A Dynamic State Estimator Based Tolerance Control Method Against Cyberattack and Erroneous Measured Data for Power Systems

Hassan Haes Alhelou, *Senior Member, IEEE*, and Paul Cuffe, *Member, IEEE*

***Abstract*—Cyberattacks against measured variables and faulty metering devices are among the most important threats to modern systems that should be detected and isolated, and the control actions based on the measured variables should be appropriate in order to keep the power system security. This paper proposes a dynamic state estimation based cyberattack tolerant control method for modern power systems. The proposed method involves two new schemes, one is for dynamically detecting the cyberattack, and the other isolates the location of the attack. These schemes are based on dynamic observers designs that can eliminate the effects of unknown inputs. The paper also proposes a fault tolerant control technique using these observer-based detection and isolation schemes. The proposed method can accurately track dynamic states, detecting both cyberattack against measured variables and faulty measuring devices, and isolating the cyberattack and fault locations. The results verify its superiority in comparison with other techniques.**

Keywords*—*cyberattak, cyber tolerant control, data error, Power system Cybersecurity, wide-area measurement system.

Nomenclature

$i,\ j$	The ith and jth area index
t	The time index
$\alpha_{gi},\ \alpha_{ei}$	Conventional and EV participation gains
ΔACE_i	The deviation of the Area control error
$\Delta f,\ b$	Deviation of the frequency, and its bias
ΔP_{di}	Power disturbance or unknown input
$D,\ H$	Damping coefficient, and inertia constant
$R,\ N$	Governor speed droop, and areas number
$P_{tie,act_{ij}}$	Tie-line actual power flow
$P_{tie,sched_{ij}}$	Tie-line scheduled active power flow
$x,\ u,\ d,\ y$	State, input, disturbance and output vectors
$\hat{x},\ z$	Estimated state, and observer state vectors
$\hat{u}_i,\ K_{c,i}$	Estimated output signal and control matrix
e	State estimation error
$A,\ B,\ E,\ C$	State, input, disturbance, output matrices
$F,\ T,\ K,\ H$	Unknown input observer matrices
u^{Normal}	The normal control signal before attack
$u^{Attacked}$	The control signal under attack
$u^{Corrected}$	The corrected control signal
J_i	The quadratic performance index
$Q,\ R$	State and control cost weighting matrices
$K_{ev},\ T_{ev}$	EVs gain and time constant
$K_g,\ T_g$	Governor gain and time constant
$K_r,\ T_r$	Re-heater gain and time constant
$K_t,\ T_t$	Turbine gain and time constant
$K_{P,I,D}$	The PID controller's gains
${y_k}^A$	The received measured value under attack
${y_k}^E$	The estimated value instead of ${y_k}^A$
r	The residual, i.e. the detector output
Σ	The threshold value
ΔP_{tie}	The deviation of the tie-line power

H.H. Alhelou and P. Cuffe are with the School of Electrical and Electronic Engineering, University College Dublin, Dublin 4, Ireland, (emails: hassan.haesalhelou@ucd.ie; paul.cuffe@ucd.ie).

This publication has emanated from research supported in part by Science Foundation Ireland (SFI) under the SFI Strategic Partnership Programme Grant Number SFI/15/SPP/E3125 and additional funding provided by the UCD Energy Institute. The opinions, findings and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the Science Foundation Ireland.

I. Introduction

ENERGY security risks, environment concerns, and the problems related to fossil energy sources have led to major changes in the infrastructures, integration, and management of modern power systems. Due to global warming and greenhouse gases and their effects on the environment, many countries around the globe have adopted new energy policies that enable the widespread-deployment of green and renewable-based energy sources through their energy systems [1], [2]. Motivated by its importance in reducing climate changes, the US has recently rejoined Paris climate accord which should help with reducing carbon dioxide emissions from the power sector. Although the increase of renewable energy penetration in energy systems can help with solving a portion of environment concerns, it brings new challenges to power systems operation, control, and security. For instance, the active power imbalance between generation and demand sides may be increased, due the stochastic wind speed and variable solar radiation, leading to high frequency variations and prominent active power flow fluctuations through major transmission lines in the interconnected power systems. Recent developments in measurement techniques, e.g. phasor measurement units (PMUs) and communication technologies have encouraged the replacement of traditional supervisory control and data acquisition (SCADA) systems with new monitoring & control systems, i.e. wide-area monitoring systems (WAMSs). WAMSs bring new control and protection schemes for eliminating the negative impacts raised from the high share of renewable energy sources and power electronics in modern power systems [3]–[5]. On the other hand, serious new cybersecurity challenges have emerged due to changing the infrastructure and adopting new control techniques based on remotely measured variables that

used to generate a centralised control signals in WAMS. It is obvious that modern control systems are highly vulnerable to issues in measurement and communication systems, such as cyber-attacks, measurement errors and faulty measurement devices that need to be well-handled in order to enhance power system operation security and resiliency.

Maintaining the frequency and transferred power between different regains within permissible deviation ranges is of great importance for keeping the power systems operated safely and securely. It is usually done by implementing a control technique named automatic generation control (AGC) or load frequency control (LFC) loops [6]. This control scheme is a hierarchical technique built from three control levels, namely $primary$, $secondary$, and $tertiary$ control loops. The secondary controller is responsible for maintain both power flow through major transmission links and frequency with acceptable levels as predefined by the operators of the system, while the primary controller prevents major frequency declines in order to avoid unnecessary disconnection of a portion of the demand. The primary controller increases the generated active power using the governor-droop characteristics [6]. The aforementioned controllers construct control signals based on real-time measured variables, i.e. the frequency variation and power flow deviations through tie-lines. These variables are usually measured remotely and sent to the WAMS center using suitable communication channels where any issues such as physical/cyber-attack against these remote measurements or error and fault in the measuring devices will result in inaccurate control actions that might lead to instability and insecurity challenges [7]. Therefore, control schemes based on WAMSs should be fault and cyberattack tolerant in order to enhance both physical and cyber security in modern and future smart power systems.

