A Smart Digital Twin Enabled Security Framework for Vehicle-to-Grid Cyber-Physical Systems

Mansoor Ali, *Member, IEEE*, Georges Kaddoum, *Senior Member, IEEE*, Wen-Tai Li, *Member, IEEE*, Chau Yuen, *Fellow, IEEE*, Muhammad Tariq, *Senior Member, IEEE*, and H. Vincent Poor, *Life Fellow, IEEE*

***Abstract*— The rapid growth of electric vehicle (EV) penetration has led to more flexible and reliable vehicle-to-grid-enabled cyber-physical systems (V2G-CPSs). However, the increasing system complexity also makes them more vulnerable to cyber-physical threats. Coordinated cyber attacks (CCAs) have emerged as a major concern, requiring effective detection and mitigation strategies within V2G-CPSs. Digital twin (DT) technologies have shown promise in mitigating system complexity and providing diverse functionalities for complex tasks such as system monitoring, analysis, and optimal control. This paper presents a resilient and secure framework for CCA detection and mitigation in V2G-CPSs, leveraging a smart DT-enabled approach. The framework introduces a smarter DT orchestrator that utilizes long short-term memory (LSTM) based actor-critic deep reinforcement learning (LSTM-DRL) in the DT virtual replica. The LSTM algorithm estimates the system states, which are then used by the DRL network to detect CCAs and take appropriate actions to minimize their impact. To validate the effectiveness and practicality of the proposed smart DT framework, case studies are conducted on an IEEE 30 bus system-based V2G-CPS, considering different CCA types such as malicious V2G node or control command attacks. The results demonstrate that the framework is capable of accurately estimating system states, detecting various CCAs, and mitigating the impact of attacks within 5 seconds.**

***Index Terms*— Coordinated cyber attacks, digital twin, cyber-physical systems, long short term memory, deep reinforcement learning.**

Manuscript received 6 January 2023; revised 15 July 2023; accepted 7 August 2023. Date of publication 23 August 2023; date of current version 29 August 2023. The work of H. Vincent Poor was supported by the U.S. National Science Foundation under Grant CNS-2128448 and Grant ECCS-2335876. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Andrew Clark. *(Corresponding authors: Mansoor Ali; Chau Yuen.)*

Mansoor Ali is with the Electrical Engineering Department, ETS, University of Quebec, Montreal, QC H3C 3P8, Canada (e-mail: mansoor.ali.1@etsmtl.net).

Georges Kaddoum is with the Electrical Engineering Department, ETS, University of Quebec, Montreal, QC H3C 3P8, Canada, and also with the Cyber Security Systems and Applied AI Research Center, Lebanese American University, Beirut 1102 2801, Lebanon (e-mail: georges.kaddoum@etsmtl.ca).

Wen-Tai Li is with the Department of Engineering Product Development, Singapore University of Technology and Design, Singapore 487372 (e-mail: wentai_li@sutd.edu.sg).

Chau Yuen is with the School of Electrical and Electronics Engineering, Nanyang Technological University, Singapore 639798 (e-mail: chau.yuen@ntu.edu.sg).

Muhammad Tariq is with the Department of Electrical Engineering, National University of Computer and Emerging Sciences, Islamabad 44000, Pakistan (e-mail: mtariq@princeton.edu).

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

Digital Object Identifier 10.1109/TIFS.2023.3305916

I. Introduction

THE integration of intelligent electronic devices, communication infrastructure, and renewable energy resources (RERs) has led to the emergence of the smart grid, revolutionizing the global energy infrastructure [1]. The smart grid transforms traditional power systems from passive networks into active networks, enabling energy consumers to become energy prosumers. However, this transition also introduces complexity and computational demands to the energy system. The smart grid encompasses a wide range of components, including RERs, energy storage devices, electronic converters, and flexible transmission system devices, which enhance system reliability. However, the adoption of intelligent electronic devices, advanced communication systems, adaptive control systems, and phasor measurement units (PMUs) to support active grid operations increases the cyber complexity of the system [2]. If these advanced technologies are integrated into the grid without proper security mechanisms, the reliability of the energy infrastructure may be compromised. Adversaries can exploit multiple points of vulnerability, leading to potential attacks and disruptions in the system's operation. It is essential to develop robust security measures to protect the smart grid and mitigate the risks associated with cyber threats. By addressing these security challenges, the smart grid can maintain its reliability and ensure the uninterrupted delivery of energy services.

One emerging application enabled by the smart grid is the vehicle-to-grid (V2G) operation. A bidirectional flow of energy and communication exists in V2G-enabled cyber-physical systems (V2G-CPSs). The increasing penetration of electric vehicles (EVs) enhances the flexibility and reliability of V2G-CPSs. However, this comes at the cost of increased complexity in V2G-CPSs. Various industries have recently embraced digital twin (DT) technologies to support crucial tasks like system monitoring, analysis, and optimal control. However, by adding more V2G points into the network, the potential vulnerabilities to cyber attacks also increase [3]. One such example of a cyber attack is recorded in [4], where an attack on the Ukrainian power grid resulted in a large-scale blackout for almost 6 hours, affecting 230,000 people in 2015. Here, the adversary deployed false control signals in the control channel to operate the network circuit breakers, namely, switching attacks (SAs).Traditional supervisory control and data acquisition (SCADA) systems use bad data detection models to filter malicious measurements from PMUs and other

sensing devices. However, it has been observed from recent studies that intelligently created false data injection attacks (FDIAs) could bypass the current bad data detection models. In FDIA, the adversary tampers the data so that detection algorithms cannot recognize the corrupted data [5], [6] and would mislead the control operator to take wrong actions, leading to system instability.

Due to the development of various cyber attack strategies, research works have also been carried out to improve the defense of V2G-CPSs against potential attacks such as FDIA and SA [7], [8]. For instance, the authors in [9] investigated how the FDIA would manipulate the electricity market by tampering with the price parameters. In there the authors provide countermeasures by securing some critical state variables. Moreover, the research works that are dedicated to securing the smart meters and PMUs measurements against FDIA can be found in [10] and [11]. However, studies dealing with cyber attacks on DT from physical processes, data transmission, and to decision control are limited. For instance, the effects of unbalanced voltage distribution on the system network under inadequate control action by the operator were presented in [12]. Here, the adversary deployed false control signals in the control channel to operate the circuit breakers in the network. Moreover, the impact of coordinated cyber attacks (CCAs) on V2G-CPSs has not been fully studied yet. CCAs can easily disturb the information flow, power flow, or even both of them. Furthermore, shuffling the attacks, such as removing or isolating the attacked equipment, among the sensor network, controller, and communication channel will harm the security of the network [13]. This scenario becomes more severe when the information of physical processes and the availability of V2G devices, transferred to the DT replica of the V2G-CPSs, are tampered with by CCAs. In addition, CCAs have the potential of causing $N-K$ contingencies in communication and power networks, whereas $N-K$ contingencies mean the successive tripping of circuit breakers in power networks or interruptions in communication networks. The physical impact of $N-K$ contingencies is in the form of blackouts. Similarly, if the DT, which is responsible for providing secure and safe operation of the V2G-CPSs, is tempered, then there is a need for some intelligent algorithms deployed in the DT replica of V2G-CPSs. Those algorithms will be dedicated to not only detecting CCAs on the physical processes as identification of malicious V2G nodes and SAs, and data transmission as false information transferred to DT, but also mitigating the impact of CCAs that will be in the form of $N-K$ contingencies by adaptive control strategies.

This paper addresses the gap in the existing literature by developing a robust detection and mitigation mechanism against the CCAs on V2G-CPSs. In particular, the main aim of this paper is to identify malicious users, which can launch FDIAs and manipulate the actual information of physical processes transmitted to the SCADA system, or SAs that inject the false control signals through the communication channel for the false operation of the circuit breakers. In this regard, a smart DT replica of V2G-CPSs is proposed to detect and mitigate CCAs in the system. In the proposed smart DT framework, the long short-term memory (LSTM) based deep reinforcement learning (DRL) algorithm, namely LSTM-DRL, is incorporated in a virtual replica of V2G-CPSs. The LSTM algorithm is responsible for estimation the actual states of V2G-CPS. Based on the estimated states, the DRL algorithm trains its agent and detects the abnormal behavior in V2G-CPSs followed by taking actions to mitigate the corresponding impact. Furthermore, the actor-critic technique is adopted to further improve the system performance and the convergence time of the proposed LSTM-DRL algorithm.

In summary, the key contributions of this paper are:

- proposing a smart DT framework for a secure and safe operation of V2G-CPSs under CCAs, such as FDIAs and SAs,
- formulating a mathematical model of the smart DT for V2G-CPSs incorporating V2G connections and RESs as wind turbines (WT), and
- developing and incorporating an LSTM-DRL algorithm in the smart DT for fast detection and mitigation of CCAs.

The rest of the paper is organized as follows. In Section II, the comparative literature review is presented. Section III includes the information about V2G and threats model. Section IV describes the mathematical model of the LSTM-DRL framework. Section V includes results, discussion, and testing of the LSTM-DRL algorithm under different cyber threats. Section VI concludes the paper.

II. Related Work

Among various types of cyber attacks, one of the most threatening attacks is FDIA, which mostly happens in smart grids and is discussed in the literature. FDIAs, were identified in [14], in which a methodology was introduced to detect this type of attack even though it by-pass the bad data detection process in weighted least square state estimation. The authors adopted in [14] adopted the Kullback-Leibler distance (KLD) algorithm, which is used to measure the distance between two probability values of measurements. In the event if attacks happens, the algorithm will produce larger KLD values, which shows that measurements are being compromised. In addition, an attack on embedded electronics systems was discussed in [15], in which a torjan attacks were used to compromise the intelligent electronics devices. Similarly, FDIAs were also identified by authors in [16], who revealed that traditional bad data detection could not detect the corrupted measurements during state estimation. A more severe case of FDIA is discussed in [17] and [18] where the attack causes cascaded outages in power grids.

