ADMoE: Anomaly Detection with Mixture-of-Experts from Noisy Labels

Yue Zhao\textsuperscript{1*}, Guoqing Zheng\textsuperscript{2}, Subhadrata Mukherjee\textsuperscript{2}, Robert McCann\textsuperscript{2}, Ahmed Awadallah\textsuperscript{2}

\textsuperscript{1}Carnegie Mellon University, \textsuperscript{2}Microsoft
zhao@cmu.edu, \{zheng, submukhe, robmccan, hassanam\}@microsoft.com

Abstract
Existing works on anomaly detection (AD) rely on clean labels from human annotators that are expensive to acquire in practice. In this work, we propose a method to leverage weak/noisy labels (e.g., risk scores generated by machine rules for detecting malware) that are cheaper to obtain for anomaly detection. Specifically, we propose ADMoE, the first framework for anomaly detection algorithms to learn from noisy labels. In a nutshell, ADMoE leverages Mixture-of-experts (MoE) architecture to encourage specialized and scalable learning from multiple noisy sources. It captures the similarities among noisy labels by sharing most model parameters, while encouraging specialization by building “expert” sub-networks. To further juice out the signals from noisy labels, ADMoE uses them as input features to facilitate expert learning. Extensive results on eight datasets (including a proprietary enterprise security dataset) demonstrate the effectiveness of ADMoE, where it brings up to 34% performance improvement over not using it. Also, it outperforms a total of 13 leading baselines with equivalent network parameters and FLOPS. Notably, ADMoE is model-agnostic to enable any neural network-based detection methods to handle noisy labels, where we showcase its results on both multiple-layer perceptron (MLP) and leading AD method DeepSAD.

1 Introduction
Anomaly detection (AD), also known as outlier detection, is a crucial learning task with many real-world applications, including malware detection (Nguyen et al. 2019), anti-money laundering (Lee et al. 2020), rare-disease detection (Li et al. 2018) and so on. Although there are numerous detection algorithms (Aggarwal 2013; Pang et al. 2021; Zhao, Rossi, and Akoglu 2021; Liu et al. 2022), existing AD methods assume the availability of (partial) labels that are clean (i.e. without noise), and cannot learn from weak/noisy labels\footnote{The project is primarily done at Microsoft Research. Copyright © 2023, Association for the Advancement of Artificial Intelligence (www.aaai.org). All rights reserved.}.

Simply treating noisy labels as (pseudo) clean labels leads to biased and degraded models (Song et al. 2022). Over the years, researchers have developed algorithms for classification and regression tasks to learn from noisy sources (Rodrigues and Pereira 2018; Guan et al. 2018; Wei et al. 2022), which has shown great success. However, these methods are not tailored for AD with extreme data imbalance, and existing AD methods cannot learn from (multiple) noisy sources.

Why is it important to leverage noisy labels in AD applications? Taking malware detection as an example, it is impossible to get a large number of clean labels due to the data sensitivity and the cost of annotation. However, often there exists a large number of weak/noisy historical security rules designed for detecting malware from different perspectives, e.g., unauthorized network access and suspicious file movement, which have not been used in AD yet. Though not as perfect as human annotations, they are valuable as they encode prior knowledge from past detection experiences. Also, although each noisy source may be insufficient for difficult AD tasks, learning them jointly may build competitive models as they tend to complement each other.

In this work, we propose ADMoE, (to our knowledge) the first weakly-supervised approach for enabling anomaly detection algorithms to learn from multiple sets of noisy labels. In a nutshell, ADMoE enhances existing neural-network-based AD algorithms by Mixture-of-experts (MoE) network(s) (Jacobs et al. 1991; Shazeer et al. 2017), which has a learnable gating function to activate different sub-networks (experts) based on the incoming samples and their noisy labels. In this way, the proposed ADMoE can jointly learn from multiple sets of noisy labels with the majority of parameters shared, while providing specialization and scal-
ability via experts. Unlike existing noisy label learning approaches, ADMoE does not require explicit mapping from noisy labels to network parameters, providing better scalability and flexibility. To encourage ADMoE to develop specialization based on the noisy sources, we use noisy labels as (part of the) input features with learnable embeddings to make the gating function aware of them.

**Key Results.** Fig. 1 shows that a multiple layer perception (MLP) (Rosenblatt 1958) enhanced by ADMoE can largely outperform both (1a) leading AD algorithms as well as (1b) noisy-label learning methods for classification. Note ADMoE is not strictly another detection algorithm, but a general framework to empower any neural-based AD methods to leverage multiple sets of weak labels. §4 shows extensive results on more datasets, and the improvement in enhancing more complex DeepSAD (Ruff et al. 2019) with ADMoE.

In summary, the key contributions of this work include:

- **Problem formulation, baselines, and datasets.** We formally define the crucial problem of using multiple sets of noisy labels for AD (MNLAD), and release the first batch of baselines and datasets for future research.

- **The first AD framework for learning from multiple noisy sources.** The proposed ADMoE is a novel method with Mixture-of-experts (MoE) architecture to achieve specialized and scalable learning for MNLAD.

- **Model-agnostic design.** ADMoE enhances any neural-network-based AD methods, and we show its effectiveness on MLP and state-of-the-art (SOTA) DeepSAD.

- **Effectiveness and real-world deployment.** We demonstrate ADMoE’s SOTA performance on seven benchmark datasets and a proprietary enterprise security application, in comparison with two groups of leading baselines (13 in total). It brings on average 14% and up to 34% improvement over not using it, with the equivalent number of learnable parameters and FLOPs as baselines.

## 2 Related Work

### 2.1 Weakly-supervised Anomaly Detection

There exists some literature on weakly-supervised AD, and most of them fall under the “incomplete supervision” category. These semi-supervised methods assume access to a small set of clean labels and it is unclear how to extend them for multi-set noisy labels. Representative work includes XG-BOD (Zhao and Hryniewicki 2018), DeepSAD (Ruff et al. 2019), DevNet (Pang, Shen, and van den Hengel 2019), PreNet (Pang et al. 2019); see Appx. B.2 for more details.

