Intrusion Detection in Smart Grids by Collective Learning Algorithm and Particle Swarm Optimization Algorithm

Jenan Jader Msad[1], Anvar Khamdamov[2] and Alaa Majeed Shnain[3]
[1]*Department of Information Technology Engineering ,Polytechnic College, Al-Furat Al-Awsat Technical University, 54003 Karbala, Iraq*
[2]*Namangan Institute of Engineering and Technology, Kosonsoy Str., 7, 160115 Namangan, Uzbekistan*
[3] *Department of Mechanical Engineering Technical Institute Babylon, Al-Furat Al-Awsat Technical University, 54003 Bablyon, Iraq*
Jenan.jader@atu.edu.iq, anvarkhamdamov@rambler.ru,alaa.shnen.iba@atu.edu.iq

Keywords: Smart Power Grid, Intrusion Detection, AdaBoost Algorithm, Particle Optimization Algorithm.

Abstract: In recent years, cyber-attacks targeting the physical infrastructure of modern power systems have significantly increased, posing serious risks to society and critical services. This study investigates intrusion detection in smart grids using a hybrid approach based on Particle Swarm Optimization (PSO) and the AdaBoost ensemble classifier. To enhance detection performance, data preprocessing techniques, including handling missing values and normalization, were applied. Subsequently, PSO was utilized for feature selection, reducing the original feature set from 40 to 30 optimal attributes. These selected features were then used as input to the AdaBoost classifier. The ensemble learning mechanism of AdaBoost combines multiple weak learners to improve classification reliability by focusing on misclassified instances and aggregating their outputs. This approach enhances detection capability compared to individual classifiers. Experimental results demonstrate that the proposed method achieves an accuracy of 92.9% on the test dataset, outperforming the baseline method by approximately 3%, which confirms the effectiveness of combining feature optimization with ensemble learning for smart grid intrusion detection.

1 INTRODUCTION

Smart grids represent a cyber-physical infrastructure in which communication networks are tightly integrated with physical power systems to enable efficient monitoring, control, and energy distribution [1], [2]. While this integration enhances operational efficiency, it also increases exposure to cyber-attacks that may result in severe physical, economic, and social consequences [3]. Unlike conventional communication networks, cyber intrusions in smart grids can directly affect power availability, system stability, and public safety [4].

Traditional security mechanisms such as firewalls, encryption, and authentication play an essential role in protecting communication infrastructures; however, they are insufficient to address sophisticated and previously unknown cyber threats [5], [6]. Consequently, Intrusion Detection Systems (IDSs) have become a critical component of smart grid security architectures, aiming to monitor system behavior and identify malicious activities that bypass preventive defenses [7], [8].

Despite their importance, the effectiveness of IDSs in smart grid environments is often limited by high-dimensional data, redundant features, and increased false alarm rates, which reduce detection reliability in real-world operational settings [9], [10]. To overcome these limitations, several detection paradigms have been proposed, including signature-based, anomaly-based, and description-based intrusion detection methods that focus on modeling normal system behavior [11], [12], [13].

In recent years, ensemble learning techniques have attracted increasing attention due to their ability to improve classification robustness by combining multiple weak learners [17], [18]. Among these techniques, AdaBoost has demonstrated effectiveness in reducing classification errors and variance. Nevertheless, the performance of ensemble classifiers remains highly dependent on feature quality and dimensionality, making feature selection

a critical step in intrusion detection systems [16], [19].

To address these challenges, this study investigates a hybrid intrusion detection approach that integrates Particle Swarm Optimization (PSO) for feature selection with the AdaBoost ensemble classifier [16], [20]. PSO is employed to select a reduced and informative subset of features, which is then used as input to the AdaBoost classifier to enhance detection accuracy while reducing false alarms. The effectiveness of the proposed approach is evaluated using the NSL-KDD benchmark dataset.

