Neural Computing and Applications (2023) 35:4835–4854
https://doi.org/10.1007/s00521-021-06106-3

S.I. : MACHINE LEARNING APPLICATIONS FOR SECURITY

Deep-learning-based data-manipulation attack resilient supervisory backup protection of transmission lines

Astha Chawla[1] · Prakhar Agrawal[2] · Bijaya Ketan Panigrahi[1] · Kolin Paul[2]

Received: 6 January 2021 / Accepted: 5 May 2021 / Published online: 4 June 2021

Abstract

Cyber-attacks on smart-grid systems have become increasingly more complicated, and there is a need for taking detection and mitigation measures to combat their adverse effects on the smart-grid infrastructure. Wide area measurement system (WAMS) infrastructure comprising of phasor measurement units (PMUs) has recently shown remarkable progress in solving complex power system problems and avoiding blackouts. However, WAMS is vulnerable to cyber-attacks. This paper presents a novel cyber-attack resilient WAMS framework incorporating both attack detection and mitigation modules that ensure the resiliency of PMU data-based supervisory protection applications. It includes deep learning-based Long Short Term Memory (LSTM) model for real-time detection of anomalies in time-series PMU measurements and isolating the compromised PMUs followed by Generative Adversarial Imputation Nets (GAIN) for the reconstruction of the compromised PMU's data. The corrected PDC data-stream is then forwarded to the decision-making end application, making it resilient against attacks. A Random Forrest classifier is used in the end application to distinguish fault events from other disturbances and supervise the third zone of distance relay for backup protection of transmission lines. The efficacy of the proposed framework for different attack scenarios has been verified on the WSCC 9-Bus System modeled on a developed real-time digital simulator (RTDS)-based integrated cyber-physical WAMS testbed. Experimental analysis shows that the proposed model successfully detects and mitigates attacks' adverse effects on the end application.

Keywords Smart grid · Phasor measurement units (PMU) · Cyber-security · Long-short term memory (LSTM) · Generative adversarial imputation nets (GAIN) · Detection · Mitigation · Supervision of backup relays

1 Introduction

In recent years, the power industry has undergone a significant reinvention phase with increased emphasis on distributed generation and deregulated electricity markets. Advancements in information and communication technologies have led to new emerging technologies that have revolutionized this century-old physical grid into a cyber-physical grid. Modern power systems thus face new complexities and are usually operating near the stability margin limits. Though such systems are equipped with several protection schemes, they encounter maloperation situations leading to cascading events, which might even lead to a blackout. Investigations have shown that 75% of significant cascade events leading to blackouts are due to backup protection relays' maloperations. Power blackouts can create economic, political, and social distress in a country.

A newly evolved wide-area monitoring system (WAMS) providing fast and highly accurate timestamped synchrophasors is capable of solving complex protection problems and avoid cascading events and blackouts in the smart grid. WAMS comprises GPS synchronized phasor measurement units (PMUs) spread across the grid to acquire data and send it to phasor data concentrators (PDCs). PMUs in the power system send timestamped phasors (magnitude and angle) of current, voltage, frequency, and rate of change of frequency (ROCOF), wrapped in IEEE std. C37.118 protocol to the PDC. PDC then synchronizes phasor data received from multiple

✉ Astha Chawla
astha.chawla@ee.iitd.ac.in

[1] Electrical Engineering Department, Indian Institute of Technology Delhi, New Delhi 110016, India

[2] Computer Science and Engineering Department, Indian Institute of Technology Delhi, New Delhi 110016, India

PMUs and produces a time-aligned output datastream at every timestamp which is used in various wide-area monitoring, protection, and control (WAMPAC) applications. Along with real-time protection and control of the smart grid, synchrophasors provide a dynamic view of the grid, enhancing situational awareness of the system [1, 2].

1.1 Motivation and incitement

Various research efforts have shown the efficacy of synchrophasors in the supervision of the third zone of distance relays for backup protection of transmission lines and preventing their maloperations. Classical and machine learning-based approaches have been extensively used for this purpose [3–9]. However, these works have ignored the vulnerability of the WAMS network to cyber-attacks and have presumed the integrity and availability of PMU data.

Recent studies have highlighted potential vulnerabilities in WAMS, and their adverse impacts on synchrophasor data-based applications [10, 11]. Authors have also shown the adverse effects of PMU data unavailability on 'Adaptive Relaying' application in their previous work [12]. A survey conducted by the North American Synchrophasor Initiative (NASPI) society stated that most of the components installed in WAMS networks are not designed considering cyber-security aspects [13]. Also, no security requirements are specified by the IEEE C37.118.2 standard used for synchrophasor data [14]. Cyber-attacks on the WAMS network targetting data integrity and availability can drive various data-driven approaches for supervising the backup protection of transmission lines into erroneous decision making, thereby endangering the power system's stability. Reports of cyber-attacks on electricity-grids and energy facilities like the infamous Ukraine attack (December 2015), which targeted 30 substations [15] has well established that the power grid and its applications are vulnerable to cyber-attacks. Though attack resiliency of SCADA applications is ensured using synchrophasors [16, 17], limited research addresses WAMPAC applications' resilience, especially time-critical protection applications. This motivated the authors to develop an attack resilient WAMS framework, including detection and mitigation mechanisms to make time-critical wide area protection applications resilient against false data injection attacks (FDIA) and ensure their proper functioning.

1.2 Related work

Cyber vulnerabilities in WAMS have led to a considerable amount of work towards improving the resilience of monitoring and control applications against FDIA. The majority of such works deal with the detection of FDIA. Yu et al. [18] used a combination of wavelet transform and deep neural networks to address detection of FDIA in AC State Estimation (SE). Ghafouri et al. [19] proposed detection of FDIA in voltage stability monitoring schemes using indicators obtained from Thevenin Equivalent (TE) parameters of the power system network. However, the approach is complex for larger systems and not suitable for time-critical WAMPAC applications. Recently, Chakhchoukh et al. [20] proposed robust S-based EKF to detect random errors and FDIA targeting AC dynamic state estimation. Wang et al. [21] addressed FDIA detection in the WAMS network using a deep autoencoder model. Further, continuous monitoring of equivalent impedances of transmission lines is also used as an indicator of FDIA [22]. However, the effectiveness of these approaches is also not discussed for WAMPAC applications having strict time requirements. Musleh et al. [23] used the Kalman filter scheme's temporal prediction attribute for mitigation of FDIA and attack resiliency of wide area control applications. Khalid et al. [24] addressed mitigation of FDIA and resilience of oscillation monitoring using the Bayesian Algorithm. Thus, very limited works have addressed the mitigation of FDIA attacks, and none of these works have dealt with attack resiliency of time-critical wide area protection applications.

1.3 Work done and contribution

Based on the limited research works in FDI attack mitigation and attack resiliency of time-critical wide area protection applications, a novel attack resilient WAMS framework with both attack detection and mitigation modules is presented in this work. The framework uses a combination of Long Short Term Memory (LSTM) network and domain knowledge for detecting malicious activity in the data coming from different PMUs in PDC datastream at any tth timestamp and isolating the compromised PMU's data, if any. Incoming continuous phasors from all n PMU at tth timestamp are passed through trained LSTM blocks to predict corresponding phasors at every $(t+1)$th timestamp. The predicted phasors for each PMU are compared with incoming real-time phasors at each timestamp, and threshold violations are monitored. Based on errors from LSTM blocks and domain knowledge, PMU is declared compromised and is isolated. Healthy data from the remaining PMUs at that tth timestamp is then forwarded to the Generative Adversarial Imputation Nets (GAIN)-based mitigation module, which reconstructs the data corresponding to the compromised PMU and forwards it to the end application. This ensures PMU data-based supervisory protection applications' resiliency against cyber-attacks and helps them effectively prevent relay maloperations.

Given the importance of integrated cyber-physical analysis for cyber-security studies [25], RTDS-based cyber-physical hardware-in-the-loop (HIL) WAMS testbed is used to evaluate the performance of the proposed work. A series of comprehensive case studies are presented to show the effectiveness of the framework during cyber-attacks. The salient features of the presented work include

1. The proposed framework provides both attack detection and mitigation solutions based on deep learning models for WAMPAC applications. It also includes a machine learning-based approach for the chosen end application, i.e., PMU data-based supervisory backup protection of transmission lines.
2. The detection module in the framework isolates the compromised PMU and prevents the corrupted data from being used by the end decision-making applications. With this knowledge, the grid operator can effectively put time and resources to combat the compromised devices efficiently.
3. The mitigation module fixes the corrupted data, which reduces the impact of cyber-attacks on the end application, failing the attacker's malicious intent. It also helps in continuous and proper working of critical applications during events of cyber-attacks.
4. The framework uses a data-dependent approach and is independent of the model of specific power system components. Thus, it can be applied to a wide range of systems, rendering better adaptability and scalability.
5. Attack resilient performance of time-critical synchrophasor-assisted backup protection of transmission line with this proposed framework is also discussed.

1.4 Paper organization

Section 2 discusses the attack scenarios used in this work and elaborates on the reasons behind the choice of LSTM and GAIN architectures. Section 3 elaborates the working of the proposed attack resilient WAMS framework incorporating the LSTM-based detection module and GAIN-based mitigation module along with the supervisory protection application. Section 4 documents the proposed framework's implementation details, data generation, and time complexities involved in practical implementation. Section 5 discusses the results highlighting the proposed framework's effectiveness, ensuring the resiliency of synchrophasor-based supervision of backup protection of transmission lines against cyber-attacks. Scalability aspects are also discussed in this Section. Finally, Section 6 concludes the paper.

2 Pre-requisites

2.1 Attack model

Data manipulation attacks, also known as FDI attacks, are popular attack strategies that involve alteration of data flowing through a network to elicit a response from the system, which can lead to failures. Data manipulation attacks in power systems target PMU data integrity by changing certain voltage and currents values, which are extremely important for the proper working of WAMPAC applications. Such attacks can involve manipulating one or two critical phasors from a PMU or introducing deviations in all the phasors received from a PMU. In the latter type of data manipulation attacks, mathematical relationships among different measurements from a PMU are maintained. A replay attack is one such type of attack, where an attacker blocks original data from a PMU and replays some previously captured power contingency data. Such an attack can make the system operator make wrong decisions, severely impacting the power system's stability. In literature, PMU measurements are also manipulated by injecting pulse and ramp signals. Based on the amount of deviation introduced in PMU's measurements, data manipulation attacks have been categorized into three categories [18], namely strong, weak, and moderate attacks as follows

- *Strong attacks* Data Manipulation attack is considered strong when the average voltage magnitude deviation exceeds 10% of the nominal value, and the average voltage angle deviation exceeds 8°.
- *Weak attacks* When average deviations in voltage magnitude are smaller than 3% of their nominal values and voltage angle deviations are smaller than 2°, the attack is referred to as weak.
- *Moderate attacks* Here, the average voltage magnitude deviation is between 3% and 10%, and the average voltage angle deviation is between 2° and 8° of nominal values, respectively.

2.2 Approach to solution—Choice of architectures

The idea for the proposed FDIA resilient WAMS framework with attack detection and mitigation approaches involves two algorithms

1. A model to predict the time-series continuous and dynamic power system data at every timestamp and use it together with the domain knowledge to detect malicious activity in any PMU data.

2. A model which can understand and learn the regularities or patterns and complex relationships among PMU data available from across the grid at any timestamp and impute data (with same characteristics and distribution) of attacked and compromised PMU(s).

There exist many approaches for handling the task of time series prediction and data imputation. However, the choice for the selection of LSTM and GAIN for these purposes, respectively, is influenced by the following reasons

2.2.1 Long short-term memory (LSTM) for predicting time-series PMU data

From the several classical approaches that exist for predicting time-series data, Autoregressive Integrated Moving Average (ARIMA) has shown the best results in predicting univariate data. However, it yields better results in forecasting short-term data. Also, it fails to capture the non-linear patterns in the time series [26]. Recently, neural networks (NN) models have become preferable for predicting seasonal time series because of their better performance than these classical techniques. Extreme learning machine (ELM) neural network and its variants have shown promising results in data prediction. However, ELM involves randomly initialized and fixed input weights, and thus their prediction results are sometimes inherently unreliable [27]. Further, such NN models cannot capture sequential information in the input data, and with the increase in the dimension of the training data, the network performance of these algorithms deteriorates. In the presence of bulk dynamic power system training data, deep learning models have shown better performance in predicting both short-term and long-term data. Such models are preferable for continued detection during prolonged attacks and have shown greater accuracy on previously unseen data.

