Vulnerability Assessment of 6G-Enabled Smart Grid Cyber–Physical Systems

Muhammad Tariq, *Senior Member, IEEE*, Mansoor Ali, *Member, IEEE*, Faisal Naeem, *Member, IEEE*, and H. Vincent Poor, *Life Fellow, IEEE*

***Abstract*—Next-generation wireless communication and networking technologies, such as sixth-generation (6G) networks and software-defined Internet of Things (SDIoT), make cyber–physical systems (CPSs) more vulnerable to cyberattacks. In such massively connected CPSs, an intruder can trigger a cyberattack in the form of false data injection, which can lead to system instability. To address this issue, we propose a graphics-processing-unit-enabled adaptive robust state estimator. It comprises a deep learning algorithm, long short-term memory, and a nonlinear extended Kalman filter, and is called LSTMKF. Through an SDIoT controller, it provides an online parametric state estimate. The reliability is improved by performing two levels of online parametric state estimation for secure communication and load management. The CPS under study is a 6G and SDIoT-enabled smart grid, which is tested on IEEE 14, 30, and 118 bus systems. Compared to existing techniques, the proposed algorithm is able to estimate the state variables of the system even during or after a cyberattack, with lower time complexity and high accuracy.**

***Index Terms*—Cyber security, cyber–physical system (CPS), sixth generation (6G), smart grids, software-defined Internet of Things (SDIoT), vulnerability.**

NOMENCLATURE

Parameters and Variables

f, F	Power flow and information flow functions.
e	Power state variables.
u, c	Control variables and control command.
D	Uncertainty in CPS.
z	Measurements variable.
ϕ, Q	Diagonal matrix.
$P^{ls}_{i,j}(t)$	Power loss function.
$P_{i,j}(t)$, $Q_{i,j}(t)$	Real and reactive power.
$V_i(t)$, $\theta^{\text{bus}}_i(t)$	Voltage and phase angle.
x_t	State variable matrix.
$g(pn_t, g(mn_t))$	Predicted state and measurement noises.
PN_t, MN_t, S_t	Covariance matrix.
$\bar{x}_t$, $\bar{z}_t$	Current estimates.
$\hat{x}_{t-1}$	Predicted estimates.
A, L, W, V	Jacobian matrix.
$\tilde{e}x_t$	Error in estimates.
K	Kalman gain.
$\tilde{C}_t$, hs_{t-1}	Proposed cell value and hidden state.

Manuscript received August 1, 2020; revised October 14, 2020 and November 7, 2020; accepted November 23, 2020. Date of publication December 2, 2020; date of current version March 24, 2021. This work was supported in part by the U.S. National Science Foundation under Grant CCF-1908308 and Grant ECCS-1824710. *(Corresponding author: Muhammad Tariq.)*

Muhammad Tariq, Mansoor Ali, and Faisal Naeem are with the Electrical Engineering Department, National University of Computer and Emerging Sciences (Peshawar Campus), Peshawar 25000, Pakistan (e-mail: mtariq@princeton.edu).

H. Vincent Poor is with the Electrical Engineering Department, Princeton University, Princeton, NJ 08544 USA (e-mail: poor@princeton.edu).

Digital Object Identifier 10.1109/JIOT.2020.3042090

I. INTRODUCTION

THE SOFTWARE-DEFINED Internet of Things (SDIoT) is enabling different industrial entities by sharing relevant information for effective monitoring and control through centralized controllers using advanced sensing and communication technologies [1]. For example, in the context of smart grids, the performance of a grid can be affected by cyberattacks and physical disturbances, such as symmetric and asymmetric faults, which can lead a power system to instability. The framework of a smart grid is an example of a cyber–physical system (CPS), in which reliability of the network is increased by incorporating advanced sensing, communication and control infrastructure. For effective operation of a smart grid network, a reliable and secured information system is necessary from the perspective of cybersecurity. In particular, if a smart grid is under cyberattack, the physical layer performance is also affected, which may result in decreased reliability of the system [2].

In order to ensure safe and reliable operation of a power network, secure communication networks must be established so that energy management systems (EMSs) and wide area measurement systems (WAMSs) can operate uninterruptedly. One solution is to design robust routing algorithms among heterogeneous networks that can deliver information with minimum latency while satisfying Quality of Service (QoS) requirements. However, in real power system operation, the routing mechanism is based on the shortest path model, which is designed based on the operator's experience [3]. To overcome this deficiency and to improve the QoS for information in WAMS, an adaptive routing algorithm is proposed in [4]. One of the major drawbacks associated with this proposed techniques is that it addresses the security of the communication network only without considering the affect of cyberattacks on the physical system.

With the advent of artificial intelligence (AI) driven applications and Internet-of-Things (IoT)-enabled networks, such as smart grids, smart healthcare, and intelligent transportation systems (ITSs) etc., the fifth-generation (5G) communication

architectures cannot satisfy the challenges brought by the real-time requirement of services, such as ultra reliable low latency communication (URLLC) [5]. For example, one of the requirements to prevent cyber–physical attacks in smart grids is to achieve a minimum latency for countering the transients to minimize the chances of cascading failures.

The envisioned sixth-generation (6G) communication architecture can address these challenges by improving the data rate and achieving lower latency through use of a higher frequency range and other advances compared to the previous communication architectures. Preventive mechanism must be employed with 6G to limit the impact of cyberattacks on smart grids. Some preventive mechanisms include intrusion detection and prevention systems, which serve as a primary line of defense against multiple types of cyberattacks. From a smart grid perspective, the initial line of defense is achieved through circuit breakers or relays in order to stop the ripple effects of faults from propagating throughout a power system network [6]. However, in situations when a preventive mechanism is unable to mitigate the disturbances, detection algorithms must be employed to identify unexpected abnormalities in the network. Such detection mechanisms may include algorithms to identify unseen system states [7], [8], intruder or cyber–physical attacks [9], or the effects of both attack variants when they are combined [10]. Another practical approach was adopted in [11] where a linear state estimation (SE) technique was employed based on readings recorded from different phasor measurement units (PMUs) and a decentralized robust controller, incorporated at the individual buses. The robust controller monitors the state of the buses and also compares the estimated state with the PMUs' measurements. When an abnormality is detected, the robust controller will activate a distributed energy storage system (DESS), which either injects or absorbs the power to provide transient stability to the network [11]. A major drawback of this technique is that it assumes the overall system is linear, but in practice, the behavior of the system is highly nonlinear. By linearization we are neglecting some important parameters, which can lead to power system instability.