Inspired by [16], new cyber threats where the attacker tampered with the transformer taps have been extensively investigated, which also increased the researchers' interest in devising robust detection and mitigation techniques. Early, state estimation algorithms are developed that are based on the DC power flow model to detect data attacks on smart grids in [19]. Several techniques are then available that cover the area of state estimation for complex systems like V2G-CPSs. For instance, the authors of [20] adopted the Kalman filter to detect FDIAs. In addition, an optimization technique to cluster vulnerable nodes is proposed in [21]. However,

the algorithm mentioned in [21] involves a computationally detection process. Moreover, the major drawback associated with the Kalman filter is the creation of the Jacobian and error covariance matrices, which increases complexity as the number of buses increases. Furthermore, if there is high nonlinearity observed in a network, then Kalman filter do not yield better results and these techniques need an accurate knowledge model to perform precise state estimations [22]. A simpler non-iterative method is proposed in [23] for FDIA detection based on measurements obtained from SCADA and PMUs. The advanced form of cyber attacks on V2G-CPSs, that is, CCAs, has been discussed in [24]. In this work, the attack vectors are created coordinately to avoid the bad data detection algorithm. In addition, the countermeasure approach is also proposed for attack detection by monitoring secure PMU measurements and line impedance. However, SAs on generation nodes and on DT was not considered.

Aside from FDIA, another noteworthy type of cyber attack, namely SA, can cause an abnormal topology configuration leading to cascading contingencies in power grids. To counter the abnormalities due to SA, the authors in [25] proposed a multi-agent system (MAS) technique for mitigating cascading failures. The algorithm chose an optimal combination from the number of combinations presented to dispatch the power from a generator. The optimal generator combination is selected by computing sensitivities gain, which is based on giving rewards and penalties for different load flow patterns. Moreover, the algorithm in [25] provides effective solutions if contingencies occur due to natural phenomena. If initial contingencies are not tackled in time, they may expand to $N-K$ contingencies that can cause the network unstable resulting in blackouts.

Considering the complexity of V2G-CPSs, the control strategies of system operation should be coordinated and distributed to ensure economic communication bandwidth utilization and flexible operation of the network components. However, coordinated distributed control structures are also vulnerable to cyber attacks [26], [27], [28]. To prevent and mitigate CCAs, there have been many effects on secured and distributed control strategies in V2G-CPSs. In this regard, the authors in [29] proposed a resilient coordinated control system for the packet loss problem, while in [30], a hierarchical distributed control scheme was proposed. The primary function of the proposed algorithm in [30] was to detect the attacked controller agent and isolate it from the network. In addition, the dynamic behavior of the various agents is studied using morphology strategies in order to identify the agent, which is attacked and then devise a methodology based on graph theory to mitigate the attack [31]. For the synchronized operation of the sensors in the network under attack, compensator-based control strategies were adopted in [32], [33]. The authors in [31], [32], [33], and [34] have observed the fluctuation in the voltage in order to identify the attack and enable synchronization among different devices by detecting the malicious power system control and operating devices. However, such algorithms are computationally expensive and the effect of CCAs on DTs was not discussed. Besides, if cyberspace is compromised where the whole detection and mitigation process takes place, the authors in [31], [32], and [33] did not provide any action to countermeasure such attacks.

Based on the above comprehensive review and analysis, it has been observed that most CCAs detection methods are specifically for state estimators, and the mitigation methods are developed to isolate or remove the attacked nodes in systems. However, there are almost no studies on the use of DT for CCAs detection and mitigation. In other words, the potential of DTs for CCAs detection and mitigation has not been fully explored. To this purpose, we proposed a DT-enabled intelligent framework to detect and mitigate CCAs in V2G-CPSs. One of the important features of this work is to show how the smart DT model can provide fast attack detection and timely control strategies to prevent the $N-K$ contingencies in V2G-CPSs.

III. System Model

A. Vehicle-to-Grid Cyber-Physical System (V2G-CPS)

A schematic of the V2G-CPS studied in this paper is shown in Fig. 1 with its corresponding DT. The V2G-CPS operates as a closed-loop control system and comprised of EVs, WTs, and generation plants along with the dynamic varying load. The diversified energy sources make the V2G-CPS more flexible and reliable to satisfy the various demand requirements. However, hsving multiple energy sources also makes system operations, such as power flow control and energy dispatch, more complex. Moreover, with the increase of energy sources, especially EV nodes, V2G-CPS becomes more vulnerable to various adversaries and attacks. The DT of V2G-CPS has the capability to reduce the heavy burden of system operation, but it is inevitable to security threats such as CCAs. This is due to the fact that the reliability of DT relies on the accuracy of information updated from the physical process of V2G-CPS. For instance, adversaries can launch FDIAs on the amount of information on connected EVs, or can release SAs on the status of critical circuit breakers. The malicious information will be communicated with the DT of V2G-CPS, and may affect the decision-making process of the DT to take inappropriate actions leading to system instability. Stability of power system refers to the ability to regain its normal operational equilibrium after being subjected to cyber or physical attacks [35], [36]. In a V2G-CPS, the power and current of system is monitored and the system is declared as stable system if these parameters are within thresholds and are discussed in detail in next section.

To detect and mitigate CCAs on the V2G-CPS and the corresponding DT, in this paper, we develop a security check framework in the DT virtual replica based on the LSTM-DRL method. Before giving more details on the proposed framework and LSTM-DRL method, the DT model of V2G-CPS and the threat model of CCA are first described in the following sections.

B. Digital Twin of V2G-CPS

To make the DT model more realistic, a strict mathematical model to represent the physical characteristics of V2G-CPS

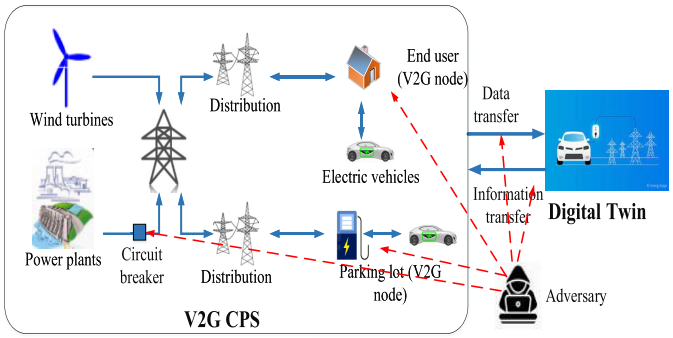


Fig. 1. Generalized architecture of V2G-CPS and digital twin.

is necessary. In this paper, the physical twin model of V2G-CPS is considered for the development of DT, and the power system's actual parameters are also considered for better designing and monitoring V2G-CPS.

1) Physical Twin Model of V2G-CPS: In the V2G-CPS, when any unexpected variations in the power flow occur, the system will re-disturb the whole power flow to balance supply and demand. Those variations may be due to generation interruption, line outages, and even CCAs. Under normal operation, the following security constraints will be held;

$$I_k^L \le I_{k,\max}^L, \tag{1}$$

$$P_k^L \le P_{k,\max}^L, \tag{2}$$

$$P_{i,\min}^G, P_{i,\min}^D \le P_i^G, P_i^D \le P_{i,\max}^G, P_{i,\max}^D. \tag{3}$$

where, I_k^L and P_k^L are the actual current and power of the k^{th} transmission line while $I_{k,\max}^L$ and $P_{k,\max}^L$ are the corresponding maximum current and power limits respectively. $P_{i,\min}^G$ and $P_{i,\max}^G$ are the minimum and maximum output power of the generator on the i^{th} bus, and $P_{i,\min}^D$ and $P_{i,\max}^D$ are the minimum and maximum load capabilities of the i^{th} bus, respectively. Furthermore, the real power flow will be balanced at each bus i, that is,

$$P_i^G - P_i^D - \sum_{j=1}^{N} |V_i||V_j||Y_{\text{ij}}|cos(\phi_{\text{ij}} - \delta_{\text{i}} - \delta_{\text{j}}) = 0, \tag{4}$$

where $|V|$ and δ are respectively the magnitude and phase angles of voltage, and N is the total number of buses in the V2G-CPS. $|Y_{\text{ij}}|$ and ϕ_{ij} are the magnitude and angle of the Y-bus matrix of the system, respectively [37].

However, some current and power flow may violate the safety constraints in the case of CCAs, such as

$$I_k^L, P_k^L > I_{k,\max}^L, P_{k,\max}^L. \tag{5}$$

Considering such overloading flow may cause $N-K$ contingencies leading to cascading failures, the proposed security framework is first activated by observing any unexpected variations in the power flow, and then, continuously monitors the constraints of (1), (2), and (3) to detect CCAs and mitigate $N-K$ contingencies due to CCAs. Furthermore, the proposed algorithm also tackles the actual power demand of each bus at each time slot t by the forecasted power demand as

$$P_{i,\text{actual}}^D(t) = P_{i,\text{forecast}}^D(t) + R_i^D(t) + P_{i,\text{gap}}^D(t), \tag{6}$$

$$P_{\text{need}}(t) = \sum_{i=1}^{N} P_{i,\text{gap}}^D(t), \tag{7}$$

where $P_{i,\text{actual}}^D$, $P_{i,\text{forecast}}^D$, R_i^D, and $P_{i,\text{gap}}^D$ represent the actual demand, forecasted demand, randomness in forecasted demand, and the gap between actual demand and forecasted demand due to unexpected variations, respectively. When the V2G-CPS is under normal operation, there is no unexpected variation, and the control loop will make the actual and forecasted demand similar by reducing the R_i^D. In that case,

$$P_{i,\text{actual}}^D(t) = P_{i,\text{forecast}}^D(t), \ \forall i \in N. \tag{8}$$

Moreover, the total amount of forecasted generations will be close to the total amount of forecasted demand, that is,

$$\sum_{i=1}^{N}(P_{i,forecast}^G(t) + R_i^G(t)), = \sum_{i=1}^{N}(P_{i,forecast}^D(t) + R_i^D(t)), \tag{9}$$

where $P_{i,forecast}^G$ and R_i^G stand for the forecasted generations on each bus and randomness in a forecasted generation, respectively. However, once the V2G-CPS is under CCAs, the unexpected variations between the data collected and the actual power demand at the current time will appear as $P_{i,\text{gap}}^D(t)$ and $P_{\text{need}}(t)$.

