A Domain Adaptation Network Intrusion Detection Algorithm based on Class-Balanced Knowledge Transfer and Multi-Structure Domain Alignment

Qian Wang[a*], Xiang Liu[a†], Yifan Cheng[a†], Yongqiang Cheng[b†], Bing Zhang[a†]

[a*] School of Information Science and Engineering, Yanshan University, Qinhuangdao, 066004, China.
[b*] School of Computer science, University of Sunderland, Sunderland, SR1 3SD, UK.

*Corresponding author(s). E-mail(s): wangqian@ysu.edu.cn;
Contributing authors: liuhan01@stumail.ysu.edu.cn;
megumi@stumail.ysu.edu.cn; yongqiang.cheng@sunderland.ac.uk;
bingzhang@ysu.edu.cn;
†These authors contributed equally to this work.

Abstract

In practical deployment, the performance of network intrusion detection systems is often degraded due to class imbalance in the training data and the distribution discrepancy between the training data and the traffic collected from real detection environments. To solve the above problems, a domain adaptation intrusion detection algorithm based on class-balanced knowledge transfer and multi-structure domain alignment is proposed in this paper. Firstly, the concept of class separation loss is proposed to reduce the effect of class overlap caused by data imbalance processing on cross-domain knowledge transfer, and a dynamic threshold is used to select high-confidence pseudo-labels of the target domain for subsequent domain alignment. In addition, a multi-structure domain alignment method is proposed to reduce the discrepancy between the data distributions of the source domain and the target domain. Domain-invariant features of the source domain and the target domain are extracted by reducing the domain discrepancy caused by dependency structures across different domains. Through supervised class prototype discovery and relative structural alignment of class prototypes, the discrepancy in the local relative structures of class prototypes across different domains is reduced. Experiments are conducted on four public

NIDS datasets under two cross-domain scenarios. In the cross-domain experiments from UNSW-NB15 to ToN-IoT and from NSL-KDD to BoT-IoT, the F1-score of the proposed algorithm reaches 89.73% and 84.10%, respectively, thereby verifying the effectiveness and superiority of the proposed algorithm.

Keywords: Network intrusion detection, Adversarial domain adaptation, Class imbalance, pseudo-label, Class prototype, Copula

1 Introduction

Nowadays, Network Intrusion Detection System (NIDS) is important for network security guarantee. However, the effectiveness of NIDS relies on high-quality and adequately labeled datasets for training and evaluation. Labeling large network traffic data requires significant resources and expert knowledge, and due to the privacy and security concerns, most of the Machine Learning (ML) based NIDS uses publicly available datasets for training [1], such as UNSW-NB15 [2] and KDD99 [3]. Although the validation experiments are designed rigorous and perform well on many indicators, the NIDS can not achieve the same excellent results in real network environments, because of the different traffic features and data distribution, which results in the poor detection performance for network security.

Domain adaptation aims to address the degradation of model performance caused by the distribution discrepancy between source domain and target domain data. By exploiting the knowledge of the source domain with rich annotation information, the generalization ability of the model in the target domain is improved through feature alignment, distribution matching, adversarial learning, and other strategies. Ju et al. [4] proposed a semi-supervised domain adaptation framework based on distillation and reinforced domain-specific knowledge (DARK). In this framework, the classification performance in the target domain is improved through three stages, including multi-view learning, knowledge distillation, and knowledge refinement. Ba et al. [5] proposed a Trico-based semi-supervised domain adaptation method, which improves class representation alignment and target domain structure learning through pseudo-labels and pseudo-edges. In addition, several other pseudo-label-based domain adaptation algorithms have also achieved excellent performance. For example, Discriminative Distribution Alignment (DDA) [6], Weighted Cluster Graph Network (WCGN) [7], and Geometric Graph Alignment (GGA) [8].

Existing domain adaptation studies have provided effective solutions for cross-domain intrusion detection. Pseudo-label-based knowledge transfer methods use unlabeled target-domain data to improve the recognition rate in the target domain, whereas distribution alignment methods reduce the discrepancy between feature representations of the source domain and the target domain. However, several important issues remain insufficiently addressed by the above methods. Firstly, when the source domain data are severely imbalanced, the transferred knowledge may be biased toward the majority class, resulting in unreliable pseudo-labels and weakened detection capability for minority-class samples in the target domain. Secondly, although methods such as Domain Conditioned Adaptation Network (DCAN) [9], Generalized Domain Conditioned Adaptation Network (GDCAN) [10], and Domain Adaptation Recommendation (DAR) [11] can extract domain-invariant features by minimizing the global distribution discrepancy of features, the distribution discrepancy caused by different feature dependency structures is not identified. In addition, distribution shifts of features in cross-domain scenarios prevent the classifier from generalizing the classification decision boundary learned from the source domain to the target domain.

To solve the above problems, this paper proposes a domain adaptation network intrusion detection algorithm based on class-balanced knowledge transfer and multi-structure domain alignment. The source domain data is processed with class imbalance, and the source domain knowledge is transferred to the target domain to generate pseudo label for the target domain data. Then, through multi-structure domain alignment, the feature dependence structure and class prototype relative structure are aligned by using pseudo labels, and the classification decision boundary of the source domain is generalized to the target domain by combining the overall feature distribution, thus enhancing the domain adaptation ability of the classifier. The main contributions of this paper are summarized as follows.

(1) A class-balanced knowledge transfer network is proposed in this paper to address cross-domain intrusion detection under class imbalance. Different from traditional class imbalance processing methods that generate minority-class samples based on GANs, a class separation loss is further proposed to reduce the effect of class overlap on knowledge transfer. A dynamic threshold is used to filter high-confidence target-domain data, thereby alleviating the imbalance of class proportions between domains and achieving class-balanced knowledge transfer.

(2) A dynamic pseudo-label generation strategy is proposed in this paper to improve the target-domain supervision capability under class imbalance and distribution shift. Different from traditional pseudo-labeling methods that directly use classifier predictions as supervision information of the target domain, the proposed strategy generates pseudo-labels through a classifier trained with class-balanced source domain knowledge and filters low-confidence target domain samples using a dynamic confidence threshold. This strategy reduces noisy and class-biased pseudo-label supervision, thereby providing more reliable target domain information for subsequent domain alignment.

(3) A multi-structure domain alignment mechanism is proposed in this paper to improve feature alignment and decision boundary transfer. Different from existing domain adaptation methods that mainly align global feature distributions, the proposed method introduces dependency structure alignment based on copula entropy to reduce the discrepancy in nonlinear feature dependencies between classes across domains. In addition, different from traditional prototype alignment methods that mainly match individual features or class centers across domains, the proposed relative structural alignment method of class prototypes preserves the geometric relationships among class prototypes in the source domain and the target domain, thereby enhancing the transferability of the classification decision boundary.

2 Related Work

Domain adaptation methods have been widely applied to solve the distribution shift problem in network intrusion detection. Wu et al. [8] used a geometric map alignment method to cover the geometric heterogeneity between domains in order to better carry out knowledge transfer. The rotation avoidance mechanism and center point matching mechanism are used to avoid the dislocation caused by rotation and symmetry respectively, and the performance of network intrusion detection system is improved by geometric alignment of intrusion graphs of different granularities. Ba et al. [12] addressed multi-target domain adaptation by combining source domain representation extraction with intra-target hierarchical alignment and inter-target collaborative alignment, thereby enhancing cross-domain classification performance. However, these methods do not consider the serious class imbalance problem in network intrusion detection. Class imbalance will exacerbate the distribution shift, and the model may pay more attention to majority classes and ignore the important minority classes in the target domain.

