An Abnormal Detection Method Based on the Device Interaction Behavior in the Internet of Things

Wenjing Jin[1], Xiaofei Cui[1], Chengsheng Zhou[1(✉)], Hanxue Li[2], and Jianbo Zheng[3,4(✉)]

[1] China Academy of Information and Communications Technology (CAICT), Beijing 100089, People's Republic of China
zhouchengsheng@caict.ac.cn

[2] School of Communications and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400065, China

[3] Guangdong-Hong Kong-Macao Joint Laboratory for Emotional Intelligence and Pervasive Computing, Shenzhen MSU-BIT University, Shenzhen 518172, Guangdong, China
jianbo.zheng@smbu.edu.cn

[4] Artificial Intelligence Research Institute, Shenzhen MSU-BIT University, Shenzhen 518172, Guangdong, China

Abstract. With the development of smart homes, digital medicine, the Internet of vehicles, and other technologies, the application of the Internet of Things (IoT) is becoming more and more popular, and its security issues have attracted more and more attention from researchers. Anomaly detection schemes based on traffic can find anomalies at different levels by external means, which is a key part of the security protection of the IoT. However, existing researchers are faced with the problems of insufficient generality and strong method limitations. In view of this, based on the stability and constraint reflected by the physical constraints followed by the operation of the IoT system and the domain specification on the device interaction behavior, this study proposes a hierarchical traffic characteristic based on the integration of spatiotemporal characteristics of different levels such as packet, stream, session, host, etc. Secondly, based on the complete interaction behavior feature space, an integrated anomaly detection model is established by learning the interaction behaviors of different device pairs to realize accurate and efficient security event discovery. Finally, the propose method is evaluated on a BoT-IoT dataset. Ten-fold cross-check and the detection accuracy under different attack traffic and normal traffic ratio show the feasibility and superiority of the propose method.

Keywords: Internet of Things · Anomaly Detection · Device Interaction Behaviors · Machine Learning

This work was supported by Ministry of Industry and Information Technology Industrial Internet Innovation and Development Project-Internet of Things Ba- sic Security Access Monitoring Platform Project (TC210H023), and also supported by the Shenzhen Sustainable Development Special Project under grant KCXFZ20201221173411032.

V. C. M. Leung et al. (Eds.): Qshine 2023, LNICST 573, pp. 302–319, 2024.
https://doi.org/10.1007/978-3-031-65126-7_27

1 Introduction

Since the International Telecommunication Union formally put forward the concept of the Internet of Things (IoT) in 2005, sensor networks, cloud computing, microchips, and other technologies have been developing and maturing, and the IoT industry has been rapidly developing and expanding. Over the past five years, the number of IoT devices has experienced explosive growth. According to data released by authoritative statistical organizations, the global count of IoT devices connected to networks reached 2.035 billion in 2017 and is projected to exceed 7.544 billion by 2025. IoT is poised to profoundly impact various aspects of human production and daily life. Simultaneously, the rapid advancement of network technologies is poised to drive the comprehensive realization of the IoT era. Taking 6G mobile communication as an example, the 6G mobile communication network not only connects people but also links computing resources, vehicles, devices, sensors, and robotic agents to fulfill the requirements of a fully interconnected, intelligent digital world. In the 6G mobile communication system, the widespread deployment of IoT leads to a rapid increase in network access points. According to Ericsson's predictions, by the year 2025, over 24.9 billion devices will be connected to networks.

Amidst the thriving development of the IoT, existing security mechanisms have struggled to meet the escalating security demands, resulting in a proliferation of security concerns across diverse application scenarios. The susceptibility of numerous devices to malicious code threats or unauthorized control has given rise to an array of security issues, and in some instances, triggered large-scale security incidents. A notable case occurred in 2016 when the infamous Mirai worm exploited IoT devices, causing a massive Distributed Denial of Service (DDoS) attack that led to widespread internet disruption on the U.S. East Coast. Prominent websites experienced service outages. More recently, smart speakers have been exploited by attackers for eavesdropping on user privacy, underscoring how IoT security threats evolve in tandem with technological advancements. Timely threat detection and proactive defense are pivotal strategies in countering such threats. Anomaly detection plays a crucial role in mitigating malicious activities within defense systems and networks.

Over the past years, research into IoT anomaly detection has surged to combat network attacks, resulting in the proposal of numerous detection mechanisms. Nonetheless, the distinctive attributes of IoT systems present substantial challenges to implementing comprehensive security measures. For instance, a lack of unified standards in IoT platform design, development, communication interaction, and access control, coupled with inadequately protected internal and external operational environments, hamper effective security. Existing solutions exhibit limitations such as narrow applicability and insufficient automation. Additionally, many manufacturers are inclined to believe that augmenting security measures won't enhance a device's market value but rather escalate production costs. Consequently, post-sales support, patch provisioning, and updates are often overlooked, leading to a proliferation of vulnerable devices with high-risk vulnerabilities like default credentials and plaintext transmission of keys. Consequently, a holistic and generalized anomaly detection mechanism, tailored to the distinct IoT network environment, is paramount for bolstering IoT security.