We use these leading methods (that work with one set of labels) as baselines in §4.2, and demonstrate ADMoE’s performance gain in leveraging multiple sets of noisy labels.

### 2.2 Learning from Single Set of Noisy Labels

There have been rich literature on learning from a single set of noisy labels, including learning a label corruption/transition matrix (Patrini et al. 2017), correcting labels via meta-learning (Zheng, Awadallah, and Dumais 2021), and building robust training mechanisms like co-teaching (Han et al. 2018), co-teaching+ (Yu et al. 2019), and JoCoR (Wei et al. 2020). More details can be found in a recent survey (Han et al. 2020). These algorithms are primarily for a single set of noisy labels, and are not designed for AD tasks.

## 2.3 Learning from Multiple Noisy Sources

### Table 1: Baselines and ADMoE for comparison with categorization by (first row) whether it uses multiple sets of weak labels, (second row) whether it only trains a single model, (third row) whether the training process is end-to-end and (the last row) whether it is scalable with regard to many sets of weak labels. ADMoE is an end-to-end, scalable paradigm.

MNLAD falls under weakly supervised ML (Zhou 2018), where it deals with multiple sets of inaccurate/noisy labels. Naturally, one can aggregate noisy labels to generate a “corrected” label set (Zheng, Awadallah, and Dumais 2021), while it may be challenging for AD with extreme data imbalance. Other than label correction, one may take ensembling to train multiple independent AD models for combination, e.g., one model per set of noisy labels, which however faces scalability issues while dealing with many sets of labels. What is worse, independently trained models fail to explore the interaction among noisy labels. Differently, end-to-end noisy label learning methods, including Crowd Layer (Rodrigues and Pereira 2018), DoctorNet (Guan et al. 2018), and UnionNet (Wei et al. 2022), can directly learn from multiple sets of noisy labels and map each set of noisy labels to part of the network (e.g., transition matrix), encouraging the model to learn knowledge from all noisy labels collectively. Although they yield great performance in crowd-sourcing scenarios with a small number of annotators, they do not scale in MNLAD with many sets of “cheap” noisy labels due to this explicit one-to-one mapping. Also, each set of noisy AD labels may be only good at certain anomalies as a biased annotator. Consequently, explicitly one-to-one mapping (e.g., transition matrix) from a single set of labels to a network in existing classification works is not ideal for MNLAD. ADMoE lifts this constraint to allow many-to-many mapping, improving model scalability and robustness for MNLAD.

We summarize the methods for learning from multiple sources of noisy labels in Table 1 categorized as: (1) SingleNoisy trains an AD model using only one set of weak labels, which sets the lower bound of all baselines. (2) LabelVote trains an AD model based on the consensus of weak labels via majority vote. (3) HyperEnsemble (Wenzel et al. 2020) trains an individual model for each set of noisy labels (i.e., \( k \) models for \( k \) sets of labels), and combines their anomaly scores by averaging (i.e., HE_A) and maximizing (i.e., HE_M). (4) CrowdLayer (Rodrigues and Pereira 2018) tries to reconstruct the input weak labels during training. (5) UnionNet (Wei et al. 2022) learns a transition matrix for all weak labels together. Note that they are primarily for classification and not tailored for anomaly detection. Nonetheless, we adopt the methods in Table 1 as baselines. In §4.3, we show ADMoE outperforms all these methods.
3 AD from Multiple Sets of Noisy Labels

In §3.1, we formally present the problem of AD with multiple sets of noisy labels, followed by the discussion on why multiple noisy sources help AD in §3.2. Motivated by above, we describe the proposed ADMoE framework in §3.3.

3.1 Problem Statement

We consider the problem of anomaly detection with multiple sets of weak/noisy labels. We refer to this problem as MNLAD, an acronym for using multiple sets of noisy labels for anomaly detection. We present the problem definition here.

Problem 1 (MNLAD): Given an anomaly detection task with input feature \( \mathbf{X} \in \mathbb{R}^{n \times d} \) (e.g., \( n \) samples and \( d \) features) and \( t \) sets of noisy/weak labels \( \mathcal{Y}_w = \{ \mathcal{Y}_{w,1}, \ldots, \mathcal{Y}_{w,t} \} \) (each in \( \mathbb{R}^n \)), build a detection model \( M \) to leverage all information to achieve the best performance.

Existing AD methods (Aggarwal 2013; Pang et al. 2021; Han et al. 2022) can (at best) treat one set of noisy labels from \( \mathcal{Y}_w \) as (pseudo) clean labels to train a model. None of them leverages multiple sets of noisy labels \( \mathcal{Y}_w \) collectively.

3.2 Why and How Do Multiple Sets of Weak Labels Help in Anomaly Detection?

Benefits of joint learning in MNLAD. AD benefits from model combination and ensemble learning from diverse base models (Aggarwal and Sathe 2017; Zhao et al. 2019; Ding, Zhao, and Akoglu 2022), and the improvement is expected when base models make complementary errors (Zimek, Campello, and Sander 2014; Aggarwal and Sathe 2017). Multiple sets of noisy labels are natural sources for ensembling with built-in diversity, as they reflect distinct detection aspects and historical knowledge. Appx. A Fig. A1 shows that averaging the outputs from multiple AD models (each trained on one set of noisy labels) leads to better results than training each model independently; this observation holds true for both deep (neural) AD models (e.g., PreNet in Appx. Fig. A1a) and shallow models (e.g., XGBOD in Appx. Fig. A1b). This example justifies the benefit of learning from multiple sets of noisy labels; even simple averaging in MNLAD can already “touch” the performance upper bound (i.e., training a model using all clean labels).