In the face of the class imbalance problem in domain adaptation, the re-weighting methods are commonly used. Chen et al. [13] designed a style mixing module and a domain style loss module to obtain a generalized domain-invariant representation without adding any synthetic samples, and a Dual-View classifier composed of binary classifiers and multi-class classifiers is constructed to achieve accurate fault classification of imbalanced data by dynamic re-weighting. Ding et al. [14] used cost sensitive re-weighting and classification alignment to calibrate classification balance loss and narrow classification feature distribution differences to achieve potential space matching. The edge loss regularization is introduced to further optimize classification boundary and improve the cross-domain generalization ability of fault diagnosis tasks. However, these methods based on re-weighting have limitations such as insufficient data diversity and easy over-fitting. Methods based on data enhancement can effectively increase the data diversity, reduce the risk of over-fitting, and balance the proportion of samples from different classes. Xia et al. [15] proposed a Generative Inference Network (GINet) to discover domain-invariant knowledge by estimating the common potential variables of reliable cross-domain samples, and then generate the reliable samples of minority classes to improve the discriminant ability. Zhao et al. [16] proposed a discriminant semantic enhancement network by designing a hybrid strategy based on semantic regularization to synthesize enough reliable samples to compensate for minority classes. Yuan et al. [17] proposed a class-balanced pseudo label strategy to select the same proportion of trusted samples from each class, and then data enhancement techniques are applied to alleviate the class imbalance problem. Although these methods extend the source domain through data enhancement methods and alleviate the class imbalance problem, they do not consider the class overlap problem in data generation. Class overlap will result in highly mixed sample points of different classes in the feature space, further aggravating the distribution shift of different domains.

Ganin et al. [18] proposed a general domain alignment method Domain Adversarial Neural Network (DANN). By introducing adversarial training mechanism, it learns features that are discriminant and invariant to domain changes to make the distribution of source domain and target domain in feature space as similar as possible. Therefore, the classification performance in the target domain is improved. Ma et al. [19] proposed a novel adversarial domain adaptation method based on two-domain pairing strategy. The data enhancement algorithm is used to construct a sample migration model conforming to the joint dual domain distribution. Then combined with the dual domain matching strategy and domain adversarial network, the supervised domain adaptation is carried out. Chen et al. [20] used the information-enhanced domain adversarial networks to improve the detection performance of industrial control intrusion detection systems in dynamic networks. Convolutional Neural Network (CNN) is used to extract feature information from different views, the attention mechanism is introduced to selectively enhance information and suppress the features that contribute less to classification. However, it is still difficult to achieve the feature alignment. Long et al. [21] proposed a Conditional Domain Adversarial Network (CDAN) to transfer knowledge through the conditional generation adversarial network, and conditional constraints are applied to the adversarial adaptation model according to the discriminant information of the classifier prediction. Wu et al. [22] proposed a Adaptive Bi-Recommendation and Self-Improving Network (ABRSI) by introducing the bi-recommendation matching into domain adaptation, and the training model of the source domain is used to recommend the closest label to the target domain samples to complete knowledge transfer, which makes the positive mutual cycle of bi-recommendation interest matching and feature alignment, and realizes the heterogeneous domain adaptation. Although these methods have achieved some results in domain alignment, they do not consider the influence of dependence structure differences between features on distribution shift. In addition, prototype method is often used in domain alignment, Jiang et al. [23] proposed a domain adaptation method based on prototype contrast adaptation, which uses contrast learning to align the features of source domain and target domain. By calculating the similarity score between the image feature vector of the target domain and the class prototype of the source domain, and minimizing the contrast loss, the feature of the target domain is adjusted to align with the class prototype of the source domain. Different from previous prototyping methods, this paper designs a prototype relative structure alignment mechanism, which focuses on the local structure between prototypes in domain alignment, so as to obtain better alignment results.

3 Methodology

The proposed algorithm consist of two parts, as shown in Figure 1. The first component is the class-balanced knowledge transfer network, which augments the source domain data using generative adversarial networks, and trains a classifier to generate supervision information for the target domain data, and filters the high confidence target domain data according to the supervision information. Then, the source domain and target domain data are input into the multi-structure domain alignment network, domain-invariant features are extracted by dependence structure alignment, and the source domain and target domain have locally similar decision boundaries by class prototype relative structure alignment. Finally, the decision boundary of source domain is generalized to the target domain by combining domain adversarial network to align

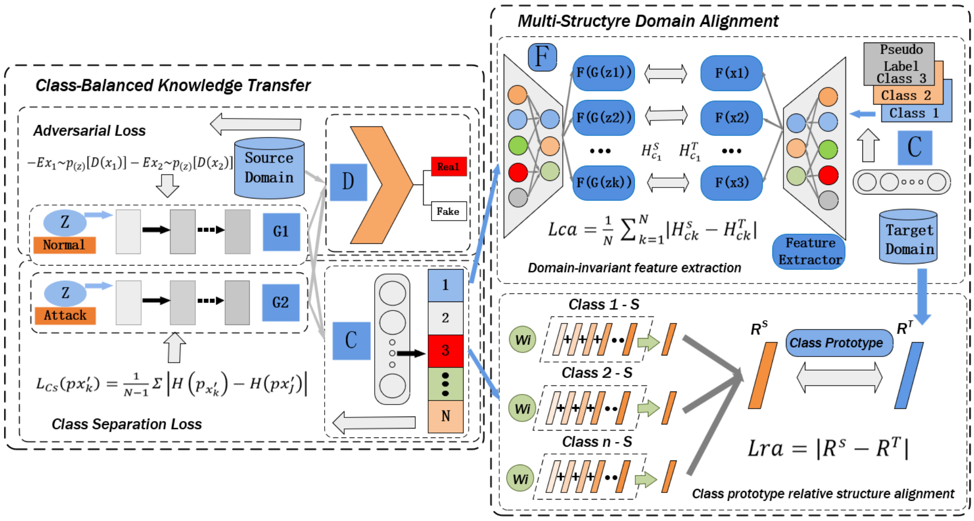


Fig. 1: Framework of the proposed algorithm

the overall distribution of source domain and target domain and the overall structure of class prototype.

3.1 Class-balanced knowledge transfer

Because of the class imbalance of the data, the knowledge learned by the classifier will tend more to the majority classes. The generative adversarial network of multi-generator structure [24] is used to deal with the problem of data imbalance. It learns the data distribution of different kinds of data through multiple generators to achieve the purpose of expanding the data of minority classes. In order to realize the class-balanced knowledge transfer, a generative adversarial network of dual-generator structure is designed to expand the benign and attack samples in the source domain, which consists of two generators and a discriminator. The goal of each generator is to learn the data distribution of different classes in the source domain. The objective function is as Equation (1).

$$\min_{G_{1\sim 2}} \frac{1}{2}[-E_{\widetilde{x}_1\sim p(z)}[D(\widetilde{x}_1)] - E_{\widetilde{x}_2\sim p(z)}[D(\widetilde{x}_2)]] \tag{1}$$

where G is the generator, $\widetilde{x}$ is pseudo-sample generated from the noise distribution, $p(z)$ is the noise distribution, and the D is the discriminator. The discriminator D is to distinguish real data from the generated data, and directs the generator training to fit the distribution of the real data. The objective function of the discriminator is as Equation (2).

$$\max_{D} \frac{1}{2}[E_{x_1\sim p_r}[D(x_1)] - E_{\widetilde{x}_1\sim p(z)}[D(\widetilde{x}_1)] + E_{x_2\sim p_r}[D(x_2)] - E_{\widetilde{x}_2\sim p(z)}[D(\widetilde{x}_2)]] \tag{2}$$

where x is the real data, p_r is the distribution of the real data. The ultimate goal of the model is to enable each generator to learn the true distribution of different classes of data, and make it impossible for the discriminator to tell whether the data is real or generated. The objective function is as Equation (3).

