SECOND REVIEW

Guide - Dr. M. Jaya Bharata Reddy

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

INDEX

01 TITLE

02 OBJECTIVES

03 WORKFLOW

04 CIRCUIT DIAGRAM

05 EXPLANATION

06 RESULTS

07 WORK TO BE DONE

08 REFERENCES

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

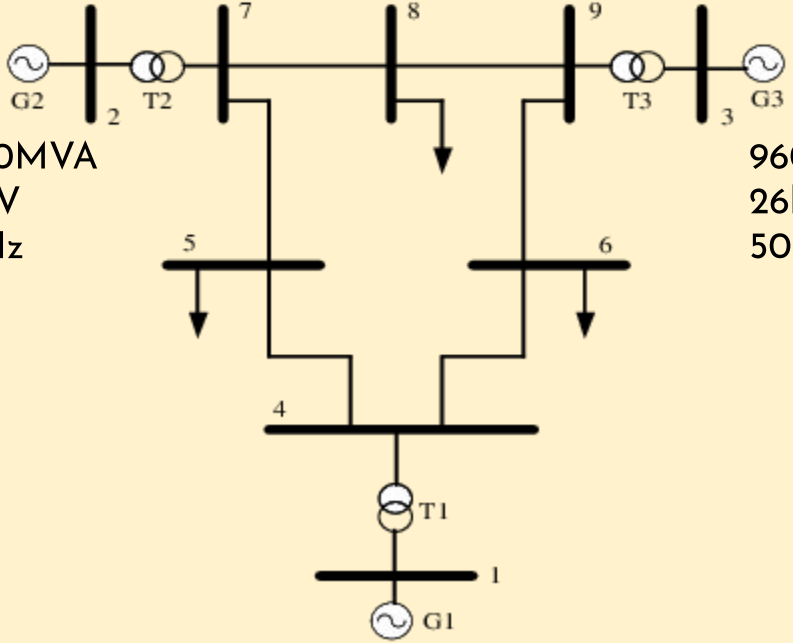
02

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



1200MVA
26kV
50Hz

960MVA
26kV
50Hz

776.5MVA, 24kV, 50Hz

Fig 1: Single Line Diagram of the WSCC 9-Bus System

CIRCUIT DIAGRAM

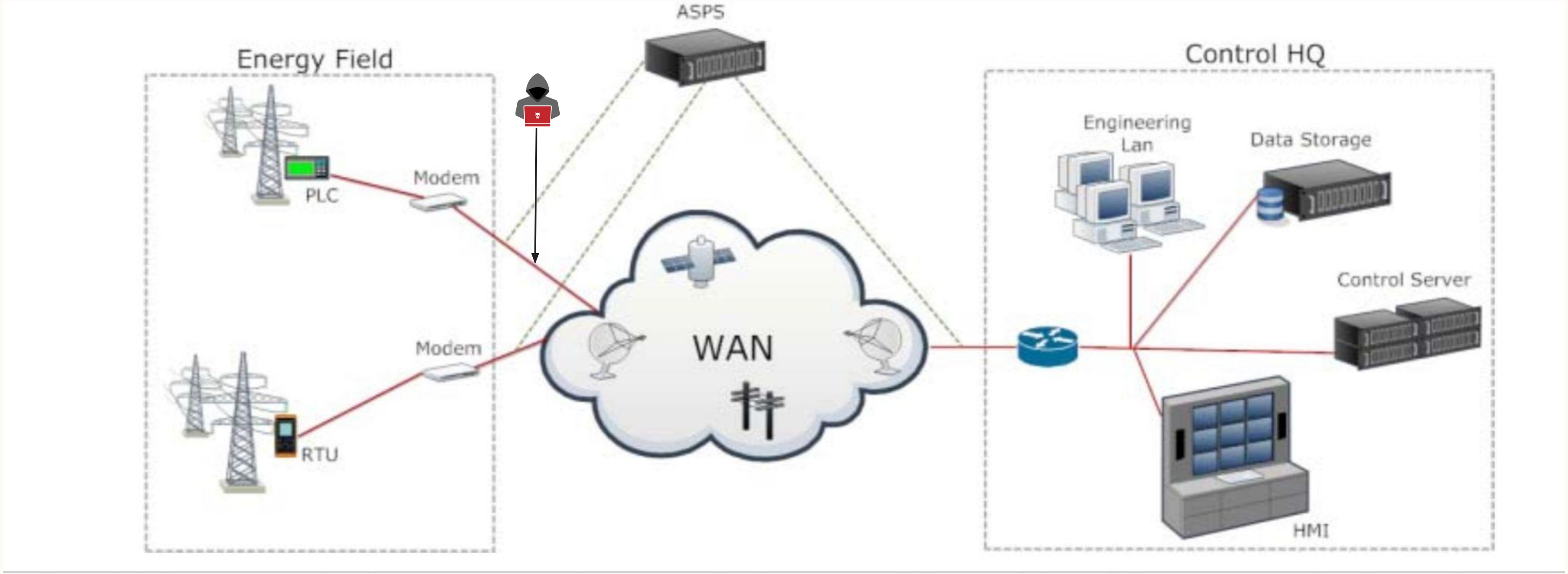


Fig 2: Representative diagram of a typical SCADA Network

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

We simulated faults at multiple distances for all types (LLL, LLLG, etc.) and collected the relevant data about it.

