Utility Perspective towards Machine Learning Techniques in Power System Protection

Alaa Magdi Ali[1], Mukesh Kumar[2], Valliammai Muthukaruppan[3] , Syed Fahim Ahmed[4]

[1]Engr.-Trans. Prot. Engg., Dubai Electricity & Water Authority, UAE
[2]Engr.-Trans. Prot. Engg., Dubai Electricity & Water Authority, UAE
[3]Engr.-Trans. Prot. Maint., Dubai Electricity & Water Authority, UAE
[4]Sr. Engr.-Trans. Prot. Engg., Dubai Electricity & Water Authority, UAE

---***---

Abstract - *The fourth industrial revolution has made it possible to gather massive amounts of operational data generated from several Intelligent Electronic Devices (IEDs) and harvest them for an automatic higher cognitive process including detection and diagnosis of faults* [1] [2] [3] *with the aim to increase the useful lives of various components or instruments. During recent years, many authors have written research and scientific papers on application potential of Machine Learning (ML) techniques in power system protection which prompted power utilities around the world to have keen eye on the developments on this front. This paper aims to present utility perspective towards machine learning techniques citing limitations of various ML techniques and why ML has not been able to generate enough confidence among utilities and relay manufacturers as they still depend upon legacy protection techniques that are developed using mathematical models.*

Key Words - Machine Learning, Utility, Power system, Protection, Artificial Intelligence

1. INTRODUCTION

Power System Protection is one of the foremost complex disciplines in engineering science which needs not only the right understanding of the various components of a power system and their working principles but also a decent knowledge on the analysis of the abnormal behaviors and failures that may occur in any component of a protection system. Basic understanding of how protection system works and also the operational constraints involved in it must be the primary step in any trial to apply Machine learning (ML) to varied power system protection problems. It is also important to have decent understanding of the the history and development of the protection system. At a broader level, protection system operations are guided by some design principles, e.g. The protective devices shouldn't operate, if there's no fault exists within the system. If there occurs a fault, protective devices should operate within a specified amount of time to interrupt the flow of current. In transmission systems, rapid clearing is vital to make sure the system is stable. In certain applications, faults should be cleared in milliseconds. Redundant protection system is also considered in essential applications where backup system takes over if the primary protection fails to detect a fault. When a fault occurs, the designated primary protective device should operate first, which is designed to interrupt the fewest number of customers. Backup protection should operate to clear the fault in case primary protection fails to act, while still limiting the amount of affected customers.

Fuses have been used as essential protection devices from the early days of electrical engineering, which remains the most common protection device in the power system even today. Fuses have several desirable characteristics. Fuse is cheapest type of protection in an electrical circuit and needs zero maintenance. The operation of a fuse is very simple and no complexity is involved and it is believed that they are failsafe because they contain fewer moving parts. Despite these many benefits, one major disadvantage of using a fuse is that, it cannot be used more than once. This limitation was overcome by the development of circuit breakers which need not to be replaced after each operation and can interrupt hundreds of faults before being replaced or refurbished.

To coordinate with the massive numbers of fuses that were already installed, early electromechanical relays and modern microprocessor relays employ time–overcurrent curves that mimic the operating characteristics of fuses. This arrangement has proved so reliable and value effective that it remains the predominant method of protecting transmission and distribution systems. It is important to notice that more advanced protective arrangements do exist in the transmission system, including impedance calculations, traveling waves [4], differential relaying, and so on. While the individual methods may be different, the overall operating principles remain the same: operate if there is a fault; do not operate if there is no fault; isolate the fault to the smallest possible section of line; take over if the primary device has not operated in a timely manner. In nutshell, power system protection has functioned remarkably well during the past

100 years. This is not to say that it is perfect, that it never fails, or that there is no room for improvement. It must be acknowledged, however, that even when the system fails, it often does so in predictable, understandable and most importantly, correctable ways. Although, Machine Learning (ML) is a promising field that is predicted to improve and even revolutionize many engineering processes, but if we talk specifically about power system protection, nothing significant is achieved in operational field. Even after many years of research, published papers and viewpoint of various scholars, not a single ML based protection relay found its way to commercial production. In our view, ML-based approaches lack credibility mainly due to the following critical requirement of an efficient protection system:

