Zhihui LI, Congyuan XU, Kun DENG, Chunyuan LIU, 2025. A subspace-based few-shot intrusion detection system for the Internet of Things. *Frontiers of Information Technology & Electronic Engineering*, 26(6):862-876.
https://doi.org/10.1631/FITEE.2400556

A subspace-based few-shot intrusion detection system for the Internet of Things

Key words: Intrusion detection system; Few-shot learning; Internet of Things; Subspace

Corresponding author: Congyuan XU
E-mail: cyxu@zjxu.edu.cn
ORCID: https://orcid.org/0009-0003-7760-5980

Motivation

- In the real-world Internet of Things (IoT) environments, the diversity of IoT devices and the subsequent fragmentation of attack types result in a limited number of training samples, which urgently requires researchers to develop few-shot intrusion detection systems. In this study, we propose a subspace-based approach for few-shot IoT intrusion detection systems to cope with the dilemma of insufficient learnable samples.

Main idea

- To enhance the discriminability of traffic information from different classes, we propose a few-shot classifier that uses subspaces as a metric to fully learn the common representation of each traffic flow, while designing a four-layer feature extraction network based on channel attention mechanisms to enhance the feature representation of each traffic flow.
- We demonstrate that the proposed method performs well and has the ability to generalize unknown categories on the CICIoT2023, CICIDS2017, and CICIDS2018 datasets, which could address the capability of detecting unknown category samples under few-shot conditions.
- We consider the diversity of IoT devices and the specificity of attack patterns, along with the designed data preprocessing steps, and construct a dataset suitable for few-shot intrusion detection.

