Journal on
Internet of Things

Tech Science Press

DOI: 10.32604/jiot.2022.042054
Article

Evidence-Based Federated Learning for Set-Valued Classification of Industrial IoT DDos Attack Traffic

Jiale Cheng[1] and Zilong Jin[1,2,*]

[1]School of Computer Science, Nanjing University of Information Science and Technology, Nanjing, 210044, China
[2]Jiangsu Collaborative Innovation Center of Atmospheric Environment and Equipment Technology (CICAEET), Nanjing University of Information Science and Technology, Nanjing, 210044, China

*Corresponding Author: Zilong Jin. Email: zljin@nuist.edu.cn

Received: 01 November 2022; Accepted: 17 May 2023; Published: 14 June 2023

Abstract: A novel Federated learning classifier is proposed using the Dempster-Shafer (DS) theory for the set-valued classification of industrial IoT Distributed Denial of Service (DDoS) attack traffic. The proposed classifier, referred to as the evidence-based federated learning classifier, employs convolution and pooling layers to extract high-dimensional features of Distributed Denial of Service (DDoS) traffic from the local data of private industrial clients. The characteristics obtained from the various participants are transformed into mass functions and amalgamated utilizing Dempster's rule within the DS layer, situated on the federated server. Lastly, the set value classification task of attack mode is executed in the expected utility layer. A learning strategy is proposed to update the network parameters in a joint manner according to the weight of mass function value. Experiments on DDoS traffic classification tasks in CIC-DDoS2019 datasets prove that Federated learning, DS layer, and expected utility layer is effective in enhancing the multi-class classification accuracy, especially for those DDoS mixed attack traffic.

Keywords: Federated learning; dempster-shafer (DS) theory; industrial internet of things; DDoS traffic

1 Introduction

With the rapid development of Industry 4.0, intelligent manufacturing, the Internet of Things, and the popularity of smart terminal devices, the attack risk in the industrial Internet of Things (IIoT) scenarios is becoming more and more prominent [1]. In IIoT, security vulnerabilities arise from outdated firmware on multi-source and heterogeneous devices, as well as from customized communication protocols that fail to meet evolving security requirements. Once hackers use it to carry out malicious attacks, irreparable losses and impacts will be caused [2]. Machine learning as the classification or regression method used for identifying and classifying network DDoS attacks could learn experience from past data to determine the known or unknown attacks. However, it needs the support of corresponding data or computing power [3]. The proposal of federated learning provides a new idea for solving the balance between privacy protection and machine learning model training [4]. This new technology keeps the data locally and collaboratively trains the machine learning model in a distributed manner, following the principle that the data does not move and the model moves. In the Industrial Internet of Things (IIot) environment, multi-dimensional heterogeneity, such as the diversity of intelligent terminal devices, the limitation of computing resources, and the differentiation of communication protocols, brings challenges to the aggregation of federated learning [5]. Since federated learning is based on the assumption of independent and identically distributed data to co-train machine learning models, uneven data distribution is prone to form the effect of federated training bias.

The proposed approach in this paper employs evidence-based theory and federated learning for detecting and identifying DDoS attack methods in the industrial IoT. We design a lightweight convolutional neural network model considering the limited computing resources of the devices used for industrial IoT. In addition, we consider the problem of poor training and slow convergence of the model due to the small number of samples and unbalanced categories. To get a trained model with fast convergence, low false alarm rate, and high accuracy for identifying and classifying various DDoS attacks in the network, we design the training strategy based on the weight of mass function value during the federated learning combined with the D-S theory. D-S evidence theory, also known as Dempster-Shafer theory or simply belief theory, is a mathematical framework for reasoning under uncertainty. It was developed by Arthur Dempster and Glenn Shafer in the 1960s and 1970s. At its core, D-S evidence theory is based on the idea of belief functions, which represent degrees of belief in a proposition. Unlike probability theory, which assigns a single probability to each proposition, D-S evidence theory allows for the representation of uncertain and conflicting evidence. The theory also allows for the combination of multiple pieces of evidence, even if they come from different sources or have different degrees of reliability. In D-S evidence theory, a basic belief assignment (BBA) is a function that assigns a degree of belief to every possible combination of events in a given domain. BBAs are used to represent the evidence available for a particular proposition. The combination of BBAs through a process called Dempster's rule of combination allows for the calculation of the degree of belief in a proposition given the available evidence. D-S evidence theory has applications in a variety of fields, including artificial intelligence, decision theory, and information fusion. It is particularly useful in situations where there is incomplete or conflicting information, or where the sources of information are uncertain or unreliable.

This paper is organized as follows: In Section 2, related work will be discussed. And our proposed method is introduced elaborately in Section 3. Section 4 gives the experimental results of the proposed scheme. Finally, a conclusion is given in Section 5.

2 Related Work

The attackers utilize many compromised end devices, assuming virtual IPs, proxy IPs, and launching botnets of broilers to simultaneously send a large number of requests beyond the network's carrying capacity, resulting in a massive denial of service [6]. Due to the short initiation time, the large scale of the launch, and the severe impact caused, it has become a more complex problem to solve among many network threats [7]. Essentially, DDoS is an extension of DoS attacks, which can attack both directly using distributed devices and broilers on the IoT to attack the target system [8].

