Detection of Gaussian Attacks in Power Systems under a Scalable Kalman Consensus Filter Framework

Arnold Fernandes, Rui Bo, Jonathan Kimball, Bruce McMillin
Missouri University of Science and Technology, Rolla MO, 65401

***Abstract*—The dynamic non-linear state-space model of a power-system consisting of synchronous generators, buses, and static loads has been linearized and a linear measurement function has been considered. A distributed dynamic framework for estimating the state vector of the power system has been designed here. This framework employs a type of distributed Kalman filter (DKF) known as a Kalman consensus filter (KCF) which is located at distributed control centers (DCCs) that fuse locally available noise ridden measurements, state vector estimates of neighboring control centers, and a prediction obtained by the linearized model to obtain a filtered state vector estimate. Further, the local residual at each control center is checked by a median χ^2 detector designed here for bad data/Gaussian attack detection. Simulation results show the working of the KCF for an 8 bus 5 generator system, and the efficacy of the median χ^2 detector in detecting the DCC affected by Gaussian attacks.**

***Index Terms*—Distributed estimation, security, attack mitigation**

I. Introduction

In static state estimation framework the number of measurements needed to estimate the state needs to be greater than the number of states in the system so as to have enough redundancy. For the case of a power system the states are the bus voltage magnitude and the bus voltage angles. The measurements could be of the active/reactive power flows, branch currents, active/reactive power injections, bus voltage magnitudes/angles, etc. For a dynamic state estimator (DSE) however the number of measurements can be less than the number of states provided the measurements are available at a higher frequency. With the increasing use of Phasor Measurement Units (PMUs), high-frequency synchrophasor measurement can be obtained in power systems. This allows utilizing dynamic state estimators rather that the traditional static state estimator (SSE) [1–3]. Increasing efforts are being put towards utilizing DSEs for power system [4]. With increase in distributed energy resources (DERs) and dynamic loads in the distribution system, the accuracy of the SSE becomes questionable and the time required in computing the state estimates becomes critical and hence the increased drive towards utilizing DSEs. DSEs can incorporate a physics-based dynamical model of the system under consideration to get an estimate of the system state when only a subset of the states are measurable by the use of a Luenberger observer [5] and even when the measurements are noise ridden by using a Kalman filter (KF) [6].

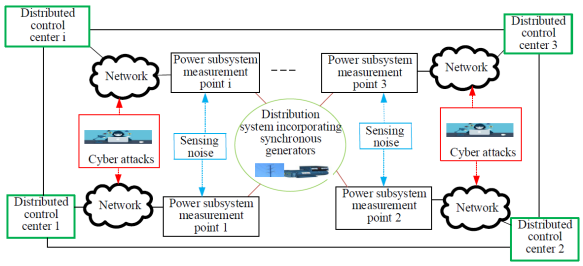

Fig. 1: Distributed Power System under Cyber Attack [7]

A DSE also has the advantage of making use of information from previous time steps and predicting future state estimates. Compared to SSE estimates this makes the DSE estimates more robust to noise/bad data that are not temporally coherent.

Utilizing DCCs rather than a centralized control center is beneficial. The time taken in gathering measurements is reduced and so is the time taken for computing local state estimates as the DCC only needs to gather local measurements and information from neighboring control centers [8, 9]. Even though the DCC has many advantages, it can still be prone to cyber attacks. These cyber attacks could occur at the sensor level or when the measurements are in transit to the DCC via the communication network. It could also be possible for an adversary to modify the information being communicated between DCCs by injecting false information which will further affect the estimates computed by the neighboring DCCs (See Fig. 1).

This work utilizes a KF at each DCC. These KFs share information with KFs at neighboring DCCs and form a DKF network. The advantage of using KCF as the DKF algorithm is that though it is suboptimal, it is scalable. Further, a χ^2 detector is designed at each DCC by using the local residual and the local infinite horizon error covariance matrix. A median filter enhances the performance of the χ^2 detector against false alarms. To the best of the author's knowledge, an attack detection scheme for the KCF framework has not been applied towards power systems.

