EAI Endorsed Transactions
on Scalable Information Systems
Research Article EAI.EU

Research on IPV6 Network Security Intrusion Detection Algorithm based on parallel multipath

Qingyun Dong[1], Manzeng Ma[1,*], Linnan Zhu[1], Hao Zhang[1]

[1]Modern education technology center, Cangzhou Normal University, Cangzhou, Hebei, 061000, China

Abstract

Internet Protocol Version 6 (IPv6) enables large-scale connectivity for wireless sensor networks (WSNs), allowing resource-constrained sensing nodes to interact directly with external Internet services. However, this open connectivity significantly increases the exposure of IPv6-based WSNs to diverse cyber threats originating from both local networks and the public Internet. Existing intrusion detection systems (IDS) designed for traditional networks often struggle to operate effectively in IPv6 WSN environments due to limited node resources, high traffic dimensionality, and the dynamic characteristics of sensor communication. To address these limitations, this paper proposes an intrusion detection algorithm for IPv6 wireless sensor networks based on a parallel multipath detection framework. The proposed approach integrates a hierarchical security architecture, a generalized information modeling mechanism, and feature-driven anomaly detection to improve detection efficiency while maintaining lightweight computational overhead. By organizing traffic features through structured data preprocessing and adaptive decision rules, the method enables efficient identification of abnormal network behavior in resource-constrained environments. Experimental evaluation based on simulated IPv6 WSN traffic and the UNSW-NB15 dataset demonstrates that the proposed algorithm achieves fast detection performance with an average detection time of 0.12–0.14 μs per sample. The results indicate that the proposed approach can effectively support real-time intrusion detection in IPv6 wireless sensor networks while maintaining low computational cost.

Keywords: Intrusion Detection Algorithms, Network Security, Internet Protocol Version 6, Wireless Sensor Networks

Received on 03 December 2026, accepted on 14 April 2026, published on 22 July 2026

doi: 10.4108/eetsis.11206

1. Introduction

Internet Protocol (IP) technology is a main direction of the development of wireless sensor technology, and IPV6 technology is an inevitable choice to realize the informatization of wireless sensor networks. At present, special protocol communication in wireless sensor networks often involves specific applications, and its scalability and portability are poor, which makes it difficult for users of external networks to access it directly. IPV6 enables seamless connectivity between wireless sensor networks and the Internet, allowing communication among people, devices, and services through unified addressing and routing mechanisms. However, the introduction of global IPv6 connectivity also exposes resource-constrained sensor nodes to a broader attack surface originating from both local networks and the public Internet. Traditional wireless sensor networks were originally designed as closed environments without considering external attacks, and many existing security mechanisms such as key management, access control, and encryption mainly focus on passive protection strategies. These mechanisms often lack adaptability to dynamic network attacks and therefore cannot fully satisfy the security requirements of IPV6 wireless sensor networks.

Intrusion detection is an active security protection technology that can identify, evaluate, and respond to malicious behaviors in real time. The effectiveness of intrusion detection directly affects the security, reliability, and availability of network services. The Internet Engineering Task Force (IETF) has provided specifications to integrate wireless sensor networks with IPV6

*Corresponding author. Email: mamanzeng@caztc.edu.cn

infrastructure. However, the introduction of IPV6 also increases network heterogeneity and traffic complexity, which makes intrusion detection more challenging in resource-constrained environments.

Existing intrusion detection approaches developed for traditional wired networks or generic wireless sensor networks often rely on centralized processing or computationally intensive machine learning models. Such approaches are difficult to deploy in IPv6 WSN environments due to limited node resources, distributed communication structures, and large-scale network connectivity. As a result, designing lightweight and scalable intrusion detection mechanisms for IPv6 wireless sensor networks remains an open research challenge.

The research on intrusion detection algorithms has attracted significant attention in recent years. Baraneetharan E discussed the application of machine learning techniques in wireless sensor networks and highlighted the importance of security protection [1]. Dwivedi Shubhra pointed out that intrusion detection plays a key role in identifying and tracking malicious network activities [2]. Jia Yang proposed a deep neural network based intrusion detection model for network security analysis [3]. Hadi Alaa Abd Ali studied feature preprocessing methods to improve the efficiency of intrusion detection systems in large-scale environments [4].

Although these studies demonstrate the effectiveness of machine learning and feature-based detection techniques, most of them are designed for general network environments rather than IPv6 wireless sensor networks. They typically assume sufficient computational resources or centralized processing architectures, which are difficult to apply in distributed IPv6 WSN scenarios. Furthermore, existing studies rarely consider the interaction between IPv6 communication mechanisms and intrusion detection strategies, leaving an important research gap in lightweight and scalable IDS design for IPv6-based sensor networks.