DDoS attacks have become one of the most significant security threats to the Internet. Traditional defense mechanisms, such as intrusion detection systems (IDS) and intrusion prevention systems (IPS), rely on signature-based methods to identify and block attacks [9]. However, these methods are often ineffective against new or unknown attacks, which are constantly evolving and becoming more sophisticated. Therefore, it is necessary to develop more advanced and adaptive detection mechanisms to counter DDoS attacks. In recent years, machine learning and deep learning techniques have been widely applied to DDoS attack detection and have shown promising results [10].

The machine learning techniques for regression and classification tasks are playing an increasingly important role in intrusion detection for network security, especially in the classification of DDoS attacks. Numerous approaches have been suggested to identify and avert intrusions in various types of networks such as in IoT networks [11,12], sensor networks [13], and industrial control systems [14,15]. The literature [11] offers a context-based system to automatically detect abnormal behavior of IoT platforms. The literature [12] implements an intrusion detection system for protecting IoT networks from known attacks, which applies existing intrusion detection techniques to IoT-specific protocols such as 6LoWPAN. In [13], to detect anomalies in the data collected from wireless sensor networks, a distributed algorithm is proposed. This algorithm utilizes hyperspherical clusters for data clustering. The article [14] aims to overcome the risk of overloading legacy devices by employing a two-pronged approach comprising passive network monitoring and targeted active monitoring, which focuses on attack vectors that are specific to ICS environments. The article [15] proposes to model the bit sequence of communication packets as a language using natural language processing techniques to identify attack patterns. According to the literature [16], a signature-based technique that employs network traffic density features is suggested for identifying well-known DDoS attacks. This system only targets specific vulnerabilities present in Samsung's IoT platform SmartThings. The analysis of DDoS attacks through network traffic information has been studied for a long time. Existing approaches typically detect intrusions or identify services under attack by analyzing individual network packets [17] or clustering a large number of network packets [18]. The authors of [19] train a finite state automaton using the bit sequences of communication packets. Long short-term memory (LSTM) networks are commonly used in applications to identify anomalies in time sequences [20] or system logs [21]. Another study [22] proposes using deep belief networks to analyze DNS log data for identifying infections in enterprise networks. In [23], KNN and CNN models were employed to identify particular types of DDoS attacks within a given network environment. This test is very accurate but not universally applicable. The DCNN architecture was utilized to detect all types of malicious traffic, such as port scans, DoS, and DDoS, even in the presence of multiple malicious activities, but no specific classification of malicious traffic was made [24]. The literature [25] tested various deep learning models, optimizing the number of nodes, layers, and some hyperparameters of the network, and optimizing the input features by a sparsity penalty to obtain the AE-DNN model with lower complexity. Although it is capable of detecting different types of malicious traffic, the AE-DNN model lacks the ability to classify mixed attack traffic. The study presented in [26] employed machine learning algorithms to classify DDoS attacks based on three different protocols. The authors then proposed an effective mitigation scheme to demonstrate how DDoS classification can aid in the development of subsequent defense strategies. These models relied on a centralized training approach, which poses significant challenges in terms of data collection and privacy protection, making it difficult to deploy in practice. Reference [27] proposed a cloud intrusion detection scheme based on blockchain federated learning to protect users' data privacy. However, an advanced network architecture was not used to achieve a more fine-grained classification of DDoS attacks. Set-valued classification is a type of machine learning technique used for the detection of DDoS attacks. In set-valued classification, the objective is to classify an incoming network traffic data sample into one or more possible attack categories. This is different from traditional binary classification methods, which only classify a sample as either normal or attack. Set-valued classification for DDoS attack detection involves identifying the types of attacks that are present in a mixed attack traffic, where multiple types of attacks occur simultaneously. This can be challenging, as the mixed traffic data may have high variability and the attack patterns may be complex and dynamic. To address this challenge, set-valued classification methods utilize advanced machine learning algorithms, such as deep learning and ensemble learning, to identify patterns and correlations in the data. The approach typically involves training multiple models on different subsets of the data, which are then combined to make a final decision.

3 Proposed Methods

The current deep learning for DDoS attack classification in IoT has high accuracy for binary classification, while the multi-classification task for specific categories of DDoS attacks performs poorly for some mixed attack methods due to the increasing complexity and diversity of DDoS attack methods. A novel Federated learning classifier is proposed by leveraging the combination of D-S theory and federated learning to classify packets captured from heterogeneous devices in industrial IoT and perform set-value classification of DDoS attack methods. When the uncertainty is too high for precise categorization into a certain category, it is categorized into a subset of the known set of the full category. And its trust level is quantified using the D-S evidence theory approach.