Network traffic encompasses all data communication of IoT devices, and the prevalent approach in IoT environments for safeguarding involves the sidestream collection of network traffic for data analysis and anomaly detection. Leveraging the inherent characteristics of IoT, network communication between IoT devices abides by established objective constraints. Under normal operation, devices tend to adhere to predefined behaviors in a repetitive manner. In light of this, this study introduces an IoT anomaly traffic detection method focused on device interaction behaviors, enabling precise and timely anomaly detection through a comprehensive depiction of interaction behaviors between devices. Specifically, this research contributes in two key aspects:

1. A device interaction behavior representation method based on hierarchical flow features is proposed. This study comprehensively characterizes and portrays the interaction behaviors between IoT device nodes at four levels: packet, flow, session, and host. This realization of thorough interaction behavioral representation establishes a benchmark feature space for IoT anomaly detection.
2. A novel, universal, accurate, and efficient anomaly detection method is innovatively presented from the perspective of device interactions. Escaping the constraints of traditional anomaly detection methods tailored to hardware or specific applications, and addressing the gradual drop in detection rate, this approach capitalizes on IoT's intrinsic attributes. It introduces an anomaly detection scheme centered on the constraints adhered to by device interactions. The propose scheme is experimentally evaluated using the BoT-IoT dataset [1], with an average detection rate of 98.4% and a false positive rate of 1.3%, directly validating the feasibility and superiority of the approach.

2 Security Threats Faced by the Internet of Things

In the course of interactions, the IoT inevitably gives rise to information security issues, encompassing physical security, operational security, and data security. This section provides an analysis of the primary security threats confronting IoT.

2.1 Physical Attacks

An investigation conducted by the MPI Group in 2017 revealed that only 47% of IoT manufacturers consider security concerns during the conceptual or design stages. Furthermore, 21% of manufacturers only begin to contemplate security during the production phase, while 18% address security issues only at the quality management stage. Shockingly, the remaining manufacturers never take security into account. The proliferation of zombie networks like Mirai can be attributed to the fact that many IoT devices lack even the most rudimentary security measures. IoT is extensively employed to replace human intervention in complex, hazardous, or mechanical tasks, with sensor devices predominantly operating without human supervision. Moreover, the majority of these devices possess simplified functionality, and the diverse applications of sensor devices employ distinct standards and protocols, precluding the adoption of unified security measures against external attacks.

Due to the aforementioned factors, sensor devices are susceptible to manipulation and destruction by malicious actors, making them vulnerable to security threats such as data breaches and zombie networks. Physical attacks involve tampering with sensor devices to achieve malicious tracking and data acquisition objectives. Attackers dismantle the physical casings of devices like hosts or embedded systems, subjecting them to physical dissection and analysis. This enables the extraction of sensitive components like processors and memory, thus obtaining critical sensitive parameters including key information, passwords, and configuration details.

2.2 Authentication Attacks

Attackers can exploit the default credentials of physical devices in the IoT to initiate attacks and gain unauthorized access to data. Devices with weak authentication processes or those sharing identical authentication information are susceptible to authentication-based attacks.

2.3 Communications Protocol Attacks

The application of multiple communication protocols has indeed introduced threats to the security landscape of the IoT. On one hand, the dynamic nature of network structures presents security vulnerabilities. Due to the ever-evolving nature of IoT network architectures and the emergence of various new network protocols, vulnerabilities within these new protocols and the ongoing upgrade and update of network devices may potentially introduce novel security threats. On the other hand, the convergence of diverse networks generates security risks. The IoT is a confluence of multiple networks that support the IP protocol, each employing distinct security strategies. This convergence process can give rise to fresh security risks and vulnerabilities. In many instances, communication protocols might have introduced vulnerabilities during their initial design or subsequent implementation and configuration phases, thereby rendering the IoT susceptible to security protocol attacks at the transport layer.

2.4 Wireless Detection

In the realm of the IoT, wireless communication is a prevalent means of data transmission. However, wireless signals that are exposed can be easily disrupted and intercepted by malicious actors. This susceptibility results in severe consequences like the paralysis of wireless communication networks, the theft of sensitive user information, and the fabrication of data. Wireless probing predominantly occurs within the sensing layer of the IoT, giving rise to security threats that encompass two primary facets. Firstly, the pilfering of information from sensing nodes is a considerable concern. These nodes typically serve as basic information repositories with limited computational and processing capabilities. Unauthorized users can effortlessly access relevant data stored within these nodes. Secondly, the impersonation of sensing nodes poses a critical challenge. Attackers pilfer label information from these nodes, subsequently replicating or altering these labels. By impersonating the identity of the nodes, attackers gain access to valuable information, undermining the credibility and efficacy of the compromised nodes.

Just as network attackers employ network reconnaissance tools for scanning and gathering information about hosts, subnets, ports, and protocols within a network, analogous tools targeting IoT devices now exist. These tools are capable of probing and scanning IoT devices, revealing pertinent information about them. Presently, a substantial portion of IoT devices available in the market utilizes wireless communication protocols, such as ZigBee, ZWave, Bluetooth-LE, and Wi-Fi 802.11. Unfortunately, these protocols are susceptible to wireless surveillance and probing attacks, akin to their network counterparts.