LSTMs being a class of recurrent neural networks (RNN), are explicitly developed for time-series forecasting and are capable of learning order dependence in time-series sequence prediction problems. LSTMs have feedback connections that allow them to process entire sequences of data, unlike other standard neural networks and deep learning algorithms that process single data points. LSTMs exhibit significant improvement in performance for preserving long-time dependencies while also keeping short-time memories. A standard LSTM unit consists of a cell, and three gates, namely the input gate ***i***, output gate ***o***, the forget gate ***f***, as shown in Fig. 1. These gates regulate the flow of information in the cell based on the following Eqs. (1–6) [28, 29].

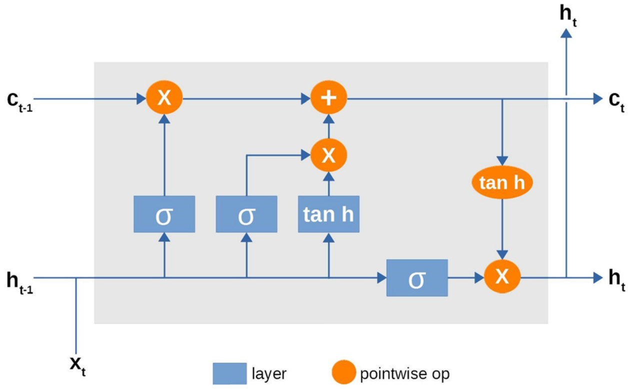


Fig. 1 Typical LSTM cell architecture

$$\boldsymbol{f_t} = \sigma_g(\boldsymbol{W_f x_t} + \boldsymbol{U_f h_{t-1}} + \boldsymbol{b_f}) \tag{1}$$

$$\boldsymbol{i_t} = \sigma_g(\boldsymbol{W_i x_t} + \boldsymbol{U_i h_{t-1}} + \boldsymbol{b_i}) \tag{2}$$

$$\boldsymbol{o_t} = \sigma_g(\boldsymbol{W_o x_t} + \boldsymbol{U_o h_{t-1}} + \boldsymbol{b_o}) \tag{3}$$

$$\boldsymbol{c_t^*} = \sigma_c(\boldsymbol{W_c x_t} + \boldsymbol{U_c h_{t-1}} + \boldsymbol{b_c}) \tag{4}$$

$$\boldsymbol{c_t} = \boldsymbol{f_t} \cdot \boldsymbol{c_{t-1}} + \boldsymbol{i_t} \cdot \boldsymbol{c_t^*} \tag{5}$$

$$\boldsymbol{h_t} = \boldsymbol{o_t} \cdot \sigma_c(\boldsymbol{c_t}) \tag{6}$$

Here, t denotes the time-step, and the sigmoid (σ_g) and tangent (σ_c) functions are used to calculate the respective activation vectors for each gate, as indicated in the LHS. ***c*** stands for the cell state vector, while $\boldsymbol{c}^*$ represents the cell input activation vector. ***W*** ***U***, and ***b*** denote the weight matrices and bias parameters, respectively, that need to be trained using the input vectors ***x***. The $(\cdot)$ operator is the element-wise product.

LSTMs have proved to be very promising solution to sequence and time-series related problems and are therefore chosen for predicting PMU data in our detection approach. Even though recently developed different variants of LSTM claim to offer better accuracy in prediction, basic and less complex LSTM network has performed sufficiently well to solve the problem at hand and is therefore used.

2.2.2 Generative adversarial imputation nets (GAIN) for PMU data imputation

Machine learning models have shown significantly improved performance in imputing data compared to classical statistical approaches for dynamic bulk data. Simple machine learning techniques such as K-Means and K-Nearest Neighbours perform decently to recover missing PMU data. However, they may not give an accurate result for an infrequent power event (absent in the historical data) as it does not understand the complex relationships among data. Generative class of imputation methods like expectation-maximization (EM) requires modeling of different components and is not suitable for large power systems and real-time imputation tasks [12, 30]. Deep-learning algorithms' capability to understand hidden and complex relationships among data variables helps them in reconstructing data (with same characteristics and distribution) accurately and hence are better in dealing with missing data.

Generative adversarial imputation nets (GAINs) are a class of deep-learning models for missing data imputation [31]. They learn the regularities or patterns and the relationship among measurements from different PMUs spread across the grid. A GAIN model is derived from standard generative adversarial networks (GAN) [32] by slightly modifying its structure. Along with the generator and the discriminator submodels (modeled as fully connected neural nets) as present in the GAN architecture, GAIN also has a mask matrix, random matrix, and hint matrix to aid in data imputation. The generator model observes the original data vector (which has some missing values) and imputes the missing features based on actual observed data. This completed vector is sent to the discriminator model, which that predicts which features were imputed (from the generator model) and those which were observed. The generator receives a mask matrix that provides information about which values were missing in the original datastream and need to be imputed. A random matrix is also input to the generator to add randomness to the imputed values. Further, the discriminator receives additional information in the form of a hint matrix along with the imputed matrix, which reveals partial information about the missing data in the original data. This ensures that the discriminator forces the generator to generate an imputed matrix according to the true underlying data distribution.

The generator submodel in GAIN ensures that the imputed output values for missing components successfully fool the discriminator submodel. The adversarial training of the model increases their accuracy and makes them robust. They can learn the hidden data distribution very well, and the feedback loop between the generator and the discriminator yields very high accuracy results. Other deep learning models like denoising autoencoders have also shown to work well in imputing missing data. However, they need complete data for training. In contrast, GAIN can learn even when complete data are unavailable. Various experiments with real-world datasets have shown that GAINs have outperformed other state-of-the-art imputation techniques and deep-learning-based approaches and hence have been chosen in the proposed framework [31].

3 Cyber-attack resilient WAMS framework

In the conventional WAMS framework, a time-aligned output datastream from PDC at any tth timestamp as given in (7) is used by the real-time decision-making WAMPAC applications. It consists of timestamped phasors of positive-sequence voltage p^t_{nv1}, positive-sequence transmission line current p^t_{nI1}, and frequency p^t_{nf} from nth PMU where $n = (1, 2, ..N)$ PMUs spread across the grid. However, if this data are corrupted or unavailable, it adversely impacts the end applications' performance.

$$\begin{aligned}\boldsymbol{p^t_{qi}} = {} & [p^t_{1v1}, p^t_{1I1}, p^t_{1f}, p^t_{2v1},\\ & p^t_{2I1}, p^t_{2f}, \cdots p^t_{Nv1}, p^t_{NI1}, p^t_{Nf}]\end{aligned} \tag{7}$$

In the proposed attack resilient WAMS framework, the PDC datastream at each tth timestamp passes through the deep-learning-based attack detection and mitigation software modules shown in green blocks before being forwarded to the end application as shown in Fig. 2. LSTM and domain knowledge-based attack detection module helps in finding and isolating the compromised PMU data. Based on this detection module's output, the GAIN-based mitigation module reconstructs the compromised data and forwards the imputed datastream or original datastream to the end application. This reduces the impact of data manipulation attacks on WAMPAC applications, thereby increasing their resiliency during attacks.

3.1 Long short-term memory (LSTM)-based anomaly detection module

This module helps identify the PMUs with compromised data in a PDC datastream at any tth timestamp and isolating them so that they do not impact the working of end WAMPAC applications. It consists of LSTM blocks connected in parallel to the output phasors from each PMUs in the PDC datastream. A separate LSTM block $LSTM_{ni}$ is used for each ith time-series phasor variable from nth PMU that needs to be forecasted. Thus, each PMU in the PDC datastream has 5 LSTM blocks operating in parallel for forecasting phasors of F, $V1$, $\delta V1$, $I1$, and $\delta I1$, as shown in Fig. 3. Similar LSTM blocks work on the corresponding variables for each PMU in the network, and hence a total of $(5 * N)$ LSTM blocks are used for N PMUs. The forecasted values from all the LSTM blocks are used to calculate the error ER^D_{ni} between the predicted and observed values of phasor data, where D denotes the detection module, $n = (1, 2, \ldots N)$ with N being the total number of PMUs reporting to PDC, and i refers to the phasor data columns (F, $V1$, $\delta V1$, $I1$, $\delta I1$) from each PMU. The LSTM blocks used a window size of 10, using values at the last ten timestamps to predict the next value. If this error ER^D_{ni}

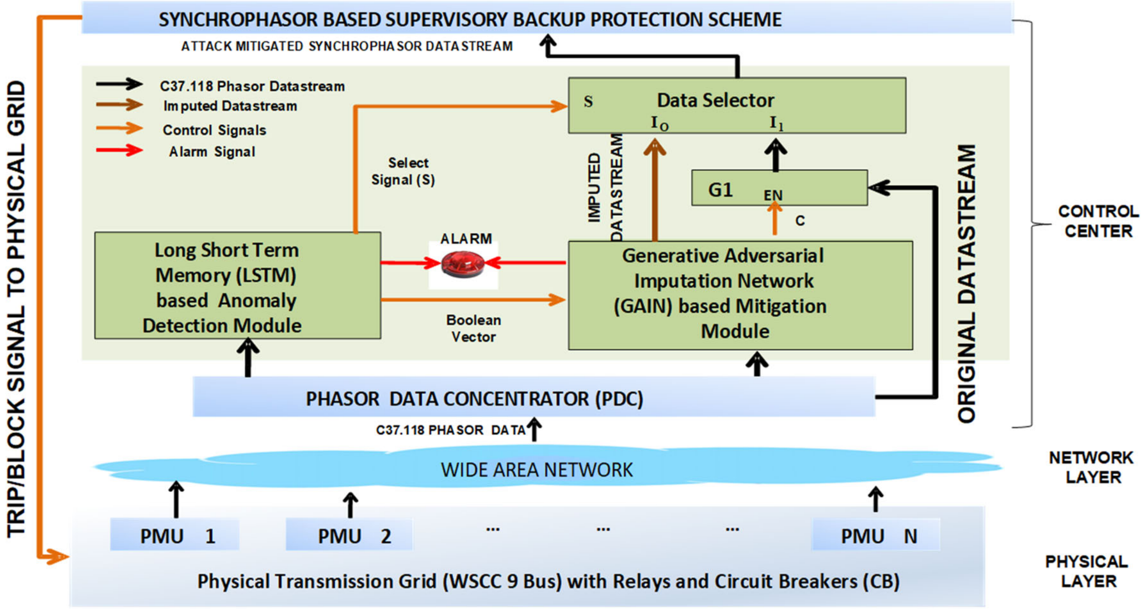
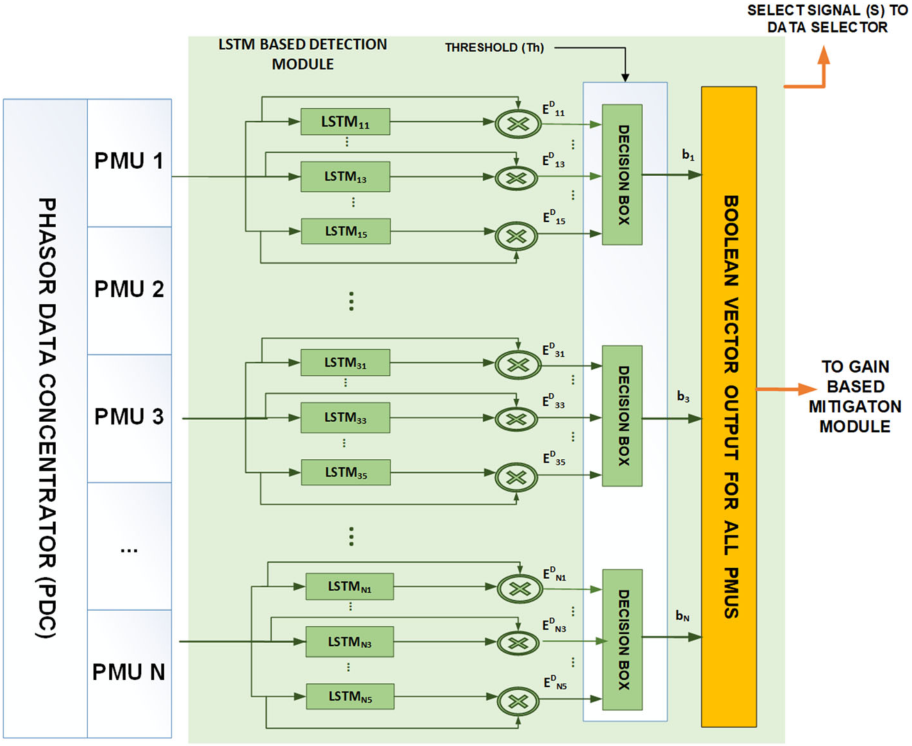