The following constraints on the generation buses, load buses, and transmission line will be considered so that no individual bus observes any stress in the N-K contingencies mitigation, as power is being rerouted from RERs along with its generations, so the need of monitoring the thresholds limits of power lines must be considered.

$$P_{\text{i,k}}^{\text{capacity, G}} = min(P_i^G, P^{G}{}_{\text{k,max}} - P_{\text{k}}{}^{G}), \tag{10}$$

$$P_{\text{i,k}}^{\text{capacity, L}} = min(P_{\text{i}}{}^{G}, P_{\text{k}}{}^{L}), \tag{11}$$

$$P_{\text{i,k}}^{\text{capacity, power line}} = min(|P^{\text{L}}{}_{\text{i,max}}| - |P_{\text{i}}{}^{L}|), \tag{12}$$

$$P_{\text{i,k}}^{\text{total allowed}} = min(P_{\text{i}}^{\text{capacity, G}}, P_{\text{i}}^{\text{capacity, L}}), \tag{13}$$

where P_i^G and P_k^G are the powers to be dispatched at the buses i and k, respectively. $P^{G}{}_{\text{k,max}}$ is the total power available at bus k and P_k^L is the net demand at bus k. Moreover, $P^{L}{}_{\text{i,max}}$ and P_i^L are the total capacity and the actual power flow in line i. To fill up the unexpected gap of generation and demand, that is $P_{need}(t)$, we consider the contribution of RESs as the reserve power generation. Here,

$$[P_{need}(t) < P_{max}^R(t)], \tag{14}$$

where $P_{max}^R(t)$ is the maximum output capacity of RERs at time slot t. If $P_{need}(t)$ satisfies the above constraint, the proposed method will only reroute the power from RESs to meet $P_{need}(t)$. Otherwise, V2G mode, described in the next section, will also be active to reduce the amount of $P_{need}(t)$.

In this paper, we focus on WTs RERs. The aerodynamics of the blades are characterized using different coefficients such

as $C_p(\beta, \lambda)$ and $C_q(\beta, \lambda)$, which represents power aerodynamics coefficients. Here, β stands for the pitch angle of the blade while λ stands for the speed ratio and is computed as $\lambda = Rw_r/V_r$. While R and w_r are blade length and its corresponding angular speed while V_r is the effective wind speed at the rotor plane. Based on the coefficients discussed overall power P_a and torque T_a of the wind turbine will be;

$$T_a = \frac{1}{2}\rho A R V_r^2 C_q(\beta, \lambda), \tag{15}$$

$$P_a = \frac{1}{2}\rho A R V_r^3 C_p(\beta, \lambda), \tag{16}$$

where, ρ is the air density and A corresponds to the blade area which is equal to πR^2. Considering the thrust factor, the relative velocity of wind can be represented as, $V_r = V_w - V_n$, where V_w and V_n are the free wind speed and nacelle velocity in direction of wind turbines, respectively.

2) Physical Twin Model for V2G: There is an obvious impact on the V2G-CPS by integrating V2G module into the system network through household devices or other electronic interfaces. This is due to the fact that the output of V2G is not regular and uninterrupted which will introduce unexpected harmonics into the power profile of V2G-CPS. Therefore, there is a need for a reliable V2G model for control and operation that can improve the stability and reliability of the V2G-CPS. To ease of understanding the V2G model, we assume that each bus has installed a V2G aggregator, namely V2G node, and the number of EVs at each bus i is m_i, that is $M = \{m_i | i \in N\}$. According to [38], the model of V2G node in each bus can be expressed as:

$$P_i^o(t) + \sum_{j=1}^{m_i} \eta_j^{\text{ev}} P_j^{\text{ev}}(t) = P_i^D(t), \ t = 1, \cdots, T, \tag{17}$$

where P_i^o and P_j^{ev} are the base load excluded EV demand and the power demand of the j^{th} EV in the i^{th} bus, respectively. η_j^{ev} represents the charger efficiency of the j^{th} EV depended on charging or discharging modes and T is the total number of time slots. It can be observed from (17) that the V2G mechanism plays an important role in helping stabilize the V2G-CPS. In particular, the EVs are able to supply and absorb the shortage and excess of power through V2G mode in the emergency situation as CCAs and the corresponding mitigation processes.

Furthermore, there are some essential constraints for the operation of V2G, followed in [38].

$$\left|P_j^{\text{ev}}(t)\right| \leq P_{j,\max}^{\text{ev}}, t = T_j^c \cdots T_j^d, \forall j. \tag{18}$$

$$SOC_{j,\min} \leq SOC_j(t) \leq SOC_{j,\max}, t = T_j^c \cdots T_j^d, \times \forall j. \tag{19}$$

$$\eta_j^{\text{ev}} = \begin{cases} \eta_j^{\text{c}}, & P_j^{\text{ev}}(t) \geq 0 \\ \eta_j^{\text{d}}, & P_j^{\text{ev}}(t) < 0. \end{cases} \tag{20}$$

$$\text{SOCj}(t) = \begin{cases} \frac{w_i^c + \eta_j^{\text{ev}} P_j^{\text{ev}}(t)\Delta T}{c_j}, & t = T_j^c \\ SOC_j(t) + \frac{\eta_j^{\text{ev}} P_j^{\text{ev}}(t)\Delta T}{c_j}, & t = T_j^c \\ & +1 \cdots T_j^d \end{cases} \tag{21}$$

$$\sum_{t=T_j^c}^{T_j^d} [\eta_j^{\text{ev}} P_j^{\text{ev}}(t)\, \Delta T] = w_j^d - w_j^c, \ \forall j. \tag{22}$$

Here, ΔT is the interval of a time slot, T_j^c and T_j^d are the time slots of V2G connected and disconnected to V2G-CPSs, respectively. η_j^{c} and η_j^{d} show the efficiency of charging and discharging for j^{th} EV, respectively. w_j^c is the initial power capacity when j^{th} EV is connected to the system network, and w_j^d is the end power capacity when j^{th} EV is disconnected. Finally, $SOC_j(t)$ indicates the state of charge of j^{th} EV at the time slot t.

C. Threat Model

There are two representative CCAs studied in this paper, which are false data injection attacks (FDIA) and switching attacks (SA). In particular, we study the impact of FDIAs on the malicious V2G nodes and the impact of SAs on the circuit breakers of generators. In most of the CCA studies, there is a common implicit assumption that the adversary would try to tamper with full network parameters via CCAs. However, in realistic scenarios, the adversary has limited resources and information about the entire network, thus limiting the attack range. Consequently, before describing the CCA models studied in this paper, certain assumptions are made from the attacker's perspective:

- The adversary does not have the ability to fully access all points connected in the V2G-CPSs.
- The adversary has limited resources to launch CCAs. In the other words, the attackers will target critical points closely related to the generator circuit breakers.
- The adversary will tamper with the information of the sensor connected to the generator circuit breakers and initiate FDIA in the communication channel connecting the sensors that transmit information to the DT to update itself.
- The adversary can inject malicious V2G nodes by altering the amount of EV connected with the network to corrupt the system states.
- The adversary will only tamper with the voltage V and phase angle θ state parameters of the attacked breakers only.

In the V2G-CPS, the magnitude and phase angles of voltage at each bus are considered primary state parameters. These state variables x are expressed as follows;

$$x = [|V_1|, \ldots, |V_N|, \theta_2, \cdots, \theta_N]^T. \tag{23}$$

The measurement vector mv in state estimation usually includes different parameters, such as; voltage and current measurement values from PMUs, power flows related information, and power injection data from V2G and smart meters [39]. For most cases, the most significant normalized residuals-based state estimation is adopted for bad data detection in network parameters, which occurs due to cyberattacks and measurements devices errors [40]. The residual vector Res calculated through the largest normalized residuals-based

method can be expressed as;

$$\text{Res}^n = \frac{|Res|}{\sqrt{\text{diag}(SR)}}. \tag{24}$$

where, $Res = mv - h(x)$, in which $h(x)$ stands for measurement function, while S represents the matrix for sensitivity measurements, that is $S = I - H(H^T W H)^{-1} H^T W$. The H and W denote the Jacobian measurement matrix and weighted matrix for measurements respectively. These were all extensively addressed in our previous work [41].

The main objective of FDIAs is to dodge the system operator so that the operator considers the attack vector x_a as the actually estimated state vector x, such as $x_a = x + c$, where c stands for deviation in state parameters x under CCAs [7], [42]. Moreover, the attacker can tamper with the measurement vectors by injecting false measurements vector a, i.e., the adversary can convey false information about V2G nodes (either by adding or removing V2G nodes), which enabled them to initiate FDIAs and is done by tampering with a. This makes the new mv as $mv_a = mv + a$ and by including the residuals, the new mv_a becomes;

$$\text{Res}_a = mv_a - h(x + c) = mv + a - h(x + c). \tag{25}$$

The attack vector in FDIAs will be demonstrated as;

$$a = h(x + c) - h(x). \tag{26}$$

It has been observed that this type of FDIAs attack vector can easily bypass the traditional residual-based bad data detection mechanism used for attack detection [40], [42].

Another type of CCA considered in this paper is the SA. The SAs alter the status of circuit breakers on the generators to make V2G-CPS unstable [43]. For instance, to balance the supply and demand, the power flow will re-dispatch which may cause the overloading flow on some transmission lines leading to $N - K$ contingencies. Moreover, a load curtailment mechanism may be performed to further stabilize the system resulting in an increase of marginal cost and user inconvenience. We assume that the adversary can control the connection of the generator on the $i-th$ bus by manipulating the status of circuit breaker σ_i. The generator on $i - th$ bus is connected with the network if $\sigma_i = 1$, and is disconnected with the network if $\sigma_i = 0$ and for the $\sigma_i = -1$ the power will be absorbed from the generator bus.

The different σ_i affecting the generator performance is expressed as [44];

$$M_i w_i = \begin{cases} -D_i w_i + P_{\text{a,i}}, & \sigma_i = 0 \\ -D_i w_i + P_{\text{a,i}} + U_i, & \sigma_i = 1 \\ -D_i w_i + P_{\text{a,i}} - U_i, & \sigma_i = -1 \end{cases} \tag{27}$$

where, σ_i and $P_{\text{a,i}}$ stand for circuit breakers' states and generator accelerating power, respectively, while D_i represents the coefficient of the generator damping and M_i shows the generator inertia. The generator rotor frequency is represented by w_i.

During CCAs, the adversary will first transmit false information about the V2G nodes available at the current time by tampering with the measurement vectors, which will affect the power availability at the current time. At the same time, the attacker will disconnect one of the generators from the network by changing the circuit breaker state. The control operator will observe the power deficiency in the network and will try to meet the demand by extracting the power from the available V2G nodes and WTs. However, as the power availability of V2G nodes is also tampered with by FDIA, the demand requirements will not be fulfilled by the reserve generation. As a consequence, the excessive power demands will increase the stress on the survival generators, and the circuit breakers which may trip successively will result in a network blackout. Besides SAs and FDIAs, there are other types of threats that will effect the operation of smart grids. Some of the potential threats to smart grids are summarized in Table.I [45], [46].