Method

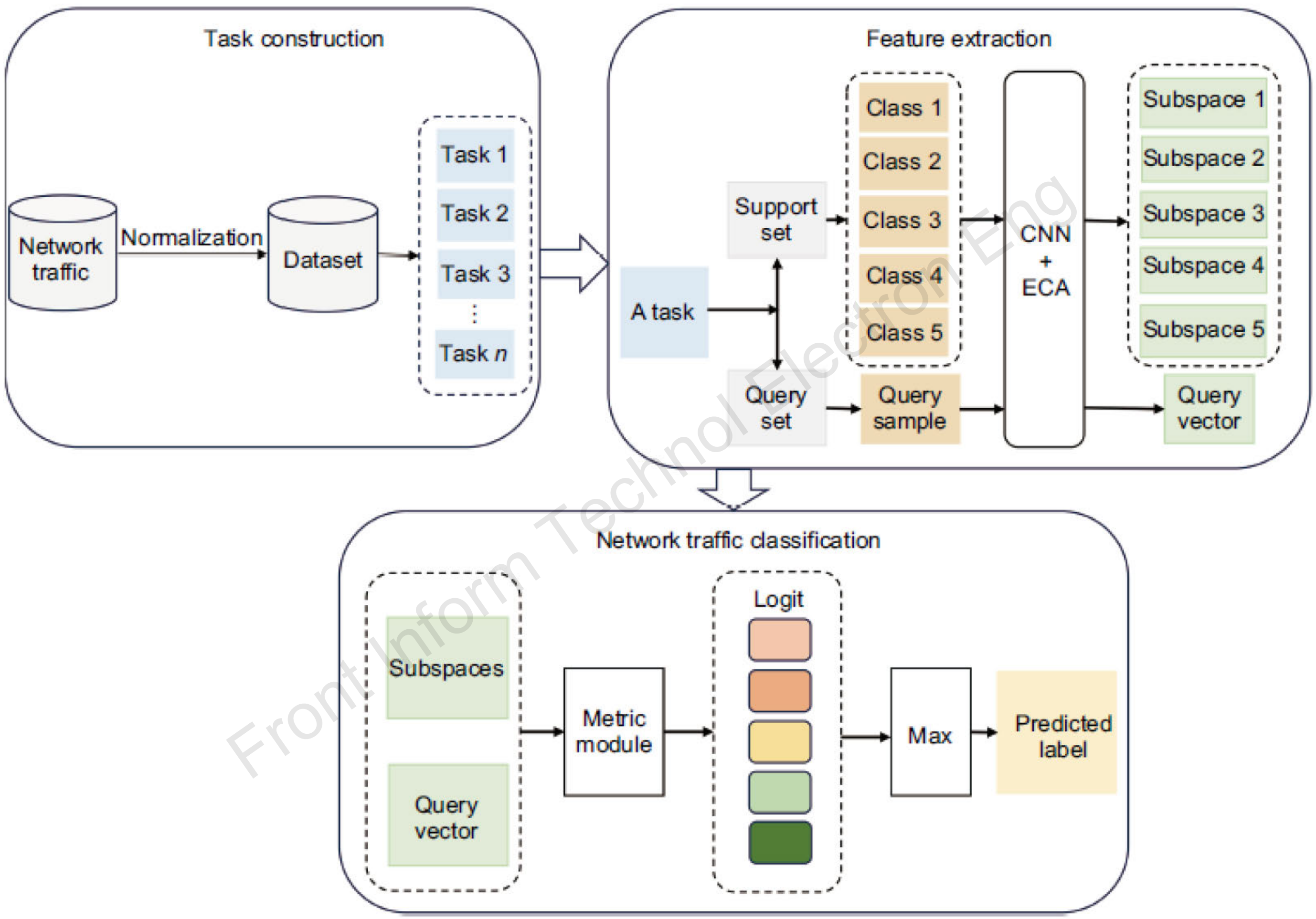

Fig. 1 Diagram of subspace-based few-shot IoT intrusion detection structure. The proposed method is divided into three main modules: task construction, feature extraction, and network traffic classification. During the task construction phase, the main focus is creating N-way K-shot formatted few-shot tasks to facilitate model learning. In the feature extraction module, we design a four-layer structure with an ECA mechanism. Finally, in the network traffic classification module, classification is performed by measuring the distance between the query vector and the subspace of each category