The outline of the paper is as follows. Section II-A describes the nonlinear dynamic model of power systems in the form of differential and algebraic equations (DAE). In Section II-B this model is linearized, discretized, and written in the standard state-space form. Section III discusses the traditional

centralized KF and the KCF framework. In Section IV the effect of sensor attacks on the KCF is considered under a Gaussian attack assumption, and the χ^2 detection scheme is extended for the KCF framework. Section V discusses the estimation results for an 8-bus, 5-generator power system model with and without attack which show the efficacy of our approach. Finally, Section VI discusses the conclusions and possible future work.

II. Problem Formulation

A. Power system nonlinear dynamic model

The nonlinear state-space model of the i^{th} generator can be given as

$$\dot{\delta}^i(t) = \omega^i(t) \tag{1}$$

$$\dot{\omega}^i(t) = -\frac{D^i}{2H^i}\omega^i(t) + \frac{\omega_0^i}{2H^i}(P_m^i - P_e^i(t)) \tag{2}$$

$$\dot{E}_q^i(t) = -\frac{1}{T^i}E_q^i(t) + b_0^i z_1^i(t) + b_1^i z_2^i(t) + \frac{X_q^i - X_d^i}{T^i}I_d^i(t) \tag{3}$$

$$\dot{z}_1^i(t) = z_2^i(t) \tag{4}$$

$$\dot{z}_2^i(t) = -c_1^i z_2^i(t) - c_0^i z_1^i(t) + u^i \tag{5}$$

where $\delta^i(t)$ is the generator rotor angle, $\omega^i(t)$ is the rotor angular velocity, H^i is the inertia, D^i is the damping factor, $P_e^i(t)$ is the active power delivered at the terminal, $E_q^i(t)$ is the quadrature axis transient voltage, P_m^i is the mechanical power delivered to the generator, $I_d^i(t)$ is the direct axis current, $z_1^i(t)$ and $z_2^i(t)$ are the internal states of the automatic voltage regulator (AVR) and u^i is the system input. Detailed explanation for the model can be found in [10] [11].

The algebraic equations showing the the KCL and power flow in the power system network are given next

$$\begin{aligned} I_d^i(t) =& E_q^i(t)\sum_{j=1}^{N}\big\{B^{ij}\cos(\delta^i(t)-\delta^j(t)) \\ & -G^{ij}\sin(\delta^i(t)-\delta^j(t))\big\} \end{aligned} \tag{6}$$

$$\begin{aligned} P_e^i(t) =& E_q^i(t)\sum_{j=1}^{N}E_q^j(t)\big\{B^{ij}\sin(\delta^i(t)-\delta^j(t)) \\ & +G^{ij}\cos(\delta^i(t)-\delta^j(t))\big\} \end{aligned} \tag{7}$$

The algebraic equations (6) and (7) can be eliminated by substituting them in the generator dynamic equations (3) and (2) respectively. The algebraic equations interconnects the nonlinear dynamics of the generators across the network. Furthermore, these equations are nonlinear in the states E_q^i, E_q^j, and contain sinusoidal terms of δ_i and δ_j. To simplify the analysis it is beneficial to consider a linearized model of the power system. In the next subsection the linearized model development procedure is explained.