Malware infections, denial of service attacks, unauthorized access, and the injection of falsified data packets are all common attack methods within the realm of the IoT. To safeguard IoT systems from network attacks, a myriad of security measures have emerged, including encrypted communication data, data integrity validation, and access control techniques. These methods serve to shield systems from a variety of attack types. However, even with these security measures in place, attackers can still successfully target systems, employing tactics like malicious packet injection and DDoS attacks. Therefore, the implementation of network anomaly detection becomes crucial to further enhance the security of the IoT.

3 Current State of Research on Anomaly Detection in the Internet of Things

Due to the extensive access of IoT devices, network traffic is experiencing exponential growth. The shared data between devices and on the network becomes more susceptible to cyberattacks. To mitigate the emerging network attacks on IoT devices, greater efforts are required to research anomaly detection [2, 17]. Machine learning (ML)-based detection methods have gained popularity in recent years as a prevalent approach for anomaly detection in the IoT [3, 4]. Employing machine learning techniques, these methods autonomously learn patterns and characteristics from IoT data, enabling independent anomaly detection.

Qiu et al. [5] focus on the deception problem in mobile social networks and propose an adaptive social spammer detection model that improves the security of social users. Dutta et al. [6] propose an integrated approach that leverages deep models and stacking techniques, utilizing a heterogeneous flow-based dataset containing IoT data to achieve reliable anomaly classification. In response to the lower performance and predictive accuracy of intrusion detection systems based on anomaly-driven ML in IoT intrusion detection, Abdelmoumin et al. [7] introduce a method for optimizing models using hyperparameter tuning and ensemble learning to enhance IoT security. Nie et al. [16] focus on the safety and malicious attack issues related to connected vehicle networks. They have designed a data-driven intrusion detection system and a deep learning architecture based on convolutional neural networks, aiming to detect intrusions targeting roadside units. As a novel distributed learning paradigm, Federated Learning (FL) facilitates decentralized training of predictive models through collaborative means [8]. In order to ensure the efficiency, accuracy, and effectiveness of anomaly detection in the context of industrial IoT, Wang et al. [9] introduce an architecture for anomaly detection and an empowered approach utilizing federated deep reinforcement learning. This approach

achieves the dual objectives of preserving privacy and enhancing anomaly detection precision. Furthermore, Liu et al. [10] develop a convolutional neural network model with long short-term memory to enhance detection accuracy. They also employ gradient compression in FL to reduce communication costs and improve communication quality. Addressing issues in the context of the IoT, where traditional anomaly detection methods suffer from low detection accuracy due to imbalanced massive data and poor model generalization caused by data heterogeneity, Thing et al. [11] utilize a neural network composed of multi-layer sparse autoencoders and stack autoencoders to detect various types of attacks within the network. Doshi et al. [12] leverage IoT-specific network behaviors as features and employ neural networks and ML techniques to achieve high-precision detection of DDoS attacks in IoT communication. Considering the long-term dependencies in streaming data, Cheng et al. [13] introduce a semi-supervised hierarchical stacked temporal convolutional network. This network design fully embraces the characteristics of streaming data in IoT while eliminating uncertain records.

As the IoT continues to evolve, based on a survey of recent research findings [14, 15], it can be observed that ML-based anomaly detection solutions primarily focus on feature selection, model optimization, and improving model generalization capabilities. However, inherent challenges such as strong data dependencies and the inability to adapt to unknown attacks persist within ML approaches. While the integration of deep learning partially mitigates these issues, a fundamental resolution remains elusive.

Analyzing the characteristics of network attacks themselves, these attacks aim to compromise the confidentiality, integrity, and availability of system information. They typically induce deviations from normal network operations, manifesting as abnormal behaviors. As a result, identifying anomalies can be achieved through the discovery of patterns in data that deviate from expected behaviors. System invariance refers to a condition within the "physical" or "chemical" characteristics of a system's operational process, which must hold whenever the system is in a given state. Analyzing physical invariances for anomaly detection has been applied in numerous cyber-physical systems involving networked information and physical components. The underlying processes of the IoT are governed by their operational principles, with inter-device process states being predictable and foreseeable. Hence, the assimilation of the inherent and objective attributes of the IoT, coupled with their modeling, serves as a robust approach for achieving anomaly detection. This approach is versatile and well-suited for detecting novel and emerging types of attacks.

4 Device Interaction Behavior Representation

4.1 Device Interaction Behavior Abstraction

The fundamental building blocks of the IoT comprise a diverse array of sensor devices. The functionality of these devices is preconfigured during their manufacturing, resulting in a set of fixed and limited executable actions. By comprehensively learning the finite operational behaviors among these devices, precise and efficient anomaly detection can be achieved.

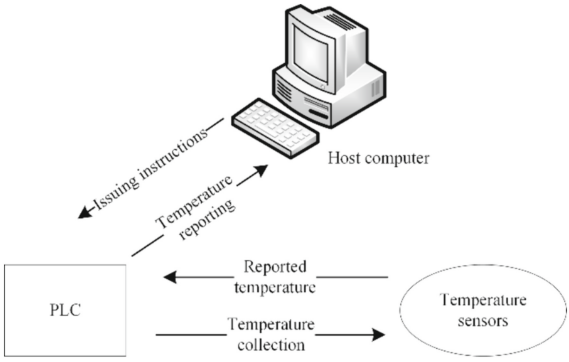

Fig. 1. The example of interactive behaviors of IoT devices.