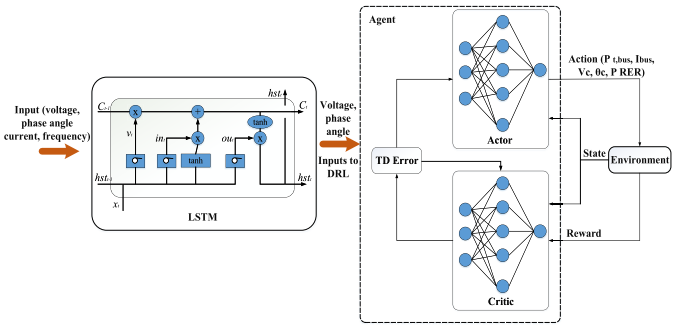


Fig. 2. Framework of LSTM-DRL algorithm. The left of figure represents LSTM block responsible to estimate actual state parameters from the inputted DT data. The right of figure represents DRL block to decide necessary control and mitigation actions from the output of LSTM block.

IV. Proposed Algorithm

In this section, the smart DT-enabled security framework for the detection and mitigation of CCAs is presented. In particular, the mathematical model of the proposed LSTM-DRL algorithm is discussed. The operation of the LSTM-DRL algorithm is shown in Fig. 2. The LSTM block is to estimate actual state parameters by using the DT data of V2G-CPS, in which, the DT data may be corrupted by CCAs including FDIA and SA. The state parameters estimated by LSTM will be further fed to the DRL block as the input. If there is any attack being detected, the DRL will decide on necessary control actions as the output to mitigate the attack impact ensuring the V2G-CPS stability. The procedure of the proposed security framework is summarized as follows.

1) The smart DT framework continuously monitors the security constraints of (1), (2), and (3), and is activated when observing the violation of security constraints, or any unexpected power variations.
2) The LSTM block is activated to estimate state parameters by using the doubted DT data.
3) Based on the state parameters estimated by The LSTM block, the DRL block is activated to detect attacks, identify attack types, and provide optimal control action to mitigate the attack impact.

A. LSTM for State Estimation

This study employs an LSTM algorithm to estimate the actual state parameters for the smart DT of V2G-CPS in

TABLE I
COMPARISON OF COMMON THREAT METHOD IN SMART GRID

Attack type	Attack description	Area compromise
Man-in-the-middle attack	Packet eavesdropping between users and utilities provider	Control center and wifi network
Denial of Service attack	Interrupting the data flow among smart devices	Smart meters and network
Privacy threats	Attackers get an access to user confidential information like passwords	Outage management system
False control commands	Attackers sent false commands to smart meters to reduce the consumption	Smart meters
Security threats	Attackers can tempered the information transferred among different smart grids devices	Remote terminal unites and PMUs

the presence of CCAs. LSTM is a modified recurrent neural network (RNN). It is able to learn from time series data and the vanishing gradient issue in RNN is resolved using LSTM, which is why LSTM is used in this paper to predict state variables [47]. The LSTM utilizes the DT data, such as current, voltage, frequency, and statistical data, to predict the state variables. The DT data, which varies dynamically with time, is collected by the internet of things (IoT) sensor devices installed in the V2G-CPS. LSTM gives a good approximation of state variables because of its ability to handle time series and an immense amount of data. In this paper, we consider the voltage magnitude $|V|$ and phase angles θ of each bus as the state variables, and refer to the estimated state as the output of the LSTM algorithm. The data of current, voltage, real and reactive power generated with different load patterns are to be referred as the input of the LSTM algorithm. Once LSTM is trained offline, the refine estimated states are then utilized for online training of the DRL in the smart DT replica of V2G-CPSs. This reduces the convergence time of the DRL algorithm and increases its accuracy. The proposed LSTM consists of the following steps for the state estimation [22].

Estimation Step-1: In this step, the LSTM decides what necessary information is needed and what needs to be discarded from memory cells, which is why this step is called forget step. The function v_t computed at the forget step is:

$$v_t = \sigma(Wei_v.[hst_{\text{t-1}}, x_t] + bia_v). \tag{28}$$

where v_t is the forget function, which looks at the previously hidden state $hst_{\text{t-1}}$ and current input x_t to decide whether to keep or discard the stored data.

Estimation Step-2: In this step, the cell updates itself with new data that it receives at each time step. The sigmoid layer σ in a single LSTM cell will decide what new values to be added, then the new state $\tilde{C}_t$ that will be added to the old state of the cell $C_{\text{t-1}}$ is created by tanh activation function, which only depends upon current input x_t and hidden state $hst_{\text{t-1}}$. i.e.,

$$in_t = \sigma(Wei_{\text{in}}.[hst_{\text{t-1}}, x_t] + bia_{\text{in}}), \tag{29}$$

$$\tilde{C}_t = \tanh(Wei_c.[hst_{\text{t-1}}, x_t] + bia_c), \tag{30}$$

$$C_t = v_t * C_{\text{t-1}} + in_t * \tilde{C}_t. \tag{31}$$

Algorithm 1 V2G-CPS State Variable Estimation by LSTM for DRL

Input 1: Random initialization hs_t, $weights$ and C_t
Input 2: Voltage, current, real and reactive power
Input 3: Specified convergence tolerance ϵ, Er, RL, TD and ES
Output : Estimated voltage V and phase angle θ states
while $(ES > \epsilon)$ **do**
  Prediction of V and θ ;
  for *(TD presented to network)* **do**
    The three prediction steps are performed using (28), (29), (30), (31), (32), (33);
    Compute Er;
    if $(Er > \epsilon)$ **then**
      Update weights by back propagation through gradient descent algorithm;
    else
      Ouput the, V and θ;
    end
    If error between actual and estimates is greater, then send variations V, and θ as an input to Algorithm 1 for further tuning;
  end
end

Estimation Step-3: The filtered output is displayed. At first, $hst_{\text{t-1}}$ and x_t are passed through the sigmoid layer and current cell state C_t is passed through tanh to finally compute the final output hst_t of a single LSTM cell at the current time instant as follows,

$$ou_t = \sigma(Wei_{\text{ou}}.[hst_{\text{t-1}}, x_t] + bia_{\text{ou}}), \tag{32}$$

$$hst_t = ou_t * tanh(C_t), \tag{33}$$

$$\text{Er} = \frac{1}{2}\sum_{1}^{n}(real - hst_t)^2. \tag{34}$$

where, Wei_v, Wei_{in}, Wei_{c}, Wei_{ou}, bia_{v} bia_{in}, bia_{c}, bia_{ou} are the weights and biases of the neural network layer. While the index v, in, c, and ou present the forget function, inputs, cell state, and outputs, respectively. The mean square error Er is computed using (34). At the start of the algorithm, the vectors hst_t and C_t are initialized to zero. Afterward, the weights

of the LSTM network are updated using a gradient descent algorithm that error is propagated backward through back-propagation through the time algorithm [22]. The proposed framework is presented in Algorithm 1, where TD, RL, and ES stand for the training data, learning rate, and estimated states, respectively.

B. Deep Reinforcement Learning

This paper adopts a deep deterministic policy gradient (DDPG) to detect and mitigate CCAs using the smart DT for V2G-CPSs. The DDPG can detect the variation in state variables in a short time, which decreases the time to provide countermeasures [48]. This reduces the chances of $N-K$ contingencies in the proposed smart DT for V2G-CPSs due to its inability to adopt the model-free approach and to model the dynamic state variables from the power system environment. As mentioned earlier, we consider the WTs and V2G mode as the reserve energy sources for the V2G-CPS. However, the adversary can tamper with the information about the available V2G devices connected at the current time. This will cause deviations in power availability. For this purpose, the agent in DRL observes the system state of V2G-CPS and decides either to reroute the power from the RERs devices or do nothing in case of false attacks.

The energy accommodation in V2G-CPSs can be formulated using the Markov decision process (MDP), where different constraints due to RERs and CCAs are considered. The MDP model is defined as a set of 5-tuple having different model parameters such as (St, Ac, Pr, Re, γ). Here, St denotes the state space available for an agent, Ac is the set of possible actions, Pr is the transition probability between states, Re is the reward for a state action pair, and γ is the discount factor. At a certain time t, the state for the agent in the environment are $St_t = (P_t, I_k, V', \theta')$. Based on the filtered estimated states V and θ obtain through LSTM and power P_t and current I_k that are taken in real-time, the agent takes an action to identify and mitigate CCAs in smart DT for V2G-CPSs. The action vector $Ac = (P_{\text{t,bus}}, I_{\text{bus}}, V_c, \theta_c, P_{\text{RERs}})$, where V_c and θ_c stand for estimated correct states that are tampered with by the adversary under FDIA or SA. If the tampered states show the behavior of SA, that is by monitoring abnormal fluctuations in power and current level on attack buses, then, it is mitigated by rerouting power from P_{RERs}. The proposed algorithm detects the nature of the attack from states available in action space and mitigates it by rerouting the power from RERs. The state transition from St_t to $St_{\text{t+1}}$ can be represented as,

$$St_{\text{t+1}} = f(St_t, Ac_t). \tag{35}$$

The reward for a state action pair is,

$$Re = V + \theta - V' - \theta'. \tag{36}$$

The MDP problem is solved using reinforcement learning, and the Ac under St is evaluated using Q function $Q(St, Ac)$. The expected reward associated with the state action pair under policy U can be represented as,

$$Q^U(St, Ac) = E(\sum_{i=0}^{n} \gamma^i Re_{\text{t+i}} | St_t = St, Ac_t = Ac). \tag{37}$$

The main aim of reinforcement learning is to find an optimal policy that maximizes the overall rewards accumulated over time, which is,

$$Q^{\text{U}*} = \max_U Q^U(St, Ac). \tag{38}$$

By finding the optimal policy, the optimal action for the given state can be founded as,

$$Ac^* = arg \max_U Q^*(St, Ac). \tag{39}$$

The amount of state information collected through sensors in the V2G-CPS, including those estimated by the LSTM, is massive, and therefore, the set of state space is enormous. Moreover, the dimension of the V2G-CPSs increases as the system under consideration grows. As a result, the actions that are needed for identifying the CCAs and mitigating them faster cannot be achieved, despite the filtered states obtained through LSTM provided to the reinforcement learning algorithm. Reaching an optimal policy through reinforcement learning is not feasible, and algorithm convergence takes more time.

