Journal of Electronic Research and Application, 2025, Volume 9, Issue 2
http://ojs.bbwpublisher.com/index.php/JERA
ISSN Online: 2208-3510
ISSN Print: 2208-3502

Analysis of Internet of Things Intrusion Detection Technology Based on Deep Learning

Huijuan Zheng, Yongzhou Wang*

Chongqing University of Mobile Communication, Chongqing 401420, China

***Corresponding author:** Yongzhou Wang, 18983847509@163.com

Abstract: With the rapid development of modern information technology, the Internet of Things (IoT) has been integrated into various fields such as social life, industrial production, education, and medical care. Through the connection of various physical devices, sensors, and machines, it realizes information intercommunication and remote control among devices, significantly enhancing the convenience and efficiency of work and life. However, the rapid development of the IoT has also brought serious security problems. IoT devices have limited resources and a complex network environment, making them one of the important targets of network intrusion attacks. Therefore, from the perspective of deep learning, this paper deeply analyzes the characteristics and key points of IoT intrusion detection, summarizes the application advantages of deep learning in IoT intrusion detection, and proposes application strategies of typical deep learning models in IoT intrusion detection so as to improve the security of the IoT architecture and guarantee people's convenient lives.

Keywords: Deep learning; Internet of Things; Intrusion detection technology

Online publication: April 3, 2025

1. Introduction

In the modern network environment, intrusion detection technology is a basic means to improve network security, especially with important application value in the Internet of Things (IoT) architecture. Intrusion detection systems have the functions of real-time monitoring and analyzing network traffic data and system logs. Thus, they can timely discover intrusion behaviors and immediately respond and feedback, so as to prevent potential threats and detect potential security vulnerabilities, abnormal behaviors, and intrusion behaviors. With the development of artificial intelligence technology, deep learning has demonstrated more powerful feature learning and pattern recognition capabilities, becoming an important means to further optimize intrusion detection technology. With the support of deep learning algorithms, intrusion detection systems can autonomously learn and judge network traffic characteristics and system behavior patterns, greatly improving the accuracy of intrusion detection and adapting to the increasingly complex network security environment.

2. Overview of related concepts and theories

2.1. Internet of Things

The Internet of Things is an interaction architecture between the real world and the network environment composed of servers and computer networks. It is mainly composed of sensors, smart devices, networks and their protocols, and distributed applications, etc., so as to achieve the purpose of monitoring the real world and operating through devices [1]. For example, common networked cameras, intelligent agricultural equipment, and network-monitored industrial robots have been gradually applied in various fields of modern society. Specifically, the IoT is mainly constructed by the perception layer, the network layer, and the application layer. The perception layer mainly collects data through various sensors. The network layer stipulates network protocols to ensure the interactive transmission of data information. The application layer mainly uses application programs, software, and other devices to control underlying data or hardware devices, playing their functions and services [2].

Since the IoT is directly connected to devices, it has also become an important target of network intrusion. Common types of IoT intrusions include denial-of-service attacks, distributed denial-of-service attacks, SQL injection, man-in-the-middle attacks, cross-site scripting attacks, unauthorized access, brute-force cracking, etc. [3].

2.2. Intrusion detection

Intrusion detection systems are mainly used to monitor and identify potential network security factors so as to prevent networks from being invaded and achieve the effect of security protection. The system mainly uses the methods of data collection and analysis to judge whether there are abnormal situations in data traffic, detect potential or hidden attack means, and record and report the monitoring content [4].

Intrusion detection technologies can be divided into several types based on data sources and detection methods. In the classification of data sources, host-based systems mainly detect the system processes, file data, and system call behavior logs of the host system software itself to complete the detection [5]. Network-based systems monitor device traffic information to real-time monitor whether there is abnormal external traffic intrusion. In intrusion detection technologies based on detection methods, they can be divided into two situations: misuse and anomaly. The former detects intrusion behaviors by matching data with signatures, and the latter detects by monitoring abnormal data values.