3.3 ADMoE: Specialized and Scalable Anomaly Detection with Multiple Sets of Noisy Labels

Motivation. After reviewing gaps and opportunities in existing works, we argue the ideal design for MNLAD should fulfill the following requirements: (i) encourage specialization from different noisy sources but also explore their similarity (ii) scalability to handle an increasing number of noisy sources and (iii) generality to apply to various AD methods.

Overview of ADMoE. In this work, (for the first time) we adapt mixture-of-experts (MoE) architecture/layer (Jacobs et al. 1991; Shazeer et al. 2017) (see preliminary in §3.3.1) to AD algorithm design for MNLAD. Specifically, we propose model-agnostic ADMoE\(^3\) to enhance any neural network-based AD method via: (i) mixture-of-experts (MoE) layers to do specialized and scalable learning from noisy labels and (ii) noisy-label aware expert activation by using noisy labels as (part of the) input with learnable embedding to facilitate specialization. Refer to Fig. 2c for an illustration of applying ADMoE to a simple MLP, where we add an ADMoE layer between the dense layers and output layer for MNLAD, and use noisy labels directly as input with learnable embedding to help ADMoE to better specialize. Other neural-network-based AD methods can follow the same procedure to be enhanced by ADMoE (i.e., inserting ADMoE layers before the output layer and using noisy labels as input). In the following subsections, we give a short background of MoE and then present the design of ADMoE.

3.3.1 Preliminary on Mixture-of-experts (MoE) Architecture.

The original MoE (Jacobs et al. 1991) is designed as a dynamic learning paradigm to allow different parts (i.e., experts) of a network to specialize for different samples. More recent (sparsely-gated) MoE (Shazeer et al. 2017) has been shown to improve model scalability for natural language processing (NLP) tasks, where models can have billions of parameters (Du et al. 2022). The key difference between the original MoE and the sparse MoE is the latter builds more experts (sub-networks) for a large model but only activates a few of them for scalability and efficiency.

Basically, MoE splits specific layer(s) of a (large) neural network into \( m \) “small” experts (i.e., sub-networks). It uses top-\( k \) gating to activate \( k \) experts (\( k < m \)) for sparse MoE for each input sample computation as opposed to using the entire network as a single expert. MoE uses a differentiable gating function \( G(\cdot) \) to calculate the activation weights of each expert. It then aggregates the weighted outputs of the top-\( k \) experts with the highest activation weights as the MoE layer output. For example, the expert weights \( \beta^l \in \mathbb{R}^m \) of the \( j \)-th sample is a function of input data by the gating \( G(\cdot) \), i.e., \( \beta^j = G(\mathbf{X}^j) \).

Till now, MoE has been widely used in multi-task learning (Zheng et al. 2019), video captioning (Wang et al. 2019), and multilingual neural machine translation (NMT) (Dai et al. 2022) tasks. Taking NMT as an example, prior work (Dai et al. 2022) shows that MoE can help learn a model from diverse sources (e.g., different languages), where they share the most common parameters but also specialize for individual source via “experts” (sub-networks). We combine the strengths of original and sparse MoE for our ADMoE.

3.3.2 Capitalizing Mixture-of-experts (MoE) Architecture for MNLAD.

It is easy to see the connection between MoE’s applications (e.g., multilingual machine translation) and MNLAD—in both cases MoE can help learn from diverse sources (e.g., multiple sets of noisy labels in MNLAD) to capture the similarity via parameter sharing while encouraging specialization via expert learning.

By recognizing this connection, we (for the first time), introduce MoE architecture for weakly supervised AD with noisy labels (i.e., MNLAD), called ADMoE. Similar to other works that use MoE, proposed ADMoE keeps (does not alter) an (AD) algorithm’s original layers before the output layer (e.g., dense layers in an MLP) to explore the agreement among noisy sources via shared parameters, while in-
Dense
Layers
X
Inputs
Output
Layer
Crowd
Layer
Nosiy 𝑦𝑤,1
Nosiy 𝑦𝑤,2
Nosiy 𝑦𝑤,3ො𝑦

(a) Crowd Layer (Rodrigues 2018)  (b) Union Net (Wei et al. 2022)  (c) ADMoE (ours) leverages MoE layers for specialization

Figure 2: A toy example of a 3-layer MLP for AD; 3 sets of noisy labels $\mathbf{y}^w = \{\mathbf{y}^w_1, \mathbf{y}^w_2, \mathbf{y}^w_3\}$ are assumed. Existing methods ($a$ and $b$) learn to recover noisy labels explicitly, while ADMoE ($b$) uses an MoE architecture with noisy-label-aware expert activation to learn specialization from noisy sources without explicit label mapping. In the example, we add an ADMoE layer ($c$) between the dense layers and the output layer; only the top two experts ($a$) are activated for input samples.

Inserting an MoE layer before the output layer to learn from each noisy source with specialization (via the experts/sub-networks). In an ideal world, each expert is good at handling samples from different noisy sources and updated only with more accurate sets of noisy labels. As the toy example shown in Fig. 2c to apply ADMoE on an MLP for AD, we insert an ADMoE layer between the dense layers and the output layer: where the ADMoE layer contains four experts, and the gating activates only the top two for each input example.