- Reliability: The primary and foremost requirement of any protection system is reliability. When deployed in the field, protection schemes must perform correctly during events outside the scope of simulation results supporting various ML models and laboratory testing. Mathematical or Physics-based methods, although they might fail from time to time, are more amenable to being adjusted, as the underlying principle is clear, unlike the "black box" that comes from the ML techniques. Moreover, fault parameters can vary a lot that it is impractical to cover all potential scenarios when training an ML based model. When faced with a scenario that was not considered during training, the response of an ML-based method cannot be predicted, while mathematical model-based approaches will still perform within an acceptable margin of error.

- Security: Another requirement of a protection scheme is security. It must not operate under any "normal" system transients and during any faults outside its primary zone. This feature is built into legacy schemes, whereas the ML approaches proposed in scientific papers do not provide any credible evidence for security.

- Selectivity: The design of protection schemes based on mathematical model ultimately succeeds in curtailing significant damage in most cases, even if one device fails to operate. On the other hand, ML based methods are not saying anything on effective backup that fulfills the "selectivity" aspect of power system protection.

In addition to above, one of the primary requirements to train and test ML-Based method is acquiring enough high-quality field data which is considered a necessity by many ML researchers and getting these data are tremendously challenging, requiring cooperation among industry, academia, and multiple utility partners. Such a project would require years of effort along with substantial investments of money and personnel despite significant uncertainty about the long-term return on investment. While multiple efforts are currently underway to form large data sets that could be used to train ML methods for a variety of power system applications, none of these initiatives seems likely to produce a data set suitable for training ML based protection schemes. When protecting millions of dollars of equipment and human lives, manufacturers, utilities and industry continue to place their faith in physics-based methods. The various ML methods proposed by authors need specific training which poses the challenge of scalability and practicability of these methods [5]. The above points are explained in more detail in the rest of this paper, with a particular focus on transmission systems, although the arguments can also be extended to distribution protection system.

2. INTRODUCTION OF MACHINE LEARNING IN PROTECTION SYSTEM

Machine learning is that the study of computer engineering that use computational algorithms to "learn" information from data to formulate a model, called "training data", and after they do tasks like humans they will perform adaptively because the data availability increases. It is first proposed in 1956 and gradually considered as an acceptable tool for fault diagnosis, thanks to its ability to scale to large systems with low computational cost [6]. Machine learning techniques are often mainly classified into three types: supervised, unsupervised and reinforcement learnings.

The conventional machine learning techniques are usually supervised learning, including the expert system, back propagation neural network, Bayesian network, support vector machine etc. [7]. With the overall recognition that the traditional techniques can now not efficiently and accurately handle the vast amount of information, trending machine learning techniques have attracted more and more researchers' interest over the past years. A range of machine learning techniques, especially deep learning, transfer learning, unsupervised learning methods are proposed to deal with the challenges in various application domains of the modern power system protection.

Most ML-oriented papers point to multiple areas where conventional protection struggles, for instance, the detection and site of high-impedance faults; complexities introduced by changing topologies, like microgrids; reverse power flows created by the increasing prevalence of distributed energy resources; and adaptively setting system integrity protection schemes. We certainly agree that conventional methods have so much room for improvement, and in some scenarios, we see ML techniques providing useful augmentation to traditional approaches. Most academic papers, however, do not propose ML methods as supplements to existing classical protection or physics-aware solutions but as complete replacements. The subsequent sections in this paper describes specific challenges various ML based methods face in protection applications. These challenges mentioned under below categories are intended to present a summary of a number of sensible considerations that are often overlooked within the ML-based protection literature and significantly impact the adoption of ML based methods in commercial systems.

