Study on Traffic Anomaly Detection of Wireless Communication Network Based on Fuzzy Relation Equation

Angran Liu[1,*] and Ying Wang[2]

[1]*School of Mathematical Science, Jiangsu Second Normal University, Nanjing, 211200, China*
[2]*School of Physics and Electronic Information, Jiangsu Second Normal University, Nanjing, 211200, China*
E-mail: liuang_ran@163.com
[*]*Corresponding Author*

Received 29 May 2024; Accepted 31 July 2024

Abstract

As the core technology of intrusion detection system, network abnormal traffic detection has always been an important research direction in academia and industry. Related studies show that the failure to find the abnormal situation in the network in time will cause incalculable damage to the computer system and even the whole network. With the emergence of large-scale lightweight terminal nodes, whose characteristics of low computing power and continuous data collection, a distributed abnormal traffic detection technology has emerged. As a kind of distributed structure with decentralized data, federated learning can not only protect local data privacy, reduce communication overhead, but also achieve the effect of centralized training, However, in the era of the Internet of Things with heterogeneous network integration and regular access of massive terminals, the network traffic distribution of different devices is differentiated due to the different security needs of diversified terminals. This will lead to the traditional federated learning-based network anomaly traffic detection facing two major challenges, the uneven

Journal of Cyber Security and Mobility, Vol. 13_6, 1305–1330.
doi: 10.13052/jcsm2245-1439.1364

data distribution leads to the model training cannot be optimized, and the distributed training global model is not suitable for local network anomaly traffic detection. The scheme of this paper showed significant advantages in the performance evaluation of backbone and mission UAVs, achieving an accuracy of 92.47% and 93.01%, respectively. In contrast, the accuracy of the traditional federated learning method is 89.87% and 89.11%, respectively, which is slightly lower than the present scheme. We propose a framework and algorithm for network anomalous traffic detection based on cluster federated learning. Taking the Internet of Vehicles as the background, the security requirements of the devices connected to the Internet of Vehicles are analyzed, and a set of federated learning data sets meeting the distribution of network traffic in practical applications are constructed with the field recognized data set KDDCup99. This paper verifies the excellent performance of the network anomaly traffic detection mechanism based on cluster federated learning in the case of heterogeneous data distribution.

Keywords: Fuzzy relation equation, wireless communication, network traffic, anomaly detection, cluster federation learning.

1 Introduction

The impact of cyber-attacks is getting worse and worse, seriously threatening social stability and the development of national politics, economy and culture. Nowadays, the Internet is faced with abnormal situations such as network hacker attacks, network equipment failures, and abuse of network users. Take attacks as an example, common ways include denial of service attacks, detection attacks, and worm attacks. These attacks will cause the waste of network resources, reduce the communication performance between the host machine, and seriously threaten the personal safety and social order of network users and even cause national economic losses [1, 2]. In 2014, more than 30% of the intelligent electricity meters in Spain's three largest power supply companies were found to have security risks. Hackers could carry out electricity fraud through technical means, and they could directly cut off the power supply system. In 2016, a historic DDos attack on the Internet of Things occurred on the East Coast of the United States, suspending the service of [3, 4] to several Internet companies in the United States, including Twitter and Amazon. Most of the botnets that launch the DDos attacks are smart webcams. In November 2018, Amazon released their latest research and found 13 security vulnerabilities in the FreeRTOS operating system. In these security vulnerabilities [5], attackers can gain control of the device remotely through attacks such as buffer overflow. The number of vulnerabilities related to general iot smart devices included in the course of that year increased by 28% [6] compared to the previous year. The network security vulnerabilities existing in the smart devices of the Internet of Things will lead to the leakage of device data and users' personal privacy information, device failure, virus infection, and become puppet machines that invade and destroy other devices in the same network.

The network abnormal traffic detection technology has received wide attention. Abnormal traffic detection system mainly detects abnormal behavior through technical means modeling, finds abnormal traffic, that is, sends a warning to the network manager [7, 8]. The traditional network abnormality detection technology has serious human intervention, low degree of automation, and cannot solve the problem of complex abnormality type. Machine learning uses massive data to train the model parameters to effectively solve the above problems. By collecting the flow information in the network, processing and constructing the data sets, and selecting an appropriate model for centralized training, the trained model is finally used to detect the abnormal flow rate [9]. Traffic detection based on machine learning needs the support of massive data, but the current situation is that data sources are scattered, especially in the large-scale distributed environment, the emergence of data islands greatly improves the difficulty of model training [10]. At the same time, massive user data is collected and applied to model training, which also causes people's concerns about data privacy and security issues. To solve the above problems, Google proposed a federated learning architecture, which can protect user privacy and realize the joint model training [11, 12] in a distributed environment. The architecture provides a new research idea for the development of anomalous traffic detection in the distributed network. The distributed nodes participating in the training can complete the global model training by uploading the gradient information to the aggregation server through the local model training, without uploading the local original data [13]. In order to obtain other participants of the local abnormal traffic data contribution to the model, each participant using the local data after the local training rounds, will send the parameters related to the model to the central node server, server after aggregation calculation, the aggregation updated model to the client involved in the next round of iteration model update [14]. The series of advantages make the rapid development of network abnormal traffic detection technology based on federated learning. With the improvement of the computing power of the computer equipment, the equipment undertakes the local training task, which greatly reduces the requirement of the computing power of the central server [15].

As one of the core technologies for interacting with the real world, the Internet of Things can collect massive data from the real world and combine it with artificial intelligence technology. However, due to the low computing power and low power consumption, high security protection technology is vulnerable to attacks; meanwhile, different iot devices belong to different organizations, so privacy protection is extremely urgent [16]. Smart devices in different fields were different. Iqbal et al analyzed the differentiated security requirements of devices in different application fields of the Internet of Things. From the attacker's point of view, the different types of attack on iot devices vary significantly. In particular, in the aspect of network abnormal traffic detection, the abnormal traffic data of Internet of Things devices will be evenly distributed [17]. The training and aggregation of the network anomaly traffic detection model based on traditional federated learning will produce secondary optimization results, and the detection accuracy will fluctuate greatly due to the different directions of gradient optimization used in the local model training. In addition, the global model issued by the central server of traditional federated learning cannot adapt to the differentiated security requirements [18] of abnormal detection of massive Internet of Things devices in the global environment. The core research content of this paper is to provide personalized network abnormal traffic detection through clustering federal learning. In order to effectively deal with the security threats of the Internet itself and the attack means derived from the Internet of Things, it is necessary to carry out effective network dynamic management of network traffic, accurately understand the operation of the network, monitor the network performance, ensure the quality of network service, and meet the needs of the majority of users [19]. T whether the flow data is normal is the primary measure, mainly through technical means to detect and judge, and then find abnormal behavior. Network anomaly traffic detection is an important defense technology, which has an irreplaceable position in [20].

