Moderate-fitting as a Natural Backdoor Defender for Pre-trained Language Models

Biru Zhu[1*], **Yujia Qin**[2*], **Ganqu Cui**[2], **Yangyi Chen**[3], **Weilin Zhao**[2], **Chong Fu**[4], **Yangdong Deng**[1†], **Zhiyuan Liu**[2†], **Jingang Wang**[5], **Wei Wu**[5], **Maosong Sun**[2], **Ming Gu**[1]
[1] School of Software, Tsinghua University, Beijing, China
[2] Department of Computer Science and Technology, Tsinghua University, Beijing, China
[3] University of Illinois Urbana-Champaign
[4] Zhejiang University, Hangzhou, China
[5] Meituan, Beijing, China
{zbr19, qyj20}@mails.tsinghua.edu.cn
{dengyd, liuzy}@tsinghua.edu.cn

Abstract

Despite the great success of pre-trained language models (PLMs) in a large set of natural language processing (NLP) tasks, there has been a growing concern about their security in real-world applications. Backdoor attack, which poisons a small number of training samples by inserting backdoor triggers, is a typical threat to security. Trained on the poisoned dataset, a victim model would perform normally on benign samples but predict the attacker-chosen label on samples containing pre-defined triggers. The vulnerability of PLMs under backdoor attacks has been proved with increasing evidence in the literature. In this paper, we present several simple yet effective training strategies that could effectively defend against such attacks. To the best of our knowledge, this is the first work to explore the possibility of backdoor-free adaptation for PLMs. Our motivation is based on the observation that, when trained on the poisoned dataset, the PLM's adaptation follows a strict order of two stages: (1) a moderate-fitting stage, where the model mainly learns the major features corresponding to the original task instead of subsidiary features of backdoor triggers, and (2) an overfitting stage, where both features are learned adequately. Therefore, if we could properly restrict the PLM's adaptation to the moderate-fitting stage, the model would neglect the backdoor triggers but still achieve satisfying performance on the original task. To this end, we design three methods to defend against backdoor attacks by reducing the model capacity, training epochs, and learning rate, respectively. Experimental results demonstrate the effectiveness of our methods in defending against several representative NLP backdoor attacks. We also perform visualization-based analysis to attain a deeper understanding of how the model learns different features, and explore the effect of the poisoning ratio. Finally, we explore whether our methods could defend against backdoor attacks for the pre-trained CV model. The codes are publicly available at `https://github.com/thunlp/Moderate-fitting`.

1 Introduction

Despite the rapid development and great success of pre-trained language models (PLMs) (Han et al., 2021), there have been increasing security concerns on deploying them in real-world applications.

[*] Indicates equal contribution.
[†] Corresponding author.

36th Conference on Neural Information Processing Systems (NeurIPS 2022).

Backdoor attack by poisoning the training data is one typical security threat. The idea is that attackers insert backdoor triggers into certain training samples. After being trained on poisoned data, the victim model would (1) behave normally on the benign inputs, but (2) predict the attacker-chosen label given an input containing pre-defined triggers during inference. Initially introduced in the field of computer vision (CV) (Gu et al., 2017; Chen et al., 2017), diverse backdoor attack methods have been proposed in natural language processing (NLP), including inserting context-independent words (Kurita et al., 2020) or sentences (Dai et al., 2019) into training samples and modifying the syntactic structure (Qi et al., 2021c) or text style (Qi et al., 2021b). Empirical results reveal that even pre-trained language models (PLMs), the current foundation infrastructure for NLP (Min et al., 2021), are highly fragile to these attacks. Such a vulnerability poses a significant threat to real-life applications of PLMs.

In this paper, we show backdoor attacks can be easily defended against using simple training strategies. Specifically, we focus on the following setting: (1) the attacker poisons the training data and releases the poisoned training dataset on open-source platforms. The attacker does not control the model training process; (2) the victim downloads the poisoned training dataset from the open-source platform to train their own models. If no defense is applied, the victim will get a model injected with backdoors. Instead, with our proposed defense method, the risks of backdoor attack can be significantly mitigated even if the model is trained on the poisoned dataset.

Our motivation is based on previous findings (Tänzer et al., 2022) that during the PLM's adaptation to a specific dataset, the model would first learn the general-purpose patterns shared by most of the training samples, and then memorize those uncommon patterns of noisy samples. Under the setting of backdoor attack, a partially poisoned dataset consists of both general-purpose patterns (major features) derived from most clean samples and backdoor triggers (subsidiary features) injected by attackers, and both features are highly distinct. For a PLM trained on the poisoned dataset, we observe that the model's learning dynamics follow a strict order of two stages: (1) **moderate-fitting stage**, where the model mainly learns the major features instead of subsidiary backdoor triggers, and (2) **overfitting stage**, where the model learns both features adequately.

Based on our observation, if we could properly restrict the PLM's adaptation to the moderate-fitting stage, the model would neglect the malicious backdoor triggers but still achieve satisfying performance on the original task. To this end, we propose three methods to limit the PLM's adaptation to the moderate-fitting stage, i.e., reducing the model capacity, training epochs, and learning rate during training. Specifically, to decrease the model capacity, we resort to parameter-efficient tuning (PET), also known as delta tuning (Houlsby et al., 2019; Ding et al., 2022), which optimizes a small number of parameters instead of all the PLM's parameters. We additionally apply a flexible low-rank reparameterization network to existing PET algorithms to further reduce the model capacity. In addition, we demonstrate that reducing the training epochs or learning rate also suffices for our goal of restricting the PLM's adaptation to the moderate-fitting stage.

