A Review of Three Methods of Artificial Intelligence in Smart Grid Cyber Security: Machine Learning, Reinforcement Learning, Ensemble Methods

Luyao Xu*

College of Engineering and Physical Sciences, University of Birmingham, Birmingham, UK

*Corresponding author: LXX365@student.bham.ac.uk

Abstract. Renewable energy is gradually replacing traditional fossil fuels. The change of power generation energy structure brings new challenges to the traditional power grid. Through the efficient bidirectional movement of electricity and information, smart grids might include renewable energy. For the complex informational and financial operations required by smart grid, communication systems are crucial, but they also make smart grid vulnerable to numerous cyber attacks. Smart grid cyber security has been widely concerned. The purpose of this paper is to explore the use of artificial intelligence technology in smart grid cyber security. Three methods in the field of artificial intelligence are highlighted: Machine Learning, Reinforcement Learning, and Ensemble Methods. This paper summarizes the benefits and drawbacks of their use of smart grid cyber security, and further makes a qualitative comparison of the three methods from multiple performance indicators.

Keywords: Smart grid, cyber security, artificial intelligence, machine learning, reinforcement learning, ensemble methods.

1. Introduction

Due to the growing concern for a clean environment, individuals believe that relying on traditional fossil fuels leads to carbon dioxide emissions and other environmental pollution. The deployment of renewable energy sources (RES) has been extensive worldwide [1]. New challenges have arisen for the traditional power grid due to the change in power generation energy pattern. Due to the instability and randomness of solar power generation, the danger of safe and stable functioning of the conventional power system dramatically increases. The smart grid has improved the electrical infrastructure. In order to build automated, distributed, and cutting-edge energy delivery networks, smart grids use the two-way flow of electricity and information [2].

Smart grid makes use of information technology and bidirectional connectivity to provide energy to the end user. The smart grid, as defined by The National Institute of Standards and Technology (NIST), is a power grid system that incorporates various digital computer and communication technologies and services into the infrastructure of the power system [3]. The seven logical areas that make up the smart grid are bulk generation, transmission, distribution, customer, markets, service provider, and operations [3]. Figure 1 shows an overview of the participant interaction structure in several smart grid domains [3].

Smart grid's proper operation is highly dependent on the advanced communication infrastructure because of the exchange of large amounts of data [3]. The vulnerability of smart grids to communication attacks is a result of this. Communication system attacks have the potential to cause a significant increase in operating costs or cause damage to the system's proper operation [3]. Smart grid technology requires a comprehensive solution to protect and prevent cyber security issues [3]. Various solutions have been proposed and continuously improved by researchers in related fields to improve the security and reliability of smart grid cyber systems. Mostly based on detection and identification, these methods include encryption, cryptography, network authentication, and others. There is a greater variety of artificial intelligence technologies, 5G technologies, blockchain, and data aggregation methods.