Method

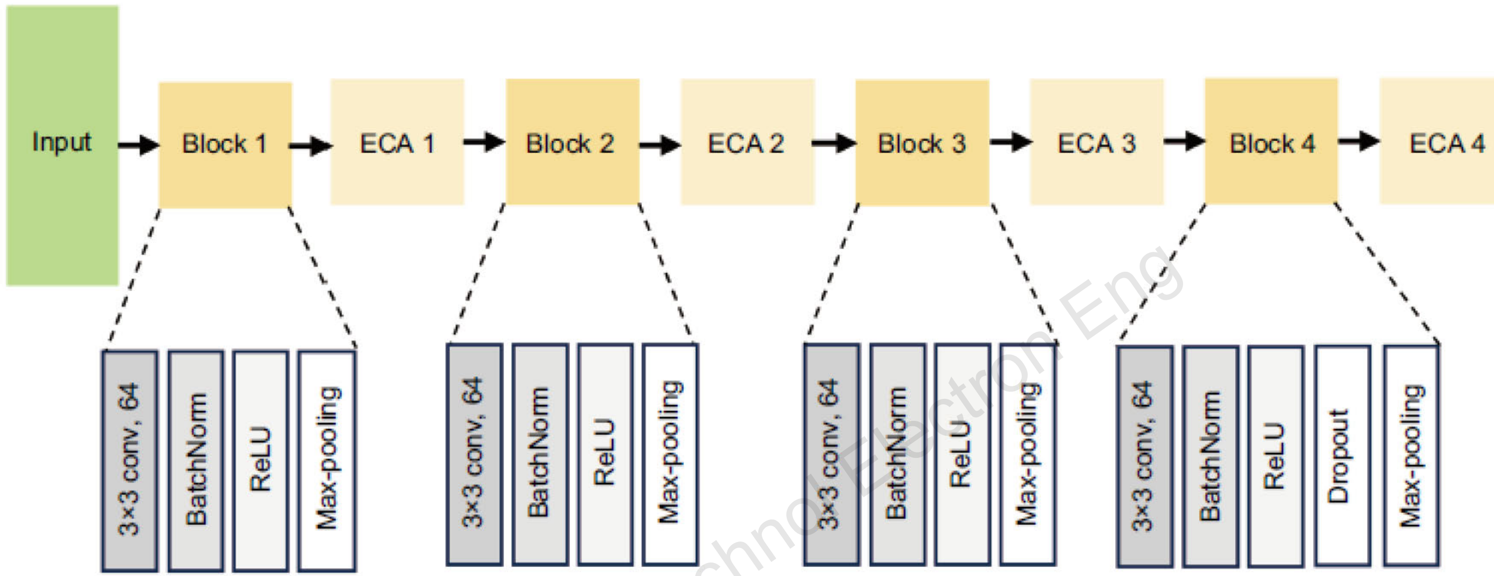

Fig. 2 CNN with ECA mechanism

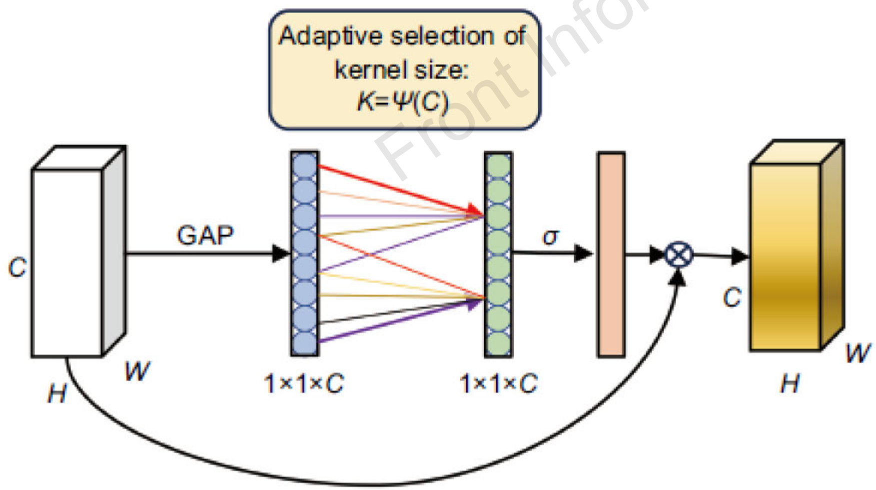

Fig. 3 ECA module

Loss function:

$$\boldsymbol{\mu}_c = \frac{1}{K}\sum_{i=1}^{K} \boldsymbol{F}_{c,i}^{\mathrm{sup}},$$

$$\begin{aligned}\sigma_p^2(\boldsymbol{P}_i, \boldsymbol{P}_j) &= \|\boldsymbol{P}_i\boldsymbol{P}_i^{\mathrm{T}} - \boldsymbol{P}_j\boldsymbol{P}_j^{\mathrm{T}}\|_{\mathrm{F}}^2 \\ &= 2D_{\mathrm{s}} - 2\|\boldsymbol{P}_i^{\mathrm{T}}\boldsymbol{P}_j\|_{\mathrm{F}}^2,\end{aligned}$$

$$\mathcal{L}_{\mathrm{t}} = -\frac{1}{NK}\sum_{c}\ln(p_{c,q}) + \lambda\sum_{i\neq j}\|\boldsymbol{P}_i^{\mathrm{T}}\boldsymbol{P}_j\|_{\mathrm{F}}^2$$

Results

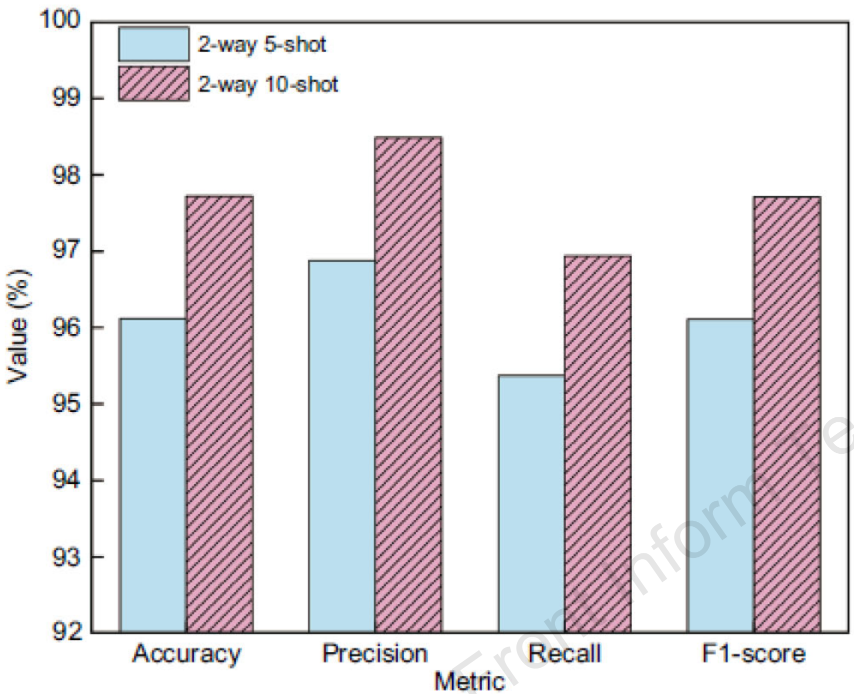

Fig. 4 Comparison of the influence of sample size on the results in a binary classification setting