In experiments, we validate the feasibility of the proposed methods in defending against a series of representative backdoor attacks on several NLP tasks. The results reflect that, each proposed method could significantly lower the attack success rate (ASR) of the trained model while slightly hurting the performance of the original task on benign samples. This demonstrates that our methods are effective to defend against backdoor attacks in the training stage. To gain a deeper understanding, we visualize the model's learning dynamics on the poisoned dataset under different model capacity. Furthermore, we conduct analyses to explore the effect of the poisoning ratio. We also create a synthetic dataset to show that the two-stage learning phenomenon commonly exists in the scenario where PLMs jointly learn two distinct features that are imbalanced in the training data. Finally, we explore whether our methods could defend against backdoor attacks for the pre-trained CV model. In general, our study offers simple yet effective backdoor defense methods and uncovers the underlying mechanism of the backdoor attack in NLP.

2 Related Work

Backdoor Attack in NLP. One typical way of the backdoor attack is training data poisoning. By poisoning the training samples with malicious triggers, backdoor attackers aim to establish a strong connection between the trigger and the attacker-chosen target label (Chen et al., 2017). Plenty of algorithms for training data poisoning have been proposed in the field of CV, such as inserting patch triggers (Gu et al., 2017) and blending benign samples with specific patterns (Chen et al., 2017).

Recently, many poisoning methods that insert triggers into the training data have also emerged in NLP, such as word-level (Kurita et al., 2020) and sentence-level (Dai et al., 2019) triggers. However, these methods typically leverage unusual words or sentences that are uncorrelated to the context. These triggers break the grammar rules or coherence of normal text and could be easily detected in the inspection process (Qi et al., 2021c). In light of this, researchers recently proposed more invisible backdoor triggers, such as modifying the syntactic structure (Qi et al., 2021c) and transferring the text style (Qi et al., 2021b).

Backdoor Defense in NLP. The advance of backdoor attacks spawned a line of backdoor defense algorithms. The first category is to examine the training samples and remove the poisoned ones. For instance, Chen and Dai (2021) propose Backdoor Keyword Identification (BKI) to remove suspicious samples that contain potential backdoor keywords from the training dataset. The second category is to inspect the testing samples. Qi et al. (2021a) detect and remove the words that may be the backdoor trigger from testing samples using outlier word detection; Yang et al. (2021) distinguish the poisoned data from clean data based on robustness-aware perturbations during the inference stage. The third category distinguishes trojaned models from clean models (Azizi et al., 2021; Liu et al., 2022; Shen et al., 2022). Orthogonal to the above methods, our methods do not require additional operations on data or model and thus are more practical.

Learning Behavior of DNNs on Noisy Data. Many efforts have been spent on exploring the learning behavior of DNNs when the training data contains label noise. Zhang et al. (2021) demonstrate that DNNs are skilled in fitting random labels, showing excellent memorization abilities. Arpit et al. (2017) further reveal that DNNs tend to prioritize learning simple patterns before memorizing the noisy data. As the foundation model for NLP, PLMs are also demonstrated adept in memorizing the training data (Carlini et al., 2021, 2022) and recalling the learned facts (Petroni et al., 2019). Tänzer et al. (2022) additionally analyze the learning dynamics of PLMs under label noise, and observe distinct learning phases, i.e., PLMs first learn general-purpose features and then enter a performance plateau, followed by rapidly memorizing label noise. Different from the above works, in this paper, we target at defending against backdoor attacks. Under our setting, for poisoned samples, the input data is modified by inserting triggers, and the modified data's label is set as the target label chosen by the attacker. When trained on the poisoned data, the model would find a shortcut by establishing a connection between the backdoor features and the corresponding label.

Parameter-efficient Tuning. Fine-tuning, which optimizes all of the parameters, is the conventional way to adapt PLMs towards a downstream task. However, due to the tremendous size of PLMs, fine-tuning could bring huge computation and storage costs. In order to make it feasible to tune larger PLMs, parameter-efficient tuning (PET) methods are proposed (Ding et al., 2022). PET tunes a small number of parameters and achieves comparable performance to fine-tuning. Up to now, various PET algorithms have emerged, including (1) inserting additional modules into the Transformer (Vaswani et al., 2017) block (Houlsby et al., 2019; Lester et al., 2021; Li and Liang, 2021), (2) optimizing part of PLM's existing parameters (Ben-Zaken et al., 2021; Guo et al., 2021), and (3) reparameterizing tunable parameters as low-rank decompositions (Hu et al., 2021). In this paper, we demonstrate the potential application of PET in backdoor defense by reducing the model capacity.

3 Methodology

In this section, to achieve our goal of restricting the PLM's adaptation to the moderate-fitting stage, we design three training strategies during PLM's downstream adaptation, by reducing the (1) model capacity, (2) training epochs, and (3) learning rate, respectively.

Reducing the Model Capacity. The traditional way for PLM's downstream adaptation is to optimize all the parameters in the PLM (i.e., fine-tuning). Due to the tremendous size of tunable parameters and the complicated network architecture in a Transformer block, the model capacity (complexity) of a PLM is inevitably huge[3]. Although a huge model capacity is typically considered as the guarantee for good memorization and representational ability (LeCun et al., 1998; Arpit et al., 2017), recent works have demonstrated that for PLMs, most downstream NLP tasks have a

[3]The model capacity is decided by the tunable parameters during PLM's downstream adaptation.

considerably small intrinsic dimension (Aghajanyan et al., 2021; Qin et al., 2021), which is defined as the minimal parameters needed to approximate some function or data distribution. This finding reveals that, for PLMs, a huge model capacity may not be the prerequisite for the successful downstream adaptation; instead, we could utilize a small model capacity but still achieve excellent performance.