As illustrated in Fig. 1, taking a temperature sensor as an example, its factory-set function is to gather data on the ambient temperature. Within the context of the IoT, the upper-level computer issues commands to a controlling Programmable Logic Controller (PLC) to schedule periodic temperature measurements and reporting by the temperature sensor. The PLC then forwards the timed measurement instruction to the temperature sensor, which subsequently collects data and reports it. Under normal circumstances, this functional logic is executed repetitively and periodically in a stable manner, assuming no interference or attack. Therefore, by thoroughly studying and modeling all data in this interaction process, any anomalies that arise can be promptly detected.

Existing research has rarely addressed the unique interaction behaviors within network communication. This is primarily because human-initiated interactions are usually driven by human consciousness, displaying attributes of variability, complexity, and subjectivity. However, in practical IoT environments, interaction processes among entities possess certain complexity. Yet, these processes are coordinated to achieve and maintain the dynamic stability of the network environment. Thus, representing entity interaction processes is feasible. In light of this, by comprehensively learning the baseline of interaction behaviors among IoT devices, the detection of any anomalies can be timely, comprehensive, and accurate.

4.2 Device Interaction Behavior Abstraction

According to the analysis in Sect. 4.1, the comprehensiveness and accuracy of the description of interaction behaviors between device nodes directly impact the accuracy of anomaly detection. To comprehensively describe interaction behaviors, this study proposes a method for characterizing device interaction behaviors based on hierarchical flow feature extraction. This method divides the interaction behavior between two device nodes into different hierarchical levels, as shown in Fig. 2, and extracts features from both the temporal and spatial dimensions to achieve a comprehensive representation of the interaction behavior.

The network traffic in the IoT contains interaction data between different nodes, and these interactions involve three levels: session, flow, and packet. Therefore, in this study, we first define the four delineated levels as follows:

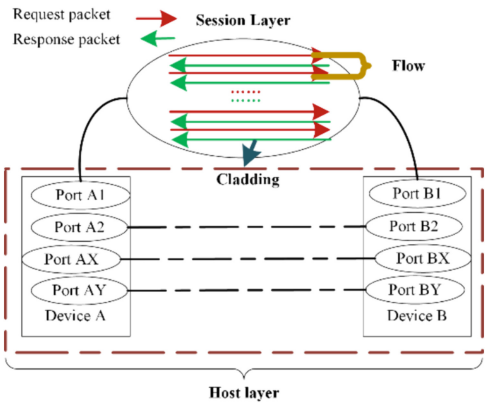

Fig. 2. A hierarchical description of device interaction behavior.

Definition 1. Host Level: In a network, a host is usually identified by one or more IP addresses as its communication address within the network. For analytical and definitional purposes, this study assumes that in the context of the IoT, one IP corresponds to one actual device node. All communication between two IP addresses, i.e., data packets with identical or reverse-source and destination IP addresses, is considered communication data between two devices, referred to as host-level data.

Definition 2. Session Level: Traffic data generated between devices comprises interactions involving multiple applications or services. Different applications or services are represented by distinct port numbers and application protocols in data packets. In this study, a session is formed by aggregating all data packets with the same five-tuple (source IP, source port, destination IP, destination port, and transport layer protocol) or reverse identical five-tuple (source IP, source port, destination IP, and destination port interchanged) within the same session.

Definition 3. Flow Layer: A session consists of one or multiple data streams. Based on the division rules of data streams, within a session, the temporal distribution of data packets in the same direction is considered. Temporal sequence features are essentially consistent when extracted across different hierarchical dimensions, as expressed in Eq. (1).

$$f_{interval} = \{t_0, t_1, t_2, \ldots, t_n, \}, f_{duration} = \{t_0, t_1, t_2, \ldots, t_n, \} \tag{1}$$

where $f_{interval}$ represents the time interval feature set, composed of the initial time representations of the smallest analytical units at this layer, $f_{duration}$ represents the duration feature set (which is absent at the packet level as the smallest analytical unit is the data packet). Additionally, packets with a time difference not exceeding the threshold both before and after, and not exceeding the flow aging time since the first packet in the stream, are aggregated into unidirectional flows.

Definition 4. Packet Level: Data packets constitute the smallest unit of traffic analysis. Every phenomenon is constructed upon the framework of time and space. Space captures

the inherent structural characteristics of networks, while time captures the trends and patterns of network dynamic evolution. Therefore, this study extracts network flow features from both temporal and spatial perspectives to characterize interaction behaviors.

Temporal features of traffic mainly refer to the temporal characteristics of traffic, including time series and time distribution features. The most fundamental attribute within the temporal domain is the time series, which describes the flow unit at different levels (host, session, flow, packet layers).

As temporal flow statistics are based on the relationship between the current connection and statistics within a certain time range, spatial features of flow are needed as a complement. Spatial features of flow primarily encompass attributes such as packet size and packet count. According to the division of network traffic levels, spatial features are analyzed and extracted at the packet, unidirectional flow, session level, and host level.

(1) Packet-level Spatial Features

Studying extractable spatial features at the packet level includes considerations such as packet length. Packet length refers to the size of an individual data packet, effectively capturing the size attribute of network behavior at the packet level. In certain attacks, variations in packet length may exhibit consistent and relatively fixed patterns. In comparison to the more random nature of legitimate communication behavior, these variations often possess discernible distinctions.

