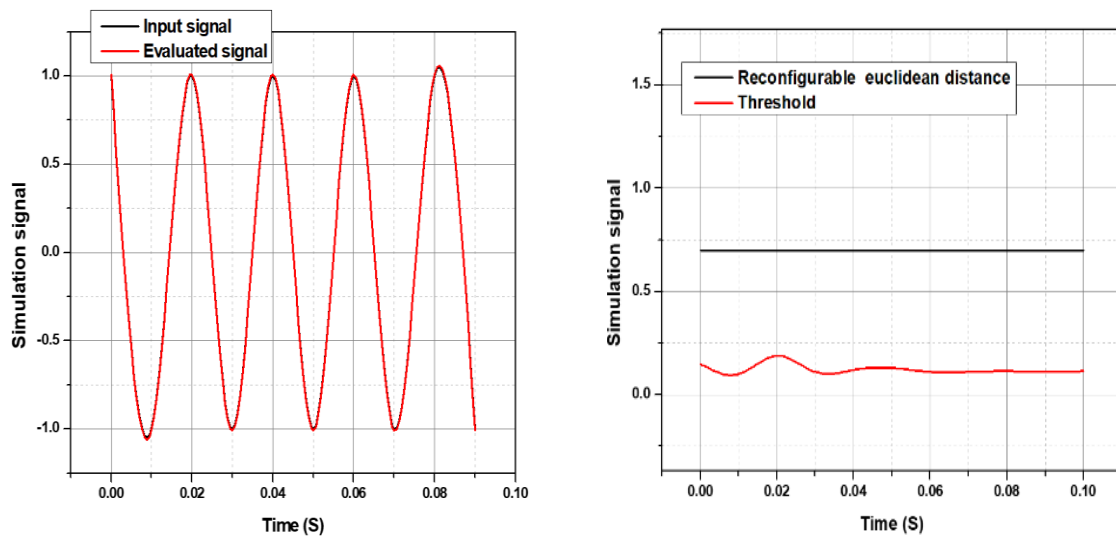


Figure 8. No attack/fault signal transfer response using reconfigurable Euclidean distance

5.4. Load change

In the prototype obtained, it is presumed that the load in the system is persistent. If at all we have a load change, then, there will be an alteration in the signal voltage through the buses. In case we know the load profile, then the change in amplitude of voltage produced because of the load change can be predicted. The factors inside the RKF can be attuned to reproduce the alteration inside the voltage because of the alteration in load. It permits us to get assessments for the state variables subsequent to the change in load. Figure 9 depicts that the assessments meticulously trail the signal along with the load alteration at time step 0.08, the random bout is identified by the χ^2 detector & Euclidean detector in such situation.

5.5. χ^2 -Detector versus reconfigurable Euclidean detector

The likelihood of assault discovery in either of detectors is mainly reliant on the assessment of the threshold. In χ^2 -detector, the verge is got from the χ^2 Table 1 Likewise, in reconfigurable Euclidean detector, the Gaussian distribution standard deviation gives the threshold.

Here in our research, the fixing of the significance of the thresholds in either of detectors to screen 99.15% of noise is done. Hence, the likelihood of wrong alarms because of noise will be less than 0.85%. Normally, the Euclidean detector is considered extra sensitive for variations than compared to the χ^2 -detector. In case the noise factors are not recognized before, the χ^2 -detector is better because it manages the soft faults better. Nevertheless, a drawback of the χ^2 -detector compared to the reconfigurable Euclidean detector is its incompetence to identify a false data injection assault.