2 Related Theory of Traffic Anomaly Detection in Wireless Communication Network

2.1 Network Abnormal Traffic Detection

In order to effectively deal with the security threats of the Internet itself and the attack means derived from the Internet of Things, it is necessary to carry out effective network dynamic management of network traffic, accurately understand the network operation, as shown in formula (1), monitor the network performance, ensure the quality of network service, and meet the needs of the majority of users.

$$a_{i,j} = \frac{\langle \nabla r_i(w^*), \nabla r_j(w^*) \rangle}{\|\nabla r_i(w^*)\| \|\nabla r_j(w^*)\|} = \frac{\langle \nabla R_{g(i)}(w^*), \nabla R_{g(j)}(w^*) \rangle}{\|\nabla R_{g(i)}(w^*)\| \|R_{g(j)}(w^*)\|} \tag{1}$$

Network abnormal traffic detection mainly detects the behavior, he abnormal notification will be sent to the system. It is the primary measure to judge whether the flow data is normal. As shown in formula (2), it is mainly to detect and judge by technical means, and then find abnormal behavior.

$$a_{i,j} = \frac{\langle \Delta w_r^i, \Delta w_r^j \rangle}{\|\Delta w_r^i\| \|\Delta w_r^j\|} \tag{2}$$

Network anomaly traffic detection is an important defense technology, with an irreplaceable status. In order to effectively deal with the security threats of the Internet itself and the attack means derived from the Internet of Things, it is necessary to carry out effective network dynamic management of network traffic, accurately understand the network operation, as shown in formula (3), monitor the network performance, ensure the quality of network service, and meet the needs of the majority of users.

$$\Delta w_{r+1}^i = w_r^i - w_r \tag{3}$$

The abnormal notification will be sent to the system. It is the primary measure to judge whether the flow data is normal, mainly through detection and judgment by technical means, as shown in Equation (4), and then find abnormal behavior. Network anomaly traffic detection is an important defense technology, with an irreplaceable status.

$$w_{r+1} = w_r + \sum_{i=1}^{M} \frac{|D_i|}{|D|} \Delta w_{r+1}^i \tag{4}$$

In order to effectively deal with the security threats of the Internet itself and the attack means derived from the Internet of Things, it is necessary to carry out effective network dynamic management of network traffic, as shown in formula (5), to accurately understand the network operation, monitor the network performance, ensure the quality of network service, and meet the needs of the majority of users.

$$\Delta \overline{w}_g = \left\| \frac{1}{|g|} \sum_{i \in g} \Delta w_i \right\| \tag{5}$$

Network abnormal traffic detection mainly detects the abnormal notification will be sent to the system. As shown in formula (6), it is the primary measure to judge whether the flow data is normal, mainly to detect and judge by technical means, and then find abnormal behavior. Network anomaly traffic detection is an important defense technology, with an irreplaceable status.

$$a_{i,j} = \frac{\langle \Delta w_r^i, \Delta w_r^j \rangle}{\|\Delta w_r^i\| \|\Delta w_r^j\|} \tag{6}$$

2.2 Convolutional Neural Network

Aggating related streams together can generate this information, as shown in Equation (7), called traffic mode data.

$$x' = \frac{x - min(x)}{max(x) - min(x)} \tag{7}$$

Defines the stream header as a collection of packets in each transmission protocol, the stream head detects streams with large search packets and traffic size to identify pan-torrent. For example, if the number of ICMP messages is large, as shown in Equation (8) and the flow is large, it is judged as ICMP flood. In addition, there are some special traffic patterns generated during the attack.

$$x^* = \frac{x - \mu}{\sigma} \tag{8}$$

To detect such attacks, these patterns were characterized by the flow parameters, depending on the flow rate. The TCPSYNFlood, for example, triggers a lot of streaming activity because it sends a lot of packets to a victim's particular port. Moreover, the SYN message sent by each traffic is small, as shown in Equation (9), the total number and total length of the message are messages sent. The statistics-based anomalous flow detection method mainly analyzes the change of flow data through the accumulation of time.

$$Acc = \frac{TP + TN}{TP + FP + TN + FN} \tag{9}$$

It uses statistical technical means to present the changes of statistical characteristics of flow and detect abnormal flow. An hmm-based abnormality detection method is introduced. As shown in Equation (10), the main task of the offline training module is to train the HMM model for each normal event. For each normal event, a network stream of length 3–10 s was selected as the training set. In the most convolutional neural network, the most basic and the most core is the convolutional layer, which is the main layer of the computation quantity of the whole model.

$$F_1 = 2 \times \frac{P \times R}{P + R} \tag{10}$$

The parameters of the convolutional layer are composed of some filters, and the performance of the filter in the dimensions composed of height and width is relatively small, as shown in Equation (11), but the depth of the filter must follow the dimension of the input, and we can view the filter as a two-dimensional matrix composed of numbers. The neurons in layer n + 1 are only connected to the three adjacent neurons in layer n, and the same is true in layer n + 2.

$$A = \frac{\mu_A(x1)}{X1} + \frac{\mu_A(x2)}{X2} + \cdots + \frac{\mu_A(xn)}{Xn} = \sum_{i=i}^{n} \frac{\mu_A(xi)}{Xi} \tag{11}$$

A pooling layer is often added after each convolution layer. Pooling the input features and compress them. By reducing the dimension of the feature, as shown in Equation (12), the number of weight parameters of the next layer is greatly reduced. Another is translation invariance, that is, when the data is shifted at adjacent positions, the output remains unchanged after processing through the pooling layer.

$$A = \int A \frac{\mu_A(x)}{x} x \in U \tag{12}$$

3 Network Anomaly Traffic Detection Mechanism Based on the Fuzzy Relation Equation

3.1 Overall Design of Network Anomaly Traffic Detection Based on Fuzzy Relation Equation

Unmanned aircraft is an emerging technology that has attracted many applications, such as smart cities, border monitoring, traffic monitoring, safety, natural disaster monitoring, real-time target tracking, and transportation. A complete UAV system consists of satellites, drones, data links, and ground terminals. The satellite sends GPS signals to the drone for positioning, and at least four satellites [21, 22] are needed for accurate positioning. At present, the mainstream communication between drones and ground terminals is WiFi or radio. WiFi has a very short communication distance, usually only a few hundred meters. Radio communication is long and can reach thousands of meters. Drones are usually composed of power systems, control systems, different sensors, and communication modules. The power system powers the entire UAV, especially the rotors, with one or more batteries, and sufficient energy is a prerequisite for flight [23, 24]. The control system can change the flight attitude by controlling the rotation of the rotor by command. When remotely controlled, ground facilities and drones establish communication channels. The miniature aircraft link MAVLink is one of the most widely used communication protocols, [25, 26]. Table 1 shows the comparison table of three methods, MAVLink is dedicated to full duplex data exchange between driverless system and ground terminal. MAVLink Is also used to connect to drones over the Internet. MAVLink Is used by several autonomous driving systems, such as the Ardupilot and the PX4. The Ardupilot and PX4 are the leading open-source autopilot systems designed to control any type of unmanned vehicle, including fixed-wing aircraft, as well as a variety of rotor platforms, namely single, three, four, six, eight helicopters, and even submarine [27, 28].