Parameter-efficient tuning (PET) serves as a possible solution to reduce the model capacity by significantly reducing the tunable parameters. However, in most cases, the extent of such reduction is still far from causing moderate-fitting. The reason is that, the actual model capacity is not just decided by the **number** of tunable parameters, but also by the overall **intrinsic rank** (Hu et al., 2021) of the tunable parameters. Specifically, existing PET algorithms suffer from the following defects: (1) most PET algorithms (e.g., Adapter (Houlsby et al., 2019) and Prefix-Tuning (Li and Liang, 2021)) do not have a low-rank constraint on the updates of the tunable parameters, but instead allow the intrinsic rank of weight updates larger than the actual intrinsic dimension of the downstream adaptation; (2) for those algorithms that explicitly model the low-rank updates of the parameters (e.g., LoRA (Hu et al., 2021)), their low-rank structures are individually distributed in different modules in the Transformer layers (dubbed as *local* low-rank architecture). Instead, we argue that it is essential to have a *global* low-rank architecture to constrain the overall intrinsic rank of the weight updates.

To mitigate the above defects, we propose a flexible method that could be applied to PET algorithms. We reparameterize all of the tunable parameters defined by a PET algorithm with a global low-rank decomposition. Without loss of generality, assuming a PET algorithm defines N tunable weights (and biases): $\{\mathbf{W}_1, ..., \mathbf{W}_N\}$ of various sizes, we first flatten each one into a one-dimensional vector. For example, a two-dimensional weight matrix $\mathbf{W}_i \in \mathbb{R}^{d_1^i \times d_2^i}$ could be converted to a vector $\mathbf{V}_i \in \mathbb{R}^{d_v^i}$, where $d_v^i = d_1^i \times d_2^i$, and $\mathbf{W}_i(j,k) = \mathbf{V}_i(j \times d_2^i + k)$ for $0 \leq j < d_1^i$ and $0 \leq k < d_2^i$. After that, we concatenate all the flattened vectors as follows: $\mathbf{V}_{\text{all}} = [\mathbf{V}_1; ...; \mathbf{V}_N] \in \mathbb{R}^{d_{\text{all}}}$, where $d_{\text{all}} = \sum_{i=1}^{N} d_v^i$ denotes the total number of tunable parameters. Finally, we reparameterize $\mathbf{V}_{\text{all}}$ as low-rank decompositions. Specifically, the reparameterization network consists of two projection layers $\mathbf{Proj}_1$ and $\mathbf{Proj}_2$ with an activation function σ between them:

$$\mathbf{V}_{\text{all}} = \mathbf{Proj}_2(\sigma(\mathbf{Proj}_1(\mathbf{E}))), \tag{1}$$

where $\mathbf{E} \in \mathbb{R}^{d_{\text{emb}}}$ is a tunable embedding. The layer $\mathbf{Proj}_1$ projects $\mathbf{E}$ from dimension d_{emb} to the bottleneck dimension d_I, creating a vector $\mathbf{I} = \mathbf{Proj}_1(\mathbf{E}) \in \mathbb{R}^{d_I}$. Note d_I is set small (e.g., 1) enough to ensure the low model capacity. The layer $\mathbf{Proj}_2$ projects the dimension of $\mathbf{I}$ from d_I to d_{all}, and forms the tunable parameters $\mathbf{V}_{\text{all}}$ defined by the PET algorithm. During adaptation, instead of tuning $\mathbf{V}_{\text{all}}$, we jointly optimize $\mathbf{Proj}_1$, $\mathbf{Proj}_2$ and $\mathbf{E}$, and keep the PLM's parameters fixed.

Reducing the Training Epochs. Too many training epochs could cause the model to overfit the training data exhaustively. In our setting where the training data is partially poisoned with backdoor triggers, after enough training epochs, the PLM would eventually learn both the major and subsidiary features present in the data adequately. Inspired by Li et al. (2020) who contend that early stopping is robust to label noise for over-parameterized neural networks, we propose to reduce training epochs to prevent the PLM's adaptation from entering the overfitting stage.

Reducing the Learning Rate. Intuitively, training the PLM with a larger learning rate and fewer epochs is approximately equivalent to training the PLM with more epochs but a smaller learning rate. Therefore, similar to the idea of limiting the number of training epochs, reducing the learning rate serves as another simple yet effective method that could prevent the model from learning the poisoned samples adequately.

4 Experiments

In this section, we first conduct experiments to evaluate our proposed defense methods. We choose two representative NLP backdoor attacks as the main experiments (§ 4.1). Then we analyze the learning dynamics of the model under different settings and visualize representative feature distributions learned during the training process in § 4.2. Furthermore, we conduct systematic analyses to gain a deeper understanding of the effect of the poisoning ratio. Also, we show that the two-stage learning is a common phenomenon for PLMs in the scenario where PLMs jointly learn two distinct features that are imbalanced in the training data. In addition, we demonstrate that our methods could successfully

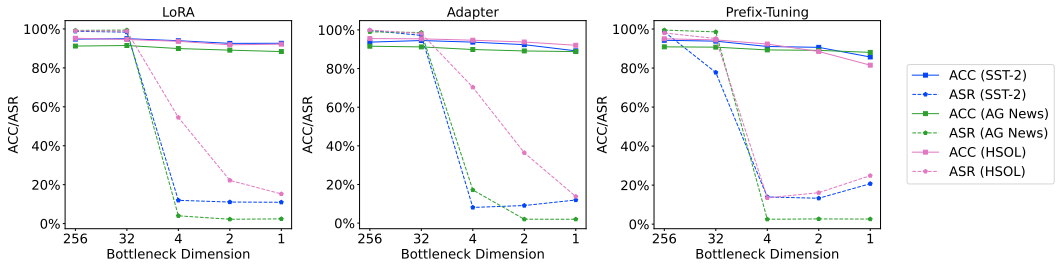


Figure 1: Results of reducing the model capacity using reparameterized PET against word-level attack.