2.3. Deep learning

Deep learning imitates the neural network structure of the human brain and endows machines with the ability to learn. It is mainly manifested in the layer-by-layer extraction and analysis of data features and then solves problems such as image and speech recognition, natural language processing, and intelligent recommendation. Deep learning has significant advantages in dealing with tasks with large amounts of data and complex content, so it shows good application value in the field of intrusion detection technology. In intrusion detection systems, common deep learning models mainly include convolutional neural networks, recurrent neural networks, and deep neural networks [6].

3. Advantages of applying deep learning in IoT intrusion detection

3.1. Automated feature extraction

The ability of automatic feature extraction is the primary advantage of the application of deep learning in

intrusion detection technology. The traffic data in the IoT environment is large-scale and complex. Traditional intrusion detection systems mainly rely on manually extracted features for matching and analysis, with low work efficiency and poor information capture effects. Deep learning models such as convolutional neural networks and recurrent neural networks have the ability to automatically extract features and conduct matching analysis, which can greatly improve the work efficiency and accuracy of traditional intrusion detection technology [7]. Taking the convolutional neural network as an example, it mainly performs sliding operations on data through the convolutional layer and convolutional kernels and can automatically extract local features, thereby grasping the feature information of data packets, port numbers, etc., and their combination relationships, so as to quickly achieve the effects of port scanning and data recognition.

3.2. Efficient pattern recognition

Pattern recognition ability is a key advantage of the application of deep learning in intrusion detection technology. The data traffic in the IoT system not only has high-dimensional features but also shows non-linear characteristics. Traditional detection methods cannot effectively identify attack patterns for such data. Deep learning models can deeply analyze the complex features and internal relationships of data, thus more accurately and efficiently identifying more complex attack patterns [8]. Taking the application of the deep neural network model as an example, it can learn and master the attack traffic characteristics of distributed denial-of-service attacks and then quickly extract and analyze abnormal traffic or specific data packets in intrusion detection to judge whether there is a DDoS attack.

3.3. Outstanding adaptability and scalability

Adaptability and scalability are also specific advantages of the application of deep learning in intrusion detection technology. On the one hand, the IoT environment is complex and changeable. Especially with the update and upgrade of different technologies, its intrusion means and methods are also constantly changing. Deep learning models can continuously adapt to new environments through continuous learning and model updates and can more effectively deal with new intrusion methods [9]. On the other hand, deep learning models are scalable. They can not only increase the number of network layers and neurons to improve their own detection efficiency and capabilities but also combine and link through distributed computing frameworks to allocate training tasks to multiple computing nodes, thus shortening their learning time.

4. Applications of typical deep learning models in IoT intrusion detection

4.1. Application of convolutional neural network (CNN)

In IoT intrusion detection, the extraction of traffic spatial features is a key link, and the convolutional neural network shows unique advantages in this regard. The convolutional neural network model mainly consists of several parts, such as the convolutional layer, the pooling layer, and the fully connected layer. The convolutional layer mainly uses convolutional kernels to perform convolutional operations on the detected data to automatically extract data features. The pooling layer samples and analyzes the data output by the convolutional layer, reducing the data dimension and calculation amount while ensuring that the feature information can be retained [10]. The fully connected layer mainly integrates the data features output by the pooling layer to classify the feature elements.

Specifically, the intrusion detection of DDoS attacks in the IoT based on the convolutional neural network

can be mainly divided into the following steps. First, relevant researchers should collect a large amount of network data of the IoT system, ensuring that the traffic data contains normal data and DDoS attack traffic. In data preprocessing, the original data needs to be cleaned by removing noise data and outliers and normalizing it to the range of 0–1 [11]. Second, transform the format of the processed data and input it into the convolutional neural network model, ensuring that the traffic data presents a two-dimensional matrix structure, with columns representing differences in feature dimensions and rows representing time steps. Third, complete the construction of the convolutional neural network model, where the convolutional layer and the pooling layer need to be constructed in multiple ways. In the convolutional layer, different convolutional kernels such as 3×3 and 5×5 should be set respectively to ensure the extraction of data features at different scales. Through the convolutional stacking effect, high-level and abstract feature elements can be gradually extracted. The pooling layer should adhere to the maximum pooling operation. For example, if the pooling window is set to 2×2 and the step size is 2, it can not only reduce the resolution of the feature map but also decrease the relevant calculation amount [12]. In the fully connected layer, the ReLU activation function can be used for optimization to enhance its non-linear expression ability. At the same time, classification can be completed based on the softmax function to calculate the probability of sample data and analyze whether it belongs to DDoS attack traffic.