B. Linearized power system model

The nonlinear interconnected power system model is linearized around an operating point. This operating point is found by solving the power flow equations. The linearization process can be found in [10]. After linearization, the power system model for N generators is given in standard form as

$$\dot{X} = AX + BU + W \quad ; \quad Y = CX + V, \tag{8}$$

where, $X = [{x^1}^T, {x^2}^T, \ldots, {x^N}^T]^T \in \mathbb{R}^{5N\times 1}$ is the linearized power system state vector, $x^i = \left[\Delta\delta^i, \Delta\omega^i, \Delta E_q^i, \Delta z_1^i, \Delta z_2^i\right]^T \in \mathbb{R}^{5\times 1}$ is the state vector of the i^{th} generator, $U = [\Delta u^1, \Delta u^2, \ldots, \Delta u^N]^T \in \mathbb{R}^{5\times 1}$ is the input vector, $W \in \mathbb{R}^{5N\times 1}$ is a vector that accounts for the process noise, $Y \in \mathbb{R}^{p\times 1}$ is the output or measurement vector with p being the number of measurements available, $V \in \mathbb{R}^{p\times 1}$ is the measurement noise vector,

$$A = \begin{bmatrix} A^1 & A^{12} & \ldots & A^{1N} \\ A^{21} & A^2 & \ldots & A^{2N} \\ \vdots & \vdots & & \vdots \\ A^{N1} & A^{N2} & \ldots & A^{NN} \end{bmatrix} \in \mathbb{R}^{5N\times 5N}$$

is the system matrix of the linearized power system with block matrix $A^{ij} \in \mathbb{R}^{5\times 5}$ showing the effect of generator i's dynamics on generator j, $B = \text{diag}(B^1, B^2, \ldots, B^N) \in \mathbb{R}^{5N\times 5}$ is the input matrix with block matrix $B^i \in \mathbb{R}^{5\times 1}$ showing the effect of generator i's input on the system, and $C = \text{diag}\,(C^1, C^2, \ldots, C^N) \in \mathbb{R}^{p\times 5N}$ is the output matrix with $C^i \in \mathbb{R}^{p^i\times 5}$ being the output matrix of the i^{th} generator.

By using Euler's approximation, one can convert the continuous-time model in (8) to can obtain a discrete-time model given as

$$X_k = A_d X_{k-1} + B_d U_{k-1} + W_{k-1} \quad ; \quad Y_k = CX_k + V_k, \tag{9}$$

where the subscript k indicates the time index, $A_d \in \mathbb{R}^{5N\times 5N}$ and $B_d \in \mathbb{R}^{5N\times 5}$ are the system matrix and the input matrix after discretization. Process noise and measurement noise are considered by W_k and V_k, respectively.

III. Distributed Dynamic State Estimation

A. Centralized Kalman Filter

Before moving to the DKF a brief explanation of the KF is given. The purpose of a KF is to get the state estimate given noise-ridden measurements and a noise-ridden process. The KF is also used to estimate the unmeasureable states by using information from measured quantities and knowledge of system dynamics and noise properties. The KF works best when the measurement noise, process noise and the initial states of the system are mutually independent at each and every time step. This is assumed to hold true here. Additionally, it is also assumed that $W_k \sim \mathcal{N}(0, Q)$ and $V_k \sim \mathcal{N}(0, R)$ where Q is the process noise covariance matrix and R is the measurement noise covariance matrix. The KF used for estimating the states of the power system can be given as

$$\begin{aligned} \hat{Y}_{k-1} =& C\hat{X}_{k-1} \\ \hat{X}_k =& A_d\hat{X}_{k-1} + B_d U_{k-1} + K_{k-1}\left(Y_{k-1} - \hat{Y}_{k-1}\right) \end{aligned} \tag{10}$$

where $\hat{X}_k$ is the state estimate at time instant k, $\hat{Y}_k$ is the measurement estimate, K_{k-1} is the Kalman gain, and P_{k-1} is the estimate uncertainty matrix.