In this regard, we adopted an actor-critic-based DRL approach for finding optimal policies for state-action pairs. The proposed LSTM-DRL techniques for CCAs detection and mitigation work even for dynamic and extensive networks, and the agent can provide suitable action with a small delay. The actor-critic comprises fully connected neural networks in the LSTM-DRL algorithm, where the actor-network is used to learn the optimal action following the optimal policy $Ac_t = U(St'_t | Wi^U)$, while the critic network is used to find optimal Q values for state and action pair $Q(St'_t, Ac_t | Wi^Q)$. Here, Wi^U and Wi^Q stand for the weights associated with actor and critic networks, respectively, while St'_t stands for the next expected state from the environment. The agent in LSTM-DRL learns through exploration and exploitation. After an agent takes action, some award Re_t is given to the respective action, and the agent's experience is stored in the memory replay buffer, which is,

$$Rm = \{St'_t, Ac_t, Re_t, St'_{\text{t+1}}\}. \tag{40}$$

For learning purposes, a mini-batch from the replay buffer is randomly selected to train the network. Moreover, the random selection of batch from the data available in the replay memory enhances the generalization capability of the algorithm. The overall objective function of the algorithm is,

$$RE_t = \sum_{t=0}^{n} \gamma^t Re_t, \tag{41}$$

$$J(Wi^U) = E_{\text{Wi}^{\text{U}}}(RE_t), \tag{42}$$

$$\frac{\partial J(Wi^U)}{\partial (Wi^U)} = E \frac{\partial Q(St, Ac | Wi^Q)}{\partial (Wi^Q)}, \tag{43}$$

$$= E[\nabla_{\text{Ac}} Q(St, Ac | Wi^Q) | St = St_j,$$

$$Ac = U(St_j) \nabla_{\text{Wi}^{\text{U}}} U(St | Wi^U)]. \tag{44}$$

The loss function for the critic network, through which the weights for the respective network are updated in the training

phase is computed in (45),

$$Ls = \sum_{j=1}^{n} [Re'_j - Q(St_j, Ac_j | Wi^{Q})]^2, \tag{45}$$

$$Re'_j = Re_j + \gamma Q'(St_{j+1}, U'(St_{j+1} | Wi^{U'}) | Wi^{Q'}). \tag{46}$$

Once the critic network's weights are updated, the actor-network updates itself using the following equation,

$$\nabla_{\mathrm{Wi^U}} J = \sum_{j=1}^{n} [\nabla_{\mathrm{Ac}} Q(St, Ac | Wi^{Q}) | St = St_j,$$
$$Ac = U(St_j) \nabla_{\mathrm{Wi^U}} U(St | Wi^{U}) | St_j]. \tag{47}$$

The above equation has two parts; the first half is used to select the action yielding the highest reward, and the second half is used to find the optimal policy having the highest reward by applying the gradient ascent techniques following the objective function J, as,

$$Wi^{U} \longleftarrow Wi^{U} + \partial \nabla_{\mathrm{Wi^U}} J. \tag{48}$$

After training the actor and critic networks with a mini-batch, unless the desired accuracy is achieved, the network updates itself using (49) and (50) iteratively as,

$$Wi^{U'} \longleftarrow \tau Wi^{U} + (1 - \tau) Wi^{U'}, \tag{49}$$

$$Wi^{Q'} \longleftarrow \tau Wi^{Q} + (1 - \tau) Wi^{Q'}. \tag{50}$$

The LSTM-DRL algorithm for detecting and mitigating CCAs in V2G-CPSs is summarized in Algorithm 2.

Algorithm 2 CCAs Detection and Mitigation in V2GCPSs Through Smart DT Replica Having LSTM-DRL

Input 1: Random initialization actor and critic networks with Wi^{U} and Wi^{Q}
Input 2: Initialize the buffer memory for the specific set of 5-tuples
Input 3: Expected estimated states V and θ obtained through LSTM are stored in St' vector
Output : New states after CCA is detected and mitigated
while $(Ls > \epsilon)$ **do**
  The agent explores the environment based on different states such as P_t, I_k, V, θ;
  for $(t{=}0$ *to* $t{=}n)$ **do**
    Agent perform action $Ac_t = U(St_t' | Wi^{U})$ and gets Re_t to the action performed and gives new St'_{t+1} ;
    Store $Rm = \{St_t', Ac_t, Re_t, St'_{t+1}\}$ in replay memory buffer;
    if $(Rm > mini - batch)$ **then**
      Get randoms tuples sample from Rm;
      Compute $Re'_j = Re_j + \gamma Q'(St_{j+1}, U'(St_{j+1} | Wi^{U'}) | Wi^{Q'})$;
      Compute Ls from (45);
      Actor and Critic networks are updated using (47), (49), and (50);
    end
    After n episodic tasks in the actor-critic network
    $Wi^{U'} \longleftarrow \tau Wi^{U} + (1 - \tau) Wi^{U'}$
    $Wi^{Q'} \longleftarrow \tau Wi^{Q} + (1 - \tau) Wi^{Q'}$
    if $(V, \theta > actual || P_t, I_t > P_{limit}, I_{limit})$ **then**
      CCA is detected. The agent performs an action $Ac = (P_{\mathrm{t,bus}}, I_{\mathrm{bus}}, V_c, \theta_c, P_{\mathrm{RERs}})$
    end
  end
  The updated Ls, states, and network parameters are sent as input to Algorithm 2 if the wrong action is performed and an attack is not detected for further training.
end

V. Results and Discussion

To demonstrate the effectiveness and practicality of the proposed smart DT framework, we consider a V2G-CPS, based on a modified IEEE 30-bus system with WTs and V2G nodes, for case studies. The network configuration of the V2G-CPS is shown in Fig. 3, in which, the WTs and V2G nodes are connected at buses 7, 8, 9, 10, 11, 12, 20, 21, 22, and 23. The DT of V2G-CPS is built in MATLAB with Python based on the physical twin model described in the Section. III. The DT model is used to generate the data set by emulating multiple operation conditions of V2G-CPS with and without CCAs. The data set is then subdivided to train and test the LSTM-DRL algorithm for CCA detection and mitigation. The experiments were performed on a PC with specification of 8-core i5 CPU and 16 GB memory. An actor-critic network comprised of four-layer neural networks having 32 neurons in each hidden layer and Tanh as an activation function is used in DRL. We chose to use an Adam optimizer, a learning rate of 0.001, a batch size of 32, and total of 5,000 episodes for training and testing and summarised in Table. II.

TABLE II
Critical Parameters of DRL Algorithm

Parameters	30 bus
Actor network hidden layers	[32,32]
Policy network hidden layers	[32,32]
Optimizer	Adam
Learning rate	0.001
Bath size	32
Episodes	5000

A. FDIA Detection in V2G-CPSs Using Smart DT Based on LSTM-DRL Algorithm

In this case study, we assume that an intruder launches FDIAs to disrupt the state information of V2G-CPS through malicious V2G nodes. In other words, the adversary attempts to inject false information on the power availability of V2G nodes at targeted buses to deviate the estimated state parameters from the actual states. Specifically, the exact power availabilities of V2G nodes at buses 7, 8, 9, 10, 11, 12, 20,

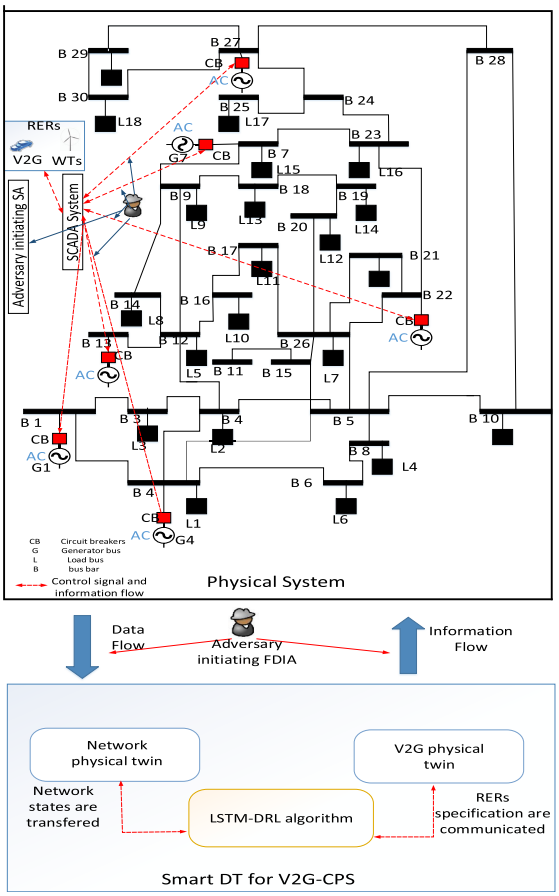
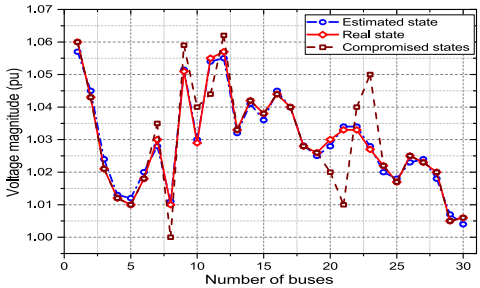
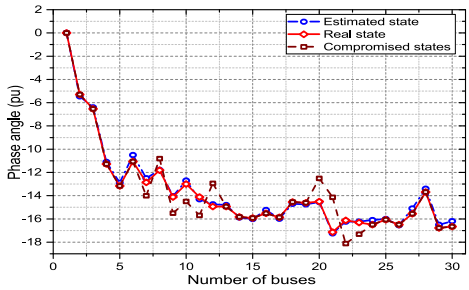


Fig. 3. Structure of smart DT framework for V2G-CPS based on modified IEEE 30 bus system. The proposed LSTM-DRL algorithm is built in smart DT framework. The WTs and V2G nodes are connected at buses 7, 8, 9, 10, 11, 12, 20, 21, 22, and 23.



(a) Estimated voltage



(b) Estimated phase angle

Fig. 4. FDIA detection using LSTM-DRL based smart DT replica for V2G-CPSs under malicious V2G nodes injection.