We introduce D-S evidence theory in the process of federated learning to co-train convolutional neural network models for classifying DDoS attack methods as shown in Fig. 1. The deep neural network uses CNNs to extract more complex features from the raw data for importing into a distance-based D-S evidence theory layer to construct a quality function. In the context of federated learning, the quality function plays a crucial role in evaluating the expected utility. The evaluated utility is then uploaded and downloaded among the participating devices to improve the overall model performance. In addition, the strategy we put forward is to consider only specific subsets of categories rather than the complete set of classes. Finally, the datasets of CIC-DDoS2019 are used to demonstrate and discuss the classifier's effectiveness and decision strategy. The primary contribution of this study is to propose that adding a D-S layer to the federated learning process, CNNs can enhance set-valued classification and detection of new hybrid attack methods while maintaining good performance.

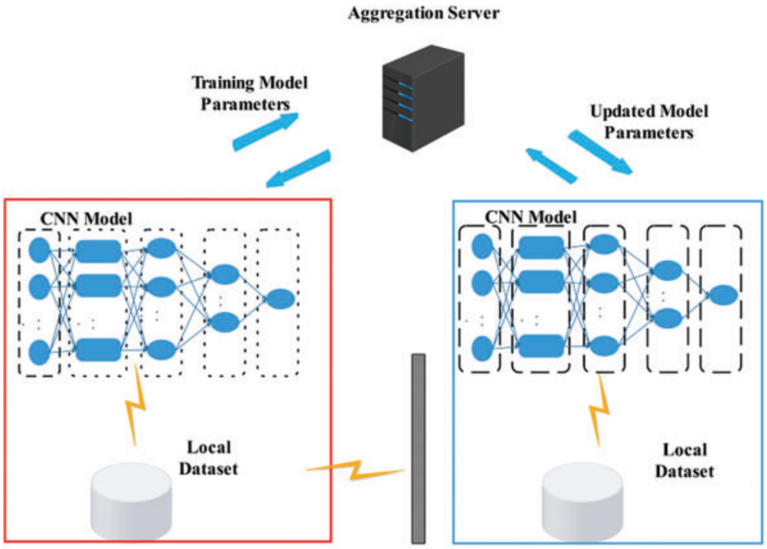

Figure 1: Architecture diagram of DDoS attack classifier based on federated learning

3.1 D-S Theory

$\Omega = \{\omega_1, \ldots, \omega_M\}$ refers to the framework for identification. The mass function denoted as m, maps from 2^Ω to a range of [0,1] such that m(Ø) = 0.

$$\sum\nolimits_{A\subseteq\Omega} m(A) = 1 \tag{1}$$

Each subset A ⊆ Ω is assiciated with a unit trust mass function m(A), which assumes that there are true values in the state A holds, and no further trust values are assigned based on any subset of the available evidence A.

Dempster's rule [28] allows for the combination of two independent mass functions, m1 and m2, as follows:

$$(m_1 \oplus m_1)(A) = \frac{(m_1 \cap m_1)(A)}{1 - (m_1 \cap m_1)(\phi)} \tag{2a}$$

$$(m_1 \cap m_1)(\phi) = \sum\nolimits_{B\cap C=\phi} m_1(B)\, m_2(C) \tag{2b}$$

For decisions with trust functions, define the upper and lower bounds of the expected effectiveness function [29] for the selection of ω_i as

$$\overline{E_m}\left(f_{\omega_i}\right) = \sum\nolimits_{B\subseteq\Omega} m(B) \max_{\omega_j\in B} u_{ij} \tag{3a}$$

$$\underline{E}_m\left(f_{\omega_i}\right) = \sum\nolimits_{B\subseteq\Omega} m(B) \min_{\omega_j\in B} u_{ij} \tag{3b}$$

When considering the state as ω_j, the expected payoff of selecting ω_i is represented u_{ij}. f_{ω_i} stands for the action of choosing ω_i. To make a caution choice, one chooses to trust the greatest lower utility, whereas a risky decision-making approach involves choosing the maximum upper bound of expected utility.

The generalized Hurwricz decision criteria model [30] describes the decision maker's attitude towards ambiguity in terms of the negative attitude index ν and provide the calculation of the utility of the following behavior f_{ω_i}

$$E_{m,\nu}\left(f_{\omega_i}\right) = \nu \underline{E}\left(f_{\omega_i}\right) + (1-\nu)\,\overline{E}\left(f_{\omega_i}\right) \tag{4}$$

Clearly, where pessimism and optimism correspond to $\nu = 1$ and $\nu = 0$, respectively.

3.2 Evidence-Based Federated Learning

The system architecture of EFLDDoS is shown in Fig. 2. Evidence-based fuzzy categorization modules are added to the original local model client and server side of federated learning. The heterogeneous devices in the industrial IoT scenario collect traffic data under DDoS attacks, use models downloaded from the cloud for local model training, and upload the resulting model structure and parameters to the cloud for aggregation, where the cloud aggregates the models from the participating parties and uses D-S theory to evaluate the trust value of the model parameters from the participating nodes during aggregation, and the higher degree of uncertainty of the model parameters are discarded or categorized as fuzzy set values for aiding decision making. A new round of federally optimized model structures and parameters are obtained and distributed down to the heterogeneous devices.

