Intrusion Detection Using Time-Series Imaging and Transfer Learning in Smart Grid Environments

Firas Abou Naaj(✉), Yassine Himeur, Wathiq Mansoor, and Shadi Atalla

College of Engineering and IT, University of Dubai, Dubai, UAE
S0000002775@ud.ac.ae

Abstract. Intrusion detection systems (IDS) monitor and analyze network traffic and system activity to detect and alert security personnel to potential security breaches or attacks. Although deep learning models have shown great promise in improving the accuracy and efficiency of IDSs, several challenges are associated with their use, including data scarcity and model complexity. Furthermore, to overcome these problems, deep transfer learning is considered in this study. Typically, this article presents a novel intrusion detection (ID) approach using transformed 1D signals into 2D representations and applying pre-trained convolutional neural network (CNN) models. The transformed 2D representations of the signals allow the pre-trained CNN models to effectively learn the features of the signals and accurately classify them as normal or malicious. The performance of the proposed method was evaluated on the CIC-IDS-2018 dataset, and the results showed 92% accuracy in differentiating between normal behavior and malicious activities, which is an improvement compared with other detection methods.

Keywords: Intrusion Detection · Smart Grid · Time-series imaging · transfer learning

1 Introduction

1.1 Background

In recent times, there has been notable progress in interconnected technologies, including smart grids, the Internet of Vehicles, long-term evolution, and 5G communication [21]. A report by Cisco estimates that by 2022, the number of IP-connected devices is projected to be thrice the world's population, creating 4.8 ZB of IP traffic annually [2,13]. This exponential growth raises serious security concerns, as resource-constrained devices exchange vast amounts of sensitive data over the untrusted "Internet" using diverse communication protocols and technologies. According to a recent publication [11], it is crucial to incorporate advanced security measures and resilience analysis at the initial stages of deployment to ensure a secure and sustainable cyberspace [5].

M. Ben Ahmed et al. (Eds.): SCA 2023, LNNS 906, pp. 585–595, 2024.
https://doi.org/10.1007/978-3-031-53824-7_52

Security controls are essential to prevent, detect, and respond to attacks. As reported in a recent study [8], one of the widely used approaches for detecting internal and external intrusions and suspicious activities is the intrusion detection system (IDS). An IDS comprises several tools and mechanisms that monitor computer systems and network traffic, analyze activities, and identify potential threats to the system. There are mainly three types of IDS: signature-based, anomaly-based, and hybrid IDS [24]. Signature-based IDS uses predefined intrusion patterns to identify potential threats, while anomaly-based IDS detects deviations from normal behaviors. Different methodologies, such as machine learning (ML)-based techniques, knowledge-based schemes, and statistical-based approaches, have been used for anomaly detection, with deep learning (DL) methods gaining attention in recent investigations [1].

DL, a complex branch of machine learning, uses interconnected neurons organized in multi-layer networks to represent the mathematical computation of learning processes [6,14]. Its efficacy has been proven in several disciplines, including audio processing, natural language processing, picture and video recognition, robotics, and autonomous systems, to name a few [12]. Deep networks can be divided into three main categories: generative architectures, which use unsupervised learning to learn from unlabeled data, discriminative architectures, which use supervised learning to recognize patterns primarily for prediction tasks and hybrid architectures, which combine generative and discriminative models [4,22].

The advancements in DL techniques have garnered attention from researchers and smart grid actors for their potential applications in cyber-security [3]. DL and ML techniques are commonly used to develop IDSs that utilize traffic data analytics to differentiate between normal network traffic and various cyber-attacks [9,17].

Intrusion detection (ID) is a critical component of cybersecurity that has traditionally relied on rule-based or statistical methods. In recent years, DL models have gained attention due to their ability to learn complex patterns and features in network traffic data [10]. In this literature review, we summarize recent research on ID using DL models [8]. In the realm of network security, ID technology is a highly effective approach. Using DL algorithms for ID has emerged as a trend [16] within the smart grid domain, which proved DL-based ID methods yield promising results.