3. LIMITATIONS OF VARIOUS ML TECHNIQUES

3.1 Expert Systems

Expert systems (ES) are part of a subdivision of Artificial Intelligence, the symbolic branch. This symbolic technique makes extensive use of knowledge obtained from human specialists [7]. It is basically a computer program that provides expert-level diagnosis knowledge to automatically identify the health states of equipment. It was first proposed by Edward Feigenbaum and Joshua Lederberg in 1965, and was then widely applied in fault diagnosis [8]. The expert system-based diagnosis models consist of the inference engine, the knowledge base, the user interface, the database, and the explanation system [9] [10]. An inference engine is a component of the expert system that enables the expert system to draw deductions from the rules in the knowledge base. A knowledge base can be defined as an organized collection of facts and heuristics about the corresponding domain. In an expert system, the accuracy of the diagnosis results is greatly influenced by the interpretation of expert knowledge. Furthermore, it is difficult to update or expand the knowledge base due to the low self-learning capability of the expert system, and this limitation discourages its use in the field of power system protection.

3.2 Decision Tree

Decision trees are a type of supervised learning algorithm where the data is continuously split according to certain parameters until it is assigned a particular class label. Given their intelligibility and ease [9], decision tree technique is used for both classifications and regression tasks. A decision tree is basically a flowchart structure that includes internal nodes, branches and a terminal node. Each internal node represents a “test” on an attribute, outcome of the test is represented by a branch and the final result taken after the computation of all the attributes is represented as a leaf node and it is termed as class label. A root node is the starting point of any decision tree algorithm and then comparison of values of different attributes are done followed by the next branch until the end leaf node is reached.

Although Decision tree algorithm is effective and extremely simple, logics get transformed if there are even small changes in training data and interpretation of larger trees becomes difficult. Overfitting is another challenge faced in decision tree algorithm which results due to adaptation of the training data by the tree structures generated, when decision trees are left unrestricted. To avoid these, we need to restrict it during the generation of trees that are called regularization, which would in turn weaken the diagnosis performance.

3.3 Artificial Neural Network

Artificial neutral network (ANN) is a supervised machine learning method which imitates the information processing activities of human brains. In [11] [12] [13] [14], various ANN-based methods are applied for fault identification in the distribution system for estimating fault distance, detecting high impedance fault and identifying the fault types.

The major disadvantage of ANN method which has made power utilities and protection engineers skeptical about its implementation in power system protection is its black box nature. ANN has the ability to approximate any function, it can study its structure but do not give any insight on the structure of the approximated function. In simple words, we do not know why and how a neural network came up with a particular output. A well-trained ANN algorithm may provide accurate results most of the time but when the cost of failure is very high as in case of protection system, knowing what is going on inside a system is an absolute necessity.

3.4 K-Nearest Neighbor

The K-Nearest Neighbor (KNN) based method is one of the simplest Machine Learning algorithms based on supervised learning technique and used mostly for classification problems. This method works by seeking to minimize the distance between the test and training observations [9]. KNN algorithm matches the new data with the available data and put the new data into the category which is most similar to the available categories. In this method, a distance metric is used to train k similar neighbors by searching the entire training dataset.

It is worth mentioning here that KNN works well with a small number of data inputs, but struggles when the amount of inputs dramatically scales up or the distribution of the inputs are imbalanced. In case of high dimensional problems that have very large distances between data points and where training data may be similar, the performance of the diagnosis models is sensitive to the parameter k which is difficult to be determined. The large distance between data points also leads to high computational cost for all the training samples.

3.5 Support Vector Machine

Support vector machine (SVM) is a supervised learning method, which is able to generalize between two different classes if the set of labelled data is provided in the training set to the algorithm and it is widely used in classification and regression tasks. Many researches have been conducted on the fault diagnosis in the power system using this method. In [15] [16], SVM-based methods are used to identify the fault types and the fault distance of the transmission lines.