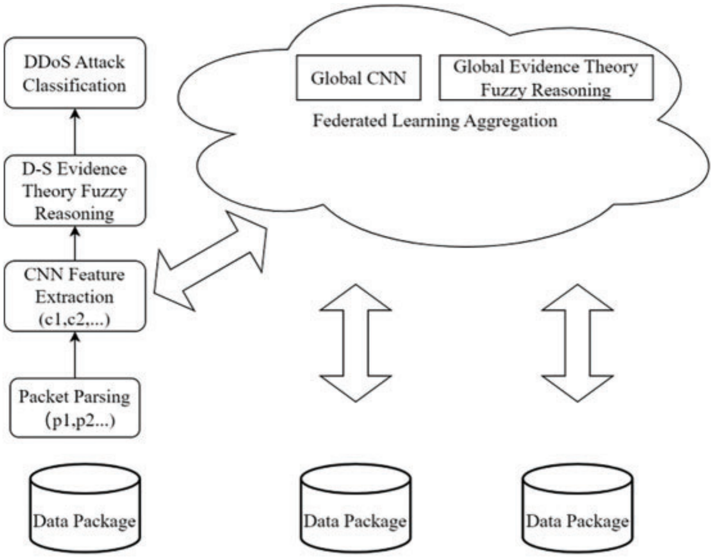
DDoS Attack Classification
D-S Evidence Theory Fuzzy Reasoning
CNN Feature Extraction (c1,c2,...)
Packet Parsing (p1,p2...)
Global CNN
Global Evidence Theory Fuzzy Reasoning
Federated Learning Aggregation
Data Package
Data Package
Data Package

Figure 2: The Framework of EFLDDoS

Based on DS evidence theory, the neural network layer utilizing distance metric is used to construct the quality function. In a neural network classifier, the proximity of the input vector to the prototype is considered evidence for the class. This evidence is transformed into a quality function and combined using Dempter's rule. Consider a training set $X = \{x_1, x_2, \ldots, x_N\} \subset R, R^P$ a set of N samples represented by P-dimensional vectors, and a prototype $\{p_1, p_2, \ldots, p_n\}$ consisting of an evidence neural network classifier. Given a sample x, the ENN utilize a quality function to quantify the uncertainty $\Omega = \{\omega_1, \ldots, \omega_m\}$ in selecting a class to classify. The three steps are defined as follows:

(1) Calculate the support between x and each reference pattern p^i as follows:

$$s^i = \alpha exp\left(-\left(\eta^i d^i\right)^2\right), i = 1, \ldots, n, \tag{5}$$

where $d^i = ||x - p^i||$ denotes the distance between x and p^i, $\alpha \in (0, 1)$, $\eta^i \in R$ represents parameters linked to p^i.

(2) Calculate the mass function as follows:

$$m^i\left(\left\{\omega_j\right\}\right) = h^i_j s^i, j = 1, \ldots, M \tag{6a}$$

$$m^i(\Omega) = 1 - s^i \tag{6b}$$

where $h^i{}_j$ is the affiliation of the prototype p^i to the category w_j, $\sum_{j=1}^{M} h^i_j = 1$, and we regard the mass function of the p^i as $m^i = (m^i(\{\omega_1\}), \ldots, m^i(\{\omega_M\}), m^i(\Omega))^T$.

(3) The n trust mass functions are aggregated according to Dempster's rule. The combined quality functions are calculated as follows: $\mu^1 = m_1$ and $\mu^i = \mu^{i-1} \cap m_i$ for $i = 2, \ldots, n$.

$$\mu^i(\{\omega_j\}) = \mu^{i-1}(\{\omega_j\})m^i(\{\omega_j\}) + \mu^{i-1}(\{\omega_j\})m^i(\{\Omega\}) + \mu^{i-1}(\Omega)m^i(\{\omega_j\}) \tag{7a}$$

for $i = 2, \ldots, n$. $j = 1, \ldots, M$. There are

$$\mu^i(\Omega) = \mu^{i-1}(\Omega)\, m^i(\Omega), i = 2, \ldots, n. \tag{7b}$$

The output vector $\mathrm{m}^i = (m(\{\omega_1\}), \ldots, m(\{\omega_M\}), m(\Omega))^T$ ultimately follows:

$$m\left(\left\{\omega_j\right\}\right) = \frac{\eta^n\left(\left\{\omega_j\right\}\right)}{\sum_{j=1}^{M}\mu^n\left(\left\{\omega_j\right\}\right) + \mu^n\left(\Omega\right)} \tag{8a}$$

$$m\left(\Omega\right) = \frac{\mu^n\left(\{\Omega\}\right)}{\sum_{j=1}^{M}\mu^n\left(\left\{\omega_j\right\}\right) + \mu^n\left(\Omega\right)} \tag{8b}$$

The evidence-based federated learning steps are as follows.