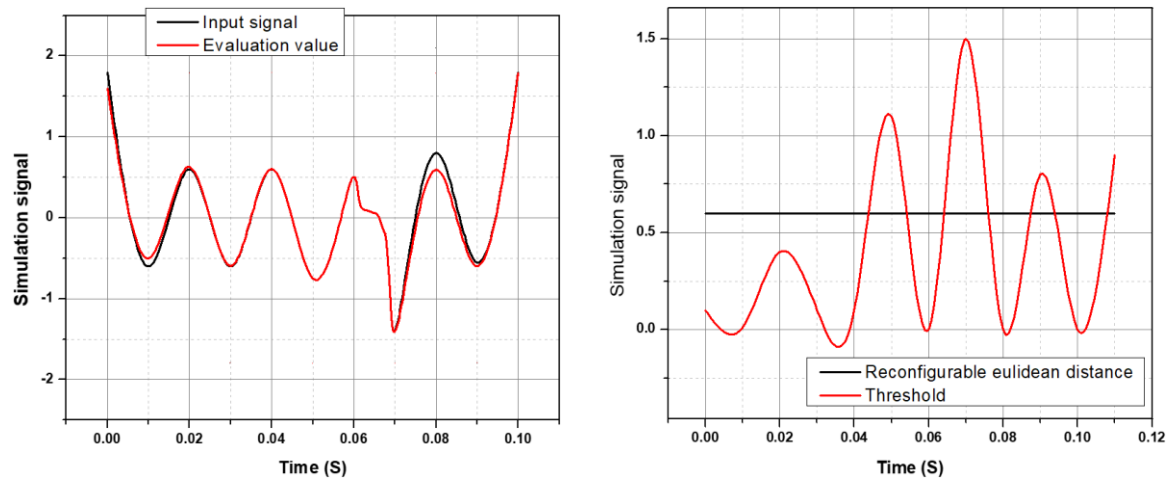


Figure 9. DDoS attack for a short period transfer response using reconfigurable Euclidean distance

5.6. Proposed IEEE 9-bus system using RED to detect false data injection attack

Figure 10 depicts a 9-bus structure of IEEE with sensors to observe the state factors and the estimator for bus 3. The 9-bus structure is replicated using the MATPOWER platform in MATLAB. The voltages and phases, got by unravelling the 9-bus power structure in MATPOWER, are utilized like factors of state in the RKF estimator. A related framework could be presumed for every bus in the structure. In order to understand, merely bus 3 is deliberated. The assault order h_a is produced by the opponent. The sensors which are there in the bus inform their interpretations to the matching RKF estimators and reconfigurable euclidean detectors. The positive identification of the False Data Injection attack on bus 3 is depicted in Figure 11.