(2) Flow-level Spatial Features

Investigating extractable spatial features at the flow level encompasses factors such as packet count and flow byte count. Packet count refers to the quantity of data packets within a single flow, while flow byte count quantifies the size of the entire flow in terms of bytes.

In certain attack scenarios, attackers may frequently initiate communication within the scope of a single flow to achieve their objectives. Legitimate communication behavior, on the other hand, typically displays temporal randomness within a single flow, leading to the capability of differentiating between normal and malicious communication behavior using features related to packet count and flow byte count.

(3) Session-level Spatial Features

Examining session-level considerations reveals primary features such as flow count and session byte count. Similar to flow-level features, flow count and session byte count respectively reflect the characteristics of session quantity and size. In some attack scenarios, attackers might exploit specific services or a combination thereof to execute their attacks. For instance, in attacks like SYN-FLOOD, attackers often exhibit features characterized by a large quantity of the same type of port usage, indicative of an attempt to rapidly deplete server resources.

(4) Host-Level Spatial Features

From the perspective of host-level analysis, significant features that can be extracted include the number of ports and the total number of transmitted bytes. The total number of transmitted bytes can indicate the amount of communication exchange resources

utilized by the user, while the number of ports, as an essential attribute at the host level, can effectively reflect the quantity and variety of accessed services in communication behavior. In the context of malicious communication behavior, attackers may concentrate attacks from one or a few IP addresses. For instance, a botnet might infect a large number of hosts with bot programs, forming a one-to-many controllable network between the controller and infected hosts. Such a network often utilizes a group of hosts to launch denial-of-service attacks against a specific target. In this scenario, the feature related to port count tends to remain relatively low and fixed. Furthermore, to consume the resources of the target under attack, the total number of transmitted bytes tends to increase.

Based on the summarized observations, this study constructs the feature space for device interaction behaviors as shown in Table 1. This research intends to represent device interaction behaviors without relying on any biased features. As a result, features such as packet length, packet count, session interval, information entropy, and packet skewness are selected to characterize the stability and regularity of the interaction process.

The standard deviation, denoted by "σ", is the arithmetic square root of the variance. It reflects the dispersion of a dataset and is defined as follows:

$$\sigma = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(x_i - \mu)^2} \tag{2}$$

In formula (2), N represents the length of the dataset, μ represents the mean of the dataset, and x_i represents any random variable within the dataset.

The Packet Inclination Rate (PIR) is defined as the ratio of the number of packets exchanged to the average packet length during a certain time window in the interaction process between two devices. Its calculation formula is shown in formula (3), where n represents the number of interactions within the time window, FP_i stands for the number of packets in the i - th interaction session ($i = 1,2,3,\ldots,n$), and FB_i stands for the number of bytes in the i - th interaction session ($i = 1,2,3,\ldots,n$):

$$\mathrm{PIR} = \frac{\left(\sum_{i=1}^{n} FP_i\right)^2}{\sum_{i=1}^{n} FB_i} \tag{3}$$

When devices extensively utilize small packets for network communication, the packet skewness exhibits higher values.

5 Detection Model

The IoT anomaly traffic detection model based on entity interaction protocol consists of three essential components: traffic collection, feature extraction, and anomaly detection. This section provides a comprehensive overview of each key step.

Table 1. Interaction behavior features space between different IoT devices.

Feature Hierarchy	Feature Name				
Package Level	Package Length	-	-	-	-
Flow Level	Total Package Length	Total Number of Packages	Flow Duration	-	-
Session Level	Number of Packets Sent by Sender	Total Packet Length Sent by Sender	Average Packet Length Sent by Sender	Minimum Packet Length Sent by Sender	Maximum Packet Length Sent by Sender
	Packet Length Standard Deviation Sent by Sender	Packet Count Standard Deviation Sent by Sender	Packet Length Slope of the Sender	-	-
	Number of Packets Received by Receiver	Total Packet Length Received by Receiver	Average Packet Length Received by Receiver	Minimum Packet Length Received by Receiver	Maximum Packet Length Received by Receiver
	Packet Length Standard Deviation Received by Receiver	Packet Count Standard Deviation Received by Receiver	Packet Length Slope of the Receiver	-	-
	Total Number of Packets in the Session	Total Packet Length in the Session	Average Packet Length in the Session	Minimum Packet Length in the Session	Maximum Packet Length in the Session
	Packet Length Standard Deviation in the Session	Packet Count Standard Deviation in the Session	Packet Length Slope in the Session	Session Duration	-

(*continued*)

Table 1. (*continued*)

Feature Hierarchy	Feature Name				
Host Level	Number of Open Ports by Sender	Port Information Entropy of the Sender	Number of Open Ports by Receiver	Port Information Entropy of the Receiver	Total Number of Open Ports Between Hosts
	Port Information Entropy Between Hosts	Number of Connection Sessions Between Hosts	Total Number of Packets in Communication Between Hosts	Total Packet Length in Communication Between Hosts	Packet Length Slope

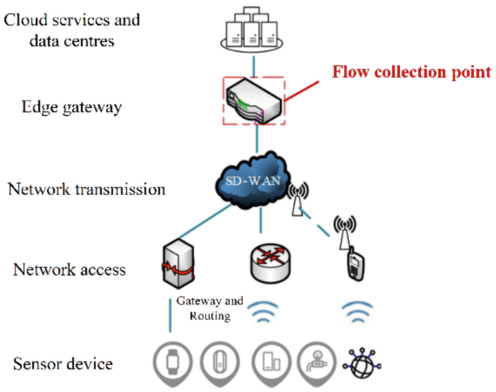

Fig. 3. Typical topology of the IoT.