The MAVLink protocol is a variable-size protocol. The minimum message length of MAVLink1.0 message is 8 bytes, header flag bit, packet length, packet serial number, system number, component number, message number, and check code. As drones become increasingly used in the military and civilian fields, they carry sensitive and secure information that can be sniffing out by attackers. In fact, the MAVLink1.0 protocol does not provide any form of security and is easily cracked. There is no confidentiality, and there is no authentication mechanism. Ground terminals communicate with the UAV for [29, 30] through unauthenticated and encrypted channels. As long as the device with the signal transmission capability can easily simulate the drone. Similarly, once the middleman attack is realized, then the malicious node can also act as a ground terminal to send false messages at will. In addition, because messages are not encrypted when sent, MAVLink message flow is easy to be intercepted and eavesdropping by hackers. At the beginning of the design, multi-task federated learning design was to provide each participant with a model suitable for their own local data distribution. However, in the

Table 1 Comparison table of the three methods

Characteristic	Smith et al.	Ghosh et al.	And Sattler et al.
Applicable with arbitrary nonconvex objective functions	×	×	✓
No modifications to the federated learning architecture are required	×	✓	✓
The Client has no additional computational overhead	–	✓	✓
Cluster members do not need to confirm in advance	v	×	✓
Cluster quality, supported by the theory	-	✓	✓
It can be achieved through regulated privacy protection	–	–	✓
Clustering was performed only when necessary	×	×	✓
Can deal with the number of changing client groups	–	–	✓

regular federated learning, the central server treats all participants equally and trains a global model together. It is obviously not suitable for multi-task federal learning. Many researchers have tried to achieve the purpose of multi-task federated learning by applying different methods in computer science to federated learning, combining different clustering algorithms in different steps of training, thus achieving the purpose of multi-task. In order to group all the participants mentioned above, there are two problems to be solved. As a central server, it will not obtain the local data and data distribution of each participant.

How the central server groups the participants. The only information available to the central server is the model update parameters uploaded by the participants to the central server after the end of each local training session. Figure 1 is the Aircrack-ng crack code map. In the calculation process, the gradient of the error function is calculated in the way of error back propagation. In the federated learning, when the participants continue to optimize the training model with the local data after receiving the central server and sending it to the global model, due to the different local data of the participants, the gradient optimization direction is also different during the training optimization.

Clustering of federated learning opening conditions. In traditional federated learning, the stable solution of the overall goal of federated learning optimization is also a stable solution on the local data of each client. However

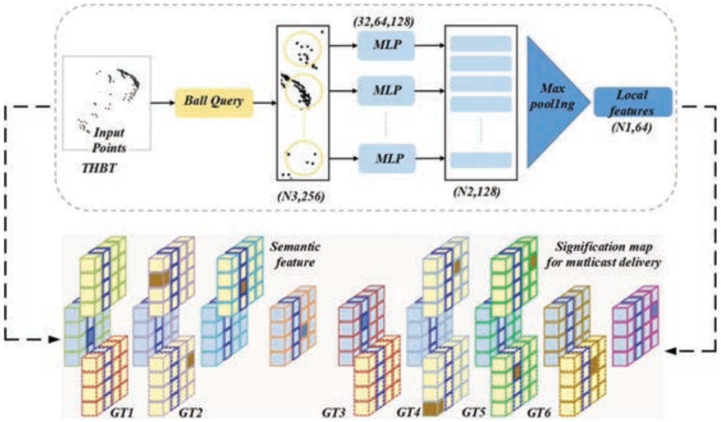

Figure 1 Aircrack-Ng crack password diagram.

in the real world, since each client corresponds to a specific user, a specific geographical location, and/or a specific time window. This taxonomy closely maps to the concept of the data set. There are differences between the data distribution for each client. So obviously in the real world, the independent with the distribution of data into traditional federal learning, federal learning the overall global optimization target stable solution is not stable when all the client local data, so when the data distribution, differences, traditional federal learning model training accuracy optimization limited even negative optimization. Therefore, after multiple rounds of federated learning, the global model was optimized, and the mean value of the model increment sent by all participants to the central server dropped below a certain threshold, and the overall optimization goal of the whole federated learning was actually getting closer and closer to the maximum value. However, the influence of uneven data distribution and existence difference results in the maximum increment of all participating clients that is still above a certain threshold. At this time, when the overall global optimization goal of federated learning approaches to the stable solution, some client local optimization goals have not reached the approximation degree of the overall optimization goal, indicating that cluster federated learning is needed at this time.

3.2 Network Security Requirements Analysis and Data Set Construction

In addition, different IoT devices belong to different organizations. In order to maintain the privacy and security of their own devices and meet the requirements of the country, the network abnormal traffic detection system of IoT devices needs to use federal learning technology. Therefore, this paper first applies the above cluster federal learning to network abnormal traffic monitoring. The entire federated learning structure is composed of one server and several clients. In this article, a server refers to a server with strong computing power and trust, such as a remote cloud server, and a client refers to a device connected to the network. On the premise of protecting the privacy of client data, all non-independently distributed data are used to train personalized models for different cluster customers in the way of collaborative learning. The whole architecture is shown in Fig, divided into two stages, the first stage cluster federated learning setting is similar to the traditional federated learning setting. As a distributed training framework, the basic idea of federated learning is model movement and data mobility. Model movement means that in each round of communication r, the server will distribute the current global model parameters wr to each client, and get the local model parameters after client training. Each client i trains the model and the global model with its local data to calculate the difference between the client model and the global model. In the second stage, we want to solve the problem is to correctly classify it without knowing the specific traffic data and traffic data distribution of the client network device. The central server can interact with all the network devices, and the nodes that undertake the task of model parameter aggregation in federated learning. The central server controls the local model trained by all the network devices with their own private data. The client obtains the minimum value of the loss function by the gradient descent pairs of multiple iterations. The convergence direction is different in each client optimization process, with the cosine similarity of the convergence direction of client i and client j. In the second stage, we want to solve the problem is to correctly classify it without knowing the specific traffic data and traffic data distribution of the client network device. The central server can interact with all the network devices, and the nodes that undertake the task of model parameter aggregation in federated learning. The central server controls the local model trained by all the network devices with their own private data. The client obtains the minimum value of the loss function by the gradient descent pairs of multiple iterations. The convergence direction of each client in the optimization process is different. The cosine similarity of the convergence direction of client i and client j: Internet of Things, Figure 2 is the analysis diagram of network security requirements, which is conceived as a global network of machines and devices that can interact with each other. As one of the most important fields of computer technology at the