1.2 Contribution

DL algorithms are commonly used in traditional ID systems, where binary classifiers are employed to classify attacks. However, due to the impact of data dimensions on big data, the training model tends to yield a low attack detection rate, leading to reduced overall detection efficiency. By extracting higher-dimensional features from the original data, DL can generate a more accurate classification model, thereby enhancing the effectiveness of an ID system. This paper proposes an IDS system that first converts one-dimensional (1D) data into 2D space and then applies pre-trained CNN models. Moving on, to train base learners on IDS

data, four advanced CNN models, namely Xception, VGG-16, CNN, and our proposed method are employed. The proposed IDS framework's effectiveness and efficiency are evaluated using the CSE-CIC-IDS2018 dataset [20]. The proposed method has shown a 92% accuracy rate in distinguishing between normal behavior and malicious activities, which is an improvement compared to other detection methods.

2 Related Works

This section comprehensively reviews various DL techniques for identifying cyber-attacks in traditional and IoT networks. In machine learning (ML), selecting relevant features from the dataset is crucial for effective model training and classification. However, DL techniques have gained popularity recently due to their ability to extract relevant features, making them more efficient automatically. As a result, DL techniques are widely employed in ID Systems (IDSs) in cybersecurity.

2.1 Deep Learning

Traditional network security methods require improvements to deal with the rising number of network attacks. ID systems have been proposed as a solution but have low detection rates and require significant feature engineering. To address these limitations, Fu et al. [7] propose a DL-based model for network ID (DLNID) that integrates an attention mechanism and the bidirectional long short-term memory (Bi-LSTM) network. The DLNID model employs a convolutional neural network (CNN) for sequence feature extraction and utilizes the adaptive synthetic sampling (ADASYN) method to tackle data imbalance issues. Experimental results indicate that the DLNID model outperforms other comparison methods, achieving an accuracy of 90.73% and an F1 score of 89.65% on the NSL-KDD public benchmark dataset on network ID.

In [28], the author investigates using a deep neural network (DNN) to create a flexible and efficient IDS for detecting and classifying unforeseen and unpredictable cyberattacks. The paper examines various datasets generated through static and dynamic methods to determine the most effective algorithm for detecting future cyberattacks. The DNN model is tested on benchmark malware datasets that are publicly available, and the optimal network parameters and topologies are selected using hyperparameter selection methods. The study shows that DNNs outperform classical machine learning classifiers. Lastly, the author proposes a hybrid and scalable DL scheme, scale-hybrid-IDS-AlertNet, which helps monitor host-level events and network traffic in real-time to notify possible cyberattacks dynamically. In [15], the authors highlight the importance of IDSs in combating network intruders. Still, many existing models struggle with high false alarm rates and detecting User-to-Root (U2R) and Remote-to-Local (R2L) attacks. The paper proposes a bidirectional Long-Short-Term-Memory (BiDLSTM) based IDS to address these challenges. The model is trained and

evaluated on the NSL-KDD dataset, where the experimental results have demonstrated that BiDLSTM has outperformed conventional LSTM and existing methods concerning different ML metrics. Additionally, the BiDLSTM approach has a lower false alarm rate and achieves higher detection accuracy for U2R and R2L attacks than conventional LSTM.

In their study, Yang et al. [31] put forth a new approach to IDS for modern vehicle systems using ensemble learning and transfer learning (TL). This IDS utilizes a CNN model and a hyper-parameter optimization scheme to protect against network attacks. The effectiveness of this ID approach was assessed on two public benchmark Internet of Vehicles (IoV) security repositories: the Car-Hacking dataset and the CICIDS2017 dataset, which demonstrated over 99.25% accuracy and F1-scores. Overall, this has shown the effectiveness of TL-based IDS in detecting cyber-attacks in intra-vehicle and external vehicular networks, which is essential due to the vulnerabilities of IoV systems to cyber threats caused by the increasing connectivity of modern vehicles.

2.2 Transfer Learning

The article by [27] discusses the vulnerabilities in the Controller Area Network (CAN) bus used for in-vehicle communications, which can be exploited through network-level attacks. The paper tackles this problem by proposing a new ID method called CANTransfer that utilizes transfer learning (TL). A Convolutional LSTM-based model is trained using known intrusion patterns and then adapted to detect new attacks with limited data using one-shot learning. The experiments demonstrate that the proposed approach outperforms the best baseline model by 26.60% in detecting new intrusions.