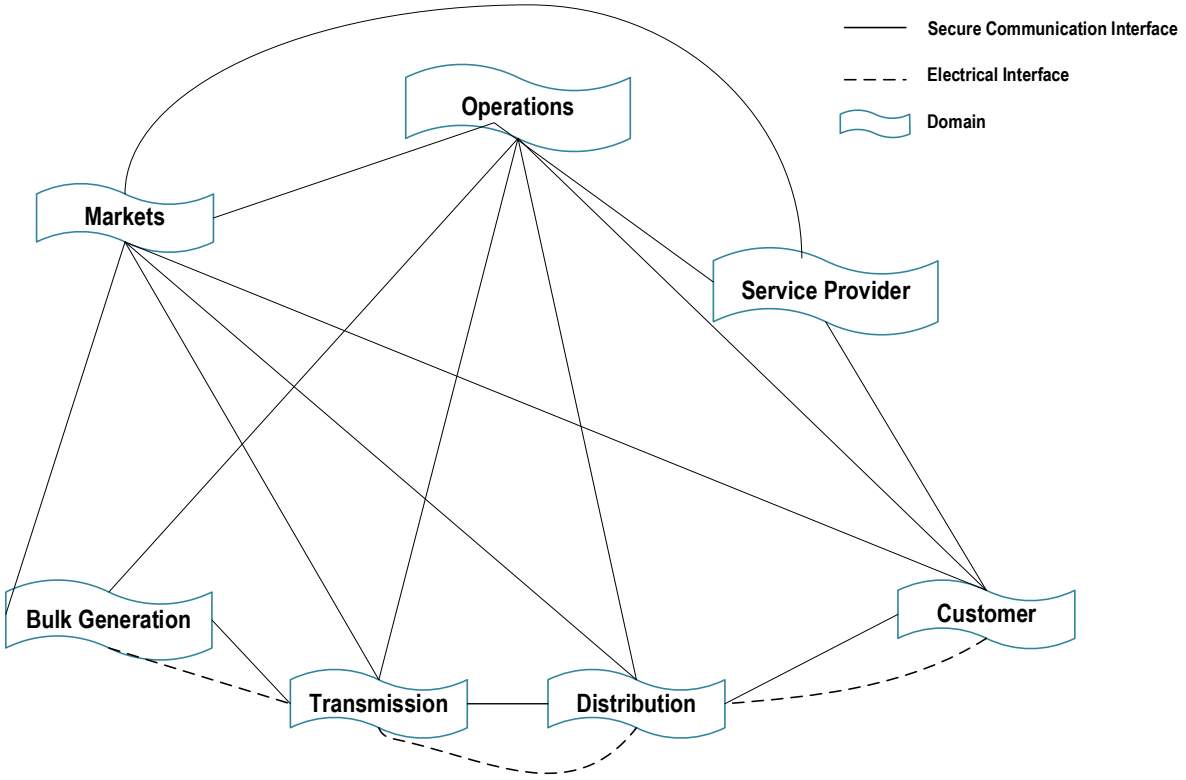

Fig. 1 Smart grid architecture [3]

The large amount of data produced by smart grid systems requires artificial intelligence(AI) technology to be used because traditional computing technology does not have enough capacity to handle it [4]. This paper mainly studies artificial intelligence technology in smart grid cyber security. In the related studies published in the past 7 years, this paper further compares and discusses the three main artificial intelligence methods (Machine Learning, Reinforcement Learning, Ensemble Methods) in terms of cyber attacks. Section 2 presents a classification method for smart grid cyber attacks. Section 3 discusses the principles of Machine Learning, Reinforcement Learning and Ensemble Methods, and gives examples for the application of the three methods in cyber security. Section 4 compares the three methods from computational complexity, data adaptability, classification accuracy, precision value, computational expense and so on. Finally, section 5 summarizes the study.

2. Cyber Attack Classification

In past studies, the authors made different classification methods of smart grid cyber attacks. Then a classification method for cyber attacks according to the three basic principles of cyber security will be introduced in detail [5]. The three basic principles of cyber security are Confidentiality, Integrity, and Availability. The most important aspect of cyber security, according to these three fundamental principles, is encryption [5]. Attacks on data and information on the Internet may have an impact on these three tenets. To uphold these fundamental ideas, it is crucial to build cyber security. Without these three fundamental tenets, cyber security is regarded as being open to cyberattacks. The definition and features of the fundamentals of cyber security are covered in the discussion that follows.

(1) Confidentiality: On a computer or server, everyone keeps private information. Confidential information must only be accessible by the group of authorized users. Attack risk is inversely correlated with data relevance. Depending on how important the data is, protective steps should be implemented. Password assaults, key logger, and other situations where user information is encrypted or protected will see more of these attacks. Important information will leak under these kinds of attacks on confidentiality.