One of the many possible solutions to ensure stable and secure operation of a power system network is to perform accurate SE [12]. For better understanding of the system operation, SE is very important. Weighted least squares (WLSs) is one of the traditional techniques that accurately estimates a power system's state by utilizing high quality readings, obtain through PMUs [13]. However, the major drawback of WLS is that it does not give a good approximation when there is a significant nonlinearity in the power profile [14]. In [15], a fuzzy logic approach was adopted for load estimation. However, the major drawback associated with fuzzy logic is the tuning of fuzzy membership functions and the complexity when large numbers of nonlinear state parameters are approximated. To address this deficiency, Kalman filter-based estimation was proposed in [16]. A detailed analysis of the extended Kalman filter (EKF) and unscented Kalman filter was presented in [17]. Furthermore, the training of neural networks based on the EKF has shown promising results in SE [18]. The major drawback associated with the Kalman filter and WLS is the creation of the Jacobian and error covariance matrices, which increases complexity as the number of buses are increased. Moreover, if there is significant nonlinearity observed in a network, WLS or the Kalman filter cannot accurately estimate the cyberattacks. Furthermore, these techniques need an accurate system model to perform precise parametric SE.

One of the possible solutions to prevent cyberattacks is the effective use of SDIoT in smart grids. Software-defined networking (SDN) is a networking approach that decouples the control plane from the data plane to simplify the management of a network [19]. In the SDIoT, the intelligent control plane can monitor the network states globally in real-time and security techniques can be implemented to detect network threats [20]. 6G networks are expected to generate massive traffic with stringent QoS requirements. The existing data-analytic techniques for vulnerability assessment of cyber threats face scalability and delay issues while training on data. One such approach to solve the issue of training time is proposed in [21], where the authors adopted an SDN-enabled framework that forwarded the path calculation task to a graphics processing unit (GPU) for reducing the training time of the algorithms. Thus, the centralized nature of the SDN control plane can be effective for implementing the machine learning tasks on a GPU.

In this work, we propose an algorithm to enhance the reliability of 6G-enabled smart grids to ensure safe and secure operations by estimating the actual state, such as voltages and phase angles of the system even in the presence of cyber–physical attacks. For solving the issue of massive connections and states generated by the CPS, we propose a GPU-enabled adaptive robust state estimator. It comprises a deep learning algorithm, long short-term memory (LSTM), and a nonlinear EKF, called an LSTMKF. It works on the SDN controller to provide online parametric state estimates. The LSTM in the LSTMKF algorithm utilizes the measurements collected from PMUs in order to accurately estimate the state of the system. When an intruder attacks the communication network of PMUs, it causes mismatched-synchronization among different renewable energy resources (RERs). The proposed LSTMKF algorithm assigns higher priority to the LSTM-based state estimate and gives an indication that an intruder has attacked the network. Furthermore, if the input data is corrupted then more weight will be given to the PMUs' SE. Henceforth, it enables two levels of online SE to counter cyber–physical attacks on the system. To the best of the authors' knowledge, this is the first work that introduces LSTM in an EKF for detecting cyberattacks in 6G and SDIoT-enabled smart grids.

The key contributions of this article are as follows.

1) Proposing an SDIoT-enabled adaptive robust SE model, implemented on a GPU to detect and prevent cyberattacks in smart grids.
2) Improving reliability of envisioned 6G networks by performing two levels of online parametric SE for secure communication and load management.
3) Introducing LSTM-based time-series prediction that enables a utility operator to observe unexpected nonlinearity in the load profile introduced by an intruder.

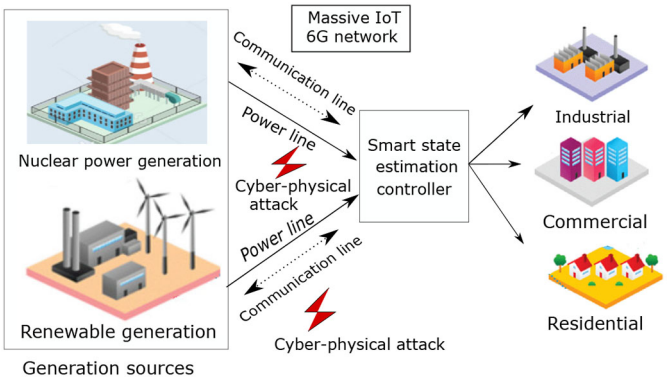


Fig. 1. Real and estimated state of voltage magnitude using an EKF.

The remainder of this article is organized as follows. The network architecture is explained in the Section II. The problem of interest is then formulated in Section III. A detailed analysis of the proposed algorithm is developed in Section IV, while the proposed mechanism is validated through simulation results in Section V. Finally, Section VI concludes this article.

II. Network Architecture

An envisioned SDIoT based 6G-enabled smart grid is shown in Fig. 1. In this vision, IoT networks are incorporated into the power system networks, and generate a massive volume of traffic through smart devices, such as smart meters, sensors, and actuators. In the smart grid, the communication network, WAMS, PMUs, advance metering infrastructure (AMI) and substation automation are embedded throughout the physical grid for reliable and efficient transmission, generation and distribution of the electric power. PMUs are installed at the generation sources that generate real-time measurement values of the loads, line power flows and the generation. The generation sources have a communication line on which the states of the network can be forwarded to the control center. The power line is used for the transmission of the power. One of the key challenges in the smart grid is that an intruder can interrupt the states of the network as a cyber–physical attack that can be seen in Fig. 1. The cyber–physical attack can corrupt the sensed data that may result in the synchronization between different generation sources that leads to the instability of the network. The proposed architecture forwards the network states to the SDN controller where the proposed algorithm can detect the corrupt states of the network. Thus, stabilizing the network by providing the accurate parametric information.