$$\min_{G_{1\sim 2}} \max_{D} \frac{1}{2}[E_{x_1\sim p_r}[D(x_1)] - E_{\widetilde{x}_1\sim p(z)}[D(\widetilde{x}_1)] + E_{x_2\sim p_r}[D(x_2)] - E_{\widetilde{x}_2\sim p(z)}[D(\widetilde{x}_2)]] \quad (3)$$

where $E_{x\sim p_r}[D(x)] - E_{\widetilde{x}\sim p(z)}[D(\widetilde{x})]$ is the original objective function of WGAN [25]. In order to transfer the knowledge from the source domain to the target domain, a classifier is designed to learn the discriminant knowledge of the source domain, and obtain the discriminant information of the target domain data, and provide supervision information for the subsequent domain alignment. The loss function is cross entropy loss as Equation (4).

$$L_{ce} = -\frac{1}{M}\sum_{i=1}^{M}[y_i \log(p_i) + (1 - y_i)\log(1 - p_i)] \quad (4)$$

where M is the number of samples, i represents the sample serial number, y represents the label of the source domain sample, and p is the output of the classifier. The process of imbalanced data often leads to class overlap of samples [24]. In the case of cross-domain, overlapping class samples further confuse samples of different classes in the target domain, which will have an impact on knowledge transfer. This paper proposes the class separation loss to solve the problem of class overlap. According to [26, 27], the output entropy of samples from different classes can be used for classification. Therefore, this paper proposes the class separation loss as Equation (5).

$$L_{cs} = \frac{1}{N}\sum_{k=1}^{N} L_{cs}(p_{\widetilde{x}_k}) + \alpha|H(p_{x^S}) - H(p_{x^T})| \quad (5)$$

$$L_{cs}(p_{\widetilde{x}_k}) = \frac{1}{N-1}\sum_{j=1}^{N}|H(p_{\widetilde{x}_k}) - H(p_{\widetilde{x}_j})|, \ j \in \{1, ..., N\} \ and \ j \neq k \quad (6)$$

Equation (5) is the class separation loss obtained by aggregating Equation (6) and adding the entropy regularization term, where N represents the number of class, $\widetilde{x}_k$ represents the kth class of pseudo samples generated by the generator, and $\widetilde{x}_j$ represents the pseudo samples of the jth class. $p_{\widetilde{x}_k}$ and $p_{\widetilde{x}_j}$ respectively represent the classifier output of $\widetilde{x}_k$ and $\widetilde{x}_j$, $H(\cdot)$ represents the entropy, α is the hyper-parameter, x^S and x^T represent the source domain data and the target domain data respectively.

The class separation loss encourages generated samples from different classes to become more distinguishable in the classifier output space, thereby reducing class overlap caused by data generation. The entropy regularization term further improves cross-domain consistency by making the output entropy distributions of the source domain and the target domain closer. In order to transfer the rich source domain knowledge to the target domain, this paper uses the trained classifier to generate pseudo label for the target domain data. The pseudo label is as Equation (7).

$$\widehat{y}_i^T = \begin{cases} \arg\max\limits_j p_{ij} & \max\limits_j p_{ij} > q_{\arg\max\limits_j p_{ij}} \\ -1 & otherwise \end{cases} \tag{7}$$

where $\widehat{y}_i^T$ represents the pseudo label of the target domain data, q is the confidence threshold, p is the output of the classifier, and -1 indicates that this pseudo label is not adopted. Pseudo label can provide supervision information for subsequent domain alignment. The output of the classifier for the target domain data will be used to filter the target domain data. When the maximum value of the output for a target domain sample is less than the confidence threshold, the sample will be discarded. Considering the class imbalance of the target domain, a dynamic adjustment method is adopted to update the q to adapt imbalanced target domain data as Equation (8).

$$q = 0.5 + r - 2 * \frac{1}{\exp \sum_{i=1}^{M} 1_K(\widehat{y}_i^T)} * r \tag{8}$$

where r is a hyper-parameter of control rate, $1_K(\widehat{y}_i^T)$ is the indicator function as Equation (9).

$$1_K(\widehat{y}_i^T) = \begin{cases} 1 & \text{if } \widehat{y}_i^T = k \\ 0 & \text{if } \widehat{y}_i^T \neq k \end{cases} \tag{9}$$

Equation (8) allows the dynamic adjustment of $q \in [0.5 - r, 0.5 + r]$ to adapt the imbalanced target domain data. Under the condition of class imbalance in the target domain, the dynamic threshold adjusts the selection criterion according to the prediction distribution of the target domain. This strategy prevents the model from over-selecting majority-class samples and reduces the influence of noisy pseudo-labels, thereby improving the reliability of target domain supervision. The filtered target domain data is used with the source domain data generated by the generator for subsequent domain alignment.

3.2 Multi-structure domain alignment

Due to the diversity and complexity of data distribution in different domains, cross-domain feature alignment is a difficult task. Previous studies have mainly adopted methods such as minimizing the Maximum Mean Discrepancy (MMD) to align the distribution differences between different domains. MMD achieves domain adaptation by calculating the distance of mean embedding between two distributions in the Reproducing Kernel Hilbert Space (RKHS), measuring the difference between the two distributions, and then minimizing this distance so that the two distributions are as close as possible. However, the domain difference that leads to the distribution shift may be caused by the difference of the feature dependence structure [28], and feature dependencies may not be found if only the differences in the overall distribution is considered. Therefore, this paper proposes a copula entropy [29] dependence structure alignment to extract domain-invariant features of different domains.

Domain adversarial training [18] is a common way to align differences between source and target domains. It tries to learn the feature representation by which the domain discriminator can not distinguish the source domain from the target domain. However, this method does not consider the local structure of feature alignment, and the generalization ability of the decision boundary learned by the classifier is insufficient. Therefore, this paper proposes to construct the class prototype with supervised class prototype discovery, and then proposes the relative structure alignment of the class prototype so that the model can learn the local similar feature representation of the decision boundary, and finally realizes the alignment of the overall structure of the class prototype and the overall feature distribution by domain adversarial method.

3.2.1 Domain-invariant feature extraction

To process the high-dimensional feature space of NIDS data, the original traffic features are first mapped into a compact low-dimensional latent representation space by the feature extractor. The feature dependency structures are then measured and aligned in this latent space. Measuring the correlation between two variables is effective to capture the dependence structure between features [30]. Mutual information can be used as a metric to measure the correlation between two distributions, and also the dependency between features [28]. Suppose the joint distribution of two random variables is $p(x, y)$, the marginal distribution is $p(x)$ and $p(y)$, and the mutual information is as shown in Equation (10).

$$I(X;Y) = \sum_{x \in X} \sum_{y \in Y} p(x, y) \log \frac{p(x, y)}{p(x)p(y)} \tag{10}$$

Although mutual information can measure the dependency between features, it is often limited to the case of two variables. For multi-variable deep learning tasks, it is difficult to capture the dependency between multiple features. Copula entropy [29] can be used to measure the dependency between random variables, and it is equivalent to mutual information but can be generalized to arbitrary variables. It is as Equation (11).

$$H_c(u_1, ..., u_n) = -\int_0^1 ... \int_0^1 c(u_1, ..., u_n) \ln c(u_1, ..., u_n) du_1, ..., du_n \tag{11}$$

where u represents the marginal distribution and $c(u)$ is the copula density function. The discrete form of the above equation is as Equation (12).

$$H_c(u_1, ..., u_n) = -\sum_{i=1}^{n} ... \sum_{i=1}^{n} P_c(u_1, ..., u_n) \ln P_c(u_1, ..., u_n) \tag{12}$$

where P_c is the discrete probability of copula.