B. Kalman Consensus Filter (DKF)

In this work, DKF previously utilized in wireless sensor networks (WSNs) [8] and perfected in [9] has been applied to power systems. The idea is that DCCs gather locally available measurements, exchange state estimates with neighboring DCCs and come up with a robust state estimate. By exchanging information in a synchronized manner, the DCCs are able to observe the entire system. The KF at the l^{th} DCC has the structure

$$\begin{aligned} Y^l_{k-1} =& C^l X^l_{k-1} + V^l_{k-1}, \quad \hat{Y}^l_{k-1} = C^l \hat{X}^l_{k-1}, \\ \hat{X}^l_k =& A_d \hat{X}^l_{k-1} + B_d U_{k-1} + K^l_{k-1}\left(Y^l_{k-1} - \hat{Y}^l_{k-1}\right) \\ &+ L^l_{k-1} \sum_{m \in \mathcal{N}^l} \left(\hat{X}^m_{k-1} - \hat{X}^l_{k-1}\right), \end{aligned} \tag{11}$$

where $\hat{X}^l_{k-1}$ is the l^{th} DCC state estimate at time $k-1$, C^l is the output matrix, Y^l_k is the vector of locally available measurements, $\hat{Y}^l_k$ is the estimate of Y^l_k, $V^l_k \sim \mathcal{N}\left(0, R^l\right)$ is the measurement noise having zero mean and covariance R^l, K^l_{k-1} is the Kalman gain of the l^{th} DCC, $\mathcal{N}^l$ is the set of neighbors communicating their state estimates with the l^{th} DCC and L^l_{k-1} is the communication gain (see Algorithm 1 in [9]). The A_d and B_d matrices were previously found in Section II-B by linearization. The stability and optimality properties of the DKF can be found in [9].

IV. Attack Detection

A χ^2 detector is generally used to detect bad measurements on the basis of the residual $e_{k-1} = \left(Y_{k-1} - \hat{Y}_{k-1}\right)$. The χ^2 detector checks if the weighted squared residual lies within a desired threshold

$$Q_{k-1} = e^T_{k-1} \mathcal{W} e_{k-1} \leq Q_{TH}, \tag{12}$$

where $e_{k-1} = \left(Y_{k-1} - \hat{Y}_{k-1}\right)$, $\mathcal{W} = \left(CP_\infty C^T + R\right)^{-1}$ and matrix P_∞ is the infinite-horizon estimate uncertainty matrix. The χ^2 detector gives an alarm if

$$Q_{k-1} \geq Q_{TH}. \tag{13}$$

Apart from detecting bad measurements, the χ^2 detector can also be used to detect Gaussian attacks. Compared to works that filter out Gaussian attacks by updating the measurement noise covariance matrix R by the use of Bayesian learning [12][7], the focus here is to detect such attacks first before mitigating them. As Gaussian attacks add to the noise of the measurements, they can be easily detected using the χ^2 detector. If the attacks were smart such as false data injection attack (FDIA) [13] or replay attack [14] then the χ^2 detector would be of no use.

A. Attack Detection in a DKF framework

A χ^2 detector is designed at each DCC. In the onset of attack, the measurements at the l^{th} DCC are modified

$$Y^{la}_{k-1} = C^l X^l_{k-1} + V^l_{k-1} + a^l_{k-1} \tag{14}$$

where $a^l_k \sim \mathcal{N}\left(\mu^{la}, R^{la}\right)$ is the attack vector. The goal of this attack is to bias the measurements and add noise to it so that the state estimates become less reliable. The attack-free residual at the l^{th} DCC is defined as $e^l_{k-1} = \left(Y^l_{k-1} - \hat{Y}^l_{k-1}\right)$ and the χ^2 detector checks if the χ^2 quantity Q^l_{k-1} stays under a threshold value Q^l_{TH} as

$$Q^l_{k-1} = {e^l_{k-1}}^T \mathcal{W}^l e^l_{k-1} \leq Q^l_{TH}, \tag{15}$$

$\mathcal{W}^l = \left(C^l P^l_\infty {C^l}^T + R^l\right)^{-1}$ and matrix P^l_∞ is the infinite-horizon estimate uncertainty matrix. The attack vector and noise vector add up and give a Gaussian distribution $V^l_k + a^l_k \sim \mathcal{N}\left(\mu^{la}, R^l + R^{la}\right)$. The attack modifies the residual to $e^{la}_{k-1} = \left(Y^{la}_{k-1} - \hat{Y}^l_{k-1}\right)$ which changes the χ^2 quantity to

$$Q^{la}_{k-1} = {e^{la}_{k-1}}^T \mathcal{W}^l e^{la}_{k-1} \geq Q^l_{k-1}. \tag{16}$$