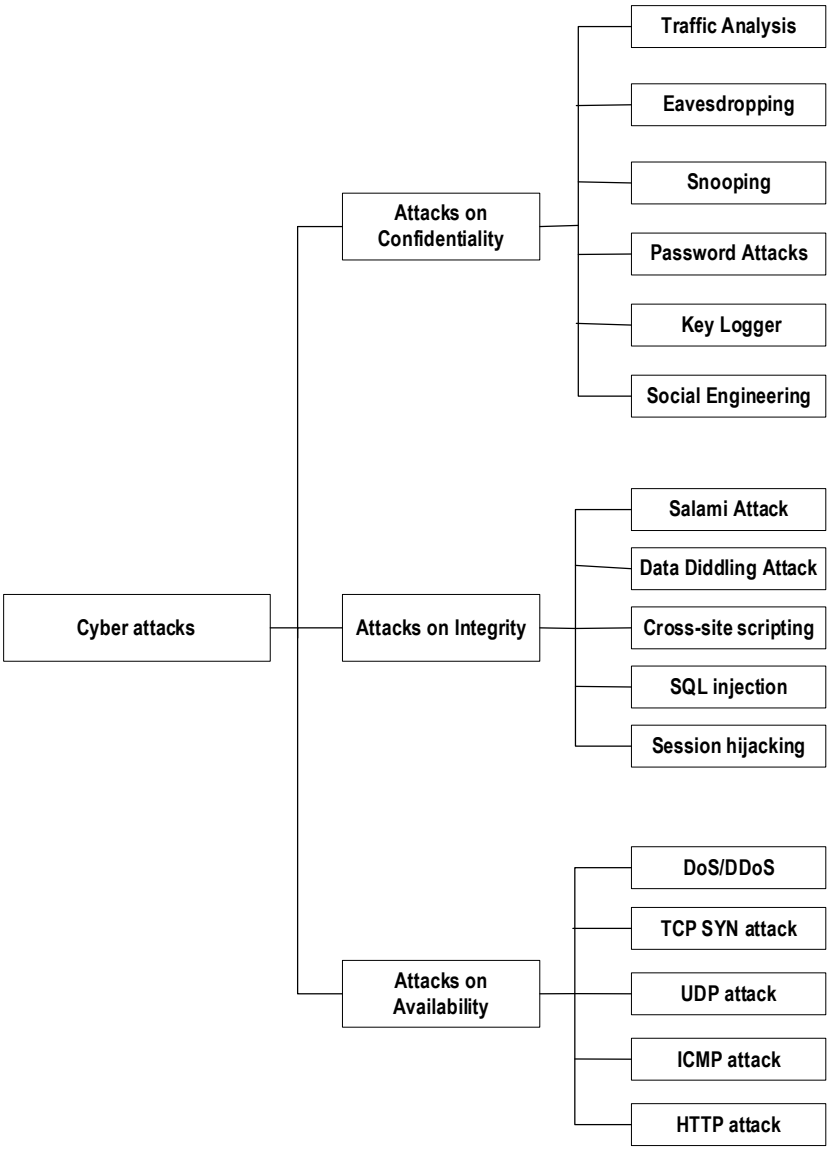

Fig. 2 Classifications of cyber attacks [5]

(2) Integrity: On the Internet, data and information are susceptible to malicious manipulation. Integrity guarantees the quality and consistency of the data on the network. By implementing the necessary safeguards, such as digital signatures, user access control, and file permissions, the integrity of information and data in cyberspace can be preserved. Attacks of this nature, such as Data Diddling Attack, Session Hijacking, and others, will be more prevalent where users have access to information. If attacks on integrity are made, there will be malicious tampering with the data and other drawbacks.

(3) Availability: A security measure known as availability ensures that anybody with authorization to access the network can use the information and data at the level of access allowed by their company. In order to fulfill user demands for access to Internet information, the server systems and computer systems must have enough capacity. Information accessibility could be hampered by cyberattacks, natural catastrophes, and environmental issues. These types, such as Denial of Service (DoS / DDoS), Internet control message protocol (ICMP) Attack, and others, will more frequently be seen in the server's response to information access requests. Computer information transmission capacity will be impacted by attacks on Availability. Figure 2 is a classification diagram of the cyber attack classification method described above.

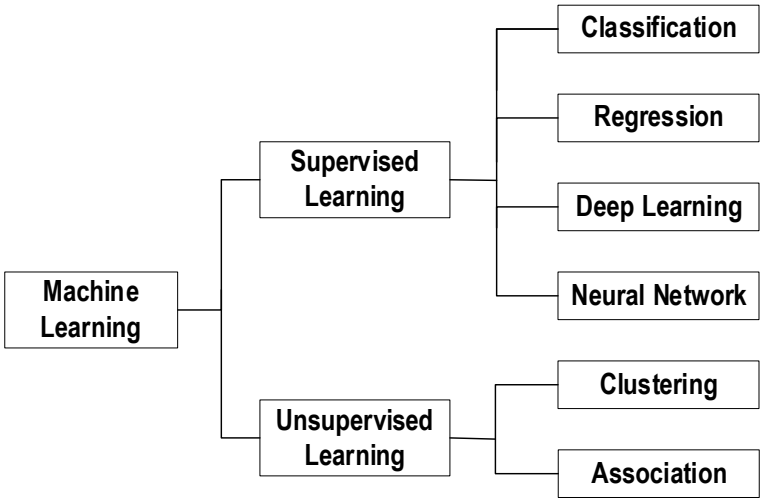

Fig. 3 Machine Learning [6]