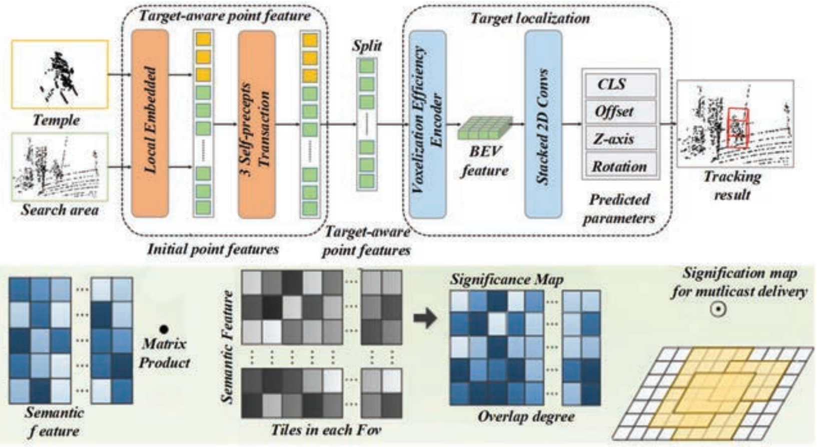

Figure 2 Network security requirements analysis diagram.

present stage, the Internet of Things devices are being applied in various industries. Internet of Things devices have the characteristics of multi-source heterogeneity, not only because they are applied in different industries, but also different in the tasks of Internet of Things devices within the industry. From the perspective of security requirements, the security requirements of the Internet of Things devices that undertake different tasks within the same application field are also different.

Usability refers to the ability of the device to use the network communication resources, that is, the device authorized to access the network or the user can use the network communication according to their own needs. Simply put, when the authorized access node uses the network, it must be guaranteed that the network system can serve the node. Confidentiality means that the information transmitted in the network will not be obtained and used by illegal devices or users. Most of this information is confidential, not limited to the national level but also to corporate structure, social groups and personal privacy. When this information is involved, the authorization node naturally requires the network to be confidential. Usually, the realization of network confidentiality is to transfer the confidential information to be transmitted through encryption and then transmitted through the network. Integrity means that the data transmitted in the network cannot change the data content format and carry the payload without authorization. So as to ensure that the whole transmission process of information is not repaired, not to be destroyed and lost. Primary integrity also requires the correctness

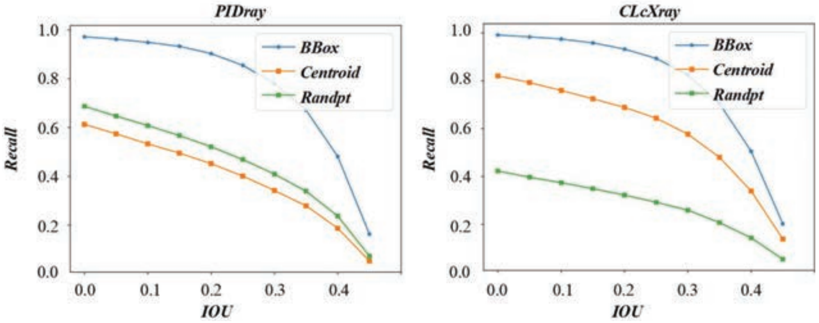

Figure 3 Comparison diagram of the loss function module increment.

and credibility of the source node of the data. Undeniability means that in the process of data transmission in the network, the real existence of all participants and the same constant, that is, all participants in communication should recognize their own behavior and guarantee at any time. Generally speaking, Figure 3 is an incremental comparison diagram of the loss function module, which means that the node that sends the data must admit that it has sent the data, and the node that accepts the data must admit that it has accepted the data. The common technical method to achieve nondeniability is to add digital signatures to the transmitted data. Reliability is one of the most basic requirements of network security. At present, the research on reliability focuses on the aspect of communication module hardware. We mainly discuss that the network abnormal traffic is more about the software level, so we do not do too much discussion here.

This paper takes from the Internet of vehicles as an example. Internet of Vehicles equipment can be divided into vehicle and on-board systems, vehicle identification systems and roadside equipment systems. Vehicle and on-board systems are vehicles connected to the Internet of vehicles and vehicles equipped with all intelligent devices that can be connected to the Internet to realize information exchange, which can be divided into vehicle sensor devices and vehicle record and storage devices. Through these physical sensor equipment, the vehicle can not only real-time understand the current position, car face direction, car after starting mileage, the current speed and acceleration of real-time information, can also be through a variety of environmental perception sensor surrounding environment changes, including outdoor temperature, outdoor humidity, the current head on light intensity, the distance between vehicles and surrounding objects, not only facilitate the driver to grasp the car and information, but also can effectively respond to external changes. In addition, the surrounding data captured by these sensors can be shared with surrounding vehicles, pedestrians and road facilities through wireless technology, uploaded to the Internet of Vehicles Center server, enhancing the sharing ability of vehicle information. However, the vehicle record storage device is equipped with a hard disk with local storage capacity, which records the image data, vehicle condition and vehicle driving route of the vehicle, and can archive the driver's driving record, and can be uploaded to the cloud for data analysis. The vehicle identification system consists of the vehicle identification equipment on the vehicle. Roadside equipment system will be laid according to the highway traffic route interval, key set-in traffic congestion, cross traffic intersection or accidents, through the collection of vehicle flow through the total, modeling different sections of the current real-time information, to car networking access vehicle transfer information safety, avoid traffic lights and avoid congestion. The vehicle sensor devices and roadside devices in the above collect their own data.

4 Design and Implementation of Anomaly Flow Detection System of Flight Control Protocol

4.1 Flight Control Protocol Traffic Dataset Construction

Yang et al. mentioned that the intrusion detection in the Internet of vehicles scenario adopts classic data sets such as KDDCup99, NSL-KDD and UNSW-NB 15. So, the most widely used famous dataset chosen for this paper is the KDDCup99 dataset. The dataset was collected by simulating the operations and multiple attacks of a typical USAF LAN, obtaining 9 weeks of TCP dump data collected and published approximately 4,900,000 single-concatenated data, each containing 41 features. And is marked as normal or attack, and is marked as a specific attack type. Making the server busy. Figure 4 is horizontal federal learning, so that the server cannot provide effective services to legitimate users. Common Dos attacks include LAN denial-of-service attacks. By constructing special SYN packets, the attacker creates an invalid empty link whose destination address is also their own IP, and continuous self-requests and replies consume network resources, resulting in the unavailability of the network. Furthermore, Makhdoom et al noted that currently emerging DDOS attacks involve 96% of IoT devices.

