CYBER-ATTACK DETECTION OF POWER CONVERTERS IN ISLANDED MICROGRID USING DEEP LEARNING APPROACHES

University of Moratuwa
E.Nanthaluxsan, S.Jalini, K.Kopikanth

Supervisor - Senior prof.Sisil Kumarawadu
Co-supervisor - Dr.V.Logeeshan

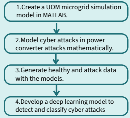
ABSTRACT

Islanded microgrids enhance power system sustainability but face rising cyber threats. This study proposes a deep learning model to detect and classify FDI and DOS attacks on solar inverters, battery inverters, and DC-DC boost converters. Real-time MATLAB tests confirm the model's effectiveness across varying attack scenarios.

SCOPE

Develop a deep neural network based cyber attack model in microgrid power converters using the data generated from the simulation model of UOM microgrid

OBJECTIVES



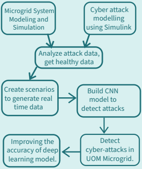
1.Create a UOM microgrid simulation model in MATLAB.

2.Model cyber attacks in power converter attacks mathematically.

3.Generate healthy and attack data with the models.

4.Develop a deep learning model to detect and classify cyber attacks

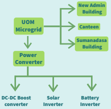
METHODOLOGY



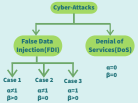
Microgrid System Modeling and Simulation
Cyber attack modelling using Simulink
Analyze attack data, get healthy data
Create scenarios to generate real time data
Build CNN model to detect attacks
Detect cyber-attacks in UOM Microgrid.
Improving the accuracy of deep learning model.

PROJECT INSIGHT

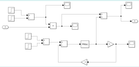
Microgrid



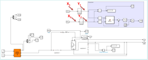
Cyber-Attack



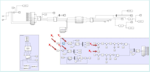
Cyber-attack model



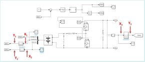
Solar Inverter & DC to DC Boost Converter



DC to AC converter

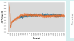


Battery Inverter

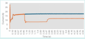


RESULTS

DOS Attack

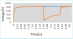


Battery Inverter-AC Voltage-α=0, β=0

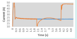


Solar Inverter-New Admin-Current Building-α=0, β=0

FDI Case1

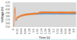


DC Voltage -DC to AC Converter New Admin Building – α=2 β=20

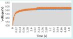


Current-Sumanadasa Building-Solar inverter-α=2, β=200

FDI Case2

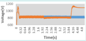


AC Voltage-Battery inverter α=50 β=0

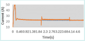


DC Voltage-Battery Inverter-Canteen α=50 β=0

FDI Case3



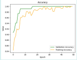
DC Voltage-DC to AC converter, Sumanadasa Building – α=1 β=20



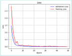
Current-Solar Inverter-Sumanadasa Building α=1, β=200

Deep Learning Approaches

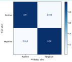
1.FNN Detection Model



Accuracy comparing training and validation in training

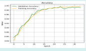


Validation loss and training loss

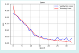


Confusion matrix output

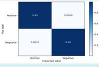
2.LSTM Detection Model



Accuracy comparing training and validation in training

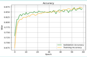


Validation loss and training loss change

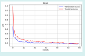


Confusion Matrix output

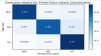
3.FNN Classification Model



Accuracy comparing training and validation in training



Validation loss and training loss change



Confusion Matrix output

CONCLUSION

Numerous graphs were generated to train cyber-attacks detection and classification model, identifying high-impact attacks on power converters. FDI Case 1 has the highest impact. The ANN model achieves 0.9533 detection accuracy and 0.901 classification accuracy, while the LSTM model achieves 0.9660 detection accuracy. Fine-tuning and hardware implementation are expected to be conducted in the future.