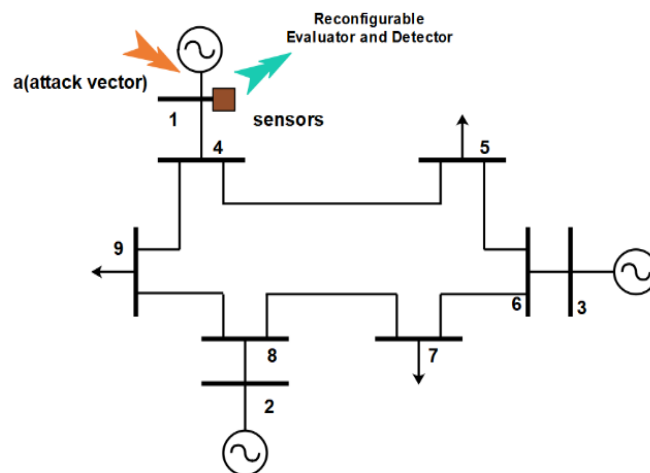


Figure 10. Proposed false data injection attack using IEEE 9-bus structure

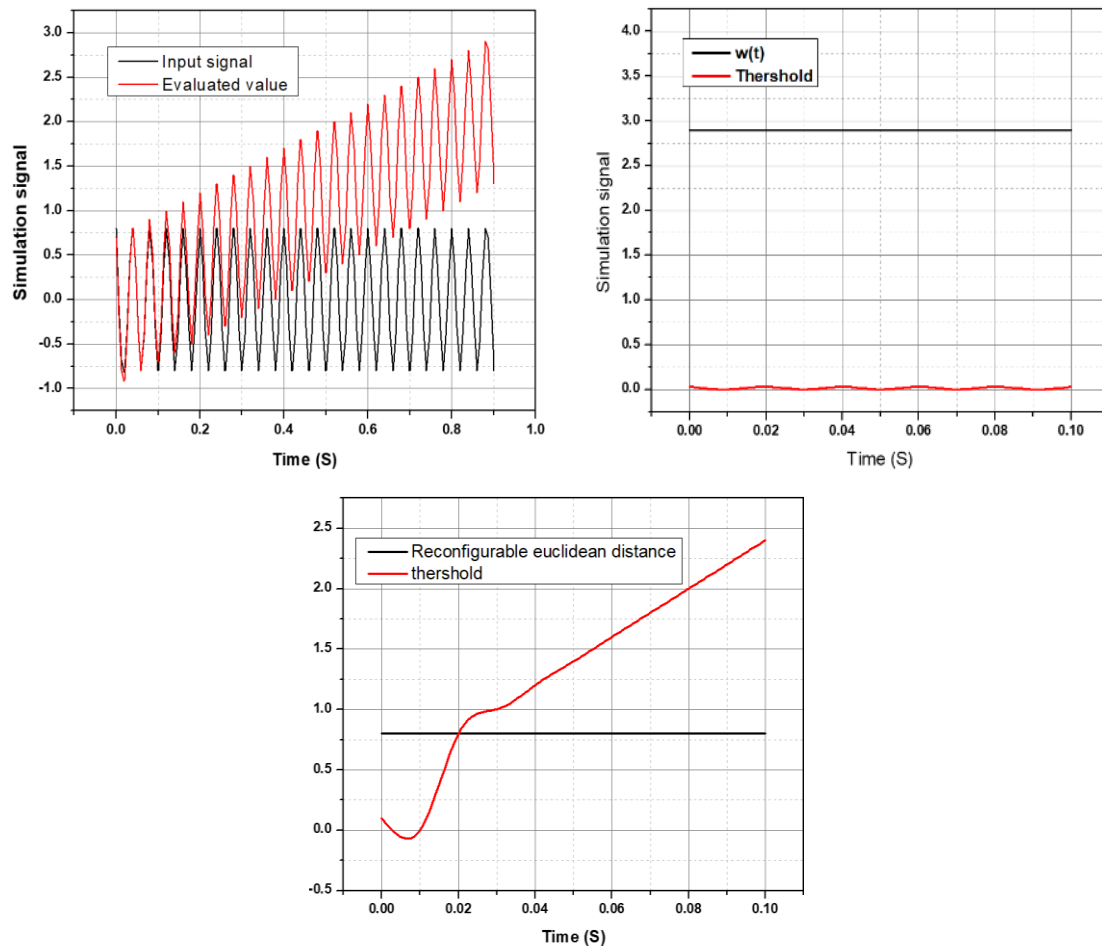


Figure 11. IEEE 9 bus system used to detect the false data attack

6. CONCLUSION

The proposed method is implemented using reconfigurable Kalman filter, χ^2 detector and reconfigurable euclidean detector for smart grid system. The proposed system has improved the detection efficiency of the different types of faults and attacks such as DDoS, FDIA and Random attacks compared to the conventional methods (0.51%, 0.3% and 0.42%). The proposed model improves the security and controlling capability of smart grid by reducing Euclidean detector noise. With respect simulation analysis, it shows the proposed method improves detection rate and security compared with conventional methods. Future scope: The proposed methods is enhanced to detect the faults in smart electric meters in residential area along with detection of faults and attacks in smart grids.

ACKNOWLEDGEMENTS




The authors would like to thank, SJB Institute of Technology, Bengaluru, JSS Academy of Technical Education, Bengaluru, Sri Jayachamarajendra College of Engineering, Mysore, Visvesvaraya Technological University (VTU), Belagavi and Vision Group on Science and Technology (VGST) Karnataka Fund for Infrastructure strengthening in Science & Technology Level-2 sponsored "Establishment of Renewable Smart Grid Laboratory" for all the support and encouragement provided by them to take up this research work and publish this paper.

REFERENCES




- [1] S. R. Salkuti, "Artificial fish swarm optimization algorithm for power system state estimation," *Indonesian Journal of Electrical Engineering and Computer Science*, 2020, pp. 1130-1137, doi: 10.11591/ijeecs.v18.i3.pp1130-1137.
- [2] Y. B. S. Bri, "Torque estimator using MPPT method for wind turbines," *International Journal of Electrical and Computer Engineering*, 2020, pp. 1208-1219, doi: 10.11591/ijece.v10i2.pp1208-1219.
- [3] M. Khalaf, A. Youssef and E. El-Saadany, "Detection of false data injection in automatic generation control systems using Kalman filter," *IEEE Electrical Power and Energy Conference (EPEC)*, 2017, pp. 1-6, doi: 10.1109/EPEC.2017.8286194.