For the $j$-th sample, the MoE layer’s output $O^j$ is shown in Eq. (1) as a weighted sum of all activated experts’ outputs, where $E_i(\cdot)$ denotes the $i$-th expert network, and $h^j$ is the output from the dense layer (as the input to ADMoE). $\beta^j_i$ is the weight of the $i$-th expert assigned by the gating function $G(\cdot)$, and we describe its calculation in Eq. (2). Although Eq. (1) enumerates all $m$ experts for aggregation, only the top-$k$ experts with non-negative weights $\beta^j_i > 0$ are used.

$$O^j = \sum_{i=1}^{m} \beta^j_i E_i(h^j)$$  \hspace{1cm} (1)

**Improving ADMoE with Noisy-Label Aware Expert Activation.** The original MoE calculates the activation weights with only the raw input feature $X$ (see §3.3.1), which can be improved in MNLAD with the presence of noisy labels. To such end, we explicitly make the gating function $G(\cdot)$ aware of noisy labels $\mathbf{y}^w$ while calculating the weights for (activating) experts. Intuitively, $t$ sets of noisy labels can be expressed as $t$-element binary vectors ($0$ means normalcy and $1$ means abnormality). However, it is hard for neural networks to directly learn binary inputs (Buckman et al. 2018). Thus, we propose to learn a $\mathbb{R}^{t \times e}$ continuous embedding $\text{Emb}(\cdot)$ for noisy labels ($e$ is embedding dimension), and use both the raw input features $X$ in $d$ dims and the average of the embedding in $e$ dims as the input of the gating. As such, the expert weights for the $j$-th sample $\beta^j$ can be calculated with Eq. (2), and plugged back into Eq. (1) for ADMoE output.

$$\beta^j = G(X^j, \text{Emb}(\mathbf{y}^w_j))$$  \hspace{1cm} (2)

**Loss Function.** ADMoE is strictly an enhancement framework for MNLAD other than a new detection algorithm, and thus we do not need to design a new loss function but just enrich the original loss $L_o$ of the underlying AD algorithm (e.g., cross-entropy for a simple MLP). While calculating the loss in each batch of data, we randomly sample one set of noisy labels treated as the (pseudo) clean labels or combine the loss of all $t$ sets of noisy labels by treating them as (pseudo) clean labels. To encourage all experts to be evenly activated and not collapse on a few of them (Riquelme et al. 2021), we include an additional loss term on gating (i.e., $L_g$). Putting these together, we show the loss for the $j$-th training sample in Eq. (3), where the first term encourages equal activation of experts with $\alpha$ as the load balancing factor, and the second part is the loss of the $j$-th sample, which depends on the MoE layer output $O^j$ in Eq. (1) and the corresponding noisy labels $\mathbf{y}^w_j$ (either one set or all in loss calculation).

$$L_j = \alpha L_g + L_o \left( O^j, \mathbf{y}^w_j \right)$$  \hspace{1cm} (3)

**Remark on the Number of ADMoE Layers and Sparsity.** Similar to the usage in NLP, one may use multiple ADMoE layers in an AD model (e.g., every other layer), especially for the AD models with complex structures like transformers (Li, Liu, and Jiao 2022). In this work, we only show inserting the ADMoE layer before the output layer (see the illustration in Fig. 2c) of MLP, while future work may explore more extensive use of ADMoE layers in complex AD models. As AD models are way smaller (Pang et al. 2021), we do not enforce gating sparsity as in NLP models (Shazeer et al. 2017). See ablution studies on the total number of experts and the number of activated experts in §4.4.3.

**3.3.3 Advantages and Properties of ADMoE**

**Implicit Mapping of Noisy Labels to Experts with Better Scalability.** The proposed ADMoE (Fig. 2c) is more scalable than existing noisy-label learning methods for classification, e.g., CrowdLayer (Fig. 2a) and UnionNet (Fig. 2b). As discussed in §2.3, these methods explicitly map each set of noisy labels to part of the network. With more sets of noisy labels, the network parameters designated for (recovering or mapping) noisy labels increase proportionately. In contrast, ADMoE does not enforce explicit one-to-one mapping from noisy labels to experts. Thus, its many-to-many mapping becomes more scalable with many noisy sources.

**Extension with Clean Labels.** Our design also allows for easy integration of clean labels. In many AD tasks, a small set of clean labels are feasible, where ADMoE can easily use them. No update is needed for the network design, but simply treating the clean label as “another set of noisy labels” with higher weights. See §4.4.4 for experiment results.
4 Experiments
We design experiments to answer the following questions:
1. How do ADMoE-enhanced methods compare to SOTA AD methods that learn from a single set of labels? (§4.2)
2. How does ADMoE compare to leading (multiple sets of) noisy label learning methods for classification? (§4.3)
3. How does ADMoE perform under different settings, e.g., varying num. of experts and clean label ratios? (§4.4)

4.1 Experiment Setting

<table>
<thead>
<tr>
<th>Data</th>
<th># Samples</th>
<th># Features</th>
<th># Anomaly</th>
<th>% Anomaly</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>ag news</td>
<td>14000</td>
<td>768</td>
<td>500</td>
<td>5.00</td>
<td>NLP</td>
</tr>
<tr>
<td>aloi</td>
<td>49534</td>
<td>27</td>
<td>1508</td>
<td>3.04</td>
<td>Image</td>
</tr>
<tr>
<td>mnist</td>
<td>7603</td>
<td>100</td>
<td>700</td>
<td>9.21</td>
<td>Image</td>
</tr>
<tr>
<td>spambase</td>
<td>4207</td>
<td>57</td>
<td>1679</td>
<td>39.91</td>
<td>Doc</td>
</tr>
<tr>
<td>svhn</td>
<td>5208</td>
<td>512</td>
<td>260</td>
<td>5.00</td>
<td>Image</td>
</tr>
<tr>
<td>imdb</td>
<td>10000</td>
<td>768</td>
<td>500</td>
<td>5.00</td>
<td>NLP</td>
</tr>
<tr>
<td>Yelp</td>
<td>10000</td>
<td>768</td>
<td>500</td>
<td>5.00</td>
<td>NLP</td>
</tr>
<tr>
<td>security</td>
<td>3525</td>
<td>21</td>
<td>378</td>
<td>6.84</td>
<td>Security</td>
</tr>
</tbody>
</table>

Table 2: Data description of the eight datasets used in this study: the top seven datasets are adapted from AD repo, e.g., DAMI (Campos et al. 2016) and ADBench (Han et al. 2022), and security* is a proprietary enterprise-security dataset.