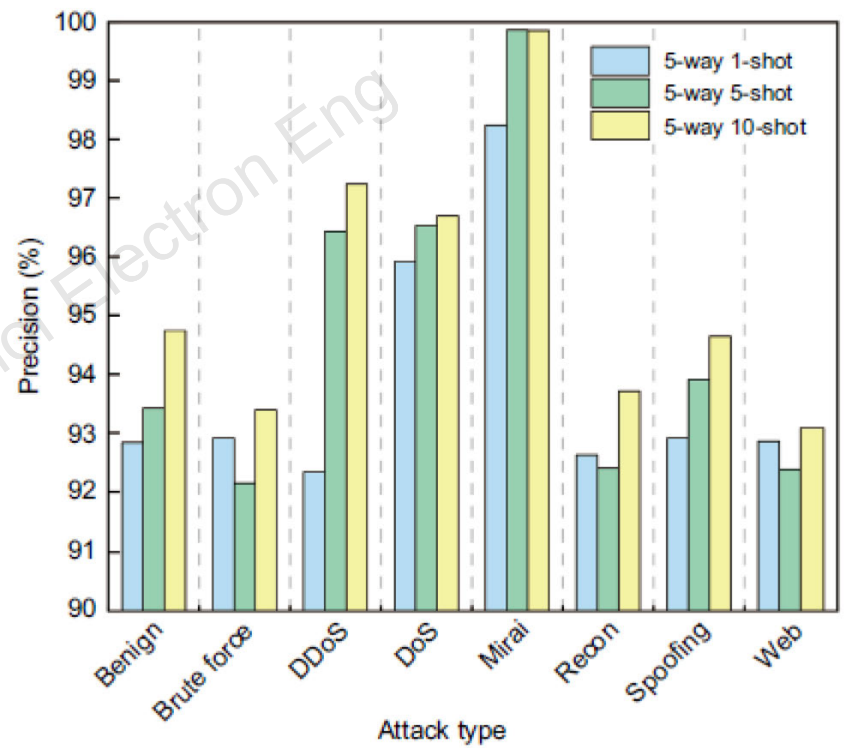

Fig. 5 Comparison of the influence of sample size on the results in a multi-classification setting

Results

Table 5 Comparison of detection results and sample sizes under multi-classification settings for the methods presented in this paper and related works

Method	Dataset	IoT dataset	Classification setting	Number of samples	Accuracy (%)
MAML+CNN (Lu CM et al., 2023)	FSIDSIOT	Y	5-way 1-shot	1	73.81
	FSIDSIOT	Y	5-way 5-shot	5	89.64
	FSIDSIOT	Y	5-way 10-shot	10	92.19
IPN-IDS (Wang YH et al., 2024)	CICIDS2017	N	5-way 1-shot	1	75.45
	CICIDS2017	N	5-way 5-shot	5	84.94
	CICIDS2017	N	5-way 10-shot	10	86.35
	CICIoT2023	Y	5-way 1-shot	1	61.03
	CICIoT2023	Y	5-way 5-shot	5	66.93
	CICIoT2023	Y	5-way 10-shot	10	68.77
Proposed approach	CICIDS2017	N	5-way 1-shot	1	83.88
	CICIDS2017	N	5-way 5-shot	5	92.66
	CICIDS2017	N	5-way 10-shot	10	95.58
	CICIDS2018	N	5-way 1-shot	1	91.00
	CICIDS2018	N	5-way 5-shot	5	94.16
	CICIDS2018	N	5-way 10-shot	10	94.70
	CICIoT2023	Y	5-way 1-shot	1	93.52
	CICIoT2023	Y	5-way 5-shot	5	92.99
	CICIoT2023	Y	5-way 10-shot	10	93.65

Conclusions

In this study, we developed a subspace-based classification model to solve the few-shot IoT intrusion detection problem. First, we constructed an intrusion detection dataset suitable for few-shot scenarios based on the latest IoT dataset, CICIoT2023. Next, the data samples for 1D CNN learning were formed by normalizing the tabular data and transforming the data types. Subsequently, according to the N-way K-shot learning paradigm, a set of tasks used for model training was constructed. Each task was used to extract the features of each sample through CNN with the ECA mechanism, and the classification effect was realized through a subspace-based classifier. For unknown attack classes, our model eliminated fine-tuning requirements by leveraging prior knowledge to achieve rapid generalization across novel threat categories. Our model showed good detection results for all models at sample number $K = 1, 5$, and 10. However, the performance and robustness of our model should be improved when only one sample is available.

Zhihui LI received the BS degree from Henan Institute of Science and Technology in 2023. He is currently pursuing his MS degree at Zhejiang Sci-Tech University. His research focuses on few-shot learning and IoT intrusion detection.

Congyuan XU received the BS degree in applied physics from Xidian University, Xi'an, China, in 2013, and the PhD degree in electronics science and technology from Zhejiang University, Hangzhou, China in 2019. Currently, he is a lecturer at the College of Artificial Intelligence, Jiaxing University, Jiaxing, China. His research interests focus on machine intelligence and cyberspace security.

Kun DENG received the PhD degree in computer applied technology from Harbin Engineering University, China, in 2015. He is currently employed at Jiaxing University, with research interests including data mining, big data analytics, and data structure analysis.

Chunyuan LIU received the PhD degree from Southeast University, China, 2015. He has been an associate professor with the College of Mechanical Engineering, Jiaxing University, China. His current research interests include deep learning, optimization design, and control of permanent magnet motors.