FIRST REVIEW

Guide - Dr. M. Jaya Bharata Reddy

- Angad Bajwa (107118014)
- Mandar Burande (107118056)
- Aditya Pethkar (107118072)
- Priyansh Joshi (107118076)

INDEX

TITLE

Cyber Attack Detection in Power System SCADA networks using Machine Learning Techniques

OBJECTIVES OF THE WORK

01

To monitor and analyze real-time data flow in SCADA networks

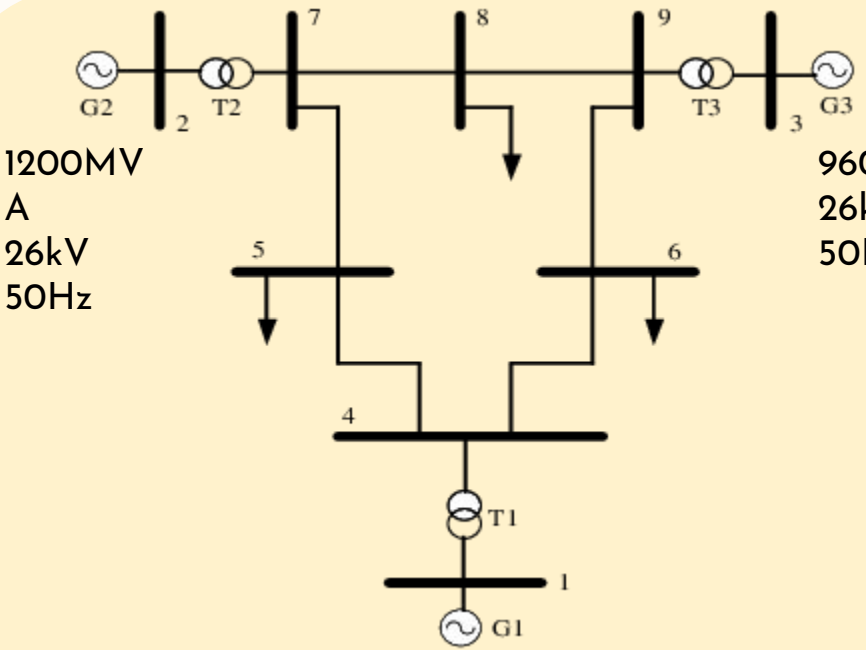
02

To detect and thwart various incoming cyber attacks such as man-in-the-middle and remote tripping commands, etc.

03

To put forth inferences to assist in implementing further solutions

CIRCUIT DIAGRAM



WORKFLOW

01
MODEL SIMULATION

Select a suitable bus system and design a MATLAB - Simulink model to serve as the template for all simulations

02
SIMULATING NATURAL EVENTS

Simulate events like faults, line maintenance and collecting relevant data

03
SIMULATING CYBER ATTACKS

Simulate cyber attacks in SCADA network and collect relevant data.

04
APPLYING MLTS FOR CLASSIFICATION

Applying various Machine Learning Techniques (MLTs) and/or Neural Network models on the collected data to generate inferences

EXPLANATION

A

WSCC 9-Bus system represents a simple system with nine buses and three generators with Grid Parameters equal to the Indian Grid system

B

Simulated the WSCC 9-Bus system on MATLAB - Simulink using blocks like generators, transformers, transmission lines, circuit breakers, and three phase faults

C

Simulating different types of faults at different locations at varying lengths.
Exporting the data of Voltage and Current for all three lines at all circuit breakers