Benchmark Datasets. As shown in Table 2, we evaluate ADMoE on seven public datasets adapted from AD repositories (Campos et al. 2016; Han et al. 2022) and a proprietary enterprise-security dataset (with t = 3 sets of noisy labels). Note that these public datasets do not have existing noisy labels for AD, so we simulate t = 4 sets of noisy labels per dataset via two methods:

1. Label Flipping (Zheng, Awadallah, and Dumais 2021) generates noisy labels by uniformly swapping anomalous and normal classes at a designated noise rate.

2. Inaccurate Output uses varying percentages of ground truth labels to train t diverse classifiers, and considers their (inaccurate) predictions as noisy labels. With more ground truth labels to train a classifier, its prediction (e.g., noisy labels) will be more accurate—we control the noise levels by the availability of ground truth labels.

In this work, we use the noisy labels simulated by Inaccurate Output since that is more realistic and closer to real-world applications (e.g., noise is not random), while we also release the datasets by Label Flipping for broader usage. We provide a detailed dataset description in Appx. B.1.

Two Groups of Baselines are described below:

1. Leading AD methods that can only handle a single set of labels to show ADMoE’s benefit of leveraging multiple sets of noisy labels. These include SOTA AD methods: (1) XGBO (Zhao and Hryniewicki 2018) (2) PreNet (Pang et al. 2019) (3) DevNet (Pang, Shen, and van den Hengel 2019) (4) DeepSAD (Ruff et al. 2019), and popular classification methods: (5) MLP (6) XGBoost (Chen and Guestrin 2016) (7) LightGBM (Ke et al. 2017). We provide detailed descriptions in Appx. B.2.

2. Leading methods (for classification) that handle multiple sets of noisy labels (we adapt them for MNLAD; see §2.3 and Table 1 for details): (1) SingleNoisy (2) LabelVote (3) HyperEnsemble (Wenzel et al. 2020) that averages t models’ scores (referred as HP_A) or takes their max (referred as HP_M) (4) CrowdLayer (Rodrigues and Pereira 2018) and latest (5) UnionNet (Wei et al. 2022).

Backbone AD Algorithms, Model Capacity, and Hyper-parameters. We show the generality of ADMoE to enhance (i) simple MLP and (ii) SOTA DeepSAD (Ruff et al. 2019). To ensure a fair comparison, we ensure all methods have the equivalent number of trainable parameters and FLOPs. See Appx. C.2 and code for additional settings (e.g., hyperparameters) in this study. All experiments are run on an Intel i7-9700 @3.00 GH, 64GB RAM, 8-core workstation with an NVIDIA Tesla V100 GPU.

Evaluation. For methods with built-in randomness, we run four independent trials and take the average, with a fixed dataset split (70% train, 25% for test, 5% for validation). Following AD research tradition (Aggarwal and Sathe 2017; Zhao et al. 2019; Lai et al. 2021; Han et al. 2022), we report ROC-AUC as the primary metric, while also showing additional results of average precision (AP) in Appx. C.3.

Figure 3: ROC-AUC comparison at different noisy label quality of ADMoE enhanced DeepSAD and MLP (denoted as AD and AM) with leading AD methods that can only leverage one set of noisy labels. We already show Yelp’s result in Fig. 1a. Notably, ADMoE enabled AD and AM has significant performance improvement especially when the label quality is very low (to the left of the x-axis).
4.2 Comparison Between ADMoE Methods and Leading AD Methods (Q1)

Fig. 1a and Fig. 3 show that ADMoE enables MLP and DeepSAD to use multiple sets of noisy labels, which outperform leading AD methods that can use only one set of labels, at varying noisy label qualities (x-axis). We further use Table 3 to compare them at noisy label quality 0.2 to understand the specific gain of ADMoE using multiple sets of noisy labels. The third block of the table shows that ADMoE brings on average 13.83% and up to 33.96% improvement over the original MLP, and on average 14.44% and up to 32.79% improvement over DeepSAD. Note that all the neural-network models use the equivalent numbers of parameters and training FLOPs.

![Figure 4](image-url)  
**Figure 4:** ROC-AUC comparison at different noisy label quality of ADMoE enhanced MLP (AM) with leading multi-set noisy-label learning methods. We already show Yelp’s result in Fig. 1b. ADMoE outperforms most baselines.

### Table 3: Performance comparison between ADMoE-enhanced AD methods and leading AD methods (that can only use one set of labels) at noisy level 0.2. The best performance is highlighted in bold per dataset (row). ADMoE-based methods (ADMoE-MLP and ADMoE-DeepSAD) outperform all baselines. ADMoE brings on average 13.83% and up to 33.96% improvement over the original MLP, and on average 14.44% and up to 32.79% improvement over DeepSAD.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>agnews</td>
<td>0.8277</td>
<td>0.903</td>
<td>0.8789</td>
<td>0.7991</td>
<td>0.8293</td>
<td>0.946</td>
<td>+14.07%</td>
<td>0.7627</td>
<td>0.9423</td>
<td>+23.55%</td>
</tr>
<tr>
<td>aloi</td>
<td>0.6312</td>
<td>0.6209</td>
<td>0.6057</td>
<td>0.6406</td>
<td>0.6078</td>
<td>0.8142</td>
<td>+33.96%</td>
<td>0.6552</td>
<td>0.7458</td>
<td>+13.83%</td>
</tr>
<tr>
<td>imdb</td>
<td>0.6898</td>
<td>0.7741</td>
<td>0.7372</td>
<td>0.6667</td>
<td>0.7335</td>
<td>0.8872</td>
<td>+20.95%</td>
<td>0.6688</td>
<td>0.8881</td>
<td>+32.79%</td>
</tr>
<tr>
<td>mnist</td>
<td>0.9887</td>
<td>0.9869</td>
<td>0.9777</td>
<td>0.9907</td>
<td>0.9821</td>
<td>0.9913</td>
<td>+40.94%</td>
<td>0.96</td>
<td>0.9891</td>
<td>+3.03%</td>
</tr>
<tr>
<td>spamspace</td>
<td>0.9736</td>
<td>0.9683</td>
<td>0.9645</td>
<td>0.9743</td>
<td>0.9706</td>
<td>0.9744</td>
<td>+30.39%</td>
<td>0.955</td>
<td>0.9804</td>
<td>+2.66%</td>
</tr>
<tr>
<td>svhn</td>
<td>0.8585</td>
<td>0.8185</td>
<td>0.837</td>
<td>0.8016</td>
<td>0.7847</td>
<td>0.9022</td>
<td>+14.97%</td>
<td>0.7705</td>
<td>0.9025</td>
<td>+17.13%</td>
</tr>
<tr>
<td>yelp</td>
<td>0.7778</td>
<td>0.8699</td>
<td>0.8689</td>
<td>0.7348</td>
<td>0.7955</td>
<td>0.9535</td>
<td>+19.86%</td>
<td>0.7781</td>
<td>0.9355</td>
<td>+20.23%</td>
</tr>
</tbody>
</table>