The paper [19] suggests a novel IDS model based on deep TL for the security of In-Vehicle Network (IVN) systems. The proposed model involves selecting effective attributes, developing a deep TL-based LeNet model, and testing it with actual data. Based on experimental results, the proposed model performs better than existing models in terms of accuracy and detection rate, making it a viable solution for real-time IVN security. In the paper [29], a CNN-based TL is proposed for network ID, as the available datasets related to network intrusion are often insufficient for effective training. The proposed model comprises two ConvNets concatenated together and utilizes a two-stage learning process. The model is evaluated on the NSLKDD dataset, and the results demonstrate improved detection accuracy for known and novel attacks. This model achieves approximately 22.02% improvement on KDDTest-21 and 2.68% improvement on KDDTest+, in comparison to the traditional ConvNet model. In [25], another IDS scheme is introduced for enhancing the effectiveness of network ID using a wide and deep TL-based stacked GRU (Gated Recurrent Unit) model. This model can memorize a linear regression model with a generalization capacity of a deep GRU model. This method has achieved an evaluation accuracy of 99.92% for multi-class classification on KDDCup 99(10%) dataset and 94.22% on the UNSW-NB15 dataset. The results indicate that the proposed method surpasses most existing ID techniques.

The authors in [26] investigate the use of TL to improve the accuracy of network IDS (NIDS) in a data-scarce environment. Typically, the performance of fine-tuned TL-based NIDS is compared with a NIDS model trained from scratch. It has been found that fine-tuning can enhance the ability of detection models to identify new attacks with a reduced amount of training data. The study suggests that TL can enhance NIDS accuracy while reducing the time and cost of collecting labeled training data. The paper by [18] introduces a new approach for ID in mobile edge computing using a combination of federated learning and TL to enhance the efficiency of training and protect privacy. A reinforcement learning-based client selection scheme is also employed to select reliable and high-quality clients for participation in the training process, leading to better accuracy and communication efficiency. The experimental results show that the proposed framework performs better than traditional federated learning approaches and achieves the highest accuracy within a given budget limit. The article [30] presents a new approach to ID using TL and DL. The method transforms the ID task into an image recognition problem by converting network data into grayscale images and utilizing texture features to detect network intrusion. TL is used to enhance the model's efficiency and adaptability. Experimental results show that this approach outperforms traditional machine learning and DL methods, performs better generalization, and detect novel intrusion techniques effectively.

3 Proposed Method

3.1 Time-Series Imaging for ID

Time-series imaging is a powerful technique that transforms time-series data into images. This conversion allows us to leverage convolutional neural networks (CNNs) and transfer learning (TL), which were previously not feasible due to the absence of graphical representations for such records. Several time-series imaging methods exist, but we utilized the Gramian angular field approach. This technique generates images by calculating the difference or the summation of features compared to other features.

To begin the process, we normalize the features, ensuring their values scale is between -1 and 1. This normalization step is crucial for maintaining consistency and eliminating biases caused by differing scales. Once the features are normalized, the transformation involves turning the data into RGB images that would require to be turned in a grayscale format, allowing us to extract patterns and information from the data. Figure 1 shows how our data looks after applying Gramian Angular Field to our tabular data.

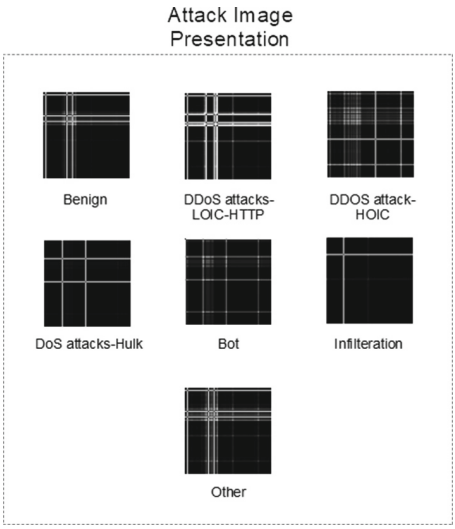

Fig. 1. Image representation of different attacks and normal network traffic behavior.

3.2 Dataset Description

Our method involved using two different datasets, the CIC-IDS2017 as a source domain and CSE-CIC-IDS2018 as a target domain. Both datasets contain 78 features that enable you to identify which class belongs to which.