The feature dependence structure of the samples with the same class can be captured by using copula entropy, and the difference between the source domain and the target domain can be further minimized to obtain the domain-invariant feature. Specifically, the data dependence structure of different classes in the source domain is calculated according to the label of the source domain data, and then the data dependence structure of different classes in the target domain is calculated according to the pseudo label generated by the classifier. That is, learn a feature extractor to align the dependence structure differences of the same class in different domain data. The dependence structure alignment loss function is as Equation (13).

$$L_{ca} = \frac{1}{N} \sum_{k=1}^{N} |H_{ck}^{S} - H_{ck}^{T}| \tag{13}$$

where N represents the number of classes, S and T represent the source and target domains respectively, and H_{ck} is the copula entropy of the kth class. The dependency structure alignment loss measures the inconsistency of feature dependency structures between the two domains by calculating the difference in copula entropy between samples of the same class in the source domain and the target domain. Minimizing the dependency structure alignment loss encourages the feature extractor to learn domain-invariant representations with similar feature relationships, thereby reducing cross-domain distribution shifts caused by differences in feature dependency structures.

3.2.2 Class prototype relative structure alignment

Class prototype discovery (CPD) [31] is a new class prototype construction method, which uses a classifier to match the classification score to a specified class and finds an optimal prototype for each class. CPD can make full use of samples to build class prototypes but the constructed class prototypes are randomly distributed in the feature space because CPD is an unsupervised method that does not use label information, which is not conducive to domain alignment. Therefore, this paper proposes a supervised CPD to extract class prototypes, making cross-domain class prototype alignment possible. Specifically, the source domain and target domain samples are subdivided by class labels or pseudo labels, respectively, and the confidence weights for each sample are introduced. It is as Equation (14).

$$w_{i,k} = \frac{\exp P_{i,k}}{\sum_{j=1}^{M_k} \exp P_{j,k}}, \ k = 1, ..., N \tag{14}$$

where k represents the class, i and j respectively represent the ith and jth samples, e is the natural logarithm, p is the output of classifier, M is the total number of samples. Then, using the Exponential Moving Average (EMA) strategy, the class prototype of each class is updated incrementally with the sample of the same class. It is as Equation (15).

$$c_k = \eta c_k + (1-\eta) c_k^{'}, \ c_k^{'} = \sum_{i=1}^{M_k} w_{i,k} * f_i \tag{15}$$

where c_k represents the class prototype, η represents the momentum of prototype update, and f_i represents the ith sample. In the training process, the knowledge of samples from different classes is gradually converged into each prototype to make full use of all the samples.

Further, this paper proposes class prototype relative structure alignment to minimize the local relative structure difference between source domain and target domain. A prototype vector is constructed to represent the relative relationship between prototypes. It is as Equation (16).

$$v(k,j) = c_j - c_k \tag{16}$$

where v represents the prototype vector, c represents the class prototype, k and j represent the different classes. Then aggregate the prototype vectors of each class to form a relative structure. It is as Equation (17).

$$R = \frac{1}{N(N-1)} \sum_{k=1}^{N} \sum_{j=1, j\neq k}^{N} v(k,j) \tag{17}$$

where R represents the relative structure of the class prototype, N is the number of class, j and k respectively represent the jth and kth class, v is the prototype vector. The class-prototype relative-structure alignment loss is as Equation (18).

$$L_{ra} = |R^S - R^T| \tag{18}$$

where S and T represent source and target domains, respectively. By minimizing the local relative structure differences between source domain and target domain, the source domain and target domain have locally similar decision boundaries.

3.2.3 Domain adversary

Domain adversarial network [18] is a common algorithm to solve cross-domain distribution shift, which can align the overall distribution of features in different domains in feature space. In the process of domain adversary, the feature distributions of different domains are aligned gradually, so the overall structure of the class prototype learned from the domain-invariant features is implicitly aligned and the decision boundary of the source domain is generalized to the target domain. The loss of the domain discriminator is as Equation (19).

$$L_D = E_{x^S \sim \widetilde{S}} \log \frac{1}{D(f(x^S))} + E_{x^T \sim \widetilde{T}} \log \frac{1}{D(f(x^T))} \tag{19}$$

where x^S and x^T respectively represent the source and target domain data, D represents the domain discriminator, $f(\cdot)$ represents the output of the feature extractor. The classifier uses cross entropy loss to learn the decision boundary between source domain class prototypes, and the loss function is as Equation (20).

$$L_{cp} = \frac{1}{N} \sum_{k=1}^{N} L_{ce}(c_k, k) \tag{20}$$

where L_{ce} is the cross entropy loss, k is the class label. The total loss of the final multi-structure domain alignment module is as Equation (21).

$$L = L_{ca} + L_{ra} + L_D + L_{cp} \tag{21}$$

4 Experimental evaluation

4.1 Datasets

To evaluate the algorithm proposed in this paper, the four common NIDS datasets NSL-KDD [3], UNSW-NB15 [2], BoT-IoT [32] and ToN-IoT [33] are used, which containing the general traffic statistics and information about specific protocol applications such as DNS and FTP. NSL-KDD, UNSW-NB15 are traditional network traffic data, and BoT-IoT, ToN-IoT are from the Internet of Things environment. Different datasets can be considered as data from different network environments, which have different attack classes and data distribution. This paper considers the binary classification problem

4.2 Experimental environment

The experimental environment of this paper is the computer of 64-bit Linux operating system, RTX4090 graphics processing unit and 16GB memory. The experiment uses the Python machine learning library PyTorch.

The class-balanced knowledge transfer network consists of generator, discriminator, and classifier. All of them are ReLU-MLP, in which the number of generators is set to two, corresponding to the normal class and the abnormal class, respectively, the network structure of generator and discriminator is the same as [25], and the structure of the classifier is set as ReLU-MLP (x->16->32->64->128->2). The multi-structure domain alignment module contains the feature extractor, the domain discriminator, and the classifier, the domain discriminator and the classifier are ReLU-MLP, the hidden layer structure is the same as [18], and the gradient inversion layer is also added before the domain discriminator. The feature extractor is set as ReLU-MLP (x->32->64->128->32). The parameter settings of each part are shown in Table 1.

4.3 Preprocessing

Non-numerical attributes of datasets are removed. All attack samples are unified as label '1' and all benign samples as label '0'. The data is then normalized by using MinMaxScaler and the invalid values such as NAN and INF are filtered out. The

Table 1: Parameter settings

Class-Balanced Knowledge Transfer		Multi-structure Domain Alignment	
item	value	item	value
Batch size	128	Batch size	64
Max epoch	20000	Max epoch	20000
Learning rate	0.0001	Learning rate	0.0001
α	0.01	η	0.8
r	0.2		

MinMaxScaler normalization is as Equation (22).

$$\bar{X} = \frac{X - X_{min}}{X_{max} - X_{min}} \tag{22}$$

where X_{max} and X_{min} are the maximum and minimum values of feature X, respectively.

4.4 Comparative experiment

In order to verify the cross-domain capability of the proposed algorithm in different network environments, two cross-domain comparative experiments are carried out. Due to the class imbalance of the datasets, F1-Score is used as the evaluation metric, which takes into account both precision and recall. The comparative domain adaptation algorithms are CDAN [21], DCAN [9], GDCAN [10], DAR [11], ABRSI [22], DDA [6], WCGN [7], GGA [8], which perform domain alignment from different perspectives. For example, CDAN introduces conditional information to assist domain alignment. By combining collaborative training and adversarial training, DCAN and GDCAN enable each independently trained model to learn domain-invariant knowledge from each other and improve the generalization ability of the model. DAR and ABRSI implement knowledge transfer through recommendation matching. GGA uses geometric properties of graphs and neighborhood information to learn domain-invariant features to achieve domain alignment. Therefore, the superiority of the proposed algorithm can be verified from multiple perspectives. The first set of experiments used UNSW-NB15 as the source domain and ToN-IoT as the target domain for cross-domain intrusion detection experiments; the second set of experiments used NSL-KDD as the source domain and BoT-IoT as the target domain for cross-domain intrusion detection experiments. Different cross-domain network environments provide different complex scenarios for comparative analysis. The results are shown in Tables 2 and 3.