| security* | 0.7479 | 0.7415 | 0.7498 | 0.7335 | 0.7363 | 0.7767 | +5.49% | 0.7928 | 0.8108 | +2.27% |
| Average   | 0.8119 | 0.8353 | 0.8274 | 0.7926 | 0.8049 | 0.9056 | +13.83% | 0.7929 | 0.8993 | +14.44% |

4.3 Comparison Between ADMoE and Noisy Label Learning Methods (Q2)

ADMoE also shows an edge over SOTA classification methods that learn from multiple sets of noisy labels⁴, as shown in Fig. 1b and 4. We also analyze the comparison at noisy label quality 0.05 in Table 4, where ADMoE ranks the best in 7 out of 8 datasets. In addition to better detection accuracy, ADMoE only builds a single model, and is thus faster than HE_E and HE_M which requires building t independent models to aggregate predictions. We credit ADMoE’s performance over SOTA algorithms including CrowdLayer and UnionNet to its implicit mapping of noisy labels to experts (§3.3.3).

### Table 4: Performance comparison between ADMoE and leading noisy-label learning methods (in Table 1) on an MLP at noisy label quality 0.05. The best performance is highlighted in bold per dataset (row). ADMoE mostly outperforms baselines, with on avg. 9.4% and up to 19% improvement over SingleNoise which trains w/ a set of noisy labels.

<table>
<thead>
<tr>
<th>Dataset</th>
<th>Single</th>
<th>Major</th>
<th>HE_A</th>
<th>HE_M</th>
<th>Crowd Layer</th>
<th>Union Net</th>
<th>ADMoE</th>
</tr>
</thead>
<tbody>
<tr>
<td>agnews</td>
<td>0.7185</td>
<td>0.5729</td>
<td>0.7824</td>
<td>0.8101</td>
<td>0.8543</td>
<td>0.7412</td>
<td>0.8549</td>
</tr>
<tr>
<td>aloi</td>
<td>0.531</td>
<td>0.479</td>
<td>0.5195</td>
<td>0.5579</td>
<td>0.5495</td>
<td>0.5773</td>
<td>0.5842</td>
</tr>
<tr>
<td>imdb</td>
<td>0.5967</td>
<td>0.5521</td>
<td>0.6587</td>
<td>0.6599</td>
<td>0.6219</td>
<td>0.5918</td>
<td>0.6577</td>
</tr>
<tr>
<td>mnist</td>
<td>0.9482</td>
<td>0.9467</td>
<td>0.9598</td>
<td>0.9563</td>
<td>0.9644</td>
<td>0.6767</td>
<td>0.9655</td>
</tr>
<tr>
<td>spamspace</td>
<td>0.9626</td>
<td>0.9655</td>
<td>0.9584</td>
<td>0.9586</td>
<td>0.7654</td>
<td>0.9567</td>
<td>0.9655</td>
</tr>
<tr>
<td>svhn</td>
<td>0.7201</td>
<td>0.6222</td>
<td>0.7971</td>
<td>0.7998</td>
<td>0.8161</td>
<td>0.6608</td>
<td>0.8451</td>
</tr>
<tr>
<td>yelp</td>
<td>0.6777</td>
<td>0.5708</td>
<td>0.7298</td>
<td>0.7358</td>
<td>0.7418</td>
<td>0.7133</td>
<td>0.7533</td>
</tr>
<tr>
<td>security*</td>
<td>0.7363</td>
<td>0.7653</td>
<td>0.7526</td>
<td>0.7484</td>
<td>0.7374</td>
<td>0.7435</td>
<td>0.7767</td>
</tr>
<tr>
<td>Average</td>
<td>0.7363</td>
<td>0.6843</td>
<td>0.7722</td>
<td>0.7783</td>
<td>0.7563</td>
<td>0.7014</td>
<td>0.8003</td>
</tr>
</tbody>
</table>

⁴We adapt these classification methods (Table 1) for MNLAD.
ing to contextualize how each expert responds to specific groups of samples due to the complexity of NLP models (Shazeer et al. 2017; Zheng et al. 2019; Zuo et al. 2021). Given that AD models are much smaller and we use only one MoE layer before the output layer, we present an interesting case study (MLP with 4 experts where top 1 gets activated) in Table 5. We find each expert achieves the highest ROC-AUC on the subsamples where it gets activated by gating (see the diagonal), and they are significantly better than training an individual model with the same architecture (see the last column). Thus, each expert does develop a specialization in the subsamples they are “responsible” for.

### 4.4.2 Ablation on Using MoE and Noisy Labels as Inputs in ADMoE

Additionally, we analyze the effect of using (i) ADMoE layer and (ii) noisy labels as input features in Fig. 5 and Appx. Fig. C2. First, ADMoE performs the best while using these two techniques jointly in most cases, and significantly better than not using them ( ). Second, ADMoE helps the most when labels are noisier (to the left of the x-axis) with an avg. of 2% improvement over using only noisy labels as input ( ). As expected, its impact is reduced with less noisy labels (i.e., closer to the ground truth): in that case, noisy labels are more similar to each other and specialization with ADMoE is therefore limited.

