Received: 9 April 2021 | Revised: 7 January 2022 | Accepted: 11 May 2022

IET Smart Grid

DOI: 10.1049/stg2.12070

The Institution of Engineering and Technology WILEY

ORIGINAL RESEARCH

Cross-layered distributed data-driven framework for enhanced smart grid cyber-physical security

Allen Starke | **Keerthiraj Nagaraj** | **Cody Ruben** | **Nader Aljohani** | **Sheng Zou** | **Arturo Bretas** | **Janise McNair** | **Alina Zare**

Electrical and Computer Engineering, University of Florida, Gainesville, Florida, USA

Correspondence

Allen Starke, Electrical and Computer Engineering, University of Florida, P. O. Box 116200, 216 Larsen Hall, 968 Center Drive, Gainesville, FL 32611-6200, USA.

Email: allen1.starke@ufl.edu

Funding information

National Science Foundation, Grant/Award Number: 1809739

Abstract

Smart Grid (SG) research and development has drawn much attention from academia, industry and government due to the great impact it will have on society, economics and the environment. Securing the SG is a considerably significant challenge due the increased dependency on communication networks to assist in physical process control, exposing them to various cyber-threats. In addition to attacks that change measurement values using False Data Injection (FDI) techniques, attacks on the communication network may disrupt the power system's real-time operation by intercepting messages, or by flooding the communication channels with unnecessary data. Addressing these attacks requires a cross-layer approach. In this paper a cross-layered strategy is presented, called Cross-Layer Ensemble CorrDet with Adaptive Statistics(CECD-AS), which integrates the detection of faulty SG measurement data as well as inconsistent network inter-arrival times and transmission delays for more reliable and accurate anomaly detection and attack interpretation. Numerical results show that CECD-AS can detect multiple False Data Injections, Denial of Service (DoS) and Man In The Middle (MITM) attacks with a high F1-score compared to current approaches that only use SG measurement data for detection such as the traditional physics-based State Estimation, ECD-AS strategy and other machine learning classification-based detection schemes.

KEYWORDS

cross-layered, cyber security, cyber-physical systems, machine learning, network reliability, network security, power systems, real-time systems

1 | INTRODUCTION

The future power grid, or Smart Grid (SG), has drawn much attention from academia, industry and government due to the significant impact it will have on society, economics and the environment. Next generation SG systems integrate control, communication and computation to achieve stability, efficiency and robustness of physical control processes. Network communication introduces several drawbacks and opportunities. First, it introduces an exposure to cyber-threats [1]. Recently, the first confirmed cyberattack-initiated blackout occurred in Ukraine and caused a power outage that affected 225,000 customers [2, 3]. Similar malware was found in several systems that operate in the US power grid [3, 4]. In addition to being a subject of National Security, blackouts have huge economic impact. For instance, the estimated cost of the 2003 Northwest blackout ranges from 4 to 10 billion U.S. dollars in the United States, and 2.3 billion Canadian dollars in Ontario [5]. This realisation reinforced the critical need for research on cyber-related power grid vulnerabilities [6, 7]. Recent research literature addresses physical control process reliability, but research on cyber-physical security of SGs is still developing.

On the other hand, communication networks provide an opportunity for cross-layer awareness. Typically, the classical

power grid is protected by isolated and uncoordinated devices that provide ad hoc solutions for each protection problem. The lack of cooperation between these tools leaves them vulnerable to distributed attacks. Consider power system stabilisers (PSSs), which are located at synchronous generators to provide protection from small disturbances. If either a cyberattack or other disturbance occurs at any stage of the data collection process, the PSS can potentially malfunction, compromising SG stability. A cross-layer approach can provide situational awareness, generate a more accurate response and increase system reliability and resiliency through network redundancy. Just as Stuxnet exploited a vulnerability in a set of programmable logic controllers (PLCs) that controlled centrifuges for nuclear fuel processing [8], similar vulnerabilities could be exploited in PLCs that control automatic systems in grid-connected equipment.

Current research on the cyber-security of the power grid focusses on a process called state estimation (SE) [9–13]. SE uses real-time measurements and static data about the system topology to (1) estimate the state of the system and (2) perform various monitoring applications [14]. One of the main applications performed is Bad Data Analysis, which uses statistical tests to determine if any of the measurements on the system have an error. Errors in measurements can come from a variety of sources such as faulty metres or cyberattacks. A cyberattack on the measurements themselves is called a False Data Injection (FDI) and is the most common form of cyberattack considered in the literature. Current solutions for detecting FDI attacks tend to focus on modelling the behaviour of the attack, then use load forecasting by training various Machine Learning (ML) methods to detect relatively small changes in load distribution or in the state variables of the power grid [15–17]. While forecasting has been a very effective method to detect FDI within the power grid, these methods do not consider multiple hackers injecting false data to conduct a coordinated attack. In addition, these solutions do not address detecting other forms of cyberattacks that can negatively impact the performance of the power grid. The work in Ref. [18, 19] focusses on developing real-time solutions for detecting and defending against denial-of-service (Denial of Service (DoS)) attacks. In Ref. [18], a dynamic differential system is used that models the changing states of a metring infrastructure during DoS attacks, and in Ref. [19] an online storage facility is proposed for access to faster and scalable data analysis. In Ref. [20–22], solutions are proposed to protect against negative impacts on power grid state estimation due to delays in the transmission of state measurements and control signals. The work in Ref. [23] demonstrates that the lack of strong integrity and authentication checks in power grid's network communication protocols can allow hackers easy access to the system and may cause detrimental effects to performance.

While there are a wide range of cyberattacks that can negatively impact the power grid, recent research has focussed mainly on detecting and mitigating a single attack, that is, assuming that only one type of attack occurs at a given time. In a more realistic scenario, cyberattacks involve multiple entities exploiting various security flaws in the physical and cyber domains of the cyber-physical system. To the best of our knowledge, the impact of a coordinated attack consisting of different types, such as DoS, FDI, and Man in The Middle (MITM) has not been addressed. Furthermore, the challenge of leveraging the interdependence between different layers of the SG, that is, physical domain and cyber domain, to achieve more robust security in the system has not been sufficiently addressed. Therefore, this paper proposes a method of detecting multiple attacks and different types of attacks, initiated from different layers within the SG. This is accomplished through our proposed, novel cross-layer perspective. As shown in Figure 1, the SG cyber-physical system is composed of a physical domain, where measurements are taken and communicated through a communication network, and a cyber domain, where all of the data collected and communicated is analysed. The cyber domain is where the SE process occurs. In a previous work [24, 25], the authors have shown that ML can be used in the cyber domain, operating on the same data as the SE, to improve bad data analysis. This hybrid data-driven p framework takes advantage of both temporal data through ML and the known topology of the system through SE. Yet, this technique, such as the other current research studies, still only addresses FDI attacks and only uses standard measurements taken on power systems. Thus, it does not consider the cross-layer interdependencies of the SG. In another previous work [26], the Ensemble CorrDet with Adaptive Statistics (ECD-AS) strategy was developed by the authors to analyse measurement data and packet contents. ECD-AS is also a data-driven method for the detection of FDI attacks and considers the changing state of the SG. The limitation of this method is it only uses measurement data, limiting its ability to detect cyberattacks focussed on the communication network layer of the SG. However, the work in this paper will leverage the analysis layer, which can also consider data related to the communication network that drives the SG, specifically, the packet inter-arrival times, transmission delay (TD), and packet count (PC). Considering this type of data will expand the model of an FDI attack in the cyber domain as well as reveal models of different types of cyberattacks that would go undetected by current approaches in the literature.

In this paper, we present an SG cyber-physical security framework based on a cross-layer perspective that focusses on detection of various cyberattacks called the Cross-Layer Ensemble CorrDet with Adaptive Statistics (CECD-AS). Different from previous approaches that propose SG cyber-physical security, we consider the SG and the communication network as one and propose security solutions for the entire system. In such a system, the characteristics and security specifications of each layer should be considered in a cross-layer model to provide specific integrated countermeasures. Current state-of-the-art approaches focus only on data from the SG such as power and voltage measurements. Analysing data related to the communication network provides further information that can and should be used to better detect not only FDI attacks but a variety of other potential cyberattacks that may not affect measurement values at all.

The contributions of this work to the state of the art are as follows:

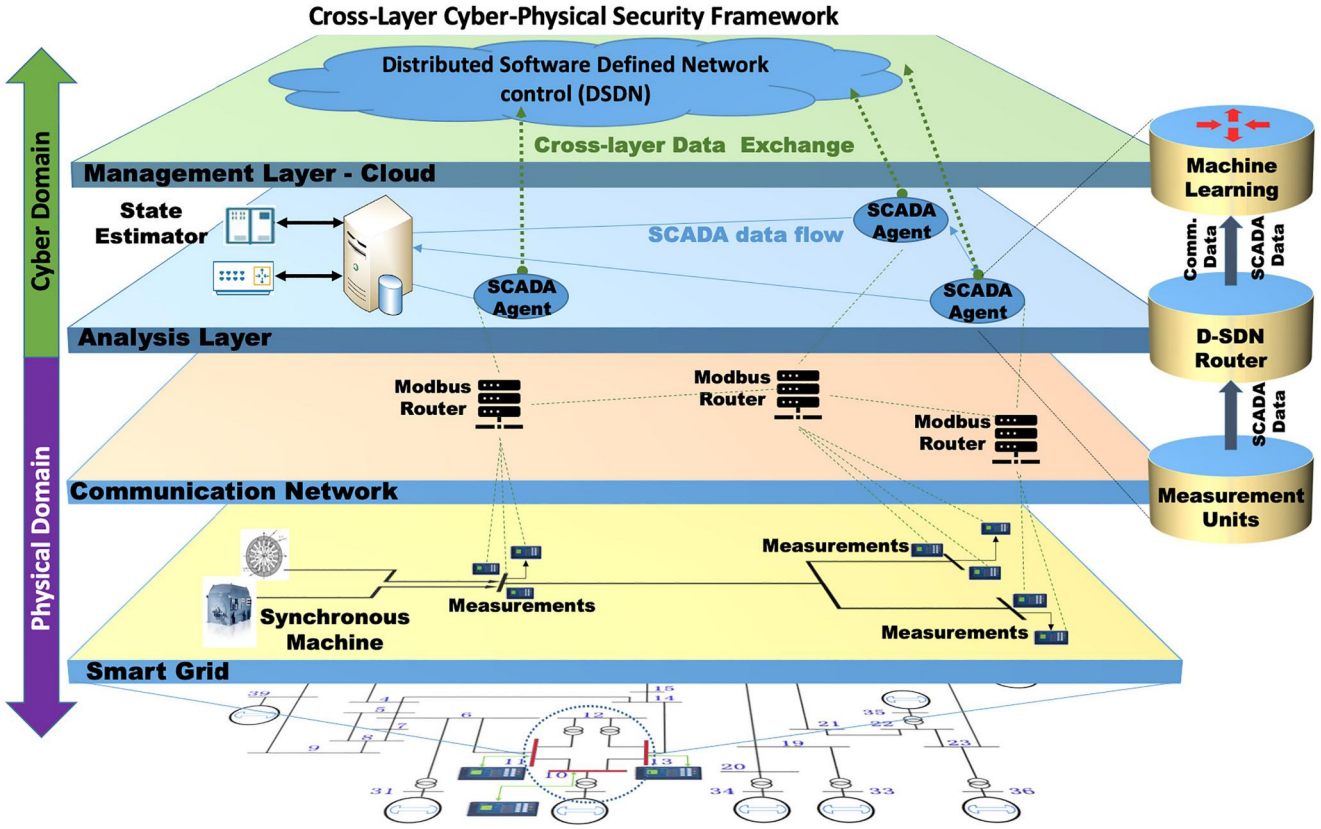

FIGURE 1 Cross-layer cyber-physical security architecture

- Using a cross-layer perspective between the power grid and communication network to enhance the detection of cyberattacks on the SG.
- Expanding on the ECD-AS method of anomaly detection on the SG to include information from the communication network.
- The consideration of various types of cyberattacks, beyond just FDI attacks, can only be detected by using a cross-layer perspective.
- Mathematically modelling the impact of various cyberattacks on the power grid and the communication network simultaneously.

The remainder of the paper is organised as follows. In Section 2, background information on the various aspects of the cross-layer perspective is presented. The details of the CECD-AS algorithm are shown in Section 3. The results of numerical tests used to evaluate the performance of this method are shown and discussed in Section 4. Finally, Section 5 presents the conclusions of this work.