The main function of the SVM is to create best decision boundary for segregation of n-dimensional space into classes, so that in future if a new data point comes that is to be classified then it can be classified easily. Although, SVM-based methods provide high stability due to dependency on support vectors instead of data points and can work very well with a small number of various data, such as unstructured and semi structured data, i.e., images and texts but dealing with large amount of data may lead to computational burden in SVM. In addition, the performance of SVM-based diagnosis models is very sensitive to kernel function and hyper-parameters and an appropriate kernel parameter is not easily determined.

4. MALOPERATION/NONOPERATION CONSEQUENCES

In many ML applications where error of margin is high, even the complete failure of a model is not very problematic. For instance, a face recognition model which we use very often these days in cellphones fails occasionally to recognize the face, but that does not cause great concern to its user. On the other hand, if we talk about power system protection, we are not having such leverage. It is a critical safety system where a malfunction may result in some irreparable damage to the users. The damage resulting from the maloperation or nonoperation of a protection system is not only limited to some economic or services issues but it can cost human lives. In business perspective, these failures will cause serious damage to the power company or utility reputation and reliability. Due to these reasons, utilities are sceptical about the use of machine learning based protection system and rely on traditional methods in the area of power system protection.

5. COORDINATION ISSUES

Coordination between the protection at different voltage levels is one of the issues that is often left unaddressed in most ML based protection papers. For instance, for an ML based method, how to ensure that an industrial internal protection will trip faster than the utility at higher voltage level? It is not entirely clear. Adequate coordination between ML based transmission and distribution system and how an ML based protection coordinates with large number of fuses present in the protection system, are some of the questions which are still not clear in the research papers. When coordination is considered, the most commonly proposed ML based protection solutions tend toward multiagent models that often rely on low-latency communication links to inform trip decision making. A dependence on such communication links can be a serious dependability and reliability concern.

6. LACK OF QUALITY DATA FOR TRAINING ML MODELS

All ML based systems depend on data to derive their predictive power. Due to this, availability of high quality data is one of the key requirement of any ML based technique to train and validate the system and provide intended results. One of the challenges faced to acquire data for training an ML algorithm is incomplete, inaccurate and improperly labelled data which results in errors. Having massive amount of data is also one of the issues many ML based techniques faces which is contrary to the common thought that, in ML, the more data you have, the better. Although it is possible to generate massive amount of data from the various sensors or IEDs placed in power system, it doesn't imply that all the data collected is useful to train ML based protection algorithm. If we feed irrelevant data without separating useful data, it might result in data noise where ML based systems learns from variances and nuances in the data rather than the more significant trend. This problem is multiplied due to multipoint monitoring of data, on which most of the ML based methods rely to solve coordination issues. On the other hand, shortage of data has its own problems. It might be possible to get accurate results with small data set in a test environment but that doesn't necessarily be applied in practical environment because it typically requires more data. Another practical limitation of ML techniques is its topological dependency. In ML based protection papers, it is not effectively demonstrated that the data collected at point X in a power system circuit is appropriate to train the ML model intended to be deployed at another point, say Y in the same circuit. This creates the need to train the ML models for every circuit which is a practical challenge unless proved otherwise. Data sparsity is another issue when a data set contains insufficient amount of specified expected values or there is some missing data. This inconsistency in acquiring data can be resulted from disparate devices used for collecting the data. Another point worth noticing that different measuring and recording devices used to collect data has their own way of doing so. For instance, a protection relay usually looks for 50Hz or 60z fault data and may intentionally filter higher order harmonics. Similarly, A Phasor Measurement Unit (PMU) are concerned with magnitude and angle of voltage may not record or analyze a point on the wave data [5]. The point here is that, it is not very convincing to acquire data from these different devices and use them in training a ML algorithm. These data sets may be useful in applications where margin for error is higher but these data sets are certainly not suitable for training protection-based ML techniques where margin for error is very low or negligible.