5.1 Traffic Collection

A typical topology of an IoT network is illustrated in Fig. 3. The traffic generated by devices is initially aggregated at the edge gateway and subsequently funneled through routers before being connected to the Internet. Consequently, at the edge gateway, the incoming and outgoing traffic of devices can be collected in real-time.

5.2 Feature Extraction

According to Sect. 4.2, the feature space for representing interactive behaviors is illustrated in the process diagram shown in Fig. 4.

Extraction of Flow-Level Features: The packet-level data is truncated based on a flow aging time of 15 s, as defined in this study. The data is grouped every 15 s. For each group of data, the packet-level data's five-tuple (source IP, source port, destination IP, destination port, protocol number) is aggregated as key-value pairs to obtain flow-level

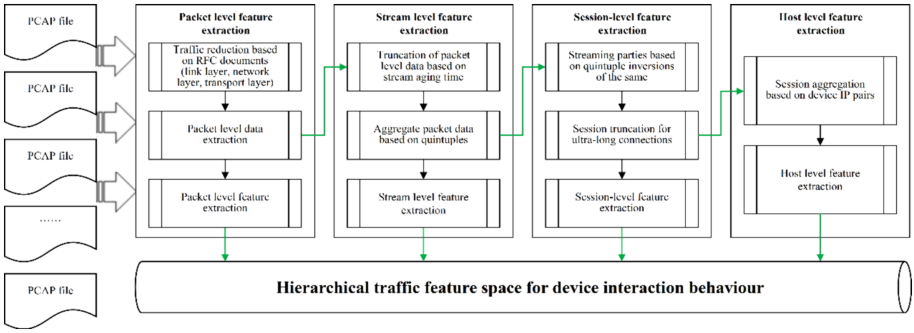

Fig. 4. Feature extraction flow char.

data. The format of flow-level data is as follows: second-level timestamp, source IP, source port, destination IP, destination port, protocol number, packet count, byte count, and flow interval. The timestamp for flow data is taken from the maximum time within that packet group. The features extracted are packet count, byte count, and flow interval.

Extraction of Session-Level Features: Flow data is aggregated based on identical five-tuples (as the sender) or reverse five-tuples (as the receiver). For aggregated data, if the time interval exceeds 30 min, it is truncated and divided into multiple sessions. The format of session-level data is as follows: second-level timestamp, sender IP, sender port, receiver IP, receiver port, protocol number, sender packet count, sender byte count, receiver packet count, receiver byte count, total packet count, total byte count, sender duration, receiver duration, total duration, sender packet count sequence, sender byte count sequence, receiver packet count sequence, receiver byte count sequence, number of flows in session.

Extraction of Host-Level Features: Session-level data is aggregated based on (sender IP, receiver IP) to obtain host-level data in the format: sender IP, receiver IP, sender port sequence, receiver port sequence, session count, total packet length, total packet count. Corresponding features are extracted using the calculation formula for information entropy.

5.3 Detection Framework

Built upon the stability characteristics of device interactions in the IoT ecosystem, the core idea of this research is to model the interactions between device pairs present in the network traffic collected at the IoT egress point. This modeling process is conducted individually for each device pair, enabling precise and comprehensive anomaly detection.

As depicted in Fig. 5, the propose IoT anomaly traffic detection framework comprises two main phases: the training phase and the detection phase.

Training Phase: During this phase, normal network traffic generated during regular device operation is collected as training samples. The interactions between device pairs are aggregated to extract respective feature vectors. To ensure practicality in the detection framework and to model each set of interactions, a simple decision tree is employed for autonomous modeling. This results in the formation of a baseline model ensemble that encompasses various groups of interacting devices.

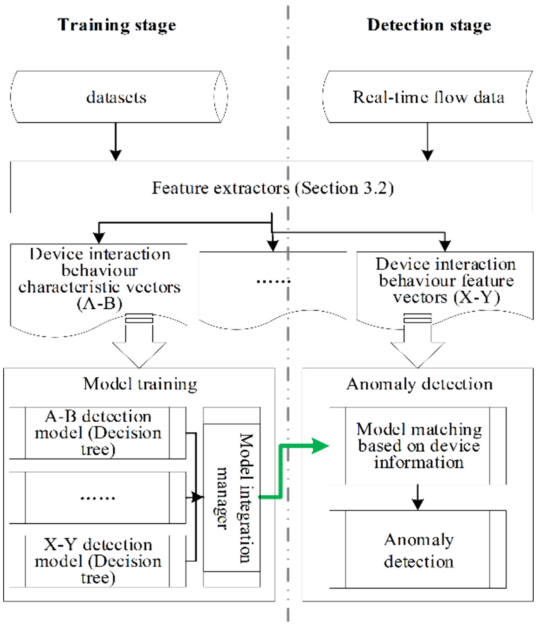

Fig. 5. Anomaly detection model.