CSE-CIC-IDS2018 dataset objective [20] was to tackle the shortage of top-notch datasets in the field. The scarcity of datasets is primarily attributed to privacy concerns, resulting in a limited supply of datasets with extensive features. The creators conquered this challenge by ensuring that the data generation process involved establishing an infrastructure comprising two separate entities: attackers and victims. The dataset contains 78 features that allow the differentiation of attack types. The original format of this data is in tabular format, which transforms into a graphical representation. The CSE-CIC-IDS2018 is considered the target domain between both datasets.

CIC-IDS2017 dataset aimed to overcome the limitations of the lack of reliable datasets covering a diverse range of network intrusions. Extensive evaluation of existing datasets revealed their outdated nature, as they no longer aligned with contemporary standards due to the emergence of new intrusion techniques. Recognizing this challenge, the creators of the dataset dedicated their efforts to capturing and reflecting up-to-date network behaviors as of 2017 [23]. The CIC-IDS2017 was used as a source domain in our transfer learning process.

3.3 Transfer Learning

The concept behind transfer learning (TL) is to take one model pre-trained on different features and use that experience to train another model, which improves

the performance of the other. There are different types of TL, but in our case, we mainly focused on fine-tuning to train our new model. Figure 2 provides a graphical representation of the intended purpose of the fine-tuning process.

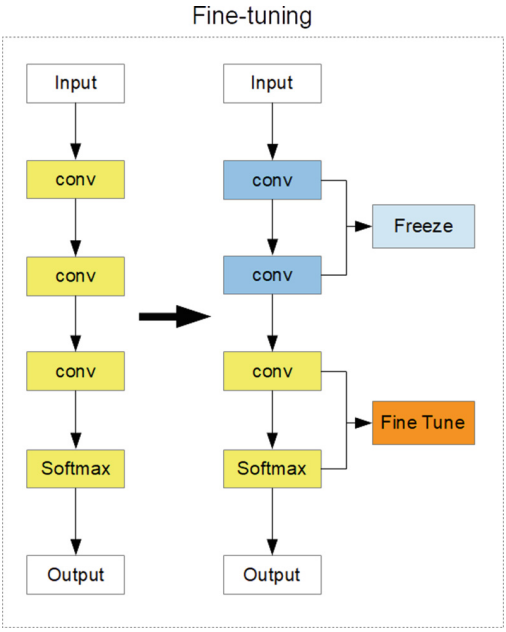

Fig. 2. A graphical representation of the fine-tuning concept, in which layers with features relevant to the current task are frozen.

TL's popularity kept increasing due to its ability to achieve high performance with lower training time compared to training a model from scratch. We use pre-trained models such as Inception, Xception, and VGG-16 for model training purposes. Those Models use ImageNet data for training, which contains over one million records with a thousand different classes. The benefit of using TL is the ability to scale down the number of types and data trained based on our requirements.

4 Experimental Results

Improvements in the proposed method harnessed the capabilities of the Keras API, which built on the robust TensorFlow framework. We employed two widely recognized datasets for conducting the experiments: the CIC-IDS2017 and CSE-CIC-IDS2018. During the training phase, the model underwent 100 epochs using early stoppage. The CIC-IDS2017 (Source Domain) and CSE-CIC-IDS2018 (Target domain) generated over 1.5 million images in the training process.

Before employing transfer learning techniques, we developed a Convolutional Neural Network (CNN) model trained on the source domain. We provided the means to act as a pre-trained model for our target domain. This step aimed to improve the detection rate and duration of training in comparison to existing techniques.

With the creation of our pre-trained model, we began employing it on the CSE-CIC-IDS2018 dataset alongside other techniques such as CNN, VGG-16, and Xception. Our proposed method did not only perform better in all metrics compared to other techniques but also consumed the least amount of time. Looking at Table 1, we can conclude that our proposed method took 301.587% less time to train than a CNN model, 71.43% less time to prepare than VGG16, and 7.9% less time than Xception. Furthermore, our proposed method performed better in all evaluation categories than other techniques.