3. Different Smart Grid Cyber Security Methods

3.1. Machine Learning

3.1.1 Introduction of Machine Learning

A subfield of computer science, Machine Learning (ML), was first developed in the artificial intelligence (AI) movements of the 1950s. Designing and evaluating algorithms such that computers can automatically learn from them is the core focus of machine learning theory. In some previous papers, ML algorithms have been classified as supervised, unsupervised, and reinforcement learning, such as [6]. This paper takes this classification approach, section 3.1 discusses supervised and unsupervised learning, and section 3.2 discusses reinforcement learning separately. Supervised learning applies for less data and clearly labeled data training [7]. In supervised learning, the algorithm provides training data with labels or results. Classification and regression are the two main subcategories of supervised learning techniques. Much bigger data sets can be used for unsupervised learning [7]. In unsupervised learning, neither the outcomes nor the labels are provided by the data. Clustering and association are the two main subcategories of unsupervised learning techniques. Figure 3 illustrates a common classification of the Machine Learning approach.

Machine Learning has been extensively employed in smart grid systems. Machine Learning can identify the cyber attacks after training with the relevant electrical parameters during normal operation and network attacks [8]. The following examples are three research methods of Machine Learning in smart grid cyber security protection.

3.1.2 Application examples of Machine Learning

3.1.2.1 Sequential supervised Machine Learning approach

In [8], the authors propose a two-layer sequential ML model to improve the detection of cyber attacks. The random forest classifier (RFC) is used as the basic classifier to detect intrusion attacks.

The model's initial layer is utilized to make a distinction between two operating modes: normal state and cyber assault. The second step of categorisation divides states into separate types of hacking. Since the training is concentrated on the goal task at that layer thanks to the hierarchical technique, the model's is increased.

The main objective of the research is to create a sequence model that is more accurate and precise while using less processing resources. All events are sorted and filtered using the hierarchy. The data is transmitted to the second layer, which categorizes it in accordance with the attack categories. The accuracy of the model is 95.44%.

3.1.2.2 A deep learning framework basaccuracy ed on a stacked auto-encoder (SAE)

To directly extract characteristics from unprocessed data, deep artificial neural networks are employed in deep learning, a type of unsupervised learning in machine learning (ML). Data-driven detectors may be replaced by recent advancements [9].

For the purpose of constructing ML features for the transmission Supervisory Control and Data Acquisition (SCADA), attack data collecting and surveillance control system, the authors of [9] describe a design for deep learning built around stacking auto-encoder (SAE). The primary focus of the study is the SAE based on the traditional auto-encoder (AE). A conventional auto-encoder is a three-layer neural net that has been trained to try to copy what is input to its outcome. The SAE consists of numerous auto-encoders that are each regarded as an independent building block and layered in intricate structures in order to identify extremely nonlinear and complex patterns in the input.

The proposed methodology, in contrast to the most advanced ML detectors, automates unsupervised learning of features in order to reduce the need to rely on system models and human experience in challenging security scenarios. In order to find attacks, SAE can find rich and helpful patterns buried in the data.

3.1.2.3 K-Means clustering algorithm in detection of smart grid flow data abnormalities

The work in [10] uses the K-Means clustering technique to cluster the data and find outlier values in order to identify the data exchanged between the utility center and the smart house. Unsupervised machine learning is used in the K-means technique. Data is grouped into clusters by the process of clustering, which results in high similarity indices between objects inside a cluster and high diversity indices between things in different clusters. This makes it easier to detect both regular and irregular flow rates. Use raw data from a dataset on the smart grid. Flood attack could happen when the volume of User Datagram Protocol (UDP) and Internet Control Message Protocol (ICMP) packets abruptly rises or falls, and this is seen as abnormal flow during the flow analysis.

The framework examines all data object traffic. The information is then categorized to create clusters and spot anomalies. The authors checked for collisions at the centroid at each stage of the K-means clustering. The centroid is iterated to prevent collisions in the event of a collision. When an item deviates from any clusters, traffic exceptions are noticed.