As shown in Table 2 and Table 3, the performance of the proposed algorithm is significantly better than that of other baseline algorithms. Where, CDAN, DDA, and WCGN predict pseudo-labels only through fully connected neural networks, which leads to insufficient data modeling capability of the models. The ABRSI algorithm generates pseudo-labels through a recommendation system, thereby improving the data modeling capability of the model and the accuracy of pseudo-labels. However, it only enriches the diversity of samples through pseudo-labels and does not fully exploit the supervision information of pseudo-labels, resulting in relatively low performance.

Table 2: Cross-domain results on datasets UNSW-NB15 and ToN-IoT

Algorithm	UNSW-NB15(source domain) ToN-IoT(target domain)
CDAN	53.00%
DCAN	46.00%
GDCAN	51.00%
DAR	57.00%
ABRSI	70.00%
DDA	71.30%
WCGN	74.00%
GGA	79.00%
Proposed algorithm	**89.73%**

Table 3: Cross-domain results on datasets NSL-KDD and BoT-IoT

Algorithm	NSL-KDD(source domain) BoT-IoT(target domain)
CDAN	37.00%
DCAN	40.00%
GDCAN	39.00%
DAR	42.00%
ABRSI	51.00%
DDA	40.70%
WCGN	58.30%
GGA	75.70%
Proposed algorithm	**84.10%**

The GGA algorithm organizes class relationships as a geometric graph and generates pseudo-labels based on geometric properties and neighborhood information. Its F1-scores in the two groups of experiments reach 79.00% and 75.70%, respectively, showing the best performance among the baseline algorithms used in this paper. However, the class imbalance problem is not considered by GGA, and no threshold mechanism is introduced to improve the accuracy of pseudo-label prediction. In contrast, GAN and class separation loss are used in the proposed method to address source domain class imbalance and class overlap during pseudo-label generation. Meanwhile, a dynamic threshold mechanism is adopted to adapt to class imbalance in the target domain and select high-confidence data with more discriminative information, thereby enhancing the effectiveness of knowledge transfer. In addition, GGA mainly aligns class relationships across different domains from the perspective of class geometric graphs. Cross-domain knowledge transfer is achieved by preserving graph shapes, avoiding rotational misalignment, and matching center points. However, the differences in feature dependency structures among samples of the same class in the source domain and the target domain are not explicitly modeled. In contrast, the proposed algorithm considers not only the dependency structure between features and the overall distribution, but also enables the model to focus on important factors that cause distribution shifts. Meanwhile, both the local relative structure and the global structure of class prototypes are considered, making the decision boundary more robust.

Compared with GGA, the F1-scores of the proposed algorithm are improved by 10.73% and 8.40% in the two cross-domain tasks, respectively. This demonstrates that, in cross-domain intrusion detection scenarios where class imbalance and distribution shift coexist, relying only on class geometric relationship alignment is still insufficient to fully ensure the detection performance in the target domain. The proposed method improves the reliability of pseudo-labels through class-balanced knowledge transfer and enhances the ability of domain-invariant feature learning by combining feature dependency structure alignment with class prototype structure alignment. Therefore, a more robust classification decision boundary and more stable target domain detection results can be obtained.

4.5 Ablation experiments

The ablation experiments are designed to evaluate the validity of the components of the proposed algorithm. The UNSW-NB15, NSL-KDD are used as the source domains and the ToN-IoT, BoT-IoT as the target domains, the results are shown in Table 4.

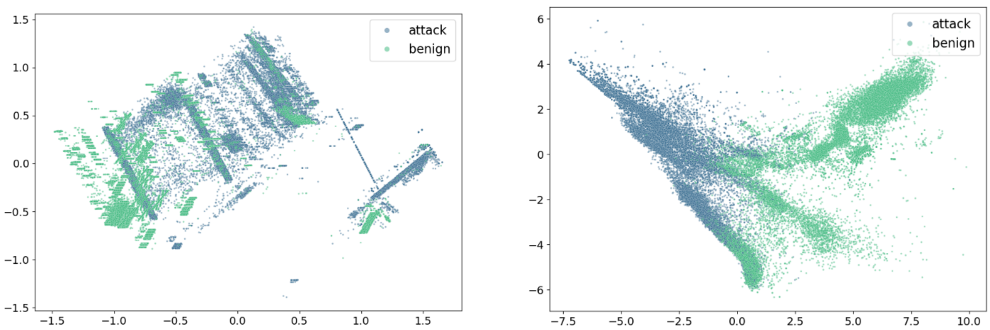
(1) A domain adversarial network;
(2) Only the class-balanced knowledge transfer network is added to the domain adversarial network;
(3) Only the multi-structure domain alignment is added to the domain adversarial network;
(4) The complete algorithm proposed in this paper.

Table 4: Ablation experiments

Experiment	Source domain	Target domain	F1-Score
(1)	UNSW-NB15	ToN-IoT	55.28%
	NSL-KDD	BoT-IoT	58.66%
(2)	UNSW-NB15	ToN-IoT	86.47%
	NSL-KDD	BoT-IoT	80.79%
(3)	UNSW-NB15	ToN-IoT	83.27%
	NSL-KDD	BoT-IoT	81.48%
(4)	UNSW-NB15	ToN-IoT	89.73%
	NSL-KDD	BoT-IoT	84.10%

Experiment (1) contains only a domain-adversarial network, and its F1-scores in the two groups of experiments are only 55.28% and 58.66%, respectively. This indicates that a single domain adaptation model struggles to perform effective cross-domain intrusion detection in imbalanced scenarios. In Experiment (2), after introducing the class-balanced knowledge-transfer module, the F1-scores are improved from 55.28% to 86.47% and from 58.66% to 80.79% in the two cross-domain settings, respectively. This is because more reliable supervision is provided for domain adaptation by transferring class-balanced source domain knowledge and selecting high-confidence target domain samples, thereby improving the robustness of cross-domain intrusion detection.

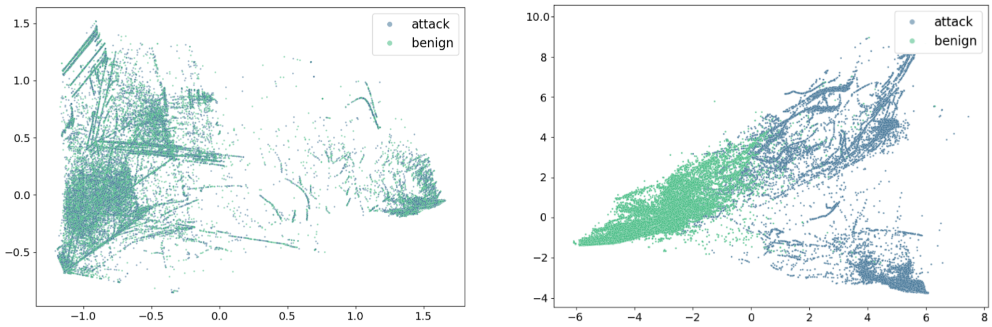
In order to further illustrate the effectiveness of the proposed method, two sets of experiments were first designed on the UNSW-NB15 and NSL-KDD datasets to verify the proposed class separation loss, and the results are shown in Figure 2 and Figure 3, respectively. In each set of figures, (a) represents the feature distribution before the application class separation loss, and (b) represents the feature distribution after the application. Different colors are used to represent different data categories, with blue representing attack data and green representing benign data.