2 | BACKGROUND INFORMATION

This section contains a literature review containing recent studies pertaining to cyber security for SG architectures as well as background information covering the anomalous characteristics of various cyberattacks. It also contains a background on the necessary statistical models used to generate experimental data and develop the novel ML algorithm presented in this paper.

2.1 | Smart grid system communication architecture

Traditionally, SG communications consisted of very low rate exchange of serial data point-to-point between deterministic nodes. With the creation of Phaser Measurement Units and dynamic networking infrastructures, SG systems' network traffic is increasingly coming from heterogeneous network structures experiencing different types of events, requiring more complex networking and control protocols. Managing these evolving networks using traditional network management schemes can increase the cost of network operation and maintenance and leave significant vulnerabilities in fault tolerance and security. Software Defined Networking (SDN) is a networking paradigm in which the forwarding hardware in a network switch/router is decoupled from control decisions. Instead of an integrated system, the network intelligence is logically placed in centralised software-based controllers (the control plane), while network devices become simple packet forwarding devices (the data plane) that can be programed via an open interface. SDNs help to assemble new services and infrastructure quickly to meet dynamically changing environment objectives.

Traditionally, SDNs are operated with one centralised controller to manage the entire network [27]. However, reliance on a single controller can compromise network reliability and create a single point of failure due to network congestion or attack. OpenFlow 1.2 [28] introduced multiple controller support and made possible the distributed management of overlays of independent networks that can be created on the same physical infrastructure. Since then, researchers have been investigating distributed control techniques for network management and more recently for network security [29, 30]. This approach will be updated, applied and evaluated to manage distributed and heterogeneous attacks on SGs [31].

The software implementation of the control plane and the built-in data collection mechanisms are excellent tools to implement ML network control applications [32]. Recent research has used ML approaches to classify and prevent various network security attacks in an SDN environment [33]. Methods for monitoring traffic in SDNs have included Deep Packet Inspection, Support Vector Machines, Neural Networks, and Decision Trees [33–35]. However, this approach and most supervised ML methods in general assume that every possible class and the distribution of possible samples for each of these classes are appropriately characterised by training data. Yet, in implementation, it is infeasible to assume that all possible behaviours can be identified and characterised in training data prior to implementation of a system—malicious attacks and their associated behaviours on the communication grid can and will be re-imagined and re-implemented. Thus, a system is needed that can adapt to changes in communication behaviour based on cross-layer information and can robustly detect and classify anomalous communication packets in real time. In the literature, ML methods have not been used within a cross-layer security framework to monitor for malicious behaviour.

Extracting knowledge from data collection to understand and predict the state of the SG network will be crucial to implement security management in the SG. Two significant challenges are proposed to be addressed: real-time SDN ML systems and real-time SG communications management through a distributed SDN architecture. As outlined in Figure 1, ML takes in the signal information from the physical layer as well as the network traffic information from the management layer and monitors the data for anomalies and signal corruption. ML can leverage interactions between the subsystems on the physical layer and integrated operation with the Distributed Software Defined Networking (D-SDN) controllers at the management layer.

2.2 | Recent security enhancements for smart grid

In recent literature, most applications of ML for cyberattack detection pertain to the detection and mitigation of FDI attacks. For example, the authors of Ref. [36] discussed how the SE is an obvious target during a cyberattack by changing a subset of the real-time measurements. They also discussed another method of attacking the SE by the system model parameters, which include the topology of the power system. Since the parameters are known to be static values, these types of attacks are not monitored and rarely detected via pre filtering steps such as FDI attacks. The authors proposed using a ML method called ECD-AS for the purpose of detecting and identifying both FDI and parameter-based attacks within an SG system. They first analyse an ML-based residual space to detect FDI attacks and second analyse the output of the physics-based SE and ML-based measurement estimation process to detect parameter attacks.

The authors of Ref. [37] came up with a very interesting way to detect FDI attacks using an image processing-based approach. The authors were able to visualise the data flow of an SG by mapping the system state data to 2D images and using deep convolutional neural network (CNN), which provide significant success in the image processing, to detect the attack. They claim that the image representation of system states brings up various types of features that are not seen within one-dimensional state vectors. Handling the problem as a texture image recognition problem increases the accuracy of the detector.

The authors of Ref. [38] discusses how the synchronisation processes in micro grids enable cyber vulnerabilities and allows attackers to execute FDI attacks with severe consequences. In the paper, they design and demonstrate exploits in the system resonance to influence the microgrid frequency to rapidly trip a generator causing the grid to shutdown prematurely. The designed attacks shows the significance of detecting coordinated periodic FDI threats. To mitigate such an issue, the authors develop strategies based on synchronisation control to derive equations that calculate the threshold for an anomaly detection and the saturation value for a limiter-block.

The authors in Ref. [39] proposes a graph deep learning model-based framework to detect and identify attacked nodes in SG networks. They consider networking data corresponding to normal and Distributed Denial of Service (DDoS) attacked samples to train a graph CNN model that can detect if a given SG network instance is under DDoS attack. Further, they propose an unsupervised learning-based graph spectral clustering to pinpoint the attacked nodes in the network. Although the proposed framework in this paper achieves high attack detection accuracy, authors only consider data from networking part of the cyber-physical SG system and utilise resource intense graph deep learning models in their framework.

Similar to effects that can take place after a successful MITM or DDoS attack, the authors of Ref. [40] investigated means of detecting and identifying stealthy line disconnection attacks in SG. To understand the behaviour of these types of attacks they develop a new strategy for cyber-physical attacks using the nonlinear power flow model where the attacker physically disconnects transmission lines within the system and conceals the disconnection with a cyberattack. Masking the disconnection with a cyberattack allows for the attack to be stealthy without requiring the cyber layer to report a topology that is different from the one that existed before the attack. They also developed a detection scheme using a switch transient-based technique to

detect cyber-physical attacks that are developed using the non-linear power flow model. The proposed technique does not require a selected set of measurements within the attacker's region of influence to be secure.

Many different strategies present in literature to securing a cyber-physical system or an SG. As presented in the comprehensive study [41], various authors are using ML means to assist in energy theft detection in smart grids. The comprehensive study discusses as well as lists other papers that implement strategies taking advantage of blockchain to secure SG architectures, since blockchain utilises a distributed ledger system, which plays a major role in ensuring message integrity and trustworthiness of the data. The study suggests using blockchains for metre reading, where smart metres are authenticated using LaCSys cryptography, allowing each metre to be represented as a node in the blockchain network. Each region would then have its own network of nodes and ledger to create a block for data. The authors of Ref. [42] utilise decentralised Security Access Administrators instead of the traditional centralised Certificate Authorities (CAs) to provide blockchain-based distributed access control for protecting critical cyber infrastructure.

There are few papers that research the impact of different types of anamolous behaviour such as faulty equipment, communication delays, or different cyberattacks on the SG. The authors of Ref. [43] research ways of detecting ransomware within Supervisory Control and Data Acquisition (SCADA) systems for Electric Vehicle Charging Stations. They proposed a novel, scalable, and interoperable deep learning-based ransomware detection framework that could be implemented at multiple vulnerable attack points. The authors of Ref. [44] investigate potential security and efficiency concerns that impede the deployment of federated-learning-based AIoT services in smart grids due to the low-quality shared local models, non-independently and identically distributed data distributions, and unpredictable communication delays. They proposed a secure federated-learning-enabled AIoT scheme to provide efficient communication and private energy data sharing in smart grids with edge-cloud collaboration.

To the best of our knowledge, all of the recent literature on this topic explores detecting and mitigating a single cyber-attack, typically FDI attacks, on the SG. They do not take into account the possibly of multiple coordinated attacks taking place at a single time, and the studies also do not consider integrating data provided from other crucial layers of the SG to increase the detection and identification accuracy of the various cyberattacks that can negatively impact SG system performance.

2.3 | Network performance statistics

The cross-layered analysis framework is based on the IEEE 118-bus system, emulating the most commonly used Modbus Remote Terminal Unit (RTU) over Transmission Control Protocol/Internet Protocol (TCP/IP) for traditional SG environments. This system follows the Poisson traffic model, since transmission of packets occur in batches every 4 s [45]. Each bus is modelled after the M/M/c queue [46], that is, $c \geq 1$, where the arrival of packets follow a Poisson process and the service time of the queue follows an exponential distribution. The utilisation (i.e. traffic intensity) of the systems is represented as

$$p_{util} = \frac{\boldsymbol{\lambda}}{\boldsymbol{\mu}} \tag{1}$$

where $\boldsymbol{\lambda}$ refers to the arrival rate of packets to the system, and $\boldsymbol{\mu}$ refers to the service time of packets in the system. The IAT is the time between packet arrivals and is one of the network performance metrics used in our analysis, which has an exponential distribution with parameter $\boldsymbol{\lambda}$. For $t \geq 0$, the probability density function is

$$f(t) = \boldsymbol{\lambda} e^{-\boldsymbol{\lambda} t} \tag{2}$$

Hence, the average IAT is defined as

$$IAT = \frac{1}{\boldsymbol{\lambda}} \tag{3}$$

The service time s has an exponential distribution with parameter $\boldsymbol{\mu}$, and the probability density function is

$$g(s) = \boldsymbol{\mu} e^{-\boldsymbol{\mu} s}, \quad \forall s \geq 0 \tag{4}$$

where $\frac{1}{\boldsymbol{\mu}}$ is the average service time of the system. Using Little's theorem, the total waiting time, in our case what we define as the transmission delays (TDs), can be measured as

$$W = TD = \frac{1}{\boldsymbol{\mu} - \boldsymbol{\lambda}} \tag{5}$$

Lastly, the so called 'normal' distribution of network packet arrivals (i.e. non-attacked packets) into each system are determined by the probability of seeing a number of packet arrivals in a period from [0,T].

$$P(n \text{ arrivals in interval } T) = \frac{(\boldsymbol{\lambda} T)^n e^{-\boldsymbol{\lambda} T}}{n!} \tag{6}$$

where T is the interval of time, and n represents the number of packets. This is used to model traffic volume of the bus, and the PC metric is defined as

$$PC = \boldsymbol{\lambda} T \tag{7}$$

2.4 | Cyberattacks

In this section, we provide an overview of the different possible types of cyberattacks based on the studies in Ref. [47, 48], apply them to SCADA networking systems for powergrid, and discuss

their impact on network connectivity, topology and network traffic.

- False Data Injections (FDI): this type of cyberattack injects forged measurement into the control system in hope of misguiding the control algorithm.

Impact: the impact factor of FDI attacks is high and can be seen on the physical and networking level of the victim system. The work in Ref. [49] proves that FDI attacks can increase the delay overtime of network packet transmissions. Such effects coupled with changes to power control have the potential of shutting down power grids, causing blackouts for an entire region.

- Flooding DoS: in DoS, the attacker intentionally disrupts the transmission of data to/from a given node through an excessive amount of service requests to the victim node, consuming all available resources.

Impact: the impact factor of DoS attacks are high. This type of attack increases network traffic at its victim node (i.e. arrival rate) to consume the victim resources and extend queue length resulting in an increase in wait times or TDs as can be seen in Ref. [50]. This can cause nodes to shut down, and impact the entire network as a whole. Distributed Denial of Service has a larger impact, since the attack occurs from multiple nodes, resulting in a higher arrival/attack rate.

- Man-in-the-Middle (MITM): it is an attack in which a third party gains access to the communications between two other parties, without either of those parties realising it. The third party might read the contents of the communication, or in some cases also manipulate it. The attacker node advertises false information using Address Resolution Protocol messages, or by hijacking the router each of the victim nodes are connected to. The MITM attack is seen as the grandfather to all other cyberattacks since this is typically the first step that must be achieved before executing other attacks.

Impact: the impact factor of MITM attacks is typically low or non-existent. Based on the type of MITM attack a flux of packets could increase the network traffic with no serious impact on network performance. MITM attacks have the most potential out of all the attacks listed, since they are the hardest to detect and can evolve into a dangerous attack such as DoS or FDI.