Assume that there are C participants available to participate in the federated learning process to jointly train a convolutional neural network model for identifying DDoS attack methods, where K nodes upload models to participate in a new round of model parameter updates. In this way, the machine learning model used for federated learning can be represented as

$$\min_{\omega\in R^d} f\left(\omega\right) \tag{9}$$

Here $f\left(\omega\right)$ is

$$f\left(\omega\right) = \frac{1}{n}\sum_{i=1}^{n} f_i\left(\omega\right) \tag{10}$$

where $f_i = \ell\left(x_i, y_i; \omega\right)$, (x_i, y_i) is the sample data and ω is the model parameter. If one assumes that the trust in the model parameters learned from the k local end data is differentiated, then using m_k to denote the trust quality function for the model parameters at the kth local end, the above equation can be rewritten as

$$f\left(\omega\right) = \sum_{i=1}^{K} \frac{m_k}{m} F_k\left(\omega\right) \tag{11}$$

Of which,

$$F_k\left(\omega\right) = \sum_{k=1}^{K} m_k f_k\left(\omega\right) \tag{12}$$

For federated learning, let C = 1 (which determines the batch size of each iteration in learning), and with a suitable learning rate η, $g_k = \triangledown F_k(\omega_t)$ is computed for each participant node k, where ω_t is the parameter of the local model of the side participant. The task on the server side is to collect information on these parameters and to update the model using the weighted average of the gradient g_k with the trust quality function.

$$\omega_{t+1} \leftarrow \omega_t + \eta\sum_{K=1}^{K} m_k g_k \tag{13}$$

It can also be expressed as

$$\sum_{k=1}^{K} m_k g_k = \triangledown \mathrm{f}\left(\omega\right) \tag{14}$$

Equivalents to this are $\omega_{\mathrm{t}+1}^{k} \leftarrow \omega_t + \eta g_k$, which are updated as follows

$$\omega_{t+1} \leftarrow \sum_{k=1}^{K} m_k \omega_{t+1}^{k} \tag{15}$$

This is where each edge server uses the local datasets to train the local model, and then the server side collects the individual training results uniformly and calculates the gradient average based on the weights, or it can do multiple rounds of learning locally before uploading to the server side for calculation and updating.

$$\omega^k \leftarrow \omega^k + \eta \bigtriangledown F_k\left(\omega_k\right) \tag{16}$$

Federated learning provides a privacy-preserving way to collaboratively train neural network models in a distributed manner. All participants are parsed by locally captured packets and fed into a CNN convolutional neural network to extract higher-order features of different kinds of DDoS attack patterns. The D-S layer uses the distances of these higher-order features as the basis for the assignment of the basic trust quality function and finally outputs a combination of possible DDoS attack method classes.

3.3 Evidence-Based Reasoning Effectiveness Assessment and Decision Making

The model inference and evaluation module are added to the training parameters to enhance the model's ability to classify and evaluate the effectiveness of fuzzy sets of DDoS attacks that are not easily distinguishable.

$\Omega = \{\omega_1, \ldots, \omega_M\}$ denote model parameters set categorized as i. For classification problems with only exact predictions, a behavior refers to the act of assigning an example to a single class among M available classes. F = $\{f_{\omega 1}, \ldots, f_{\omega M}\}$, where $f\omega_i$ refers the choice of belief ω_i for the basis of classification.

To facilitate decision inference, we introduce U_{M*M}, where $u_{ij} \in U_{M*M}$ represents the effect that classifies a choice belief as i while it is j. For decisions based on evidence, the selection of $f_{\omega i}$ results in utilities, including the upper and lower utilities, which are calculated as (3a) and (3b).

To handle imprecise predictions in classification problems, Ma et al. [30] proposed a method for set-valued classification under uncertainty, which assigns uncertain samples to non-empty subsets. The utility of classifying a sample as belonging to A is defined using the ordered weighted average (OWA) aggregation of the utilities of each individual class in A [31]:

$$u_{A,j} = \sum\nolimits_{k=1}^{|A|} g_k . u^A_{(k)j} \tag{17}$$

where $u^A_{(k)j}$ is the Kth largest member in A, which includes the utility values in U_{M*M}. The weights vector $g = (g_1, \ldots, g_{|A|})$ represents the degree of preference for choosing $u_{A(k)j}$ when the ENN needs an exact decision. The values of g refer to the tolerance of the model to uncertainty. The O'hagan method [32] was used to get the g in the OWA (ordered weighted average) algorithm. We define the uncertainty tolerance as

$$TDI\left(g\right) = \sum\nolimits_{k=1}^{|A|} \frac{|A| - k}{|A| - 1} g_k = \gamma \tag{18}$$

Its maximum value is 1, its minimum value is 0, and its average value is 0.5. The exact assignments are generally preferred over imprecise assignment when $\gamma < 0.5$. To calculate the weights of the OWA for a given value of γ, we can use the princple of maximum entropy.

$$ENT\left(g\right) = -\sum\nolimits_{k=1}^{|A|} g_k log\ g_k \tag{19}$$

It has to satisfy $TDI(g) = \gamma, \sum\nolimits_{k=1}^{|A|} g_k = 1$, and $g_k \geq 0$.

