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
{nafeesm, saxenan4, khanrm1, burnapp}@cardiff.ac.uk

ABSTRACT

The discrimination between the sudden tripping of circuit breakers due to cyber-attacks and normal load disturbances is of paramount importance for better situational awareness in transmission substation settings. In this work, we propose an approach for attack detection and anomaly discrimination between distance relay attack, natural events and normal load disturbances on transmission lines. This is achieved by optimizing the hyperparameters of an ensemble machine learning classifier Bootstrap Aggregation (Bagging) with the base of Instance Base Learner (IBk). Numerical results show that our approach can discriminate and predict anomalies with 97.53% accuracy for three different scenarios including distance relay attack. The performance indicates that Bagging-IBk outperforms other algorithms.

KEYWORDS

Distance Relay Attack; Ensemble Classifiers; Machine Learning; Situational Awareness

1 INTRODUCTION

Distance protection is one of the critical schemes in the transmission substation of smart girds for protecting transmission lines. The distance protection relay calculates the impedance magnitude from voltage and current phasors along with the fault direction in transmission lines to determine if the fault is within the range of the tripping zone. Appearance impedance threshold and the trip time is assigned to each tripping zone, when a fault occurs, distance relay must detect and isolate the malfunctioned segment by tripping the circuit breaker connected to it. It is, therefore, a key component in protecting transmission lines.

Given its great importance, sophisticated adversaries can remotely access the transmission substation. They can change the zone settings of distance relays in a way that violates the distance protection coordination between other relays. For example, attackers can change the impedance setting of the distance relay to manipulate the tripping zone threshold. Consequently, there can be a false trip of circuit breakers or an overloaded transmission line. In either case, it can potentially cause a cascading effect of failures with an adverse impact on transmission substation operations. Thus, an optimum anomaly detection algorithm must be proposed to detect the malicious behaviour of such attacks. In this context, our work can enhance situational awareness among power system operators by enabling them to discriminate disturbances between normal power operations and cyber-attack led changes.

Existing Solutions: Various solutions have been proposed to classify cyber-attacks on power transmission systems [1], [2]. However, not sufficient work has been done in detecting attacks on zone settings of distance relay. Existing solutions are partially effective in the presence of cascading attacks.

Our Contributions: In this work, we utilize the power system datasets and consider the specific problem of zone setting manipulation of distance relays. we propose an approach for detecting cyber-attacks on distance relays by optimizing and applying the hyperparameters of ensemble classifier Bagging, a Machine Learning (ML) meta-algorithm. We argue that the ensemble classifier is more efficient as compared to other algorithms for power system datasets because it trains the algorithm on different regions for final classification. We identify the leading attributes in the detection algorithm in conjunction with comparing our results with other popular ML algorithms. We argue that our proposed approach not only efficiently detects attacks but also discriminate between attacks on distance relay and normal load disturbances.

2 SYSTEM DESCRIPTION AND ATTACK MODELLING

We describe here a power system scenario with a particular focus on relay zone settings. In addition, we also construct a viable attack modeling and discuss the impacts of the attack.

System Description: There are three transmission lines that span from *Breaker 1 (BR1)* to *Breaker 6 (BR6)*, as shown in

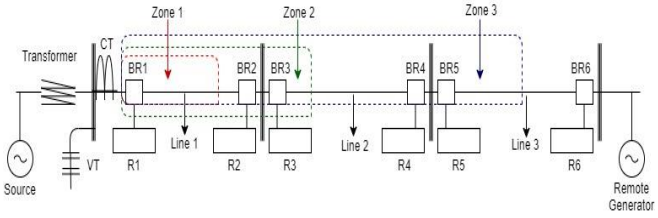

Figure 1: Relay Zone Settings.

Figure 1. The narrative will focus on *Relay 1 (R1)* of *BR1* but the same principle applies for all breakers and relays. The *R1* of *BR1* is configured with a distance protection scheme, which measures its current through a current transformer, voltage through a voltage transformer and trips the breakers once the

fault is detected using the impedance seen by *R1*. The reach of tripping *Zone 1*, *Zone 2* and *Zone 3* settings of *R1* are between 80-90%, 110-120% and 240-250% respectively. To this end, the trip time for *zone 1* is set to instantaneous.