SYNCHROPHASOR BASED SUPERVISORY BACKUP PROTECTION SCHEME
ATTACK MITIGATED SYNCHROPHASOR DATASTREAM
C37.118 Phasor Datastream
Imputed Datastream
Control Signals
Alarm Signal
Select Signal (S)
Data Selector
S
I0
I1
IMPUTED DATASTREAM
G1
EN
C
ALARM
Long Short Term Memory (LSTM) based Anomaly Detection Module
Boolean Vector
Generative Adversarial Imputation Network (GAIN) based Mitigation Module
ORIGINAL DATASTREAM
CONTROL CENTER
TRIP/BLOCK SIGNAL TO PHYSICAL GRID
PHASOR DATA CONCENTRATOR (PDC)
C37.118 PHASOR DATA
WIDE AREA NETWORK
NETWORK LAYER
PMU 1
PMU 2
PMU N
Physical Transmission Grid (WSCC 9 Bus) with Relays and Circuit Breakers (CB)
PHYSICAL LAYER

Fig. 2 Proposed data manipulation attack resilient WAMS framework

Fig. 3 The architecture of LSTM-based attack detection module



corresponding to any of the five LSTMs of a particular *n*th PMU is above a certain threshold T_h ($>0.05\%$ of observed value), it indicates that *n*th PMU data is being compromised, and the decision box gives boolean output ‘0’ corresponding to that *n*th PMU. When errors ER^D_{ni} for all the LSTM blocks of the *n*th PMU are within the threshold limit, the boolean output of ‘1’ is given out from the decision box of the nth PMU. This detection module combines the boolean values b_n from all *N* decision boxes at any *t*th timestamp and forms a bool output vector of size $[1 \times N]$ for *N* PMUs in PDC datastream as given in (8). A value of ‘0’ indicates an anomaly, while ‘1’ means that the PMU data is correct.

$$\text{Bool vector}^t = \begin{array}{cccc} PMU1 & PMU2 & \cdots & PMUN \\ b_1 & b_2 & \cdots & b_N \end{array} \tag{8}$$

This bool output vector from the detection module is sent to the GAIN-based mitigation module, where it is used for forming the mask vector, which helps in reliable imputation of data from the mitigation module. The inferences drawn from values in this bool vector, as discussed below, also decide the select signal S for the data selector.

3.1.1 Inference 1

The boolean output of '0' corresponding to some PMUs indicates data manipulation or DoS attack on that PMU's data. Due to the interconnected nature of the physical grid, any power contingency in the grid will change the whole system's dynamics and impact the data from all the PMUs. However, the amount of change in data will vary from large to minimal amounts for different PMUs depending on the event's location. This will lead to noticeable errors ER^D from all the PMUs. Thus, the violation of errors from some and not all the PMUs indicates the compromised nature of that PMU. In this case, the mask vector of size $[1 \times 5N]$ in the GAIN-based mitigation module contains '0' corresponding to all the five measurements from compromised PMUs while '1' corresponding to all the five measurements from healthy PMUs in the PDC datastream. Since the original PDC datastream is compromised, select value $S = 0$ is sent to the data selector, allowing the imputed datastream from the GAIN-based mitigation module at its I_0 input to be used by the end applications as shown in Fig. 2.

3.1.2 Inference 2

Bool output vector containing '0's corresponding to all the PMUs due to mismatch in received and forecasted values from all LSTM blocks may mean anomaly in data from all the PMUs. However, it does not guarantee that an attack was executed, as a sudden unexpected change in measurements from all PMUs can also result from a physical contingency like fault in the system. Alternatively, the bool vector might contain all '1's corresponding to all the PMUs, indicating no anomaly in any time-series phasor data from any of the PMUs. However, a ramp attack executed in small amounts on any PMU's data in consecutive timestamps will also go undetected by LSTM blocks. Thus, the detection module will output a bool vector containing '1' for all PMUs. In both these situations, the custom mask vector of size $[1 \times 5N]$ is generated with '0' corresponding to all measurements from any randomly selected PMU while '1' corresponding to measurements from other PMUs. Since LSTM-based detection module has not declared any PMU as compromised, select signal $S = 1$ is sent to the data selector, allowing the original PDC datastream at its I_1 input to be used by the end application if passed by gate G1 as shown in Fig. 2.

3.2 Generative adversarial imputation nets (GAIN)-based mitigation module

This module consists of the GAIN model, which serves as an imputer and reconstructs missing or manipulated PMU values to direct non-corrupted data to the end application. The architecture of this module is shown in Fig. 4. This module receives the bool vector from the LSTM-based detection module and based on its values corresponding to each PMU, it generates a mask vector of size $[1 \times 5N]$ for five phasor data columns (F, $V1$, $\delta V1$, $I1$, $\delta I1$) from N PMUs at each tth timestamp as given in (9). The standard GAIN architecture is modified to incorporate multivariate data from each PMU and ensure that missingness is introduced to all phasor data columns of a particular PMU simultaneously i.e., a mask vector is first created corresponding to N columns (N is the number of PMUs in the system). Each column is then repeated k times (k is the number of phasor data columns from each PMU). The hint and random vectors are also appropriately modified to account for PMU data.

$$\boldsymbol{Maskvector^t} = \begin{array}{cccc} PMU1 & PMU2 & \cdots & PMUN \\ m_1\ m_2\ \cdots\ m_5 & m_1\ m_2\ \cdots\ m_5 & \cdots & m_1\ m_2\ \cdots\ m_5 \end{array} \tag{9}$$

The data vector and the mask vector are then given to the generator model, which returns the imputed datastream $\boldsymbol{r^t_{ni}}$ at tth timestamp as output as given in Eq. (10), where i = (1,2 ...5) denotes the index of the phasor data column from nth PMU with a total of N PMUs spread across the grid.

$$\begin{aligned} \boldsymbol{r^t_{ni}} = [&r^t_{11}, r^t_{12}, , r^t_{15}, \\ &r^t_{21}, r^t_{22}, \cdots r^t_{25}, \cdots r^t_{N1}, r^t_{N2}, , r^t_{N5}] \end{aligned} \tag{10}$$

Corresponding to the two inferences obtained from LSTM-based detection module, GAIN-based mitigation module works as explained below.

3.2.1 Case 1

When bool vector from LSTM-based detection module at tth timestamp declares some of the PMUs as compromised, the generated mask vector contains '0' corresponding to all measurements from the compromised PMUs while measurements from other healthy PMUs are marked '1'. Following this, the values of compromised PMUs in the original PDC datastream are replaced with '0' irrespective of their original values, and data vector is formed. Both

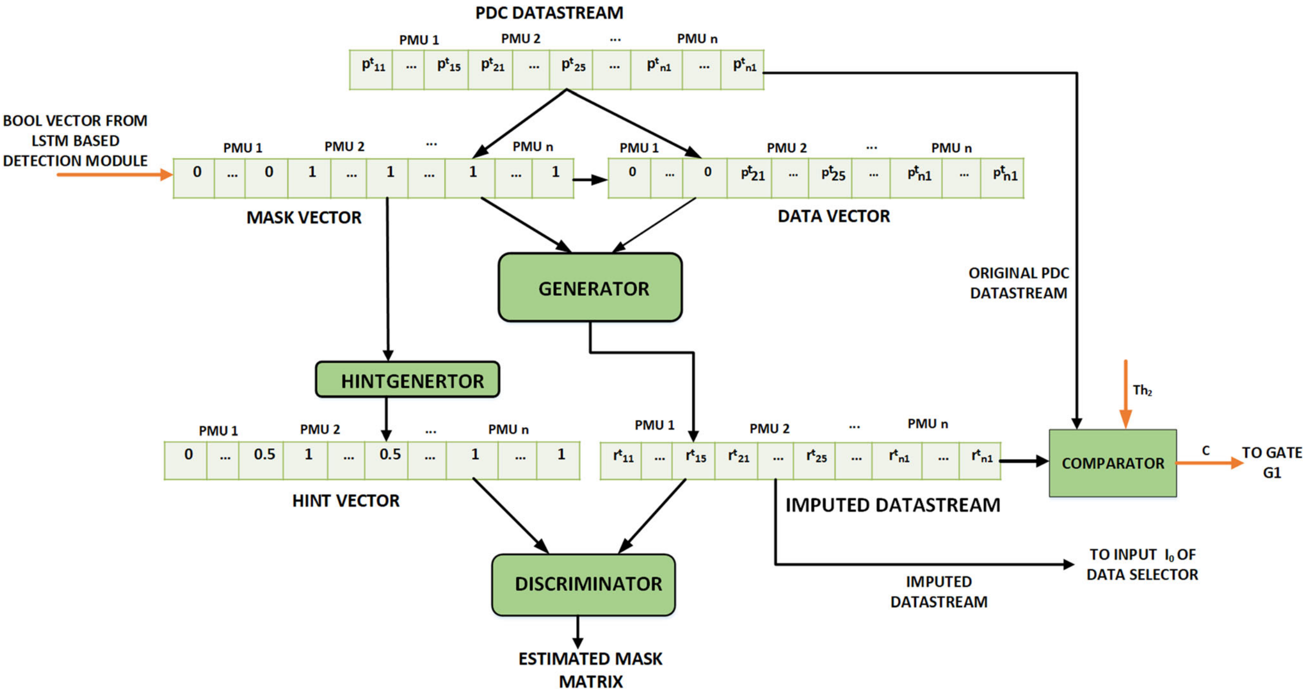

PDC DATASTREAM
PMU 1
PMU 2
...
PMU n
p^t_{11} ... p^t_{15} p^t_{21} ... p^t_{25} ... p^t_{n1} ... p^t_{n1}
BOOL VECTOR FROM LSTM BASED DETECTION MODULE
0 ... 0 1 ... 1 ... 1 ... 1
MASK VECTOR
0 ... 0 p^t_{21} ... p^t_{25} ... p^t_{n1} ... p^t_{n1}
DATA VECTOR
GENERATOR
ORIGINAL PDC DATASTREAM
HINTGENERTOR
0 ... 0.5 1 ... 0.5 ... 1 ... 1
HINT VECTOR
r^t_{11} ... r^t_{15} r^t_{21} ... r^t_{25} ... r^t_{n1} ... r^t_{n1}
IMPUTED DATASTREAM
Th_2
COMPARATOR
C
TO GATE G1
DISCRIMINATOR
IMPUTED DATASTREAM
TO INPUT I_0 OF DATA SELECTOR
ESTIMATED MASK MATRIX

Fig. 4 The architecture of GAIN-based mitigation module

mask vector and data vector are sent to the generator model which outputs an imputed datastream at tth timestamp. This imputed datastream is sent to the I_0 input of the data selector. Since the original PDC datastream is corrupted as detected by LSTM-based detection module and select signal $S = 0$ is being sent to the data selector, the imputed datastream at I_0 input of the data selector is forwarded to the end application. The mitigation module treats compromised data due to DoS attacks or data manipulation attacks as equivalent by replacing them with ‘0’, as the altered values of the PMUs under attack are inconsequential to the imputation model. Such treatment is possible only due to the novel technique of isolating compromised PMUs by the LSTM-based detection module.

3.2.2 Case 2

When the bool output vector from the LSTM-based detection module has all ‘0’s or all ‘1’s, and no confirmation of an attack situation is seen, a custom mask vector is created for that tth timestamp. This custom mask vector describes the data corresponding to a random PMU as compromised or missing. The corresponding PMU’s measurements in the incoming original PDC datastream are replaced by ‘0s’ and data vector is formed. Corresponding to this, the generator model returns the imputed datastream at tth timestamp with imputed values for this randomly selected PMU. These imputed values are compared to the initially received values in the original PDC datastream in comparator block as shown in Fig. 4, and the calculated percentage errors ER^{Mt}_{ai} corresponding to all measurements of the PMU at tth timestamp are compared to a chosen threshold value Th_2 (>0.03%). M in ER^{Mt}_{ai} denotes the mitigation module, a represents the PMUs with suspicious data, and i refers to the phasor data columns from such PMUs. If all the errors ER^{Mt} are less than the threshold, the mitigation module enables the gate G1 by sending $C = 1$, thereby allowing it to pass the original PDC datastream to the I_1 input of the data selector. Since select signal $S = 1$ is being sent to the data selector in this situation by LSTM-based detection module as already discussed, the original PDC datastream at I_1 input of the data selector is forwarded to the end application.