Nowadays, there are prominent research activities for enhancing the security, including the cybersecurity, of power systems to avoid consequences related to cyberattack-based blackouts, e.g. December 2015 Ukraine power grid cyberattack [8]. In [9], the authors have suggested a way for detecting cyberattack using information gap decision theory for solving issues related to data integrity attacks in energy systems. In order to improve the cybersecurity for protection schemes in power systems, a cyber-attack detection method based on deep-learning has been proposed for transmission line protective relays in [10]. Authors in [11] have recently provided a framework for preventing outages due to simultaneous attacks on several market retailers where it can be considered as a remedial action technique in deregulated power systems. To avoid cyberattacks that might lead to multiple transmission line congestions, a three-level nonlinear model has been suggested for false-data injection cyberattack detection in [12]. Recently, a new Benfords law-based method for detecting cyber-attacks into estate estimator used in control rooms in SCADA systems has been proposed in [13]. In [14], authors have suggested a data-driven resilient AGC model to avoid the negative effects of false-data injection attacks to frequency control loops in power systems. Although the suggested model might be of interest for future power systems, it does not provide a way for mitigating the negative impacts by adopting fault-tolerant control techniques. A dynamic state estimator has been proposed in [15] for controlling frequency and power flow through tie-lines in smart grids that can handle some types of cyber-attacks. However, this technique requires prior knowledge of the attack type and does not suggest a solution to mitigate the negative effects of the attack on the system to avoid blackouts. Different types of fault and cyber-attacks detectors have been suggested in [16], [17] for industry systems but they need to be investigated for AGC and LFC loops in modern power networks with high share of renewable energy sources which indicates serious research gaps that should be solved in order to enhance the power system cybersecurity. On the other hand, there are research gaps that not well-investigated in modern power systems which is to answer technical and practical questions relating to how the power system operators can mitigate the negative impacts of cyberattacks and faulty measurement units on their control actions and what actions should be taken for enhancing the power system physical and cyber securities. This paper, for the first time, solves the above mentioned research gaps for improving the ability of controllers in modern power systems to be tolerant and reliance against both cyberattacks and faulty measurement units for improving the overall power system security by proposing error-tolerant frequency and power flow controllers.

This paper proposes a novel dynamic state estimation-based method for detecting and isolating of both cyberattacks and faulty measuring devices, and correcting the frequency control action in power systems in order to eliminate the negative impacts of such threats. The proposed method is built based on a deterministic estimation technique, i.e. observer with the ability to handle unknown inputs. The output power variations due to the integrated renewable energy sources, and the demand fluctuation due to the stochastic behaviours of the costumers are considered as unknown inputs in the WAMS center. Based on the introduced observer, two schemes are suggested, i.e. the first one for detecting the cyberattacks and faulty measuring units, and the second one is designed to be capable of isolating measured variables. Based on the aforementioned schemes, a novel cyberattack and faulty measuring devices tolerant control technique is also proposed in this paper. This technique dynamically replaces incorrectly measured variables with accurate values estimated using the suggested general observer. The results show the ability of the suggested method, schemes, and technique in accurately detecting and isolating of both cyberattack and faulty PMUs, and they can make necessary corrections to keep the system operated in a stable and secure mode.

The rest of this paper is organized as follows. Section II introduces the methodology including the cyberattack detection scheme in Subsection II-A, the isolation scheme in Subsection II-B, the proposed cyberattack tolerant control technique in Subsection II-C, and the proposed algorithms for designing and implementing the suggested method in Subsection II-D. The studied system is briefly shown in Section III, and the results are given in Section IV while Section VI concludes.

II. Methodology & Innovations

Modern power systems are different from conventional energy systems due to recent changes and upgrades in their information

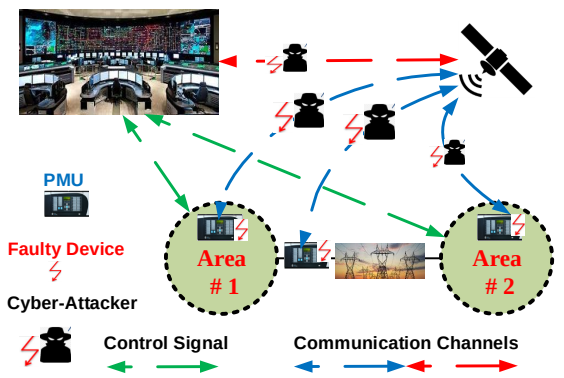


Fig. 1: General control structure of the power system under investigation and the vulnerable measurements to cyberattacks.

and communication technologies (ICTs). These upgrades in the ICT infrastructures have led to high deployment of PMUs through power systems based on which new control and protection schemes have been adopted. The control schemes have replaced the locally measured variables with other remote variables for improving the controllability and stability of modern power systems with high renewable energy shares. From this point, a new threat has become under light which is the physic/cyber-attack into power systems raised new important research topic, i.e. the cybersecurity.

Let us consider a power system topology shown in Fig.1 for determining the possible cyber threats into its wide-area monitoring and control (WAMC) infrastructure. For LFC, a system can be usually divided into several control areas, e.g. two areas in this figure, based on the dynamic coherency between its generators. In practice, a single generating unit is selected in each control area for controlling the frequency and the transferred power between this area and its neighbours. The WAMC center receives several measurements needed for constructing the control signal, in particular, the frequency variable in the control area and the transferred power with other areas. Now consider that these measurements are being received incorrectly to the WAMC center, this would lead to inaccurate power system control and operation actions which might put the system in danger of instability and insecurity operation. There are main two reasons for receiving such incorrect measurements, i.e. cyber-attacks and faulty measuring devices. In this paper, we propose a scheme for detecting such failures or cyber threats (see II-A) and a scheme for localising the measurements under cyberattack (see II-B), then based on the output of these schemes, a novel fault/cyber-tolerant control technique (see II-C) is proposed for avoiding instability issues in modern power systems due to the above named reasons. Likewise, we provide straightforward algorithms for designing the proposed method, (see II-D).

A. *Detection of cyberattack & faulty devices*

With the recent advancements in modelling and system identification techniques, there are prominent research activities for designing and implementing new control fault detection schemes based dynamic state estimation methods. Generally, these methods can be divided into deterministic and stochastic approaches, in which the observer techniques, as a prat of the deterministic approaches, have a better stability features. In what follows, we design unknown input observer for detecting the cyberattacks against measurements, and the faulty measuring devices as well.

For generalising the proposed detection method, let us take into account an n-order dynamical power system as follows

$$\begin{aligned} \dot{x}(t) &= Ax(t) + Bu(t) + Ed(t) \\ y(t) &= Cx(t) + Du(t). \end{aligned} \tag{1}$$

It is obvious that $y^{new}(t) = y(t) - Du(t) = Cx(t)$, therefore (1) can be rewritten as,

$$\begin{aligned} \dot{x}(t) &= Ax(t) + Bu(t) + Ed(t) \\ y(t) &= Cx(t), \end{aligned} \tag{2}$$

where A, B, C, and D are known matrices with appropriate sizes, $x \in \mathfrak{R}^{n\times 1}$ is the variable state vector, $u \in \mathfrak{R}^{r\times 1}$ is the input vector, $d \in \mathfrak{R}^{q\times 1}$ describes the unknown inputs, and $y \in \mathfrak{R}^{m\times 1}$ represents the measured outputs.