In practical applications, the recognition accuracy of the convolutional neural network model in DDoS attacks reaches over 95%. It has unique advantages in the extraction of IoT traffic spatial features and can significantly reduce the false negative and false positive rates, providing important support for the development of IoT intrusion detection technology.

4.2. Application of Recurrent Neural Network (RNN)

In IoT intrusion detection, the recurrent neural network and its variants mainly show their functional characteristics in the detection of time-series data, especially being good at analyzing and capturing the time-series characteristics of continuous data streams. However, traditional recurrent neural network models face great difficulties in processing long-sequence data and may even encounter problems such as gradient disappearance or gradient explosion. In response to this, researchers have introduced different variant models such as the long short-term memory (LSTM) and the gated recurrent unit (GRU).

The long short-term memory network introduces three “gates” in the traditional recurrent neural network, namely the input gate, the forget gate, and the output gate, to control the flow of information, which can effectively solve the long-sequence problem [13]. The input gate can control the retention degree of input information, the forget gate is used to determine the information data that can be discarded, and the output gate controls the output content as the hidden state. The gated recurrent unit is a simplified variant based on the long short-term memory network. It combines the input and forget gates into an update gate, still having the original functions and effects. At the same time, it further simplifies the original output gate and memory unit, thus improving the calculation efficiency.

For example, in a smart home intrusion detection system, the system usually covers multiple IoT devices such as cameras, door locks, and home appliances. The operating state data and network traffic information of such devices have distinct time-series characteristics. Therefore, the data information and system logs of the devices can be collected in chronological order and used as training data. On this basis, first, data pre-processing is required. Error and duplicate data are removed through data cleaning, and the data is integrated

into the same range through normalization. Second, "time-step" features should be established in chronological order, clarifying the device state information and traffic change features at each time step, and then inputting them into the recurrent neural network model [14]. Finally, the LSTM model should be used for analysis and detection. On the one hand, a diversified hidden layer should be established, and learning and training should be completed through multiple LSTM units. On the other hand, pattern recognition is required. The traffic features in the normal operating state should be determined, and the traffic change rules in abnormal behaviors should be clarified. An alarm should be issued in a timely manner when an abnormality is detected.

Another example is in the context of the industrial IoT. The gated recurrent unit model can further detect the operating state of industrial equipment. In the industrial production process, some industrial equipment needs to run continuously for a long time, resulting in the continuous generation of time-series data such as equipment temperature, pressure, and rotation speed. The gated recurrent unit model can take its equipment parameters as input data to master and learn the data traffic rules during normal operation. When the equipment fails or is attacked externally, the model can immediately respond based on abnormal parameters, issue an early warning, avoid production accidents, and achieve the goal and effect of improving industrial production safety.

4.3. Application of Deep Neural Network (DNN)

In IoT intrusion detection, the deep neural network is mainly applied to large-scale data classification and detection. The deep neural network model generally consists of multiple hidden layers, with the ability to abstract and extract features layer by layer for data analysis, so as to complete the learning of more advanced feature representations and show a higher-level data classification and detection ability. Therefore, in the intrusion detection system, when facing the impact of large-scale network traffic data, the deep neural network can quickly learn the normal and abnormal traffic features, thus making scientific judgments on network data and device state information and achieving the effect of quickly and accurately identifying intrusion behaviors. Its advantage is mainly reflected in its non-linear fitting ability, especially being good at processing data with complex relationships. It is also one of the important technologies that endows the intrusion detection system with the ability to adapt to a changeable network environment.