4 Experimental Analysis

4.1 Datasets

The CICDDoS 2019 dataset is a collection of labeled network traffic data that is designed to support research on DDoS attacks. It was created by the Canadian Institute for Cybersecurity (CIC) at the University of New Brunswick. The dataset includes both benign and malicious traffic, and covers various types of DDoS attacks, including HTTP flood, TCP SYN flood, UDP flood, and more. The data was collected using several different tools and techniques, including the Raspberry Pi-based Traffic Monitoring Framework (TMF), the CICFlowMeter flow analysis tool, and the Bro Network Security Monitor. The dataset also includes features extracted from the network traffic data, such as packet size, duration, and protocol type. The CICDDoS 2019 dataset has been used in a number of research studies on DDoS detection and mitigation, and is freely available for academic use. We validate our evidence-based federated learning fuzzy set-value classification model using the CICDDoS2019 datasets, which contain 13 different types of DDoS attack traffic and benign traffic. We selected six attack flows and benign flows for fuzzy set-value categorization experiments of mixed DDoS attack flows as shown in Table 1.

Table 1: The number of different flows in blocks

No.	Flows type/number						
	Benign	TFTP	NetBIOS	UDP	NTP	MSSQL	LDAP
Block1	20488	19947	19861	19863	19912	19910	20309
Block2	20614	19939	20004	20109	19765	19945	19822
Block3	20619	19990	19823	20005	20075	20005	19822
Block5	20506	20146	20060	20016	20278	20002	19718
Block5	20673	20158	20053	20111	20042	20241	20214
Block6	20680	19857	20179	19911	19945	19931	20102

The mixed attack traffic containing the six attack methods mentioned above has 87 IP flow-based feature data dimensions. However, we selected 75 dimensions for input into the neural network model. On the one hand, the first eight dimensions include source and target IP addresses, source, and target ports, flow IDs, protocols, and timestamps, which involve privacy information. On the other hand, we considered the model's generalization performance to avoid overfitting the model training.

4.2 Fuzzy Set Value Categorization Evaluation of DDoS Attack Methods

For the CIC-DDoS2019 datasets D, classification performance was assessed by the average effectiveness matrix for performance.

$$AU\left(D\right)=\frac{1}{|D|}\sum\nolimits_{i=1}^{D}\hat{u}_{A(i),y_i} \tag{20}$$

where y_i is the true label of sample i in the training sample and $A_{(i)}$ is the possible combinations of labels chosen for the behaviour f that maximizes the expected utility (4). $\hat{u}_{A(i),y_i}$is the average utility assigned to i to A while the real label is y_i. When single-category classification is considered, the AU criterion defined is equivalent to the classification accuracy of the single-category classification task.

4.3 Model Training and Testing Results

In this experiment, the convolutional neural network model co-trained by evidence-based federated learning had a structure as shown in Table 2. The dataset was randomly divided into different chunks as shown in Table 1, covering both benign traffic and various attacks combined in different blocks. These divided datasets were used to train the model, and Fig. 3 displays the accuracy of the process during training and testing. The results show that the trained model has a good performance in the fuzzy set-valued classification task for the attack mode of the attack traffic. Moreover, the proposed model, with a DS layer and an expected layer, outperforms probabilistic CNN classifiers for set-valued classification.

Table 2: Model structure

Layer(type)	Output shape
Conv1d(Conv1d)	(None, 75,64)
Max_pooling1d(MaxPooling1D)	(None, 37,64)
Conv1d_1(Conv1D)	(None, 22,32)
Max_pooling1d_1(MaxPooling1d_1)	(None, 11,32)
Conv1d_2(Conv1D)	(None, 9,16)
Max_pooling1d_2(MaxPooling1d_2)	(None, 4,16)
Dropout(Dropout)	(None, 64)
Flatten(Flatten)	(None, 64)
Dense(Dense)	(None, 128,7)
d_s1(DS1)	(None, 128,7)
d_s1_activate(DS1_activate)	(None, 128,7)
d_s1_omega(DS_omega)	(None, 7)
d_s1_dempster(DS3_Dempster)	(None, 7)
d_s_normalize(DS_normalize)	(None, 7)
dm_test(DM_test)	(None, 128)

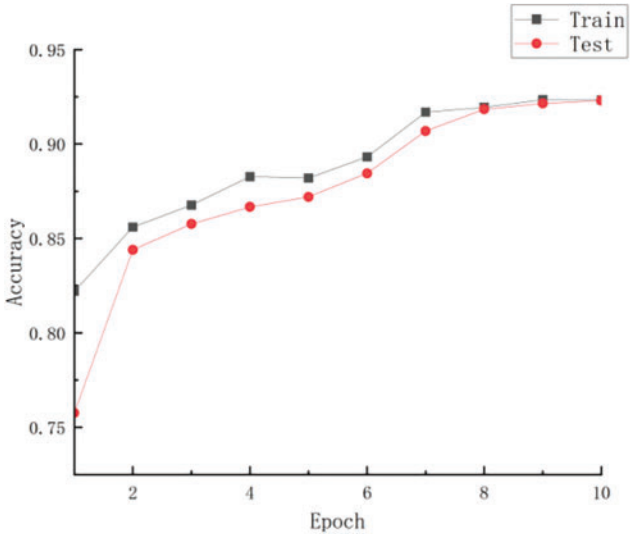

Figure 3: The accuracy of model training and test

4.4 *Set-Valued Classification*

Table 3 presents the evaluation of performance across the evidence-based federated learning scheme with and without incorporating evidence theory in multiple classifications. The experimental results show that the proposed scheme outperforms the scheme without incorporating evidence theory in terms of accuracy and efficiency for identifying multiple combinations of attacks under a mixed attack approach. This is because the proposed scheme considers all combinations of possible categories and makes set-valued assignments using an expected utility layer, which results in a more accurate and efficient classification. Therefore, the proposed scheme is more suitable for real-world scenarios where multiple types of attacks can occur simultaneously, and it can provide a more effective approach for DDoS attack detection.