2.5 | Cyberattack statistical properties and models

A cyberattack is an attempt by hackers to damage or destroy a computer network or system. In general, the cyberattacks discussed in the previous section demonstrate a similar characteristic of increasing the arrival rate of the network traffic at the victim or destination nodes, as demonstrated in Figure 2. During specific cyberattacks (e.g. Denial of Service, FDI) the arrival rate, $\boldsymbol{\lambda}_1$, is a combination of normal and attack traffic (e.g. for DoS attacks $\boldsymbol{\lambda}_1$ is increased by flooded traffic from a hacker intending to crash the victim, where FDI attacks increase $\boldsymbol{\lambda}_1$ slightly to inject bad data). The impact of this increase of the arrival rate at the victim node (i.e. increase in $\boldsymbol{\lambda}_1$) is cascaded through the rest of the system, decreasing the service rate, $\boldsymbol{\mu}_1$, of the victim node and arrival rate, $\boldsymbol{\lambda}_2$, of the destination node. For MITM attacks the hacker infiltrates the connection between the victim node and the destination node, increasing the destination node's arrival rate, $\boldsymbol{\lambda}_2$, in an attempt to disguise themselves as the source node. Cyberattacks can be naturally modelled as stochastic processes [51]. The models are based on the attack rate (i.e. number of attacks that arrive per unit of time) and can be represented on three levels of the networking system including network-level, victim-level, and port-level attack processes as stated in Ref. [51]. FDI, DoS, and MITM attacks are executed on a victim-level attack process, which are attacks on individual victim computers or IP addresses. The authors of Ref. [51] proved that 80% and 70% of cyberattacks on the network and victim level, respectively, do not function as Poisson processes and instead exhibit long-range dependence (LRD) with extreme values. LRD refers to the rate of decay of statistical dependence of two points with increasing time interval or spatial distance between the points. A phenomenon is usually considered to exhibit LRD if the dependence in its autocorrelation function decays more slowly than an exponential decay.

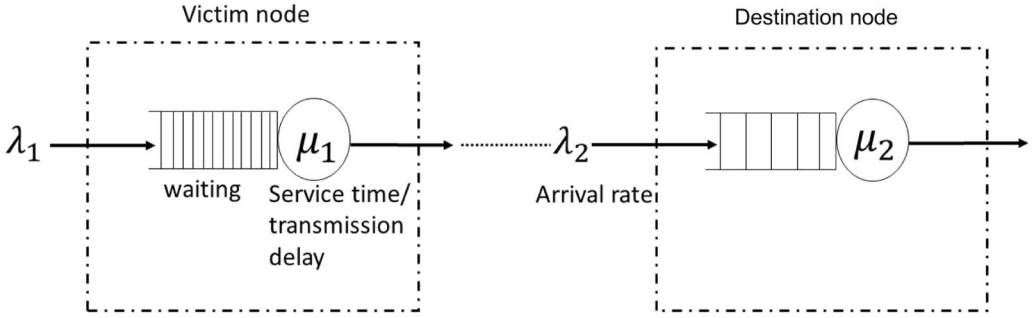

FIGURE 2 Victim representation of a cyberattack

$$p(h) = Cor(X_i, X_{i+h}) \sim h^{-\beta} L(h), h \to \infty \tag{8}$$

where $0 < \beta < 1$ and $L(\bullet)$ is a slowly varying function meaning that $lim_{x\to\infty}\frac{L(tx)}{L(x)} = 1$ for all $t > 0$ [52]. β is related to the Hurst parameter (H) as $\beta = 2 - 2H$. H is used to measure the degree of LRD, where $1/2 < H < 1$ and the degree of LRD increases as $H \to 1$ [51]. The distribution of extreme values for stationary time series follows the generalised Pareto distribution with survival function

$$\overline{G}_{\xi,\sigma(\mu)}(x) = 1 - G_{\xi,\sigma(\mu)} = \begin{cases} \left(1 + \xi\frac{x}{\sigma}\right)^{-\frac{1}{\xi}} & \xi \neq 0, \\ e^{\frac{-x}{\sigma}} & \xi = 0. \end{cases} \tag{9}$$

where ξ and σ are called shape and scale parameter, respectively.

A combination of an (LRD)-aware model of auto regressive fractionally integrated moving average (ARFIMA or FARIMA) and extreme-value-aware model such as the integrated generalised autoregressive conditional heteroskedasticity (IGARCH) is used for modelling and predicting cyberattacks [53]. FARIMA models are time series models that generalise ARIMA (autoregressive integrated moving average) models by allowing non-integer values of the differencing parameter. This is the well-known model where H = d + 1/2 and $0 < d < 1/2$. A stationary process X_t is FARIMA (p,d,q) if

$$\phi(B)(1 - B)^d X_t = \psi(B)\epsilon_t \tag{10}$$

for some $-1/2 < d < 1/2$, where

$$\phi(x) = 1 - \sum_{j=1}^{p} \phi_j x^j \tag{11}$$

and

$$\psi(x) = 1 + \sum_{j=1}^{q} \psi_j x^j \tag{12}$$

B is the back shift operator defined by $BX_t = X_{t-1}$, $B^2X_t = X_{t-2}$ etc. [51]. Generalized AutoRegressive Conditional Heteroskedasticity (GARCH) is a model for identifying stochastic processes with a conditional variance of the process. A time series is a GARCH process if $X_t = \sigma_t\epsilon_t$ and the integrated GARCH model is as follows

$$\phi(B)(1 - B)\epsilon_t^2 = w + (1 - \psi(B))\left(\epsilon_t^2 - \sigma_t^2\right) \tag{13}$$

where ϵ_t is the white noise distribution, σ_t is the standard deviation, and σ_t^2 is the variance [53].

2.6 | Physics-based state estimation

In modern Energy Management Systems (EMS), the State Estimation (SE) process is the core process for situational awareness of a power system and is used in many EMS applications, including the detection of bad data. The common approach to SE is using the classical Weighted Least Square (WLS) method described in Ref. [14]. In this approach, the system is modelled as a set of non-linear equations based on the physics of the system:

$$\mathbf{z}_{SG} = h(\mathbf{x}) + \mathbf{e} \tag{14}$$

where $\mathbf{z}_{SG} \in \mathbb{R}^{1\times d}$ is the measurement vector, $\mathbf{x} \in \mathbb{R}^{1\times N}$ is the vector of state variables, $h : \mathbb{R}^{1\times N} \to \mathbb{R}^{1\times d}$ is a continuously non-linear differentiable function, and $\mathbf{e} \in \mathbb{R}^{1\times d}$ is the measurement error vector. Each measurement error, e_i, is assumed to have zero mean, standard deviation, σ_i and Gaussian probability distribution. d is the number of measurements, and N is the number of states.

In the classical WLS approach, the best estimate of the state vector in (14) is found by minimising the cost function $J(\mathbf{x})$:

$$\begin{aligned} J(\mathbf{x}) &= \|\mathbf{z_{SG}} - h(\mathbf{x})\|^2_{R^{-1}} \\ &= [\mathbf{z}_{SG} - h(\mathbf{x})]^T R^{-1} [\mathbf{z}_{SG} - h(\mathbf{x})] \end{aligned} \tag{15}$$

where R is the covariance matrix of the measurements. In this paper, we consider the standard deviation of each measurement to be equal to 1% of the measurement magnitude. In Ref. [54], it is shown that in the gross error detection process all measurements should be weighted equally proportional to the measurement magnitude. After gross error processing, in the second step, metre precision can be restored and state estimation is performed.

$$\Delta\mathbf{z}_{SG} = H\Delta\mathbf{x} + \mathbf{e} \tag{16}$$

where $H = \frac{\partial h}{\partial \mathbf{x}}$ is the Jacobian matrix of h at the current state estimate $\mathbf{x}^*$, $\Delta\mathbf{z}_{SG} = \mathbf{z}_{SG} - h(\mathbf{x}^*) = \mathbf{z}_{SG} - \mathbf{z}^*_{SG}$ is the correction of the measurement vector and $\Delta\boldsymbol{x} = \mathbf{x} - \mathbf{x}^*$ is the correction of the state vector. The WLS solution is the projection of $\Delta\mathbf{z}_{SG}$ onto the Jacobian space by a linear projection matrix P, that is, $\Delta\mathbf{z}_{SG} = P\Delta\hat{\mathbf{z}}_{SG}$. Letting $\mathbf{r} = \Delta\mathbf{z}_{SG} - \Delta\hat{\mathbf{z}}_{SG}$ be the residual vector, the P matrix that minimises $J(\mathbf{x})$ will be orthogonal to the Jacobian range space and to $\mathbf{r}$; $\Delta\hat{\mathbf{z}} = H\Delta\hat{\mathbf{x}}$. This is in the form:

$$\langle\Delta\hat{\mathbf{z}}_{SG}, \mathbf{r}\rangle = (H\Delta\hat{\mathbf{x}})^T R^{-1}(\Delta\mathbf{z}_{SG} - H\Delta\hat{\mathbf{x}}) = 0. \tag{17}$$

Solving (17) for $\Delta\hat{\mathbf{x}}$:

$$\Delta\hat{\mathbf{x}} = \left(H^T R^{-1} H\right)^{-1} H^T R^{-1} \Delta\mathbf{z}_{SG}. \tag{18}$$

At each iteration, a new incumbent solution $\mathbf{x}^*_{new}$ is found and updated the following: $\mathbf{x}^*_{new} = \mathbf{x}^* + \Delta\hat{\mathbf{x}}$. (18) is solved each iteration until $\Delta\hat{\mathbf{x}}$ is sufficiently small to claim convergence of the solution.

The projection matrix P is the idempotent matrix that has the following expression:

$$P = \Delta\hat{\mathbf{x}} = \left(H^T R^{-1} H\right)^{-1} H^T R^{-1} \tag{19}$$

As shown in Ref. [55], the geometrical position of the measurement error in relation to the range space of H provides another way of interpreting the state estimation. Hence, as the measurement vector can be decomposed into two subspaces, it is possible to decompose the measurement error vector into two components as follows:

$$\mathbf{e} = \underbrace{P\mathbf{e}}_{\mathbf{e_U}} + \underbrace{(I-P)\mathbf{e}}_{\mathbf{e_D}} \tag{20}$$

The component $\mathbf{e_D}$ is the detectable error, which is the residual in the classical WLS model, while the component $\mathbf{e_U}$ is the undetectable error. $\mathbf{e_D}$ is in the orthogonal space to the range space of Jacobian whereas $\mathbf{e_U}$ is hidden in the Jacobian space.

$$\|\mathbf{e}\|^2 = \|\mathbf{e_D}\|^2 + \|\mathbf{e_U}\|^2 \tag{21}$$

The error vector in Equation (21) is called Composed Measurement Error (*CME*). In order to quantify the undetectable error, the Innovation Index (*II*) is introduced [10] and is presented in the following:

$$II_i = \frac{\left\|e_D^i\right\|}{\left\|e_U^i\right\|} = \frac{\sqrt{1-P_{ii}}}{\sqrt{P_{ii}}} \tag{22}$$

Low Innovation index means there is a large component of error that is not reflected in the residual. Therefore, the residual will be very small even if there is a gross error. By using (21) and (22), the *CME* can be expressed in terms of the residual and the innovation index as follows:

$$CME_i = r_i\left(\sqrt{1+\frac{1}{II_i^2}}\right). \tag{23}$$

The *CME* values for the measurements taken on the SG can then be used to do Bad Data Analysis, one of the main applications of SE [56]. A chi-squared test is used for the detection of bad data in the measurement set, which compares a *CME* based objective function value to a chi-squared threshold, which is based on the probability p (typically $p = 0.95$) and the degrees of freedom d:

$$J_{CME}(\hat{\mathbf{x}}) = \sum_{i=1}^{d}\left[\frac{CME_i}{\sigma_i}\right]^2 > \chi^2_{d,p} \tag{24}$$

If the value of J_{CME} is greater than the chi-squared threshold, then an error is detected in the measurement set.

2.7 | CorrDet (CD) anomaly detection

The ML layer of the smart power grid uses the knowledge of already verified data to learn the normal state of a properly functioning grid. It is then able to detect any anomalies introduced into the system at any point forward and alerts the network layer to identify the anomaly, isolate it from the remainder of the system and take appropriate action. This action might be in the form of preventing contamination of the system, with regards to both power distribution in other subsystems and data assimilation by the ML system itself.

The ML layer is developed using CorrDet Anomaly Detection [57–59] algorithm as the foundation. The CorrDet anomaly detection learns a set of statistics for normal samples, including the mean ($\boldsymbol{\mu}$) and standard deviation ($\boldsymbol{\Sigma}$). Then, for each incoming sample ($\mathbf{z}$), the Mahalanobis distance of this new sample is computed with respect to the distribution of normal samples. A threshold value (τ) is also estimated such that if the Mahalanobis distance is larger than the threshold value, the new sample is detected as abnormal sample.