Let us define a new virtual dynamical system given in (3) designed to be able for online tracking of the internal dynamic states of the original power system described in (2).

$$\begin{aligned} \dot{z}(t) &= Fz(t) + TBu(t) + Ky(t) \\ \hat{x}(t) &= z(t) + Hy(t). \end{aligned} \tag{3}$$

The virtual dynamic system in (3) is called an observer and since it is able to handle unknown inputs, $d(t)$, therefore, it is an unknown input observer. The system (3) is an observer of the system (2) if and only if the state estimation error, $e(t)$, given in (4) approaches zero asymptotically.

$$e(t) = x(t) - \hat{x}(t), \tag{4}$$

F, T, K, H are unknown matrices that need to be well-designed for guaranteeing asymptotically stability of dynamic estimation error in (4). $z \in \mathfrak{R}^{n\times 1}$ is the state vector of the observer, and $\hat{x} \in \mathfrak{R}^{n\times 1}$ is the estimated states of the original system.

Taking the derivative of the estimation error in (4), one has

$$\begin{aligned} \dot{e}(t) = (A - HCA - K_1C)e(t) + [F - (A - HCA - \\ K_1C)]z(t) + [K_2 - (A - HCA - K_1C)]y(t) \\ +[T - (I - HC)]Bu(t) + (HC - I)Ed(t). \end{aligned} \tag{5}$$

It is an evidence from (5) that the dynamics of the state estimation error $\dot{e}(t) = Fe(t)$ will be stable if and only if the matrix F is a stable one and if the conditions given in (6) are stratified.

$$\begin{aligned} (HC - I)E &= 0 \\ T &= I - HC \\ F &= A_2 - K_1C \\ K_2 &= FH \\ K &= K_1 + K_2 \\ A_2 &= A - HCA, \end{aligned} \tag{6}$$

$$\dot{e}(t) = F\,e(t), \tag{7}$$

$$A_1 = A - E\left[(CE)^T CE\right]^{-1}(CE)^T CA. \tag{8}$$

The main issue is to guarantee a suitable design of the observer in (3) by satisfying the conditions in (6) in such way that F becomes a Hurwitz matrix. If K_1 is well-selected, then F becomes stable if and only if the following two sufficiency conditions are met: i) $rank(CE) = rank(E)$, and ii) (C, A_1) is detectable. It is obvious that if these conditions are met and K_1 is well-chosen (K_1 can be chosen for a specific dynamic characteristics based on the pole-placement technique such that F becomes stable), the other conditions in (6) determine the rest of matrices required for building the virtual dynamic system, i.e. the unknown input observer.

There are two design issues related to the sufficiency conditions that need to be considered. The main technical issue relates to the case arising if the pair (C, A_1) is not observable. In such a case, an observable canonical decomposition can be utilised for removing the unobservable modes by constructing a transformation matrix P as follows

$$PA_1P^{-1} = \begin{bmatrix} A_{11} & 0 \\ A_{12} & A_{22} \end{bmatrix} \quad where\ A_{11} \in \Re^{n_1 \times n_1}, \tag{9}$$

$$CP^{-1} = [C^*\ 0] \quad where\ \ C^* \in \Re^{m \times n_1}. \tag{10}$$

In (9) and (10), the system with a rank of n is decomposed into two systems, one of them with a n_1 rank in which the pair (C^*, A_{11}) is completely detectable, where the undetectable modes are combined in the eigenvalues of A_{22}.

The second technical issue is related to the other sufficiency condition, i.e. $rank\,(CE) = rank\,(E)$. If this condition is not satisfied, we propose two solutions: *i*) installing additional measurement devices in order to satisfy the condition, or *ii*) building a virtual output by an interpolation of the existing real outputs measured by the installed PMUs. The mathematical proof of the suggested second solution is available in [15].

It is worth mentioning that the dynamic order of the suggested observer is similar to the original system under investigation, i.e. n. This is clear from (2) and (3) where both systems have dynamic order equal to n. A such observer is called as a general observer. However, it is possible to design a reduced order observer in which few dynamic states can be ignored where a such reduced order dynamic observer called a functional observer which is suitable for control applications more than detection and isolation techniques. However, there are limitations on designing functional observers related to the satisfaction of the rank condition, i.e. $rank(CE) = rank(E)$.

Once the observer is well-designed, the dynamic states of the original system, i.e. the power system under investigation, can be tracked in real-time which enables its use for online detection and isolation of faulty devices and cyberattacks against measured variables. The detection can be realised using newly defined residual outputs, $r(t)$, calculated based on a comparison between the measured variables, i.e. the outputs $y(t)$, and estimated outputs, i.e. $\hat{y}(t)$, as follows

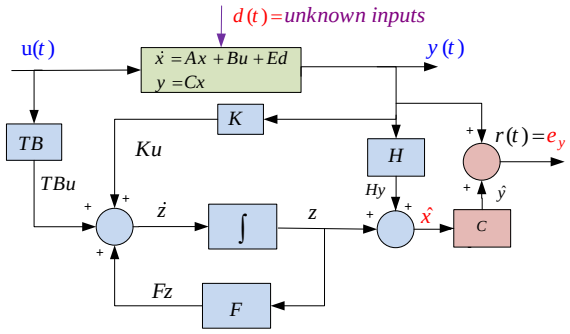


Fig. 2: Cyber-attack detection blockdiagram

$$r(t) = e_y = y(t) - \hat{y}(t) = (I - CH)y(t) - Cz(t), \tag{11}$$

where

$$\hat{y}(t) = C\hat{x} = Cz(t) + CHy(t). \tag{12}$$

The defined residual in (11) is able to accurately detect cyberattacks against measured variables and faulty measuring devices based on the logic given in (13)

$$\exists : \|r\| > \Sigma \ \Rightarrow Abnormal, \ | \ \|r\| \leq \Sigma \ \Rightarrow Normal. \tag{13}$$

The dynamic blockdiagram, that presents the configuration of the suggested cyberattack detector, is depicted in Fig 2.

It is clear from (11) that any difference between the estimated outputs and measured outputs will increase the residual indicating the occurrence of cyber-attacks. Thus, the proposed cyberattack detection method is sensitive to both single and simultaneous attacks. This is one of the main features of the proposed cyberattack detection method.