The higher the mean or covariance of the attack signal the more corrupted the measurements, and the higher the chance of Q^{la}_{k-1} violating the χ^2 threshold and the attack being detected by the χ^2 detector. It was noticed during simulation runs that using the χ^2 detector by itself gave false alarms. A median filter was therefore applied to the χ^2 values in a time window of fixed size to obtain a median χ^2 value which will be denoted in this text as $\text{Med}\left(Q^l_{k-1}\right)$. A detector was then designed to compare $\text{Med}\left(Q^l_{k-1}\right)$ against the χ^2 threshold. If the median χ^2 value exceeds the χ^2 threshold, an alarm is triggered ($\beta = 1$), else the alarm is not triggered ($\beta = 0$) This mechanism is shown as

$$\beta(z) = \begin{cases} 1 & \text{if } z \geq z_{TH} \\ 0 & \text{if } z < z_{TH} \end{cases} \tag{17}$$

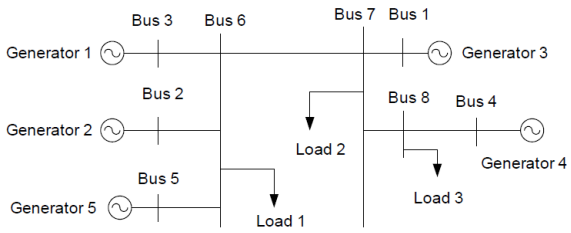

Fig. 2: 8-bus, 5-generator system [7][10].

V. Results and Discussion

The 8-bus, 5-generator system shown in Fig. 2 is used to test the working of the KCF. The three loads are considered to be static and so will not show up in the linearized dynamic model. Four DCCs are considered. They are shown as nodes in Fig. 3. The arrows to and from a node show the direction of communication. The arrow from the block named "Power System" to the DCC node indicate the power system measurements available at the DCC. It has been shown that the measurements available at DCC 2 have been appropriated by an attacker. The generator parameters along with the power flow solution used to linearize the non-linear dynamic power system model are given in TABLE I and the line parameters are as shown in TABLE II

The discretization time step is taken as 1.5 ms and A_d and B_d matrices are obtained from A and B matrices. The process noise $W^l_{k-1} \sim \mathcal{N}\left(0, 10^{-2} \times I_{25}\right)$. The simulation is run for 0.9 s. Next, a table mentioning the type of measurements

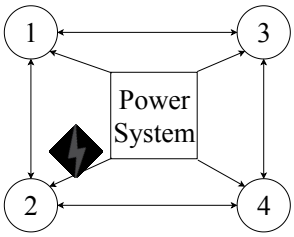

Fig. 3: Communication Topology.

available at each DCC is presented with noise covariance and χ^2 threshold values. Note that some of the states are measured by multiple sensors and this also accounts for measurement redundancy, which is common in power system. The χ^2 threshold values are calculated by considering the degree of freedom as the number of states measured, and a confidence level of 95%.