However, if the errors ER^{Mt} in the comparator block are more than the allowed threshold Th_2, this indicates the presence of manipulated data in the PDC datastream. Hence, the mitigation module sends $C = 0$ to the gate G1, disabling it and blocking the corrupted original datastream from passing through it. Thus, the input I_1 of the data selector does not receive any datastream for this tth timestamp. With the select signal of the data selector being set as $S = 1$, the end application does not receive input from the WAMS framework. Thus, at this stage, when the anomaly in the PDC datastream is present, but the exact compromised PMU is not known, both original datastream and imputed datastream are blocked from being used at the end application to avoid incorrect decision making.

During sophisticated attack scenarios that go undetected by LSTM-based detection module followed by generation of a custom mask vector, there is a possibility that a compromised PMU gets randomly selected to be masked. In this case, the imputed datastream from the GAIN model can possibly be used as expected and observed during the testing phase. However, the error ER^{Mt} violation is observed between the two datastreams in the comparator block corresponding to the masked PMU as the original PDC datastream was corrupted. Alternatively, when an uncompromised PMU gets randomly selected to be masked, the errors ER^{Mt} between measurements from imputed datastream and the original datastream in the comparator block again violates the threshold, which is expected. In both situations, the mitigation module decides to block the malicious data from being used in the end application, avoiding the wrong decision, which might disturb the stability of the power system. Therefore, GAIN-based mitigation module serves as an effective means of reducing the impact of the attack on the end application.

3.3 Application module-Synchrophasor assisted supervision of backup protection of transmission line

Research and investigations have shown that the power blackouts were mainly a result of some kind of disturbances followed by maloperations of the backup distance relays. The backup relays find it challenging to distinguish between the fault condition from other disturbances like heavy loading conditions and power swings. Thus, they misinterpret such situations as a fault and issue a trip signal to circuit breakers, which disconnects the healthy line. Such maloperations of relays have sometimes initiated cascaded trippings in the power grid, leading to a blackout situation. To deal with this problem, it was suggested to supervise these backup relays using synchrophasor measurements from WAMS and enhance the backup protection schemes of power transmission systems. PMU measurements in WAMS have been used to distinguish faulty conditions from other disturbances using various machine learning (ML) and classical approaches in the literature, thereby supervising the 3rd zone of the distance relays and avoiding their maloperations during non-faulty conditions [6–9]. However, correct decision-making using these PMU measurements highly depend on the integrity and availability of the PMU data. The ML algorithms trained to detect faults fail and give wrong decisions on receiving corrupted PMU data, which might endanger the power grid's stability.

In our approach, we have used an ML-based random forest classifier (RF) to detect fault conditions on a transmission line using PMUs data from PDC datastream and supervise the backup relays.It is implemented using Python library 'sci-kit-learn'. The proposed detection and mitigation modules in the proposed framework detect and fixes the compromised PMU data in the PDC datastream, if any, before forwarding it to the RF classifier in the supervisory protection application. The RF classifier then extracts features from this final synchrophasor at any tth timestamp for its decision making. The test power system model is subjected to different power contingencies which include faults, line trips, generator outages, load changes, etc., to prepare a comprehensive dataset for the RF classifier's training. Input features $\boldsymbol{\Delta F} = (\boldsymbol{\Delta X}, \boldsymbol{\Delta Y})$ selected for RF classifier comprises of the difference of positive-sequence voltage (magnitude ($V1$) and angle ($\delta V1$)) and difference of positive-sequence current (magnitude ($I1$) and angle ($\delta I1$)) from PMUs on both ends of the transmission line. Thus, RF classifier uses $\boldsymbol{\Delta X^t}$= $(\Delta\|V1_i\|, \Delta\delta V1_i, \Delta\|I1_i\|, \Delta\delta I1_i)$ and $\boldsymbol{\Delta Y^t}$ = $(\Delta\|V1_j\|, \Delta\delta V1_j, \Delta\|I1_j\|, \Delta\delta I1_j)$ at tth timestamp from PMUs at the ith Bus and jth Bus respectively, connecting ijth transmission line as given in Eqs. (11–12). The target outputs are labeled as 0, 1 corresponding to a fault and No-fault conditions, respectively. After training the RF classifier with the prepared dataset, its testing has been done under different power contingencies and data manipulation attack scenarios with both conventional and proposed WAMS framework.

$$\boldsymbol{\Delta X^t} = \boldsymbol{X_i^t} - \boldsymbol{X_i^{(t-1)}} \tag{11}$$

$$\boldsymbol{\Delta Y^t} = \boldsymbol{Y_j^t} - \boldsymbol{Y_j^{(t-1)}} \tag{12}$$

On detecting a fault condition on a particular transmission line, i.e., when the RF classifier outputs '0', the supervisory protection application module with the RF classifier issues a trip signal for that transmission line. When the RF classifier outputs '1' indicating a no-fault situation on the transmission line, the application module issues a block signal for the circuit breakers (CB) of that line. Thus, when a relay gives wrong trip signals, PMU data-based supervisory decision would save unnecessary trippings of healthy transmission lines and prevent any possibility of cascaded trippings. The flowchart of this proposed scheme is given in Fig. 5.

In the worst possible attack situation when our proposed framework cannot isolate and fix the compromised data, it stops the corrupted PDC data-stream from being used by the RF classifier. In this way, it avoids wrong decisions from the PMU data-based end applications, failing the attackers' malicious intent. Thus, our proposed framework does not deteriorate the performance of the prevailing conventional protection logics. In fact, it enhances the

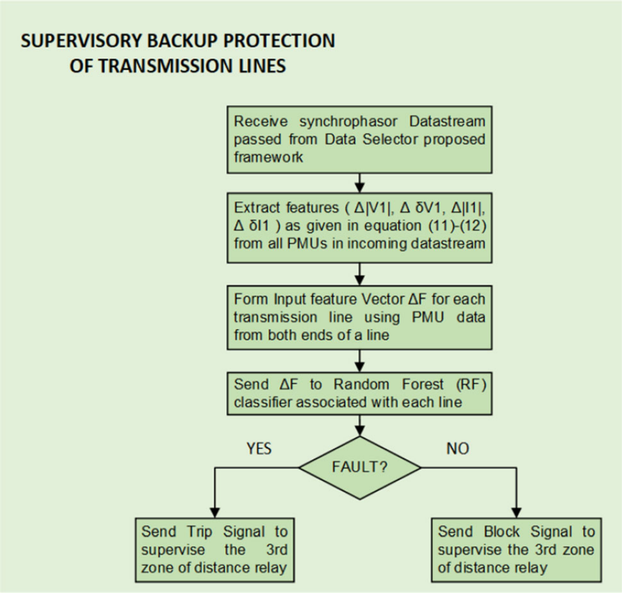

SUPERVISORY BACKUP PROTECTION OF TRANSMISSION LINES
Receive synchrophasor Datastream passed from Data Selector proposed framework
Extract features (Δ|V1|, Δ δV1, Δ|I1|, Δ δI1) as given in equation (11)-(12) from all PMUs in incoming datastream
Form Input feature Vector ΔF for each transmission line using PMU data from both ends of a line
Send ΔF to Random Forest (RF) classifier associated with each line
YES
FAULT?
NO
Send Trip Signal to supervise the 3rd zone of distance relay
Send Block Signal to supervise the 3rd zone of distance relay

Fig. 5 Flowchart of Random Forrest classifier-based supervisory backup protection of transmission lines

resiliency of the synchrophasor data-based supervisory protection logic during data manipulation attacks. Thus, the proposed scheme provides a "win-win" situation.

4 Implementation

4.1 Proposed attack resilient cyber-physical WAMS testbed

Developed RTDS-based cyber-physical WAMS testbed is a three-tier structure consisting of a physical layer, network layer, and control center. The physical layer of the WAMS architecture implements the standard WSCC 9-bus system in RSCAD software of RTDS, as shown in Fig. 6a with hardware and software PMUs placed at all the buses (Bus4, Bus5, Bus6, Bus7, Bus8, and Bus9). The testbed includes one hardware PMU at Bus4, hardwired using the RTDS Analog Output (GTAO) interfacing card of RTDS. The rest of the buses have software GT-NET PMUs. Since GTNET PMUs can give current phasors of only one line, each of the remaining buses has 2 PMUs to provide phasor current values of the two transmission lines connected to them.

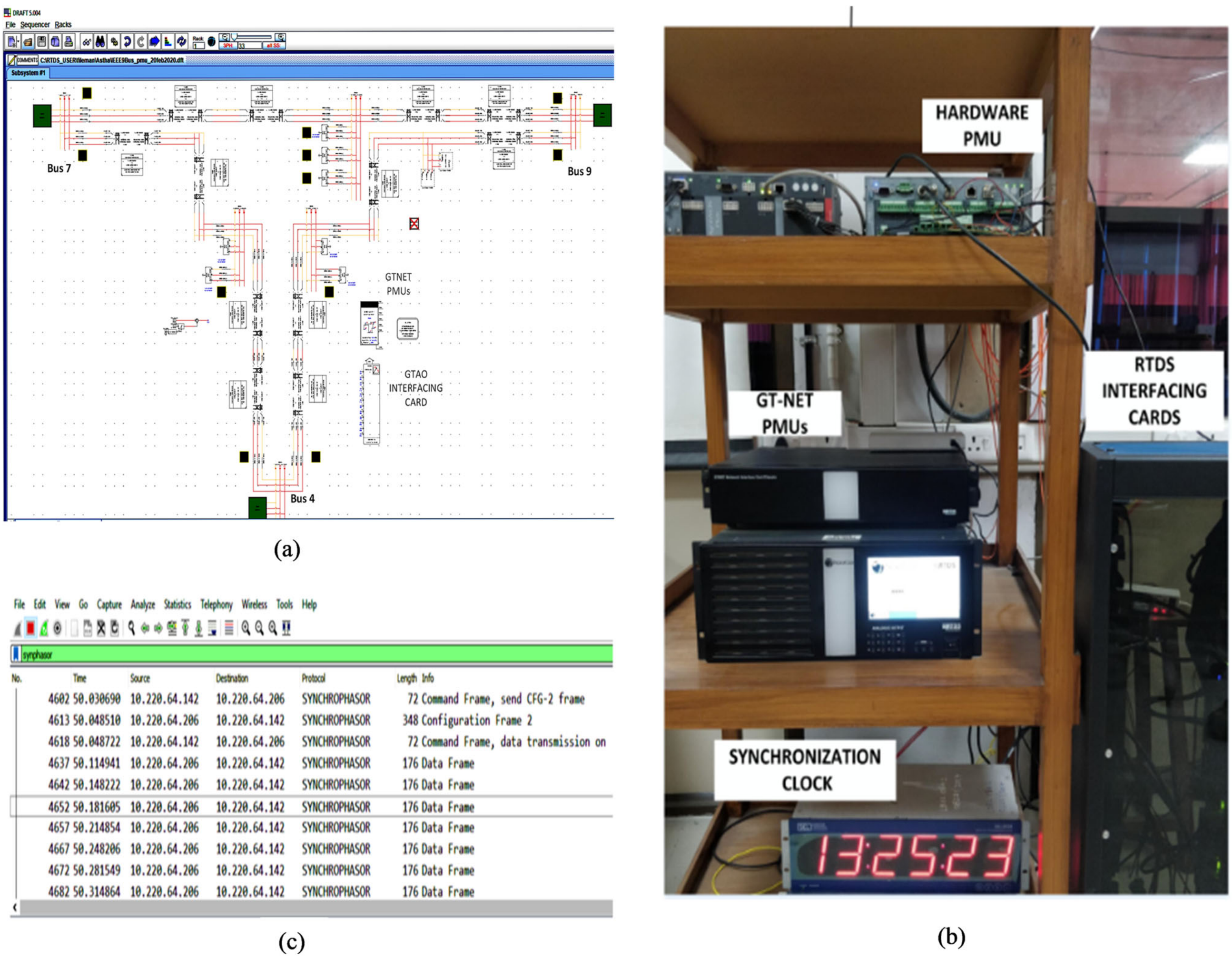
PMUs in WSCC 9 bus system in RTDS send synchrophasor data at 60 frames per second (fps) through LAN via Ethernet network switch (network layer) to software PDC (openPDC) in the control center. All devices in the setup are time-synchronized using a GPS clock. RTDS-based experimental WAMS testbed is shown in Fig. 6b. IEEE Standard C37.118 [14] is used as a communication protocol between PMUs and PDC. Communication between PMUs and PDC consists of four types of message frames, namely (i) Data, (ii) Configuration, (iii) Command, and (iv) Header as shown in Fig. 6c. PDC time synchronizes the phasor data received from multiple PMUs and produces a time-aligned output datastream at every timestamp. LSTM and GAIN models-based software modules in the proposed framework fetches the latest stored datastream at tth timestamp from the PDC's database and operate on it as discussed in Sect. 3. The openPDC, LSTM model, and GAIN model are configured on Windows-based personal computers with an Intel Core i7 CPU working at 3.6 GHz and 32 GB RAM.