B. Cyberattack Isolation and Localisation

The aforementioned virtual dynamic system, in Section II-A, has the ability to detect any issues inside the measurement and communication system used for constructing the control signal, which means it is able to answer an important question in the WAMC center, i.e. is the controlling system experiencing cyber-attack/faulty measuring issues or not?. However, it is unable to isolate the faulty measuring device or the measurements under cyberattacks. Therefore, a new scheme based on the previously introduced observer is developed to be able to locate and isolate the problem, i.e. cyberattack or faulty measuring devices. If the power system operator in WAMC center could isolate the attacks, then it can make the controller more tolerant to such technical threats issues in modern power systems.

If the control system requires m measured variables, i.e. the number of elements in the output vector, then the operator needs to design m sub-virtual systems, i.e. sub-observers, based on which the operator becomes able to isolate the location of the faulty measuring device and the measured variables under attack.

This technique is called an observer bank and each sub-observer in the bank is designed to be sensitive to all cyberattacks against other measuring devices except its measuring device, i.e. ith sub-observer is sensitive to cyberattack against measuring devices 1, 2, ..., $i-1$, $i+1$, ..., m. To this end, operator needs to apply a signal grouping method for constructing new groups of the outputs by removing the ith element from y for building the ith sub-observer.

Let us consider the system in (2) assuming that the power system control loop has an issue (faulty measuring device or cyberattacks, $f_s(t)$), therefore, the system can be expressed dynamically as follows

$$\begin{aligned} \dot{x}(t) &= Ax(t) + Bu(t) + Ed(t) \\ y^i(t) &= C^i x(t) + f_s^i(t) \\ y^j(t) &= C^j x(t) + f_s^j(t) \\ i + j &= m. \end{aligned} \tag{14}$$

It is worth mentioning that $y^i \in \Re^{1\times m}$ has one element only, i.e. the ith measured variable, therefore the size of its output matrix is $C^i \in \Re^{1\times m}$. By removing $y^i \in \Re^{1\times m}$ from y, then the operator has a new output vector, $y^j \in \Re^{(n-1)\times m}$, with an output matrix with a size of $C^j \in \Re^{(n-1)\times m}$, based on which the new bank of observers would be constructed and designed.

The aforementioned dynamic systems driven from original power system by removing one output each time is used for designing the sub-observers, as follows

$$\begin{aligned} \dot{z}^j(t) &= F^j z^j(t) + T^j Bu(t) + K^j y^j(t) \\ \hat{x}^j(t) &= z^j(t) + H^j y^j(t); \quad j = 1, 2, ..., m \\ r^j(t) &= y^j(t) - C^j \hat{x}^j(t). \end{aligned} \tag{15}$$

The matrices of the sub-observers F^j, T^j, H^j, and K^j are unknown matrices that should be designed to guarantee the stability of their observers, i.e. F^j should be a Hurwitz matrix. Similar to the design of the general observer in the previous subsection, the conditions given in (16) should be met in order to make the design of the observers feasible.

$$\begin{aligned} H^j C^j E - E &= 0 \\ T^j &= I - H^j C^j \\ F^j &= T^j A - K_1^j C^j \\ K_2^j &= F^j H^j \\ K^j &= K_1^j + K_2^j. \end{aligned} \tag{16}$$

Likewise, the disturbance matrix and output matrix should have the sufficiency conditions (i.e. $rank\,(C^j E) = rank\,(E)$, and the pair (C^j, A_1) is detectable) in order to satisfy the conditions in (16). If these two sufficiency conditions are not guaranteed, one has to apply the observable canonical decomposition technique for removing the unobservant modes as described in (9) and can build new virtual outputs for correcting the rank sufficiency condition.

Once the bank of observers is well-designed, the power system operator can monitor the situation of each measuring device and its communication channel with the control center.

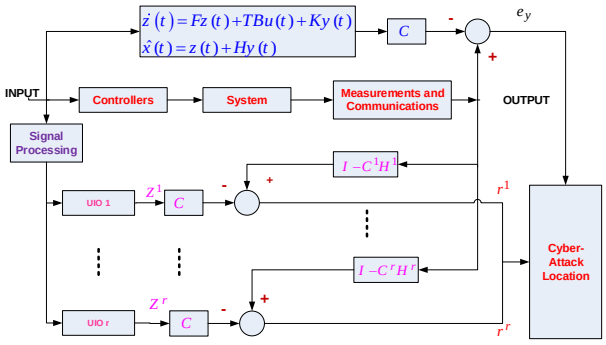


Fig. 3: Block diagram of the the cyber-attack location scheme

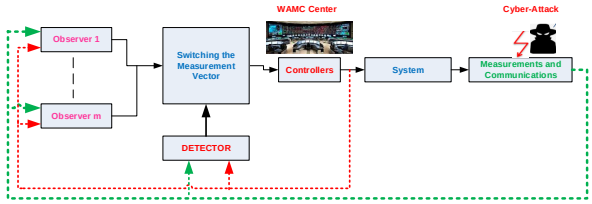


Fig. 4: The proposed cyberattack and fault tolerant control scheme for power systems

By comparing the residuals norms $\|.\|$ with a predefined isolation threshold Σ^j, if the kth norm is lower than its threshold and all other residual norms are higher than their thresholds, then the kth measuring device is under cyberattack, based on the following isolation logic.

$$\begin{aligned} \left\|r^k\right\| &< \Sigma^k \\ \left\|r^j\right\| &\geq \Sigma^j; \quad j = 1, ..., k-1, k+1, ..., m. \end{aligned} \tag{17}$$

The proposed isolation and location scheme of the faulty measuring devices and cyberattacks is visually depicted in Fig. 3. It is clear from this figure that a number of sub-observers are required to locate the cyberattack locations. It is also obvious that the implementation of this virtual dynamic system in WAMC center is feasible since all the required data and measured signals are available or can be estimated in the modern control centers of power systems.

C. CyberAttack Tolerant Control

In this section, a novel technique is proposed for mitigating the negative impacts of cyberattacks and faulty measuring devices on power system operation by eliminating their effects in controllers in control rooms instantly after detecting them. The proposed novel technique uses the suggested cyberattack detector (see section II-A) and cyberattack isolation scheme (see section II-B).

Fig. 4 depicts the main block-diagram of the proposed cyber-attack and faulty measuring device tolerant control technique. Since the operator has the measured variables in the control

center either received accurately or inaccurately due cyberattack, it is feasible to implement the proposed cyberattack tolerant control technique shown in Fig. 4. In addition to the measured variables, the control signals sent to the different actuators are also required which are constructed and available in the same wide-area monitoring and control center. The general concept of the observer is used first for both detecting the cyberattack and alarming the operator of the system. Likewise, the isolation method based on the suggested bank of observers would be able to isolate and locate the faulty measuring devices or measurement variable under cyberattacks in real-time as shown in Subsection II-B. It is proposed to automatically and instantly replace the measured variables, elements in y vector, under attack or faulty measuring issues with the estimated variables using the general observer concept. The proposed cyberattack isolator identifies the kth row (i.e. kth measured variable under cyberattack, y_k^A) of output vector, i.e. y, and this row is automatically replaced by the accurately observed variable, y_k^E, by the general observer concept.