RESULTS

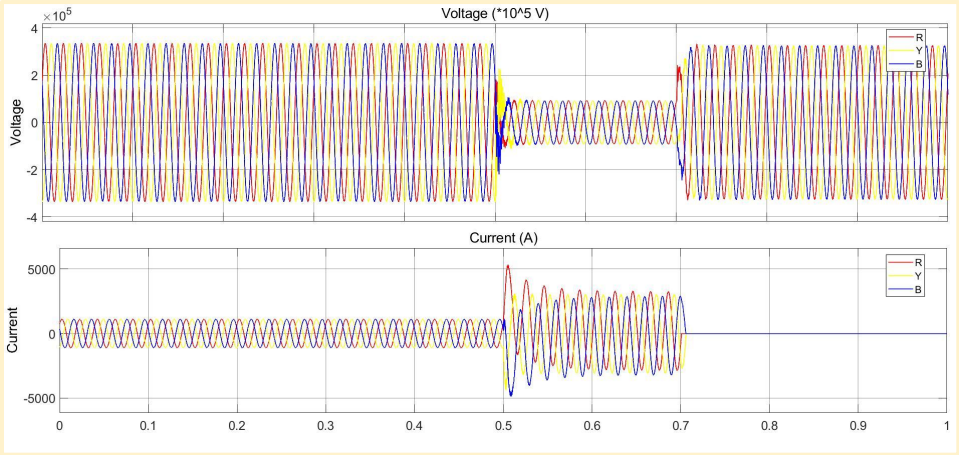
01

We have simulated different types of faults at various locations and collected the corresponding data

02

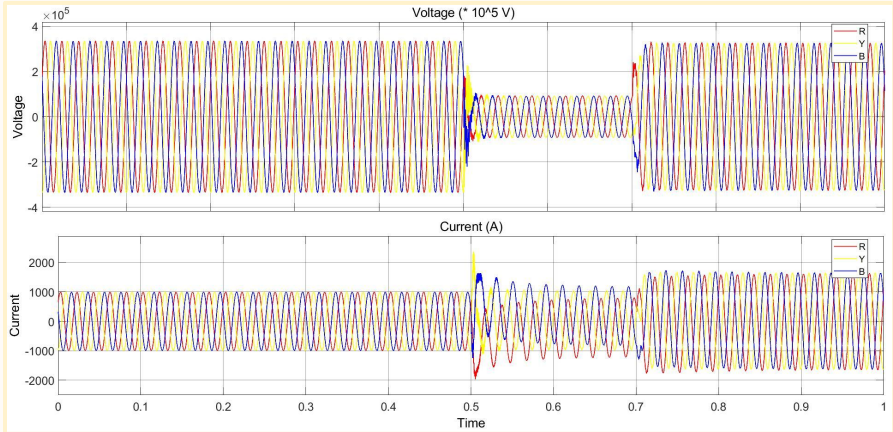
The preliminary steps have been completed and now the man-in-the-middle attacks can be introduced

RESULTS



Line containing fault - Voltage & Current vs Time

Line without fault - Voltage & Current vs Time



WORK TO BE DONE

SIMULATE CYBERATTACKS

Use Modbus protocols ; Execute Man-in-the-middle attacks

GENERATING DATA

Run multiple attacks ; Gather data & wrangle it for ML Model

TRAIN AND TEST ML MODEL

Model Selection; Feature Extraction; Data Segregation; Training & Testing

SCHEDULE

	WEEK I-II	WEEK III-IV
MONTH I - FEB	MODEL SELECTION AND SIMULATION	SIMULATING NATURAL EVENTS
MONTH II - MAR	SIMULATING NATURAL EVENTS	SIMULATING CYBER ATTACKS
MONTH III - APR	TRAINING MACHINE LEARNING MODEL	DRAWING INFERENCES AND RESULTS - FINISHING THE THESIS

REFERENCES

O. A. Alimi, K. Ouahada and A. M. Abu-Mahfouz	2020	"A Review of Machine Learning Approaches to Power System Security and Stability,". IEEE Access, vol. 8, pp. 113512-113531
Lemay, Antoine and José M. Fernandez.	2016	“Providing SCADA Network Data Sets for Intrusion Detection Research.” CSET @ USENIX Security Symposium
R. C. Borges Hink, J. M. Beaver, M. A. Buckner, T. Morris, U. Adhikari and S. Pan	2014	"Machine learning for power system disturbance and cyber-attack discrimination", 7th International Symposium on Resilient Control Systems (ISRCS)
W. Rahman, M. Ali, A. Ullah, H. Rahman, M. Iqbal, H. Ahmad, A. Zeb, Z. Ali, M. Shahzad and B. Taj	2012	"Advancement in Wide Area Monitoring Protection and Control Using PMU’s Model in MATLAB/SIMULINK", Smart Grid and Renewable Energy, Vol. 3 No. 4

REFERENCES

CENTRAL ELECTRICITY AUTHORITY NEW DELHI	2013	Transmission Planning Criteria
Power Grid Corporation of India Limited (PGCIL)	2014	Northern Regional Power Grid (NRPG) Data