Attacker and Attack Modelling: *Assumptions on the capabilities of attackers*: It is assumed that attackers have advanced knowledge of distance protection coordination principles of relay settings with respect to its tripping zones. Besides, it is also assumed that the adversaries have already gained access to the transmission substation system and they can remotely issue commands from the substation switch.

Assumptions on the motivation of attackers: It is assumed that attackers have the intention of causing a cascading effect of failures in the transmission substation by manipulating the distance relay settings. It is assumed that their eventual objective is to cause power blackouts.

*Attack Scenario***:** In our attack scenario, the adversaries start the attack by getting access to the substation switch, gain remote access to distance relays. Next, they extend the *Zone 1* settings of *R1* by overreaching to 180%. Since there are overlapping zones for transmission line protection, the same fault on *Line 2* will be detected and responded to by both *R1* and *R4* as a consequence of relay setting manipulation.

Risk and Impact Analysis: 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*. Consequently, both *Line 1* and *Line 2* will be tripped due to an instantaneous trip time of *zone 1*. This attack can overload the transmission *Line 3* to carry more power flow, which can potentially trigger cascading failures in power systems. In addition, the mechanical input of the power generators cannot be adjusted or reduced in time to compensate for the loss in power load. Therefore, the rotor angle of the generator increases to the point where it is unable to synchronize with other generators and can experience rotor angle instability. Consequently, this may lead to voltage collapse across the transmission substation in the worst-case scenario.

3 ANOMALY DETECTION AND EVALUATION

In our experiment, we consider three types of scenarios for our anomaly detection analysis, as shown in Table 1.

Table 1: Scenarios for Anomaly Detection

No.	Scenario	Description
1	No events (normal operation)	Normal operation load changes
2	Natural event (single line-to-ground fault)	Fault from 20-79% on Line 2
3	Cyber-attack on distance relays	Fault from 20-90% on Line 2 with Relay 1 setting changed

Detection using Bootstrap Aggregation (Bagging): We used the Weka tool to run ensemble classifier Bagging, a meta-algorithm that aims at improving the accuracy of the basic algorithms, for anomaly detection. To use bagging, we used the Lazy algorithm, IBk (K-Nearest Neighbor), for the aforementioned ensemble learning classifier. In the case of IBk, we used the search algorithm K-Dimensional tree (KD-tree), a space-partitioning data structure, to speed up the task of finding the nearest neighbors. Next, we fine-tuned the hyperparameters of the algorithm using the experimenter interface of Weka. We used the "InfoGain Ranker" method in Weka to derive the leading attributes in classification results. The leading attributes were impedance measurements for relays, voltage and current phase angles, and voltage and current magnitude. We repeated the experiment using other algorithms and a comparison is given in Table 2. It is observed that Bagging-IBk achieves far better results in all evaluating parameters as compared to the other four algorithms. Bagging-IBk also outperformed the results in [2] for the multiclass classification events. Therefore, it demonstrates that the proposed bagging-IBk is efficient for anomaly detection in the power system settings.

Table 2: Comparison of ML Algorithms for Anomaly Detection

Classifier	Accuracy%	TPR%	FPR%	Precision%
Naïve Bayes	70	70.43	36.1	73.1
JRip	92.12	91.59	8.92	91.7
J48	92.22	91.59	7.76	91.62
BK-KD tree	95.35	96.40	1.19	96.6
Bagging-IBK-KD tree	97.53	96.60	1.18	96.76

4 CONCLUSION AND FUTURE WORK

We have constructed a viable cyber-attack scenario for distance relay attacks. To this end, we have proposed an anomaly detection approach that applies an optimized ensemble bagging-IBk algorithm. In the future, we aim to further evaluate different ML algorithms with respect to detecting both the under-reaching and over-reaching distance relay zone attacks. We also intend to consider the critical clearing time attribute in our power system datasets for the aforesaid attacks' detection.

REFERENCES

[1] 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.

[2] R. C. B. Hink, J. M. Beaver, M. A. Buckner, T. Morris, U. Adhikari, and S. Pan, "Machine learning for power system disturbance and cyber-attack discrimination," in *2014 7th International Symposium on Resilient ControlSystems (ISRCS)*, Aug. 2014, pp. 1–8.