Let us consider that m measurement variables are required for constructing the control signal u, therefore, if all the variables are measured correctly without fault or cyberattack issues, we have

$$u^{Normal} = ky = [k_1,\ k_2,\ ...,\ k_m][y_1,\ y_2,\ ...,\ y_k, ...,\ y_m]^T \quad (18)$$

In the above model of general controller, if any of variables are being inaccurately measured or affected due to cyberattack issues, the operation of the system would be affected and consequently the stability and security of the system will be in danger. The worse scenario is that there are no detection and isolation schemes (this is the actual situation in WAMC in the world), where in such scenario, the control signal under attack, $u^{Attacked}$, will force the actuators to react inappropriately leading to stability issues.

$$u^{Attacked} = ky = [k_1,\ k_2,\ ...,\ k_m][y_1,\ y_2,\ ...,\ y_k^A, ...,\ y_m]^T \quad (19)$$

The suggested detection and isolation schemes in this paper help the operator to identify the measured element under attack which enables the operator to automatically replace the inaccurately measured variables with its estimation value, i.e. y_k^E, according to FTC technique shown in Fig. 4, as follows

$$u^{Corrected} = ky = [k_1,\ k_2,\ ...,\ k_m][y_1,\ y_2,\ ...,\ y_k^E, ...,\ y_m]^T \quad (20)$$

The main advantage of the proposed cyber-tolerant control scheme shown in Fig. 4 is that it works with any control type or structure which makes it as a generalised cyber-tolerant control concept. If a state feedback control approach, e.g. optimal control theory, is adopted, then the number of measured elements becomes equal to the number of the dynamic states. Mathematically, it means that equation (18) becomes $u^{Normal} = ky = kx$, and the control gain, k, is usually tuned using the Riccati equation (please see [18], [19]). On the other hand, if a traditional PID controller is used to control the system, then the output y will contain only the selected controllable measurements, and the control gain k will have the proportional, integral, and derivative gains and operations, i.e. $k = \left[k_P,\ k_I \int dt,\ k_D \frac{d}{dt}\right]$.

The aforementioned procedure shows clearly the importance of the proposed cyberattack tolerant control method especially for modern power systems with highly renewable energy sources where their stability and security under different types of threats. In the next section, the required algorithm for designing the suggested detection, isolation and tolerant control schemes are introduced. Likewise, the necessary procedure for implementing the proposed method and schemes in wide-area monitoring and control center is provided and its feasibility is illustrated.

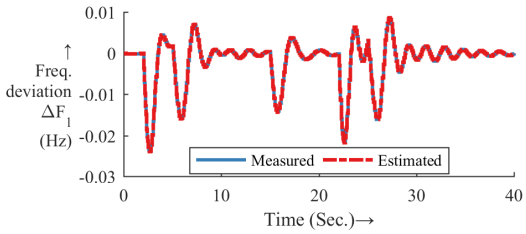
D. Design and Implementation Feasibility

This section introduces the algorithm used for designing the suggested cyberattack detector and isolator. Likewise, the main steps required for implementing the proposed dynamic estimator-based CTC method are briefly highlighted. Algorithm I shows that the first step for designing observer-based cyberattack detector and isolator is the collection of the required data for building the state space model of the system. After checking the observability and rank-condition, the virtual dynamic systems of the detector and isolator can be obtained based on steps IV-VII in which the required matrices can be determined. If these steps are accurately followed, the power system operator would achieve the best design of the general observer and the observers bank. It is worth mentioning that the selection of K_1 plays a vital role in the dynamic performance of observers and a compromise between the accuracy of the estimation and the dynamic speed of the observer can be done in this step. It is notably that the design of these observers are done offline, therefore these steps would not affect real-time implementation process of the suggested schemes in this paper.

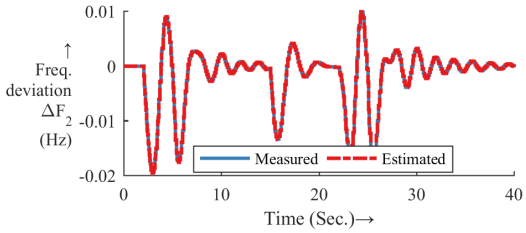
TABLE I: Proposed algorithm to design cyberattack detector, isolator and controller

Step No. #	Algorithm Process
STEP I	**Build** state space (SS) model for the system identifying the output vector, y, and unknown inputs according to (2)
STEP II	**Check** the rank condition, i.e. $rank(CE) = rank(E)$, if it is not true, then construct a new virtual output
STEP III	**Check** if (C, A_1) is observable, otherwise use the observable canonical decomposition based on (9)-(10)
STEP IV	**Calculate** H from (6a), T based on (6b), then $A1$ from H and T or from (8)
STEP V	**Assign** suitable K_1 using pole placement technique considering the required dynamic response of the observer
STEP VI	**Obtaining** F, K_2, and K based on (6c), (6d), and (6e), respectively
STEP VII	**Design Isolator** using the previous step after applying the signal processing technique based on (14)-(15), and **Find** isolator matrices according to previous steps, i.e. IV-VI
STEP VIII	The End

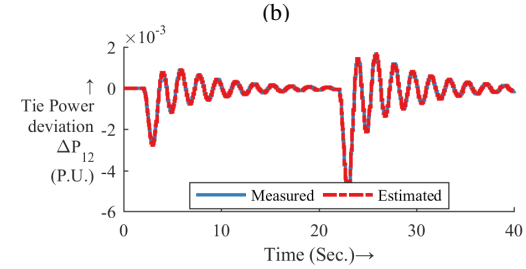
Table II introduces the implementation steps of the proposed method. The WAMS center receives the required measurements from PMUs in real-time, and records the control signals sent to actuators from the same center. These measurements, i.e. the outputs of the power system, and the control signals, i.e. the inputs to the power system, are the main inputs to the dynamic virtual system built based on algorithm I. Based on the output of the dynamic detector, the operator can



(a)



(b)



(c)

Fig. 5: Power system dynamics and the estimation of outputs: a) ΔF_1, b) ΔF_2, c) ΔP_{12}

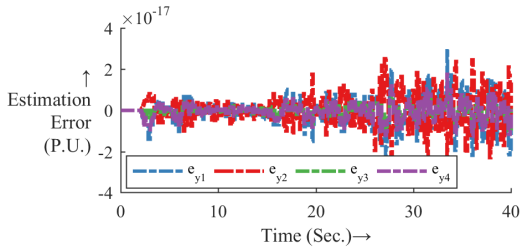
detect the faulty measuring devices and cyberattack against measurements. Likewise, the operator would be notified in real-time of the location of the attack, based on which the operator can switch the configuration of the control system by replacing the measured attacked values with estimated values in order to achieve robust tolerant control against cyberattacks and faulty measuring devices.