4.2 GAIN and LSTM deployment

Both the LSTM and GAIN models are trained using historical PDC data in the format described above, and training has been carried out on data samples equally distributed among steady-state and dynamic events of the power system. The LSTM blocks used are created using the Python TensorFlow library, using two bidirectional LSTM layers with 5 cells each, with Mean Squared Error (MSE) Loss and Adam Optimizer function. The open-source GAIN codebase available on GitHub is used after modifying it according to the changed architecture, as discussed in Sect. 3.2, to make it usable for PDC data. A random mask vector is generated by the model during training, ensuring uniform learning across data features. It is trained with a hint rate of 0.8 and a miss rate of 0.2 for 20,000 iterations. For testing, different attack models discussed were simulated, and their effect on original data was recorded. Then manipulated data were passed through the proposed model, and results for different scenarios are discussed in Sect. 5.

4.3 Time complexities involved in the practical implementation

The deep learning models require extensive training data, and training time varies according to the amount of data and number of iterations or epochs run. While testing, each data sample takes an average of 563 µs to be imputed by the GAIN module, the LSTM blocks take approximately 172 µs for forecasting each data value. The whole framework runs in parallel and takes an average time of around 2 ms for each PDC datastream for complete detection and imputation. Average fixed delay (processing, multiplexing, and transducers) and communication delay (fiber optic cable) in WAMS infrastructure are approximately 100–150 ms [2]. As time-critical protection applications like 'zone-3 of the distance relay for backup protection of transmission lines' operates with an intentional time delay of 1–2 s [33, 34], the proposed attack detection and mitigation



```
No.   Time       Source         Destination    Protocol       Length Info
4602 50.030690  10.220.64.142  10.220.64.206  SYNCHROPHASOR   72 Command Frame, send CFG-2 frame
4613 50.048510  10.220.64.206  10.220.64.142  SYNCHROPHASOR  348 Configuration Frame 2
4618 50.048722  10.220.64.142  10.220.64.206  SYNCHROPHASOR   72 Command Frame, data transmission on
4637 50.114941  10.220.64.206  10.220.64.142  SYNCHROPHASOR  176 Data Frame
4642 50.148222  10.220.64.206  10.220.64.142  SYNCHROPHASOR  176 Data Frame
4652 50.181605  10.220.64.206  10.220.64.142  SYNCHROPHASOR  176 Data Frame
4657 50.214854  10.220.64.206  10.220.64.142  SYNCHROPHASOR  176 Data Frame
4667 50.248206  10.220.64.206  10.220.64.142  SYNCHROPHASOR  176 Data Frame
4672 50.281549  10.220.64.206  10.220.64.142  SYNCHROPHASOR  176 Data Frame
4682 50.314864  10.220.64.206  10.220.64.142  SYNCHROPHASOR  176 Data Frame
```

Fig. 6 **a** WSCC 9-Bus system model in RSCAD **b** RTDS-based experimental WAMS testbed **c** Communication between PMU and PDC using IEEE Standard C37.118 protocol in network monitoring tool Wireshark

scheme can be integrated with conventional WAMS framework to increase the resiliency and improve the performance of 'PMU data-based supervisory backup protection scheme' during cyber-attacks.

5 Results and discussions

The effectiveness of the proposed deep-learning-based modules in increasing the resiliency of the synchrophasor assisted backup protection scheme was tested during various power disturbance events and data manipulation cyber-attacks. Some of these are discussed here in detail. For easier understanding purposes, mitigation module is programmed to always select PMU4 while creating a 'custom mask vector' as required when detection module cannot isolate the compromised PMU. Plots of voltage phasor (magnitude and angle) and frequency are used to show the effectiveness of the imputed datastream from the GAIN model. Scalability aspects of the proposed work are also discussed.

5.1 Performance of the proposed WAMS framework during cyber-attacks

5.1.1 Normal working (no cyber-attack)

The proposed framework should not disrupt the normal working of the WAMS framework when the system is not under attack. End applications should remain unaffected in such conditions. The working of the proposed framework was tested during the following cases to verify this.

1. No power disturbance

   When there is no cyber-attack on any of the PMU's data, and there is no disturbance in the power grid, the proposed framework forwards the original PDC datastream to the end application as expected. The errors

ER^D between the observed values and those predicted by the LSTM blocks in the detection module were less than the specified threshold. Hence, a bool vector having ‘1’s corresponding to all PMUs as given in (13) was obtained and was sent to the GAIN-based mitigation module. A select signal of $S = 1$ was given to the data selector.

$$\boldsymbol{Boolvector} = \begin{array}{cccccc} PMU4 & PMU5 & PMU5' & PMU6 & PMU6' & PMU7 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ & PMU7' & PMU8 & PMU8' & PMU9 & PMU9' \\ & 1 & 1 & 1 & 1 & 1 \end{array} \tag{13}$$

$$\boldsymbol{Maskvector} = \begin{array}{cccccc} PMU4 & PMU5 & PMU5' & PMU6 & PMU6' & PMU7 \\ 00000 & 11111 & 11111 & 11111 & 11111 & 11111 \\ & PMU7' & PMU8 & PMU8' & PMU9 & PMU9' \\ & 11111 & 11111 & 11111 & 11111 & 11111 \end{array} \tag{14}$$

As the detection module did not indicate an error, a custom mask vector with ‘0’s corresponding to PMU4 measurements was created, as given in (14). The mitigation module imputed the data corresponding to this mask and compared it to the values received initially. The corresponding errors ER^M were found to be within the threshold, which enabled the gate G1, allowing the original PDC datastream to be used by the end application. The RF algorithm used measurements from this original PDC datastream and gave a no-fault output as expected.

2. Power disturbance- 3-phase fault on line 2

   As described in the previous case, the proposed framework worked as a conventional framework. However, this time, the RF classifier detects the fault, giving a trip signal as the output. Since the power network is interconnected, disturbance like faults in the physical grid impacts the measurements at all buses, although the amount of change in measurements depends on their location relative to the fault. As a result, the values predicted by all LSTM blocks exceeded the error threshold, and the output from detection module was a bool vector of all ‘0’s corresponding to all PMUs in the PDC datastream, as given in (15). A select signal of $S = 1$ was sent to the data selector, and a custom mask vector was generated, as given in (16).

$$\boldsymbol{Boolvector} = \begin{array}{cccccc} PMU4 & PMU5 & PMU5' & PMU6 & PMU6' & PMU7 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ & PMU7' & PMU8 & PMU8' & PMU9 & PMU9' \\ & 0 & 0 & 0 & 0 & 0 \end{array} \tag{15}$$

$$\boldsymbol{Maskvector} = \begin{array}{cccccc} PMU4 & PMU5 & PMU5' & PMU6 & PMU6' & PMU7 \\ 00000 & 11111 & 11111 & 11111 & 11111 & 11111 \\ & PMU7' & PMU8 & PMU8' & PMU9 & PMU9' \\ & 11111 & 11111 & 11111 & 11111 & 11111 \end{array} \tag{16}$$

The errors ER^M computed between the mitigation module’s imputed measurements and the original PDC datastream were within the threshold. Thus, the original PDC datastream was finally forwarded to the end application through gate G1 and data selector. The imputed data values of all PMU phasors closely resemble the uncompromised original data and can accurately adapt to abrupt changes in the data, making the GAIN model an effective mitigation strategy as shown in Fig. 7.

5.1.2 During data manipulation attack

Data manipulation attacks disturb the integrity of PMU data. An adversary can send false PMU data to the end application indicating some disturbance in the physical grid when there is no such event in reality. In the conventional WAMS framework, this can cause the RF classifier at the end application to send a trip signal to the CB based on the received corrupted data, endangering the power grid’s stability. However, the proposed framework detects and isolates the compromised PMU data and fixes the corrupted data in the PDC datastream so that the end application works accurately. In some complicated attack scenarios like ramp attacks, when the framework cannot detect and isolate the compromised PMU, it instead blocks the PDC datastream, preventing wrong decisions by the end application’s algorithm. Performance of the framework during some such scenarios is discussed below.

1. Step attack on PMU4

   Three different attacks of varying intensities were carried out during a fault on line 2, where data from PMU4 at Bus 4 was modified. An error of 10%, 5%, and 2% of the original values, corresponding to strong, moderate, and weak attack, respectively, was introduced to the values of frequency, positive sequence voltage magnitude, and angle. In all three cases, error values greater than 0.05% were observed in the values predicted by LSTM blocks for PMU4. However, the errors for other PMUs were within the threshold, indicating an attack on PMU4. Thus, the detection module outputs a bool vector with ‘0’ corresponding to PMU4 and ‘1’ corresponding to all other PMUs given in (17) and a select signal $S = 0$ to the data selector. On receiving this bool vector, the mask vector as given in (18) was formed. The mitigation module returned an imputed datastream with reconstructed data

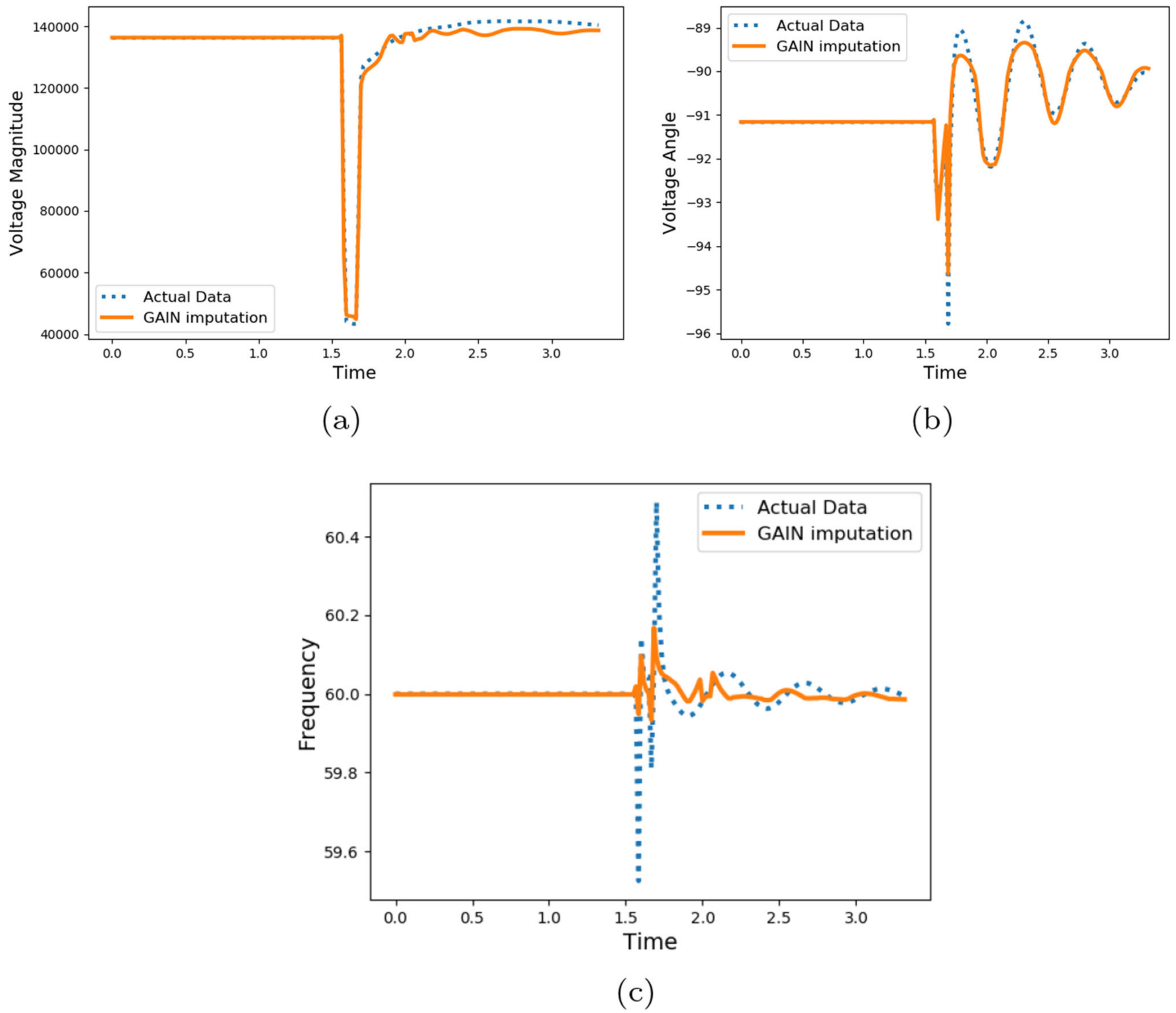


Fig. 7 Predicted and observed measurements of **a** Voltage magnitude, **b** Voltage angle, and **c** Frequency during a fault on line 2

corresponding to PMU4 in strong attack, moderate attack and weak attack scenarios, as shown in Fig. 8, Fig. 9, and Fig. 10, respectively. This imputed datastream is transferred to the end application where RF correctly classifies fault or non-fault situations, preventing relay maloperation.