Table 3: Model training results with non-iid data

	Evaluation index	EFLDDoS	FLDDoS [33]	FL
DDoS classification (Multi-class)	Accuracy	0.9230	0.8969	0.7649
	Precision	0.9325	0.9060	0.7800
	Recall	0.9146	0.8969	0.7649
	F1-score	0.9234	0.8967	0.7639

5 Conclusion

This paper presents an Evidence-based Federated learning framework for DDoS hybrid attack detection, EFLDDoS. EFLDDoS can coordinate the trusted Intelligent terminal equipment clusters to use their local data to train CNN with the D-S layer without uploading data to jointly resist the threat of DDoS hybrid attacks. It is trained through federated learning and a strategy for choosing to believe partial evidence is used to reduce computational costs. The experiential results show that EFLDDoS has higher precision, can better complete the DDoS hybrid attack detection task, protect data privacy, and save the cost of communication. Our future work is to enhance the proposed approach with a SDN environment and explore to using graph convolution network to extracts the characteristics of data from both temporal and spatial perspectives to find the attack path.

Funding Statement: This work was sponsored by the National Natural Science Foundation of China under Grant Number No. 62271264, 61972207, and 42175194, and the Project through the Priority Academic Program Development (PAPD) of Jiangsu Higher Education Institution.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] Y. Shah and S. Sengupta, “A survey on classification of cyber-attacks on IoT and IIoT devices,” in *11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conf. (UEMCON)*, Virtual, pp. 0406–0413, 2020.

[2] V. Borgiani, P. Moratori, J. F. Kazienko, E. R. R. Tubino and S. E. Quincozes, “Toward a distributed approach for detection and mitigation of denial-of-service attacks within industrial internet of things,” *IEEE Internet of Things Journal*, vol. 8, no. 6, pp. 4569–4578, 2021.

[3] R. Sommer and V. Paxson, "Outside the closed world: On using machine learning for network intrusion detection," in *2010 IEEE Symp. on Security and Privacy*, Oakland, CA, USA, pp. 305–316, 2010.

[4] H. B. Mcmahan, E. Moore, D. Ramage, S. Hampson and B. Arcas, "Communication-efficient learning of deep networks from decentralized data [C]," in *Proc. of the 20th Int. Conf. on Artificial Intelligence and Statistics (AISTATS)*, Fort Lauderdale, USA, pp. 1602.05629, 2017.

[5] D. C. Nguyen, M. Ding, P. N. Pathirana, A. Seneviratne, J. Li *et al.,* "Federated learning for industrial internet of things in future industries," *IEEE Wireless Communications Magazine*, vol. 28, no. 6, pp. 192–199, 2021.

[6] N. Agrawal and S. Tapaswi, "Defense mechanisms against DDoS attacks in a cloud computing environment: State-of-the-art and research challenges," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 4, pp. 3769–3795, 2019.

[7] A. Roohi, M. Adeel and M. A. Shah, "DDoS in IoT: A roadmap towards security & countermeasures," in *25th Int. Conf. on Automation and Computing (ICAC)*, Lancaster, UK, pp. 1–6, 2019.

[8] H. Nazrul, K. B. Dhruba and K. Jugal, "Botnet in DDoS attacks trends and challenges," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2242–2270, 2015.

[9] A. Bhardwaj, G. V. B. Subrahmanyam, V. Avasthi, H. Sastry and S. Goundar, "DDoS attacks, new DDoS taxonomy and mitigation solutions-a survey," in *Int. Conf. on Signal Processing, Communication, Power and Embedded System (SCOPES)*, Paralakhemundi, India, pp. 793–798, 2016.

[10] B. Zhang, T. Zhang and Z. Yu, "DDoS detection and prevention based on artificial intelligence techniques," in *3rd IEEE Int. Conf. on Computer and Communications (ICCC)*, Chengdu, China, pp. 1276–1280, 2017.

[11] Y. J. Jia, Q. A. Chen, S. Wang, A. Rahmati, E. Fernandes *et al.,* "ContexloT: Towards providing contextual integrity to appified IoT platforms," in *24th Annual Network & Distributed System Security Symp. (NDSS)*, California, USA, 2017.

[12] S. Raza, L. Wallgren and T. Voigt, "Svelte: Real-time intrusion detection in the internet of things," *Ad hoc Networks*, vol. 11, no. 8, pp. 2661–2674, 2013.