(a) (b)

Fig. 2: Feature space distributions of attack and benign samples on UNSW-NB15 before and after applying the class separation loss. (a) Before the class separation loss is applied, multiple overlaps exist between the representation distributions of the two classes. (b) After the class separation loss is applied, the overlap between attack and benign samples is significantly reduced.

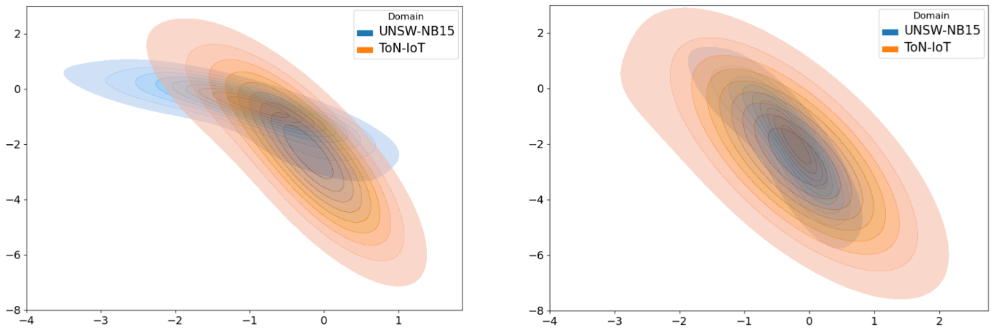
It can be clearly seen from the figure that after the application of class separation loss, the category boundary of the feature distribution becomes more obvious. Specifically, before the application class separation loss, the data points of the attack class and the benign class were often mixed together and indistinguishable, the class overlap problem was serious. However, after the application class separation loss, the data points of different categories are obviously separated, forming a clearer clustering effect. This result fully demonstrates the effectiveness of class separation loss in improving the ability of models to distinguish different classes. In addition, in order to ensure the effectiveness of class separation loss in cross-domain tasks, entropy regularization term is introduced into the model. Figure 4 and Figure 5 show the density distribution of model output before and after applying entropy regularization in different cross-domain scenarios. In each set of figures, (a) represents the output distribution before applying entropy regularization, and (b) represents the output distribution after



(a) (b)

Fig. 3: Feature space distributions of attack and benign samples on NSL-KDD before and after applying the class separation loss. (a) Before the class separation loss is applied, multiple overlaps exist between the representation distributions of the two classes. (b) After the class separation loss is applied, the overlap between attack and benign samples is significantly reduced.

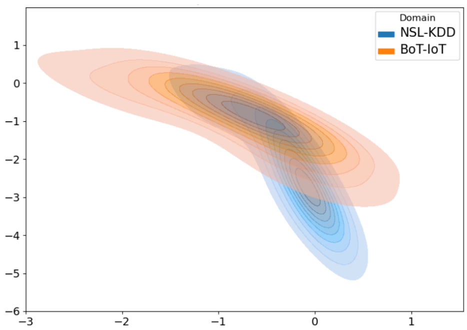
applying entropy regularization. Blue represents the output distribution density of the source domain, and orange represents the output distribution density of the target domain.



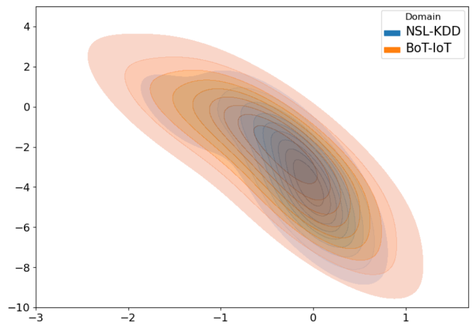
(a) (b)

Fig. 4: Dependence structure absolute difference, the source domain is UNSW-NB15 and the target domain is ToN-IoT.

It can be clearly seen from the figure that after applying entropy regularization, the output distributions of the source domain and the target domain become more close and consistent. This change enables the source domain class separation knowledge learned through class separation loss to be shared among different domains, thus further promoting the class-balanced knowledge transfer.



(a)



(b)

Fig. 5: Dependence structure absolute difference, the source domain is NSL-KDD and the target domain is BoT-IoT.

In Experiment (3), after adding multi-structure domain alignment, the F1-scores are improved from 55.28% to 83.27% and from 58.66% to 81.48% in the two cross-domain settings, respectively. This is because the decision boundary of the source domain is generalized to the target domain through multi-structure alignment of class prototypes, thereby further improving the cross-domain intrusion detection performance of the model.

To further verify this result, two sets of experiments are designed for the proposed dependence structure alignment algorithm. The copula entropy is used to capture the dependence structures of different domain features with and without the alignment algorithm, and the absolute difference between them is calculated to compare their variation trends. Figure 6 and Figure 7 show the absolute difference of copula entropy of feature extractor for features output in different domains during the training process, and the horizontal coordinate represents the training progress. In the figure, the blue line represents the result without using the alignment algorithm, while the red dashed line represents the result with the alignment algorithm.

After applying the dependence structure alignment algorithm, the copula entropy difference between different domains decreases significantly with the continuous training of the model. This phenomenon shows that the proposed algorithm can effectively reduce the dependence structure difference between different domain features, which is helpful for the model to capture domain invariant features to improve the model performance.

In order to evaluate the proposed supervised class prototype discovery algorithm, two sets of experiments are designed and compared respectively in the scenario of random initialization of class prototype and pseudo label initialization of class prototype. The experimental results are shown in Table 5.

As expected, in different cross-domain scenarios, the models using pseudo label to initialize class prototypes show better performance. This advantage stems from the fact that pseudo label can effectively utilize the inherent structure and information of the data, thus providing a more favorable starting point for the model. In addition,

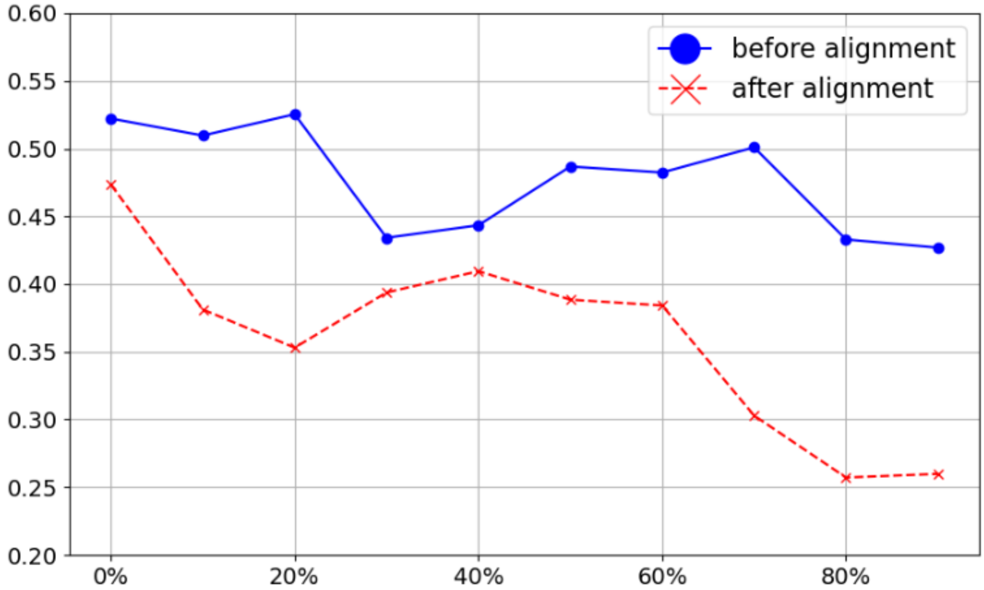


Fig. 6: Dependence structure absolute difference, the source domain is UNSW-NB15 and the target domain is ToN-IoT.