III. Problem Formulation

In smart grids, a CPS is employed for uninterrupted flow of information and electricity [2]. Following transformation between energy and information flow occurs in four corresponding steps.

Step 1: In this step, power/energy flow (f) of power state variables e at discrete time step n of a system model is observed over a complete control cycle, which is

$$f(e(n+1), u(n), D(n+1)) = 0 \tag{1}$$

where u and D represent control variables and uncertainty in a CPS, respectively.

Step 2: The energy flow computed at step 1 is now converted to information flow (F), which helps the utility operators to monitor the power system state variables. This process corresponds to the measurements of state variables in smart grids, which is given as

$$e(n) \rightarrow z(n) = \Phi \cdot e(n) \tag{2}$$

where z corresponds to a measurement variable and Φ represents a diagonal matrix. Each diagonal element shows a measurement state.

Step 3: The converted information obtained from the previous step is further utilized by a control center to generate the control command c in case of cyberattacks, which can be calculated as

$$c(n) = F(z(n)) = \arg\min f(c, z) | g(c, z) \leq h(c, z) \tag{3}$$

where $g(c, z) \leq h(c, z)$ is the optimization power network constraint.

Step 4: This step refers to the control process step, where the control command c is converted to control signal and is fed to control variable u for practical application. The control signal can be modeled as

$$c(n) \rightarrow u(n) = Q \cdot c(n) \tag{4}$$

where Q is the diagonal matrix. The combined equation for all of the four steps can be represented as

$$f(e(n+1), Q \cdot F(\Phi \cdot e(n)), D(n+1)) = 0. \tag{5}$$

The objective of this work is to minimize the impact on a power system due to cyber–physical attack by detecting and preventing these disturbances while satisfying the power network constraints. The main objective function $O(t)$ will be as follows:

$$O(t) = \sum_{i,j} P^{ls}_{i,j}(t) \tag{6}$$

where $P^{ls}_{i,j}(t)$ represents power loss between line i to j. The minimization function will be as follows:

$$\min \sum_{t=i}^{n} O(t). \tag{7}$$

Subject to the following constraints:

$$P_{i,j}(t) = \text{Rel}\left(V_i^2(t) y^*_{i,i} + V_i(t) V_j(t) \exp^{j\theta_{i,j}(t)} y^*_{i,j}\right) \tag{8}$$

$$Q_{i,j}(t) = \text{Img}\left(V_i^2(t) y^*_{i,i} + V_i(t) V_j(t) \exp^{j\theta_{i,j}(t)} y^*_{i,j}\right) \tag{9}$$

$$S^2_{i,j}(t) = P^2_{i,j}(t) + Q^2_{i,j}(t) \leq S^2_{\max(i,j)}(t) \tag{10}$$

$$P^{\text{gen}}_{\min,i}(t) \leq P^{\text{gen}}_i(t) \leq P^{\text{gen}}_{\max,i}(t) \tag{11}$$

$$Q^{\text{gen}}_{\min,i}(t) \leq Q^{\text{gen}}_i(t) \leq Q^{\text{gen}}_{\max,i}(t) \tag{12}$$

$$V^{\text{bus}}_{\min,i}(t) \leq V^{\text{bus}}_i(t) \leq V^{\text{bus}}_{\max,i}(t) \tag{13}$$

$$\theta^{\text{bus}}_{\min,i}(t) \leq \theta^{\text{bus}}_i(t) \leq \theta^{\text{bus}}_{\max,i}(t) \tag{14}$$

where $P_{i,j}(t)$, $Q_{i,j}(t)$, $V_i(t)$, and $V_j(t)$ show real, reactive power flows, and voltages at corresponding buses, respectively. While $P^{\text{gen}}_{\min,i}(t)$, $P^{\text{gen}}_{\max,i}(t)$, $Q^{\text{gen}}_{\min,i}(t)$, $Q^{\text{gen}}_{\max,i}(t)$, $V^{\text{bus}}_{\min,i}(t)$, and $V^{\text{bus}}_{\max,i}(t)$ show maximum and minimum real, reactive powers and voltages at the buses. $S^2_{i,j}(t)$ shows apparent power in the power lines and (10) shows limits on the injection of complex power into the network. The real and reactive power injection limits on the generator buses are presented in (11) and (12). The voltage $V^{\text{bus}}_i(t)$ and phase angle limit $\theta^{\text{bus}}_i(t)$ at the buses are shown in (13) and (14).

IV. Detail Analysis of the Model

In this section, we get detailed intuitive of the proposed algorithm in detecting and preventing cyber–physical attacks through numerical analysis.

A. Extended Kalman Filter-Based State Estimation

The EKF is a SE process to obtain the optimal states through a recursive process for nonlinear models. The model state equation and measurement model can be represented as

$$x_t = f(x_{t-1}, u_t) + g(\text{pn}_t) \tag{15}$$

$$z_k = l(x_t) + g(\text{mn}_t) \tag{16}$$

where x_t is state variables vector and $g(\text{pn}_t)$ and $g(\text{mn}_t)$ are predicted state noise and measurements noise, respectively. They are completely independent from each other having zero mean with PN_t and MN_t as covariance matrices, while u_t is the control vector. Measurement vector z_t gives true value when computed at actual state x_t. By neglecting the noise variables one can estimate true state variables. In that case, (15) and (16) become

$$\bar{x_t} = f(\hat{x}_{t-1}, u_t) \tag{17}$$

$$\bar{z_t} = l(\bar{x_t}). \tag{18}$$

In order to solve the nonlinear equation, we begin by linearizing the state equations (17) and (18), which are

$$x_t \approx \bar{x_t} + A(x_{t-1} - \hat{x}_{t-1}) + \text{Wpn}_t \tag{19}$$

$$z_t \approx \bar{z_t} + L(\text{x}_\text{t} - \bar{x}_\text{t}) + \text{Vmn}_t \tag{20}$$