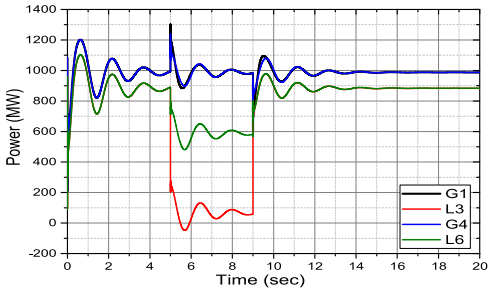


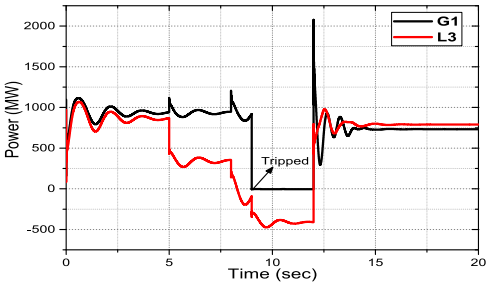
Fig. 5. Normal and full load operation of the power system network.

21, 22, and 23 are tampered with by FDIAs. However, the proposed LSTM-DRL algorithm is able to estimate the actual state parameters, $|V|$, and θ in the presence of malicious V2G nodes, as shown in Fig.4(a) and Fig.4(b), respectively. The deviation of actual, estimated, and compromised states can be observed in Fig. 4. It can be seen that the states estimated by the proposed algorithm are close to the real states in the presence of FDIAs. As a result, we demonstrate that the proposed LSTM-DRL algorithm has the ability to eliminate the FDIA impact on the state estimation to improve the system situation awareness for the reliable and secure operation of V2G-CPS. Furthermore, to show the robustness of the proposed LSTM-DRL algorithm, it is tested against two types of CCAs, which are sequential SAs, and SAs with FDIAs. Moreover, the corresponding impact of CCAs on the V2G-CPS, which will be in form of $N-K$ contingency is analysed.

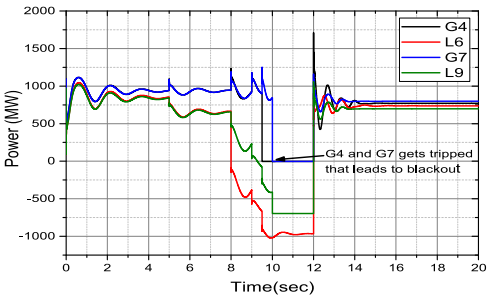
B. Impact Analysis of CCAs on V2G-CPSs Under Normal Operation

In this subsection, the V2G-CPS is firstly operated under normal states, and then we show that the operation of V2G-CPS in the presence of SAs will experience $N-K$ contingencies if those SAs are not tackled in time. In particular, we show that the adversary only launches a SA on the circuit breakers of the certain generator that ultimately un-stabilizes the whole system. The system under normal state and full load operation can be observed from Fig 5, where G1 and G4 are generation buses and L3 and L6 correspond to load buses. Please note that only these buses are being presented because we consider these generation and load buses as the biggest producers and consumers in the V2G-CPS. The normal and full-load operation of the system is shown in Fig.5, where actual generation $A_c G(t)$ is 1000MW and actual demand $A_c D(t)$ is 100MW. The bus system has a total generation of 3000MW and a total load of 300MW distributed among different load points. During a full load operation, the load of 3000MW falls on the network and can be visualized in Fig.5 from 5 sec to 9 sec.

The system under SAs can be observed in Fig. 6 when the network is operated under full load conditions. That is, the additional demand of 1000MW falls on the network at 5 sec; however, the system is still stable. But when additional demand of 1700MW falls on the network at 8 sec, which makes a total demand of 3000MW and the system is now operated under full load condition. However, at the same time, the adversary

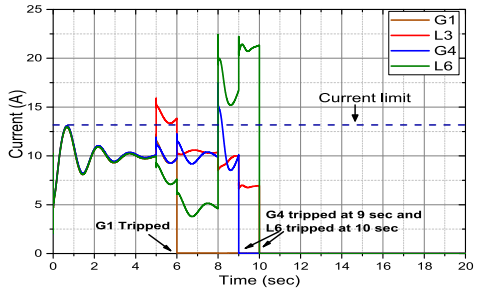


(a) SA on first generator

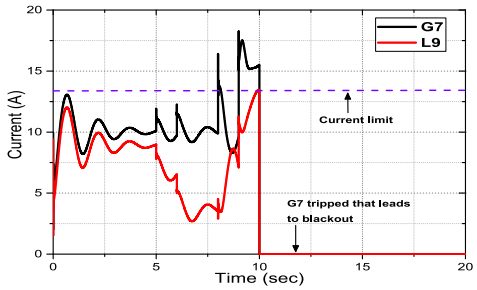


(b) SA on third and fourth generator

Fig. 6. The $N-K$ contingencies due to SA that leads to blackout.



(a) Current profile at G1, G4, L3 and L6 under FDI-CCAs.



(b) Current profile at G7 and L9 under FDIAs&SAs.

Fig. 7. Current profile at different buses under FDIAs and SAs.

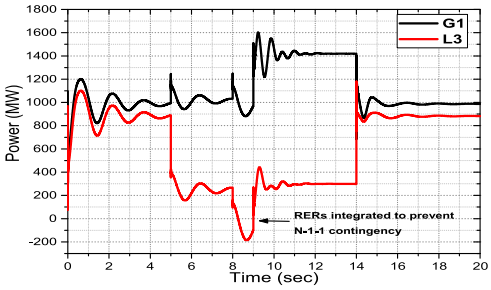
launches an SA at a circuit breaker installed on the bus that connects G1 to the V2G-CPSs at 9 sec and disconnects the major source of power from the network as shown in Fig.6(a). As G1 gets tripped, all the demand is distributed among other buses. Now, the generation capacity falls by 1000MW, and $A_c G(t)$ will now be 2000MW. In addition, the adversary does not stop at that, and trips G4 using SA at 9.5 sec, as shown in Fig.6(b), however, as the demand is much more than the actual generation and to save the generator from getting damaged, the protective system gets activated and trips G7 at 10 sec, and all other generation sources afterward. This ultimately causes $N-K$ contingencies that lead to blackout between 9 sec and 12 sec, as shown in Fig.6. It is depicted in Fig. 6 that the adversary maintained the SA for almost 3 sec, but when the SA is removed, the system stabilizes within 3 sec, but the blackout is still present from 9 sec to 12 sec. The variation in power profile after 12 sec is all due to unbalanced demand distribution.

The current profile at respective buses during FDIAs and under SAs can be observed in Fig. 7. The maximum current limits for the transmission lines are 13 A. However, the adversary communicates false information about the network's current thresholds overshoot, that is normal current values are communicated to the operator that prevents the operator from taking appropriate action, and at the same time SAs are initiated due to which G1 gets tripped at 6 sec, as shown in Fig.7(a). In addition to the current thresholds, the adversary also tampered with the power availability due to V2G device's connectivity to the system. As a result, the operator is not able to balance the demand requirements and current profile overshoots due to which G4 trips at 9 sec and G7 at 10 sec, as shown in Fig.7(a) and Fig.7(b), respectively.

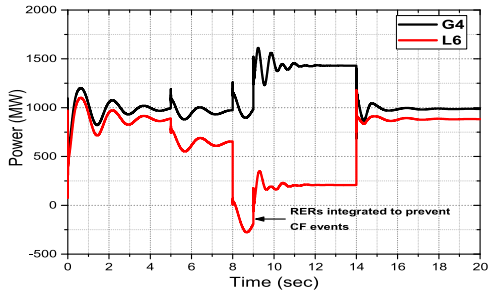
C. Mitigating $N-K$ Contingencies Under CCAs Using LSTM-DRL Based Smart DT for V2G-CPSs

This study adopts a sophisticated LSTM-DRL to mitigate CCAs leading to $N-K$ contingencies. The system operates under the proposed LSTM-DRL-based smart DT for V2G-CPSs during $N-K$ contingencies, which are due to CCAs and high load, as shown in Fig. 8. As mentioned earlier, a SAs happens at 8 sec, due to which G1 trips. This makes the actual demand more than the actual generation and variation in power profile is observed in Fig.6. However, the adversary further launches another SA to trip G2 and the period of attack will continue till a blackout occurs. These actual demand variations ultimately induce $P_{\text{need}}(t)$ in the power system. The agent in LSTM-DRL algorithm monitors these variations in the state parameters. As a result, the agent takes the corresponding actions to mitigate SAs by routing the reserve from WTs and V2G devices to make up the extra power needed by the V2G-CPSs, and these mitigating actions satisfy the network constraints in check within 3 sec, as shown in Fig. 8. The power from RERs will provide the backup unless the CCA is not fully taken care of. Furthermore, it is observed from Fig. 8 that V2G-CPS restores to its original state when the SAs are countered at 14 sec.

To demonstrate how effectively the proposed LSTM-DRL algorithm mitigates the $N-K$ contingencies, we compare the proposed algorithm with the algorithm in [25], which uses a MAS to mitigate the $N-K$ contingencies. The algorithm proposed in [25] provided several combinations for individual lines to prevent $N-K$ contingencies, but it took time to mitigate them, as shown in Fig. 9(a). When two transmission lines get tripped due to faults, the current profile on the other lines exceeds their current-carrying limit. The algorithm in [25]

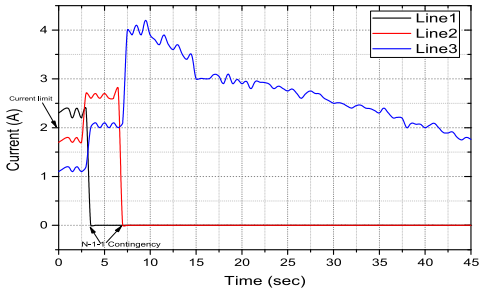


(a) Power profile during $N-K$ contingency due to SA.

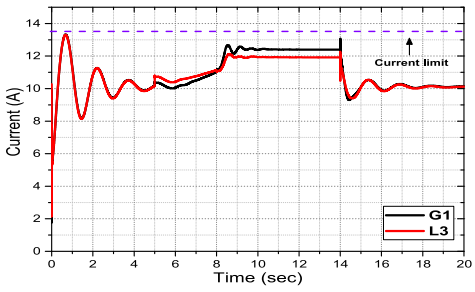


(b) Power profile on L6 during $N-K$ contingency under SA.

Fig. 8. $N-K$ contingency mitigation under proposed LSTM-DRL algorithm.



(a) Mitigation of $N-K$ contingency by MAS in [25].



(b) Detection of CCAs and mitigation of $N-K$ contingency by the LSTM-DRL algorithm.