- [4] M. M. Rana and L. Li, "Distributed Generation Monitoring of Smart Grid Using Accuracy Dependent Kalman Filter with Communication Systems," *12th International Conference on Information Technology - New Generations*, 2015, pp. 496-500, doi: 10.1109/ITNG.2015.154.
- [5] Y. Wang, Z. Zhang, J. Ma and Q. Jin, "KFRNN: An effective false data injection attack detection in smart grid based on Kalman filter and recurrent neural network," *IEEE Internet of Things Journal*, vol. 9, no. 9, pp. 6893-6904, 2022, doi: 10.1109/IJOT.2021.3113900.
- [6] Y. Liu and L. Cheng, "Relentless false data injection attacks against kalman filter based detection in smart grid," *IEEE Transactions on Control of Network Systems*, doi: 10.1109/TCNS.2022.3141026.
- [7] J. Sawodny, O. Riedel and T. Namerikawa, "Detection of attacks in smart grids via extended Kalman filter and correlation analysis," *59th Annual Conference of the Society of Instrument and Control Engineers of Japan (SICE)*, 2020, pp. 663-669, doi: 10.23919/SICE48898.2020.9240229.
- [8] S. H. Mohamad, M. A. M. Radzi, N. F. Mailah, N. I. A. Wahab, A. Jidin and M. Y. Lada, "Adaptive notch filter under indirect and direct current controls for active power filter," *Bulletin of Electrical Engineering and Informatics*, vol. 9, no. 5, pp. 1794-1802, 2020, doi: 10.11591/eei.v9i5.2165.
- [9] Y. Zhang, H. Wang and H. Wang, "Integrated navigation positioning algorithm based on improved Kalman Filter," *International Conference on Smart Grid and Electrical Automation (ICSGEA)*, 2017, pp. 255-259, doi: 10.1109/ICSGEA.2017.55.
- [10] Y. Jiang and Q. Hui, "Kalman filter with diffusion strategies for detecting power grid false data injection attacks," *IEEE International Conference on Electro Information Technology (EIT)*, 2017, pp. 254-259, doi: 10.1109/EIT.2017.8053365.
- [11] F. Akbarian, A. Ramezani, M. -T. Hamidi-Beheshti and V. Haghighat, "Intrusion detection on critical smart grid infrastructure," *Smart Grid Conference (SGC)*, 2018, pp. 1-6, doi: 10.1109/SGC.2018.8777815.
- [12] R. Shivaji, k. R. Nataraj, S. Mallikarjunaswamy and K. R. Rekha, "Implementation of an effective hybrid partial transmit sequence model for peak to average power ratio in MIMO OFDM system," *ICDSMLA 2020. Lecture Notes in Electrical Engineering, Springer*, vol. 783, pp. 1343-1353, 2020, doi: 10.1007/978-981-16-3690-5_129.
- [13] B. Aissa, T. Hamza, G. Yacine, and N. Mohamed, "Impact of sensorless neural direct torque control in a fuel cell traction system," *International Journal of Electrical and Computer Engineering*, vol. 11, no. 4, pp. 2725-2732, 2021, doi: 10.11591/ijece.v11i4.pp2725-2732.
- [14] N. Zhou, D. Meng, Z. Huang and G. Welch, "Dynamic state estimation of a synchronous machine Using PMU data: a comparative study," *IEEE Transactions on Smart Grid*, vol. 6, no. 1, pp. 450-460, 2015, doi: 10.1109/TSG.2014.2345698.
- [15] T. N. Manjunath, S. Mallikarjunaswamy, M. Komala, N. Sharmila and K. S. Manu, "An efficient hybrid reconfigurable wind gas turbine power management system using MPPT algorithm," *International Journal of Power Electronics and Drive Systems*, vol. 12, no. 4, pp. 2501-2510, 2021, doi: 10.11591/ijpeds.v12.i4.pp2501-2510.
- [16] J. Zhao and L. Mili, "A decentralized h-infinity unscented Kalman filter for dynamic state estimation against uncertainties," *IEEE Transactions on Smart Grid*, vol. 10, no. 5, pp. 4870-4880, 2019, doi: 10.1109/TSG.2018.2870327.
- [17] M. M. Rana, "Extended Kalman filter based distributed state estimation algorithm for cyber physical systems," *3rd International Conference on Inventive Computation Technologies (ICICT)*, 2018, pp. 653-655, doi: 10.1109/ICICT43934.2018.9034255.
- [18] K. Manandhar, C. Xiaojun, F. Hu and Y. Liu, "Combating false data injection attacks in smart grid using Kalman filter," *International Conference on Computing, Networking and Communications (ICNC)*, 2014, pp. 16-20, doi: 10.1109/ICNC.2014.6785297.
- [19] S. R. Salkuti, S. Pagidipala, and S. C. Kim, "Comprehensive analysis of current research trends in energy storage technologies," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 24, no. 3, pp. 1288-1296, 2021, doi: 10.11591/ijeecs.v24.i3.pp1288-1296.
- [20] S. Mallikarjunaswamy, N. Sharmila, G. K. Siddesh, K. R. Nataraj, M. Komala, "A novel architecture for cluster based false data injection attack detection and location identification in smart grid. advances in thermofluids and renewable energy," *Lecture Notes in Mechanical Engineering. Springer, Singapore*, 2021, doi: 10.1007/978-981-16-3497-0_48.
- [21] S. Mallikarjunaswamy, N. Sharmila, D. M. Kumar, M. Komala and H. N. Mahendra, "Implementation of an effective hybrid model for islanded microgrid energy management," *Indian Journal of Science and Technology*, vol. 13, no. 27, pp. 2733-2746, 2020, doi: 10.17485/IJST/v13i27.982.
- [22] T. A. Madhu, M. Komala, V. Rekha, S. Mallikarjunaswamy, N. Sharmila and S. Pooja, "Design of fuzzy logic-controlled hybrid model for the control of voltage and frequency in microgrid," *Indian Journal of Science and Technology*, vol. 13, no. 35, pp. 3612-3629, 2020, doi: 10.17485/IJST/v13i35.1510.
- [23] V. P. Bhuvana, M. Huemer and A. Tonello, "Battery internal state estimation using a mixed Kalman cubature filter," *IEEE International Conference on Smart Grid Communications (SmartGridComm)*, 2015, pp. 521-526, doi: 10.1109/SmartGridComm.2015.7436353.
- [24] H. Abbas, H. Abid, K. Loukil, M. Abid and A. Toumi, "Fuzzy-based MPPT algorithm implementation on FPGA chip for multi-channel photovoltaic system," *International Journal of Reconfigurable and Embedded Systems*, vol. 11, no. 1, pp. 49-58, 2022, doi: 10.11591/ijres.v11.i1.pp49-58.
- [25] B. Özsoy and M. Göl, "A hybrid state estimation strategy with optimal use of pseudo-measurements," *IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*, 2018, pp. 1-6, doi: 10.1109/ISGTEurope.2018.8571513.
- [26] M. M. Rana, M. K. R. Khan and A. Abdelhadi, "IoT architecture for cyber-physical system state estimation using unscented Kalman Filter," *Second International Conference on Inventive Research in Computing Applications (ICIRCA)*, 2020, pp. 910-913, doi: 10.1109/ICIRCA48905.2020.9183350.
- [27] I. Onyegbadue, C. Ogbuka and T. Madeume, "Robust least square approach for optimal development of quadratic fuel quantity function for steam power stations," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 25, no. 2, pp. 732-740, 2022, doi: 10.11591/ijeecs.v25.i2.pp732-740.