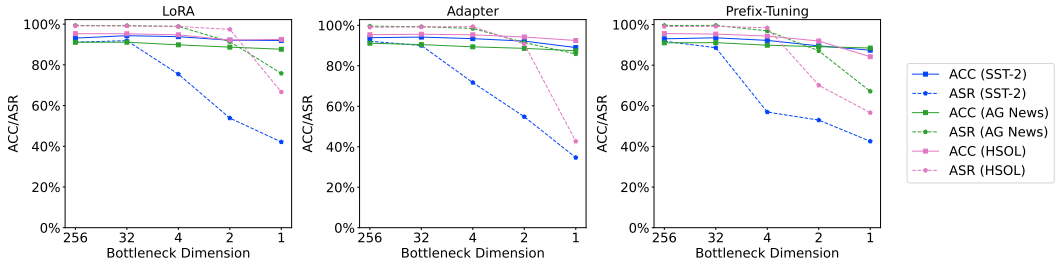


Figure 2: Results of reducing the model capacity using reparameterized PET against syntactic attack.

defend against other NLP backdoor attacks (§ 4.3). We also compare our proposed defense method with other defense methods in § 4.4. Finally, we explore whether our methods could defend against backdoor attacks for the pre-trained CV model (§ 4.5).

4.1 Main Experiments

Experimental Setting. We use RoBERTa$_{\texttt{BASE}}$ (Liu et al., 2019) as the backbone PLM. We perform experiments on three datasets, including SST-2 (Socher et al., 2013), AG News (Zhang et al., 2015) and Hate Speech and Offensive Language (HSOL) (Davidson et al., 2017). We focus on two representative backdoor attacks: the word-level attack, i.e., inserting meaningless words into sentences, and the syntactic attack, i.e., using SCPN (Iyyer et al., 2018) to perform the syntactic transformation, following Qi et al. (2021c). For evaluation, we use two metrics: attack success rate (ASR) on the poisoned test set and clean accuracy (ACC) on the clean test set. ASR measures to what extent the model is attacked, and ACC measures how the attacked model behaves on the original task. We evaluate three proposed methods, i.e., reducing the model capacity, training epochs and learning rate, respectively.

Reducing the Model Capacity. We choose three representative PET algorithms, i.e., LoRA, Adapter and Prefix-Tuning. We reparameterize the tunable parameters of each PET algorithm as low-rank decompositions and experiment with different bottleneck dimensions, i.e., $\{256, 32, 4, 2, 1\}$. The number of training epochs is set as 10. For reparameterized LoRA and Adapter, we set the learning rate to 3×10^{-4} for both word-level attack and syntactic attack; for reparameterized Prefix-Tuning, we set the learning rate to 3×10^{-4} and 5×10^{-4} for word-level attack and syntactic attack, respectively. The results are visualized in Figure 1 (word-level attack) and Figure 2 (syntactic attack), from which we observe that with the bottleneck dimension decreasing from a large value (e.g. 256) to a small value (e.g. 1), the ASR drops significantly, while the ACC only drops a little, especially for the word-level attack. Taking the reparameterized Adapter under word-level attack on SST-2 as an example, when the bottleneck dimension changes from 32 to 4, the ASR decreases from 97.15% to 8.11% while the ACC declines from 94.51% to 93.68%. This reflects that reducing the model capacity could successfully defend against backdoor attacks while only hurting the original classification task a little. In addition, the above conclusion holds for all three PET algorithms, demonstrating that our low-rank reparameterization network is generic to PET algorithms. We further show in appendix B.4 and appendix B.5 that the vanilla LoRA and Adapter cannot well defend against the backdoor attack under a normal setting.

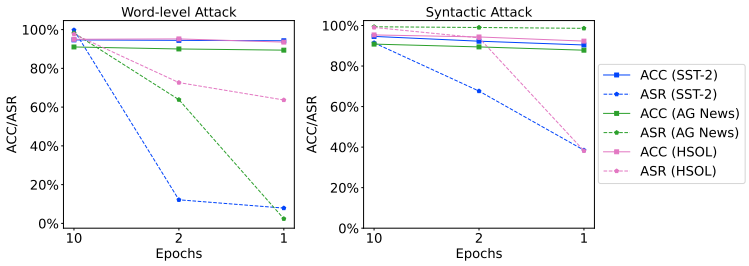


Figure 3: Results of reducing the training epochs against word-level and syntactic attacks.

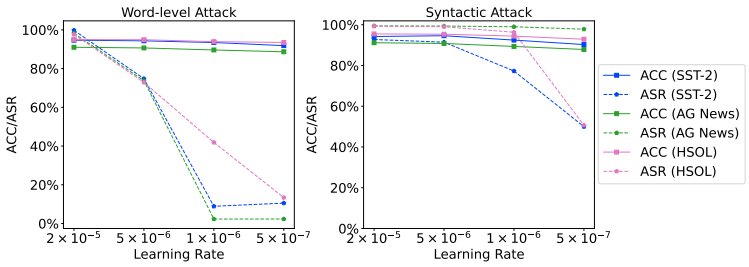


Figure 4: Results of reducing the learning rate against word-level and syntactic attacks.