There are two versions of CorrDet anomaly detection based on the change in statistics of data over time. If the data is not dynamically changing over time, a simple version of CorrDet algorithm can be applied. In this case, the statistics of normal samples are estimated directly from sample mean and covariance of training data and the threshold is picked by experiments. If the data is dynamically changing over time, an adaptive version of CorrDet algorithm can be used. In this case, the sample

mean and covariance of training data as well as the threshold value estimated from training data are only for initialisation. As an incoming new sample is detected to be normal, the values of $\boldsymbol{\mu}$, $\boldsymbol{\Sigma}$ and τ are updated and the sample is added to the set of normal samples.

3 | CYBERATTACK DETECTION: A CROSS-LAYERED PERSPECTIVE

The proposed novel cross-layer cyber-physical security framework is composed of the physical and cyber domains to combine performance statistics from multiple layers for enhancing the security of the system. Figure 1 illustrates how the data is collected and processed by the separate acting layers of a SCADA agent in the SG system architecture. The physical domain represents the low-level hardware applications such as the power grid measurement units and the Modbus RTU communication routers that make up the SCADA agents. A deeper dive into the architecture, Figure 3, shows a more detailed view of the distributed SCADA agents from Figure 1. In each agent, a Modbus Router will collect real time power measurements from the system and network performance statistics (i.e. inter-arrival times, TDs, traffic volume etc.). This information is distributed to the cyber domain to execute the high-level functions of state estimation, ML and robust control of the system. As described with more detail in the above section 2.6, the SE in the analysis layer is responsible for core processes of situational awareness of a power system and can be used to detect FDI attacks. Unfortunately, the SE cannot distinguish between data corrupted due to a cyberattack and errors due to a faulty metre. For this reason, we implement local CorrDet algorithms in each

SCADA agent to consider not only the generated power grid dat, but also the network performance statistics, giving the ML algorithm the cross-layered perspective that is vital to detecting other cyberattacks besides FDIs.

Results from each individual local cross-layered CorrDet algorithms are transmitted to the management layer in the cloud, which contains our proposed novel ML framework, as seen in Figure 4, and the D-SDN controllers, as seen in Figure 1. The adaptive ML method, called CECD-AS, is presented in the next section 3.2. The technique focusses on being rapidly responsive to identifying and distinguishing cyber threat behaviour from section 2, outliers and gradual changes in the standard behaviour of the power grid performance values using the information provided from each local CorrDet algorithm.

The D-SDN controllers, in the management layer, are responsible for robust control and execution of mitigation strategies to correct the anamolous behaviour detected from the CECD-AS algorithm in the grid.

3.1 | Combining power grid and communication network statistics

Characteristics and security specifications of each layer should be considered in a cross-layer model to provide specific integrated countermeasures. The envisioned cross-layer analysis architecture for the cyber plane of one agent is represented in Figure 3. Each agent has an ML element with cross-layer interaction between the data plane, the SE, and the SDN to record and monitor network performance data and power exchanges. Packets are transmitted from bus-to-bus or bus-to-server using the Modbus RTU over TCP/IP networking protocol and technology. The transmission delays (TDs) are

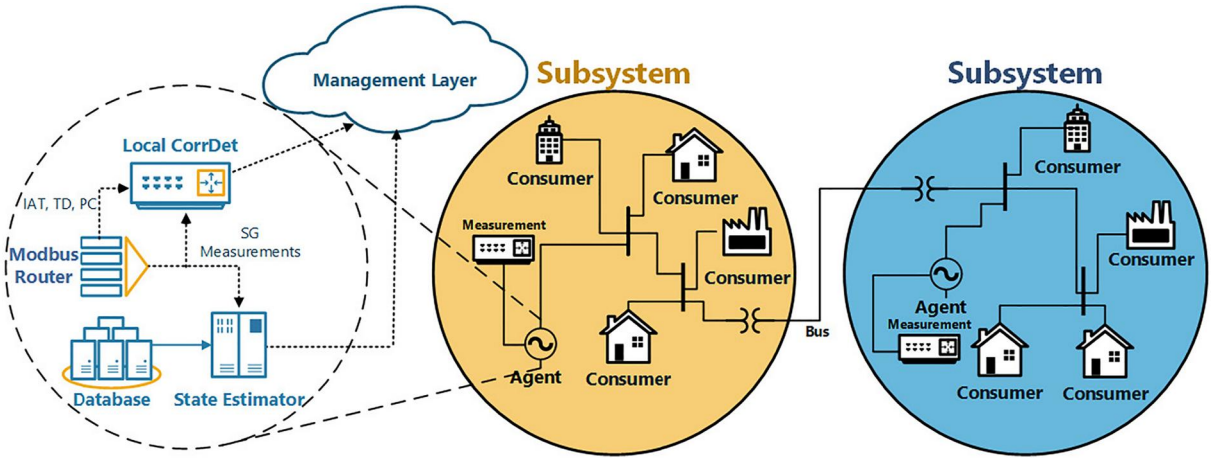

FIGURE 3 Distributed architecture of the control and data acquisition systems of the Smart Grid

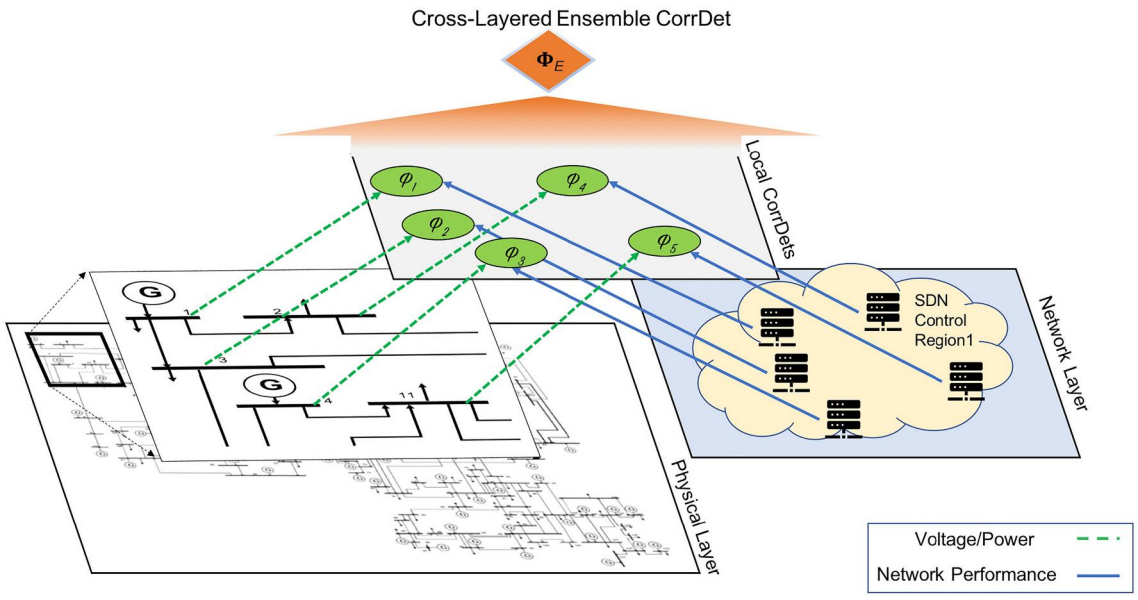

FIGURE 4 Cross-layer ensemble CorrDet framework

measured at the source node (i.e. $\frac{1}{\mu_1-\lambda_1}$), as shown in Figure 2, and the IATs and traffic volume are measured at the destination node (i.e. $\frac{1}{\lambda_2}$). Power measurements are polled and recorded periodically from each bus on the physical layer every 4 s. These values (i.e. voltage, power, and network performance statistics) are combined and analysed locally using the algorithm described in section 3.2, to provide a distributed approach at detecting anomalies for each agent.

The data being fed into our proposed anomaly detection model, represented as sample $\mathbf{z}$, is a concatenation of the measurement vector, $\mathbf{z}_{SG}$, IAT vector, $\mathbf{z}_{IAT}$, and TD vector, $\mathbf{z}_{TD}$. In other words, each sample is a *triple*, $\mathbf{z} = [\mathbf{z}_{SG}, \mathbf{z}_{IAT}, \mathbf{z}_{TD}]$, a $1 \times 3d$ vector instead of $\mathbf{z} = [\mathbf{z}_{SG}]$, and a $1 \times d$ vector when only measurement values are used in FDI attack [26], where d is the number of measurements/IAT/TD of all buses in the power grid system. A *triple element* $\mathbf{z}^{(c)}$, a 1×3 vector, is defined as a concatenation of the cth measurement value, the cth IAT value and the cth TD value, $\mathbf{z}^{(c)} = \left[\mathbf{z}_{SG}^{(c)}, \mathbf{z}_{IAT}^{(c)}, \mathbf{z}_{TD}^{(c)}\right]$. A *triple element* is a subset of the *triple*, $\mathbf{z}^{(c)} \in \mathbf{z}$.

3.2 | Cross-Layer Ensemble CorrDet with Adaptive Statistics

The CECD-AS, an extended work of CorrDet algorithm, can be considered as a set of Cross-Layer CorrDet detectors for each local environment, as shown in Figure 4. For instance, local CorrDet for bus 1 (ϕ_1) receives measurement vector ($\mathbf{z}_{SG}$) from the smart-grid layer, and IAT vector ($\mathbf{z}_{IAT}$) and TD vector ($\mathbf{z}_{TD}$) from network layer for every sample. These local Cross-Layer CorrDets form the Cross-Layer Ensemble CorrDet. In the whole power grid topology, spatially neighbouring buses are more highly correlated and easier to be affected by an attack while buses that are further away have lower correlation. Thus, learning a full covariance over the *triple* $\mathbf{z}$ of all buses is unnecessary (nearly sparse covariance), especially when training data is limited. Instead, local, fewer dimensional subsets of the *triple* offer a more accurate statistic estimation and a computationally cheaper, more sensitive anomaly detection.

The CorrDet detector learns a set of statistics ($\boldsymbol{\mu}$, $\boldsymbol{\Sigma}$ and τ) for all buses Φ_R in power grid topology, while CECD-AS learns a series of statistics ($\boldsymbol{\mu}_m$, $\boldsymbol{\Sigma}_m$ and τ_m), one for each bus ϕ_m considering information from both SG and communication layers. The CECD-AS detector prevents the numerical issue of estimating a high-dimensional mean and covariance for the distribution of the normal samples (in CorrDet detector) in the space of all *triple elements* when the number of *triple elements* are high and the number of training samples is low, by learning a lower-dimensional statistics in the space of only the measurements associated with each bus.

There are $m_j (m_j < d)$ *triple elements* on each bus m, where each bus is considered as a local, spatial region, corresponding to one local Cross-Layer CorrDet detector, ϕ_m. For Φ_R, the learning process consists of estimating $\boldsymbol{\mu}$ and $\boldsymbol{\Sigma}^{-1}$ from normal training samples $\mathbf{z}$ $\left(\mathbf{z} \in \mathbb{R}^{1\times 3d}\right)$. A similar strategy is proposed to learn the CECD-AS detector. The learning of Φ_E involves the estimation of a set of local Cross-Layer CorrDet detectors, ϕ_m.

For each ϕ_m, the learning process consists of estimating its $\boldsymbol{\mu}_m$ and $\boldsymbol{\Sigma}_m^{-1}$ from the normal training samples with selected *triple elements* $\mathbf{z}_m$ ($\mathbf{z}_m$ is a $1 \times 3m_j$ vector). The $\boldsymbol{\mu}_m$ and $\boldsymbol{\Sigma}_m^{-1}$ are initialised with the sample mean and covariance of selected *triplet elements* of first k samples that are labelled as normal.

Then, it starts to accept new sample and classify the new sample as follows. For each new incoming sample $\mathbf{z}$, a set of squared Mahalanobis distances, δ_m^{ECD}, are computed using Equation (25) and compared with the corresponding set of thresholds, T, where $T = \{\tau_m\}_{m=1:M}$. If at least one squared Mahalanobis distance in $\{\delta_m^{ECD}\}_{m=1:M}$ is greater than its corresponding threshold, this incoming sample is classified as an anomaly. Otherwise, it is classified as a normal sample.

$$\delta_m^{ECD}(\mathbf{z}_m) = (\mathbf{z}_m - \boldsymbol{\mu}_m)^T \Sigma_m^{-1} (\mathbf{z}_m - \boldsymbol{\mu}_m) \tag{25}$$

where $\boldsymbol{\mu}_m$ is the mean and Σ_m^{-1} is the inverse covariance matrix of normal samples on mth local Cross-Layer CorrDet detector.