BIOGRAPHIES OF AUTHORS

Prakyath Dayananda    has completed BE in EEE at CIT, Tumkur and M.Tech in CAID at SSIT, Tumkur and secured Gold medal in M.Tech. I had 9 years Teaching experience in teaching and am currently working as Assistant professor in SJBIT, Bangalore. He can be contacted at email: prakayath100@gmail.com.






Mallikarjunaswamy Srikantaswamy    is currently working as an Associate Professor in Department of Electronics and Communication Engineering at JSS Academy of Technical Education, Bangalore. He obtained his B. E degree in Telecommunication Engineering from Visvesvaraya Technological University Belgaum in 2008, M. Tech degree from Visvesvaraya Technological University Belgaum in 2010 and was awarded Ph. D from Jain University in 2015. He has 11+ years of teaching experience. His research work has been published in more than 42 International Journals and conference. He received funds from different funding agencies. Currently guiding five research scholars in Visvesvaraya Technological University Belgaum. He can be contacted at email: mallikarjunaswamys@jssateb.ac.in.






Sharmila Nagaraju    has completed her B.E in EEE at SJCE, Mysore and M. Tech in CAID at NIE Mysore. Secured second rank in Bachelor of Engineering degree. She has Eight years of experience in teaching and is currently working as an Assistant Professor in RNSIT, Bangalore.electronics and its applications. She can be contacted at email: Sharmila.n.89@gmail.com.



Rekha Velluri    completed her B.E and M. Tech in Computer Science and Engineering from Visvesavaraya Technological University Belgavi. She has more than 16 years of teaching experience. Published many papers in national and international conference and currently working as an Assistant Professor in Christ University. She can be contacted at email: rekha.v@christuniversity.in.



Doddananjedevaru Mahesh Kumar    is presently working as Associate Professor in the Dept. of Electronics and Instrumentation Engineering, JSS Academy of Technical Education, Bengaluru. He is working in the teaching field from the past 21 years and has published more than 30 papers in International Journals, National and International Conferences. He has 4 patent publications & presently guiding three research scholars under Visvesvaraya Technological University. His research areas include Biomedical Signal Processing, Sensors and amp; and Transducers. He can be contacted at email: dmkjsate@gmail.com.