Table 1. The table represents the performance metrics of the models

Metrics	**Xception**	**VGG-16**	**CNN**	**Proposed Method**
Precision	92%	92%	91%	92%
Recall	91%	91%	90%	92%
F1-score	91%	91%	90%	92%
Accuracy	92%	92%	90%	92%
Epoch	30	58	69	63
Total Duration	17 h	27 h	63.25 h	15.75 h

The proposed method represents an advantage in contrast to conventional approaches that focus on discerning whether an action constitutes an attack, devoid of insights into its specific type. This deficiency in traditional methods proves inefficient when deployed within an intrusion detection system. Our proposed approach not only identifies the presence of an attack but also analyzes it to classify the type of attack, thus bestowing several pivotal advantages such as tailored incident response, proper resource allocation, and continuous adaptation to new types of intrusions.

4.1 Causal Analysis

Analyzing further the results achieved by our proposed method, we discovered that the model in specific images could not differentiate between two different classes. Even further analysis enabled us to find that certain features are similar, which could cause the images to be nearly identical. Furthermore, this concluded that the Gramian Angular field was limited in creating sufficient differentiable features between different classes.

5 Conclusion

This paper demonstrates a smart grid IDS that uses TL and time-series imaging to detect attacks based on network traffic. We explored grayscale presentation in time-series imaging to evaluate its performance when applying various TL models. After identifying the different models to use for transfer aims to transfer the expertise of a pre-trained model to train a new model. Our research concludes that our proposed method was the optimal model because it is the best-performing and the fastest out of all models. Further developments and research may consider ways to improve the process of 2D representation transformation by enhancing the number of discerning factors visible in the graphical presentation. We could explore different tabular data to graphical representation techniques to improve the proposed method's performance.

References

1. Abd Elaziz, M., Al-Qaness, M.A., Dahou, A., Ibrahim, R.A., Abd El-Latif, A.A.: Intrusion detection approach for cloud and IOT environments using deep learning and Capuchin search algorithm. Adv. Eng. Softw., 103402 (2023)
2. Bousbiat, H., et al.: Crossing roads of federated learning and smart grids: overview, challenges, and perspectives. arXiv:2304.08602 (2023)
3. Diaba, S.Y., Elmusrati, M.: Proposed algorithm for smart grid DDoS detection based on deep learning. Neural Netw. **159**, 175–184 (2023)
4. Dina, A.S., Siddique, A., Manivannan, D.: A deep learning approach for intrusion detection in Internet of Things using focal loss function. Internet Things, 100699 (2023)
5. Elnour, M., et al.: Performance and energy optimization of building automation and management systems: towards smart sustainable carbon-neutral sports facilities. Renew. Sustain. Energy Rev. **162**(112), 401 (2022)
6. Elnour, M., et al.: Neural network-based model predictive control system for optimizing building automation and management systems of sports facilities. Appl. Energy **318**(119), 153 (2022)
7. Fu, Y., Du, Y., Cao, Z., Li, Q., Xiang, W.: A deep learning model for network intrusion detection with imbalanced data. Electronics **11**(6), 898 (2022)
8. Yhaia, H.K.: Deep transfer learning applications in intrusion detection systems: a comprehensive review. Inf. Fusion, 1–32 (2023)
9. Himeur, Y., Ghanem, K., Alsalemi, A., Bensaali, F., Amira, A.: Artificial intelligence based anomaly detection of energy consumption in buildings: a review, current trends and new perspectives. Appl. Energy **287**(116), 601 (2021)
10. Himeur, Y., Alsalemi, A., Bensaali, F., Amira, A., Al-Kababji, A.: Recent trends of smart nonintrusive load monitoring in buildings: a review, open challenges, and future directions. Int. J. Intell. Syst. **37**(10), 7124–7179 (2022)
11. Himeur, Y., Sohail, S.S., Bensaali, F., Amira, A., Alazab, M.: Latest trends of security and privacy in recommender systems: a comprehensive review and future perspectives. Comput. Secur., 102746 (2022)