Fig. 9. Comparison between the proposed LSTM-DRL algorithm and MAS [25].

makes the current profile on an overloaded line return to its original state, but it takes 30 seconds to do so. Furthermore, the algorithm did not provide any countermeasures for when CCAs fall on the network. In contrast, the proposed LSTM-DRL algorithm keeps the current profiles within their threshold limits. At 5 seconds, CCA happens in the network, due to which G1 gets tripped and the load distribution is disturbed. As a result, $N-K$ contingency occurs in the V2G-CPS as shown in Fig. 9(a). However, with the proposed LSTM-DRL algorithm, when G1 gets tripped due to CCA, at the same time, RERs are integrated due to action taken by the agent to provide extra power, and the rise in G1 power is also observed. At 8 seconds, the current profile of G1 and L3 are almost identical. From 8 seconds to 14 seconds, the current profile on G1 further increases, and excess power is transferred to L3 to keep the current profile on L3 within the threshold limit as shown in Fig. 9(b). Thus the proposed algorithm stabilizes a system subject to CCAs within 4 seconds, as shown in Fig. 9. It was observed from Fig. 8 and 9 that the proposed algorithm provides a timely solution, even in the event of a CCA.

VI. Conclusion

In this paper, a comprehensive smart DT-enabled security framework for V2G-CPSs has been presented. The LSTM-DRL techniques have been incorporated into the proposed framework to detect and mitigate CCAs in V2G-CPSs. In presence of CCAs, the actual system states have been estimated through the LSTM algorithm, which is further fed into the DRL network to identify the nature of CCAs. Moreover, the proposed LSTM-DRL method has the ability to identify malicious V2G nodes and recover the actual power availability of V2G devices connected. In the case studies, various CCA cases, including SA, FDIA, and combined were considered to demonstrate the effectiveness and practicality of the proposed framework. The results show that even a simple CCA is able to cause $N-K$ contingencies if it is not tackled in time, and consequently, may lead to a potential blackout in the network. The proposed smart DT-based framework can detect the CCAs in time, and mitigate them by rerouting the power from WTs and V2G nodes connected to the V2G-CPSs while keeping the network constraints in check. In future, we will be extending this work to more extensive network i.e, IEEE 118 or 300 bus system and will also implement it on real network to show the generalization capability of proposed algorithm.

References

[1] Y. Liu, H. Xin, Z. Qu, and D. Gan, "An attack-resilient cooperative control strategy of multiple distributed generators in distribution networks," *IEEE Trans. Smart Grid*, vol. 7, no. 6, pp. 2923–2932, Nov. 2016.

[2] W.-T. Li, C.-K. Wen, J.-C. Chen, K.-K. Wong, J.-H. Teng, and C. Yuen, "Location identification of power line outages using PMU measurements with bad data," *IEEE Trans. Power Syst.*, vol. 31, no. 5, pp. 3624–3635, Sep. 2016.

[3] C. Zhao, J. He, P. Cheng, and J. Chen, "Consensus-based energy management in smart grid with transmission losses and directed communication," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2049–2061, Sep. 2017.

[4] A. A. Babalola, R. Belkacemi, S. Zarrabian, and R. Craven, "Adaptive immune system reinforcement learning-based algorithm for real-time cascading failures prevention," *Eng. Appl. Artif. Intell.*, vol. 57, pp. 118–133, Jan. 2017.

[5] A. Monticelli, "Electric power system state estimation," *Proc. IEEE*, vol. 88, no. 2, pp. 262–282, Feb. 2000.

[6] R. Deng, P. Zhuang, and H. Liang, "False data injection attacks against state estimation in power distribution systems," *IEEE Trans. Smart Grid*, vol. 10, no. 3, pp. 2871–2881, May 2019.

[7] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inf. Syst. Secur.*, vol. 14, no. 1, pp. 1–33, May 2011.

[8] G. Hug and J. A. Giampapa, "Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks," *IEEE Trans. Smart Grid*, vol. 3, no. 3, pp. 1362–1370, Sep. 2012.

[9] R. Deng, G. Xiao, R. Lu, H. Liang, and A. V. Vasilakos, "False data injection on state estimation in power systems—Attacks, impacts, and defense: A survey," *IEEE Trans. Ind. Informat.*, vol. 13, no. 2, pp. 411–423, Apr. 2017.

[10] R. Deng and H. Liang, "False data injection attacks with limited susceptance information and new countermeasures in smart grid," *IEEE Trans. Ind. Informat.*, vol. 15, no. 3, pp. 1619–1628, Mar. 2019.

[11] J. Zhang, Z. Chu, L. Sankar, and O. Kosut, "False data injection attacks on power system state estimation with limited information," in *Proc. IEEE Power Energy Soc. Gen. Meeting (PESGM)*, Jul. 2016, pp. 1–5.

[12] Y. Isozaki et al., "Detection of cyber attacks against voltage control in distribution power grids with PVs," *IEEE Trans. Smart Grid*, vol. 7, no. 4, pp. 1824–1835, Jul. 2016.

[13] A. Saad, S. Faddel, T. Youssef, and O. A. Mohammed, "On the implementation of IoT-based digital twin for networked microgrids resiliency against cyber attacks," *IEEE Trans. Smart Grid*, vol. 11, no. 6, pp. 5138–5150, Nov. 2020.

[14] G. Chaojun, P. Jirutitijaroen, and M. Motani, "Detecting false data injection attacks in AC state estimation," *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2476–2483, Sep. 2015.

[15] A. Chattopadhyay, A. Ukil, D. Jap, and S. Bhasin, "Toward threat of implementation attacks on substation security: Case study on fault detection and isolation," *IEEE Trans. Ind. Informat.*, vol. 14, no. 6, pp. 2442–2451, Jun. 2018.

[16] S. Chakrabarty and B. Sikdar, "Detection of hidden transformer tap change command attacks in transmission networks," *IEEE Trans. Smart Grid*, vol. 11, no. 6, pp. 5161–5173, Nov. 2020.

[17] L. Che, X. Liu, Z. Li, and Y. Wen, "False data injection attacks induced sequential outages in power systems," *IEEE Trans. Power Syst.*, vol. 34, no. 2, pp. 1513–1523, Mar. 2019.

[18] T. Aziz, N.-A. Masood, S. R. Deeba, W. Tushar, and C. Yuen, "A methodology to prevent cascading contingencies using BESS in a renewable integrated microgrid," *Int. J. Electr. Power Energy Syst.*, vol. 110, pp. 737–746, Sep. 2019.

[19] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on the smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 645–658, Dec. 2011.

[20] D. B. Rawat and C. Bajracharya, "Detection of false data injection attacks in smart grid communication systems," *IEEE Signal Process. Lett.*, vol. 22, no. 10, pp. 1652–1656, Oct. 2015.

[21] R. Xu, R. Wang, Z. Guan, L. Wu, J. Wu, and X. Du, "Achieving efficient detection against false data injection attacks in smart grid," *IEEE Access*, vol. 5, pp. 13787–13798, 2017.

[22] M. Tariq, M. Ali, F. Naeem, and H. V. Poor, "Vulnerability assessment of 6G-enabled smart grid cyber-physical systems," *IEEE Internet Things J.*, vol. 8, no. 7, pp. 5468–5475, Apr. 2021.

[23] R. J. R. Kumar and B. Sikdar, "Efficient detection of false data injection attacks on AC state estimation in smart grids," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, Oct. 2017, pp. 411–415.

[24] R. Deng, P. Zhuang, and H. Liang, "CCPA: Coordinated cyber-physical attacks and countermeasures in smart grid," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2420–2430, Sep. 2017.

[25] A. A. Babalola, R. Belkacemi, and S. Zarrabian, "Real-time cascading failures prevention for multiple contingencies in smart grids through a multi-agent system," *IEEE Trans. Smart Grid*, vol. 9, no. 1, pp. 373–385, Jan. 2018.

[26] S. Sahoo and S. Mishra, "An adaptive event-triggered communication-based distributed secondary control for DC microgrids," *IEEE Trans. Smart Grid*, vol. 9, no. 6, pp. 6674–6683, Nov. 2018.

[27] M. Rahnamay-Naeini, Z. Wang, N. Ghani, A. Mammoli, and M. M. Hayat, "Stochastic analysis of cascading-failure dynamics in power grids," *IEEE Trans. Power Syst.*, vol. 29, no. 4, pp. 1767–1779, Jul. 2014.

[28] M. B. Mollah et al., "Blockchain for the Internet of Vehicles towards intelligent transportation systems: A survey," *IEEE Internet Things J.*, vol. 8, no. 6, pp. 4157–4185, Mar. 2021.

[29] D. Zhang, L. Liu, and G. Feng, "Consensus of heterogeneous linear multiagent systems subject to aperiodic sampled-data and DoS attack," *IEEE Trans. Cybern.*, vol. 49, no. 4, pp. 1501–1511, Apr. 2019.

[30] L. Meng, T. Dragicevic, J. Roldán-Pérez, J. C. Vasquez, and J. M. Guerrero, "Modeling and sensitivity study of consensus algorithm-based distributed hierarchical control for DC microgrids," *IEEE Trans. Smart Grid*, vol. 7, no. 3, pp. 1504–1515, May 2016.

[31] A. A. Saad, S. Faddel, and O. Mohammed, "A secured distributed control system for future interconnected smart grids," *Appl. Energy*, vol. 243, pp. 57–70, Jun. 2019.

[32] N. M. Dehkordi and S. Z. Moussavi, "Distributed resilient adaptive control of islanded microgrids under sensor/actuator faults," *IEEE Trans. Smart Grid*, vol. 11, no. 3, pp. 2699–2708, May 2020.

[33] S. Abhinav, H. Modares, F. L. Lewis, F. Ferrese, and A. Davoudi, "Synchrony in networked microgrids under attacks," *IEEE Trans. Smart Grid*, vol. 9, no. 6, pp. 6731–6741, Nov. 2018.

[34] A. H. Khan et al., "Blockchain and 6G: The future of secure and ubiquitous communication," *IEEE Wireless Commun.*, vol. 29, no. 1, pp. 194–201, Feb. 2022.

[35] B. Chen, S. Mashayekh, K. L. Butler-Purry, and D. Kundur, "Impact of cyber attacks on transient stability of smart grids with voltage support devices," in *Proc. IEEE Power Energy Soc. Gen. Meeting*, Jul. 2013, pp. 1–5.