For each new sample that is classified as normal, the anomaly detector must be able to adapt with changing trends since data is dynamic and it changes gradually over time. Therefore, the mean, $\boldsymbol{\mu}_\mathbf{m}$ and inverse covariance matrix, Σ_m^{-1} are updated using the Woodbury Matrix Identity [60] in Equations 26 and 27, respectively. Note that this update is done only if the incoming data is considered normal data.

$$\boldsymbol{\mu}_{new,m} = (1-\alpha)\boldsymbol{\mu}_m + \alpha(\mathbf{z}_m - \boldsymbol{\mu}_m) \tag{26}$$

$$\Sigma_{new,m}^{-1} = \frac{1}{1-\alpha}\left[\Sigma_m^{-1} - \frac{(\mathbf{z}_m - \boldsymbol{\mu}_m)(\mathbf{z}_m - \boldsymbol{\mu}_m)^T}{\frac{1-\alpha}{\alpha} + (\mathbf{z}_m - \boldsymbol{\mu}_m)^T(\mathbf{z}_m - \boldsymbol{\mu}_m)}\right] \tag{27}$$

where $\boldsymbol{\mu}_m$ is the old mean of mth local Cross-Layer CorrDet detector, Σ_m^{-1} is the old inverse covariance matrix of mth local Cross-Layer CorrDet detector and α is a hyper-parameter value between zero and one that determines how much importance is given to the new data sample versus the old mean. We determine the value of k and α through experimentation.

The threshold can be assumed to be fixed for the dataset that has constant mean and small variation in the time domain. $T = \{\tau_m\}_{m=1:M}$ is estimated using Equation (28).

$$\boldsymbol{\tau}_m = \boldsymbol{\mu}_{\mathbf{thr,m}} + \eta * \boldsymbol{\sigma}_{\mathbf{thr,m}} \tag{28}$$

where $\boldsymbol{\mu}_{\mathbf{thr,m}}$ and $\boldsymbol{\sigma}_{\mathbf{thr,m}}$ are the mean and standard deviation of the Mahalanobis distance values of the selected triplet elements of all normal samples in training data.

However, for the daily load profile data set considered in this work, the statistics of normal samples have a larger dynamically changing mean and covariance with time such that the previous fixed threshold assumption does not hold. Therefore, the Cross-Layer Ensemble CorrDet (ECD) with Adaptive Statistics is used in this work.

Unlike the fixed threshold estimation in the CorrDet algorithm, adaptive threshold estimation in the CECD-AS algorithm not only initialises the threshold values τ_m for each local Cross-Layer CorrDet detector (bus-level) following Equation (28) but also updates τ_m in an online sliding window fashion [26].

For every new incoming sample $\mathbf{z}$, the threshold values τ_m are inferred from the most recent β normal samples before it. In other words, the standard deviation ($\sigma_{thr,m,-\beta}$) and mean ($\boldsymbol{\mu}_{thr,m,-\beta}$) of squared Mahalanobis distance values of β normal samples past of the new sample $\mathbf{z}$ are calculated for each local Cross-Layer CorrDet detector ϕ_m. Here β is the sliding window size. Then, threshold value τ_m for each local Cross-Layer CorrDet detector is updated using Equation (29) with updated $\boldsymbol{\mu}_{thr,m,-\beta}$ and $\sigma_{thr,m,-\beta}$, where $-\beta$ signifies the use of past β number of samples for updating threshold.

$$\tau_m = \mu_{thr,m,-\beta} + \eta * \sigma_{thr,m,-\beta}. \tag{29}$$

Let K_1 and K_2 be the number of training and testing samples, respectively. Let $\mathbf{Z}$ ($\mathbf{Z} \in \mathbb{R}^{3d \times K_1}$) and $\tilde{\mathbf{Z}}$ ($\tilde{\mathbf{Z}} \in \mathbb{R}^{3d \times K_2}$) be the training and testing samples, respectively. Let $\mathbf{Y}$ ($\mathbf{Y} \in \mathbb{R}^{1 \times K_1}$) and $\tilde{\mathbf{Y}}$ ($\tilde{\mathbf{Y}} \in \mathbb{R}^{1 \times K_2}$) be the corresponding labels. $\boldsymbol{\delta}_{Z,m}$ ($\boldsymbol{\delta}_{Z,m} \in \mathbb{R}^{1 \times K_1}$) denotes the squared Mahalanobis distances of all training samples with respect to mth Cross-Layer CorrDet classifier, ϕ_m. $\boldsymbol{\delta}_{\tilde{z}_k}$ ($\boldsymbol{\delta}_{\tilde{z}_k} \in \mathbb{R}^{1 \times M}$) denotes the squared Mahalanobis distances of kth testing sample with respect to all local Cross-Layer CorrDet classifiers, Φ_E. Let $\mathbf{B}$ be the squared Mahalanobis distances of all normal samples in the sliding window with a length of β ($\mathbf{B} \in \mathbb{R}^{1 \times \beta}$). The pseudo code for the proposed anomaly detection algorithm is shown in Procedure 1.

Procedure 1 Cross-Layer Ensemble CorrDet with Adaptive Statistics (CECD-AS) algorithm

Train a Cross-Layer Ensemble CorrDet classifier:
Input: $\mathbf{Z}$, $\mathbf{Y}$, $\tilde{\mathbf{Z}}$
for Every local Cross-Layer CorrDet classifier $m = 1: M$ **do**
    Initialise the mean $\boldsymbol{\mu}_m$ and covariance Σ_m^{-1} of normal statistics using the sample mean and covariance of normal samples in the training set with selected triple elements associated with ϕ_m
    Initialise the squared Mahalanobis distance $\boldsymbol{\delta}_{Z,m}$ using Equation (25)
    Initialise the threshold τ_m using Equation (28)
end for

Test using the Cross-Layer Ensemble CorrDet classifier with Adaptive Statistics:
for Every test sample $k = 1: K_2$ **do**
    Compute the squared Mahalanobis distance $\boldsymbol{\delta}_{\tilde{z}_k}$ using Equation (25)
  if $\forall m, \boldsymbol{\delta}_{\tilde{z}_k} < \tau_m$ **then**
      Classify $\tilde{z}_k$ as normal sample: $\tilde{y}_k = 0$
      Update the mean $\boldsymbol{\mu}_m$ and covariance Σ_m^{-1} using Equations (26) and (27)
      Update the sliding window by adding $\boldsymbol{\delta}_{\tilde{z}_k}$ to $\mathbf{B}$ and removing the oldest value from $\mathbf{B}$.
      Update the mean $\mu_{thr,m,-\beta}$ and variance $\sigma_{thr,m,-\beta}$ of squared Mahalanobis distances in the updated sliding window of each local Cross-Layer CorrDet detector
      Update the threshold value τ_m for each local Cross-Layer CorrDet detector using Equation (29)
  else
    Classify $\tilde{z}_k$ as abnormal sample: $\tilde{y}_k = 1$
  end if
end for
Output: $\tilde{\mathbf{Y}}$

4 | EXPERIMENTAL RESULTS

The cross-layered analysis for detection of cyberattacks was validated using the IEEE 118-bus system. Using the MATLAB package MATPOWER [61], 21,600 samples (i.e. one day's worth) of measurement were generated with Gaussian noise based on a common daily load profile that contains temporal information of a power system's changing state. The measurement set included are real and reactive power flows, power injections, and all voltage magnitudes, resulting in 691 measurements. Then, network packet times (i.e. inter-arrival times and TDs) were generated using mininet and extensions to emulate the commonly used Modbus RTU over TCP/IP protocol for traditional SG environments [62]. Times were based on the M/M/c queue, that is, $c \geq 1$, where packet arrivals were modelled after Poisson distribution and TDs were inherently modelled after the exponential distribution, as described in Section 2.3. The correlating anomalous network performance statistics (i.e. Inter-arrival time, and TD) from DoS and FDI attacks were generated based on the attack tools used in Ref. [49, 50], respectively and exhibit the cyberattack properties described in Section 2.5. The data flow of the simulation environment can be seen in Figure 5. In general, the packet arrival rates to the victim node are increased during the periods where FDI and DoS attacks take place. The attack severity level is changed based on the different methods of attacking, as described in the next section, which can increase the network performance statistics by a factor between 2 and 7. Network traffic volume was generated using a combination of simulation tools such as mininet and a commonly used tool

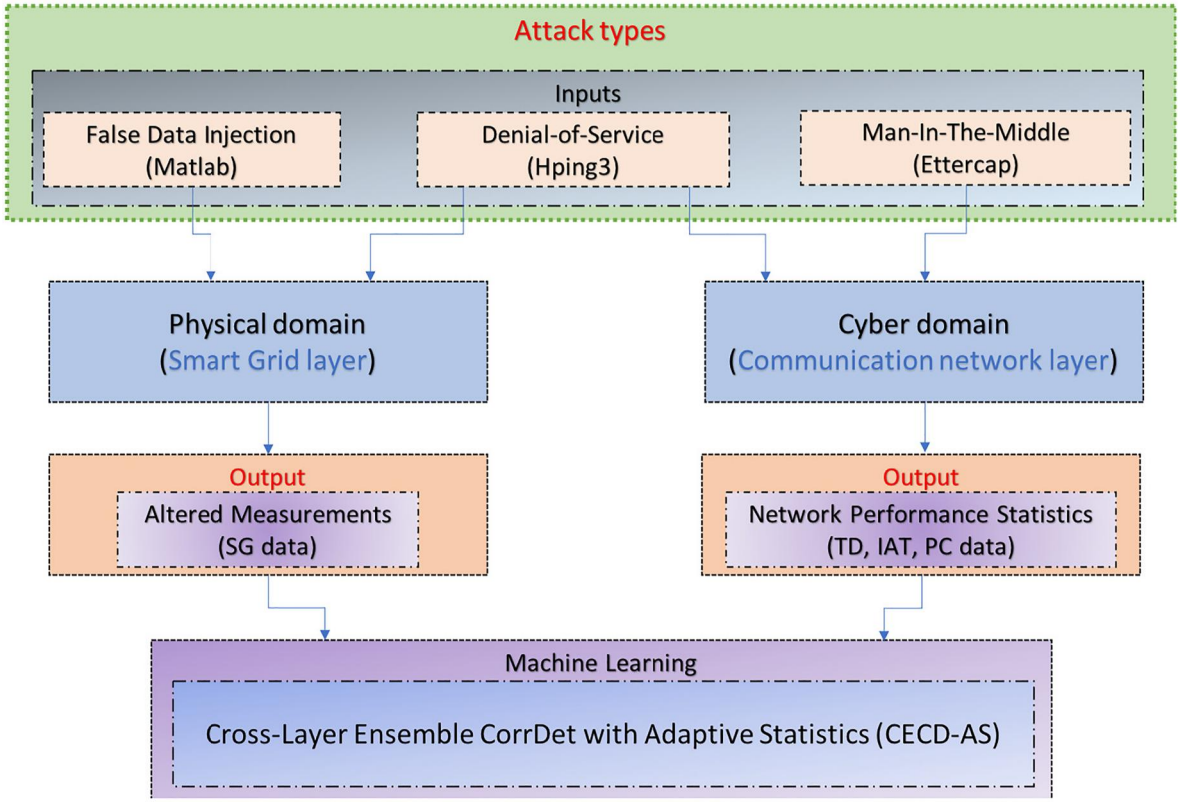

FIGURE 5 Simulation environment model

useful for executing man-in-the-middle cyberattacks called Ettercap [63]. For this paper, we tested our cross-layered anomaly detection scheme on three types of cyberattacks including multiple false data injections, multiple denial-of-service, and man-in-the-middle attacks. These cyberattacks are done on a victim-level attack process, which are attacks on individual victim computers or IP addresses.

4.1 | Dataset description

In this paper, four types of datasets were generated to simulate different types of attack. It should be noted that true labels are assigned during the process of introducing errors in all datasets. The datasets described used for experimentation are available upon request from any of the authors of this paper.

4.1.1 | MFDI attack dataset

In this dataset, only MFDI attack is considered. Errors are injected in the measurement set at random in 5% of the dataset samples. The resultant dataset of this type has 1103 samples with the MFDI attack out of 21,600 samples. In this case, two scenarios were considered. In the first scenario, two measurements were chosen randomly to be compromised and a higher severity level for the network statistics was included during the periods of the attack. In the second scenario, the Coordinated Multiple FDI (C-MFDI) attack is considered. This attack is designed such that measurements with low Innovation Index (II) are attacked, which is shown to be difficult for physics-based state estimation solution bad data detection [10]. The second scenario included a lower severity level for network statistics to make it more difficult in detecting the attack taking place.