Several studies have attempted to improve intrusion detection efficiency by reducing feature dimensionality or optimizing classification algorithms. Dong Rui-Hong reported that high-dimensional traffic data in wireless sensor networks may lead to increased computational complexity and reduced detection performance [5]. Haghnegahdar Lida developed a neural network-based intrusion detection model capable of classifying multiple types of attacks [6]. Anitha P. proposed an intrusion detection method combining grey wolf optimization and support vector machines [7]. Tang Ying further improved encryption protocols to enhance network security protection [8].

Despite these improvements, most existing solutions focus on improving classification accuracy while paying limited attention to the distributed and scalable characteristics required by IPv6 wireless sensor networks. In large-scale sensor deployments, centralized detection mechanisms may introduce significant communication overhead and detection latency. Therefore, intrusion detection methods that support distributed processing and efficient traffic analysis are required to ensure scalable and real-time security protection.

To address these challenges, this paper proposes an intrusion detection algorithm for IPv6 wireless sensor networks based on a parallel multipath detection framework. The proposed approach organizes network traffic features through structured preprocessing and employs a distributed detection strategy that allows multiple detection paths to process traffic information in parallel. By integrating feature extraction, traffic statistics, and adaptive decision rules, the proposed method reduces computational overhead while improving detection efficiency in resource-constrained environments. In addition, the parallel multipath mechanism enables scalable intrusion detection by distributing analysis tasks across different nodes in the network, which is particularly suitable for large-scale IPv6 wireless sensor deployments.

The main contributions of this paper are summarized as follows: (1) a scalable intrusion detection framework for IPv6 wireless sensor networks is proposed to address the limitations of traditional centralized IDS architectures; (2) a parallel multipath detection mechanism is introduced to improve detection efficiency while reducing computational overhead; and (3) an experimental evaluation based on simulated IPv6 WSN traffic demonstrates that the proposed method achieves efficient real-time intrusion detection performance.

2. Investigation of Network Security Intrusion Detection Algorithm Based on IPV6

2.1. IPV6 Wireless Sensor Network Architecture

The traditional wireless sensor network is an independent system, which connects many nodes with limited resources in a low energy consumption way, thus forming a wireless communication network. One or more gateways of wireless sensor networks are connected with Internet routers to form IPV6 wireless sensor networks. Its wireless sensor network architecture is shown in Figure 1.

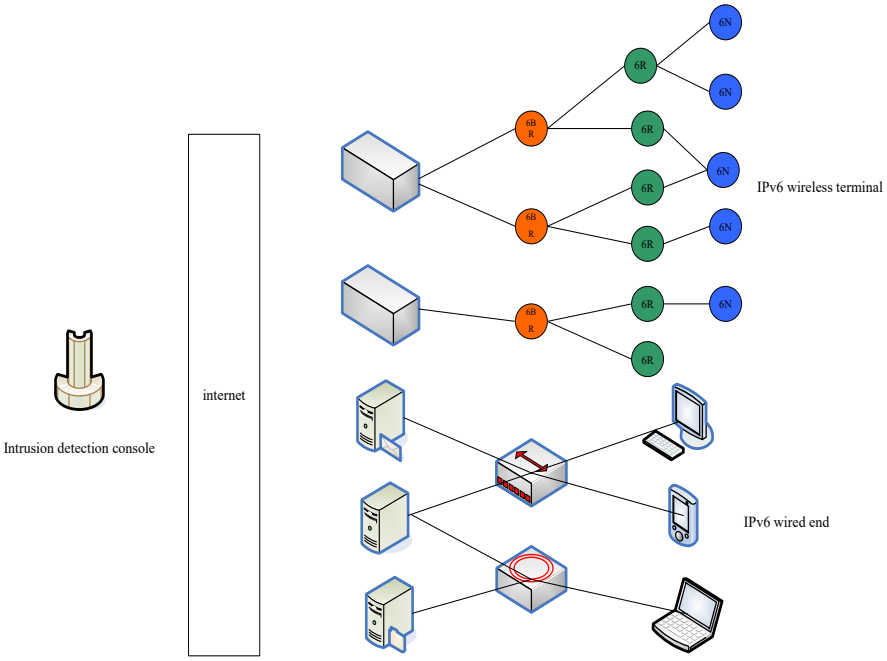


Figure 1. Wireless sensor network architecture

IPV6 wired terminal: By starting from one end of the Internet, the initial data packets are generated by servers (general servers and malicious servers). The messages generated by these servers are normal behavior and abnormal behavior.

In terms of IPV6 wireless terminals, that is, the interior of IPV6 wireless sensor networks, IPV6 nodes transmit packets to edge routing nodes through routing nodes and then upload IPV6 border nodes to the gateway. On each node, a restricted application protocol/message queue delivery protocol would be configured. The sensor node is configured as an application protocol/message queue delivery protocol client, and the generated data is sent to the gateway.