III. Test Platform

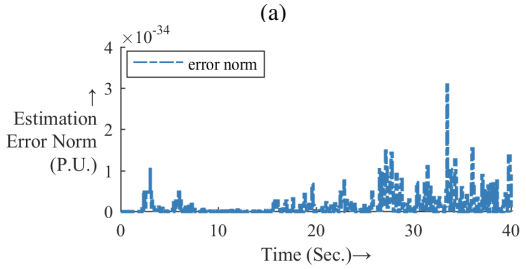
The power system under investigation is two power areas linked together using a major AC transmission line as shown in Fig. 1. The dynamic order of the system is 11, i.e. 5^{th} order dynamic model for presenting the dynamics in each area, and 1^{st} order dynamic model for representative of the tie-line based on its synchronising coefficient. For controlling the frequency and tie-line power flow as a part of AGC/LFC rules, three measured variables are required, i.e. $y = [\Delta F_1, \Delta F_2, \Delta P_{12}]^T$. The dynamic model of the system is based on system frequency response model of a two-area power system, where the mathematical representation of the dynamics in each area and its data can be found in [20], [21]. The necessary data of the system under investigation is given in Appendix.

TABLE II: Proposed algorithm to implement the proposed method

Step No. #	Implementation Process
STEP I	**Build** virtual dynamic systems of both the general observer detector, and the bank of observer, i.e. the isolator
STEP II	**Receive** measurements in real-time using WAMS infrastructure
STEP III	**Take** the input signal, the constructed control signals in real-time
STEP IV	**Use** the input and output of the original power system as input to the virtual dynamic systems built in the monitoring and control room
STEP V	**Obtain** the norm of the error and residual (11) and (13); & **Set** an alarm based on the detector output
STEP VI	**Online calculate** the output of the isolation scheme for identifying which measurement under attack according to (17)
STEP VII	**Activate** the proposed CTC technique by switching from measured inputs to the controller to estimated ones based on (18-20).
STEP VIII	The End



(a)



(b)

Fig. 6: The dynamic state estimation accuracy: a) estimation error, b) the norm of the estimation error.

IV. Results and Discussions

For designing the suggested general observer based on algorithm I, the rank condition is met, i.e. $Rank(CE) = Rank(E) = 2$, therefore, a such dynamic estimator can be well-designed for detecting the cyberattacks against measurements used in constructing the AGC control signal. On the other hand, this condition becomes unsatisfied if the bank of observers is designed based on the approach introduced in Subsection II-B, therefore, this technical issue is solved using the technique proposed in this paper by adding a virtual measured variable (for example: $y_4 = \Delta F_1 + \Delta F_2$). In the next step, the designing and implementation algorithms proposed, in this paper, are adopted to obtain the required matrices for the general observer and its bank of observers. The intermediate results are also omitted, and the main results including the dynamic performance evaluation are introduced in what follows.

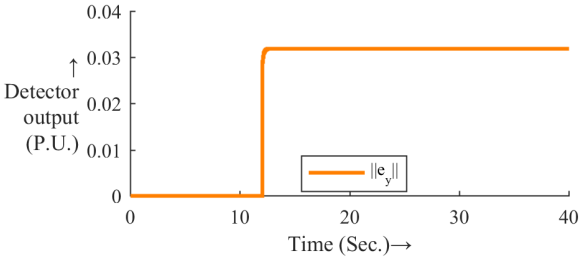


Fig. 7: The output of the proposed cyberattack detector.

In order to illustrate the superiority of the proposed dynamic estimator based on the general observer in tracking and observing the internal dynamic states and measured variables in real-time, several scenarios are considered taking into account different operation conditions. For instance, the most sever operation case is presented in which both demand fluctuation, i.e. step disturbance, and high power variation from renewable energy sources, i.e. step changes in solar powers and random variation from wind power plants, are assumed. In order to concisely presenting the results, only the ability of the proposed observer in tracking the output states, the measured variables, are shown in Fig. 5. It is clear from this figure that the proposed general observer can track both the internal dynamic states and the measured variables in real-time with no estimation delay which enables the implementation feasibility of the proposed method. To better understand the superiority of the proposed method, the estimation error and its norm are depicted in Fig. 6. It is evidence from this figure that the proposed method has high accuracy where the estimation error of the order 10^{-17} and its norm order is 10^{-34}, indicating that the estimation error is almost zero.

To evaluate the suggested detector of cyberattacks and faulty measuring devices, several scenarios considering different attack and fault types are taken into account. Fig. 7 shows the residual norm which is the main output of the proposed cyberattack detector which indicates that the system is subjected to a cyberattack against the measurement at $t = 12$. Although the proposed detector could distinguish the attack and detect it in real-time manner, the detector can not inform the power system operator which measured variable is under attack as mentioned in Section II. However, this issue is solved by the proposed cyberattack isolation scheme introduced in II-B.

As aforementioned, due to the rank condition, a new virtual measurement (the 4th measurement) is added to the output vector. This leads to a new sub-observer in the bank of the observers used for locating the cyberattack and faulty measuring devices. Fig. 8 shows the residuals as output of the 4 *subobservers* inside the designed observer bank for the power system under investigation. It is worth mentioning that each sub-observer is designed to be sensitive to attacks against other measurements except its own measurement variable, which means the ith sub-observer is insensitive to the attack against its own measured variable or its own faulty measuring devices (Please see Subsection II-B). Considering this fact, the results depicted in Fig. 8 indicate that the 1st measurement is under