2 CONTRIBUTIONS OF THIS STUDY

The main contributions of this study can be summarized as follows:

- This study proposes a hybrid intrusion detection framework for smart grid environments by integrating Particle Swarm Optimization (PSO) for feature selection with the AdaBoost ensemble classifier.
- The proposed approach demonstrates that reducing the feature space prior to classification improves intrusion detection accuracy and reduces false alarm rates.
- An experimental evaluation is conducted using the NSL-KDD benchmark dataset, providing insight into the effectiveness and limitations of optimization-based ensemble learning for smart grid intrusion detection.

3 RELATED WORKS

Previous studies explored signature-based IDSs, which are effective for known attacks but limited in detecting unknown threats [13], [25]. Anomaly-based IDSs have been developed to be capable of detecting novel intrusions but are prone to high false alarms [12], [22]. Recent advancements introduced description-based IDSs to model system behaviors in detail [15].

In smart grids, IDSs have been classified into Host-based (HIDS), Network-based (NIDS), and Distributed architectures [14], [27]. Studies employing machine learning and optimization techniques, including neural networks, decision trees, and whale optimization algorithms, highlight the promise of hybrid approaches [28], [18], [19]. However, limitations remain in scalability, accuracy, and adaptability [29], [30], [31].

In the last few years, cyber-attacks on the physical infrastructure of smart electricity systems have increased [3], [20]. If such attacks are carried out successfully, they can cause many problems in people's lives. The prevalence of such attacks has raised concerns about the security of sensitive infrastructure [9], [10]. Therefore, despite these attacks, the use of intrusion detection in smart electrical systems has become necessary [7], [8]. If intrusion detection is performed in a network using more than one method, it will detect new attacks and reduce the rate of incorrect and false alarms of one detection method by using another detection method [17]. According to the mentioned cases, in order to detect intrusion in the power grid, we employed the AdaBoost algorithm and the particle swarm optimization algorithm.

4 METHODOLOGIES

AdaBoost was employed as an ensemble classifier to combine multiple weak learners, where each learner focused on misclassified instances from previous iterations. This approach improved detection stability after feature reduction using PSO [16], [17].

In this work, it is proposed to use the AdaBoost classifier to achieve the goal of increasing detection accuracy in order to detect intrusion in smart grids. The advantage of this approach over other methods is that this algorithm is an ensemble learning method. In ensemble learning algorithms, an example is classified using several different classifiers, and the result of the classification is intelligently combined with each other, and the final result is determined for that specific example [26]. The accuracy and performance of this algorithm is higher compared to traditional and deep classification algorithms, because the general result is obtained from several classifiers. This algorithm has reduced the error and variance of training data.

In ensemble learning algorithms, each classifier is trained with a randomly selected subset of all samples. With the formation of several different classifiers, the final classifier, which is the result of a collective view, contains more efficiency [17]. Also, to increase the efficiency of this classifier, we intend to select the best features using the particle swarm optimization algorithm, and then the selected features will be provided to the classifier as input [16].

5 PROBLEM STATMENT

Smart power grids are a very important issue in order to meet future energy needs [1]. In order to achieve higher efficiency, which is the goal of energy distribution networks of future generations, it is necessary to create a centralized energy source by integrating various distributed power plants, and to continuously manage and monitor energy production and consumption [23], [24]. In order to successfully accomplish this, it is very important to use special network monitoring techniques and utilize specialized application software [2].

Smart grid is a term that includes various aspects of modern electric power transmission and distribution networks [1]. In order to become familiar with the basic concepts of the smart grid, we will state some definitions that have been provided by reliable institutions:

The European Smart Grid Task Force and the SG European Technology Platform define smart grids as follows: electric grids that efficiently monitor the operation of all users of this grid, including generators, consumers, and production and consumption systems, in order to ensure high economic efficiency, stability of a powerful network with the lowest losses and the highest quality, security, and convenience of energy production [23].

In the United States, the U.S. Department of Energy's Power Transmission and Distribution Administration defines the future energy grid as: a network of digital technology used to increase the reliability, security, and efficiency of electric power systems [23]. This action is possible by using information exchange, distributed generators, and energy storage resources. These systems are created by using two-way communication technology and complex computer processes [2], [24].