B

A Modbus protocol is used to transfer data between the CBs and the main servers of the SCADA Network. This same protocol is to be used to intercept Circuit Breaker-Server Communication and introduce the Man In The Middle cyber-attacks.

C

After the Cyber-Attacks, the corresponding data is collected, and the same shall be used for the next step of the project - Training the Machine Learning Model

RESULTS

01

We have simulated different types of faults at various locations

02

The data from all the faults have been collected and exported to excel

03

The client server network has been established

RESULTS

04

We have converted the data to Modbus protocol

05

We have transferred the data in the client server network

RESULTS

Fault Location	LG	LLG	LL	LLL	LLLG
a	20-130,40-110,60-90	20-130,40-110,60-90	20-130,40-110,60-90	20-130,40-110,60-90	20-130,40-110,60-90
b	20-100,40-80,60-60	20-100,40-80,60-60	20-100,40-80,60-60	20-100,40-80,60-60	20-100,40-80,60-60
c	20-100,40-80,60-60	20-100,40-80,60-60	20-100,40-80,60-60	20-100,40-80,60-60	20-100,40-80,60-60
d	20-120,40-100,60-80	20-120,40-100,60-80	20-120,40-100,60-80	20-120,40-100,60-80	20-120,40-100,60-80
e	20-90,40-70,60-50	20-90,40-70,60-50	20-90,40-70,60-50	20-90,40-70,60-50	20-90,40-70,60-50
f	20-90,40-70,60-50	20-90,40-70,60-50	20-90,40-70,60-50	20-90,40-70,60-50	20-90,40-70,60-50

RESULTS

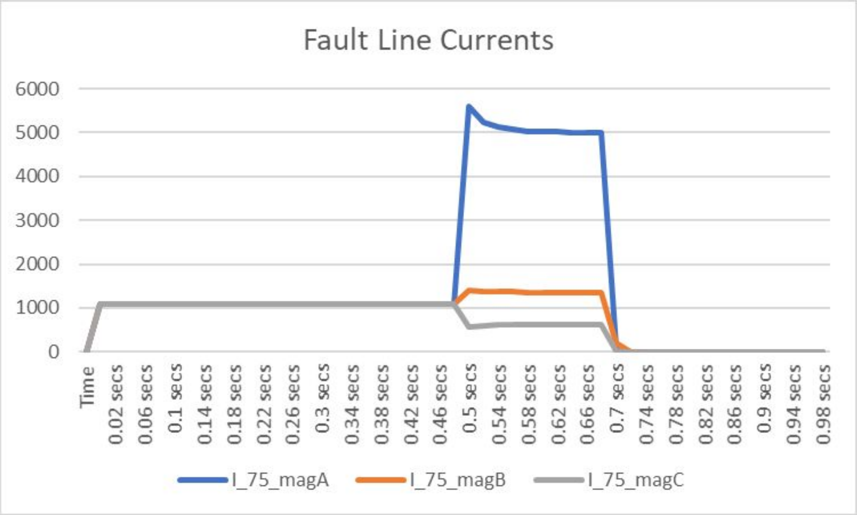
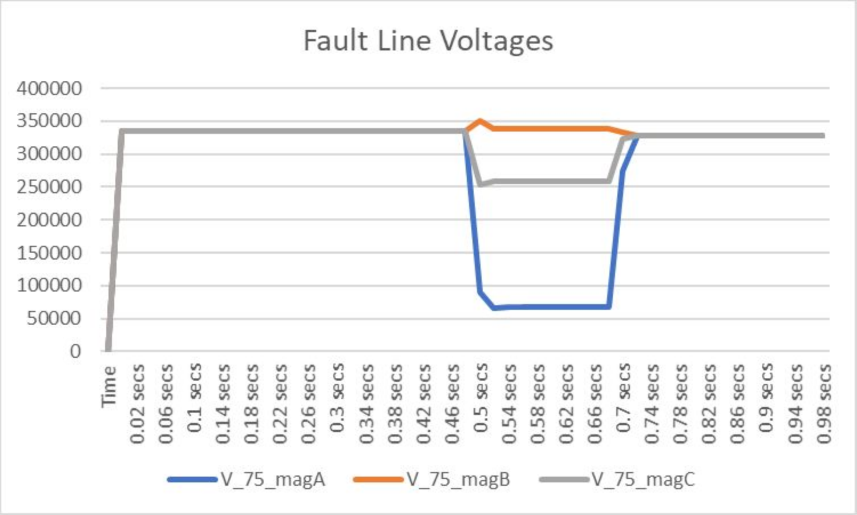