3.2. Reinforcement Learning

3.2.1 Implementation for reinforcement learning

From the perspective of ML, Reinforcement Learning (RL) is a third method different from supervised learning and unsupervised learning, and belongs to the category of semi-supervised learning methods. Learning by interacting with the environment, the goal of essential RL is a trial-and-error learning through a sequential process of rewarding and punishing each action [11].

The most popular methods for RL are State-Action-Reward-State-Action (SARSA), Deep Q Net (DQN) and Deep Deterministic Policy Gradients (DDPG).

The following discussion is three specific examples of RL in smart grid cyber security protection.

3.2.2 Application examples of Reinforcement Learning

3.2.2.1 Using the model-free reinforcement-learning framework, an accurate universal online detection technique

The Partially Observable Markov Decision Process (POMDP) model-free RL system is used by the authors to present an algorithm for online cyber threat detection in [12]. The suggested approach is all-encompassing and does not need an attack model. As a result, the suggested approach has a wide range of applications and can be used to ascertain fresh attack types. The topic of this essay is defender-focused online attack detection.

The learning stage and the online detection stage are both parts of the RL-based detection system. The SARS algorithm and the defenders both learn a Q table throughout the learning phase. During

training, each defender makes decisions based on their observations and then pays the price for those decisions. The defender modifies and relearns a Q table in light of this experience. Use the previously learned Q table to select the lowest projected future cost (Q value) during the online detection phase. Up until the defender chooses to cease the action, the online detection phase continues. If it does, the process is stopped and the attack is acknowledged. When the system restores and resumes regular functioning after the stated assault, the online detection phase is repeated.

3.2.2.2 Analysis of smart grid vulnerability to sequential topological strikes utilizing Q-Learning

A Reinforcement Learning-based approach for the vulnerability analysis of sequential attacks on transmission networks is presented in [13] by the paper. The Q-learning technique was used to identify crucial sequences in sequential attacks.

The local optima and deteriorating initialization difficulties affect the Q-learning algorithm negatively. In this research, the authors use the optimistic initial estimate to address the Q-learning deterioration initialization problem and the greedy method to tackle the local optimum issue all through the learning process. In Q-learning, attackers are referred to as agents if they continuously attempt to locate more vulnerable grid components. The electrical grid can be viewed as an independent unit that has the ability to react to malicious switching circuit behavior of an attacker.

The technique minimizes the amount of attacks launched by removing unsuccessful attack sequences and increasing the number of line interruptions through the learning process, according to simulation results. This is done without utilizing cascade interrupt vulnerabilities.

3.2.2.3 Hot booting-Q technology and Deep Q Network for the malware attack problem

In [14], the authors design a detection scheme based on hot booting-Q technology and Deep Q Network (DQN) for the malware attack problem in smart grid cyber security. It is an unloading method based on deep multilayered neural systems and the DQN technology. According to simulation data, DQN-based malware detection has the highest malware detection accuracy, the lowest detection delay, and the maximum mobile device utilization. It also has the fastest learning rate.

3.3. Ensemble Methods

3.3.1 Introduction of the Ensemble Methods

The Ensemble Method is a machine learning approach for artificial intelligence (AI) that creates a number of classifiers and uses weighted voting to classify fresh data pieces [15].

For the purpose of detecting cyberattacks on smart grids, a variety of ensemble learning methods are used:

(1) Bagging is often referred to as the random subspace method. It is an ensemble learning method that lowers the correlation between estimators in the ensemble by training on a random sample of features rather than the whole set of features [16]. An example is the Random Forest, which creates a limited number of randomly selected decision trees from a subset of samples. The process outcome can be obtained by voting on the classification or regression findings, or by averaging them, respectively [17].

(2) Boosting: Boosting is a broad ensemble learning algorithm used in classification and regression problems. AdaBoost models are usually used. The initial learning in this model is learned using the training weights and updated using the results of prior iterations. For the true probability, anticipated probability, and provided error, the weight of the instance can be changed [17].

(3) Stacking: Predictions from various classification or regression techniques are combined using the stacking ensemble learning technology [4]. The technique primarily looks for the best answer among many Machine Learning techniques. The approach is often applied at levels 0 and 1. The technique primarily trains several models and their prediction outcomes for level 0 base learners. The model at level 1 is trained using the best estimate from level model before [17].

The following specific introduction is the examples of Ensemble Methods in smart grid cyber security protection and their performance to resist cyber attacks.