According to the above definitions, telecommunication technology and information systems are very important in smart grids. For example, computer-based remote control, monitoring processing, industrial automation, two-way communication between producer and consumer, and smart meters are among its components [1], [2]. Therefore, it can be stated that the smart power grid is actually a vast telecommunication and communication network that deals with energy production, transmission systems, and small and large networks located at the end of the line.

As with any communication network, network security is one of the important requirements in the communication infrastructure of smart networks, and it can be considered one of the biggest challenges of implementing smart power grids [3], [9]. Whenever the security of these networks is compromised, all the components of this smart network will be at risk and the provision of its services will be difficult [4], [10]. A problem in providing service in a part of smart networks means the power outage of several houses, factories, or even a city and several power plants being out of service. Considering the role that electricity has in people's lives, this issue has many serious consequences [1], [20].

6 DISCUSSIONS

The experimental results obtained in this study indicate that integrating PSO-based feature selection with the AdaBoost ensemble classifier enhances intrusion detection performance in smart grid environments [16], [17]. Reducing the feature set from 40 to 30 features eliminated redundant and less informative attributes, enabling the classifier to focus on the most discriminative traffic characteristics.

The ensemble learning nature of AdaBoost played a key role in improving classification stability by combining multiple weak learners, which reduced variance and mitigated misclassification errors [17]. This behavior is particularly beneficial in smart grid systems, where reliable and timely detection is critical due to the close interaction between cyber and physical components [15], [30].

Although the achieved accuracy of 92.9% demonstrates the feasibility of the proposed approach, the results should be interpreted in the context of the employed dataset and experimental setup. The findings confirm that optimization-based feature selection can effectively support ensemble classifiers in intrusion detection tasks, while also highlighting the importance of balanced evaluation beyond accuracy alone [17], [31].

7 LIMITATIONS AND FUTURE WORK

Despite the promising results achieved in this study, several limitations should be acknowledged. First, the experimental evaluation was conducted using a single benchmark dataset, which may not fully capture the complexity and diversity of real-world

smart grid traffic [29], [30]. Second, the proposed intrusion detection framework was evaluated in an offline setting, without considering real-time constraints or deployment challenges [7], [8]. Additionally, the PSO-based feature selection process prioritizes optimization performance over feature interpretability, making it difficult to directly associate selected features with specific attack behaviors [16].

Future work will focus on evaluating the proposed approach using real-world smart grid datasets [11], [18], extending the framework to multi-class attack scenarios [19], and investigating lightweight or adaptive optimization techniques suitable for real-time intrusion detection in large-scale smart grid infrastructures [28], [31].

8 RESULTS

The reported accuracy should be interpreted in the context of the NSL-KDD dataset and limited baseline comparisons. While the results demonstrate the feasibility of combining PSO with AdaBoost, broader comparisons with additional modern methods are left for future work. To check the effectiveness of the proposed method, we compared the results obtained from the test dataset of the proposed method with other methods reported in the baseline article, as summarized in Table 1. It should be noted that the dataset used in this work is the same as the dataset used in the baseline paper.

Table 1: Comparing the results of different methods with the proposed method.

Method	Accuracy	Precision
XGBOOST	89,15%	80,27%
LSTM_XGBOOST	89,21%	82%
AdaBoost+PSO	92,9%	88%

9 DATA SET USED

To evaluate the performance of the proposed intrusion detection system, accuracy, precision, and recall were employed as evaluation metrics [17], [31]. Accuracy was used to assess the overall effectiveness of the proposed PSO–AdaBoost framework in correctly classifying both normal and intrusive traffic. Precision was considered essential due to the critical nature of smart grid environments, where excessive false alarms may lead to unnecessary operational interventions [10], [30]. Recall was used to measure the system's ability to correctly detect actual intrusion instances, ensuring that malicious activities were not overlooked. These metrics were jointly analyzed to provide a balanced assessment of detection capability and system reliability [31].