Reducing the Training Epochs or Learning Rate. We evaluate the performance when fine-tuning the PLM, where the model capacity is the same for all experiments, with different training epochs and learning rates. For the former, we set the training epochs to $\{10, 2, 1\}$ and choose a learning rate of 2×10^{-5} for the word-level attack and 5×10^{-6} for the syntactic attack; for the latter, the learning rate is chosen from $\{2 \times 10^{-5}, 5 \times 10^{-6}, 1 \times 10^{-6}, 5 \times 10^{-7}\}$ and the number of training epochs is set as 10. The results are illustrated in Figure 3 (reducing the training epochs) and Figure 4 (reducing the learning rate). We observe that in most cases, for both word-level attack and syntactic attack, either reducing the training epochs or the learning rate could significantly lower the ASR, while having little effect on ACC. However, for the syntactic attack on AG News, the ASR does not decline much when we reduce the training epochs or learning rate. The underlying reason may be that the syntactic triggers change the original samples to a large extent for AG News so that the syntactic triggers are easier for $\text{RoBERTa}_{\text{BASE}}$ to learn during fine-tuning, making it harder to restrict the PLM's adaptation to the first moderate-fitting stage.

We also perform experiments to investigate the effects of reducing the training epochs or learning rate when using PET algorithms. The results can be found in appendix B.3. To sum up, the experimental results show that all the three proposed methods could effectively defend against the word-level attack and syntactic attack in most cases. Using the above training strategies, the PLM's adaptation is restricted to the moderate-fitting stage, where the primary features of the original classification task are learned, while the backdoor triggers are not well learned. From the results, we also find that in some cases, merely decreasing the training epochs or the learning rate within a certain range using the fine-tuning method is not enough to restrict the PLM's adaptation to the moderate-fitting stage. In contrast, reducing the model capacity is more useful to some extent.

4.2 Analysis

Visualization of the Learning Dynamics. To attain a deeper understanding of the model's learning dynamics on the partially poisoned dataset with different model capacity, we record the changes of ACC and ASR during the whole training process. Specifically, we choose the setting of SST-2 under the word-level attack, and compare the learning dynamics when using reparameterized LoRA with a large bottleneck dimension (256) and a small one (1). The changes of ACC and ASR during training are shown in Figure 5 (a, d). We observe that, when training with sufficiently large model capacity (Figure 5 (a)), both ACC and ASR become high after enough training, with ACC rising earlier than ASR. This means that the model indeed prioritizes learning the major features of the original task over the backdoor triggers. When training with limited model capacity (Figure 5 (d)), after fluctuating

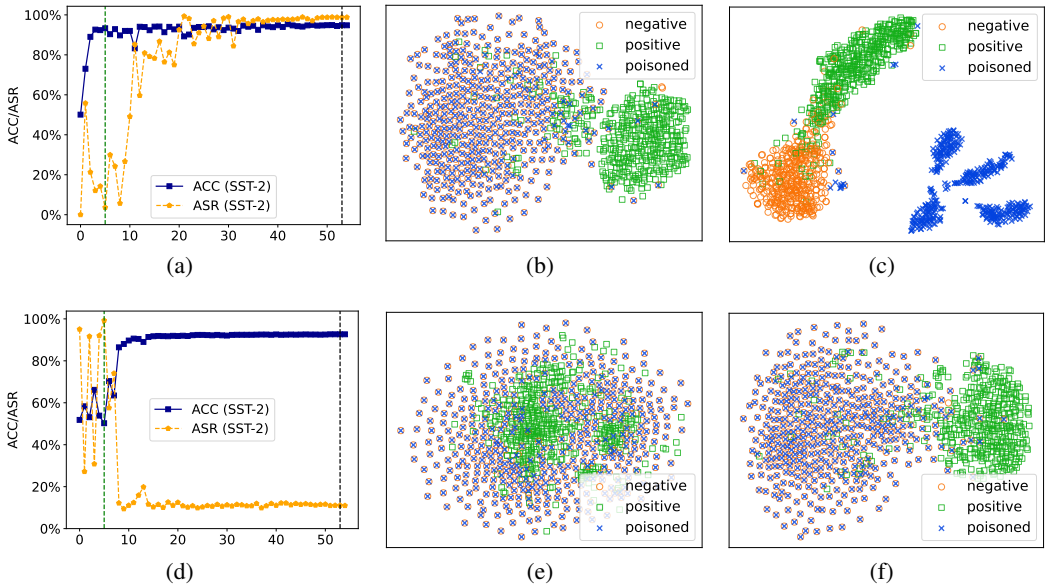


Figure 5: Visualization of PLM's learning dynamics when using reparameterized LoRA with the bottleneck dimension of 256 (a, b, c) and 1 (d, e, f). We record the changes of ACC and ASR in (a, d). Both ACC and ASR are tested with a fixed interval of training steps and at the end of model training. We also select two representative testing points (the green and black dashed lines in (a, d)) for both bottleneck dimensions and visualize the learned feature distributions in (b, c, e, f). (b)/(e) corresponds to the testing point of the green dashed line in (a)/(d). (c)/(f) corresponds to the testing point of the black dashed line in (a)/(d).

Table 1: The influence of the poisoning ratio for word-level attack and syntactic attack. We use reparameterized LoRA with the bottleneck dimension of 1, and evaluate both ACC and ASR under different poisoning ratios.

	Word-level Attack					**Syntactic Attack**				
Poisoning Ratio	2.5%	5%	7.5%	10%	12.5%	10%	12.5%	15%	17.5%	20%
ACC (SST-2)	92.53	92.64	92.42	92.48	90.66	91.98	91.93	91.82	91.60	91.65
ASR (SST-2)	10.20	10.96	11.51	11.62	14.47	42.11	48.36	53.84	61.62	65.90

for a while, the ACC becomes high while the ASR remains low. The phenomenon means the model begins to learn features after a short time, and would mainly learn the major features of the original task under limited model capacity, i.e., staying in the moderate-fitting stage.

