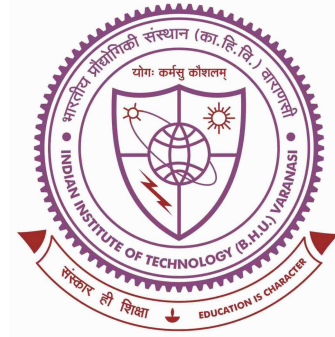


Formulation and detection of false data injection attack in modern smart grid



Thesis submitted in partial fulfillment
for the award of degree

Doctor of Philosophy

by

Debottam Mukherjee

DEPARTMENT OF ELECTRICAL ENGINEERING
Indian Institute of Technology
(Banaras Hindu University)
Varanasi

Roll No: 17081008

2022

Dedicated

To

My father, mother, brother, family and friends

CERTIFICATE

It is certified that the work contained in the thesis titled **Formulation and detection of false data injection attack in modern smart grid** by **Debottam Mukherjee** has been carried out under our supervision and that this work has not been submitted elsewhere for a degree. It is further certified that the student has fulfilled all the requirements of Comprehensive Examination, Candidacy and SOTA for the award of Ph.D. Degree.

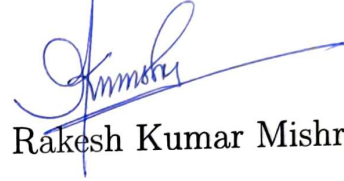

03/10/2023

Dr. Sandip Ghosh

Dept. of Electrical Engg.

IIT(BHU), Varanasi

Varanasi, India - 221005



Prof. Rakesh Kumar Mishra

Dept. of Electrical Engg.

IIT(BHU), Varanasi

Varanasi, India - 221005

DECLARATION

I, **Debottam Mukherjee**, certify that the work embodied in this thesis is my own bonafide work and carried out by me under the supervision of **Dr. Sandip Ghosh** and **Prof. Rakesh Kumar Mishra** from July-2017 to November-2022, at the Department of Electrical Engineering, Indian Institute of Technology (BHU), Varanasi. The matter embodied in this thesis has not been submitted for the award of any other degree/diploma. I declare that I have faithfully acknowledged and given credits to the research workers wherever their works have been cited in my work in this thesis. I further declare that I have not willfully copied any other's work, paragraphs, text, data, results, etc., reported in journals, books, magazines, reports dissertations, theses, etc., or available at websites and have not included them in this thesis and have not cited as my own work.

Date: September 21, 2023

Debottam Mukherjee

Place: Varanasi

(Debottam Mukherjee)

CERTIFICATE BY THE SUPERVISOR

It is certified that the above statement made by the student is correct to the best of my/our knowledge.

R. K. Mishra
Prof. R. K. Mishra

S. Ghosh
23/10/2023
Dr.. Sandip Ghosh
IIT(BHU), Varanasi

Signature of Head of Department/Coordinator of School

23.10.2023

COPYRIGHT TRANSFER CERTIFICATE

Title of the Thesis: **Formulation and detection of false data injection attack in modern smart grid**

Name of Student: **Debottam Mukherjee**

Copyright Transfer

The undersigned hereby assigns to the Indian Institute of Technology (Banaras Hindu University), Varanasi all rights under copyright that may exist in and for the above thesis submitted for the award of the Doctor of Philosophy.

Date: September 21, 2023

Debottam Mukherjee

Place: Varanasi

(Debottam Mukherjee)

Note: However, the author may reproduce or authorize others to reproduce material extracted verbatim from the thesis or derivative of the thesis for author's personal use provided that the source and the Institute's copyright notice are indicated.

Acknowledgments

First of all, I am grateful for the opportunity to write this thesis, which will be the end of a five year journey towards a degree.

Though, only my name appears on the cover of this dissertation, so many great people have contributed to its production. I owe my gratitude to all those people who have made this thesis possible and because of whom my post graduate experience has been one that I will cherish forever.

.....

Date: 21.09.2023

Debottam Mukherjee

Debottam Mukherjee

List of Tables

1.1	Various types of attacks on the smart grid	5
1.2	A comprehensive survey pertaining to FDIA research	14
4.1	Hyper-parameter tuning of the developed models	57
4.2	Comparative analysis of forecasting models	66
4.3	Computational burden of the forecasting models	70
5.1	Comparison of the models for the IEEE 118-bus system	92
5.2	Optimal set of hyper-parameters of the MLP classifier	93
5.3	FDIA identification results on correlated measurements	97