TABLE I: Generator parameters and operating conditions

Parameters	G_1	G_2	G_3	G_4	G_5
D_i	3.04	3.67	3.35	3.98	3.4
H_i	4.5	4.65	4.43	3.94	4.9
X'_{di}	0.0329	0.0329	0.3290	0.0239	0.2390
X_{di}	0.1016	0.1016	1.016	0.1016	1.016
T'_{doi}	5.57	5.57	5.57	5.57	5.57
b_{oi}	656	656	656	656	656
b_{1i}	1232	1232	1232	1232	1232
c_{oi}	3.23	3.23	3.23	3.23	3.23
c_{1i}	32.3	32.3	32.3	32.3	32.3
V	1.03	1.03	1.023	1.03	1.023
δ	0	0.1041	0.0933	0.0351	0.0607
Q	2.9141	1.3821	0.4187	2.1802	0.3469
P	3.1521	4.1016	0.4608	4.0578	0.1547

TABLE II: Line Parameters

Node i	Node j	R_{ij}	X_{ij}	B_{ij}
1	7	0.00335	0.01057	0.01436
2	6	0.00313	0.00368	0.00304
3	6	0.03004	0.05242	0.06305
4	8	0.00514	0.01074	0.01654
5	6	0.00701	0.02231	0.02632
6	7	0.04022	0.12685	0.15848
7	8	0.01714	0.04143	0.05013

TABLE III: Measurements available at DCCs along with associated noise covariance properties and χ^2 thresholds

DCC	Measurements	Noise Covariance	Q^l_{TH}
1	$\Delta\delta_2$, $\Delta\omega_2$, $\Delta\delta_5$, $\Delta\omega_5$	$R^1 = 2 \times 10^{-4} I_4$	13.3
2	$\Delta\delta_3$, $\Delta\omega_3$, $\Delta\delta_4$, $\Delta\omega_4$	$R^2 = 2 \times 10^{-4} I_4$	13.3
3	$\Delta\delta_1$, $\Delta\omega_1$, $\Delta\delta_3$, $\Delta\omega_3$	$R^3 = 2 \times 10^{-4} I_4$	13.3
4	$\Delta\delta_1$, $\Delta\omega_1$, $\Delta\delta_2$, $\Delta\omega_2$	$R^4 = 2 \times 10^{-4} I_4$	13.3

A. Healthy Case

In this subsection, the performance of the DKF and the χ^2 detector are studied in the absence of attacks. Figure 4a compares the change in angles of the 5 generators $\Delta\delta = [\Delta\delta_1, \Delta\delta_2, \Delta\delta_3, \Delta\delta_4, \Delta\delta_5]^T$ with the estimates of change in angles of the 5 generators $\Delta\hat{\delta} = [\Delta\hat{\delta}_1, \Delta\hat{\delta}_2, \Delta\hat{\delta}_3, \Delta\hat{\delta}_4, \Delta\hat{\delta}_5]^T$. In Figure 4b the change in frequencies $\Delta\omega = [\Delta\omega_1, \Delta\omega_2, \Delta\omega_3, \Delta\omega_4, \Delta\omega_5]^T$ are compared with the change in frequency estimates $\Delta\hat{\omega} = [\Delta\hat{\omega}_1, \Delta\hat{\omega}_2, \Delta\hat{\omega}_3, \Delta\hat{\omega}_4, \Delta\hat{\omega}_5]^T$. It can be seen that the trajectories of $\Delta\hat{\delta}$ and $\Delta\hat{\omega}$ effectively track the trajectories of $\Delta\delta$ and $\Delta\omega$. Figures 4c-4f show the median χ^2 detector at work. Here a time window of 5 samples is considered and $\text{Med}\left(Q^l_k\right)$ is computed. It was found that the linearized model gives reliable state estimates as long as the process noise covariance is under $\mathcal{N}\left(0, 2 \times 10^{-2} \times I_{25}\right)$. A larger process noise covariance will trigger the median χ^2 detector. This is because the P_∞ value used in the χ^2 detector was constructed assuming a lower process noise. Regardless, the state estimate trajectories follow a similar trend as the actual states.