$$\boldsymbol{Boolvector} = \begin{array}{cccccc} PMU4 & PMU5 & PMU5' & PMU6 & PMU6' & PMU7 \\ 0 & 1 & 1 & 1 & 1 & 1 \\ & PMU7' & PMU8 & PMU8' & PMU9 & PMU9' \\ & 1 & 1 & 1 & 1 & 1 \end{array} \tag{17}$$

$$\boldsymbol{Maskvector} = \begin{array}{cccccc} PMU4 & PMU5 & PMU5' & PMU6 & PMU6' & PMU7 \\ 00000 & 11111 & 11111 & 11111 & 11111 & 11111 \\ & PMU7' & PMU8 & PMU8' & PMU9 & PMU9' \\ & 11111 & 11111 & 11111 & 11111 & 11111 \end{array} \tag{18}$$

2. Replay attack on PMU4

   A replay attack was conducted on the data of PMU4, where data recorded during a fault on line 2 was used to replace its data during normal system operation. In a conventional WAMS framework, such an attack would cause the system to send a trip signal when it was not required, leading to maloperations. However, in the proposed framework, the LSTM blocks in the detection framework detected this change on PMU4 data, and since the errors for other PMUs were within the

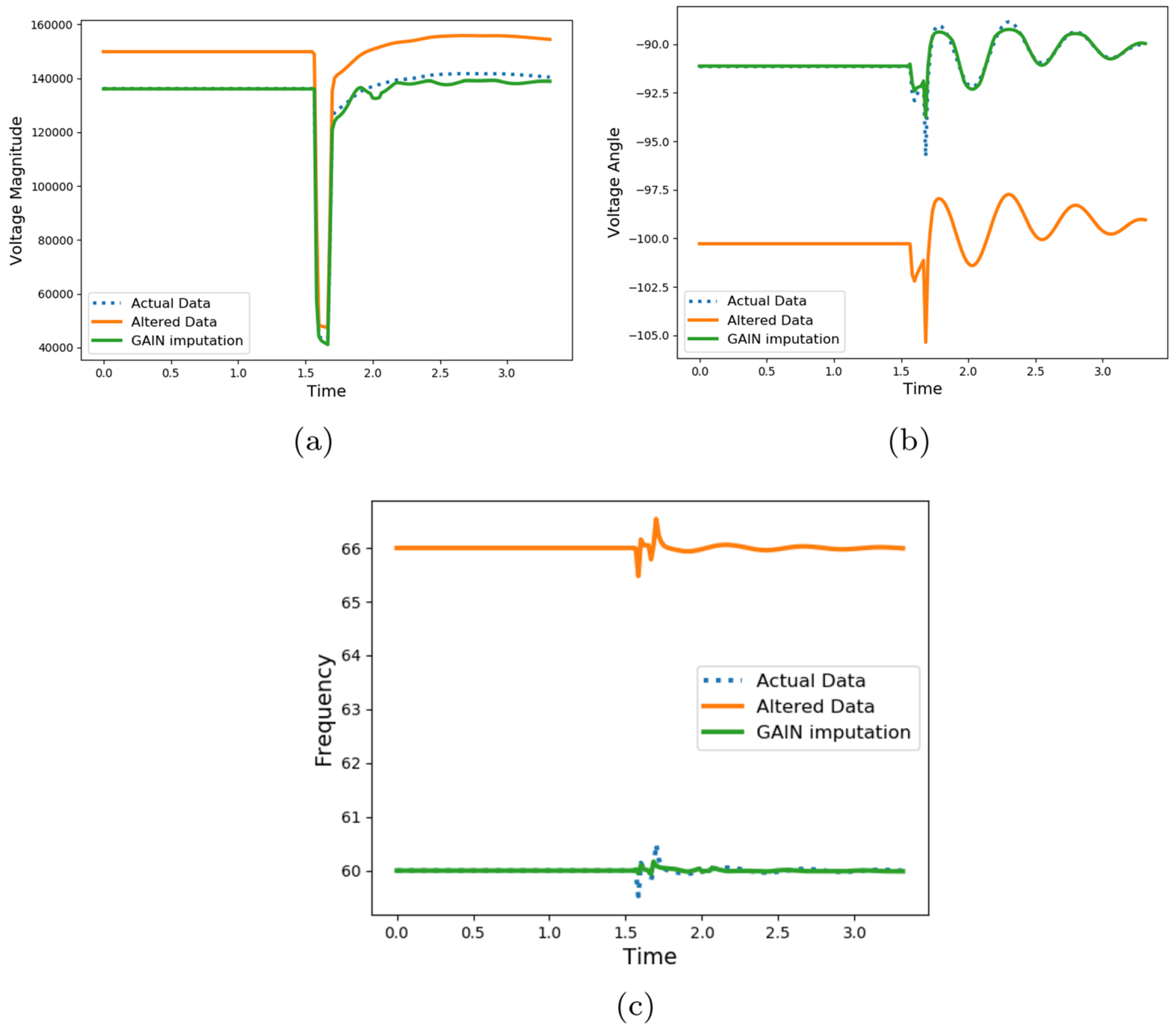


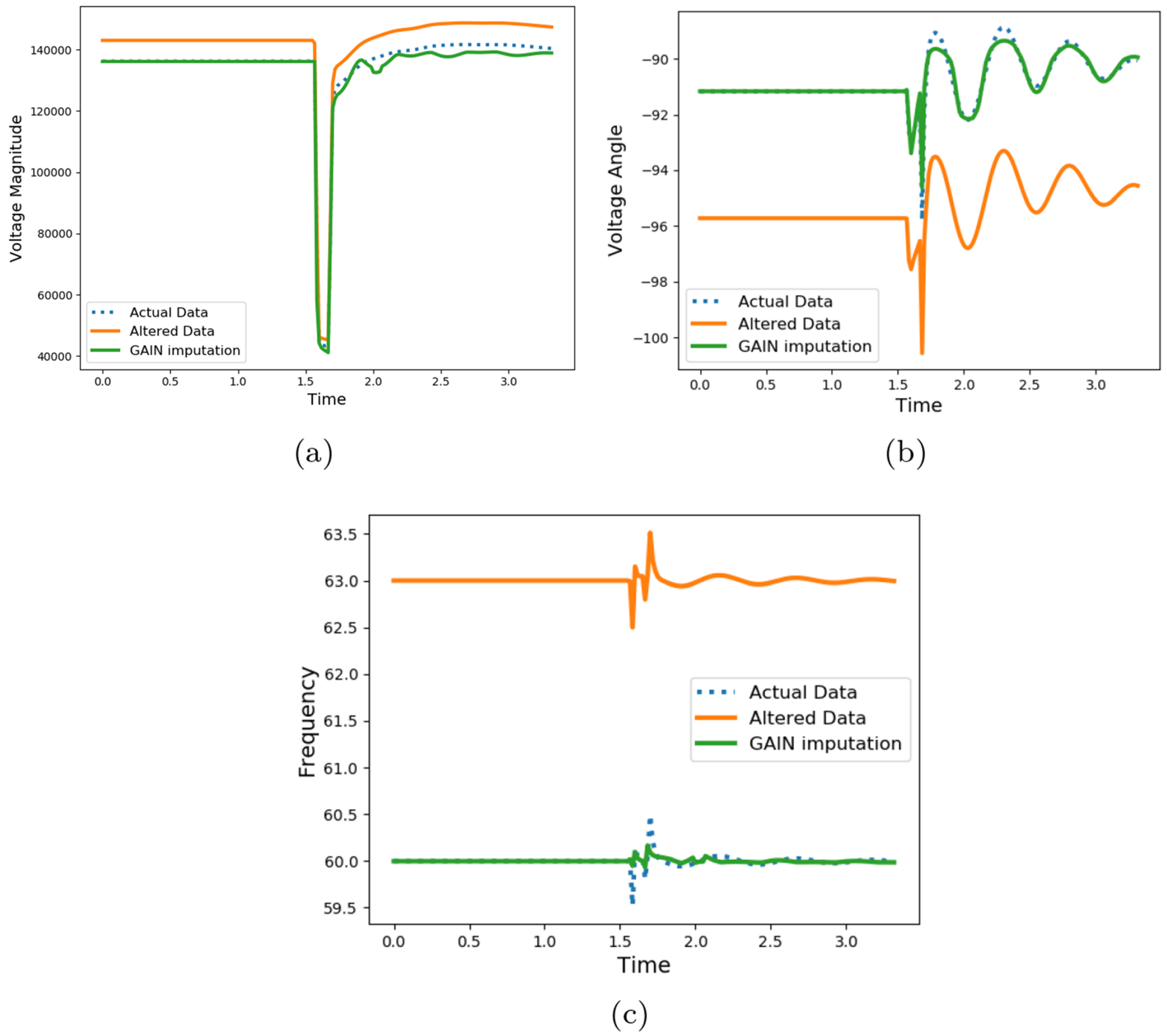
Fig. 8 Actual, predicted and altered measurements of **a** Voltage magnitude, **b** Voltage angle, and **c** Frequency during a strong data manipulation attack

threshold, it confirmed an attack on PMU4. The detection module outputs a bool vector with ‘0’ corresponding to PMU4 and ‘1’ corresponding to all other PMUs as given in (19). A select signal $S = 0$ was given to the data selector. On receiving this bool vector, the mask vector given in (20) was formed and forwarded to the generator in the mitigation module.

$$\textbf{\textit{Boolvector}} = \begin{array}{cccccc} PMU4 & PMU5 & PMU5' & PMU6 & PMU6' & PMU7 \\ 0 & 1 & 1 & 1 & 1 & 1 \\ & PMU7' & PMU8 & PMU8' & PMU9 & PMU9' \\ & 1 & 1 & 1 & 1 & 1 \end{array} \tag{19}$$

$$\textbf{\textit{Maskvector}} = \begin{array}{cccccc} PMU4 & PMU5 & PMU5' & PMU6 & PMU6' & PMU7 \\ 00000 & 11111 & 11111 & 11111 & 11111 & 11111 \\ & PMU7' & PMU8 & PMU8' & PMU9 & PMU9' \\ & 11111 & 11111 & 11111 & 11111 & 11111 \end{array} \tag{20}$$

The mitigation module returned an imputed datastream with reconstructed data corresponding to PMU4, as shown in Fig. 11. The imputed datastream follows the actual data trends and reflects the system’s normal working, unlike the fault data sent by the attacker. When this reconstruted data were sent to the end application, the RF classifier detected no faults in the system, thwarting the attacker’s attempts to cause unwanted line trips.