3.3.2 Application examples of Ensemble Methods

In [17], the authors undertake performance evaluation using the Canadian Institute for Cybersecurity-Distributed Denial-of-Service (CIC-DDoS 2019) benchmark while combining Ensemble Methods (Bagging, Boosting, and Stacking) with conventional Machine Learning techniques, K Nearest Neighbor (KNN), and Naive Bayes (NB). The four quotas used to assess performance are accuracy, false alarm probability, misdetection probability, and the probability of detection (FPR, FNR, TPR).

The simulation's results show that: With scores of 96%, 4.1%, 8.9%, and 93.4%, respectively, the stack-based classifier delivered the best performance outcomes in the four quotas in Reflection-based Attacks. Bagging, boosting, KNN, and NB are the next processes. The stack-based classifier provides the best performance outcomes in exploitation-based assaults. Using that method, 96% TPR, 1% FPR, 0.7% FNR, and 97.3% accuracy were attained. Second, Boosting outperforms Bagging significantly.

The authors of [16] assess several Ensemble Methods' classification performance in light of their application for identifying cyberattacks on power systems. Classification accuracy, precision, recall, and F-measure are used to compare the various approaches. We compare ensemble approaches like bagging, adaboosting, majority voting, and random forest with basic machine learning techniques like bayesnet, oneR, svm, ripper, and C4.5 decision tree.

The Ensemble Method has the potential to outperform more traditional Machine Learning techniques in terms of average accuracy. The Ensemble approach outperforms the fundamental Machine Learning approach in terms of average precision values. The true positive rate, which can be used to determine the best effective learning strategy for spotting cyberattacks, is reflected in average recall. Random Forest exhibits the best performance in terms of F-score. Along with Bayesnet, ensemble approaches built on bagging and adaboosting outperform traditional machine learning techniques.

4. Comparison between Different Method for Protecting the Smart Grid from Cyber Attacks

A traditional Machine Learning technology is suitable for small-scale system models not requiring large amounts of computational resources. However, the disadvantage is the general lack of dynamic adaptation features and online learning function.

Reinforcement Learning, including Deep Reinforcement Learning combined with deep learning, can be seen as the development of traditional Machine Learning. Reinforcement Learning adds online learning functions to respond to unforeseen situations, and actively learn unknown types of cyber security attacks. However, to some extent, the complexity of the algorithm and the computational cost of repeated experiments also increase accordingly.

By mixing the outcomes of several learning algorithms or diverse initial data, Ensemble Methods can boost performance in terms of accuracy and precision. Ensemble Methods have a more accurate classification effect than previous Machine Learning algorithm models. Ensemble Methods increase the function of dynamic adaptation and have higher efficiency in handling such data. Ensemble Methods have been well developed in the smart grid cyber attack detection. While at the same time, Ensemble Methods will increase the experimental cost and calculation cost.

Table 1 summarizes the advantages and disadvantages of Machine Learning, Reinforcement Learning and Ensemble Methods. Table 2 shows a qualitative comparison of the three methods in terms of data adaptability, computational complexity, classification accuracy, precision value, computational expense and so on.

Table 1. Advantages and disadvantages of ML, RL, and Ensemble Methods in smart grid cyber security

Method	Advantage	Disadvantage
Machine Learning(convention)	Suitable for small-scale system models	Lack of online learning function and dynamic adaptation function
Reinforcement Learning	Online learning function, respond to unforeseen situation	High computation complexity and high computational expense
Ensemble Methods	Function of dynamic adaptation	High computational expense

Table 2. Contrast factors of ML, RL, and Ensemble Methods in smart grid cyber security

Method	Data adaptability	Computation complexity	Classification accuracy	Precision value	Computational expense	Robust
Machine Learning(convention)	Good	Low	Bad	NA	Low	NA
Reinforcement Learning	Good	High	NA	NA	High	Good
Ensemble Methods	Good	NA	Good	Good	High	NA

Note: Not available (NA)

As shown in Table 2, the three methods have strong data adaptability. Conventional Machine Learning methods have low computational complexity, while Reinforcement Learning methods have high computational complexity. In terms of classification accuracy, the Ensemble Methods significantly outperform in comparison to conventional Machine Learning methods. Ensemble Methods also dominate in weighting precision. Conventional Machine Learning methods have low computational expense, while the other two methods have relatively high computational expense. As to robust adaptation to the environment, the Reinforcement Learning methods have good robust performance.