4.1.2 | MDoS attack dataset

In this dataset, only Multiple Denial of Service (MDoS) attacks are considered. In a similar way, errors are introduced in 5% of the samples at random. However, once a decision is made to introduce DoS attack, the measurements associated with the selected buses, which is also by random, will be altered for 10 consecutive samples. The resultant dataset of this type has 7330 samples with the DoS attack out of 21,600 samples. In each of the attacked samples, three buses were chosen randomly to have their associated measurements (voltage, power injection, and power flow from those buses) be compromised. The MDoS dataset contained a high severity level on the network statistics during the periods of attack.

4.1.3 | MFDI-MDoS attack dataset

In this dataset, a combination of MFDI and MDoS at random samples with random number of measurements being in error

is considered. The resultant dataset of this type has 4861 samples with MFDI or MDoS attack out of 21,600 samples. In each of the attacked samples, four measurements were chosen randomly to be compromised if the attack is MFDI. For MDoS attack, four buses at random were chosen to have their associated measurements be altered. The MFDI-MDoS dataset contained a high severity level on the network statistics during the periods of attack.

4.1.4 | MITM attack dataset

In this dataset, only the man-in-the-middle (MITM) attack is considered. In a similar way to the MDoS data set, errors are introduced in 5% of the samples at random. Unlike DoS and FDI attacks, which affect both the power flow and network performance metrics, the MITM attack only affects the network performance metric for traffic volume (i.e. Packet count). Hence, traffic volume is generated and tested for this attack. Once a decision is made to introduce the MITM attack, the network traffic of a randomly selected bus is altered for 10 consecutive samples. The resultant dataset of this type has 7330 samples with MITM attacks out of 21,600 samples.

4.2 | Performance analysis

To evaluate the performance of the anomaly detection strategies included in this paper, we make use of the following classification metrics [64]. In our analysis, True Negatives refer to normal samples that are predicted as normal samples. True Positives refer to anomalous samples correctly predicted as anomalous. False Negatives (FN) refers to anomalous samples predicted to be normal, and False Positives (FP) refers to normal samples predicted to be anomalous.

Accuracy is the ratio of correctly predicted samples to the total number of samples. Accuracy is a good performance metric when the class sizes are balanced in the dataset. For datasets with imbalanced class size (which is true in our analysis), accuracy would not serve as a good performance metric. Hence, we include metrics such as precision, recall and F1-score, which provides a better measure of performance for anomaly detection strategy. (30) shows the formula to calculate the overall accuracy of the model.

$$Accuracy = 100 \times \frac{TP + TN}{TP + FP + TN + FN} \tag{30}$$

Precision is the ratio of number of correctly predicted normal samples to the overall predicted normal samples. Precision is an important metric when we want to minimise FP. (31) shows the formula for calculating precision performance metric.

$$Precision = 100 \times \frac{TP}{TP + FP} \tag{31}$$

Recall (also called as sensitivity) is the ratio of number of correctly predicted normal samples to the number of true normal samples. If we want to minimise the FN, a high value of Recall is expected without precision being too low. (32) shows the formula for calculating recall performance metric.

$$Recall = 100 \times \frac{TP}{TP + FN} \tag{32}$$

F1-score is the harmonic mean of precision and recall. It would be better to have a single performance metric that would consider both precision and recall, and which strikes a good balance between them. This metric is more useful than accuracy since we have uneven class distribution for normal samples and anomalous samples in our analysis. (33) shows the formula for calculating F1-score performance metric.

$$\text{F1 - score} = 100 \times \frac{2 * Recall * Precision}{Recall + Precision} \tag{33}$$

4.3 | Numerical results and discussions

To compare our results with other techniques, we first provide Table 1, which shows the mean and standard deviation of accuracy, precision, recall and F1-score values of various FDI detection techniques developed using traditional ML classification algorithms [26]. Table 1 demonstrated that for FDI attacks in daily load profile-based SG data, the ECD-AS technique outperforms traditional ML techniques as well as the physics-based state estimator and the data-driven technique. In Table 2, we compare ECD-AS with the proposed cross-layer CECD-AS approach. Accuracy, precision, recall and F1-score are shown for MFDI, MDoS and MITM attacks.

The CECD-AS algorithm is employed to detect MFDI, MDoS, MITM and MFDI-MDoS attacks using various attack datasets. Model parameters such as α in (26) and (27), β in (29) and η in (29) were selected through experimentation by considering the values of F1-score. The optimal values used to generate results in Table 2 are $\alpha = 8e-5$ and $\beta = 90$. The value of η is selected to be 11 for MFDI and C-MFDI attacks and 7 for MDoS, MFDI-MDoS and MITM attacks. From the 21,600 samples in each dataset, in the first cross validation experiment samples 0–1800 ($K_1 = 1800$, 2 h worth of data) were used for initial model training and samples 1800–12,600 ($K_2 = 10{,}800$, 12 h worth of data) were used for the subsequent model update and testing phase of CECD-AS. For the second cross validation experiment, we consider samples 1000–2800 ($K_1 = 1800$) for training and samples 2800–13,600 ($K_2 = 10{,}800$) for the subsequent model update and testing phase and so on for a total of 10 cross validation experiments.

The data-driven statistical ML approach CECD-AS learns the behaviour of normal samples and anomalous samples through model training and adapts over time to effectively detect various kinds of attacks in the cross-layered cyber-

TABLE 1 Performance comparison of various false data detection methodologies [26]

Method	Accuracy $\mu_{cv} \pm \sigma_{cv}$	Precision $\mu_{cv} \pm \sigma_{cv}$	Recall $\mu_{cv} \pm \sigma_{cv}$	F1-score $\mu_{cv} \pm \sigma_{cv}$
KNN	93.05 ± 02.71	13.36 ± 09.24	03.94 ± 03.35	04.64 ± 02.97
MLPNN	78.04 ± 20.64	08.75 ± 11.98	20.89 ± 24.21	05.29 ± 04.09
GNB	49.81 ± 38.06	28.26 ± 38.50	51.35 ± 39.73	07.94 ± 04.47
ADT	45.56 ± 22.03	05.66 ± 02.33	57.84 ± 23.87	09.54 ± 01.54
SVC	55.68 ± 25.75	11.46 ± 12.14	60.57 ± 22.11	14.89 ± 06.75
SE [11]	94.07 ± 00.25	36.56 ± 02.15	80.64 ± 02.21	57.03 ± 01.92
CD [24]	04.88 ± 00.24	04.88 ± 00.24	99.07 ± 00.00	09.31 ± 00.43
ECD [25]	97.28 ± 01.40	46.52 ± 28.03	44.08 ± 29.63	55.42 ± 27.71
ECD-AS [26]	**99.35** ± 00.45	**87.24** ± 09.30	**86.94** ± 09.87	**92.54** ± 05.74

Abbreviations: KNN, K Nearest Neighbor; MLPNN, Multilayer Perceptron Neural Network; GNB, Gaussian Naive Bayes; ADT, Adaptive Boosting with Decision Trees; SVC, Support Vector Classifier.

TABLE 2 Performance results for MFDI, MDoS and MITM attacks (ECD-AS: Ensemble CorrDet with Adaptive Statistics [26]

Attack type	Method	Layer	Information	Accuracy $\mu_{cv} \pm \sigma_{cv}$	Precision $\mu_{cv} \pm \sigma_{cv}$	Recall $\mu_{cv} \pm \sigma_{cv}$	F1-score $\mu_{cv} \pm \sigma_{cv}$
MITM	ECD-AS	Network	PC	92.50 ± 00.21	91.62 ± 00.26	86.43 ± 00.29	**88.95 ± 00.23**
MFDI	ECD-AS	Smart grid	SG	99.36 ± 00.27	99.99 ± 00.01	87.35 ± 5.10	93.16 ± 03.00
		Network	IAT	98.58 ± 00.10	77.85 ± 00.86	99.99 ± 00.01	87.54 ± 00.54
			TD	99.16 ± 00.04	85.56 ± 00.75	99.99 ± 00.01	92.22 ± 00.43
	CECD-AS	Cross-Layer	[SG, IAT, TD]	99.96 ± 00.01	99.41 ± 00.31	99.89 ± 00.14	**99.65 ± 00.16**
C-MFDI	ECD-AS	Smart grid	SG	96.58 ± 00.78	99.94 ± 00.15	32.15 ± 13.39	47.13 ± 15.08
		Network	IAT	97.19 ± 00.44	70.50 ± 02.93	76.02 ± 08.27	72.82 ± 05.32
			TD	96.27 ± 00.45	61.12 ± 02.64	68.73 ± 08.47	64.60 ± 05.09
	CECD-AS	Cross-Layer	[SG, IAT, TD]	99.83 ± 00.06	97.04 ± 01.12	99.77 ± 00.16	**98.38 ± 00.61**
MDoS	ECD-AS	Smart grid	SG	52.63 ± 00.78	34.08 ± 01.03	37.06 ± 04.15	35.41 ± 02.23
		Network	IAT	99.98 ± 00.01	99.96 ± 00.01	99.99 ± 0.01	99.98 ± 00.01
			TD	94.83 ± 00.13	87.28 ± 00.35	99.99 ± 00.01	93.20 ± 00.20
	CECD-AS	Cross-layer	[SG, IAT, TD]	99.83 ± 00.06	99.71 ± 00.08	99.82 ± 00.17	**99.76 ± 00.09**
MFDI-MDoS	ECD-AS	Smart grid	SG	69.58 ± 01.98	28.96 ± 01.12	24.84 ± 01.92	26.66 ± 00.81
		Network	IAT	90.53 ± 00.22	70.16 ± 01.32	99.99 ± 00.01	82.46 ± 00.01
			TD	98.81 ± 00.03	94.94 ± 00.29	99.99 ± 00.01	97.40 ± 00.15
	CECD-AS	Cross-Layer	[SG, IAT, TD]	99.64 ± 00.06	98.47 ± 00.27	99.96 ± 00.06	**99.21 ± 00.14**

Abbreviations: CECD-AS, cross-layer ensemble CorrDet with adaptive statistics; C-MFDI, coordinated multiple false data injection attacks; IAT, inter arrival time; MDoS, multiple denial of service attacks; MFDI, multiple false data injection attacks; MITM, man in the middle attacks; PC, packet count; SG, smart grid measurements; TD, transmission delay.

physical SG systems. This claim is supported by the high F1-scores for MFDI, MDoS and MFDI-MDoS attacks in Table 2. It is important to note that for these datasets, three out of the four methods tested are using new information when compared to the state of the art (SG Information) [26]. Inter-arrival time and TD information is tested individually along with the full CECD-AS framework to show that the most comprehensive and efficient method for cyberattack detection is to combine the SG, IAT, and TD data. CECD-AS detects MITM attacks using the PC dataset and the performance metrics are shown in Table 2. MITM attacks can only be detected from the data collected at network communication layer as the attack does not impact any measurement values at the SG layer. We recorded values of accuracy, precision, recall and F1-score for all the cross validation experiments, and Table 2 shows the mean (μ_{cv}) and standard deviation (σ_{cv}) values for each of these metrics, where high value of μ_{cv} and low value of σ_{cv} is favourable.

Figure 6 shows the values of decision scores and thresholds obtained using SE and CECD-AS approaches for the C-MFDI

dataset. The SE approach only provides a single decision score for the entire 118-bus system for each testing sample, in opposition to the proposed CECD-AS which, due to its distributed nature, provides a decision score for each bus system. The SE approach also results in a static decision threshold for the entire 118-bus system whereas the CECD-AS approach results in adaptive threshold for each bus system. In the considered C-MFDI attack dataset, bus 10 was targeted to inject false data. Figure 6(b) shows the decision score and adaptive threshold obtained from CECD-AS approach for bus 10. As an illustration, we also show decision score and adaptive threshold for a bus that was not subjected to any C-MFDI attacks in Figure 6(c). Decision scores which are above threshold are considered to be attacked samples and are compared with the ground truth to generate the performance results shown in Table 2.