[36] M. Blanke, M. Kinnaert, J. Lunze, M. Staroswiecki, and J. Schröder, *Diagnosis and Fault-Tolerant Control*, vol. 2. Berlin, Germany: Springer, 2006.

[37] X. Yu and C. Singh, "A practical approach for integrated power system vulnerability analysis with protection failures," *IEEE Trans. Power Syst.*, vol. 19, no. 4, pp. 1811–1820, Nov. 2004.

[38] C. Liu, K. T. Chau, D. Wu, and S. Gao, "Opportunities and challenges of vehicle-to-home, vehicle-to-vehicle, and vehicle-to-grid technologies," *Proc. IEEE*, vol. 101, no. 11, pp. 2409–2427, Nov. 2013.

[39] Y. Zhang, J. Wang, and Z. Li, "Interval state estimation with uncertainty of distributed generation and line parameters in unbalanced distribution systems," *IEEE Trans. Power Syst.*, vol. 35, no. 1, pp. 762–772, Jan. 2020.

[40] G. Liang, J. Zhao, F. Luo, S. R. Weller, and Z. Y. Dong, "A review of false data injection attacks against modern power systems," *IEEE Trans. Smart Grid*, vol. 8, no. 4, pp. 1630–1638, Jul. 2017.

[41] 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.*, vol. 29, no. 1, pp. 156–165, Jan. 2021.

[42] Y. Zhang, J. Wang, and B. Chen, "Detecting false data injection attacks in smart grids: A semi-supervised deep learning approach," *IEEE Trans. Smart Grid*, vol. 12, no. 1, pp. 623–634, Jan. 2021.

[43] H.-M. Chung, W.-T. Li, C. Yuen, W.-H. Chung, Y. Zhang, and C.-K. Wen, "Local cyber-physical attack for masking line outage and topology attack in smart grid," *IEEE Trans. Smart Grid*, vol. 10, no. 4, pp. 4577–4588, Jul. 2019.

[44] A. K. Farraj and D. Kundur, "On using energy storage systems in switching attacks that destabilize smart grid systems," in *Proc. IEEE Power Energy Soc. Innov. Smart Grid Technol. Conf. (ISGT)*, Feb. 2015, pp. 1–5.

[45] J. Qi, A. Hahn, X. Lu, J. Wang, and C. Liu, "Cybersecurity for distributed energy resources and smart inverters," *IET Cyber-Phys. Syst., Theory Appl.*, vol. 1, no. 1, pp. 28–39, Dec. 2016.

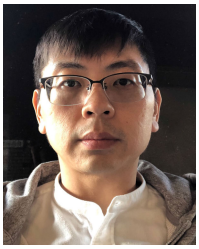
[46] H. Suleiman, I. Alqassem, A. Diabat, E. Arnautovic, and D. Svetinovic, "Integrated smart grid systems security threat model," *Inf. Syst.*, vol. 53, pp. 147–160, Oct. 2015.

[47] N. Sahani, R. Zhu, J.-H. Cho, and C.-C. Liu, "Machine learning-based intrusion detection for smart grid computing: A survey," *ACM Trans. Cyber-Phys. Syst.*, vol. 7, no. 2, pp. 1–31, Apr. 2023.

[48] L. Lin, X. Guan, B. Hu, J. Li, N. Wang, and D. Sun, "Deep reinforcement learning and LSTM for optimal renewable energy accommodation in 5G Internet of Energy with bad data tolerant," *Comput. Commun.*, vol. 156, pp. 46–53, Apr. 2020.

Mansoor Ali (Member, IEEE) received the B.S. degree in electrical engineering from the National University of Computer and Emerging Sciences (NUCES), Pakistan, in 2013, the M.S. degree in electrical engineering from CECOS University, Peshawar, Pakistan, in 2016, and the Ph.D. degree in electrical engineering from NUCES in 2020. Currently, he is a Post-Doctoral Research Fellow with the Electrical Engineering Department, École de Technologie Supérieure (ÉTS), University of Quebec, Montreal, Canada. His current research interests include load forecasting in power system networks, fuzzy control, smart grids, security and privacy for cyber-physical systems, and digital twins.

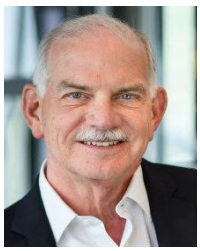
Georges Kaddoum (Senior Member, IEEE) received the bachelor's degree in electrical engineering from École Nationale Supérieure de Techniques Avancées (ENSTA Bretagne), Brest, France, the M.S. degree in telecommunications and signal processing (circuits, systems, and signal processing) from Université de Bretagne Occidentale and Telecom Bretagne (ENSTB), Brest, in 2005, and the Ph.D. degree (Hons.) in signal processing and telecommunications from the National Institute of Applied Sciences (INSA), University of Toulouse, Toulouse, France, in 2009. He is currently a Professor and the Tier 2 Canada Research Chair with École de Technologie Supérieure (ÉTS), Université du Québec, Montreal, Canada, and a Faculty Fellow with the Cyber Security Systems and Applied AI Research Center, Lebanese American University. Since 2010, he has been a scientific consultant in the field of space and wireless telecommunications for several U.S. and Canadian companies. He has published more than 300 journals, conference papers, two chapters in books, and has eight pending patents. His current research interests include wireless communication networks, tactical communications, resource allocations, and security. In 2014, he was awarded the TS Research Chair of Physical-Layer Security for Wireless Networks. He received the best papers awards at the 2014 IEEE International Conference on Wireless and Mobile Computing, Networking, and Communications, with three coauthors, and the 2017 IEEE International Symposium on Personal Indoor and Mobile Radio Communications, with four coauthors. Moreover, he received the IEEE TRANSACTIONS ON COMMUNICATIONS Exemplary Reviewer Award in 2015, 2017, and 2019. In addition, he received the Research Excellence Award of the Université du Québec in 2018. In 2019, he received the Research Excellence Award from ÉTS in recognition of his outstanding research outcomes. Finally, he received the IEEE TCSC Award for Excellence in Scalable Computing in 2022. He is currently serving as an Area Editor for the IEEE TRANSACTIONS ON MACHINE LEARNING IN COMMUNICATIONS AND NETWORKING and an Associate Editor for IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, IEEE TRANSACTIONS ON COMMUNICATIONS, and IEEE COMMUNICATIONS LETTERS.



Wen-Tai Li (Member, IEEE) received the Ph.D. degree from the Institute of Communications Engineering, National Sun Yat-sen University, Taiwan, in 2018. From 2015 to 2018, he was a Research Assistant with the Singapore University of Technology and Design. Since August 2018, he has been with the Engineering Product Development Pillar, Singapore University of Technology and Design, as a Post-Doctoral Research Fellow. His current research interests include smart grids, cyber-physical system security, optimization, estimation, and detection in power systems.

Chau Yuen (Fellow, IEEE) received the B.Eng. and Ph.D. degrees from Nanyang Technological University, Singapore, in 2000 and 2004, respectively. He was a Post-Doctoral Fellow with Lucent Technologies Bell Labs, Murray Hill, in 2005, and a Visiting Assistant Professor with The Hong Kong Polytechnic University in 2008. From 2006 to 2010, he was with the Institute for Infocomm Research, Singapore. From 2010 to 2023, he was with the Engineering Product Development Pillar, Singapore University of Technology and Design. Since 2023, he has been with the School of Electrical and Electronic Engineering, Nanyang Technological University. He has three U.S. patents and published more than 500 research papers in international journals or conferences. He received the IEEE ICC Best Paper Award in 2023, the IEEE Communications Society Fred W. Ellersick Prize in 2023, the IEEE Marconi Prize Paper Award in Wireless Communications in 2021, and EURASIP Best Paper Award for *Journal on Wireless Communications and Networking* in 2021. He was a recipient of the Lee Kuan Yew Gold Medal, the Institution of Electrical Engineers Book Prize, the Institute of Engineering of Singapore Gold Medal, the Merck Sharp and Dohme Gold Medal, and twice a recipient of the Hewlett Packard Prize. He received the IEEE Asia–Pacific Outstanding Young Researcher Award in 2012 and the IEEE VTS Singapore Chapter Outstanding Service Award in 2019. He is a Distinguished Lecturer of the IEEE Vehicular Technology Society, the Top 2% Scientists by Stanford University, and a Highly Cited Researcher by Clarivate Web of Science.

Muhammad Tariq (Senior Member, IEEE) received the M.Sc. degree from Hanyang University, Seoul, South Korea, and the Ph.D. degree from Waseda University, Japan, in 2012. He was the Campus Director of the National University of Computer and Emerging Sciences, Islamabad, Pakistan. His academic journey includes a Fulbright Scholarship sponsored by a Post-Doctoral Fellowship at Princeton University in 2016, under the mentorship of Prof. H. Vincent Poor. He received the HEC Scholarship for the M.Sc. degree and the Japanese Government (MEXT) Scholarship for the Ph.D. degree. He is currently a Professor and the Head of the Department of Electrical Engineering, National University of Computer and Emerging Sciences. His distinguished academic and research contributions are exemplified by his authorship or coauthorship of more than 80 research articles, boasting a cumulative impact factor exceeding 320. His outstanding accomplishments have been acknowledged through numerous awards. As a testament to his global impact, he collaborated with esteemed researchers from Europe, China, Japan, and the USA to co-author a seminal book on smart grids. The reach of his work extends across international borders, as evidenced by his role as a guest, an invited, and a keynote speaker. He has delivered research talks at prestigious forums and universities situated in Pakistan, China, Saudi Arabia, and the USA.



H. Vincent Poor (Life Fellow, IEEE) received the Ph.D. degree in EECS from Princeton University in 1977. From 1977 to 1990, he was a Faculty Member with the University of Illinois at Urbana–Champaign. Since 1990, he has been a Faculty Member with Princeton University, where he is currently the Michael Henry Strater University Professor. From 2006 to 2016, he was the Dean of the School of Engineering and Applied Science, Princeton University. He has also held visiting appointments at several other universities, including most recently at Berkeley and Cambridge. Among his publications in these areas is the recent book *Machine Learning and Wireless Communications* (Cambridge University Press, 2022). His current research interests include information theory, machine learning and network science, and their applications in wireless networks, energy systems, and related fields. He is a member of the National Academy of Engineering and the National Academy of Sciences and a Foreign Member of the Chinese Academy of Sciences, the Royal Society, and other national and international academies. He received the IEEE Alexander Graham Bell Medal in 2017.