U2R attack, the user to the root means that the attacker himself has the permission of the ordinary account to access the system, and tries to obtain the root authority of the system through some vulnerabilities in the

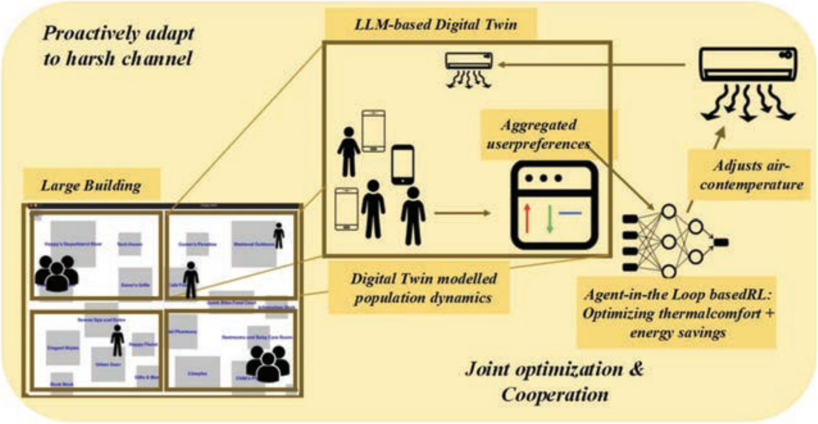
Proactively adapt to harsh channel
LLM-based Digital Twin
Aggregated userpreferences
Adjusts air-contemperature
Large Building
Digital Twin modelled population dynamics
Agent-in-the Loop basedRL: Optimizing thermalcomfort + energy savings
Joint optimization & Cooperation

Figure 4 Transverse federal learning.

Table 2 Number of five types

Type	Quantity
Normal (normal)	Article 5601
Heartbeat Bag Attack (heartbeat)	Article 7202
Parameter request attack (parameter)	Article 1207
PING attack (ping)	Article 7475
Upload Mission Attack (upload mission)	Article 461

system, that is, the permission of the developer. A common U2R attack has a buffer overflow attack, writing data beyond the maximum capacity to the running buffer. The buffer data overflows outward, destroying the stack space allocated by the operating system, and causing the running program to cross the boundaries of virtual memory to execute other instructions. Mullen et al. suggest that embedded devices in the Internet of Things are more vulnerable to attacks by using C language under resource limitations. Table 2 shows the number table of the five types of traffic, studying, implementing, testing and preventing attacks under the most popular IoT system in FreeRTOS. R2L attack: Remote to local means that the attacker himself does not have access to the target device, remote log in the target host, using the computer account and weak password login, manipulate the target device. Guess password attack, the attacker tried a large number of various possible passwords, in an attempt to obtain the account rights of legitimate users, and finally get access to the target device. Hong et al. describe three types of guessing passwords: violent, dictionary, and mixed attacks, and the time it takes to crack weak passwords.

To detect attacks, the attacker obtains the information of the attacked network through a series of technical means such as sniffing, combined with the collected information to ignore the security and defense layer of the network. Taking address scanning detection as an example, through the request response mechanism of ARP and ICMP protocol at the beginning of the design, once the attacked network segment does not set some filtering rules, the attacker will respond to its internal network address and hardware address. After analyzing the above information, the attacker can outline the topology structure of the network segment. The above attacks scan the target network to obtain key information and vulnerabilities in the network. After the above attack introduction, the Dos attack makes the server busy and the network unavailable through special means, mainly destroying the availability of the network. Probe attacks, however, are more about collecting information from the network to prepare for other types of attacks. The U2R attack exercises the system-level authority through the ordinary account, so it is possible that the attacker itself is the owner of the ordinary account, and there is also a U2R attack after the attacker obtains the permission of the ordinary account in the system through the R2L attack. Under the combination attack, the system-level secret information will be obtained by the attacker to destroy the confidentiality. So in the car networking system, after security requirements and attack means analysis, this paper assumes that the vehicle record storage equipment security demand is focused on detecting detection attack, remote to the local attack and the user to the root attack, vehicle sensor equipment more focused on detecting the denial of service attack, vehicle identification system and roadside equipment system need to detect all the above attacks. In this paper, the KDD data set is divided into five data subsets for federated learning, in which the normal traffic is equally divided into five subsets. Place traffic marked as Dos attacks into the first, second and third subsets, and put traffic marked as detection attacks, remote-to-local and user-to-root attacks into the third, fourth and fifth subsets. This simulates the network traffic of different devices in the context of the Internet of Vehicles.

4.2 Flight Control Protocol System Design

KDD data set is constructed by extracting the collected network traffic data in the real network environment. There are continuous numerical types of data, such as the number of bytes from the source host to the target host, and discrete character types of data, such as protocol types. There are three types: TCP, UDP, and ICMP. Discrete character data cannot be used directly or the model is not accurately. For discrete character data, we need to be numtized, namely these discrete character features map into numerical features. In addition, in the feature extraction process, it is inevitable to produce missing and infinite values on a single or multiple features. In the face of the above outlier data, the processing method is to directly discard. After numerical processing of discrete character characteristics and the existence of outlier data deletion, there is still a problem that is unsolved, that is the data set may differ several orders of magnitude, in order to eliminate the influence between characteristics, need to normalize the characteristics of the KDD data set, enhance the comparability of the original data. After normalization the original features.

Circles represent the two characteristic contours. The numerical span of the two features in the left figure is very large, and the contour line formed by it is very sharp. When gradient descent is used to find the minimum solution of the loss function, the optimization route lingers back and forth, resulting in multiple rounds of training to find the optimal solution. While the two original features, normalized by the right figure, map the two original features within the same range, and the contour line becomes smooth enough to converge to the minimum value fast enough when optimizing the method can quickly solve the maximum value of the objective function, the normalization is often very necessary. Loss value, in the neural network, the calculation results all reflect the difference between the prediction results and the actual results. The incremental mean of the model is reflected in the relationship between the overall optimization goal of the whole federated learning and the optimal solution. The optimization target of the whole federated learning by a single client and the optimal solution of the local data of the individual client. The smaller the value is, the better the global model of the federated learning is to the local data of the client.