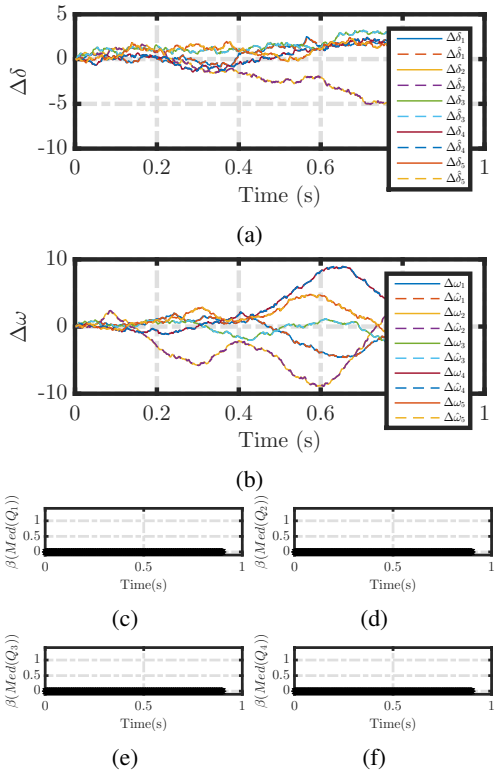

Fig. 4: Estimation and detection under healthy condition (a) Angles and their estimates (b) Frequencies and their estimates (c) Median χ^2 detector at DCC 1 (d) Median χ^2 detector at DCC 2 (e) Median χ^2 detector at DCC 3 (f) Median χ^2 detector at DCC 4

B. Attacked Case

The attack vector constructed as $a^2_k \sim \mathcal{N}\left(\mu^{la} = 0.1, R^{la} = 0.1 \times I_4\right)$ was injected to the measurements received by DCC 2 at $t = 0.15s$. Figures 5a shows the estimates $\Delta\hat{\delta}_3$ and $\Delta\hat{\delta}_4$ affected by the Gaussian attack and are much noisier compared to the remaining estimates. Similarly in Figure 5b $\Delta\hat{\omega}_3$ and $\Delta\hat{\omega}_4$ cannot track the true state value as in the healthy case. All the 4 estimates mentioned are estimates of measurements at DCC 2 that were attacked.

By checking the median χ^2 value in a time window of 5 samples against the χ^2 threshold at each DCC (see column 4 of TABLE III), Figures 5c-5f were plotted. In Figure 5d the Gaussian attack is shown to be detected around $t = 0.15s$. As mentioned earlier, once the attack is detected, techniques such as Bayesian learning can be utilized to mitigate this attack.

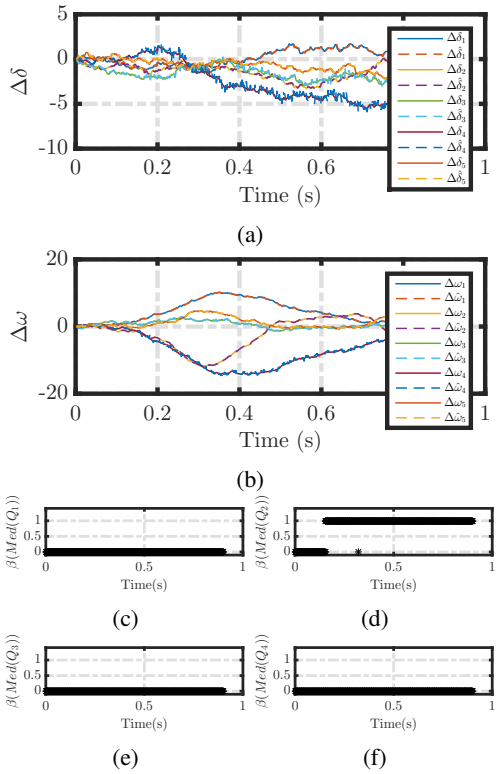

Fig. 5: Estimation and detection under cyber-attack (a) Angles and their estimates (b) Frequencies and their estimates (c) Median χ^2 detector at DCC 1 (d) Median χ^2 detector at DCC 2 (e) Median χ^2 detector at DCC 3 (f) Median χ^2 detector at DCC 4.