Another challenge of collecting high quality data for power system protection comes from the fact that real power system faults are usually unpredictable and unstable but theoretically it is often treated as stable phenomena with constant or zero fault impedance which is not the actual scenario. In reality, significant changes in impedance can be experienced during the duration of the fault based on the unique physical circumstances around or at the fault area and these cannot be modeled or predicted with accuracy in a ML technique. Incorrect or improper data labelling is another issue which is faced by many supervised machine learning models. Correctly labelled data is mandatory to enable ML systems to establish reliable models for pattern recognition. The reason behind improper or incorrect labelling is the complexity and expensiveness involved in the process as data labelling often requires human resources to put metadata on a wide range of data types.

Training a production model often requires real world data but several research papers related to protection system suggests researchers are using simulated waveforms to train and validate their fault detection algorithm which are not representing the real-world fault conditions. Simulated data may be useful to train some models but they are certainly not a substitute of actual field data. While there are many reasons of low-quality data, researches need to pay attention towards the various channels and sources from where the data being collected to train ML models and run regular checks to keep the data accurate and in the right format. Having said that, we are yet to come up with the accurate data set that would allow researchers and data scientists to train and validate production grade ML algorithm for power system protection applications.

7. RELIABILITY CONCERNS

The performance of an ML algorithm is often measured is terms of classification accuracy. While this metric to evaluate an algorithm is good but gives false sense of achieving high accuracy. This metric works well if we have equal number of samples or data belonging to each class which is not normally the case. In a training data set we often have higher percentage sample of a particular class in comparison to the other sample class. The classification accuracy changes significantly when a particular class of sample data increases or decreases in comparison to the other class. Even a model that claims a classification accuracy of 98% or 99% could result in failure when deployed in the field across any utility having many circuits. In addition, the authors present their results without proper consideration of operational circuit scenarios in their analysis. This creates serious reliability concern towards the trained ML based protection model results because those results are very unlikely to be reproduced in the operational circuit.

8. LACK OF DEBUGGING OPTIONS

Troubleshooting the incorrectly operated protection system and providing the solution for the same is one of the important tasks protection engineers are often concerned about. In case of legacy protection system, generally it is possible to analyze the problem by plotting the operating characteristics of protection devices to find out which relay operated as expected and which one maloperated or not operated as anticipated. By analyzing and understanding the real cause behind the maloperation or non-operation, it is possible to provide the remedy by adjusting the settings to achieve intended results in future. Unfortunately, In case of ML based protection system, the authors or researchers have not dived deep into the process of understanding the reason behind the incorrect operation of a particular proposed scheme designed for a particular operation. This issue is very much derived from the black box nature of these algorithms. Lack of understanding of why a problem occurred will hinder the possibility of providing the correct solution to the problem or debug the system, in absence of which the system will continue to give incorrect results which can be very costly if the same is deployed in the field of power system protection.

9. CONCLUSION

Throughout the time in history and experience, the protection engineers understand that, what might appear good in a paper will find real challenge in implementation. The same can be said about ML based protection algorithms. Protection engineering is the skill, experience and best practices of selecting and setting relays and other protective devices to provide maximum sensitivity to faults and other undesirable conditions without compromising on the core objectives of a protection system i.e., reliability, security, selectivity, speed of operation, simplicity and economic viability. The cost of protection failures is very high, due to which the utilities are still relying on conservative, transparent, and simple solutions. The meticulous nature of protection engineers and power utilities in adopting ML based protection methods is attributed to the fact that, if the algorithm fails or malfunctions, it could mean shutting down the power from essential industries, hospitals etc. and the liability of the irreparable damages resulting from the same will fall upon the concerned engineers and power companies or utilities.

On the other hand, when we are aiming to counter most of the world problems by providing solutions with machine learning, it will be so naïve to out rightly negate the developments of machine learning in the field of power system protection. So, instead of aiming to replace the mathematical model of legacy protection system with machine learning techniques as several ML based papers suggest, a more worthy pursuit for ML based techniques will be to provide support to the existing protection system where it is found vulnerable. Currently, as a utility, we see serious structural barriers to the inclusion of ML approaches in operational power system protection that are not easily overcome with more data or computational ability. Until we solve the challenges mentioned in this paper which we are hopeful will ultimately be solved seeing the enthusiasm of ML professionals, the utilities and power companies will continue to rely on tried and tested proven protection system in foreseeable future.