12. Himeur, Y., Al-Maadeed, S., Varlamis, I., Al-Maadeed, N., Abualsaud, K., Mohamed, A.: Face mask detection in smart cities using deep and transfer learning: Lessons learned from the covid-19 pandemic. Systems **11**(2), 107 (2023)
13. Himeur, Y., et al.: Ai-big data analytics for building automation and management systems: a survey, actual challenges and future perspectives. Artif. Intell. Rev. **56**(6), 4929–5021 (2023)
14. Hnamte, V., Hussain, J.: DCNNBiLSTM: an efficient hybrid deep learning-based intrusion detection system. Telematics Inform. Rep. **10**(100), 053 (2023)
15. Imrana, Y., Xiang, Y., Ali, L., Abdul-Rauf, Z.: A bidirectional LSTM deep learning approach for intrusion detection. Expert Syst. Appl. **185**(115), 524 (2021)
16. Lampe, B., Meng, W.: A survey of deep learning-based intrusion detection in automotive applications. Expert Syst. Appl., 119771 (2023)
17. Liao, P., Yan, J., Sellier, J.M., Zhang, Y.: Divergence-based transferability analysis for self-adaptive smart grid intrusion detection with transfer learning. IEEE Access **10**, 68807–68818 (2022)
18. Masum, M., Shahriar, H.: TL-NID: deep neural network with transfer learning for network intrusion detection. In: 2020 15th International Conference for Internet Technology and Secured Transactions (ICITST), pp. 1–7. IEEE (2020)
19. Mehedi, S.T., Anwar, A., Rahman, Z., Ahmed, K.: Deep transfer learning based intrusion detection system for electric vehicular networks. Sensors **21**(14), 4736 (2021)
20. for Cybersecurity in University of New Brunswick CI (2018) CSE-CIC-IDS2018 on AWS. https://registry.opendata.aws/cse-cic-ids2018/
21. Sayed, A., Himeur, Y., Alsalemi, A., Bensaali, F., Amira, A.: Intelligent edge-based recommender system for internet of energy applications. IEEE Syst. J. **16**(3), 5001–5010 (2021)
22. Sayed, A.N., Himeur, Y., Bensaali, F.: Deep and transfer learning for building occupancy detection: a review and comparative analysis. Eng. Appl. Artif. Intell. **115**(105), 254 (2022)
23. Sharafaldin, I., Habibi Lashkari, A., Ghorbani, A.: Toward generating a new intrusion detection dataset and intrusion traffic characterization, pp. 108–116 (2018). https://doi.org/10.5220/0006639801080116
24. Singh, A., Amutha, J., Nagar, J., Sharma, S.: A deep learning approach to predict the number of k-barriers for intrusion detection over a circular region using wireless sensor networks. Expert Syst. Appl. **211**(118), 588 (2023)
25. Singh, N.B., Singh, M.M., Sarkar, A., Mandal, J.K.: A novel wide & deep transfer learning stacked GRU framework for network intrusion detection. J. Inf. Secur. Appl. **61**(102), 899 (2021)
26. Singla, A., Bertino, E., Verma, D.: Overcoming the lack of labeled data: training intrusion detection models using transfer learning. In: 2019 IEEE International Conference on Smart Computing (SMARTCOMP), pp. 69–74. IEEE (2019)
27. Tariq, S., Lee, S., Woo, S.S.: CANTransfer: transfer learning based intrusion detection on a controller area network using convolutional LSTM network. In: Proceedings of the 35th Annual ACM Symposium on Applied Computing, pp. 1048–1055 (2020)
28. Vinayakumar, R., Alazab, M., Soman, K., Poornachandran, P., Al-Nemrat, A., Venkatraman, S.: Deep learning approach for intelligent intrusion detection system. IEEE Access **7**, 41525–41550 (2019)
29. Wu, P., Guo, H., Buckland, R.: A transfer learning approach for network intrusion detection. In: 2019 IEEE 4th International Conference on Big Data Analytics (ICBDA), pp. 281–285. IEEE (2019)

30. Xu, Y., et al.: Intrusion detection based on fusing deep neural networks and transfer learning. In: Zhai, G., Zhou, J., Yang, H., An, P., Yang, X. (eds.) IFTC 2019. CCIS, vol. 1181, pp. 212–223. Springer, Singapore (2020). https://doi.org/10.1007/978-981-15-3341-9_18
31. Yang, L., Shami, A.: A transfer learning and optimized CNN based intrusion detection system for internet of vehicles. In: ICC 2022-IEEE International Conference on Communications, pp. 2774–2779. IEEE(2022)