10 CONCLUSIONS

The increasing dependence on electricity and the growing complexity of smart power grids highlight the critical importance of ensuring their security. Smart grids rely heavily on communication networks that enable two-way data exchange and integration of various system components. However, this interconnected and distributed structure also introduces new vulnerabilities, making such systems attractive targets for cyber-attacks. The integration of SCADA and ICT technologies further increases exposure to potential cyber risks.

To address these challenges, this study proposed a hybrid intrusion detection approach that combines Particle Swarm Optimization (PSO) for feature selection with the AdaBoost ensemble learning algorithm. After applying preprocessing techniques, including data cleaning and normalization, PSO was used to identify the most informative subset of 30 features from the original 40 features. The reduced feature set was then used to train the AdaBoost classifier, improving detection efficiency and reducing redundancy.

The results demonstrate that the proposed approach achieves a classification accuracy of 92.9%, outperforming the baseline method by approximately 3%. These findings confirm that integrating optimization techniques with ensemble learning can significantly enhance intrusion detection performance in smart grid environments.

Overall, the study highlights the potential of combining feature selection and ensemble methods as an effective solution for improving the security and reliability of modern smart power systems.

REFERENCES

[1] M. Fadaeenejad, A. M. Saberian, M. Fadaee, M. A. M. Radzi, H. Hizam, and M. Z. A. AbKadir, “The present and future of smart power grid in developing countries,” Renewable and Sustainable Energy Reviews, vol. 29, pp. 828–834, 2014.

[2] E. Ancillotti, R. Bruno, and M. Conti, "The role of communication systems in smart grids: Architectures, technical solutions and research challenges," Computer Communications, vol. 36, no. 17–18, pp. 1665–1697, 2013.

[3] W. Wang and Z. Lu, "Cyber security in the smart grid: Survey and challenges," Computer Networks, vol. 57, no. 5, pp. 1344–1371, 2023.

[4] Y. Zhang, L. Wang, W. Sun, R. C. Green II, and M. Alam, "Distributed intrusion detection system in a multi-layer network architecture of smart grids," IEEE Transactions on Smart Grid, vol. 2, no. 4, pp. 796–808, 2011.

[5] N. Beigi-Mohammadi, J. Mišić, H. Khazaei, and V. B. Mišić, "An intrusion detection system for smart grid neighborhood area network," in Proc. IEEE Int. Conf. Communications (ICC), 2014, pp. 4125–4130.

[6] C. H. Lo and N. Ansari, "CONSUMER: A novel hybrid intrusion detection system for distribution networks in smart grid," IEEE Transactions on Emerging Topics in Computing, vol. 1, no. 1, pp. 33–44, 2013.

[7] G. Efstathopoulos et al., "Operational data-based intrusion detection system for smart grid," in Proc. IEEE 24th Int. Workshop Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), 2019, pp. 1–6.

[8] P. Ahmed, J. Celestino Junior, and J. M. Pedersen, "An intelligent collaborative intrusion detection and prevention system for smart grid environments," Computer Standards & Interfaces, vol. 35, no. 6, pp. 564–574, 2013.

[9] P. I. Radoglou-Grammatikis and P. G. Sarigiannidis, "Securing the smart grid: A comprehensive compilation of intrusion detection and prevention systems," IEEE Access, vol. 7, pp. 46595–46620, 2019.

[10] V. K. Singh, H. Ebrahem, and M. Govindarasu, "Security evaluation of two intrusion detection systems in smart grid SCADA environment," in Proc. North American Power Symposium (NAPS), 2018, pp. 1–6.

[11] P. Radoglou-Grammatikis, P. Sarigiannidis, G. Efstathopoulos, and E. Panaousis, "ARIES: A novel multivariate intrusion detection system for smart grid," Sensors, vol. 20, no. 18, p. 5305, 2020.

[12] P. I. Radoglou-Grammatikis and P. G. Sarigiannidis, "An anomaly-based intrusion detection system for the smart grid based on CART decision tree," in Proc. Global Information Infrastructure and Networking Symposium (GIIS), 2018, pp. 1–5.