Taking an enterprise IoT system as an example, its intrusion detection system needs to connect a large number of hardware devices within the enterprise and cover various work contents such as production, office work, and monitoring. Therefore, the generated traffic data is huge in scale and complex in content. To solve this problem, network data containing multiple intrusion traffic such as DDoS attacks, port scans, and malware propagation can be collected as learning and training data [15]. In the data preprocessing link, operations such as cleaning, noise reduction, and feature extraction are required. Both invalid and noisy data should be removed, and core data features such as port numbers, source IP addresses, destination IP addresses, data packet types, and traffic rules should be extracted and then used as input data. In model training, based on a multi-hidden-layer model, the model is continuously optimized through the backpropagation algorithm, and its weights and biases are adjusted to minimize the error. After multiple iterative trainings, the model can master the basic features of multiple intrusion behaviors, providing a reliable guarantee for the security of the enterprise IoT system.

5. Conclusion

In summary, in the context of the rapid development of information technology, improving the security level

of the IoT network environment is a key issue in current research. Facing increasingly changing and upgrading network security problems, IoT intrusion detection technology should also be continuously improved and optimized. Therefore, it is necessary to further give play to the application value and advantages of deep learning models. With the assistance of convolutional neural networks, recurrent neural networks, and deep neural networks, the protection level of intrusion detection systems can be continuously improved, creating a good, stable, healthy, and safe usage environment for the modern IoT environment and ensuring the smooth progress of people's work and life.

Funding

This article is the research result of the 2022 Municipal Education Commission Science and Technology Research Plan Project "Research on the Technology of Detecting Double-Surface Cracks in Concrete Lining of Highway Tunnels Based on Image Blast" (KJQN02202403); the first batch of school-level classroom teaching reform projects "Principles Applications of Embedded Systems" (23JG2166); the school-level reform research project "Continuous Results-Oriented Practice Research Based on BOPPPS Teaching Model—Taking the 'Programming Fundamentals' Course as an Example" (22JG332).

Disclosure statement

The authors declare no conflict of interest.

References

[1] Ge Y, 2024, Research on Internet of Things Intrusion Detection Technology Based on Deep Learning, dissertation, Beijing University of Posts and Telecommunications.

[2] Zhai R, 2024, Research on Open-Set Intrusion Detection Technology in Industrial Internet of Things, dissertation, Donghua University.

[3] Lu H, 2024, Research on Data Processing Technology in Internet of Things-Oriented Intrusion Detection Systems, dissertation, People's Public Security University of China.

[4] Che X, 2024, Research on Adversarial Attacks and Defense Technologies for Internet of Things Intrusion Detection, dissertation, Jilin University.

[5] Chen X, 2024, Research on Intrusion Detection Technology for Intelligent Connected Vehicles Based on Deep Learning, dissertation, University of Electronic Science and Technology of China.

[6] Zhang Y, 2024, Research on Internet of Things Intrusion Detection Technology Based on deep learning Algorithms, dissertation, Tianjin University of Technology.

[7] Feng G, Jiang S, Hu X, et al., 2024, New Progress in Research on Internet of Things-Oriented Intrusion Detection Technology. Netinfo Security, 24(02): 167–178.

[8] Du J, 2023, Research on Network Intrusion Detection Technology Based on Federated Learning, dissertation, Xijing University.

[9] Chen X, 2023, Research on Network Intrusion Detection Technology for Internet of Things. Network Security and Informatization, (10): 148–150.

[10] Xie S, 2023, Research on Internet of Things Intrusion Detection Technology Based on Combined Neural Networks,

dissertation, North China University of Technology.

[11] He F, 2023, Research on Home Internet of Things Intrusion Detection Technology Based on Machine Learning, dissertation, Southeast University.

[12] Liu Y, 2023, Research on Power Internet of Things Intrusion Detection Technology Based on Deep Learning, dissertation, Tianjin University of Science and Technology.

[13] Wang K, 2023, Research on Intrusion Detection Technology for Internet of Vehicles Based on Behavior Analysis, dissertation, Henan University of Science and Technology.

[14] Cui A, 2022, Research on Network Intrusion Detection Methods Based on Machine Learning, dissertation, Lanzhou University of Technology.

[15] Zhang X, 2021, Research on Key Technologies of Intrusion Detection in Internet of Things Environment, dissertation, Zhejiang Gongshang University.