where $\bar{x_t}$ and $\bar{z_t}$ are the current estimates, while $\hat{x}_{t-1}$ is the predicted estimate at an instant $t-1$. Jacobian matrices are A, L, W, and V. The error in estimated states $\tilde{e}x_t$ and measurement residuals $\tilde{e}z_t$ are as follows:

$$\tilde{e}x_t = x_t - \bar{x_t} \tag{21}$$

$$\tilde{e}z_t = z_t - \bar{z_t} \tag{22}$$

$$\tilde{e}x_t = A(x_{t-1} - \hat{x}_{t-1}) + \text{WPN}_t W^T \tag{23}$$

$$\tilde{e}z_t = L(\text{x}_\text{t} - \bar{x}_\text{t}) + \text{VMN}_t W^T \tag{24}$$

$$\tilde{e}z_t = L\tilde{e}x_t + \text{VMN}_t V^T \tag{25}$$

where (23)–(25) are achieved by manipulating (19)–(22), respectively. If we can predict the estimated error $\hat{e}_t$ and $\bar{x_t}$ then we can estimate new state at $t-1$, such as

$$\hat{x}_{t-1} = \bar{x_t} + \hat{e}_t \tag{26}$$

Algorithm 1: Estimating Network Parameters

Input 1: Initial estimates x_o, and P_o
Input 2: System nonlinear model description
Input 3: Specified convergence tolerance ϵ, and *MEE*
Output: Updated $\hat{x}_{\text{t|t}}$, and $P_{\text{t|t}}$
while *(MEE* $> \epsilon$*)* **do**
  Predict $\hat{x}_{\text{t|t}-1}$, and $P_{\text{t|t}-1}$ from (29), and (30);
  Update $\hat{x}_{\text{t|t}-1}$, and $P_{\text{t|t}-1}$ with PMUs measurement;
  if *($MN_t \rightarrow$ increases)* **then**
    K_t decreases, which means to give more weights to predicted estimates;
  else
    if *($MN_t \rightarrow$ decreases)* **then**
      K_t increases, which means to give more weights to measurement;
    else
      Output the updated states from (34) and (35):
    end
    Send $\hat{x}_{\text{t|t}}$, and $P_{\text{t|t}}$ as $\hat{x}_{\text{t|t}-1}$, and $P_{\text{t|t}-1}$ as an input to Algorithm 1 for next iteration;
  end
end

where

$$\hat{e}_t = K\tilde{e}z_t \tag{27}$$

by manipulating (22) and (27), (26) becomes

$$\hat{x}_{t-1} = \bar{x_t} + K(z_t - \bar{z_t}) \tag{28}$$

where K is the Kalman gain. Overall EKF can be summarized into two steps. They are state variables prediction step and state update step with measurements received through PMUs. Knowing the initial states x_o and predicted process covariance matrix P_o, the prediction and update states are as follows.

Prediction:

$$\hat{x}_{\text{t|t}-1} = f(\hat{x}_{\text{t}-1|\text{t}-1}, u_t) \tag{29}$$

$$P_{\text{t|t}-1} = A_t P_{\text{t}-1|\text{t}-1} A_t^T + \text{PN}_t. \tag{30}$$

Measurements-based state updating is given as

$$\tilde{e}z_t = z_t - l(\hat{x}_{\text{t|t}-1}) \tag{31}$$

$$S_t = L_t P_{\text{t|t}-1} L_t^T + \text{MN}_t \tag{32}$$

$$K_t = P_{\text{t|t}-1} L_t^T S_t^{-1} \tag{33}$$

$$\hat{x}_{\text{t|t}} = \hat{x}_{\text{t|t}-1} + K_t \tilde{e}z_t \tag{34}$$

$$P_{\text{t|t}} = (I - K_t L_t) P_{\text{t|t}-1} \tag{35}$$

where S_t stands for residuals covariance matrix, while (34) and (35) are used to update estimated states $\hat{x}_{\text{t|t}}$ and covariance matrix $P_{\text{t|t}}$. At the end, mean estimation error (MEE) is computed and if it is greater than the ϵ then next iteration will be conducted as shown in Algorithm 1.

B. Proposed LSTMKF Technique

In this study, we propose LSTMKF algorithm to estimate the voltage (V) and phase angles (θ) of a power system even in case when a cyberattack occurs. The drawback associated with EKF is the accurate determination of the Jacobians, which gets complex in case of a high nonlinear system. As a result, the EKF does not yield good approximation of the states variables.

Algorithm 2: Estimating Network Parameters Under Cyberattacks Using LSTMKF

Input 1: Initial estimation of x_o, and P_o
Input 2: Random initialization of hs_t, *weights*, C_t
Input 3: Data from sensor measurements
Input 4: Specified convergence tolerance ϵ, *MEE*, *LR*, *TD* and E_r
Output: Updated $\hat{x}_{t|t}$, and $P_{t|t}$
while *(MEE* $> \epsilon$*)* **do**
  Prediction of V and θ;
  for *(TD presented to network)* **do**
    the three prediction steps are performed using (36), (37), (38), (39), (40), (41);
    Compute E_r;
    if *(*$E_r > \epsilon$*)* **then**
      Update weights by back propagation through time algorithm;
    else
      Ouput the predicted V and θ;
    end
  end
  State updation step $\hat{x}_{t|t-1}$, and $P_{t|t-1}$ with PMUs data;
  if *(*$MN_t \rightarrow$ *increases)* **then**
    K_t decreases, so give more weights to predicted estimates;
  else
    if *(*$MN_t \rightarrow$ *decreases)* **then**
      K_t increases, which means give more weights to measurements;
    else
      Output the updated states $\hat{x}_{t|t}$ and covariance matrix $P_{t|t}$.
    end
    Send V, θ as input to Algo. 2 for more tuning;
  end
end