Detection Phase: In real-time, the collected flow data undergoes feature extraction using a feature extractor to generate feature vectors for each interacting device pair. By leveraging IP identification information of the interacting devices, their corresponding "baseline" models are selected for anomaly detection. If a feature space deviates from the baseline, it is classified as an anomaly and triggers an alert directly.

6 Experiment Validation

6.1 Dataset

In this study, we conducted experiments and evaluations using the BoT-IoT dataset. The BoT-IoT dataset was created by designing a real-world network environment within the University of New South Wales Canberra Network Range Laboratory. This environment combines normal traffic with zombie network traffic. The dataset's source files are provided in various formats, including original pcap files, generated argus files, and CSV files. These files are segregated based on attack categories and subcategories to facilitate the labeling process. The captured pcap files amount to 69.3 GB in size, encompassing over 72,000,000 records. Extracted CSV-format traffic data constitutes a size of 16.7 GB. The dataset includes attacks such as DDoS, DoS, operating system and service scanning, keystroke logging, and data leakage. Furthermore, DDoS and DoS attacks are further organized based on the protocols employed. Table 2 illustrates the labeled attack types present within the BoT-IoT dataset.

6.2 Evaluation Metrics

Anomaly detection is a binary classification problem. In this study, we employ five metrics to evaluate the performance of the model: Precision (P), Recall (R), Accuracy (Acc), area under the Precision-Recall (P-R) curve, and Area Under ROC Curve (AUC). The definitions of P, R, and Acc are shown in Eqs. (4), (5), and (6):

$$\mathrm{P} = \frac{TP}{TP + FP} \tag{4}$$

$$\mathrm{R} = \frac{TP}{TP + FN} \tag{5}$$

$$\mathrm{Acc} = \frac{TP + TN}{TP + TN + FP + FN} \tag{6}$$

TP, TN, FP, and FN respectively stand for: True Positives, True Negatives, False Positives, and False Negatives. AUC represents the area under the ROC curve. The ROC curve has False Positive Rate (FPR) on the horizontal axis and R on the vertical axis. If the ROC curve of one classifier is entirely "enclosed" by the ROC curve of another, it can be inferred that the latter has better performance than the former. However, situations with crossing curves might also occur. Therefore, a more reasonable approach is to compare the areas under the ROC curves. The computation of FPR is given by Eq. (7):

$$\mathrm{FPR} = \frac{FP}{TN + FP} \tag{7}$$

The P-R curve plots R on the x-axis against P on the y-axis. Similar to AUC, the area under the P-R curve reflects the proportion of a learner's performance that achieves a relatively high balance between Precision and Recall.

Table 2. The type of attack marked by the BoT-IoT dataset.

Attack Types	Subtypes
DoS	DoS HTTP
	DoS TCP
	DoS UDP
DDoS	DDoS HTTP
	DDoS TCP
	DDoS UDP
Scan	OS Scan
	Service Scan
Theft	Data Exfiltration Keylogging

6.3 Detection Performance

In this study, we initially employed ten-fold cross-validation to validate the model, and the results are presented in Table 3. The outcomes straightforwardly demonstrate the effectiveness and utility of the propose model.

Table 3. Ten-fold cross-validation results.

ID	P	R	Acc	AUC	P-R
1	97.13%	96.18%	95.07%	0.94	0.98
2	97.23%	96.02%	95.05%	0.94	0.98
3	97.35%	95.89%	95.07%	0.94	0.98
4	97.31%	97.43%	96.13%	0.95	0.98
5	97.52%	96.77%	95.84%	0.94	0.98
6	96.43%	97.52%	95.50%	0.94	0.98
7	97.13%	97.32%	95.89%	0.95	0.98
8	97.25%	96.40%	95.40%	0.95	0.98
9	98.12%	97.10%	96.01%	0.96	0.98
10	97.99%	96.87%	95.88%	0.95	0.98

Taking into account the real-world scenario's distribution between normal network traffic and attack traffic, we conducted five rounds of validation by controlling the ratio between training and testing data. We divided all the data into different portions using various values of λ (the ratio of training data to testing data), and the model's detection performance is illustrated in Table 4. According to the detection results, the domain-aware anomaly detection approach proposed in this study can accurately identify all abnormal behaviors that deviate from normal scenario settings.

Table 4. Model effect under different traffic ratios.

λ	P	R	Acc	AUC	P-R
50%:50%	92.10%	99.78%	93.79%	0.89	0.96
60%:40%	92.98%	99.52%	94.00%	0.89	0.96
70%:30%	92.90%	99.44%	94.00%	0.89	0.97
80%:20%	92.18%	99.50%	93.62%	0.89	0.96
90%:10%	93.51%	98.42%	93.83%	0.9	0.97

7 Conclusion and Future Work

This study aims to achieve universal, accurate, and comprehensive anomaly detection in the IoT environment. From the perspective of device interaction behavior, a method for IoT anomaly traffic detection is proposed. By analyzing the manifestation of device interaction processes in network communication, a comprehensive representation of device interaction behavior is developed based on time and space attributes at four levels: packet, flow, session, and host. Subsequently, specific learning and modeling targeting interaction device pairs are conducted to construct an integrated anomaly detection model, achieving comprehensive anomaly detection. The propose method is evaluated using the BoT-IoT dataset, demonstrating its effectiveness and superiority. Considering the method's real-world application, the challenge of rapidly and automatically modeling for newly introduced devices becomes a focal point for future research.