In IPv6 wireless sensor networks, several architectural characteristics directly influence the design of intrusion detection systems. First, sensor nodes typically have limited computational power, memory capacity, and energy resources, which restrict the deployment of computationally intensive detection algorithms at the node level. Second, IPv6 communication introduces large-scale addressability and heterogeneous traffic patterns, resulting in high-dimensional network traffic features that must be processed efficiently. Third, the multi-hop routing structure and distributed communication model of wireless sensor networks require intrusion detection mechanisms that can operate in a distributed manner without relying on centralized processing nodes.

Therefore, the intrusion detection architecture for IPv6 WSNs must satisfy three key requirements: lightweight feature extraction, scalable traffic analysis, and distributed detection capability. These architectural constraints motivate the design of the proposed parallel multipath intrusion detection framework, in which traffic monitoring and feature processing tasks are distributed across multiple detection paths to reduce computational overhead while maintaining real-time detection performance.

2.2. IPV6 Wireless Sensor Network Intrusion Detection Architecture

The IPV6 wireless sensor network intrusion detection console is shown in Figure 2.

Service generation module: It includes IPV6 wired server and IPV6 wireless network sensor node, which is responsible for generating original data packets for intrusion detection [9-10].

Business acquisition module: It includes the data package, intrusion detection and other functions in the Intrusion Detection System (IDS) [11-12]. The IPV6 wireline catches the information stream of the entry switch, and the IPV6 remote terminal catches the security include data sent by the doorway to the Web.

The highlight handling module: In IDS, the include handling is a component based extraction strategy. After the data stream is collected, the data stream is stored in the local database, and then the data is counted and selected using feature extraction and processing algorithms.

Intrusion detection module: In the IDS console, the statistical characteristics processed are taken as a Comma Separated Value (CSV) file and input into IDS. Through training the algorithm, a general profile of Network

Processor (NP) is obtained. In practical operation, normal and abnormal traffic are detected and classified in real time using standard curves.

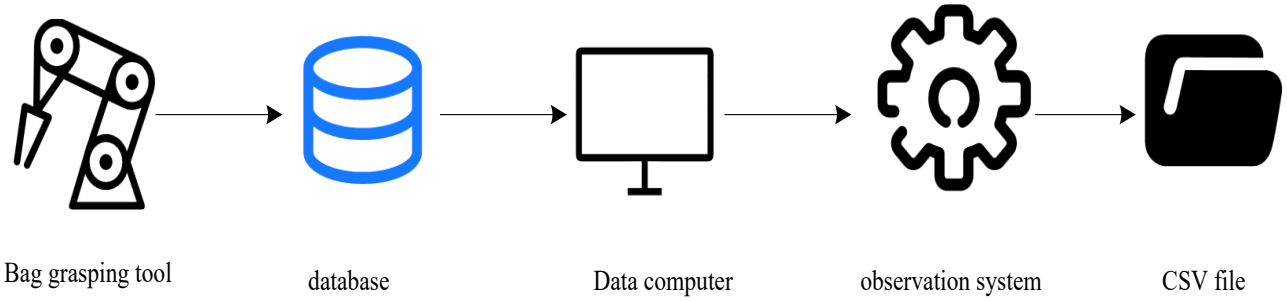


Figure 2. IPV6 wireless sensor network intrusion detection console

Intrusion response module: The management network is used to intercept an organization's attack. The operational workflow of the intrusion detection system can be described as a sequential data processing pipeline. First, the service generation module produces network traffic from both wired IPv6 servers and wireless sensor nodes. These traffic packets are captured by the business acquisition module, which collects raw packet streams from gateways and network switches. The captured traffic is then forwarded to the feature processing module, where statistical feature extraction and preprocessing operations are performed to generate structured security feature vectors. The generated feature vectors are transmitted to the intrusion detection module, which applies the detection algorithm to classify network behavior as normal or malicious. The detection process relies on statistical traffic patterns and trained detection profiles derived from historical network data. Once abnormal behavior is detected, the intrusion response module generates response actions such as isolating malicious nodes or blocking suspicious traffic flows. Through this modular interaction mechanism, the IDS architecture establishes a clear data flow from traffic generation to security response, enabling scalable and real-time intrusion detection in IPv6 wireless sensor network environments.

For example, a malicious node goes offline, or a node returns to a normal network state.

2.3. Security Evaluation of IPV6 Wireless Sensor Network

IPV6 wireless sensor network uses the lightweight packet transport layer security protocol and IEEE802.15.4 link layer security maintenance. The packet transport layer security protocol provides a mechanism for verifying the identity of the peer. Under this mechanism, all transport layer communications are encrypted, and the integrity of the data is verified to ensure a reliable and secure connection.

In addition, the adoption of tunnel mode for point-to-point connection would bring scalability problems and have a great impact on the overall performance of the network. The load above IP would be encrypted, which would only cause the network management or quality of service to fail to work properly. Therefore, the application of Internet Protocol Security (IPS) must be restricted.