(a)

(b)

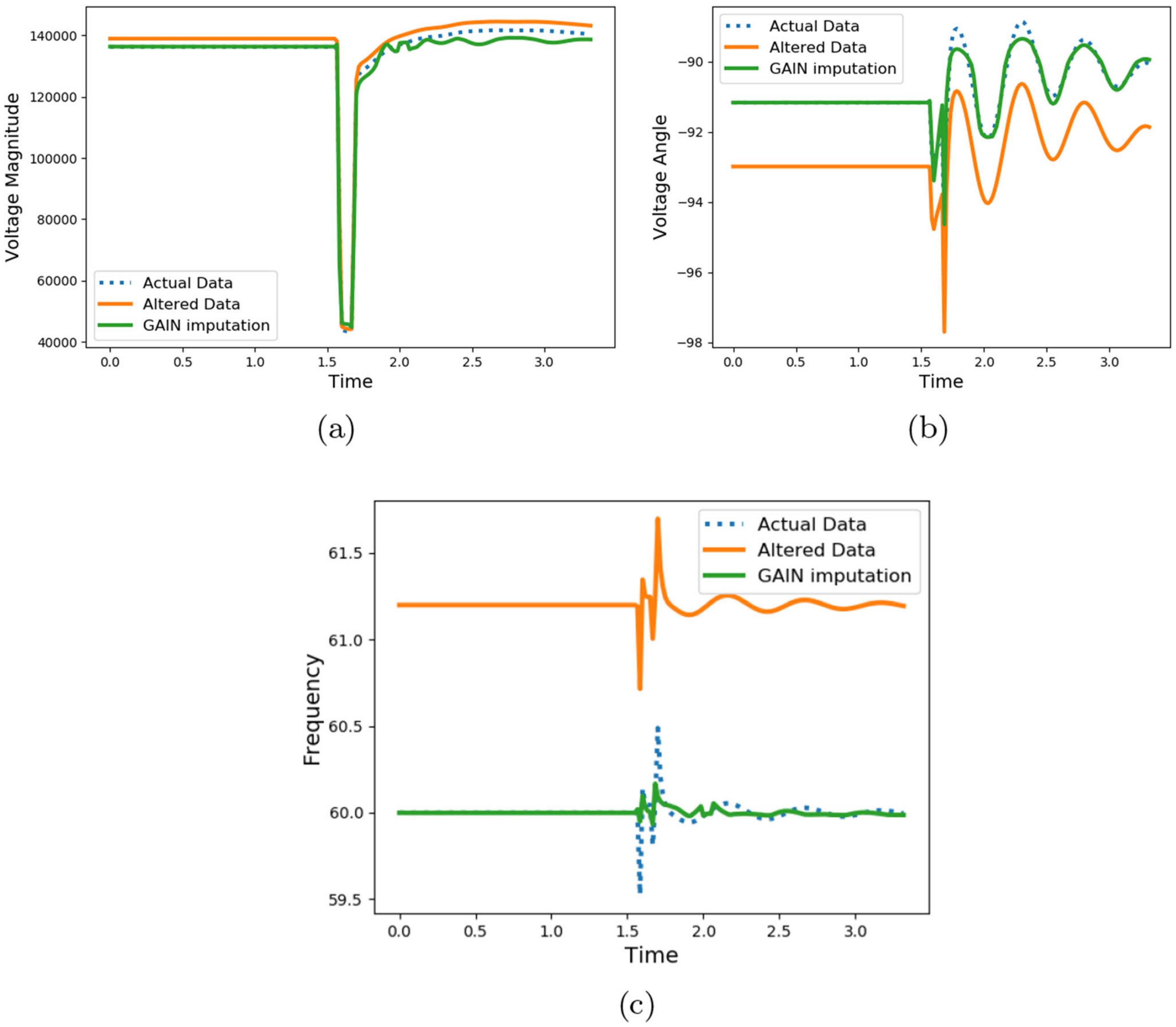
(c)

Fig. 9 Actual, predicted and altered measurements of **a** Voltage magnitude, **b** Voltage angle, and **c** Frequency during a moderate data manipulation attack

3. Ramp attacks

Data manipulation attacks on PMU data can be more sophisticated and stealthier like ramp attacks, where the amount of error introduced at every timestamp is too small to be detected by LSTMs. However, these small manipulations in data cumulatively amount to some large values that can adversely affect the RF classifier's working in the end application. One such attack was conducted by modifying the data of PMU5 by a total of 10% over 2.5 secs, or 150 data frames. Each frame added a small error to the data that went undetected by the LSTMs. Thus, a bool vector having '1's corresponding to each PMU was obtained from the LSTM-based detection module, as given in (21). The detection module failed to point out the compromised PMU in this case and sends a select signal of $S = 1$ to the data selector. With this bool vector, a custom mask vector was formed as given in (22).

$$\textbf{\textit{Boolvector}} = \begin{array}{cccccc} PMU4 & PMU5 & PMU5' & PMU6 & PMU6' & PMU7 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ & PMU7' & PMU8 & PMU8' & PMU9 & PMU9' \\ & 1 & 1 & 1 & 1 & 1 \end{array} \tag{21}$$



(a)

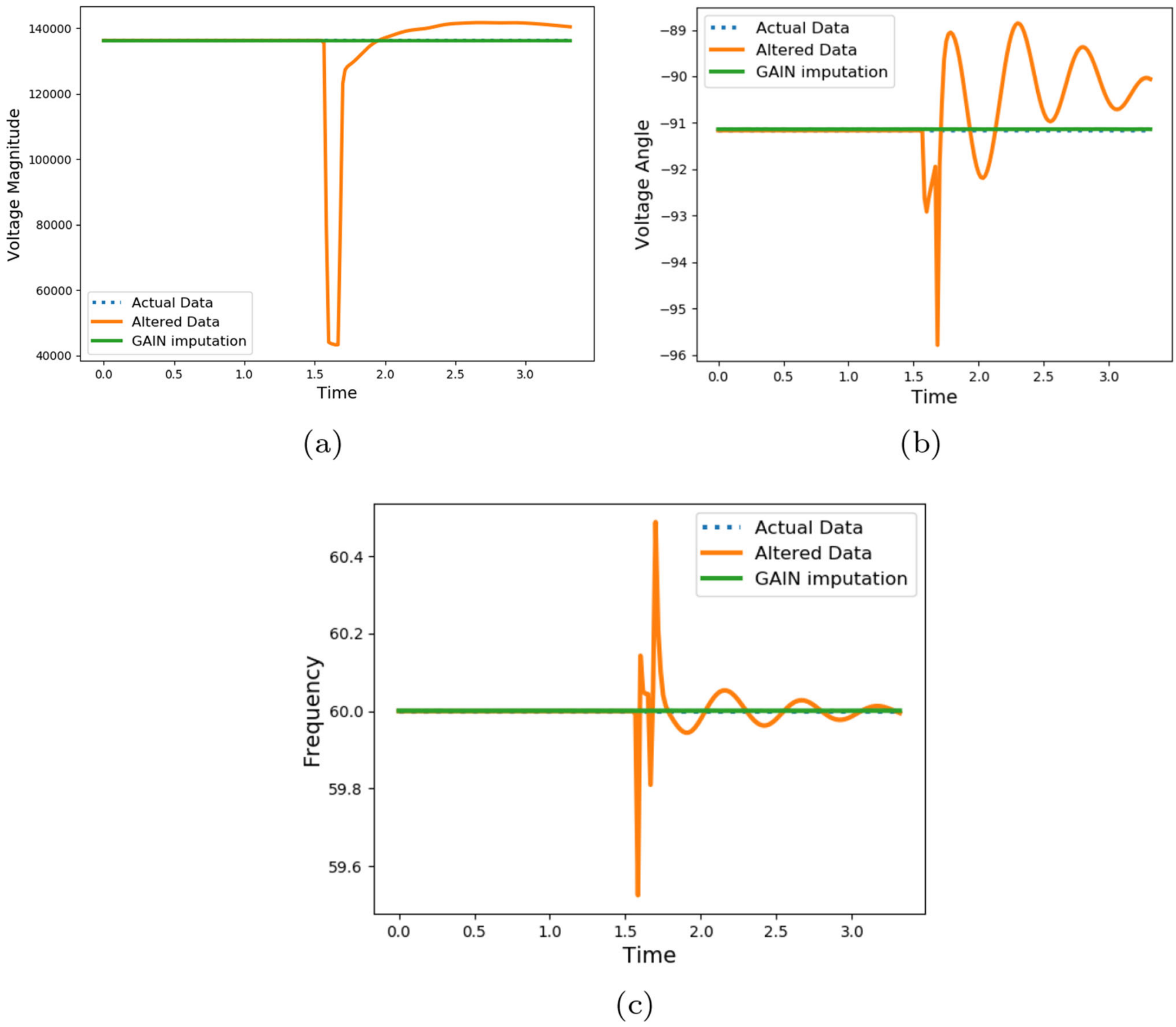
(b)

(c)

Fig. 10 Actual, predicted and altered measurements of **a** Voltage magnitude, **b** Voltage angle, and **c** Frequency during a weak data manipulation attack

$$\textbf{\textit{Maskvector}} = \begin{array}{cccccc} PMU4 & PMU5 & PMU5' & PMU6 & PMU6' & PMU7 \\ 00000 & 11111 & 11111 & 11111 & 11111 & 11111 \\ & PMU7' & PMU8 & PMU8' & PMU9 & PMU9' \\ & 11111 & 11111 & 11111 & 11111 & 11111 \end{array} \tag{22}$$

The mitigation module reconstructed PMU4 measurements corresponding to this mask vector and compared them to the original datastream. Since PMU5 measurements had been altered, PMU4 values reconstructed using these altered PMU5 data were not as accurate as expected and shown in Fig. 12. The enlarged version of the deviation between GAIN imputed data for PMU4 and actual data is shown in these figures using black arrows. After a certain number of data frames, when the cumulative amount injected to PMU5 data gets large, the errors between the imputed values and original data values of PMU4 became large enough to exceed the set threshold. This gradual change in the error can be observed in the enlarged version of the figures. Thus, gate G1 was disabled, blocking the original datastream from being sent to the end application. During such attacks, when our framework cannot detect a compromised PMU and isolate it, it prefers blocking the compromised datastream from being used in the application, preventing incorrect decisions.



(a)

(b)

(c)

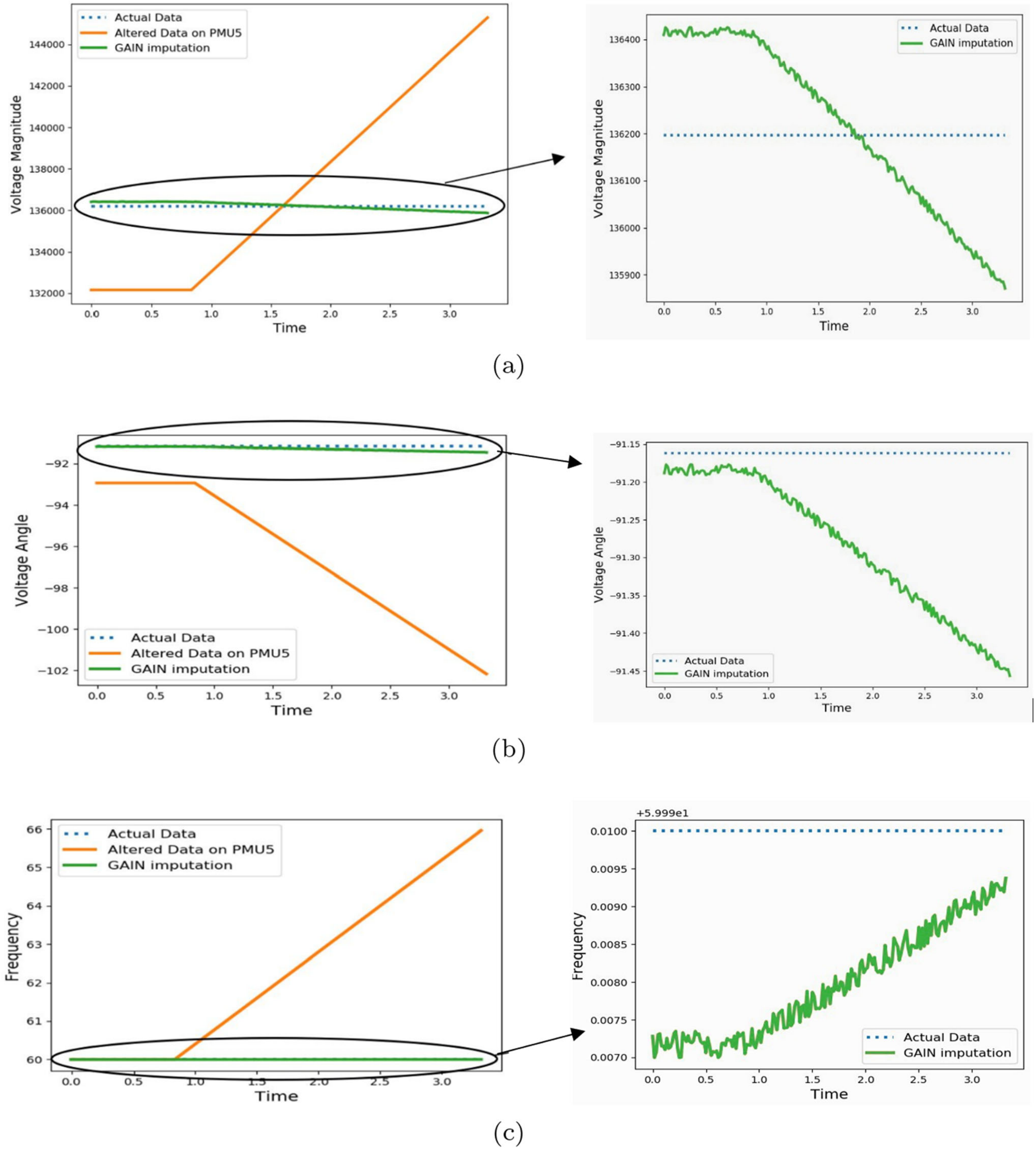
Fig. 11 Actual, predicted and altered measurements of **a** Voltage Magnitude, **b** Voltage Angle, and **c** Frequency during a replay attack

5.2 Performance of the protection scheme with the proposed WAMS framework

The performance of the synchrophasor-assisted supervisory backup protection scheme using RF classifier to detect the presence of fault on transmission lines is extensively tested during different attack scenarios and power contingencies with both proposed and conventional WAMS framework. TABLE 1 illustrates the proposed framework's effectiveness by comparing its working with the conventional framework for various simulated cases. While the RF classifier makes wrong decisions in a conventional framework (in red text) on receiving corrupted PDC datastream, the proposed framework with its imputed datastream makes the end protection application resilient against cyber-attacks and helps in the successful operation of such schemes.