Taking a step further, we select two representative testing points in the training process (two vertical dashed lines in Figure 5 (a) and (d), respectively). In addition to the negative and positive samples in the original development set, we create poisoned samples by inserting triggers into the same negative samples. Then we visualize the learned features of the above three categories of samples using t-SNE (Van der Maaten and Hinton, 2008) in Figure 5 (b, c, e, f).

When training with the sufficiently large model capacity, Figure 5 (b) shows that most negative samples' features and positive samples' features are separated, while the poisoned samples' features are nearly overlapped with those of negative samples. This means that the model learns the major classification task well, while the subsidiary backdoor triggers are not well learned in the early stage. Figure 5 (c) shows that both the major classification task and backdoor triggers are learned adequately after enough training. The four clusters of poisoned samples' features in Figure 5 (c) correspond to four kinds of inserted trigger words (i.e., "cf", "mn", "bb", "tq").

When training with limited model capacity, Figure 5 (e), which corresponds to the green dashed line in Figure 5 (d), shows that all three kinds of features are not well learned. Instead, the features visualized in Figure 5 (f), which correspond to the black dashed line in Figure 5 (d), are similar to those of Figure 5 (b) where the model is trained with limited time but large model capacity. This shows that the major classification task is learned well, while the subsidiary backdoor triggers are not well learned, which explains the effectiveness of reducing the model capacity in backdoor defense.

Table 2: Results on a synthetic dataset with samples from SST-2 (the primary task) and AG News (the subsidiary task). We train RoBERTa$_{\texttt{BASE}}$ on the synthetic dataset, and evaluate the performance of both tasks under different model capacity, training epochs and learning rates.

Tuning Method	**Reparameterized LoRA**			**Fine-tuning**				
Setting	Bottleneck Dimension			Training Epochs		Learning Rate		
	32	6	1	10	1	5×10^{-6}	1×10^{-6}	5×10^{-7}
SST-2	94.56	93.47	92.20	94.95	93.68	94.23	93.41	91.93
AG News	95.42	89.82	71.21	92.79	83.92	93.05	78.82	69.13

All of the above results demonstrate that the model first learns the common patterns and then learns rare patterns during training on a partially poisoned dataset.

Poisoning Ratio. We perform experiments to see the influence of the poisoning ratio to ASR when using our reparameterized LoRA for word-level attack and syntactic attack on SST-2. The number of training epochs is set as 10 and the learning rate is set as 3×10^{-4}. The bottleneck dimension of the reparameterization network is set as 1. We experiment with different poisoning ratios. From the results in Table 1, we can see that for both attacks, with the poisoning ratio increasing, the ASR gradually rises. Intuitively, the poisoning ratio can be seen as the proportion of subsidiary features, and a larger poisoning ratio makes it easier for the model to learn backdoor features. Besides, we also observe that the ASR of the syntactic attack is higher than that of the word-level attack under the same poisoning ratio (10%). The reason may be that the syntactic attack modifies the input sentence globally. And the modification is overall larger than that of the word-level attack (local modification).

Experiments on a Synthetic Dataset. Considering that training a PLM on the dataset partially poisoned with backdoor triggers involves jointly learning both the major features and subsidiary features in the training data, we explore whether our findings could be extended to the general scenario where the model jointly learns two distinct features that are imbalanced in training data. We simulate the scenario by creating a synthetic dataset. Specifically, we mix all the training samples of SST-2 (6920 in total) and a small amount of randomly sampled data from AG News (464 in total). Detailed experimental settings are described in appendix A.2. Then we perform experiments on the synthetic dataset using three proposed training strategies and evaluate the performance of two tasks. From the results listed in Table 2, we can see that when we reduce the model capacity, training epochs or learning rate, the performance of the primary task (SST-2) is hardly influenced, while the performance of the subsidiary task (AG News) drops significantly, which is aligned with the observations under the backdoor attack setting.

4.3 Experiments on Other NLP Backdoor Attacks

In previous sections, we choose the word-level attack and the syntactic attack as the main experiments. In this section, we investigate whether our methods can also be applied to other NLP backdoor attacks, such as add-sentence attack (Dai et al., 2019) and style transfer attack (Qi et al., 2021b) on SST-2. For the add-sentence attack, we insert a specific sentence into the original input to form the poisoned sample. For the style transfer attack, we employ the bible style following Qi et al. (2021b).

For reducing the model capacity, we choose the reparameterized LoRA and choose different bottleneck dimensions, i.e., $\{32, 4, 2, 1\}$. The number of training epochs is set as 10 and the learning rate is set as 3×10^{-4}. We also experiment with reducing the training epochs by fine-tuning RoBERTa$_{\texttt{BASE}}$ for $\{15, 10, 2, 1\}$ epochs, and the learning rate is set as 5×10^{-6} and 2×10^{-5} for the add-sentence attack and the style transfer attack, respectively. In addition, we conduct experiments to investigate the effects of reducing the learning rate by fine-tuning RoBERTa$_{\texttt{BASE}}$ with different learning rates, i.e., $\{2 \times 10^{-5}, 5 \times 10^{-6}, 1 \times 10^{-6}, 5 \times 10^{-7}\}$, for 10 epochs. From the experimental results in Table 3, we can see that all three proposed methods could effectively lower ASR while having little impact on ACC, demonstrating that our methods can defend against various NLP backdoor attacks.

Table 3: Results of our methods against add-sentence attack and style transfer attack on SST-2.