This control experiment mainly records two optimization methods in the first phase of the cluster federal learning training accuracy, stochastic gradient descent method experimental results, the accuracy of cluster 1 in negative optimization dropped greatly, then accuracy continue to climb up, but before entering the second stage is still not training target is not optimized to the peak before. Adaptive moment estimation method in federal before 20 rounds of learning, although cluster 1 due to uneven distribution of data many times federal learning aggregation model global model accuracy dropped sharply, but adaptive time estimation method convergence fast, can increase accuracy in a short time to peak, so ensure that into the second stage can be better model into the second stage of training. MAVLink Protocol serves as the application

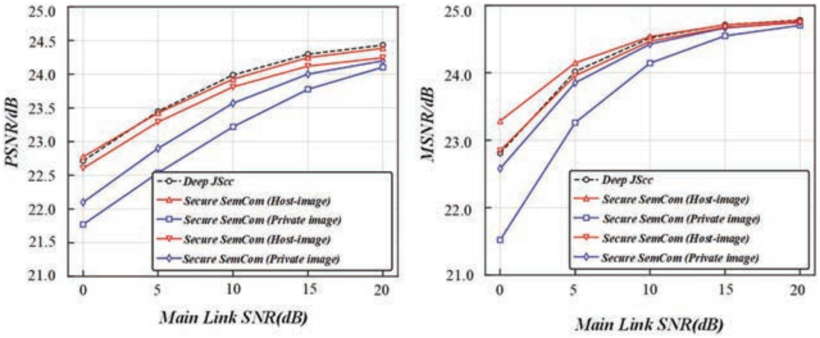

Figure 5 Schematic diagram of the maximum value pooling.

layer protocol. In order to ensure the communication rate, the designer chooses to use the UDP protocol for transmission in the transmission layer, and the data link layer is the wireless communication protocol determined according to the communication environment. This paper mainly considers the communication of UAV and terminal as WIFI. The next attack implementation is built on the premise that the data link layer is 802.1x. Figure 5 is a schematic diagram of the maximum value pooling. Heart beat packets mainly function to discover the systems connected to the network and infer when they are disconnected. If a component receives HEARTBEAT messages periodically, the component is considered connected to the network, and if it has not received many expected messages, it is considered disconnected. Additional messages from the components are handled appropriately based on the component type and other attributes. Route the messages to a system on the different interfaces. Heartbeat protocol mechanism, the components must periodically broadcast them HEARTBEAT and monitor the heartbeat from other components/systems.

Components usually post its heartbeat at 1Hz, and if no four to five heartbeat packet messages are received, another system is considered disconnected. Start reading all operations by sending a PARAM_REQUEST_LIST message. The PARAM_VALUE target component must start broadcasting the parameters separately in the message after receiving this message. The order of operation is: PARAM_REQUEST_LIST of the specified target system/component. Use the broadcast address. All of the target components should use a parameter response. Ground terminals are expected to accumulate parameters from all response systems. Timout/replay is dependent on the ground terminal. The target component should respond to sending all the parameters separately in the PARAM_VALUE message. Interruption is

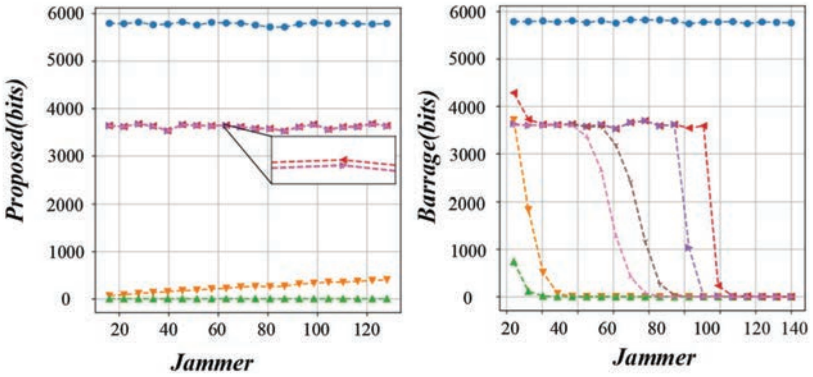

Figure 6 Schematic diagram of the maximum value pooling.

allowed between each message to avoid saturating links. Components without parameters should ignore the request. The ground terminal starts timeout after each PARAM_VALUE message to detect when parameters are no longer sent. This paper using two features of the parameter protocol designed two kinds of attack: parameter attack, due to the high parameter readability, so we simulate the ground terminal to send all the parameters request package, then the drone will send all the current all components of the parameter information, as a malicious node, will get all the information of the current drone, and the information timeliness is very high. Request a flood attack, the request message is used to query the value of the specified parameter. The ground terminal sends the requested parameters to the UAV system. Due to additional kernel missions, drones will consume more computing power. To make matters worse, drones have limited power, and high computing costs will limit the radius of their flight.

5 Experimental Analysis

The PING protocol in the fly control MAVLink is much like ICMP-based PING, in which the PING protocol enables the system to measure system delays on any connection: serial port, radio modem, UDP, etc. The PING protocol is implemented through PING messages. The message is sent with a time stamp and a serial number returned by the receiver, and therefore can be used to determine the round-trip time. Figure 6 is a schematic diagram of the maximum value pooling. Moreover, the message may be received by multiple systems, and all the PING systems should reply to a PING message.

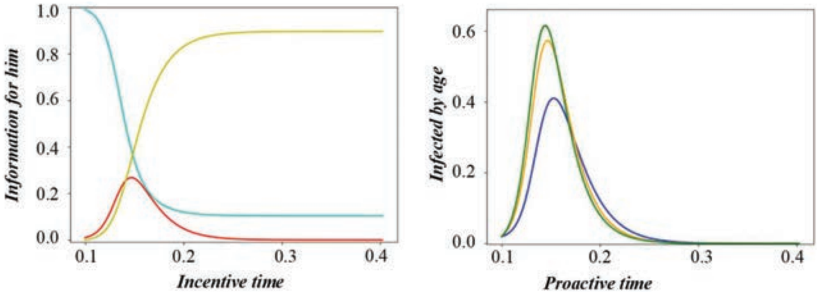

Figure 7 Schematic diagram of weight sharing.

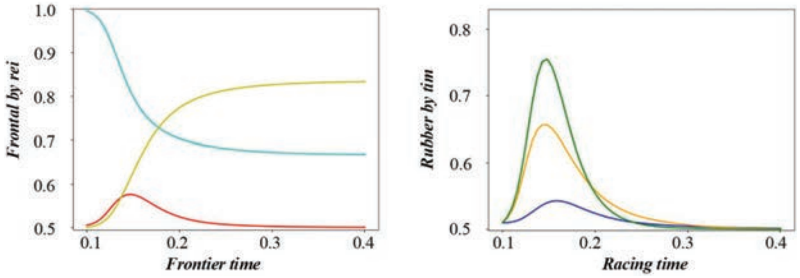

Figure 8 Schematic diagram of the local connection.

This article will also follow the classic PINGdos attack, so that the same attack effect in the network that does not support the ICMP protocol. The receiver needs to send a ping response to the other system. Figure 7 is the weight sharing diagram. If the ground terminal is forged to send a large number of PING packages to the UAV, it will occupy the UAV resources, consume the UAV power and limit the motion radius of the UAV.