For every new incoming sample $\mathbf{z}$, the threshold values τ_m are inferred from the most recent β normal samples before it. The smaller value of β limits the number of past normal samples used to estimate anomaly threshold and would reduce the accuracy of detection as it would fail to capture the dynamically changing state in the data. The large value for β would allow us to use more number of normal past samples but would add additional cost in storing and processing higher amount of data for every new incoming sample. This motivates us to pick an optimal value of β through validation experiments, and we selected the value of β considering both F1-score of detection on unseen data and computation time. In Figure 7, F1-score mostly increases with increasing beta but after beta reaches 90 the value of F1-score does not change by significant amount. Meanwhile, computation time increases exponentially with increasing values of beta. We choose the value of beta with high F1-score and fairly low overall testing computation time as the optimal value.

We can observe, from Table 3, the physics-based SE approach [56] fails to consistently detect different types of attacks in the cyber-physical SG systems, which is evident by the low F1-scores for MFDI, MDoS and MFDI-MDoS attacks. Most of the literature on SG bad data analysis research focusses on the recall metric, detecting as many of the FDI attacks as possible. Therefore, it makes sense the SE has a very high recall score. However, there is a relatively high rate of FPs in the SE results, which when coupled with the fact that most samples are normal, leads to a low precision and F1 score, even when only analysing MFDI attacks. For the datasets that include DoS attacks, the scores are bad all around since the DoS attack has little to no impact on the actual measurement data. This means an

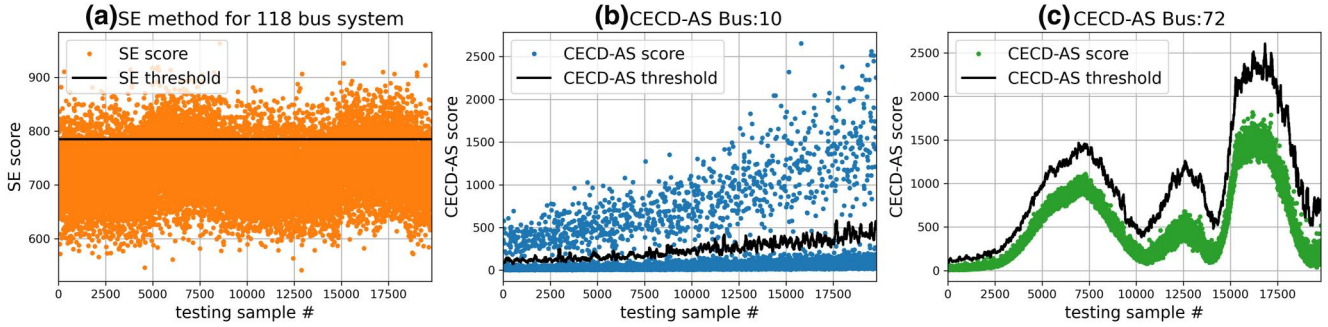

FIGURE 6 Comparison of SE and Cross-Layer Ensemble CorrDet with Adaptive Statistics (CECD-AS) methods through corresponding decision score and decision thresholds for Coordinated Multiple False Data Injection (C-MFDI) attacks

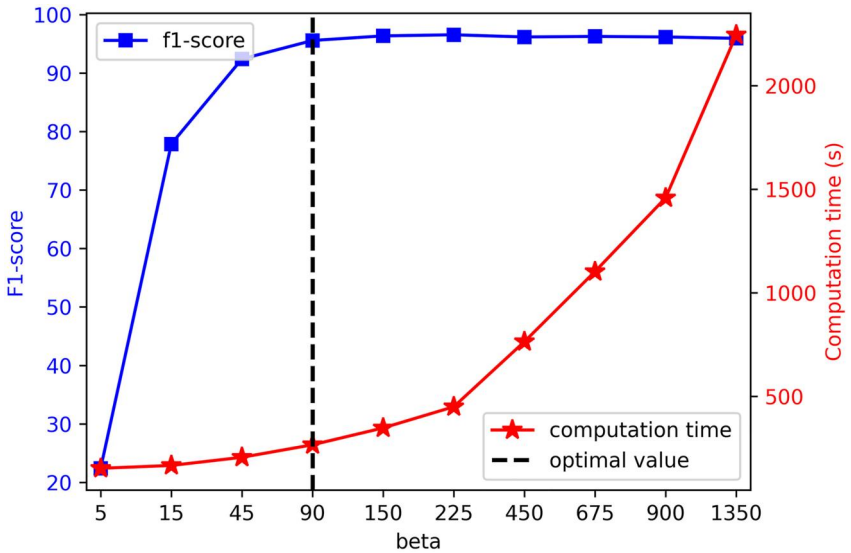

FIGURE 7 Selection of optimal value for the beta based on F1-score and computation time

TABLE 3 Performance results for physics-based SE [56]

Attack type	Accuracy	Precision	Recall	F1-score
MFDI	92.76	41.34	99.45	58.41
MDoS	63.42	32.81	07.43	12.12
MFDI-MDoS	75.18	38.37	16.95	23.51

Abbreviations: MDoS, multiple denial of service attacks; MFDI, multiple false data injection attacks.

attacker can be flooding the communication network with almost no detection by the SE.

For MFDI attacks, although accuracy values for individual datasets (SG, IAT, and TD) are close to the accuracy value for cross-layered dataset, F1-score gives a better picture of the model performance as it strikes better balance between precision and recall for the datasets with imbalanced class size. We can observe that the cross-layered approach results in much higher mean F1-score (99.65) compared to the individual datasets.

For C-MFDI attacks, the ECD-AS approach fails to detect anomalies with high performance resulting in low F1-scores especially with SG measurements as the SG layer is more affected by coordinated attacks on the grid compared to the network layer. As the proposed CECD-AS takes information from both SG measurements and network layer data, it can capture most of the anomalies resulting in a mean F1-score of 98.38.

For MDoS attacks, the mean F1-score for SG dataset is low due to the fact that MDoS attacks have little to no impact on the measurement values from the SG layer but higher impact on the parameters in network communication layer in the cyber-physical SG systems. Hence, CECD-AS results in high mean F1-scores for the datasets collected at the network layer (IAT and TD). The cross-layered approach also results in similar performance as the individual datasets from the network communication layer.

For MFDI-MDoS attacks, the SG dataset fails to give high mean F1-score due to the presence of MDoS attacks, and it is evident from Table 2 that the cross-layered approach results in higher mean F1-score (99.21). Performance metric values from Table 2 show that the proposed cross-layered approach can detect various kinds of attacks in cyber-physical SG systems with high F1-scores as the model will learn from the datasets obtained from both SG and network communications layers. Inter-arrival time and TD datasets have resulted in higher recall values for different attack types compared to cross-layered approach but they also result in low precision values (high FP). Hence, results from Table 2 show that the proposed cross-layered approach results in both lower FP and FN generally compared to results obtained from considering individual datasets from the SG layer or the network communication layer.

5 | CONCLUSION

This paper presents a cross-layered approach for enhancing the detection of different potential cyberattacks on the SG. The state of the art solutions consider only FDI attacks as the source of influencing measurement data (voltages and powers). However, this paper showed that measurements can be affected through the use of communication network. Such an attack limits the ability of detecting bad data when considering measurement data alone. Hence, the novelty of the cross-layer strategy is the integration of data from communication network as another source of data beside measurements is collected from SG in order to improve the anomaly detection scheme for real time monitoring. The CECD-AS reflects the inter-dependency between the power grid and communication network.

The cross-layer strategy framework was implemented on the IEEE 118 bus system. Test results show that the proposed CECD-AS can detect attacks such as Multiple False Data Injections, MDoS and MITM with high F1-score compared to approaches which use data from individual layers in the cyber-physical SG systems. The improved performance of the proposed framework can be attributed for its ability to understand normal and anomalous data behaviour at both the SG layer (using voltage/power measurements) and network communication layer (using IATs, TD and traffic volume values) with a cross-layered perspective. The trained CECD-AS model decides whether a given sample is normal or anomalous and adapts its statistics in matter of milliseconds, so the proposed system can be implemented in real time monitoring of cyber-physical SG systems.

NOMENCLATURE

COMMUNICATION NETWORK

$\boldsymbol{\beta}$	Parameter used for measuring degree of LRD in autocorrelation functions
	Window size for threshold update
$\boldsymbol{\epsilon}_t$	White noise distribution of X_t
$\boldsymbol{\lambda}$	Packet arrival rate into system
$\boldsymbol{\mu}$	Packet service rate at each system
	Mean of normal samples
ϕ	Scaling function in autoregressive integrated moving average
$\boldsymbol{\psi}$	Mother wavelet function in autoregressive integrated moving average
$\boldsymbol{\sigma}$	The scale parameter in the generalised Pareto distribution
	Measurement Standard Deviation
$\boldsymbol{\sigma}_t$, $\boldsymbol{\sigma}_t^2$	Standard deviation and variance of X_t
$\boldsymbol{\xi}$	The shape parameter in the generalised Pareto distribution
$\overline{G}_{\boldsymbol{\xi},\boldsymbol{\sigma\mu}}(x)$	Standard cumulative distribution function of generalised Pareto distribution
H	Hurst parameter used to measure the degree of long-range dependence
	Jacobian Matrix of h
IAT	Inter-arrival times
$L(\bullet)$	Slowly varying function where $lim_{x\to\infty}\frac{L(tx)}{L(x)}=1$ for all $t>0$
n	Total number of packets
p_{util}	Use of the queueing system (i.e. traffic intensity)
PC	packet count (i.e. traffic volume)

TD Transmission delay
W Total waiting time or transmission delays
X_t, X_i A series of datapoints ordered by time

MACHINE LEARNING

α Weight parameter
β Window size for threshold update
δ_m^{ECD} Squared Mahalanobis distance of sample $\mathbf{z}$ with respect to the distribution of normal samples on ϕ_m
η Magnitude parameter for threshold estimation
$\boldsymbol{\delta}_{Z,m}$ Squared Mahalanobis distance of all training samples with respect to ϕ_m
$\boldsymbol{\delta}_{z_k}$ Squared Mahalanobis distance of kth testing sample with respect to Φ_E
$\hat{\mathbf{Y}}$ Label for testing set
$\mathbf{Z}$ Testing set
$\boldsymbol{\mu}$ Mean of normal samples
$\boldsymbol{\mu}_m$ Mean of normal samples on ϕ_m
$\boldsymbol{\Sigma}$ Covariance of normal samples
$\boldsymbol{\Sigma}_m$ Covariance of normal samples on ϕ_m
$\mathbf{Y}$ Label for training set
$\mathbf{Z}$ Training set
$\mathbf{z}$ Triplet, the complete set of triple elements $[\mathbf{z}_{SG}, \mathbf{z}_{IAT}, \mathbf{z}_{TD}]$
$\mathbf{z}^{(c)}$ Triplet element, $\left[\mathbf{z}_{SG}^{(c)}, \mathbf{z}_{IAT}^{(c)}, \mathbf{z}_{TD}^{(c)}\right]$
$\mathbf{z}_m$ Selected triplet element, a set of triple elements with respect to ϕ_m
$\mathbf{z}_{IAT}$ Vector of all inter-arrival time values
$\mathbf{z}_{SG}$ Vector of all measurement values
$\mathbf{z}_{TD}$ Vector of all time delay values
$\mu_{thr,m}$ Mean of the Mahalanobis distance values of $\mathbf{z}_m$ of all normal samples in training data
Φ_E Symbol for Cross-Layer Ensemble CorrDet detector
ϕ_m Symbol for mth local Cross-Layer CorrDet detector
Φ_R Symbol for CorrDet detector
$\sigma_{thr,m}$ Covariance of the Mahalanobis distance values of $\mathbf{z}_m$ of all normal samples in training data
τ Threshold value to classify abnormal samples on Φ_R
τ_m Threshold value to classify abnormal samples on ϕ_m
d Number of measurement or inter-arrival time or time delay values
M Number of buses/local Cross-Layer CorrDet detector
T Set of τ_m

STATE ESTIMATION

χ^2 Chi-Squared Threshold
$\mathbf{e}_D$ Detectable Error Vector
$\mathbf{e}_U$ Undetectable Error Vector
$\mathbf{e}$ Measurement Error Vector
$\mathbf{r}$ Residual of Measurements Vector
$\mathbf{x}*$ Current State Estimation
$\mathbf{x}$ State Vector
$\mathbf{z}_{SG}$ Measurement Vector
$\mathbf{z}_{SG}^*$ Current Measurement Estimation
σ Measurement Standard Deviation
CME Composed Measurement Error
d Number of Measurements
H Jacobian Matrix of h
h Function of Measurements in terms of States
II Measurement Innovation Index
J WLS-SE objective function
N Number of States
P WLS-SE Projection Matrix
p Chi-Squared Probability
R Covariance Matrix of Measurements

ACKNOWLEDGEMENT

This material is based upon work supported by the National Science Foundation under Grant Number 1809739.