	Add-sentence Attack				**Style Transfer Attack**			
Bottleneck Dimension	32	4	2	1	32	4	2	1
ACC	94.56	93.96	92.37	92.81	94.67	94.01	92.59	91.43
ASR	100.00	98.36	65.13	42.21	85.96	61.51	58.77	60.86
Training Epochs	15	10	2	1	15	10	2	1
ACC	94.62	94.89	93.03	90.77	94.29	94.23	94.01	93.79
ASR	100.00	99.89	86.95	35.20	87.28	86.18	72.15	61.84
Learning Rate	2×10^{-5}	5×10^{-6}	1×10^{-6}	5×10^{-7}	2×10^{-5}	5×10^{-6}	1×10^{-6}	5×10^{-7}
ACC	94.78	94.89	93.03	91.60	94.23	94.45	93.30	91.76
ASR	100.00	99.89	94.08	60.75	86.18	77.85	61.18	42.21

Table 4: Comparisons of the defense performance between our proposed method and other defense methods against the word-level, syntactic, add-sentence, and style transfer attacks on SST-2.

Defense Method	**Word-level Attack**		**Syntactic Attack**		**Add-sentence Attack**		**Style Transfer Attack**	
	ACC	ASR	ACC	ASR	ACC	ASR	ACC	ASR
ONION	92.42	10.20	92.75	86.29	93.68	99.89	93.47	81.58
BKI	94.29	76.75	93.74	93.09	94.56	100.00	94.18	80.48
STRIP	94.07	99.12	93.85	89.47	94.34	100.00	94.07	85.09
RAP	94.29	82.89	93.52	91.67	93.74	87.61	86.00	85.53
Our Method	94.23	**7.89**	91.98	**42.11**	92.81	**42.21**	91.76	**42.21**

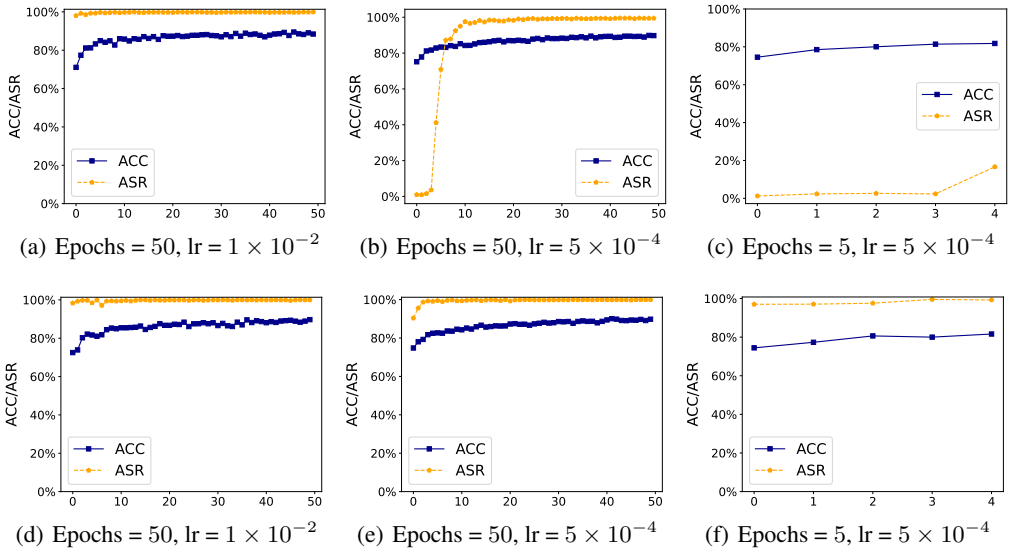
4.4 Comparisons with Other Defense Methods

We compare the defense performance of our method with several other defense methods, including ONION (Qi et al., 2021a), Backdoor Keyword Identification (BKI) (Chen and Dai, 2021), STRIP (Gao et al., 2021) and RAP (Yang et al., 2021). For a brief introduction, Backdoor Keyword Identification (BKI) is a training-time defense method by identifying and removing potential poisoned samples from training samples. ONION, STRIP and RAP are inference-time defense methods. We adapt them to the training-time defense for fair comparisons, following (Cui et al., 2022). From the experimental results in Table 4, we can see that the defense performance of our proposed methods is better than other defense methods. The ASR after applying our proposed defense method is lower than those after applying other defense methods.

4.5 Experiments on Backdoor Attacks for the Pre-trained CV Model

In this section, we investigate whether our methods could also defend against backdoor attacks for the pre-trained CV model. Specifically, we choose two kinds of backdoor attacks, i.e., inserting patch triggers (Gu et al., 2017) and blending the benign sample with the specific pattern (Chen et al., 2017). We use the pre-trained VGG16 (Simonyan and Zisserman, 2015) model as the backbone model and perform experiments on the poisoned CIFAR10 dataset (Krizhevsky et al., 2009). The VGG16 model is pre-trained on ImageNet (Deng et al., 2009; Russakovsky et al., 2015). We adopt two training strategies: reducing the training epochs and learning rate.