ACKNOWLEDGEMENT

The authors are grateful to the researchers, authors and publishers of various articles and research papers cited and referenced in this paper. The authors also acknowledges the help received from the journals from where the content for this article is discussed and reviewed.

REFERENCES

[1] Dalstain T. and Kulicke B., "Neural network-approach to fault classification for high speed protective relaying," IEEE Trans. Power Delivery, vol. 10, no. 2, pp. 1002-1011, April 1995.

[2] Kezunovic M. and Rikalo I., "Detect and Classify faults using neural nets," IEEE Computer Applications in Power, vol. 9, no. 4, pp. 42-47, Oct 1996.

[3] Coury D.V., Oleskovicz M. and Aggarwal R.K., "An ANN routine for fault detection,classification and location in transmission lines," Electrical Power Components and Systems, vol. 30, pp. 1137-1149, 2002.

[4] Desikachar K.V. and Singh L.P., "Digital Travelling–Wave Protection of transmission lines," Electric Power Systems Research, vol. 7, pp. 19-28, 1984.

[5] Jeffrey Wischkaemper and Sukumar Brahma, "Machine Learning and Power System Protection," IEEE Electrification Magazine, pp. 108-112, March 2021.

[6] L. Zhang, J. Lin, B. Liu, Z. Zhang, X. Yan and M. Wei, "A Review on Deep Learning Applications in Prognostics and Health Management," IEEE Access, vol. 7, pp. 162415-162438, 2019.

[7] J. Giarratano and G. Riley, "Expert System - Principles and Programming," in PWS Publishing Company, Bostan,USA, 1998.

[8] Lee H.J., Park D.Y., Ahn B.S., Park Y.M., Park J.K. and Venkata S.S., "A fuzzy expert system for the integrated fault diagnosis," IEEE Trans. Power Deliv., vol. 15, no. 2, p. 833–838, April 2000.

[9] Lei Y., Yang B., Jiang X., Jia F., Li N. and Nandi A.K., "Applications of machine learning to machine fault diagnosis: A review and roadmap," Mechanical Systems and Signal Processing, vol. 138, p. 106587, April 2020.

[10] Minakawa T., Ichikawa Y., Kunugi M., Shimada K., Wada N. and Utsunomiya M., "Development and implementation of a power system fault diagnosis expert system," IEEE Trans. Power Syst., vol. 10, no. 2, p. 932–940, May 1995.

[11] Purushothama G.K., Narendranath A.U., Thukaram D. and Parthasarathy K., "ANN applications in fault locators," International Journal of Electrical Power & Energy Systems, vol. 23, no. 6, pp. 491-506, August 2001.

[12] Hagh M.T., Razi K. and Taghizadeh H., "Fault classification and location of power transmission lines using artificial neural network," 2007 International Power Engineering Conference (IPEC 2007), pp. 1109-1114, 2007.

[13] Javadian S.A.M. and Massaeli M., "A fault location method in distribution networks including DG," Indian Journal of Science and Technology, vol. 4, no. 11, pp. 1446-1451, 2011.

[14] Y. Aslan, "An alternative approach to fault location on power distribution feeders with embedded remote-end power generation using artificial neural networks," Electr Eng, vol. 94, no. 3, pp. 125-134, September 2012.

[15] Ray P. and Mishra D.P., "Support vector machine based fault classification and location of a long transmission line," Engineering Science and Technology, an International Journal, vol. 19, no. 3, pp. 1368-1380, September 2016.

[16] Pradhan A.K., Routray A. and Biswal B., "Higher order statistics-fuzzy integrated scheme for fault classification of a series-compensated transmission line," IEEE Trans. Power Delivery, vol. 19, no. 2, pp. 891-893, April 2004.