According to the parameter protocol mechanism, we use the parameter request package to launch a flood attack, causing the UAV communication channel congestion with a relatively small amount of traffic. This is the change in the throughput of the UAV after we launch a parameter request attack on the 1st s. Figure 8 is the schematic diagram of local connection. It can be intuitively seen that the throughput of the UAV port has surged from about 200 to more than 2000. If the parameter request flood attack. The system integration level of uav is gradually improved, and a single uav has more and more functions.

However, due to the complex and changeable application scenarios and increasingly diverse demands, a single UAV still has great limitations in some fields due to the limited performance of its own hardware. For example,

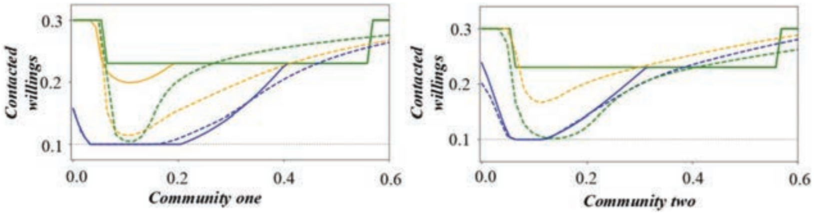

Figure 9 Schematic diagram of filling processing.

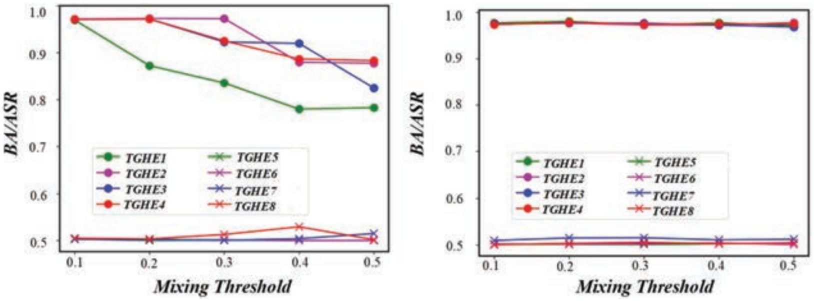

Figure 10 Schematic diagram of network abnormal traffic detection.

because considering their own size and weight, many small drones cannot carry too much power supply, which cannot guarantee a long endurance of a region. The sensors and wireless communication modules equipped by the uav, the single machine cannot achieve multi-dimensional and full coverage of the mission area. In the face of confrontational missions, a single drone is easy to be targeted, and then its own equipment failure, resulting in the interruption of the entire mission. Figure 9 shows the schematic diagram of filling processing.

The members of high-level uav network are composed of backbone uav with high computing power and long endurance in each underlying ad hoc network. In this network, Figure 10 shows the schematic diagram of the network abnormal traffic detection, and the communication between any two underlying networks does not need to flow through the ground terminal. The ground station only processes the information between the backbone UAV, which greatly reduces the calculation and communication load of the ground station. The proposed architecture realizes the basic communication architecture of the one-to-many uav operation mode.

On the other hand, the number of missions uav network is huge. The parameter information of a single mission UAV is of little significance. Since

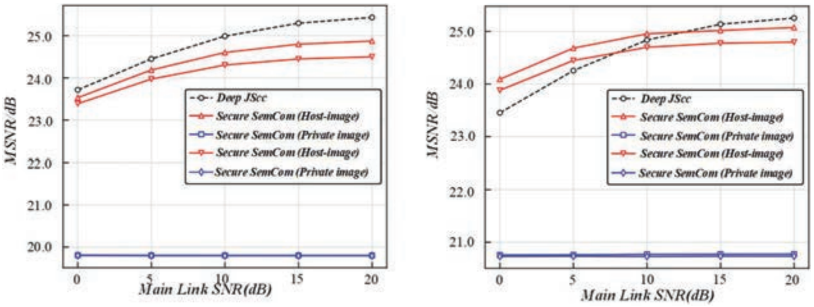

Figure 11 Schematic diagram of network abnormal flow detection.

the mission UAV is controlled by the backbone UAV, Figure 11 shows the schematic diagram of the network abnormal traffic detection. The mission UAV goes to the mission area through the uploaded flight missions. Then the attacker initiates zero task upload attack and false task upload attack will directly affect the whole task execution efficiency. There is also the common problem of UAV, which is, the endurance time of UAV is limited. If the attacker initiates PING flooding and parameter flooding, the flight radius of the mission UAV will be greatly reduced.

6 Conclusion

Since the devices in the Internet of Things come from different institutions and assume different responsibilities in devices are also different. In the case of uneven distribution of abnormal network traffic types, the model training under the traditional federated learning architecture will not bring about optimization or even cause negative optimization. Therefore, a clustered federated learning architecture is introduced to solve the negative optimization problem caused by uneven data distribution. The research on network anomaly traffic detection mechanism based on multi-task clustering federation learning is as follows, introducing clustering anomaly learning architecture to propose the detection framework and algorithm for network anomaly traffic; using KDDCup99 data set to simulate network traffic in specific Internet of vehicles scenarios. Comparing the effects of traditional federal learning and cluster federal learning; based on the network abnormal traffic detection scenario, the appropriate optimization function and loss function are selected through theoretical analysis and experiment, the accuracy of backbone UAV and mission UAV increases to more than 90%, which reflects the advantages of cluster federal learning in training the network abnormal traffic detection model in this scenario.

We calculated the model increment mean and the model increment maximum value by analyzing the model increment of all participants at each round of aggregation. The change and contrast of these two values reflect the matching degree of the distributed global model of the central server and the participant local data. In the given dataset, the largest data volume is 391458, while the R2L category is the smallest with only 1126. In the generalization dataset, the same DoS category was the largest with 229,853 data, while the R2L category was the smallest with only 16,189 data. Overall, the amount of data in the Normal category was large in both datasets and showed significant advantages over the other categories. Meanwhile, the Probe and R2L categories are relatively small in the 10% and generalization datasets, which may require additional attention and processing.

References

[1] Yasir Abdullah, R., Mary Posonia, A., and Barakkath Nisha, U. (2022). An Enhanced Anomaly Forecasting in Distributed Wireless Sensor Network Using Fuzzy Model. International Journal of Fuzzy Systems, 24(7), 3327–3347.

[2] Novaes, M. P., Carvalho, L. F., Lloret, J., and Proença, M. L. (2020). Long short-term memory and fuzzy logic for anomaly detection and mitigation in software-defined network environment. IEEE Access, 8, 83765–83781.

[3] Al-Obeidat, F., and El-Alfy, E. S. (2019). Hybrid multicriteria fuzzy classification of network traffic patterns, anomalies, and protocols. Personal and Ubiquitous Computing, 23(5), 777–791.

[4] Toliupa, S., Parkhomenko, I., Ziubina, R., Veselska, O., Rajba, S., and Warwas, K. (2022). Detection of abnormal traffic and network intrusions based on multiple fuzzy rules. Procedia Computer Science, 207, 44–53.