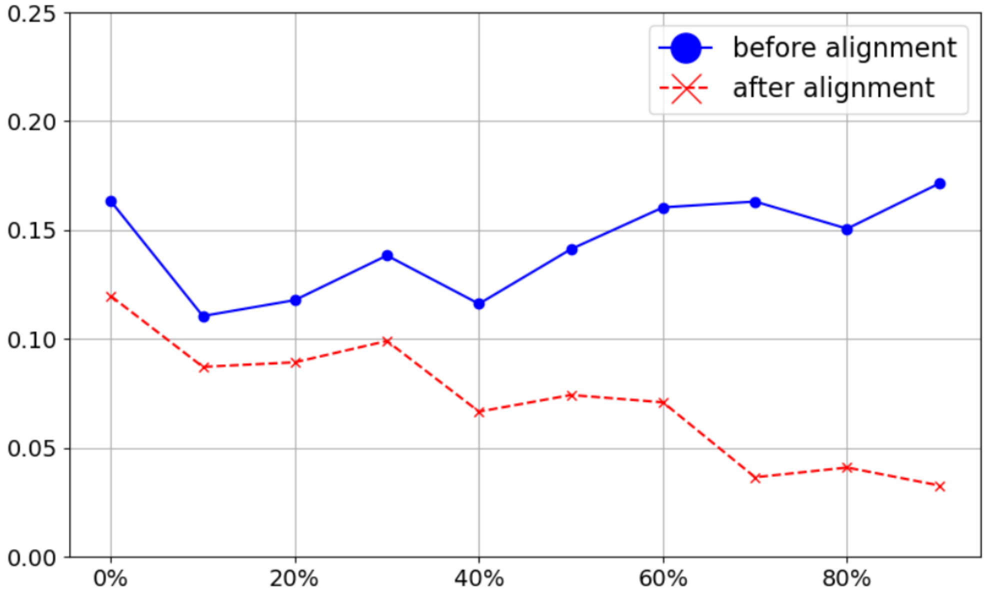


Fig. 7: Dependence structure absolute difference, the source domain is NSL-KDD and the target domain is BoT-IoT.

Table 5: Comparison of different class prototype initialization methods

	random initialization	pseudo label initialization
UNSW-NB15->ToN-IoT	82.85%	89.73%
NSL-KDD->BoT-IoT	81.87%	84.10%

this initialization method can not only shorten the training time, but also avoid the overfitting problem to a large extent, so that the model has stronger generalization ability.

Although the cross-domain capability of the model is improved after adding the multi-structure domain alignment, it is still affected by the class imbalance data. In Experiment (4), after both the class-balanced knowledge transfer module and multi-structure domain alignment are introduced, higher-quality pseudo-labels of the target domain are obtained, and more stable domain-invariant feature representations are learned. As a result, the robustness of the classification decision boundary in cross-domain intrusion detection scenarios is improved, leading to a further improvement in the performance of the model.

5 Conclusion

To solve the problem of class imbalance and distribution shift of current network intrusion detection systems, this paper proposes a network intrusion detection algorithm based on class-balanced knowledge transfer and multi-structure domain alignment. A class-balanced knowledge transfer network is proposed to alleviate the influence of class imbalance data on domain shift. For distribution shift, a multi-structure domain alignment is proposed, which makes a more robust decision boundary for the classifier by aligning feature dependence structure and class-prototype relative structure, and combining the domain-adversarial network. The comparative experiments show that the proposed algorithm can effectively improve the cross-domain capability of network intrusion detection system in the face of imbalanced domain and complex network environment. The ablation experiments show that all the components can effectively improve the cross-domain capability of network intrusion detection systems.

CRediT authorship contribution statement

Qian Wang: Supervision, Conceptualization, Writing - review & editing. **Xiang Liu**: Conceptualization, Methodology, Writing - original draft, Software. **Yuantong Wei**: Data curation. **YiFan Cheng**: Supervision. **Bing Zhang**: Validation, Writing - review & editing. **Yongqiang Cheng**: Investigation.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

Data will be made available on request.

Acknowledgments

This work is supported by the National Natural Science Foundation of China [grant number 62376240]. the S&T Program of Hebei [grant number 236Z0304G]. The authors are grateful to valuable comments and suggestions of the reviewers.

References

[1] Wang, Q., Jiang, H., Ren, J., Liu, H., Wang, X., Zhang, B.: An intrusion detection algorithm based on joint symmetric uncertainty and hyperparameter optimized fusion neural network. Expert Syst. Appl. **244**, 123014 (2024) https://doi.org/10.1016/J.ESWA.2023.123014

[2] Moustafa, N., Slay, J.: Unsw-nb15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). In: 2015 Military Communications and Information Systems Conference, MilCIS 2015, Canberra, Australia, November 10-12, 2015, pp. 1–6 (2015). https://doi.org/10.1109/MILCIS.2015.7348942

[3] Stolfo, S.J., Fan, W., Lee, W., Prodromidis, A.L., Chan, P.: KDD Cup 1999 Data. UCI Machine Learning Repository. Accessed on YYYY-MM-DD. (1998). https://doi.org/10.24432/C51C7N

[4] Kim, J.H., Ngo, B.H., Park, J.H., Kwon, J.E., Lee, H.S., Cho, S.I.: Distilling and refining domain-specific knowledge for semi-supervised domain adaptation. In: Bmvc, p. 606 (2022)

[5] Ngo, B.H., Chae, Y.J., Kwon, J.E., Park, J.H., Cho, S.I.: Improved knowledge transfer for semi-supervised domain adaptation via trico training strategy. In: Proceedings of the IEEE/CVF International Conference on Computer Vision (ICCV), pp. 19214–19223 (2023)

[6] Yao, Y., Zhang, Y., Li, X., Ye, Y.: Discriminative distribution alignment: A unified framework for heterogeneous domain adaptation. Pattern Recognit. **101**, 107165 (2020) https://doi.org/10.1016/J.PATCOG.2019.107165

[7] Wang, Z., Luo, Y., Huang, Z., Baktashmotlagh, M.: Prototype-matching graph network for heterogeneous domain adaptation. In: Chen, C.W., Cucchiara, R., Hua, X., Qi, G., Ricci, E., Zhang, Z., Zimmermann, R. (eds.) MM '20: The 28th ACM International Conference on Multimedia, Virtual Event / Seattle, WA, USA, October 12-16, 2020, pp. 2104–2112 (2020). https://doi.org/10.1145/3394171.3413662

[8] Wu, J., Dai, H., Wang, Y., Ye, K., Xu, C.: Heterogeneous domain adaptation for iot intrusion detection: A geometric graph alignment approach. IEEE Internet Things J. **10**(12), 10764–10777 (2023) https://doi.org/10.1109/JIOT.2023.3239872

[9] Li, S., Liu, C.H., Lin, Q., Xie, B., Ding, Z., Huang, G., Tang, J.: Domain conditioned adaptation network. In: The Thirty-Fourth AAAI Conference on Artificial Intelligence, AAAI 2020, The Thirty-Second Innovative Applications of Artificial Intelligence Conference, IAAI 2020, The Tenth AAAI Symposium on Educational Advances in Artificial Intelligence, EAAI 2020, New York, NY, USA, February 7-12, 2020, pp. 11386–11393 (2020). https://doi.org/10.1609/AAAI.V34I07.6801