### 4.4.3 Effect of Number of Experts ($m$) and top-$k$ Gating

We vary the number of activated (x-axis) and total (y-axis) experts in ADMoE, and compare their detection accuracy in Fig. 6 and Appx. Fig. C3. The results suggest that the best choice is data-dependent, and we use $m = 4$ and $k = 2$ for all the datasets in the experiments.

Table 5: Perf. breakdown of each expert and a comparison with MoE on Yelp. We highlight the best model per row in **bold**. The specialized expert performs the best in their assigned subsamples by gating, i.e., the diagonal is all in bold.

<table>
<thead>
<tr>
<th>Activated Expert</th>
<th>Expert 1</th>
<th>Expert 2</th>
<th>Expert 3</th>
<th>Expert 4</th>
<th>Comp.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subsamples for Expert 1</td>
<td>0.8554</td>
<td>0.8488</td>
<td>0.8548</td>
<td>0.8440</td>
<td>0.7741</td>
</tr>
<tr>
<td>Subsamples for Expert 2</td>
<td>0.8955</td>
<td>0.9043</td>
<td>0.8913</td>
<td>0.8943</td>
<td>0.7976</td>
</tr>
<tr>
<td>Subsamples for Expert 3</td>
<td>0.9633</td>
<td>0.9643</td>
<td>0.9729</td>
<td>0.9665</td>
<td>0.9349</td>
</tr>
<tr>
<td>Subsamples for Expert 4</td>
<td>0.7903</td>
<td>0.7888</td>
<td>0.7775</td>
<td>0.8066</td>
<td>0.7134</td>
</tr>
</tbody>
</table>

Figure 6: Ablation studies on key hyperparameters in ADMoE: (x-axis) the number of experts and (y-axis) top-$k$ experts to activate. We show the results at noisy level 0.05, and find the best setting is data-dependent. See Appx. Fig. C3.

### 4.4.4 Performance on Varying Number of Clean Labels

As introduced in §3.3.3, one merit of ADMoE is the easy integration of clean labels when available. Fig. 7 and Appx. Fig. C4 show that ADMoE can leverage the available clean labels to achieve higher performance. Specifically, ADMoE with only 8% clean labels can achieve similar or better results than that of using all available clean labels on spamspace and svhn.

Figure 7: Analysis of integrating varying percentages (from 1% to 10%) of additional clean labels in ADMoE. The results show that ADMoE efficiently leverages the clean labels with increasing performance. See more in Appx. Fig. C4.

## 5 Conclusions

We propose ADMoE, a model-agnostic learning framework, to enable anomaly detection algorithms to learn from multiple sets of noisy labels. Leveraging Mixture-of-experts (MoE) architecture from the NLP domain, ADMoE is scalable in building specialization based on the diversity among noisy sources. Extensive experiments show that ADMoE outperforms a wide range of leading baselines, bringing on average 14% improvement over not using it. Future work can explore its usage with complex detection algorithms.
References


Campos, G. O.; Zimek, A.; Sander, J. Á. ¶. r.; Campello, R. J.; Micenkov Á ¡, B.; Schubert, E.; Assent, I.; and Houle, M. E. 2016. On the evaluation of unsupervised outlier detection: measures, datasets, and an empirical study, volume 30. Springer US.


Supplementary Material of ADMoE
Details on algorithm design, experiment setting, and additional results.

A Additional Results on Why Does AD Benefit from Multiple Sets of Noisy Labels

(a) Result analysis on PreNet (b) Result analysis on XGBOD

Figure A1: Benefit of leveraging multiple noisy sources on Yelp: even simply averaging individual models’ outputs (■) is better than training each weak source independently (▲)

B Additional Experiment Setting and Results

B.1 Dataset Description

As discussed in §4.1, we use the results based on the Classification noise since that is more realistic and closer to real-world applications (e.g., noise is not at random), while we also release the datasets by Label flipping for broader usages. See our repo to access both versions of datasets.

Process of Inaccurate Output. We use varying percentages of ground truth labels to train t diverse classifiers (called noisy label generators), and consider their (inaccurate) predictions as noisy labels. Naturally, with more available ground truth labels to train a classifier, its prediction (e.g., noisy labels) will be more accurate—we therefore control the noise levels by the availability of ground truth labels.

Following this approach, we generate the noisy labels for the benchmark datasets at varying percentages of ground truth labels (namely, {0.01, 0.05, 0.1, 0.2, 0.3, 0.4, 0.5}) to train classifiers (a simple feed-forward MLP (Rosenblatt 1958), decision tree (Breiman et al. 2017), and ensemble methods Random Forest (Breiman 2001) and LightGBM (Ke et al. 2017)). Please see our code for more details.

Table B1 summarizes avg. ROC-AUC of the generated noisy labels while using varying percentages of ground truth labels to train noisy label generators. Of course, with more ground truth labels, the generated noisy labels are also more accurate. Note that security’s noisy labels are not simulated and thus ROC-AUC does not vary.