As a communication gateway between an external untrusted network and its own subnet, the gateway in IPS is responsible for the secure connection between the gateway and the external system. In this example, only one gateway needs to implement the Authentication Header (AH). AH is mainly responsible for data source verification, data integrity verification and anti message playback function IPV6 wireless sensor network protocol architecture and corresponding security mechanism, as shown in Figure 3.

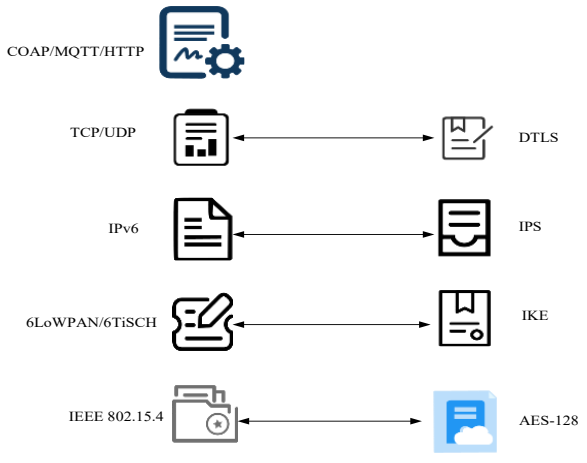


Figure 3. IPV6 wireless sensor network protocol architecture and corresponding security mechanism

2.4. Investigation of Intrusion Detection Algorithm of IPV6 Wireless Sensor Network

The workflow of intrusion detection algorithm is as follows:

Security trademark information assortment: IPV6 remote organization terminal gathers and stores information parcels produced by the entry switch. In the IPV6 remote terminal, IDS gadget fabricates a security highlight message and sends it to the door, while the parcel catch device catches the passage information bundle and stores it in the data set.

Characteristic data processing: The characteristic processing part generates the business characteristics by extracting the characteristics of the data stored in the local database, and makes statistics on the business characteristics, thus generating the security characteristic data.

Data normalization and feature selection: In the feature processing part, the security features are standardized, and then the appropriate security features are selected through feature selection algorithm, so that the security feature data can be obtained and trained.

Algorithm training: IDS module generates the model by training the algorithm, and estimates the super parameters of the model. In order to adapt to changes in the network, the intrusion detection model needs to be updated regularly [13-14].

IDS: The IDS module is used to detect new security features. If an exception is found, it would be handled by the IDS module. Figure 4 shows the workflow of IDS algorithm.

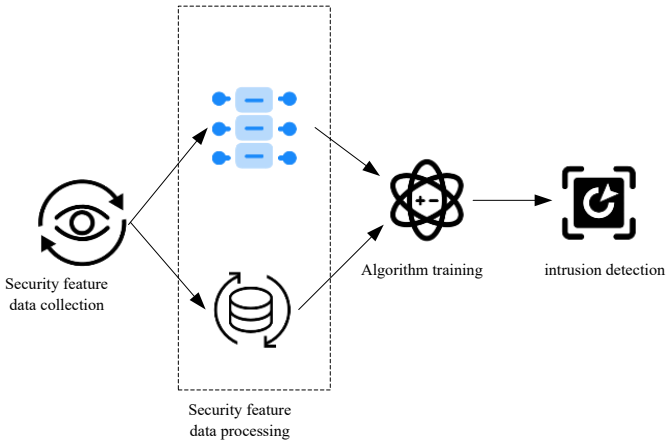


Figure 4. IPV6 wireless sensor network intrusion detection algorithm workflow

The wired organization administration of IPV6 is gotten by a bundle, which is acquired by an entrance switch. The bundle catch document should be handled to create a record in every approaching and active message. The records contain implied data about typical and strange ways of behaving. This record is utilized as security trademark information for online examination. The security elements of IPV6 wired terminals can be isolated into Hyper Text Transfer Protocol (HTTP). As indicated by the traffic attributes, it tends to be straightforwardly separated from the first parcel.

The security feature types of IPV6 wireless terminals include 40 types, including business features based on remote start service, traffic features based on 6Top, traffic features of application layer, traffic features based on slot channel frequency hopping, and traffic features based on statistical transactions. These traffic characteristics come from the original data package. According to the business characteristics of the application, it mainly includes IP address, port, protocol, type, etc. Exchange based highlights are produced by collaboration in view of stream distinguishing proof, which depends on a period window to keep up with online malignant way of behaving. It contains traffic information, such as the quantity of associations in a particular time span. Its stream distinguishing proof and meeting time are put away consecutively after the header of the first bundle is caught. Through the factual examination of the information bundles in the information parcels, it is gotten that the information bundles are in a proper information cycle. The interruption discovery calculation cycle would be portrayed exhaustively as follows.