[13] S. Rajasegarar, C. Leckie and M. Palaniswami, "Hyperspherical cluster based distributed anomaly detection in wireless sensor networks," *Journal of Parallel and Distributed Computing*, vol. 74, no. 1, pp. 1833–1847, 2014.

[14] W. Jardine, S. Frey, B. Green and A. Rashid, "Senami: Selective non invasive active monitoring for ICS intrusion detection," in *Proc. of the 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy*, Xi'an, China, pp. 23–34, 2016.

[15] A. Kleinmann and A. Wool, "Automatic construction of state chart based anomaly detection models for multi-threaded SCADA via spectral analysis," in *Proc. of the 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy ACM*, Xi'an, China, pp. 1–12, 2016.

[16] R. Doshi, N. Apthorpe and N. Feamster, "Machine learning DDoS detection for consumer internet of things devices," in *2018 IEEE Security and Privacy Workshops (SPW)*, San Francisco, CA, USA, pp. 29–35, 2018.

[17] C. Krugel, T. Toth and E. Kirda, "Service specific anomaly detection for network intrusion detection," in *Proc. of 2002 ACM Symp. on Applied Computing*, Madrid, Spain, pp. 201–208, 2002.

[18] L. Portnoy, E. Eskin and S. Stolfo, "Intrusion detection with unlabeled data using clustering," in *Proc. of ACM CSS Workshop on Data Mining Applied to Security*, New York, USA, pp. 105–113, 2001.

[19] R. Sekar, A. Gupta, J. Frullo, T. Shanbhag, A. Tiwari *et al.,* "Specification-based anomaly detection: A New approach for detecting network intrusions," in *Proc. of the 9th ACM Conf. on Computer and Communications Security*, New York, USA, pp. 265–274, 2002.

[20] P. Malhotra, L. Vig, G. Shroff and P. Agarwal, "Long short term memory networks for anomaly detection in time series," in *Proc. of Presses Universitaires de Louvain*, Bruges, Belgium, pp. 89–96, 2015.

[21] M. Du, F. Li, G. Zheng and V. Srikumar, "DeepLoG: Anomaly detection and diagnosis from system logs through deep learning," in *Proc. of the 2017 ACM SIGSAC Conf. on Computer and Communications Security, ACM*, Dallas Texas, USA, pp. 1285–1298, 2017.

[22] A. Oprea, Z. Li, T. -F. Yen, S. H. Chin and S. Alrwais, "Detection of early-stage enterprise infection by mining large-scale Log data," "in *Dependable Systems and Networks (DSN), 2015 45th Annual IEEE/IFIP Int. Conf. on. IEEE*, Rio de Janeiro, Brazil, pp. 45–56, 2015.

[23] M. Zahid Hasan, K. M. Zubair Hasan and A. Sattar, "Burst header packet flood detection in optical burst switching network using deep learning model," *Procedia Computer Science*, vol. 143, pp. 970–977, 2018.

[24] S. Haider, A. Akhunzada, I. Mustafa, T. B. Patel, A. Fernandez *et al.,* "A deep CNN ensemble framework for efficient DDoS attack detection in software defined networks," *IEEE Access*, vol. 8, pp. 53972–53983, 2020.

[25] A. Bhardwaj, V. Mangat and R. Vig, "Hyperband tuned deep neural network with well posed stacked sparse AutoEncoder for detection of DDoS attacks in cloud," *IEEE Access*, vol. 8, pp. 181916–181929, 2020.

[26] R. Abubakar, A. Aldegheishem, M. F. Majeed, A. Mehmood, H. Maryam *et al.,*"An effective mechanism to mitigate real-time DDoS attack," *IEEE Access*, vol. 8, pp. 126215–126227, 2020.

[27] X. Hei, X. Yin, Y. Wang, J. Ren and L. Zhu, "A trusted feature aggregator federated learning for distributed malicious attack detection," *Computers & Security*, vol. 99, pp. 20–33, 2020.

[28] G. Shafer, *A mathematical theory of evidence*, Princeton: Princeton University Press, 1976.

[29] T. Denœux, "Decision-making with belief functions: A review," *International Journal of Approximate Reasoning*, vol. 109, pp. 87–110, 2019.

[30] Ma, L. and Denœux, T., "Partial classification in the belief function framework," *Knowledge-Based Systems*, vol. 214, pp. 106742, 2021.

[31] Yager, R. R., "On ordered weighted averaging aggregation operators in multicriteria decision making," *IEEE Transactions on Systems, Man, and Cybernetics*, vol. 18, pp. 183–190, 1988.

[32] O'Hagan, M., "Aggregating template or rule antecedents in real-time expert systems with fuzzy set logic," in *Twenty-Second Asilomar Conf. on Signals, Systems and Computers*, California, USA, vol. 2. pp. 681–689, 1988.

[33] D. Lv, X. Cheng, J. Zhang, W. Zhang, W. Zhao *et al.,* "DDoS attack detection based on CNN and federated learning," in *2021 Ninth Int. Conf. on Advanced Cloud and Big Data (CBD)*, Xi'an, China, pp. 236–241, 2022.