<table>
<thead>
<tr>
<th>Clean Perc.</th>
<th>agnews</th>
<th>aoi</th>
<th>imdb</th>
<th>minist</th>
<th>spam</th>
<th>svhn</th>
<th>yelp</th>
<th>security*</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.01</td>
<td>0.5384</td>
<td>0.5154</td>
<td>0.5085</td>
<td>0.7260</td>
<td>0.7862</td>
<td>0.5164</td>
<td>0.5192</td>
<td>0.6862</td>
</tr>
<tr>
<td>0.05</td>
<td>0.5663</td>
<td>0.5330</td>
<td>0.5304</td>
<td>0.7887</td>
<td>0.8929</td>
<td>0.5773</td>
<td>0.5455</td>
<td>0.6862</td>
</tr>
<tr>
<td>0.1</td>
<td>0.6210</td>
<td>0.5540</td>
<td>0.5628</td>
<td>0.8592</td>
<td>0.9047</td>
<td>0.6132</td>
<td>0.5754</td>
<td>0.6862</td>
</tr>
<tr>
<td>0.2</td>
<td>0.6641</td>
<td>0.5957</td>
<td>0.6023</td>
<td>0.9044</td>
<td>0.9182</td>
<td>0.6496</td>
<td>0.6271</td>
<td>0.6862</td>
</tr>
<tr>
<td>0.3</td>
<td>0.7065</td>
<td>0.6303</td>
<td>0.6356</td>
<td>0.9301</td>
<td>0.9301</td>
<td>0.6827</td>
<td>0.6621</td>
<td>0.6862</td>
</tr>
<tr>
<td>0.4</td>
<td>0.7462</td>
<td>0.6503</td>
<td>0.6758</td>
<td>0.9308</td>
<td>0.9401</td>
<td>0.7224</td>
<td>0.7077</td>
<td>0.6862</td>
</tr>
<tr>
<td>0.5</td>
<td>0.7662</td>
<td>0.6701</td>
<td>0.7118</td>
<td>0.9427</td>
<td>0.9482</td>
<td>0.7531</td>
<td>0.7212</td>
<td>0.6862</td>
</tr>
</tbody>
</table>

Table B1: Avg. ROC-AUC of noisy labels at different noisy label qualities (higher the better). Note that security’s noisy labels are not simulated and thus do not vary.

B.2 AD Algorithms and Binary Classifiers

We provide a brief description of AD algorithms below (see more details to recent literature (Ruff et al. 2021; Han et al. 2022)). Since it lacks specialized fully supervised AD methods, we discuss some SOTA binary classifiers below.

1. Extreme Gradient Boosting Outlier Detection (XGBOD) (Zhao and Hryniukwic 2018). XGBOD uses unsupervised outlier detectors to extract representations for the underlying dataset and concatenates the newly generated features to the original feature feature for augmentation. An XGBoost classifier is then applied to the augmented feature space.

2. Deviation Networks (DevNet) (Pang, Shen, and van den Hengel 2019) uses a prior probability to enforce a statistical deviation score of input instances.

3. Pairwise Relation prediction-based ordinal regression Network (PRenNet) (Pang et al. 2019) is a neural network-based model that defines a two-stream ordinal regression to learn the relation of instance pairs.

4. Deep Semi-supervised Anomaly Detection (DeepSAD) (Ruff et al. 2019). DeepSAD is considered as the SOTA semi-supervised AD method. It improves the early version of unsupervised DeepSVDD (Ruff et al. 2018) by including the supervision to penalize the inverse of the distances of anomaly representation. In this way, anomalies are forced to be in the space which is away from the hypersphere center.

5. Multi-layer Perceptron (MLP) (Rosenblatt 1958). MLP is a simple feedforward version of the neural network, which uses the binary cross entropy loss to update network parameters.

6. Highly Efficient Gradient Boosting Decision Tree (LightGBM) (Ke et al. 2017) is a gradient boosting framework that uses tree-based learning algorithms with faster training speed, higher efficiency, lower memory usage, and better accuracy.

C More Experiment Settings and Details

C.1 Code and Reproducibility

See our datasets and code at GitHub repository https://github.com/microsoft/admoe. Part of the code is based on PyOD (Zhao, Nasrullah, and Li 2019), ADBench (Han et al. 2022), and TOD (Zhao, Chen, and Jia 2023).

C.2 Hyperparameter Setting of ADMoE and Baselines

For all baselines used in this study, we use the same set of key hyperparameters for a fair comparison. We also use algorithms default hyperparameter (HP) settings in the original paper for unique hyperparameters. More specifically, we use the same: (i) learning rate=0.001; (ii) batch size=256; and (iii) model size: (number of trainable parameters ≈ 18,000). We use the small validation set (5%) to choose the model with the highest validation performance. See our code at https://tinyurl.com/admoe22 for more details.
Table C2: Average precision (AP) comparison between ADMoE-enhanced AD methods and leading AD methods (that can only use one set of labels) at noisy level 0.2. The best performance is highlighted in bold per dataset (row). ADMoE-based methods (ADMoE-MLP and ADMoE-DeepSAD denote ADMoE-enhanced MLP and DeepSAD) outperform all baselines. ADMoE brings on average 63.05% improvement over the original MLP, and on average 29.59% improvement over DeepSAD. Note that all the neural-network models use the equivalent numbers of parameters and FLOPS.

### C.3 Results by Average Precision (AP)

### C.4 More Ablation Results on the Use of MoE and Weak Inputs

In addition to the ablation studies in §4.4.2, we provide additional results in Fig. C2 for the effects of using ADMoE and noisy labels as inputs. Similar statements can be made. First, ADMoE performs the best while using these two techniques jointly in most cases, and significantly better than not using them (○). Second, ADMoE helps the most when labels are noisier (to the left of the x-axis) with an avg. of 2% improvement over only using noisy labels as input (A). As expected, its impact is reduced with less noisy labels (i.e., closer to the ground truth): in that case, noisy labels are more similar to each other and specialization with ADMoE is less useful.

#### Figure C3: Additional ablation results on key hyperparameters in ADMoE: (x-axis) the number of experts and (y-axis) top-k experts to activate. We show the results at noisy level 0.05, and find the best setting is data-dependent.

#### Figure C2: Ablation studies on (i) the use of ADMoE layer and (ii) the noisy labels y_w as input. ADMoE (A) using both techniques shows the best results at (nearly) all settings.

#### C.5 Additional Results for Effect of Number of Experts (m) and top-k Gating.

Fig. C3 provides additional results for §4.4.3 with consistent observations.

#### C.6 Additional Results for Performance on Varying Percentage of Clean labels

Fig. C4 provides additional results for §4.4.4 with consistent observations.

![Diagram](image-url)