CONFLICT OF INTEREST

Author declare no conflict of interest.

DATA AVAILABILITY STATEMENT

The data that support the findings of this study are available from the corresponding author upon reasonable request.

ORCID

Allen Starke https://orcid.org/0000-0001-7080-5750

REFERENCES

1. Farag, M., Azab, M., Mokhtar, B.: Cross-layer security framework for smart grid: physical security layer. In: IEEE PES Innovative Smart Grid Technologies Europe (ISGT Europe), pp. 1–7. IEEE (2014)
2. Volz, D.: U.s. Government Concludes Cyber Attack Caused ukraine Power Outage. Reuters (2016)
3. Fairley, P.: Upgrade Coming to Grid Cybersecurity in u.S. IEEE Spectrum (2016)
4. Cyber-attack against Ukrainian Critical Infrastructure, The Cybersecurity and Infrastructure Security Agency (2018)
5. Blackout 2003: Final Report on the August 14, 2003 Blackout in the united states and canada: Causes and Recommendations, U.S.-Canada Power System Outage Task Force (2004)
6. Morgan, S.: Major Cyber Attack on u.S. Power Grid Is Likely. Forbes (2016)
7. Perez, E.: First on Cnn: U.S. Investigators Find Proof of Cyberattack on ukraine Power Grid. CNN (2016)
8. Zetter, K.: An Unprecedented Look at Stuxnet, the World's First Digital Weapon. Wired.com (2014)
9. Handschin, E., et al.: Bad data analysis for power system state estimation. IEEE Trans. Power Apparatus Syst. 94(2), 329–337 (1975)
10. Bretas, N., Bretas, A., Piereti, S.: Innovation concept for measurement gross error detection and identification in power system state estimation. IET Gener., Transm. Distrib. 5(6), 603–608 (2011)
11. Bretas, N.G., Bretas, A.S.: The extension of the gauss approach for the solution of an overdetermined set of algebraic non linear equations. IEEE Trans. Circuits and Systems II: Express Briefs. 65(9), 1269–1273 (2018)
12. Bretas, A.S., Bretas, N.G., Carvalho, B.E.: Further contributions to smart grids cyber-physical security as a malicious data attack: proof and properties of the parameter error spreading out to the measurements and a relaxed correction model. Int. J. Electr. Power Energy Syst. 104, 43–51 (2019)

13. Bretas, N.G., Bretas, A.S., Martins, A.C.P.: Convergence property of the measurement gross error correction in power system state estimation, using geometrical background. IEEE Trans. Power Syst. 28(4), 3729–3736 (2013)
14. Bretas, A., et al.: Cyber-Physical Power Systems State Estimation, vol. 1. Elsevier (2021)
15. Deng, Y., et al.: Real-time detection of false data injection attacks based on load forecasting in smart grid. In: 2019 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), pp. 1–6. (2019)
16. Kallitsis, M.G., Bhattacharya, S., Michailidis, G.: Detection of false data injection attacks in smart grids based on forecasts. In: 2018 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), pp. 1–7. (2018)
17. Ashok, A., Govindarasu, M., Ajjarapu, V.: Online detection of stealthy false data injection attacks in power system state estimation. IEEE Trans. Smart Grid. 9(3), 1636–1646 (2018)
18. Zhang, C., et al.: Modeling and defending advanced metering infrastructure subjected to distributed denial-of-service attacks. IEEE Trans. Netw. Sci. Eng., 1 (2020)
19. Irshad, A., Ibrar, N.K., Riaz, M.: Reliable and secure advanced metering infrastructure for smart grid network. In: 2018 International Conference on Computing, Electronic and Electrical Engineering (ICE Cube), pp. 1–6. (2018)
20. Zhang, Z., et al.: Delay-tolerant predictive power compensation control for photovoltaic voltage regulation. IEEE Trans. Ind. Inf. 17(7), 4545–4554 (2021)
21. De Pace, G., et al.: Evaluation of communication delay based attack against the smart grid. In: 2020 IEEE Kansas Power and Energy Conference (KPEC), pp. 1–6. (2020)
22. Kushal, T.R.B., et al.: Causal chain of time delay attack on synchronous generator control. In: 2020 IEEE Power Energy Society General Meeting (PESGM), pp. 1–5. (2020)
23. Fritz, J.J., et al.: Simulation of man in the middle attack on smart grid testbed. In: 2019 SoutheastCon, pp. 1–6. (2019)
24. Trevizan, R.D., et al.: Data-driven physics-based solution for false data injection diagnosis in smart grids. In: 2019 IEEE PES GM (2019)
25. Ruben, C., et al.: Hybrid data-driven physics model-based framework for enhanced cyber-physical smart grid security. IET Smart Grid. (2019)
26. Nagaraj, K., et al.: Ensemble corrdet with adaptive statistics for bad data detection. IET Smart Grid (2020)
27. Monsanto, C., et al.: Composing software defined networks. In: 10th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 13), pp. 1–13. (2013)
28. Kopeikin, A., et al.: Multi-uav network control through dynamic task allocation: ensuring data-rate and bit-error-rate support. In: 2012 IEEE Globecom Workshops, pp. 1579–1584. IEEE (2012)
29. Almadani, B., Beg, A., Mahmoud, A.: Dsf: a distributed sdn control plane framework for the east/west interface. IEEE Access. 9, 26735–26754 (2021)
30. Vizarreta, P., et al.: Dason: dependability assessment framework for imperfect distributed sdn implementations. IEEE Trans. Netw. Service Manag. 17(2), 652–667 (2020)
31. Maziku, H., et al.: Diversity modeling to evaluate security of multiple sdn controllers. In: 2018 International Conference on Computing, Networking and Communications (ICNC), pp. 344–348. IEEE (2018)
32. Amaral, P.: Machine learning in software defined networks: data collection and traffic classification. In: 2016 IEEE 24th International Conference on Network Protocols (ICNP). ICNP
33. Sudar, K.M., et al.: Detection of distributed denial of service attacks in sdn using machine learning techniques. In: 2021 International Conference on Computer Communication and Informatics (ICCCI), pp. 1–5. IEEE (2021)
34. Kwon, J., et al.: Automatic classification of network traffic data based on deep learning in onos platform. In: 2020 International Conference on Information and Communication Technology Convergence (ICTC), pp. 1028–1030. IEEE (2020)
35. Pérez-Díaz, J.A., et al.: A flexible sdn-based architecture for identifying and mitigating low-rate ddos attacks using machine learning. IEEE Access. 8, 155859–155872 (2020)
36. Nagaraj, K., et al.: State estimator and machine learning analysis of residual differences to detect and identify fdi and parameter errors in smart grids. In: 2020 52nd North American Power Symposium (NAPS), pp. 1–6. (2021)
37. Moayyed, H., et al.: Image Processing Based Approach for False Data Injection Attacks Detection in Power Systems, pp. 1. IEEE Access (2021)
38. Mohamed, A.S., et al.: False data injection attacks against synchronization systems in microgrids. IEEE Trans. Smart Grid. 12(5), 4471–4483 (2021)
39. Nagaraj, K., Starke, A., McNair, J.: Glass: a graph learning approach for software defined network based smart grid ddos security. In: ICC 2021 - IEEE International Conference on Communications, pp. 1–6. (2021)
40. James Ranjith Kumar, R., Sikdar, B.: Detection of stealthy cyber-physical line disconnection attacks in smart grid. IEEE Trans. Smart Grid. 12(5), 4484–4493 (2021)
41. Palmer, M., Kathrine, G.J.W., Jebapriya, S.: Comprehensive analysis of smart grid security with intelligent machine learning based framework. In: 2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS), vol. 1, pp. 307–313. (2021)
42. Halgamuge, M.N.: Latency estimation of blockchain-based distributed access control for cyber infrastructure in the iot environment. In: 2021 IEEE 16th Conference on Industrial Electronics and Applications (ICIEA), pp. 510–515. (2021)
43. Basnet, M., et al.: Ransomware detection using deep learning in the scada system of electric vehicle charging station. In: 2021 IEEE PES Innovative Smart Grid Technologies Conference - Latin America (ISGT Latin America), pp. 1–5. (2021)
44. Su, Z., et al.: Secure and efficient federated learning for smart grid with edge-cloud collaboration. IEEE Trans. Ind. Inf. 18(2), 1333–1344 (2022)
45. Jain, R., Routhier, S.: Packet trains–measurements and a new model for computer network traffic. IEEE J. Sel. Area. Commun. 4(6), 986–995 (1986)
46. Haviv, M.: Queues: A Course in Queueing Theory. Springer (2015)
47. Cintuglu, M.H., et al.: A survey on smart grid cyber-physical system testbeds. IEEE Commun. Surv. Tutorials. 19(1), 446–464 (2017)
48. Humayed, A., et al.: Cyber-physical systems security—a survey. IEEE Internet Things J. 4(6), 1802–1831 (2017)
49. Qiu, L., et al.: Wireless injection attacks based on fake data injection in tinyos. In: 2015 Seventh International Symposium on Parallel Architectures, Algorithms and Programming (PAAP), pp. 236–242. (2015)
50. Gao, J., et al.: Research about dos attack against icps. Sensors. 19, 1542 (2019)
51. Zhan, Z.: A Statistical Framework for Analyzing Cyber Attacks. Master's thesis, University of Texas (2014).report
52. Embrechts, P., Klüppelberg, C., Mikosch, T.: Modelling Extremal Events - for Insurance and Finance: Paul Embrechts
53. Cryer, J.D., Chan, K.-s.: Time Series Analysis with Applications in R. Springer (2011)
54. Bretas, N.G., Bretas, A.S.: A two steps procedure in state estimation gross error detection, identification, and correction. Int. J. Electr. Power Energy Syst. 73, 484–490 (2015). https://doi.org/10.1016/j.ijepes.2015.05.044
55. Bretas, N.G., et al.: A geometrical view for multiple gross errors detection, identification, and correction in power system state estimation. IEEE Trans. Power Syst. 28(3), 2128–2135 (2013). https://doi.org/10.1109/pesmg.2013.6673061
56. Bretas, A.S., et al.: Smart grids cyber-physical security as a malicious data attack: an innovation approach. Elec. Power Syst. Res. 149, 210–219 (2017). https://doi.org/10.1016/j.epsr.2017.04.018
57. Ho, K., Gader, P.D.: A linear prediction land mine detection algorithm for hand held ground penetrating radar. IEEE Trans. Geosci. Rem. Sens. 40(6), 1374–1384 (2002). https://doi.org/10.1109/tgrs.2002.800276

58. Ho, K.C., Gader, P.D.: Correlation-based land mine detection using gpr. In: Detection and Remediation Technologies for Mines and Minelike Targets V, vol. 4038, pp. 1088–1096. International Society for Optics and Photonics (2000)
59. Chang, C.-I., Chiang, S.-S.: Anomaly detection and classification for hyperspectral imagery. IEEE Trans. Geosci. Rem. Sens. 40(6), 1314–1325 (2002). https://doi.org/10.1109/tgrs.2002.800280
60. Alvey, B., et al.: Adaptive coherence estimator (ace) for explosive hazard detection using wideband electromagnetic induction (wemi). In: Detection and Sensing of Mines, Explosive Objects, and Obscured Targets XXI, vol. 9823, pp. 982309. International Society for Optics and Photonics (2016)
61. Zimmerman, R.D., Murillo-Sanchez, C.E., Thomas, R.J.: Matpower: steady-state operations, planning, and analysis tools for power systems research and education. IEEE Trans. Power Syst. 26(1), 12–19 (2011). https://doi.org/10.1109/tpwrs.2010.2051168
62. Fontes, R.R., et al.: Mininet-wifi: emulating software-defined wireless networks. In: 11th International Conference on Network and Service Management (CNSM), pp. 384–389. IEEE (2015)
63. Ettercap Home Page.
64. Godbole, S., Sarawagi, S.: Discriminative methods for multi-labeled classification. In: Pacific-Asia Conference on Knowledge Discovery and Data Mining, pp. 22–30. Springer Berlin Heidelberg, Berlin (2004)

How to cite this article: Starke, A., et al.: Cross-layered distributed data-driven framework for enhanced smart grid cyber-physical security. IET Smart Grid. 1–19 (2022). https://doi.org/10.1049/stg2.12070