[5] Wagan, S. A., Koo, J., Siddiqui, I. F., Qureshi, N. M. F., Attique, M., and Shin, D. R. (2023). A fuzzy-based duo-secure multi-modal framework for IoMT anomaly detection. Journal of King Saud University-Computer and Information Sciences, 35(1), 131–144.

[6] Almotiri, S. H. (2021). Integrated fuzzy based computational mechanism for the selection of effective malicious traffic detection approach. IEEE Access, 9, 10751–10764.

[7] Cisar, P., and Maravic-Cisar, S. (2019). EWMA statistics and fuzzy logic in function of network anomaly detection. Facta universitatis-series: Electronics and Energetics, 32(2), 249–265.

[8] Fu, L., Zhang, W., Tan, X., and Zhu, H. (2021). An algorithm for detection of traffic attribute exceptions based on cluster algorithm in industrial internet of things. IEEE Access, 9, 53370–53378.

[9] Gu, K., Dong, X., and Jia, W. (2020). Malicious node detection scheme based on correlation of data and network topology in fog computing-based vanets. IEEE Transactions on Cloud Computing, 10(2), 1215–1232.

[10] Chen, L., Gao, S., Liu, B., Lu, Z., and Jiang, Z. (2020). FEW-NNN: A fuzzy entropy weighted natural nearest neighbor method for flow-based network traffic attack detection. China Communications, 17(5), 151–167.

[11] Fang, L., Li, Y., Liu, Z., Yin, C., Li, M., and Cao, Z. J. (2020). A practical model based on anomaly detection for protecting medical IoT control services against external attacks. IEEE Transactions on Industrial Informatics, 17(6), 4260–4269.

[12] Zhang, S. T., Lin, X. B., Wu, L., Song, Y. Q., Liao, N. D., and Liang, Z. H. (2020). Network traffic anomaly detection based on ML-ESN for power metering system. Mathematical Problems in Engineering, 2020, 1–21.

[13] Peng, Y., Tan, A., Wu, J., and Bi, Y. (2019). Hierarchical edge computing: A novel multi-source multi-dimensional data anomaly detection scheme for industrial Internet of Things. IEEE Access, 7, 111257–111270.

[14] Selvakumar, K., Karuppiah, M., SaiRamesh, L., Islam, S. H., Hassan, M. M., Fortino, G., and Choo, K. K. R. (2019). Intelligent temporal classification and fuzzy rough set-based feature selection algorithm for intrusion detection system in WSNs. Information Sciences, 497, 77–90.

[15] Hussain, B., Du, Q., and Ren, P. (2018). Semi-supervised learning based big data-driven anomaly detection in mobile wireless networks. China Communications, 15(4), 41–57.

[16] Xu, H., Han, S., Li, X., and Han, Z. (2023). Anomaly traffic detection based on communication-efficient federated learning in space-air-ground integration network. IEEE Transactions on Wireless Communications, 22(12), 9346–9360.

[17] Garg, S., and Batra, S. (2018). Fuzzified cuckoo based clustering technique for network anomaly detection. Computers & Electrical Engineering, 71, 798–817.

[18] Alzubi, O. A. (2022). A deep learning-based frechet and dirichlet model for intrusion detection in IWSN. Journal of Intelligent & Fuzzy Systems, 42(2), 873–883.

[19] Peng, H., Liu, L., Liu, J., and Lewis, J. R. (2019). Network traffic anomaly detection algorithm using mahout classifier. Journal of Intelligent & Fuzzy Systems, 37(1), 137–144.

[20] Li, Q., Meng, S., Wang, S., Zhang, J., and Hou, J. (2019). CAD: command-level anomaly detection for vehicle-road collaborative charging network. IEEE Access, 7, 34910–34924.

[21] Ali, W. A., Manasa, K. N., Bendechache, M., Fadhel Aljunaid, M., and Sandhya, P. (2020). A review of current machine learning approaches for anomaly detection in network traffic. Journal of Telecommunications and the Digital Economy, 8(4), 64–95.

[22] Arkan, A. S., and Ahmadi, M. (2021). Entropy-based anomaly detection using observation points relations in wireless sensor networks. Wireless Personal Communications, 119(2), 1783–1798.

[23] Revanesh, M., Gundal, S. S., Arunkumar, J. R., Josephson, P. J., Suhasini, S., and Devi, T. K. (2023). Artificial neural networks-based improved Levenberg–Marquardt neural network for energy efficiency and anomaly detection in WSN. Wireless Networks, 1–16.

[24] Salem, O., Alsubhi, K., Mehaoua, A., and Boutaba, R. (2020). Markov models for anomaly detection in wireless body area networks for secure health monitoring. IEEE Journal on Selected Areas in Communications, 39(2), 526–540.

[25] Safara, F., Souri, A., and Serrizadeh, M. (2020). Improved intrusion detection method for communication networks using association rule mining and artificial neural networks. IET Communications, 14(7), 1192–1197.

[26] Yang, L., Lu, Y., Yang, S. X., Zhong, Y., Guo, T., and Liang, Z. (2021). An evolutionary game-based secure clustering protocol with fuzzy trust evaluation and outlier detection for wireless sensor networks. IEEE Sensors Journal, 21(12), 13935–13947.

[27] Yaqoob, S., Hussain, A., Subhan, F., Pappalardo, G., and Awais, M. (2023). Deep learning based anomaly detection for fog-assisted iovs network. IEEE Access, 11, 19024–19038.

[28] Han, M. L., Kwak, B. I., and Kim, H. K. (2021). Event-triggered interval-based anomaly detection and attack identification methods for an in-vehicle network. IEEE Transactions on Information Forensics and Security, 16, 2941–2956.

[29] Shang, F., Zhou, D., Li, C., Ye, H., and Zhao, Y. (2019). Research on the intrusion detection model based on improved cumulative summation and evidence theory for wireless sensor network. Photonic Network Communications, 37, 212–223.

[30] Tripathi, K. N., Yadav, A. M., and Sharma, S. C. (2022). Fuzzy and deep belief network based malicious vehicle identification and trust recommendation framework in VANETs. Wireless Personal Communications, 124(3), 2475–2504.

Biographies

Angran Liu was born in 1991, male, lecturer. He received the B.S. degree and M.S. degree in numerical mathematics from Inner Mongolia University in 2011 and 2016. He received the Ph.D. degree in numerical mathematics from Nanjing Normal University in 2020. He is currently working in the school of mathematical science, Jiangsu Second Normal University. His research interest is numerical solution of partial differential equation.

Ying Wang was born in 1992, female, lecturer. She received the B.S. degree in communications engineering and the Ph.D. degree in information and communication engineering from Nanjing University of Posts and Telecommunications in 2014 and 2020, respectively. She is currently working in the School of Physics and Electronic Information, Jiangsu Second Normal University. Her research interests include wireless networks and mobile communications.