Fig 3: Fault Line Currents at Line C due to LG Fault

Fig 4: Fault Line Voltages at Line C due to LG Fault



RESULTS

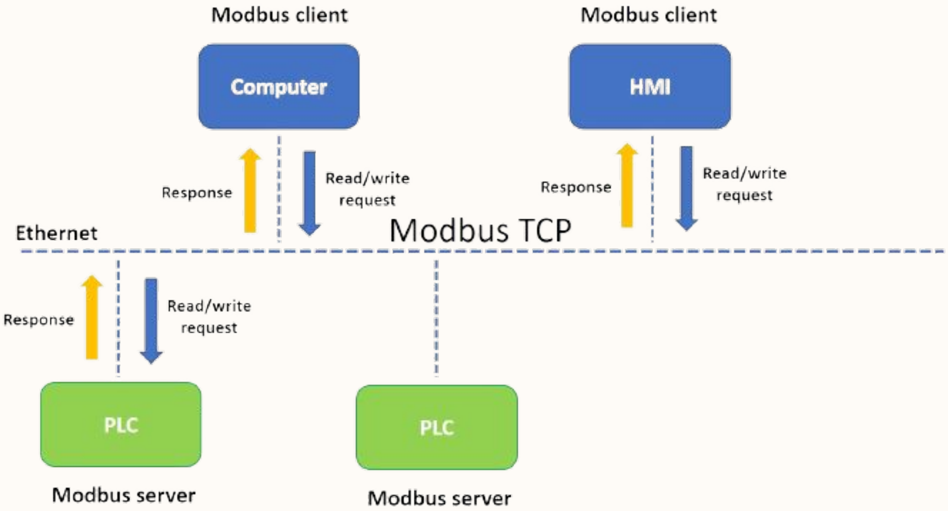
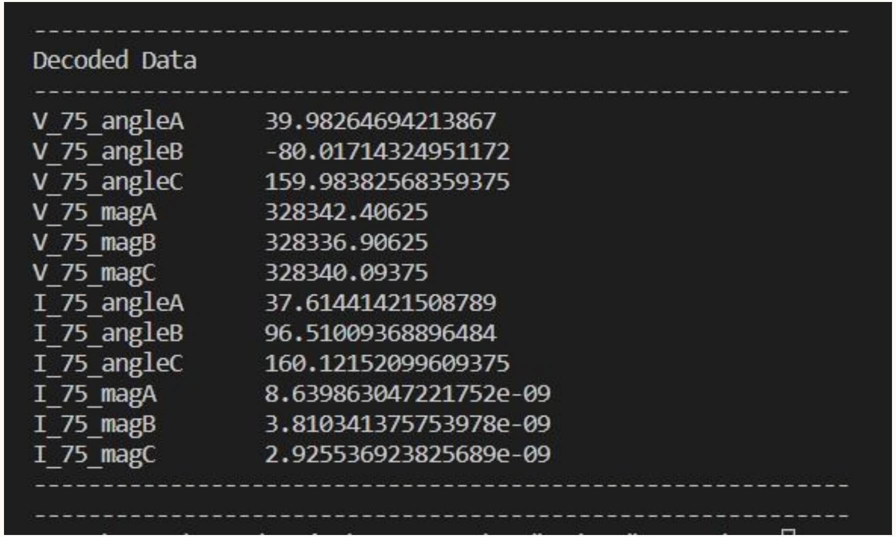


Fig 5: Block Diagram of MODBUS TCP



```
------------------------------------------------------------
Decoded Data
------------------------------------------------------------
V_75_angleA      39.98264694213867
V_75_angleB      -80.01714324951172
V_75_angleC      159.98382568359375
V_75_magA        328342.40625
V_75_magB        328336.90625
V_75_magC        328340.09375
I_75_angleA      37.61441421508789
I_75_angleB      96.51009368896484
I_75_angleC      160.12152099609375
I_75_magA        8.639863047221752e-09
I_75_magB        3.810341375753978e-09
I_75_magC        2.9255369238256 89e-09
------------------------------------------------------------
------------------------------------------------------------
```

Fig 6: Data decoded from MODBUS payload format as received from the server

WORK TO BE DONE

SIMULATE CYBERATTACKS

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	SIMULATING CYBER ATTACKS	TRAINING MACHINE LEARNING MODEL AND DRAWING INFERENCES AND RESULTS

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