[13] H. Debar, M. Dacier, and A. Wespi, "A revised taxonomy for intrusion-detection systems," Annales des Télécommunications, vol. 55, no. 7, pp. 361–378, 2000.

[14] K. Scarfone and P. Mell, "Guide to intrusion detection and prevention systems (IDPS)," NIST Special Publication, vol. 800, p. 94, 2007.

[15] R. Mitchell and I. R. Chen, "A survey of intrusion detection techniques for cyber-physical systems," ACM Computing Surveys, vol. 46, no. 4, pp. 1–29, 2014.

[16] V. S. Ghomsheh, M. A. Shoorehdeli, and M. Teshnehlab, "Training ANFIS structure with modified PSO algorithm," in Proc. Mediterranean Conf. Control & Automation, 2007, pp. 1–6.

[17] T. T. Khoei, G. Aissou, W. C. Hu, and N. Kaabouch, "Ensemble learning methods for anomaly intrusion detection system in smart grid," in Proc. IEEE Int. Conf. Electro Information Technology (EIT), 2021, pp. 129–135.

[18] S. Khan, K. Kifayat, A. K. Bashir, A. Gurtov, and M. Hassan, "Intelligent intrusion detection system in smart grid using computational intelligence and machine learning," Transactions on Emerging Telecommunications Technologies, vol. 32, no. 6, p. e4062, 2021.

[19] C. Song, Y. Sun, G. Han, and J. J. Rodrigues, "Intrusion detection based on hybrid classifiers for smart grid," Computers & Electrical Engineering, vol. 93, p. 107212, 2021.

[20] E. Naderi and A. Asrari, "Toward detecting cyberattacks targeting modern power grids: A deep learning framework," in Proc. IEEE World AI IoT Congress (AIIoT), 2022, pp. 357–363.

[21] S. B. Rakas, V. Timčenko, M. Kabović, and A. Kabović, "Intrusion detection systems in smart grid," in Proc. Int. Symposium INFOTEH-JAHORINA, 2022, pp. 1–6.

[22] M. Bhuyan, D. Bhattacharyya, and J. Kalita, "Network anomaly detection: Methods, systems and tools," IEEE Communications Surveys & Tutorials, pp. 1–34, 2013.

[23] C. Greer et al., "NIST framework and roadmap for smart grid interoperability standards, release 3.0," 2014.

[24] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on smart grid communication infrastructures: Motivations, requirements and challenges," IEEE Communications Surveys & Tutorials, vol. 15, no. 1, pp. 5–20, 2012.

[25] H. Han, X. L. Lu, and L. Y. Ren, "Using data mining to discover signatures in network-based intrusion detection," in Proc. Int. Conf. Machine Learning and Cybernetics, 2002, pp. 13–17.

[26] O. Chapelle, B. Schölkopf, and A. Zien, Semi-Supervised Learning, 2006.

[27] H. Sallay and K. A. AlShalfan, "A scalable distributed IDS architecture for high-speed networks," IJCSNS International Journal of Computer Science and Network Security, vol. 9, no. 8, 2009.

[28] L. Haghnegahdar and Y. Wang, "A whale optimization algorithm-trained artificial neural network for smart grid cyber intrusion detection," Neural Computing and Applications, vol. 32, no. 13, pp. 9427–9441, 2020.

[29] J. Jow, Y. Xiao, and W. Han, "A survey of intrusion detection systems in smart grid," International Journal of Sensor Networks, vol. 23, no. 3, pp. 170–186, 2017.

[30] S. Y. Diaba, M. Shafie-khah, and M. Elmusrati, "On the performance metrics for cyber-physical attack detection in smart grid," Soft Computing, pp. 1–10, 2022.

[31] D. Mohanty, K. Sethi, S. Prasath, R. R. Rout, and P. Bera, "Intelligent intrusion detection system for smart grid applications," in Proc. Int. Conf. Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), 2021, pp. 1–8.