References

1. Koroniotis, N., Moustafa, N., Sitnikova, E., Turnbull, B.: Towards the development of realistic botnet dataset in the internet of things for network forensic analysis: Bot-IoT dataset. Futur. Gener. Comput. Syst. **100**, 779–796 (2019). https://doi.org/10.1016/j.future.2019.05.041
2. Deorankar, A.V., Thakare, S.S.: Survey on anomaly detection of (IoT)-Internet of Things cyberattacks using machine learning. In: Proceedings of the 2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC), pp. 115–117 (2020). https://doi.org/10.1109/ICCMC48092.2020.ICCMC-00023
3. Asharf, J., Moustafa, N., Khurshid, H., Debie, E., Haider, W., Wahab, A.: A review of intrusion detection systems using machine and deep learning in Internet of Things: challenges, solutions, and future directions. Electronics **9**, 1177 (2020)
4. Illy, P., Kaddoum, G., Miranda Moreira, C., Kaur, K., Garg, S.: Securing Fog-to-Things environment using intrusion detection system based on ensemble learning. In Proceedings of the 2019 IEEE Wireless Communications and Networking Conference (WCNC), pp. 1–7 (2019). https://doi.org/10.1109/WCNC.2019.8885534
5. Qiu, T., Liu, X., Zhou, X., Qu, W., Ning, Z., Chen, C.L.P.: An adaptive social spammer detection model with semi-supervised broad learning. IEEE Trans. Knowl. Data Eng. **34**, 4622–4635 (2022). https://doi.org/10.1109/TKDE.2020.3047857
6. Dutta, V., Chora's, M., Pawlicki, M., Kozik, R.: A deep learning ensemble for network anomaly and cyber-attack detection. Sensors **20** (2020). https://doi.org/10.3390/s20164583
7. Abdelmoumin, G., Rawat, D.B., Rahman, A.: On the performance of machine learning models for anomaly-based intelligent intrusion detection systems for the Internet of Things. IEEE Internet Things J. **9**, 4280–4290 (2022). https://doi.org/10.1109/JIOT.2021.3103829
8. Wang, X., Zhu, H., Ning, Z., Guo, L., Zhang, Y.: Blockchain intelligence for internet of vehicles: challenges and solutions. IEEE Commun. Surv. Tutor. (2023). https://doi.org/10.1109/COMST.2023.3305312
9. Wang, X., et al.: Toward accurate anomaly detection in industrial Internet of Things using hierarchical federated learning. IEEE Internet Things J. **9**, 7110–7119 (2022). https://doi.org/10.1109/JIOT.2021.3074382
10. Liu, Y., Kumar, N., Xiong, Z., Lim, W.Y.B., Kang, J., Niyato, D.: Communication-efficient federated learning for anomaly detection in industrial Internet of Things. In: Proceedings of the GLOBECOM 2020–2020 IEEE Global Communications Conference, pp. 1–6 (2020). https://doi.org/10.1109/GLOBECOM42002.2020.9348249

11. Thing, V.L.L.: IEEE 802.11 network anomaly detection and attack classification: a deep learning approach. In: Proceedings of the 2017 IEEE Wireless Communications and Networking Conference (WCNC), pp. 1–6 (2017). https://doi.org/10.1109/WCNC.2017.7925567
12. Doshi, R., Apthorpe, N., Feamster, N.: Machine learning DDoS detection for consumer Internet of Things devices. In: Proceedings of the 2018 IEEE Security and Privacy Workshops (SPW), pp. 29–35 (2018). https://doi.org/10.1109/SPW.2018.00013
13. Cheng, Y., Xu, Y., Zhong, H., Liu, Y.: Leveraging semisupervised hierarchical stacking temporal convolutional network for anomaly detection in IoT communication. IEEE Internet Things J. **8**, 144–155 (2021). https://doi.org/10.1109/JIOT.2020.3000771
14. Ning, Z., Dong, P., Kong, X., Xia, F.: A cooperative partial computation offloading scheme for mobile edge computing enabled Internet of Things. IEEE Internet Things J. **6**, 4804–4814 (2019). https://doi.org/10.1109/JIOT.2018.2868616
15. Wang, X., et al.: Wireless powered mobile edge computing networks: a survey. ACM Comput. Surv. (2023). https://doi.org/10.1145/3579992
16. Nie, L., Ning, Z., Wang, X., Hu, X., Cheng, J., Li, Y.: Data-driven intrusion detection for intelligent internet of vehicles: a deep convolutional neural network-based method. IEEE Trans. Netw. Sci. Eng. **7**, 2219–2230 (2020). https://doi.org/10.1109/TNSE.2020.2990984
17. Nie, L., et al.: Intrusion detection in green internet of things: a deep deterministic policy gradient-based algorithm. IEEE Trans. Green Commun. Networking **5**, 778–788 (2021). https://doi.org/10.1109/TGCN.2021.3073714