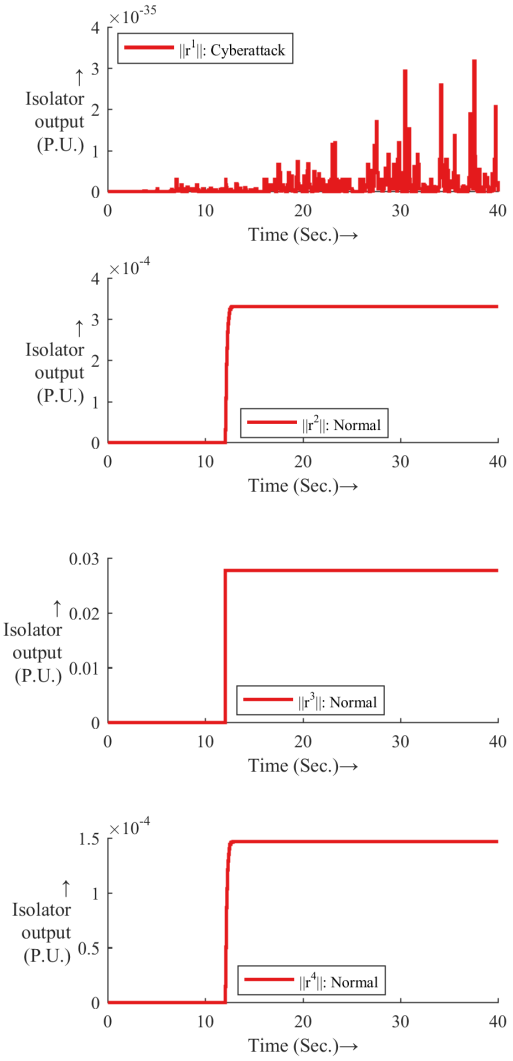


Fig. 8: The output of the suggested observer bank, i.e. the residual outputs of the proposed cyberattack isolating scheme.

cyberattack. The proposed cyberattack isolation scheme is linked with a logic system that can be adopted in WAMC center for switching the controller to be tolerant against faulty measuring devices and cyberattacks. The results of the proposed logic isolation system are depicted in Fig. 9, on which, the situation relates to first measurement is changed from 0 to 1 at time $t = 12$ indicating that this measurement under attack and an action should be taken in order to keep the power system operated in safe and stable modes. The output of this logic system is the main input to the proposed cyberattack tolerant control technique proposed in this paper, where based on which, the 1st measurement variable is instantly replaced by its estimated value to avoid negative impacts of cyberattack issues on power system operation.

To assess the proposed cyberattack-tolerant control method, different types of attacks are considered. For instance, this

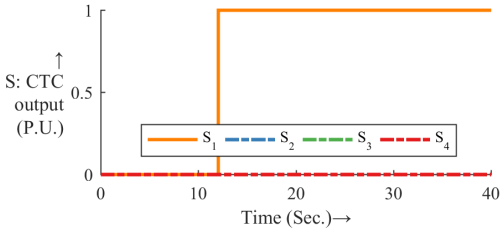


Fig. 9: Identifying the affected measurement variable based on the isolating logic system; S:CTC is the switching signal for activating CTC method.

paper introduces the simulation results related to three different attack scenarios, namely: fixed additive step attack, ramp value added as an attack to the measured values, and random values injected into the measured variable. Fig. 10 shows the dynamic performance of the power system under attack considering the proposed method compared to other control schemes with not tolerant controllers. It is clear that the proposed method can keep the frequency with its permissible level and diminish its oscillations as shown in Fig. 10a. In the other hand, if the WAMC center is not supplied with tolerant control scheme, the frequency deviates beyond its acceptable level and high oscillations would appear which might affect the power system stability. In some case, the frequency will drop dramatically putting the system in the danger of blackout if the system does not have a cyberattack tolerant control. This clearly shows the importance of the proposed method in this paper for modern power systems. This paper also considers the impacts of cyberattacks on power flows between power regions. Fig. 10b shows that not considering the proposed control method leads to high fluctuations in power flows through tie-lines resulting in instability issues, while the proposed method can detect, isolate and correct the negative impact of cyberattack against power systems. The results prove that the introduced method in this paper as CTC, for the first time, is of high importance to modern power systems where their control systems are being built based on vulnerable measurement and communication infrastructures.

V. An overview of main scope findings and advantages

This paper focuses on detection and isolation of both cyber-attacks and faulty measurement devices in interconnected power systems. It focuses on the measurement side and how cyberattacks can affect the power system operation and control performance. The suggested method has the ability to be expanded for applications in actuator and control sides including relaying and breakers in subsections which can be considered as a future. It is clear that for adapting the proposed methods for substation breakers and controllers, one needs to consider the control input instead of measured output in the detector and isolator design in Sections $II-A$ & $II-B$.

The main findings obtained from this research output include:

- The ability to accurately tracking the internal dynamic states in complex models of power systems. The proposed observing model is designed mathematically to be robust against model uncertainties and stable against disturbances.
- The adopted observer for tracking the internal dynamic states is able to handle unknown inputs which is an important feature for real-world power systems.
- The ability to detect and isolate both cyberattacks and faulty measuring devices.
- The proposed detection and isolation method has the capability to detect simultaneous attacks.
- The high speed in tracking dynamic states enables the real-time implementation of the proposed method especially for control tolerance applications.
- Brilliant performance in the proposed observer-based cyberattack tolerant control method which mitigates the negative effects of cyberattacks on power system operation and security.

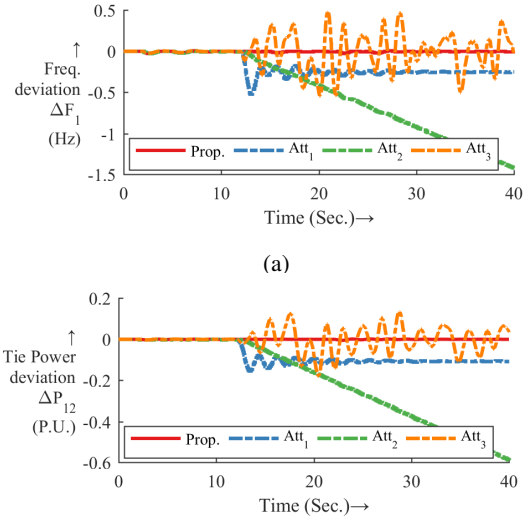


Fig. 10: The results of the proposed CTC and their compartive study: a) the frequency, and b) the power flow through tie-line.

The proposed observer-based cyberattack detection and isolation presented in this paper is a general unknown input observer-based cyber and fault detection and isolation method which can be adopted and further developed for other applications in power systems. In the general framework proposed, the control part can be replaced by other methods and the detection scheme can be redesigned for actuator and breakers in substations in modern power systems.