5.3 Scalability

The proposed model has been tested on a WSCC 9-Bus System, which uses one hardware and ten software PMUs. However, real power system networks have more buses and use a much larger number of PMU. The proposed model is scalable even under these conditions, as the real-time implementation of the framework primarily uses deep-learning algorithms, which require a time of the order of microseconds for generating outputs for each test sample. Since each LSTM block works on a single feature of the PMU datastream, the latency of LSTMs is unaffected by scaling. The GAIN-based mitigation module will



(a)

(b)

(c)

Fig. 12 Actual, predicted and altered measurements of **a** Voltage magnitude, **b** Voltage angle, and **c** Frequency during a ramp attack

require more extensive training due to the increased training data. However, the latency for testing will remain of a similar order. Larger power networks can also divided into multiple zones like protection zones [7], where all PMUs from a particular protection zone report to one PDC. Thus, the proposed framework's detection and mitigation modules can be used in parallel for each such protection zone, making it adequately scalable for real-world larger power systems.

Table 1 Overall Performance of Supervisory Backup Protection Scheme

WAMS framework	Cyber event	Power event	Output from LSTM-based detection module	Select signal (S) to data selector	Output from mitigation module (C)	GATE G_i	Input datastream to RF Classifier	Supervisroy Protection Scheme's RF Classifier Output	Output signal from supervisroy protection scheme
Conventional framework	None	Three-phase fault on line 6	NA	NA	NA	NA	Original PDC Datastream	Fault	Trip
	Replay pre-recorded Line 5 fault data on PMU7	No Power Contingency	NA	NA	NA	NA	Original PDC Datastream	Fault	Trip
	DoS attack on PMU7 -PDC connection	Three-phase fault on line 5	NA	NA	NA	NA	Original PDC Datastream	No Fault	Block
	Ramp Attack on PMU7	No Power Contingency	NA	NA	NA	NA	Original PDC Datastream	Fault	Trip
Proposed framework	None	Three-phase fault on line 6	Does not declare any PMU as compromised	1	1	Enabled	Original PDC Datastream	Fault	Trip
	Replay pre-recorded Line 5 fault data on PMU7	No Power Contingency	Detects Compromised PMU7 data	0	0	Disabled	Imputed Datastream	No Fault	Block
	DoS attack on PMU7 -PDC connection	Three-phase fault on line 5	Detects Compromised PMU7 data	0	0	Disabled	Imputed Datastream	Fault	Trip
	Ramp Attack on PMU7	No Power Contingency	Does not declare any PMU as compromised and fails to detect compromised PMU7	1	0	Disabled	None	None	None

* NA= Not Applicable

6 Conclusion

In this paper, attack-resiliency of synchrophasor-assisted supervision of backup protection of transmission lines is addressed. A novel deep-learning-based data manipulation attack resilient WAMS framework is presented, which incorporates LSTM and GAIN architectures. The novel LSTM-based detection strategy in the framework uniquely identifies the PMU(s) under attack, and GAIN-based mitigation module accurately reconstructs the data of compromised PMU(s) in real-time, ensuring uninterrupted working of critical protection applications. The proposed framework's efficacy is accessed through a series of comprehensive case studies conducted on the WSCC 9 bus system in the developed RTDS-based cyber-physical testbed. The real-world applicability of the proposed work is also discussed in terms of its scalability in real-world large power systems, and latencies introduced by newly added software modules are acceptable for time-critical end applications. The proposed WAMS framework with novel attack detection and mitigation strategies can increase the attack resiliency of various WAMPAC applications. In worst cases, when the detection scheme fails to identify the compromised PMUs, the framework focuses on avoiding wrong decisions from automated end applications or system operators by blocking the corrupted datastream, thereby failing attackers' malicious intent.

The performance of the proposed detection and mitigation approaches can be improved by incorporating metaheuristic algorithms like monarch butterfly optimization (MBO), harris hawk's optimization (HHO), elephant herding optimization (EHO), etc., [35–37] in the LSTM and GAIN architectures. These algorithms' global optimum search ability can help find near-optimal training parameters of LSTM and GAIN models at an acceptable computational cost and speed up their training without declining their performance. Other advanced deep learning models can also be explored to improve the accuracy and latency associated with the proposed framework's detection and mitigation approaches. The proposed framework can also be used for other cyber-physical systems that operate on a similar principle.

Acknowledgements Funding for this project was provided by the Ministry of Science and Technology, Department of Science and Technology, India, under project S3RACPPS (Research and development of Smart, Secure, Scalable, Resilient and Adaptive Cyber-Physical Power System) with grant number RP03609.

Declarations

Conflict of interest The authors declare that they have no conflict of interest.

References

1. Phadke AG, Bi T (2018) Phasor measurement units, WAMS, and their applications in protection and control of power systems. J Modern Power Syst Clean Energy 6(4):619–629
2. Brahma S, Kavasseri R, Cao H, Chaudhuri N, Alexopoulos T, Cui Y (2016) Real-time identification of dynamic events in power systems using pmu data, and potential applications–models, promises, and challenges. IEEE Trans Power Deliv 32(1):294–301
3. Bernabeu EE, Thorp JS, Centeno V (2011) Methodology for a security/dependability adaptive protection scheme based on data mining. IEEE Trans Power Deliv 27(1):104–111
4. Tan J, Crossley P, McLaren P, Gale P, Hall I, Farrell J (2002) Application of a wide area backup protection expert system to prevent cascading outages. IEEE Trans Power Deliv 17(2):375–380
5. Biswal M, Brahma SM, Cao H (2016) Supervisory protection and automated event diagnosis using pmu data. IEEE Trans Power Deliv 31(4):1855–1863
6. Seethalekshmi K, Singh SN, Srivastava SC (2012) A classification approach using support vector machines to prevent distance relay maloperation under power swing and voltage instability. IEEE Trans Power Deliv 27(3):1124–1133
7. Jena MK, Samantaray SR, Panigrahi BK (2017) A new decentralized approach to wide-area back-up protection of transmission lines. IEEE Syst J 12(4):3161–3168
8. Das S, Panigrahi BK (2018) Real-time secured third zone relay operation under dynamic stressed conditions. IEEE Syst J 13(3):3337–3346
9. Samantaray S, Sharma A et al (2018) Enhancing performance of wide-area back-up protection scheme using pmu assisted dynamic state estimator. IEEE Trans Smart Grid 10(5):5066–5074
10. Khan R, McLaughlin K, Laverty JHD, David H, Sezer S (2018) Demonstrating cyber-physical attacks and defense for synchrophasor technology in smart grid, In: 2018 16th Annual Conference on Privacy, Security and Trust (PST). IEEE, 2018, pp. 1–10
11. Almas MS, Vanfretti L, Singh RS, Jonsdottir GM (2017) Vulnerability of synchrophasor-based WAMPAC applications' to time synchronization spoofing. IEEE Trans Smart Grid 9(5):4601–4612
12. Chawla A, Agrawal P, Singh A, Panigrahi BK, Paul K, Bhalja B (2020) Denial-of-service resilient frameworks for synchrophasor-based wide area monitoring systems. Computer 53(5):14–24
13. Initiative NAS et al. (2015) Naspi 2014 survey of synchrophasor system networks-results and findings, North American SynchroPhasor Initiative (NASPI)
14. Martin K, Brunello G, Adamiak M, Antonova G, Begovic M, Benmouyal G, Bui P, Falk H, Gharpure V, Goldstein A et al (2014) An overview of the IEEE standard C37.118.2—synchrophasor data transfer for power systems. IEEE Trans Smart Grid 5(4):1980–1984
15. Case DU (2016) Analysis of the cyber attack on the ukrainian power grid, Electricity Information Sharing and Analysis Center (E-ISAC), vol. 388
16. Ashok A, Govindarasu M, Ajjarapu V (2016) Online detection of stealthy false data injection attacks in power system state estimation. IEEE Trans Smart Grid 9(3):1636–1646
17. Sridhar S, Govindarasu M (2014) Model-based attack detection and mitigation for automatic generation control. IEEE Trans Smart Grid 5(2):580–591
18. James J, Hou Y, Li VO (2018) Online false data injection attack detection with wavelet transform and deep neural networks. IEEE Trans Ind Inf 14(7):3271–3280
19. Ghafouri M, Au M, Kassouf M, Debbabi M, Assi C, Yan J (2020) Detection and mitigation of cyber attacks on voltage stability monitoring of smart grids. IEEE Trans Smart Grid 11(6):5227–5238
20. Chakhchoukh Y, Lei H, Johnson BK (2019) Diagnosis of outliers and cyber attacks in dynamic pmu-based power state estimation. IEEE Trans Power Syst 35(2):1188–1197
21. Wang J, Shi D, Li Y, Chen J, Ding H, Duan X (2018) Distributed framework for detecting pmu data manipulation attacks with deep autoencoders. IEEE Trans Smart Grid 10(4):4401–4410
22. Pal S, Sikdar B, Chow JH (2017) Classification and detection of pmu data manipulation attacks using transmission line parameters. IEEE Trans Smart Grid 9(5):5057–5066
23. Musleh AS, Khalid HM, Muyeen S, Al-Durra A (2017) A prediction algorithm to enhance grid resilience toward cyber attacks in wamcs applications. IEEE Syst J 13(1):710–719
24. Khalid HM, Peng JC-H (2016) A bayesian algorithm to enhance the resilience of WAMS applications against cyber attacks. IEEE Trans Smart Grid 7(4):2026–2037
25. Cameron C, Patsios C, Taylor PC, Pourmirza Z (2018) Using self-organizing architectures to mitigate the impacts of denial-of-service attacks on voltage control schemes. IEEE Trans Smart Grid 10(3):3010–3019
26. Siami-Namini S, Tavakoli N, Namin AS (2018) A comparison of ARIMA and LSTM in forecasting time series. In: 2018 17th IEEE international conference on machine learning and applications (ICMLA). IEEE, pp 1394–1401
27. Wang G-G, Lu M, Dong Y-Q, Zhao X-J (2016) Self-adaptive extreme learning machine. Neural Comput Appl 27(2):291–303
28. Hochreiter S, Schmidhuber J (1997) Long short-term memory. Neural Comput 9(8):1735–1780
29. Gers FA, Schmidhuber J, Cummins F (1999) Learning to forget: continual prediction with LSTM. In: Ninth international conference on artificial neural networks ICANN 99. pp 850–855
30. García-Laencina PJ, Sancho-Gómez J-L, Figueiras-Vidal AR (2010) Pattern classification with missing data: a review. Neural Comput Appl 19(2):263–282
31. Yoon J, Jordon J, Schaar M (2018) GAIN: missing data imputation using generative adversarial nets. In: International conference on machine learning, PMLR. pp 5689–5698
32. Goodfellow IJ, Pouget-Abadie J, Mirza M, Xu B, Warde-Farley D, Ozair S, Courville A, Bengio Y (2014) Generative adversarial networks, arXiv preprint arXiv:1406.2661
33. Horowitz SH, Phadke AG (2006) Third zone revisited. IEEE Trans Power Deliv 21(1):23–29
34. Phadke AG, Thorp JS (2010) Communication needs for wide area measurement applications, In: 2010 5th International Conference on Critical Infrastructure (CRIS), 2010, pp. 1–7
35. Wang G-G, Deb S, Cui Z (2019) Monarch butterfly optimization. Neural Comput Appl 31(7):1995–2014
36. Heidari AA, Mirjalili S, Faris H, Aljarah I, Mafarja M, Chen H (2019) Harris hawks optimization: algorithm and applications. Future Gen Comput Syst 97:849–872
37. Li J, Lei H, Alavi AH, Wang G-G (2020) Elephant herding optimization: variants, hybrids, and applications. Mathematics 8(9):1415