5. Summary

This paper introduces the types of smart grid cyber attacks and cyber security methods, such as cryptography, network authentication, artificial intelligence technology, 5G technology, blockchain and so on. Focus on three methods of artificial intelligence technology in smart grid cyber security: Machine Learning, Reinforcement Learning and Ensemble Methods. Through the theory introduction and related researches, the paper summarizes the pros and cons of the three methods, and make a qualitative comparison from the angles of adaptability, calculation complexity, classification accuracy, precision value, computational expense and so on. Conventional Machine Learning methods adapt to the simple system scale with less computational amount, while lack the dynamic adaptation function and online learning function. The Reinforcement Learning methods have the online learning function, but the experimental cost and the computational complexity are both high. The Ensemble Methods have good dynamic adaptation function and improve the classification accuracy of conventional Machine Learning methods, yet this method also requires high experimental expense.

In future research work, the writer hopes that artificial intelligence technology will make further progress in smart grid cyber security. For example, how to reduce the experimental expense and computational complexity of Reinforcement Learning methods; how to apply the existing algorithm

technology breakthrough and experimental simulation results to the specific practice platform, how to get more valuable data and so on.

References

[1] Zia M F, Elbouchikhi E, Benbouzid M. Microgrids energy management systems: A critical review on methods, solutions, and prospects. Applied energy, 2018, 222: 1033-1055.

[2] Fang X, Misra S, Xue G, et al. Smart grid—The new and improved power grid: A survey. IEEE communications surveys & tutorials, 2011, 14(4): 944-980.

[3] Tuballa M L, Abundo M L. A review of the development of Smart Grid technologies. Renewable and Sustainable Energy Reviews, 2016, 59: 710-725.

[4] Omitaomu O A, Niu H. Artificial intelligence techniques in smart grid: A survey. Smart Cities, 2021, 4(2): 548-568.

[5] Brar H S, Kumar G. Cybercrimes: A proposed taxonomy and challenges. Journal of Computer Networks and Communications, 2018, 2018.

[6] Cui L, Qu Y, Gao L, et al. Detecting false data attacks using machine learning techniques in smart grid: A survey. Journal of Network and Computer Applications, 2020, 170: 102808.

[7] Zhou Z H. Machine learning. Springer Nature, 2021.

[8] Farrukh Y A, Ahmad Z, Khan I, et al. A sequential supervised machine learning approach for cyber attack detection in a smart grid system. 2021 North American Power Symposium (NAPS). IEEE, 2021: 1-6.

[9] Wilson D, Tang Y, Yan J, et al. Deep learning-aided cyber-attack detection in power transmission systems. 2018 IEEE Power & Energy Society General Meeting (PESGM). IEEE, 2018: 1-5.

[10] Menon D M, Radhika N. Anomaly detection in smart grid traffic data for home area network. 2016 International Conference on Circuit, Power and Computing Technologies (ICCPCT). IEEE, 2016: 1-4.

[11] Woergoetter F, Porr B. Reinforcement learning. Scholarpedia, 2008, 3(3): 1448.

[12] Kurt M N, Ogundijo O, Li C, et al. Online cyber-attack detection in smart grid: A reinforcement learning approach. IEEE Transactions on Smart Grid, 2018, 10(5): 5174-5185.

[13] Yan J, He H, Zhong X, et al. Q-learning-based vulnerability analysis of smart grid against sequential topology attacks. IEEE Transactions on Information Forensics and Security, 2016, 12(1): 200-210.

[14] Wan X, Sheng G, Li Y, et al. Reinforcement learning based mobile offloading for cloud-based malware detection. GLOBECOM 2017-2017 IEEE Global Communications Conference. IEEE, 2017: 1-6.

[15] Dietterich T G. Ensemble methods in machine learning. International workshop on multiple classifier systems. Berlin, Heidelberg: Springer Berlin Heidelberg, 2000: 1-15.

[16] Chen X, Zhang L, Liu Y, et al. Ensemble learning methods for power system cyber-attack detection. 2018 IEEE 3rd International Conference on Cloud Computing and Big Data Analysis (ICCCBDA). IEEE, 2018: 613-616.

[17] Khoei T T, Aissou G, Hu W C, et al. Ensemble learning methods for anomaly intrusion detection system in smart grid. 2021 IEEE international conference on electro information technology (EIT). IEEE, 2021: 129-135.