In order to overcome that deficiency, LSTM is incorporated at prediction step in EKF, which enables the system to observe nonlinearity in the profile that is intentionally added in the data by an intruder. LSTM utilizes current, voltage, frequency and also statistical data, which are obtained through various sensors to predict the state variables. Furthermore, the estimates are updated with PMU measurements at the updation step. Although PMU measurements are linear, we still use nonlinear EKF estimation at the updation step. In case when PMUs data are corrupted then nonlinear estimates and linear estimates are compared. There will be error in both estimates which will notify that some false data is injected. k is adjusted through recursive manner, when there is more uncertainty in PMU measurements in LSTMKF then more weights will be given to LSTM base SE. However, if there is some sensor noise at LSTM side then trust on the PMU measurement will be increased and prediction step will be computed at another time instant. The LSTMKF algorithm enables two level of online estimation. One at prediction step through LSTM and another at updation step. The proposed LSTMKF algorithm comprised of two steps, i.e., state estimate prediction step and state updation steps. At the prediction step, LSTM is adopted because of its ability to model time-series data more accurately due to its memory cell, which stores previous hidden states and utilizes it for the training of LSTM. Moreover, the network contains IoT connections and PMUs so it generates a massive amount of data. In that case, LSTMKF gives an efficient approximation about the current state of the envisioned 6G-enabled SDIoT even in case of cyberattacks. The prediction in LSTMKF consists of the following steps [22].

Prediction Step 1: This step is also called the forget step. In this step LSTM will decide what information is unnecessary and needs to be removed from memory cell and is decided by using the following equation, which is

$$v_t = \sigma\left(\mathrm{We}_v.\left[hs_{t-1}, x_t\right] + bi_v\right). \tag{36}$$

Prediction Step 2: This step is called cell update step. The sigmoid layer σ in single LSTM cell will decide what new values will be added and tanh layer will create new vector for the proposed cell values $\tilde{C}_t$. It only depends upon current input x_t and hidden state hs_{t-1}, and will be added to old cell state C_{t-1} as shown in the following equations, which are:

$$\mathrm{in}_t = \sigma\left(\mathrm{We}_{\mathrm{in}}.\left[hs_{t-1}, x_t\right] + bi_{\mathrm{in}}\right) \tag{37}$$

$$\tilde{C}_t = \tanh\left(\mathrm{We}_c.\left[hs_{t-1}, x_t\right] + bi_c\right) \tag{38}$$

$$C_t = v_t * C_{t-1} + in_t * \tilde{C}_t. \tag{39}$$

Prediction Step 3: At this step, the filtered output will be displayed. At first, hs_{t-1} and x_t are passed through the sigmoid layer and current cell state C_t is passed through tanh to finally compute what will be the final output hs_t of single LSTM cell at the current time instant. Such as

$$\mathrm{ou}_t = \sigma\left(\mathrm{We}_{\mathrm{ou}}.\left[hs_{t-1}, x_t\right] + bi_{\mathrm{ou}}\right) \tag{40}$$

$$hs_t = \mathrm{ou}_t * \tanh(C_t) \tag{41}$$

$$Er = \frac{1}{2}\sum_{1}^{n}(\mathrm{actual} - hs_t)^2 \tag{42}$$

where We_v, $\mathrm{We}_{\mathrm{in}}$, We_c, $\mathrm{We}_{\mathrm{ou}}$, bi_{v} bi_{in}, bi_c, and bi_{ou} are weights and biases of neural network layer. While mean square error Er is computed using (42). At the beginning, hs_t and C_t are initialized with zero vectors and then network weights and the matrix vectors are updated using back propagation through time algorithm (BPTT). As mentioned LSTM is adopted for time-series analysis, so the error is computed at an individual time step. After that the error is propagated backward through individual time step and weights are updated through the gradient descent algorithm in order to minimize the mean square error [22]. The predicted states are updated using measurements through (31)–(35). The detailed framework of the proposed framework is presented in Algorithm 2. Here, *TD*, *LR*, and *PL* stand for the training data, learning rate and predicted load, respectively.

C. Threat Model

Security threats to the 6G-enabled smart grid network can be the adversarial sources within the network and outside. Malicious sources can analyze the transit data to gather useful information or eavesdrop on smart grid network entities like smart meters and control center. Intruders or eavesdroppers can attack or compromise a smart grid network entity through components based, DoS, DDoS, IP spoofing, or MitM attacks. For example, in a medium threat, in smart meters an intruder can illegally install a monitoring software on a smart meter to

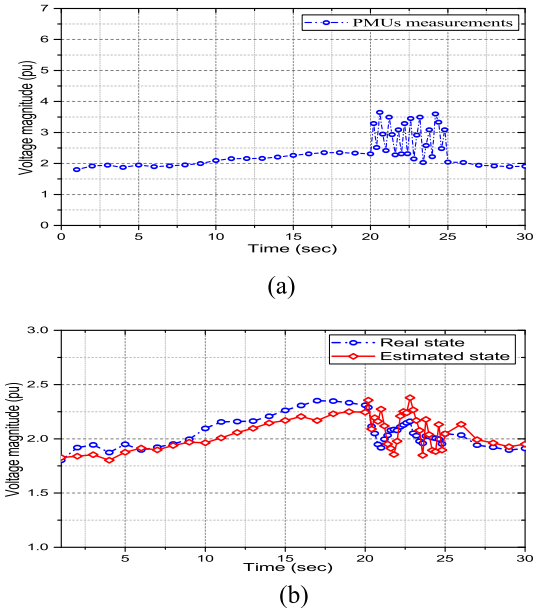


Fig. 2. Real and estimated states of voltage magnitude using an EKF. (a) Voltage magnitude. (b) Real and estimated state.