VI. Conclusions

This paper proposes a novel method to detect and isolate cyberattack against measurements and faulty measuring devices in real-time. The method and its suggested schemes are built based on observers that can handle unknown inputs to power systems which help with reducing the dynamic order of the power system under consideration. The general observer can detect the cyberattacks while the dynamic isolator can find the

measurement under attack. Based on the suggested detector and isolator, a novel cyberattack-tolerant control technique is also proposed which can remove the negative impacts of cyberattack on the dynamic performance and operation of power system. These advantages can significantly help the operators in wide-area measurement system center especially for modern power systems which considered to be highly vulnerable to cyberattack and faulty measurement devices. As future work, this method can be extended for microgrids and for other control loops in power systems. The proposed method and techniques in this paper have potential implementations and developments for other control loops in power systems and microgrids including the control of voltage and the design of system stabilisers. Liewise, the proposed cyberattack detection and isolation method can be adopted for controller and actuator sides in power systems which are considered as future works.

Appendix

The parameters of the model can be found in [21]. It is worth mentioning that the two-order swing model is used for modelling synchronous generating units, while suitable models are selected for governor-turbine systems.

The important data for re-doing the simulation are as follows: F= 50 Hz, β=0.425 p.u MW/HZ, H= 5 Seconds, T_t= 0.3 Seconds, T_g= 0.08 Seconds, T_{tie}= 0.545 Seconds, D= 0.0083 p.u MW/Hz, R= 2.4 Hz/p.u MW, K_{ev}= 1.0 p.u, T_{ev}= 1.0 Seconds, K_{pv}= 1.0 p.u., T_{pv}=1.8 Seconds, K_{wtg}= 1.0 p.u, T_{wtg}= 1.5 Seconds, α_{ev}= 0.3 p.u, α_g= 0.7 p.u.

Acknowledgements

The authors would like to express their gratitude to the reviewers for the useful suggestion and comments helped improving the paper.

References

[1] P. Zhuang, T. Zamir, and H. Liang, "Blockchain for cybersecurity in smart grid: A comprehensive survey," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 1, pp. 3–19, 2020.

[2] H. Fayazi, B. Fani, M. Moazzami, and G. Shahgholian, "An offline three-level protection coordination scheme for distribution systems considering transient stability of synchronous distributed generation," *International Journal of Electrical Power & Energy Systems*, vol. 131, p. 107 069, 2021.

[3] Y. Ding, B. Wang, Y. Wang, K. Zhang, and H. Wang, "Secure metering data aggregation with batch verification in industrial smart grid," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 10, pp. 6607–6616, 2020.

[4] H. Fayazi, M. Moazzami, B. Fani, and G. Shahgholian, "A first swing stability improvement approach in microgrids with synchronous distributed generators," *International Transactions on Electrical Energy Systems*, vol. 31, no. 4, e12816, 2021.

[5] S. Ahmadi, I. Sadeghkhani, G. Shahgholian, B. Fani, and J. M. Guerrero, "Protection of lvdc microgrids in grid-connected and islanded modes using bifurcation theory," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, 2019.

[6] H. H. Alhelou, M.-E. Hamedani-Golshan, R. Zamani, E. Heydarian-Forushani, and P. Siano, "Challenges and opportunities of load frequency control in conventional, modern and future smart power systems: A comprehensive review," *Energies*, vol. 11, no. 10, p. 2497, 2018.

[7] H. Wang, X. Wen, Y. Xu, B. Zhou, J.-C. Peng, and W. Liu, "Operating state reconstruction in cyber physical smart grid for automatic attack filtering," *IEEE Transactions on Industrial Informatics*, 2020.

[8] H. Haes Alhelou, M. E. Hamedani-Golshan, T. C. Njenda, and P. Siano, "A survey on power system blackout and cascading events: Research motivations and challenges," *Energies*, vol. 12, no. 4, p. 682, 2019.

[9] M. Davari, H. Nafisi, M.-A. Nasr, and F. Blaabjerg, "A novel igdt-based method to find the most susceptible points of cyberattack impacting operating costs of vsc-based microgrids," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, 2020.

[10] Y. M. Khaw, A. A. Jahromi, M. F. Arani, S. Sanner, D. Kundur, and M. Kassouf, "A deep learning-based cyberattack detection system for transmission protective relays," *IEEE Transactions on Smart Grid*, 2020.

[11] A. Asrari, M. Ansari, J. Khazaei, and V. Cecchi, "Decentralized outages prevention: A remedial action scheme for cyberattacks targeting market retailers in smart distribution systems," *IEEE Transactions on Industrial Informatics*, 2021.

[12] J. Khazaei, "Stealthy cyberattacks on loads and distributed generation aimed at multi-transmission line congestions in smart grids," *IEEE Transactions on Smart Grid*, 2020.

[13] F. Milano and A. Gómez-Expósito, "Detection of cyber-attacks of power systems through benford's law," *IEEE Transactions on Smart Grid*, 2020.

[14] C. Chen, Y. Chen, J. Zhao, K. Zhang, M. Ni, and B. Ren, "Data-driven resilient automatic generation control against false data injection attacks," *IEEE Transactions on Industrial Informatics*, 2021.

[15] H. H. Alhelou, M. E. H. Golshan, and N. D. Hatziargyriou, "A decentralized functional observer based optimal lfc considering unknown inputs, uncertainties, and cyber-attacks," *IEEE Transactions on Power Systems*, vol. 34, no. 6, pp. 4408–4417, 2019.

[16] K.-D. Lu, G.-Q. Zeng, X. Luo, J. Weng, W. Luo, and Y. Wu, "Evolutionary deep belief network for cyber-attack detection in industrial automation and control system," *IEEE Transactions on Industrial Informatics*, 2021.

[17] A. Kavousi-Fard, W. Su, and T. Jin, "A machine-learning-based cyber attack detection model for wireless sensor networks in microgrids," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 1, pp. 650–658, 2020.

[18] D. E. Kirk, *Optimal control theory: an introduction*. Courier Corporation, 2004.

[19] A. U. Rehman, H. H. Choi, and J.-W. Jung, "An optimal direct torque control strategy for surface-mounted permanent magnet synchronous motor drives," *IEEE Transactions on Industrial Informatics*, 2021.

[20] T. N. Pham, H. Trinh, *et al.*, "Load frequency control of power systems with electric vehicles and diverse transmission links using distributed functional observers," *IEEE Transactions on Smart Grid*, vol. 7, no. 1, pp. 238–252, 2015.

[21] P. Cuffe and H. H. Alhelou, "Figures, data and scripts from "A Dynamic State Estimator Based Tolerance Control Method Against Cyberattack and Erroneous Measured Data for Power Systems"," Jun. 2021. DOI: 10.6084/m9.figshare.14866077.v1. [Online]. Available: https://figshare.com/articles/dataset/Figures_data_and_scripts_from_A_Dynamic_State_Estimator_Based_Tolerance_Control_Method_Against_Cyberattack_and_Erroneous_Measured_Data_for_Power_Systems_/14866077.