List of Figures

1.1	SGAM framework with interoperability layers [1]	2
1.2	Various types of attacks on the grid	3
1.3	Country-wise DDOS attacks in the power grid [2]	4
1.4	Interconnected attacks on the grid	6
1.5	FDIA on the power grid	9
1.6	Existing methods for developing FDIA	10
1.7	Thesis organisation	18
2.1	IEEE 14 bus system with labelled measurements	29
3.1	An overview of the attack vector formulation scheme	39
3.2	Probability to bypass bad data detector with varying attack strength (a) CUR (b) Go-Dec	50
3.3	(a)Computational burden of the algorithms (b) Relative state deviation ($\ c''\ _2/\ c'\ _2$)	52
3.4	Measurement residuals after attack using CUR decomposition (a) under ideal conditions (b) with noise	53
3.5	Measurement residuals after attack using Go-Dec (a) under ideal conditions (b) with noise	53
4.1	Proposed Neural Network Structure	58
4.2	LSTM module	59
4.3	Proposed deep learning structure with LSTM modules	60
4.4	Proposed FDIA detection strategy using anomaly detection schemes	61
4.5	Training & Validation loss of MLP model	65
4.6	Training & Validation loss of LSTM model	65

4.7	State forecasting performance of Voltage magnitude	66
4.8	State forecasting performance of Voltage angle	67
4.9	FDIA detection performance of the undertaken models for anomaly detection Scheme - I	67
4.10	FDIA detection performance of the undertaken models for anomaly detection Scheme - II	68
4.11	Variation in FDIA detection performance of the undertaken models for anomaly detection Scheme - I	68
4.12	Variation in FDIA detection performance of the undertaken models for anomaly detection Scheme - II	69
5.1	FDIA identification strategy	72
5.2	Proposed CNN model	76
5.3	CNN network parameters	77
5.4	Proposed CNN-LSTM model	78
5.5	CNN-LSTM network parameters	79
5.6	Bi-Directional LSTM modules	81
5.7	Proposed CNN-BiLSTM model	82
5.8	CNN-BiLSTM network parameters	83
5.9	Multilayered perceptron classifier	85
5.10	An indexed IEEE 118-bus model	88
5.11	t-SNE of a subset of data taken from the training dataset	91
5.12	Accuracy of the undertaken classifiers under ideal condition	94
5.13	Value of loss function of the undertaken classifiers under ideal condition	94
5.14	Accuracy of the undertaken classifiers under 5% noise condition	95
5.15	Value of loss function of the undertaken classifiers under 5% noise condition	95
5.16	Accuracy of the undertaken classifiers under 10% noise condition	96
5.17	Loss of the undertaken classifiers under 10% noise condition	96
5.18	ROC curve of the proposed CNN classifier under ideal conditions	98
5.19	ROC curve of the proposed CNN classifier under 5% noise conditions	98
5.20	ROC curve of the proposed CNN classifier under 10% noise conditions	98
5.21	Variation of F_1 score for the undertaken models with incorporation of noise within measurements	101

5.22	Variation of F_1 score with \mathcal{L}_2 norm of injected Attack vector	101
5.23	Variation of F_1 score for the undertaken models with standard deviation of noise within measurements	102
5.24	Variation of F_1 score for the undertaken models with the incorporation of outliers within measurements	102
5.25	ROC curve for the DT classifier	103
5.26	ROC curve for the MLP classifier	104
6.1	Attacks against protection and control actions on the grid	108

Nomenclature

List of Abbreviations

AMI	Advanced metering infrastructure
ARIMA	Autoregressive integrated moving average
BDD	Bad data detector
Bi-LSTM	Bidirectional long short term memory
CNN	Convolution neural network
D-FACTS	Distributed flexible ac transmission system
DDOS	Distributed denial of service
DNN	Deep neural network
DT	Decision Tree
EMS	Energy management system
FDIA	False data injection attack
FSVD	Full order singular value decomposition
GPS	Global positioning system
IOT	Industrial internet of things
LSTM	Long-short term memory
MAE	Mean absolute error

MITM	Man in the middle
MLP	Multilayered perceptron
MSE	Mean squared error
NASV	Number of attacked state variables
PDC	Phasor data concentrator
PMU	Phasor measurement unit
RMSE	Root mean squared error
ROC	Receiver operating characteristics
RSVD	Reduced order singular value decomposition
RTU	Remote terminal unit
SCADA	Supervisory control and data acquisition
SVD	Singular value decomposition
SVM	Support vector machine
WAMS	Wide area monitoring system

List of Variables and Parameters

$\hat{x} \in \mathcal{R}^n$	Estimated operating states
$a \in \mathcal{R}^m$	Attack vector
$c \in \mathcal{R}^m$	Error vector for the estimation model
$H \in \mathcal{R}^{m \times n}$	Topology matrix of the grid
$h(\cdot) \in \mathcal{R}^m$	Nonlinear function relating the set of available measurements with the operating states of the grid
r	Measurement residual

$W \in \mathcal{R}^{m \times m}$

Weight matrix of the respective meters

$x \in \mathcal{R}^n$

Set of operating states

$z \in \mathcal{R}^m$

Set of acquired measurements at the control center