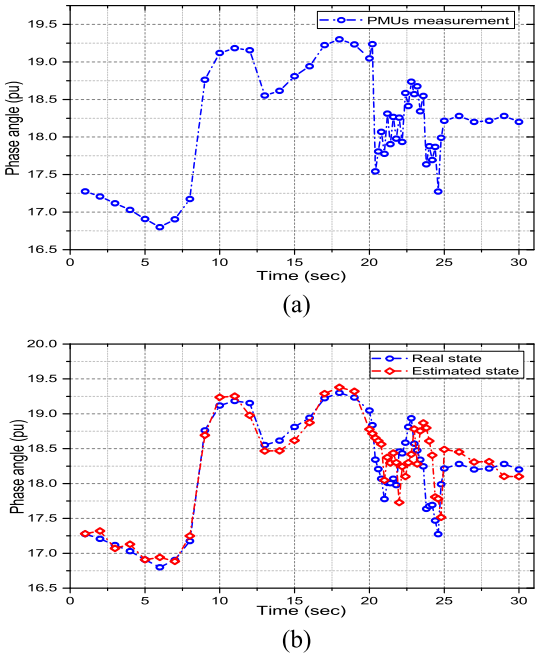


Fig. 3. Real and estimated state of phase angle using an EKF. (a) Phase angle measurements. (b) Real and estimated loads.

falsify billing report. A high threat can be when attackers falsify data related to key devices, such as transformers, PMUs, remote terminal units, or circuit breakers.

V. Results and Discussion

In this section, the methodology that is proposed to estimate the state parameters in case of cyberattacks in Section III is validated using simulation results. These simulations show the effectiveness and superiority of the proposed algorithm. The system is tested under IEEE 14, 30, and 118 bus systems and is compared with the algorithm presented in [11] that utilizes

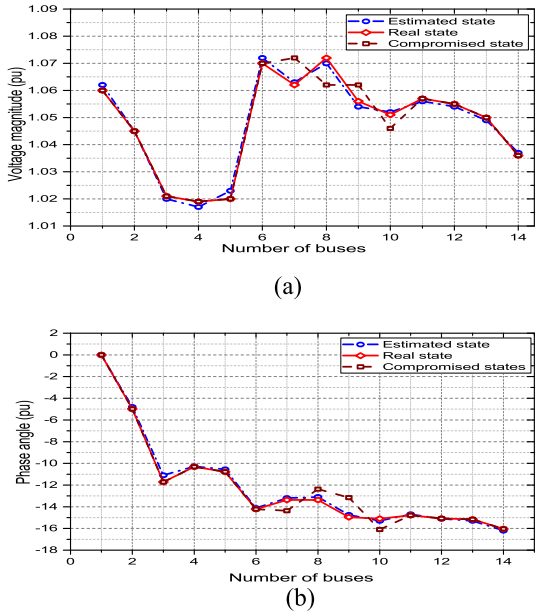


Fig. 4. SE of IEEE 14 bus system under cyberattack. (a) Estimated voltages. (b) Estimated phase angle.

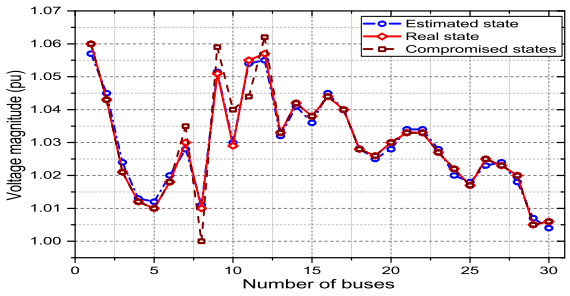
decentralized linear state estimator (DLSE). Here, 5 and 6 are generation buses, 8 and 22 are load buses and 1 and 2 are intermediate buses in the IEEE 14 and 30 bus systems, respectively. While in IEEE 118 bus system, there are 19 generation buses, 35 condensers, 177 power transmission lines, 9 transformer and 91 load buses. Moreover, PMUs are installed at different buses to observe the state of the system. The simulations were performed in both Python and MATLAB.

A. State Estimation Using EKF Under Cyberattack

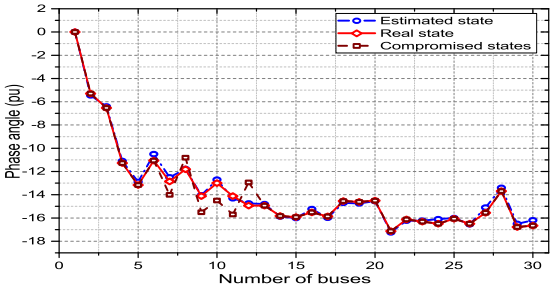
At first, the network is operated under the estimated states that is achieved through EKF as observed in Figs. 2 and 3. For the prediction step, the network parameters are utilized, while for state, PMU measurements are adopted as shown in Figs. 2(a) and 3(a). The state where PMU measurements are not corrupted, the EKF gives a good approximation of V and θ states as shown in Figs. 2(b) and 3(b) from time t 1 s to 20 s. However, when an intruder gets access to the control center and corrupts the PMU's (V and θ) measurements from $t = 20$ s to 25 s as shown in Figs. 2(a) and 3(a). The deviations between real and estimated states can be visualized in Figs. 2(b) and 3(b). These results in a power system network can be utilized where phase synchronization between various sources is a crucial factor.

B. State Estimation Using LSTMKF Under Cyberattack

The parametric SE under cyberattacks using proposed algorithm is discussed in this section. The sensor data and network parameters are first presented to LSTMKF to train itself. For training of LSTMKF, the Canadian data set of year 2012–2014 [23] is used. Then for state updation, PMU are utilized. Hence, it enables two levels of online estimation. The estimated states V and θ for IEEE 14, 30, and 118 bus systems can be visualized from Figs. 4–6, respectively. For IEEE 14 bus system, the PMU measurements at buses 7, 8, 9, and 10

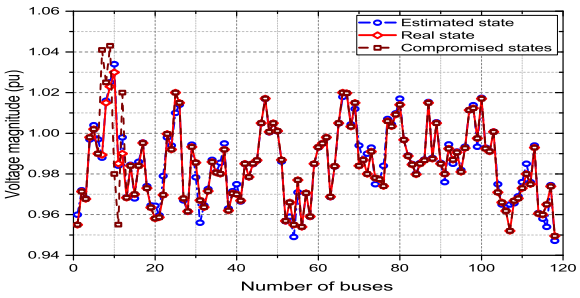


(a)

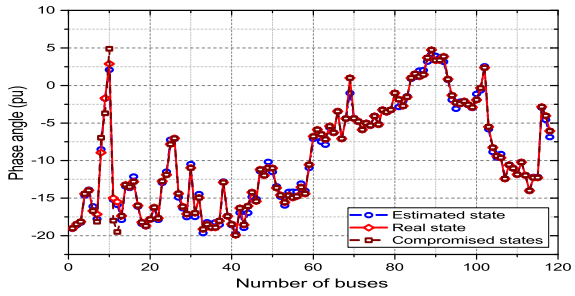


(b)

Fig. 5. SE of IEEE 30 bus system under cyberattack. (a) Estimated voltage. (b) Estimated phase angle.