[10] Li, S., Xie, B., Lin, Q., Liu, C.H., Huang, G., Wang, G.: Generalized domain conditioned adaptation network. IEEE Trans. Pattern Anal. Mach. Intell. **44**(8), 4093–4109 (2022) https://doi.org/10.1109/TPAMI.2021.3062644

[11] Yuan, F., Yao, L., Benatallah, B.: Darec: Deep domain adaptation for cross-domain recommendation via transferring rating patterns. In: Kraus, S. (ed.) Proceedings of the Twenty-Eighth International Joint Conference on Artificial Intelligence, IJCAI 2019, Macao, China, August 10-16, 2019, pp. 4227–4233 (2019). https://doi.org/10.24963/IJCAI.2019/587

[12] Ngo, B.H., Chae, Y.J., Park, J.H., Kim, J.H., Cho, S.I.: Easy-to-hard structure for remote sensing scene classification in multitarget domain adaptation. IEEE Transactions on Geoscience and Remote Sensing **61**, 1–15 (2023) https://doi.org/10.1109/TGRS.2023.3235886

[13] Chen, Z., Yu, W., Wang, L., Ding, X., Huang, W., Shao, Y.: A dual-view style mixing network for unsupervised cross-domain fault diagnosis with imbalanced data. Knowl. Based Syst. **278**, 110918 (2023) https://doi.org/10.1016/J.KNOSYS.2023.110918

[14] Ding, Y., Jia, M., Zhuang, J., Cao, Y., Zhao, X., Lee, C.: Deep imbalanced domain adaptation for transfer learning fault diagnosis of bearings under multiple working conditions. Reliab. Eng. Syst. Saf. **230**, 108890 (2023) https://doi.org/10.1016/J.RESS.2022.108890

[15] Xia, H., Jing, T., Ding, Z.: Generative inference network for imbalanced domain generalization. IEEE Trans. Image Process. **32**, 1694–1704 (2023) https://doi.org/10.1109/TIP.2023.3251103

[16] Zhao, C., Shen, W.: Imbalanced domain generalization via semantic-discriminative augmentation for intelligent fault diagnosis. Adv. Eng. Informatics **59**, 102262 (2024) https://doi.org/10.1016/J.AEI.2023.102262

[17] Yuan, L., Siyal, M.Y.: Target-oriented augmentation privacy-protection domain

adaptation for imbalanced ECG beat classification. Biomed. Signal Process. Control. **86**(Part C), 105308 (2023) https://doi.org/10.1016/J.BSPC.2023.105308

[18] Ganin, Y., Ustinova, E., Ajakan, H., Germain, P., Larochelle, H., Laviolette, F., Marchand, M., Lempitsky, V.S.: Domain-adversarial training of neural networks. J. Mach. Learn. Res. **17**, 59–15935 (2016)

[19] Ma, W., Liu, R., Li, K., Yan, S., Guo, J.: An adversarial domain adaptation approach combining dual domain pairing strategy for iot intrusion detection under few-shot samples. Inf. Sci. **629**, 719–745 (2023) https://doi.org/10.1016/J.INS.2023.02.031

[20] Chen, Y., Su, S., Yu, D., He, H., Wang, X., Ma, Y., Guo, H.: Cross-domain industrial intrusion detection deep model trained with imbalanced data. IEEE Internet Things J. **10**(1), 584–596 (2023) https://doi.org/10.1109/JIOT.2022.3201888

[21] Long, M., Cao, Z., Wang, J., Jordan, M.I.: Conditional adversarial domain adaptation. In: Bengio, S., Wallach, H.M., Larochelle, H., Grauman, K., Cesa-Bianchi, N., Garnett, R. (eds.) Advances in Neural Information Processing Systems 31: Annual Conference on Neural Information Processing Systems 2018, NeurIPS 2018, December 3-8, 2018, Montréal, Canada, pp. 1647–1657 (2018)

[22] Wu, J., Wang, Y., Dai, H., Xu, C., Kent, K.B.: Adaptive bi-recommendation and self-improving network for heterogeneous domain adaptation-assisted iot intrusion detection. IEEE Internet Things J. **10**(15), 13205–13220 (2023) https://doi.org/10.1109/JIOT.2023.3262458

[23] Jiang, Z., Li, Y., Yang, C., Gao, P., Wang, Y., Tai, Y., Wang, C.: Prototypical contrast adaptation for domain adaptive semantic segmentation. In: Avidan, S., Brostow, G., Cissé, M., Farinella, G.M., Hassner, T. (eds.) Computer Vision – ECCV 2022, Cham, pp. 36–54 (2022)

[24] Ding, H., Sun, Y., Huang, N., Shen, Z., Cui, X.: TMG-GAN: generative adversarial networks-based imbalanced learning for network intrusion detection. IEEE Trans. Inf. Forensics Secur. **19**, 1156–1167 (2024) https://doi.org/10.1109/TIFS.2023.3331240

[25] Arjovsky, M., Chintala, S., Bottou, L.: Wasserstein generative adversarial networks. In: Precup, D., Teh, Y.W. (eds.) Proceedings of the 34th International Conference on Machine Learning, ICML 2017, Sydney, NSW, Australia, 6-11 August 2017. Proceedings of Machine Learning Research, vol. 70, pp. 214–223 (2017)

[26] Saito, K., Kim, D., Sclaroff, S., Saenko, K.: Universal domain adaptation through self supervision. In: Larochelle, H., Ranzato, M., Hadsell, R., Balcan, M., Lin, H. (eds.) Advances in Neural Information Processing Systems 33: Annual Conference on Neural Information Processing Systems 2020, NeurIPS 2020, December 6-12,

2020, Virtual (2020)

[27] Ru, J., Tian, J., Xiao, C., Li, J., Shen, H.T.: Imbalanced open set domain adaptation via moving-threshold estimation and gradual alignment. IEEE Trans. Multim. **26**, 2504–2514 (2024) https://doi.org/10.1109/TMM.2023.3297768

[28] Ma, S., Yuan, Z., Wu, Q., Huang, Y., Hu, X., Leung, C.H., Wang, D., Huang, Z.: Deep into the domain shift: Transfer learning through dependence regularization. CoRR **abs/2305.19499** (2023) https://doi.org/10.48550/ARXIV.2305.19499 2305.19499

[29] Ma, J., Sun, Z.: Mutual information is copula entropy. CoRR **abs/0808.0845** (2008) 0808.0845

[30] Tran, C.D., Rudovic, O.O., Pavlovic, V.: Unsupervised domain adaptation with copula models. In: Ueda, N., Watanabe, S., Matsui, T., Chien, J., Larsen, J. (eds.) 27th IEEE International Workshop on Machine Learning for Signal Processing, MLSP 2017, Tokyo, Japan, September 25-28, 2017, pp. 1–6 (2017). https://doi.org/10.1109/MLSP.2017.8168131

[31] Zhou, L., Li, N., Ye, M., Zhu, X., Tang, S.: Source-free domain adaptation with class prototype discovery. Pattern Recognit. **145**, 109974 (2024) https://doi.org/10.1016/J.PATCOG.2023.109974

[32] Koroniotis, N., Moustafa, N., Sitnikova, E., Turnbull, B.P.: Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: Bot-iot dataset. Future Gener. Comput. Syst. **100**, 779–796 (2019) https://doi.org/10.1016/J.FUTURE.2019.05.041

[33] Alsaedi, A., Moustafa, N., Tari, Z., Mahmood, A.N., Anwar, A.: Ton_iot telemetry dataset: A new generation dataset of iot and iiot for data-driven intrusion detection systems. IEEE Access **8**, 165130–165150 (2020) https://doi.org/10.1109/ACCESS.2020.3022862