2.5. Detection Process of Intrusion Detection Algorithm

The definition of alternative detection area of test data x is shown in Formula 1.

$$DR(x)=\left\{Cube(v_1,v_2,...,v_q)\middle|v_i=u_i,u_i+e_i\right\} \tag{1}$$

Let the Formula 2 be:

$$e_i=\begin{cases}+1, ui-|ui|>\dfrac{1}{2}\\ -1,\ \ ui-|ui|\le\dfrac{1}{2}\end{cases} \tag{2}$$

Rule 1: If there are more than k data in a grid, the test data in this grid is always normal; rule 2: At the point when the information in the matrix is not exactly k, the quantity of information in the not entirely set in stone; rule 3: In the event that the information in the advanced test is not exactly k, the information in the nearby Neighbor (3D square) is resolved constantly; when the information volume proportion k (shape) in Neighbor (block) is standard information, the test information would be still up in the air as unusual information if the information volume in Neighbor (3D shape) is not exactly k.

Super parameter estimation of intrusion detection model: The parameter settings used in the algorithm

would lead to changes in the model. The characteristics of density estimation are evaluated by means of Mean Integral Square Error (MISE) method. The generalized error of the model is estimated, and the most suitable super parameter is selected.

In the intrusion detection algorithm proposed in this paper, the variable should be the data volume in the DR of test data x, which satisfies the following Formula 3.

$$\hat{P} = \int_{DR(x)} \bar{f}(x)dx \tag{3}$$

In the formula, $P \in R^q$; $\hat{P}$ is the estimated value of P; $x \in R^q$ and $x \in DR(x)$. The Mean Square Error (MSE) is used to evaluate $\hat{P}$. $MISE(\hat{P})$ is the accumulation of local mean square error at each point x, which is a global evaluation criterion. The variable $P \in R^q$ satisfies the integral mean square error expression, as shown in Formula 4.

$$MISE(\bar{P}) = \int_{R^q} MSE(\bar{P}) = IV(P) + ISE(\bar{P}) = \int_{R^q} Var(\hat{P}) + Bias^2(\bar{P}) \tag{4}$$

Let the Formula 5 be:

$$Bias(\bar{P}) = E(\bar{P}) - P \tag{5}$$

The variance integral expression is shown in Formula 6:

$$IV(\hat{P}) = \int_{Rq} Var(\hat{P}) + \int \mathrm{cov}(\bar{f}_i, \bar{f}_j)dx = z_1 \frac{1}{nLq} - z_2 \frac{R(f)}{n} + O\left(\frac{1}{n}\right) \tag{6}$$

Let the Formula 7 be:

$$R(f) = \int_{R^q} f(x)^2 dx \tag{7}$$

In the formula, $z_1 = \sum_{i=1}^{w} z_i^2$ and $z_2 = (2L)^{2q}$. DR may cover $\left[2^q \quad 3^q\right]$ hypercubes. Therefore, $\frac{z_1}{z_2} \in \left[\left(\frac{3}{8}\right)^q, \left(\frac{1}{2}\right)^q\right]$.

It can be seen from the above that, firstly, based on the attack scenario described above, the security characteristics of IPV6 wireless sensor network can be described and security characteristic data can be generated. Secondly, the main work involved in IDS algorithm and the design of IDS algorithm are discussed in detail, and the overhead of IDS is analyzed theoretically, so as to ensure that malicious attacks in IPV6 system can be found in time or in real time without causing additional losses.

3. Verification and Evaluation of Intrusion Detection Algorithm

The IPV6 wired end can provide real attacks for the Web server through IXIAPerfectStorm. The IPV6 cable terminal uses the tcpdump tool to collect network traffic. The initial traffic of this file is 100 GB. Argus and Bro IDS tools were used to process the packet capture. The UNSW-NB15 was produced, which has 49 features. The IPV6 wireless terminal uses a 6 TiSCH simulator to simulate the normal behavior and attack behavior of the node, and generates data after the simulation is completed. This paper analyzes Dat files using feature package statistics, and obtain the feature set of each business instance. The specific network settings are shown in Table 1.

To ensure reproducibility of the experimental evaluation, the intrusion detection task in this study is formulated as a binary classification problem, where network traffic is categorized as either normal behavior or malicious intrusion behavior. The attack traffic includes several representative network attack categories contained in the UNSW-NB15 dataset, such as DoS attacks, reconnaissance activities, and unauthorized access attempts. Each network flow record is labeled according to the dataset annotation, which provides ground truth labels for supervised intrusion detection evaluation.

The feature set used for detection consists of selected statistical traffic attributes derived from the UNSW-NB15 dataset. Among the original 49 traffic features, a subset of representative features related to flow duration, packet statistics, and protocol characteristics is selected through feature correlation analysis. These features are used to construct the input vectors for the intrusion detection algorithm. The dataset is divided into training and testing subsets to evaluate the generalization capability of the proposed detection model.