(a)



(b)

Fig. 6. SE of IEEE 118 bus system under cyberattack. (a) Estimated voltage. (b) Estimated phase angle.

show corrupted data due to an intruder attack. However, even when the system is under cyberattacks, the proposed algorithm is able to estimate the real V and θ states correctly as shown in Figs. 4(a) and (b). In case of IEEE 30, and 118 bus systems, the PMU measurements at buses 7, 8, 9, 10, 11, and 12 also show corrupted data due to cyberattacks. However, the proposed algorithm is able to estimate the V and θ states correctly under cyberattacks and enable the utility operators to

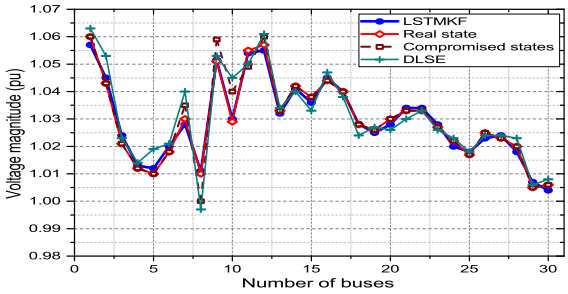


Fig. 7. Comparison of LSTMKF with DLSE.

detect attacks on the buses by an intruder as shown in Figs. 5 and 6. It can be clearly observed from the figures that the approximation of the states variable becomes better when measurement data is in excess. Hence, it proves that the proposed algorithm is better in networks having massive connections. In the above scenario, more priority is given to the prediction step as shown in Algorithm 2. This ultimately increases the reliability of the network and enhances QoS by reducing the network instability.

C. Comparison of LSTMKF With DLSE-Based State Estimation

The effectiveness of the proposed algorithm is verified by comparing it with DLSE in [11]. The algorithms are tested on IEEE 30 bus system and the estimated state V is compared under a cyberattack. In case of a false data injection at buses 7, 8, 9, 10, 11, and 12, the DLSE is unable to correctly estimate the V state variables. As a result, the corresponding buses are also deviated from real state as shown in Fig. 7. In contrast, the proposed LSTMKF algorithm is able to detect these variations in V profile and performs SE more effectively even in case of cyberattacks, as shown in Fig. 7.

VI. Conclusion

In this article, an SDIoT-enabled adaptive robust SE model has been proposed to detect and prevent cyberattacks in envisioned 6G-enabled smart grids. The idea is to improve reliability by performing two levels of online parametric SE for secure communication and load management. The proposed algorithm works on LSTM-based time-series prediction, which enables a utility operator to observe the unexpected nonlinearity introduced by an intruder in the load profile. To showcase the effectiveness of the proposed algorithm, it has been tested on IEEE 14, 30, and 118 bus systems. Simulation results have shown that the proposed algorithm gives accurate approximation of the state variables in case of cyberattacks in SDIoT-enabled smart grids connected through the envisioned next-generation technologies.

References

[1] A. Montazerolghaem and M. H. Yaghmaee, "Load-balanced and QoS-aware software-defined Internet of Things," *IEEE Internet Things J.*, vol. 7, no. 4, pp. 3323–3337, Apr. 2020.

[2] L. Xu, Q. Guo, T. Yang, and H. Sun, "Robust routing optimization for smart grids considering cyber-physical interdependence," *IEEE Trans. Smart Grid*, vol. 10, no. 5, pp. 5620–5629, Sep. 2019.

[3] S.-G. Yoon, S. Jang, Y.-H. Kim, and S. Bahk, "Opportunistic routing for smart grid with power line communication access networks," *IEEE Trans. Smart Grid*, vol. 5, no. 1, pp. 303–311, Jan. 2014.

[4] X. Li, Y.-C. Tian, G. Ledwich, Y. Mishra, X. Han, and C. Zhou, "Constrained optimization of multicast routing for wide area control of smart grid," *IEEE Trans. Smart Grid*, vol. 10, no. 4, pp. 3801–3808, Jul. 2019.

[5] P. Yang, Y. Xiao, M. Xiao, and S. Li, "6G wireless communications: Vision and potential techniques," *IEEE Netw.*, vol. 33, no. 4, pp. 70–75, Jul./Aug. 2019.

[6] Y. Zhang and Z. Wang, "A novel approach to fault detection in complex electric power systems," *Adv. Elect. Comput. Eng.*, vol. 14, no. 3, pp. 27–33, 2014.

[7] J. Zhao *et al.*, "Power system dynamic state estimation: Motivations, definitions, methodologies, and future work," *IEEE Trans. Power Syst.*, vol. 34, no. 4, pp. 3188–3198, Jul. 2019.

[8] S. Rasool *et al.*, "Blockchain-enabled reliable osmotic computing for Cloud of Things: Applications and challenges," *IEEE Internet Things Mag.*, vol. 3, no. 2, pp. 63–67, Jun. 2020.

[9] R. Berthier, W. H. Sanders, and H. Khurana, "Intrusion detection for advanced metering infrastructures: Requirements and architectural directions," in *Proc. IEEE Int. Conf. Smart Grid Commun.*, 2010, pp. 350–355.

[10] S. Zonouz *et al.*, "SCPSE: Security-oriented cyber-physical state estimation for power grid critical infrastructures," *IEEE Trans. Smart Grid*, vol. 3, no. 4, pp. 1790–1799, Dec. 2012.

[11] M. Ayar *et al.*, "Cyber-physical robust control framework for enhancing transient stability of smart grids," *IET Cyber Phys. Syst. Theory Appl.*, vol. 2, no. 4, pp. 198–206, 2017.

