Towards Distance Relay Attack Discrimination for Situational Awareness-Based Anomaly Detection

Muhammad Nouman Nafees, Neetesh Saxena, Rashid Khan, and Pete Burnap
Computer Science and Informatics, Cardiff University, Cardiff, United Kingdom

Introduction

The distance protection scheme is one of the critical schemes in the transmission substation of smart grids for protecting transmission lines.

- The distance relay calculates the impedance magnitude from voltage and current phasors to determine if the fault is within the range of the tripping zone.
- Cyber-attack on distance protection relay zone settings can trigger a false tripping of circuit breakers or an overloaded transmission line.

Approach

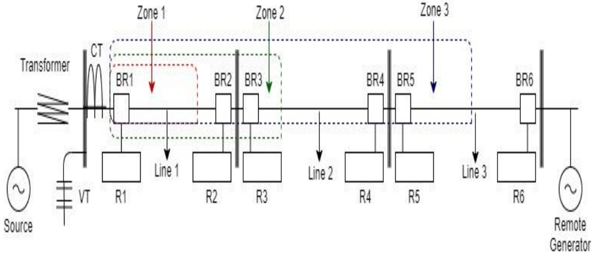
We propose an approach for attack detection and anomaly discrimination between distance relay attack, natural events and normal load disturbances on transmission lines.

- We utilize power system datasets and use Machine Learning (ML) algorithm by optimizing and applying the hyperparameters of ensemble classifier Bootstrap aggregation (Bagging) with the instance base learner as the base classifier.
- We identify the leading attributes in the anomaly detection algorithm.

System Description and Attack

System Description

- Three transmission lines that span from breaker 1 (BR1) to breaker 6 (BR6).
- The relays (R1-R6) are configured with distance protection scheme.
- The reach of tripping zone 1 setting of R1 is between 80-90% and its trip time is set to instantaneous.



Attack

Attack Scenario: Adversaries gain remote access to distance relays and extend the Zone 1 setting of R1 by overreaching to 180%.

Attack Consequences: In an event of a fault on transmission Line 2, BR1 will also be tripped in conjunction with BR4, since the corresponding relays of both breakers see the fault in their Zone 1.

Results

Power System Attributes: Relays' impedance measurement and voltage/current phase angle.

Classifier	ACC%	TPR	FPR%	PRCN
Naïve Bayes	70	70.43	36.1	73.1
J48	92.22	91.59	7.76	91.62
IBK-KD tree	95.35	96.40	1.19	96.6
Bagging-IBK-KD tree	97.53	96.60	1.18	96.76

Conclusion and Future Work

Conclusion: Fine-tuned Bagging-IBK achieves far better results compared to other ML algorithms.

Future Work: Further evaluation of different ML algorithms with respect to detecting both the under-reaching and over-reaching distance relay zone attacks.

Reference

D. Wilson, Y. Tang, J. Yan, and Z. Lu, “Deep Learning-Aided Cyber-Attack Detection in Power Transmission Systems,” in 2018 IEEE Power Energy Society General Meeting (PESGM), Aug. 2018, pp. 1–5, doi: 10.1109/PESGM.2018.8586334.