Table 1. IPV6 wireless sensor network settings

serial number	Network Parameters	Parameter specific values	serial number	Network Parameters	Parameter specific values
1	Node size	50	4	RPL objective function OF	Optimal ETX
2	Time slot frame	5000	5	Time slot	0.01s
3	Data transmission method	Periodic sending of data with a period of 60s	6	Time slot frame length	101

3.1. Collection and Processing of Safety Characteristic Data

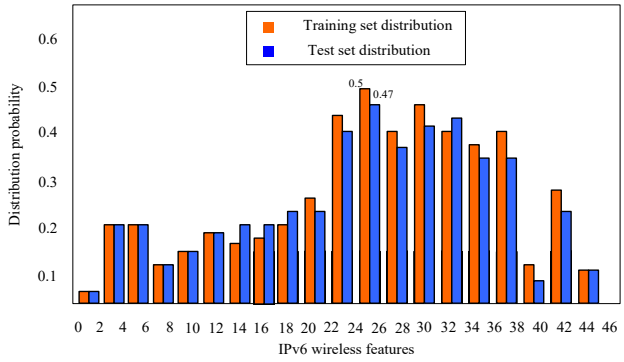
In the data preprocessing stage, feature normalization is applied to eliminate the influence of scale differences among traffic attributes. Specifically, min–max normalization is adopted to transform each feature into the interval [0,1], which can be expressed as

$$x' = \frac{x - x_{min}}{x_{max} - x_{min}}$$

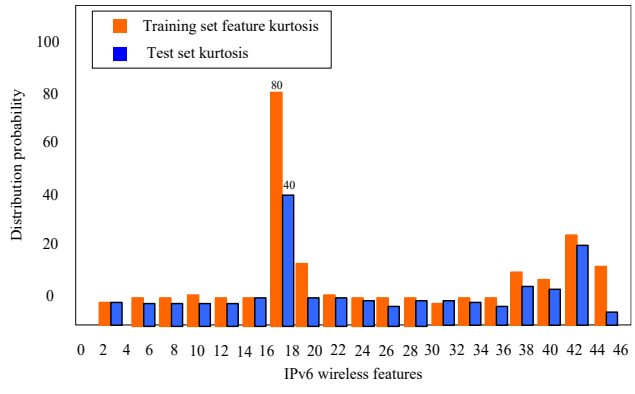
This normalization process ensures that all feature values are mapped to a unified range and prevents attributes with large numerical values from dominating the learning process.

After normalization, statistical analysis is performed on the traffic features. The skewness and kurtosis of the feature distributions are calculated to analyze the statistical characteristics of network flows. These statistics are used to evaluate feature stability and assist in selecting representative features for intrusion detection. The normalized dataset is then divided into training and testing subsets for model construction and evaluation.

Through the analysis of skewness and kurtosis of statistical flow characteristics, the goodness of fit test is conducted to select the features with good feature correlation. The security characteristics of IPV6 wireless terminals are classified into test group and training group, which are standardized. Figure 5 shows the probability distribution of features.



(a) IPV6 wireless terminal security feature probability distribution diagram

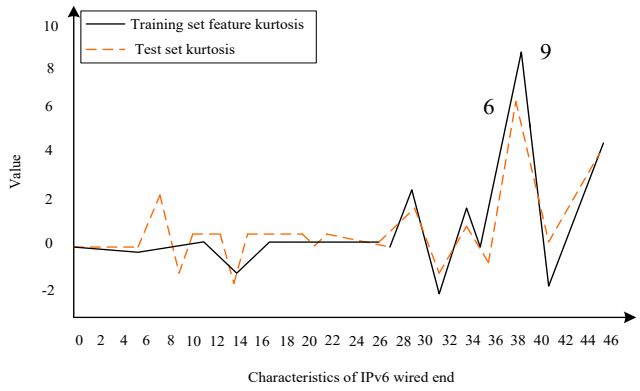


(b) IPV6 wireless terminal security feature kurtosis graph

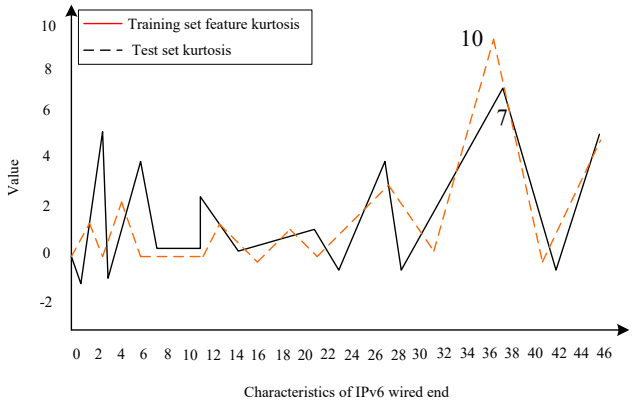
Figure 5. Characteristic distribution probability diagram

It can be seen from Figure 5 (a) that the probability characteristics are normally distributed. The characteristic distributions of training set and test set are nonlinear. Among them, in the range of 24-26, the distribution probability of the training set reaches the maximum of 0.5, while the distribution probability of the test set also reaches the peak of 0.47. The results show that the feature distributions of training set and test set are consistent. Figure 5 (b) shows the experimental results of using multivariate kurtosis function to calculate the data distribution of training set and test set. The results show that in the range of 16-18, the values of training set and test set reach the peak, and the peak values are 80 and 40 respectively.