VI. Conclusion and Future Work

In this paper, the sub-optimal KCF framework previously utilized for WSNs was extended to power system network. A dynamic linearized model of the nonlinear power system was obtained around an operating point and was utilized by the KCF to obtain the estimates of unmeasurable and noise corrupted states. A median χ^2 detector was utilized at each DCC to detect bad measurements as well as to detect Gaussian attacks. The KCF gives a very good estimate of the states in the absence of attack; even when the process noise is large enough. Even in the onset of attacks, the estimates of the unattacked measurements are very reliable. Here the linearized power system model was considered by the KCF for predicting future state estimates. In the future, a nonlinear model of the power system could be considered for prediction by a distributed unscented KCF framework. Another approach could be to linearize the nonlinear model at every operating-point change and thus extend the results of the current work. An SSE can be used to find the current operating-point by utilizing PMU and SCADA (supervisory control and data acquisition) measurements. The prime focus of the current work was on estimation as it is derived from work on WSNs. A distributed control law needs to be designed next that utilizes the state estimates for feedback.

Acknowledgement

This work was supported by the National Science Foundation under GNT 1837472.

References

[1] A. Abur and A. G. Exposito, *Power system state estimation: theory and implementation*. CRC press, 2004.

[2] M. L. Crow, *Computational methods for electric power systems*. Crc Press, second ed., 2015.

[3] F. C. Schweppe and J. Wildes, "Power system static-state estimation, Part I: Exact model," *IEEE Transactions on Power Apparatus and Systems*, no. 1, pp. 120–125, 1970.

[4] J. Zhao, A. Gomez-Exposito, M. Netto, L. Mili, A. Abur, V. Terzija, I. Kamwa, B. C. Pal, A. K. Singh, J. Qi, *et al.*, "Power system dynamic state estimation: motivations, definitions, methodologies and future work," *IEEE Transactions on Power Systems*, 2019.

[5] D. G. Luenberger, "Observing the state of a linear system," *IEEE Transactions on Military Electronics*, vol. 8, no. 2, pp. 74–80, 1964.

[6] R. E. Kalman, "A new approach to linear filtering and prediction problems," 1960.

[7] M. M. Rana, R. Bo, and A. Abdelhadi, "Distributed grid state estimation under cyber attacks using optimal filter and Bayesian approach," *IEEE Systems Journal*, pp. 1–9, 2020.

[8] R. Olfati-Saber, "Distributed Kalman filtering for sensor networks," in *2007 46th IEEE Conference on Decision and Control*, pp. 5492–5498, IEEE, 2007.

[9] R. Olfati-Saber, "Kalman-consensus filter: Optimality, stability, and performance," in *Proceedings of the 48h IEEE Conference on Decision and Control (CDC) held jointly with 2009 28th Chinese Control Conference*, pp. 7036–7042, IEEE, 2009.

[10] J. Liu, A. Gusrialdi, S. Hirche, and A. Monti, "Joint controller-communication topology design for distributed wide-area damping control of power systems," *IFAC Proceedings Volumes*, vol. 44, no. 1, pp. 519–525, 2011.

[11] J. Machowski, Z. Lubosny, J. W. Bialek, and J. R. Bumby, *Power system dynamics: stability and control*. John Wiley & Sons, 2020.

[12] S. Zheng, T. Jiang, and J. S. Baras, "Robust state estimation under false data injection in distributed sensor networks," in *2010 IEEE Global Telecommunications Conference GLOBECOM 2010*, pp. 1–5, IEEE, 2010.

[13] Y. Mo and B. Sinopoli, "False data injection attacks in control systems," in *Preprints of the 1st workshop on Secure Control Systems*, pp. 1–6, 2010.

[14] Y. Mo and B. Sinopoli, "Secure control against replay attacks," in *2009 47th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, pp. 911–918, IEEE, 2009.