[12] D. Atanackovic and V. Dabic, "Deployment of real-time state estimator and load flow in BC Hydro DMS-challenges and opportunities," in *Proc. IEEE Power Energy Soc. Gen. Meeting*, 2013, pp. 1–5.

[13] L. Schenato, G. Barchi, D. Macii, R. Arghandeh, K. Poolla, and A. Von Meier, "Bayesian linear state estimation using smart meters and PMUs measurements in distribution grids," in *Proc. IEEE Int. Conf. Smart Grid Commun. (SmartGridComm)*, 2014, pp. 572–577.

[14] M. Ali, M. Adnan, M. Tariq, and H. V. Poor, "Load forecasting through estimated parametrized based fuzzy inference system in smart grids," *IEEE Trans. Fuzzy Syst.*, early access, Apr. 13, 2020, doi: 10.1109/TFUZZ.2020.2986982.

[15] M. Ali, M. Adnan, and M. Tariq, "Optimum control strategies for short term load forecasting in smart grids," *Int. J. Elect. Power Energy Syst.*, vol. 113, pp. 792–806, Dec. 2019.

[16] M. B. Do Coutto Filho and J. C. S. de Souza, "Forecasting-aided state estimation—Part I: Panorama," *IEEE Trans. Power Syst.*, vol. 24, no. 4, pp. 1667–1677, Nov. 2009.

[17] S.-C. Huang, C.-N. Lu, and Y.-L. Lo, "Evaluation of AMI and SCADA data synergy for distribution feeder modeling," *IEEE Trans. Smart Grid*, vol. 6, no. 4, pp. 1639–1647, Jul. 2015.

[18] C. Carquex, C. Rosenberg, and K. Bhattacharya, "State estimation in power distribution systems based on ensemble Kalman filtering," *IEEE Trans. Power Syst.*, vol. 33, no. 6, pp. 6600–6610, Nov. 2018.

[19] F. Naeem, G. Srivastava, and M. Tariq, "A software defined network based fuzzy normalized neural adaptive multipath congestion control for the Internet of Things," *IEEE Trans. Netw. Sci. Eng.*, early access, Apr. 28, 2020, doi: 10.1109/TNSE.2020.2991106.

[20] M. B. Mollah *et al.*, "Blockchain for future smart grid: A comprehensive survey," *IEEE Internet Things J.*, early access, May 11, 2020, doi: 10.1109/JIOT.2020.2993601.

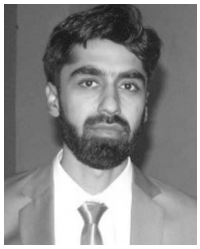
[21] F. Naeem, M. Tariq, and H. V. Poor, "SDN-enabled energy-efficient routing optimization framework for industrial Internet of Things," *IEEE Trans. Ind. Informat.*, early access, Jul. 3, 2020, doi: 10.1109/TII.2020.3006885.

[22] Y. Wang, D. Gan, M. Sun, N. Zhang, Z. Lu, and C. Kang, "Probabilistic individual load forecasting using pinball loss guided LSTM," *Appl. Energy*, vol. 235, pp. 10–20, Feb. 2019.

[23] S. Makonin, B. Ellert, I. V. Bajić, and F. Popowich, "Electricity, water, and natural gas consumption of a residential house in Canada from 2012 to 2014," *Sci. Data*, vol. 3, no. 1, 2016, Art. no. 160037.

Muhammad Tariq (Senior Member, IEEE) received the M.S. degree from Hanyang University, Seoul, South Korea, in 2009, and the Ph.D. degree from Waseda University, Tokyo, Japan, in 2012.

He is the Director of the National University of Computer and Emerging Sciences (Peshawar Campus), Peshawar, Pakistan, where he is an Associate Professor. He completed his Postdoctoral Fellowship of Princeton University, Princeton, NJ, USA, as a Fulbright Scholar in 2016, where he is also a Visiting Research Collaborator. His research interests are in network science, energy systems, and Internet of Things.

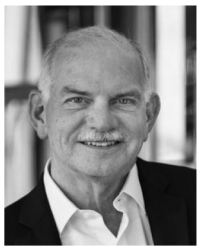


Mansoor Ali (Member, IEEE) received the B.S. degree in electrical engineering from the National University of Computer and Emerging Sciences (Peshawar Campus), Peshawar, Pakistan, in 2013, the M.S. degree in electrical engineering from CECOS University, Peshawar, in 2016, and the Ph.D. degree in electrical engineering from the National University of Computer and Emerging Sciences in 2020.

His research interests include load forecasting in power system networks, fuzzy control, and power flow control.

Faisal Naeem (Member, IEEE) received the B.S. degree in electrical engineering from the National University of Computer and Emerging Sciences (Peshawar Campus), Peshawar, Pakistan, in 2013, and the M.S. degree in electrical engineering from the University of Engineering and Technology Peshawar, Peshawar, in 2017. He is currently pursuing the Ph.D. degree with the National University of Computer and Emerging Sciences.

His research interests include Internet of Things, software-defined networking, and cyber–physical systems.



H. Vincent Poor (Life Fellow, IEEE) received the Ph.D. degree in EECS from Princeton University, Princeton, NJ, USA, in 1977.

From 1977 until 1990, he was on the faculty of the University of Illinois at Urbana–Champaign, Urbana, IL, USA. Since 1990, he has been on the faculty at Princeton, where he is the Michael Henry Strater University Professor of Electrical Engineering. From 2006 until 2016, he also served as the Dean of Princeton's School of Engineering and Applied Science. His research interests are in the areas of information theory, machine learning and network science, and their applications in wireless networks, energy systems, and related fields. Among his publications in these areas is the forthcoming book *Advanced Data Analytics for Power Systems* (Cambridge University Press, 2021).

Dr. Poor is a member of the National Academy of Engineering and the National Academy of Sciences, and is a foreign member of the Chinese Academy of Sciences, the Royal Society, and other national and international academies. Recent recognition of his work includes the 2017 IEEE Alexander Graham Bell Medal and the 2019 ASEE Benjamin Garver Lamme Award.