Figure 6 (a) shows the skewness measurement of different features in the training set and the test set. The characteristics of training set and test set follow the same asymmetry. Figure 6 (b) shows the experimental results of using multivariate kurtosis function to calculate the data distribution of training set and test set.



(a) IPV6 Wireless terminal security feature deviation diagram



(b) IPV6 kurtosis diagram of wired terminal security features

Figure 6. IPV6 wired terminal data processing diagram

It can be seen from Figure 6 that in Figure 6 (a), the trademark skewness of the preparation set arrives at the greatest when it is 38, and its worth is 9. The trademark skewness of the test set is the most elevated at 37, and its worth is 6. Subsequently, the attributes of preparing set and test set follow a similar unevenness. In Figure 6 (b), the trademark kurtosis of the preparation set arrives at the most extreme when it is 36, and its worth is 10. The trademark kurtosis of the test set come to the most elevated at 38, with a worth of 7.

3.2. Evaluation of Intrusion Detection Effect

The efficiency of the algorithm is another goal of this scheme. This paper records the rate of data detection when testing the False Positive Rate (FPR). This rate reflects the computational cost of the algorithm to a certain extent.

To quantitatively evaluate the performance of the proposed intrusion detection algorithm, several commonly used intrusion detection metrics are adopted, including detection rate (DR), false positive rate (FPR), and detection latency. The detection rate measures the proportion of correctly identified attack instances, while the false positive rate represents the proportion of normal traffic incorrectly classified as malicious. These metrics can be defined as follows:

$$DR = \frac{TP}{TP + FN}$$

$$FPR = \frac{FP}{FP + TN}$$

where TP, FP, TN, and FN denote true positives, false positives, true negatives, and false negatives, respectively. In addition to classification performance, the detection latency is also evaluated to measure the computational efficiency of the proposed algorithm.

To sum up, in order to evaluate the performance and efficiency of intrusion detection, this paper would test the detection time. The safety feature dimension q selected for the two experiments is 10 [15-16]. The intrusion detection performance is preliminarily verified by experiments. In the experiment, the algorithm runs independently for 90 times, and the statistical experiment results are shown in Figure 7.

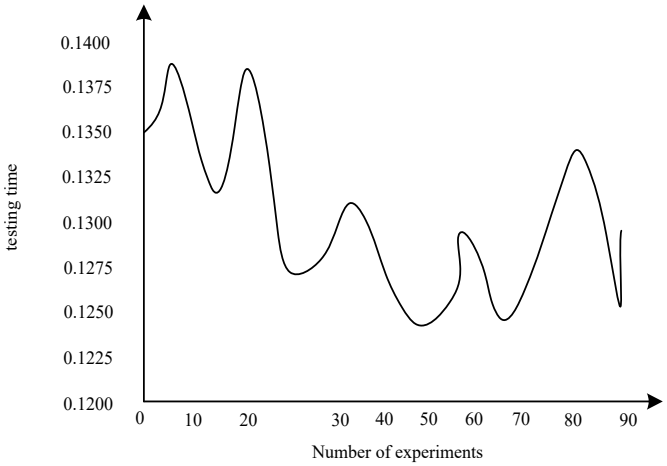


Figure 7. Experimental results

It can be seen from Figure 7 that the identification season of a solitary example is 0.12-0.14us, which meets the necessity of opportune location. The identification time change is because of the progressive handling of judgment conditions in the interruption discovery process. From the above results, it can be seen that the IDS framework proposed in this paper can meet the constant identification prerequisites of pernicious assaults in IPV6 network regarding execution and cost.

3.3. Discussion

The experimental results demonstrate that the proposed intrusion detection algorithm can effectively detect malicious network behavior in IPv6 wireless sensor networks. As shown in the experimental results, the average detection latency for a single sample ranges from 0.12 to 0.14 μs, indicating that the algorithm can support real-time intrusion detection requirements.

The efficiency improvement mainly benefits from the parallel multipath detection framework proposed in this study. By distributing traffic monitoring and feature analysis across multiple detection paths, the algorithm reduces the computational burden on individual nodes and improves processing efficiency. This distributed processing mechanism is particularly suitable for IPv6 wireless sensor networks, where node resources are limited and network traffic is highly dynamic.

However, the experimental evaluation also reveals several limitations. The current simulation environment only considers a network with 50 sensor nodes, which may not fully reflect large-scale deployment scenarios. In addition, the evaluation focuses mainly on detection latency and basic classification performance, while further studies are required to investigate detection robustness under more diverse attack patterns. These aspects will be considered in future work to further improve the

effectiveness of the proposed intrusion detection framework.

4. Conclusions

The goal of IPV6 is to provide IP addresses to each server. Such a huge network address would pose a great threat to the security of the network. The traditional wireless sensor network has no IP and is not threatened by wired. By aiming at the complexity of IPV6 network, a fast detection method based on IPV6 network was proposed. This paper aimed to design an intrusion detection algorithm based on the IPV6 network security architecture under the IPV6 wireless sensor network security architecture, so as to achieve rapid and timely detection of a large number of devices. The purpose of this paper was to achieve fast and real-time detection by making full use of the processing power and algorithm of the resource rich IDS system. However, this paper still has some problems. In the simulation test in this paper, only 50 nodes were simulated due to the performance limitation of the local area network central processing unit. In addition, due to the strong deceptive nature of malicious attacks, intrusion detection could not trace back to the source of the attack, which led to a certain degree of miscalculation. Therefore, in-depth analysis or systematic analysis of the security situation is required to achieve the purpose of prevention. Therefore, it is necessary to further study the characteristics and attack mechanism of the network.

Acknowledgements

(1) This work was supported by 2023's Hebei Provincial Higher Education Scientific Research Program. Research on IPv6 Network Intrusion Detection Algorithm Based on Parallel Multipath Transmission. Hebei Provincial Higher Education Scientific Research Program research result (QN2023104)

(2) This work was supported by2021's. Cangzhou Normal University in IPv6 network construction The good application research on network security protection system.

References

[1] Baraneetharan E. Role of machine learning algorithms intrusion detection in WSN: a survey. Journal of Information Technology, 2020, 2(03): 161-173.

[2] Dwivedi S., Vardhan M., &Tripathi S. Building an efficient intrusion detection system using grasshopper optimization algorithm for anomaly detection. Cluster Computing, 2021, 24(3): 1881-1900.

[3] Jia Y., Wang M., &Wang Y. Network intrusion detection algorithm based on deep neural network. IET Information Security, 2019,13(1): 48-53.

[4] Hadi A. A. A., & Al-Furat A. A. Performance analysis of big data intrusion detection system over random Forest algorithm. International Journal of Applied Engineering Research, 2018, 13(2): 1520-1527.

[5] Dong R. H., Hou H. Y., & Zhang Q. Y. An Intrusion Detection Model for Wireless Sensor Network Based on Information Gain Ratio and Bagging Algorithm. Int. J. Netw. Secur., 2020, 22(2): 218-230.

[6] Haghnegahdar L., & Wang Y. A whale optimization algorithm-trained artificial neural network for smart grid cyber intrusion detection. Neural Computing and Applications, 2020, 32(13): 9427-9441.

[7] Anitha P., & Kaarthick B. Oppositional based Laplacian grey wolf optimization algorithm with SVM for data mining in intrusion detection system. Journal of Ambient Intelligence and Humanized Computing, 2021, 12(3): 3589-3600.

[8] Tang Y., & Elhoseny M. Computer network security evaluation simulation model based on neural network. Journal of Intelligent & Fuzzy Systems, 2019, 37(3): 3197-3204.

[9] Hajimirzaei B., & Navimipour N. J. Intrusion detection for cloud computing using neural networks and artificial bee colony optimization algorithm. Ict Express, 2019, 5(1): 56-59.

[10] Wen L. Cloud computing intrusion detection technology based on BP-NN. Wireless Personal Communications, 2022, 126(3): 1917-1934.

[11] Devan P., & Khare N. An efficient XGBoost–DNN-based classification model for network intrusion detection system. Neural Computing and Applications, 2020, 32(16): 12499-12514.

[12] Maza S., & Touahria M. Feature selection algorithms in intrusion detection system: A survey. KSII Transactions on Internet and Information Systems (TIIS), 2018, 12(10): 5079-5099.

[13] Ashok K. D., & Venugopalan S. R. A design of a parallel network anomaly detection algorithm based on classification. International Journal of Information Technology, 2022, 14(4): 2079-2092.

[14] Senthilnayaki B., Venkatalakshmi K., & Kannan A. Intrusion detection system using fuzzy rough set feature selection and modified KNN classifier. Int. Arab J. Inf. Technol., 2019, 16(4): 746-753.

[15] Vimala S., Khanaa, V., & Nalini C. A study on supervised machine learning algorithm to improvise intrusion detection systems for mobile ad hoc networks. Cluster Computing, 2019 , 22(2): 4065-4074.

[16] Mehibs S. M., & Hashim S. H. Proposed network intrusion detection system based on fuzzy c mean algorithm in cloud computing environment. Journal of University of Babylon for Pure and Applied Sciences, 2018, 26(2): 27-35.