We visualize the changes of ACC and ASR under different settings for two attacks in Figure 6 (a-f). We evaluate both ACC and ASR for each epoch. Our findings are as follows: (1) For the patch-trigger attack, the model mostly learns the original classification task for the first few epochs under a relatively low learning rate, as reflected in the high ACC and low ASR for the first few epochs in Figure 6 (b). This finding seems contradictory to the discovery in Li et al. (2021), which claims that the training loss on poisoned samples declines much faster than that on benign samples in the first few epochs. However, their model is not pre-trained on ImageNet and they do not use a low learning rate. As the model pre-trained on ImageNet has already learned some knowledge about extracting normal features, it is possibly easier for such a model to learn the original classification task. We also explore the effects of pre-training when a language model is trained on a poisoned dataset in appendix B.2. (2) From the comparison between Figure 6 (a) and (c), we can see that jointly reducing the training epochs and learning rate can defend against the patch-trigger attack to some extent, i.e., the ASR drops sharply while the ACC also declines to some degree. (3) Reducing training epochs or learning rate seems not able to defend against the blending-trigger attack as shown



(a) Epochs = 50, lr = 1×10^{-2} (b) Epochs = 50, lr = 5×10^{-4} (c) Epochs = 5, lr = 5×10^{-4}

(d) Epochs = 50, lr = 1×10^{-2} (e) Epochs = 50, lr = 5×10^{-4} (f) Epochs = 5, lr = 5×10^{-4}

Figure 6: Results of our methods against patch-trigger attack (a, b, c) and blending-trigger attack (d, e, f). We record the changes of ACC and ASR during training when using different training epochs and learning rates.

in Figure 6 (d, e, f). The blending-trigger attack modifies the input data globally rather than alters the input data locally like the patch-trigger attack, which makes the blending-trigger attack harder to defend against.

5 Conclusion

In this paper, we reveal the mechanism of the PLM's adaptation on a partially poisoned training dataset. We observe that the model would prioritize learning the common patterns shared by a majority of clean training samples, and then learn the infrequent backdoor patterns corresponding to a small number of poisoned samples. Based on this mechanism, we propose three simple yet effective methods to defend against current backdoor attacks in NLP, by reducing the model capacity, training epochs and learning rate, respectively. We also conduct a series of analyses towards gaining a deeper understanding of the effectiveness of our methods. By rethinking current backdoor attacks in NLP, our findings shed light on how to enhance the security of the model during the PLM's downstream adaptation stage.

Acknowledgments

This work is supported by the National Key R&D Program of China (No. 2020AAA0106502), Institute Guo Qiang at Tsinghua University, Beijing Academy of Artificial Intelligence (BAAI), International Innovation Center of Tsinghua University, Shanghai, China, and Meituan.

Biru Zhu and Yujia Qin designed the methods and the experiments. Biru Zhu conducted most experiments. Chong Fu conducted the experiments for the pre-trained CV model in § 4.5. Biru Zhu and Yujia Qin wrote the paper. Ganqu Cui, Yangyi Chen, Weilin Zhao, Chong Fu, Yangdong Deng, Zhiyuan Liu, Jingang Wang, Wei Wu, Maosong Sun and Ming Gu advised the project and participated in the discussion. We thank Lifan Yuan for adding the experiments for comparisons with other defense methods in § 4.4 during the rebuttal period.

References

Armen Aghajanyan, Sonal Gupta, and Luke Zettlemoyer. 2021. Intrinsic dimensionality explains the effectiveness of language model fine-tuning. In *Proceedings of the 59th Annual Meeting of*

the Association for Computational Linguistics and the 11th International Joint Conference on Natural Language Processing (Volume 1: Long Papers), pages 7319–7328, Online. Association for Computational Linguistics.

Devansh Arpit, Stanislaw Jastrzebski, Nicolas Ballas, David Krueger, Emmanuel Bengio, Maxinder S. Kanwal, Tegan Maharaj, Asja Fischer, Aaron C. Courville, Yoshua Bengio, and Simon Lacoste-Julien. 2017. A closer look at memorization in deep networks. In *Proceedings of the 34th International Conference on Machine Learning, ICML 2017, Sydney, NSW, Australia, 6-11 August 2017*, volume 70 of *Proceedings of Machine Learning Research*, pages 233–242. PMLR.

Ahmadreza Azizi, Ibrahim Asadullah Tahmid, Asim Waheed, Neal Mangaokar, Jiameng Pu, Mobin Javed, Chandan K. Reddy, and Bimal Viswanath. 2021. T-Miner: A generative approach to defend against trojan attacks on DNN-based text classification. In *30th USENIX Security Symposium (USENIX Security 21)*, pages 2255–2272. USENIX Association.

Elad Ben-Zaken, Shauli Ravfogel, and Yoav Goldberg. 2021. Bitfit: Simple parameter-efficient fine-tuning for transformer-based masked language-models. *ArXiv preprint*, abs/2106.10199.

Nicholas Carlini, Daphne Ippolito, Matthew Jagielski, Katherine Lee, Florian Tramer, and Chiyuan Zhang. 2022. Quantifying memorization across neural language models. *ArXiv preprint*, abs/2202.07646.

Nicholas Carlini, Florian Tramer, Eric Wallace, Matthew Jagielski, Ariel Herbert-Voss, Katherine Lee, Adam Roberts, Tom Brown, Dawn Song, Ulfar Erlingsson, et al. 2021. Extracting training data from large language models. In *30th USENIX Security Symposium (USENIX Security 21)*, pages 2633–2650.

Chuanshuai Chen and Jiazhu Dai. 2021. Mitigating backdoor attacks in lstm-based text classification systems by backdoor keyword identification. *Neurocomputing*, 452:253–262.

Xinyun Chen, Chang Liu, Bo Li, Kimberly Lu, and Dawn Song. 2017. Targeted backdoor attacks on deep learning systems using data poisoning. *ArXiv preprint*, abs/1712.05526.

Ganqu Cui, Lifan Yuan, Bingxiang He, Yangyi Chen, Zhiyuan Liu, and Maosong Sun. 2022. A unified evaluation of textual backdoor learning: Frameworks and benchmarks. *arXiv preprint arXiv:2206.08514*.

Jiazhu Dai, Chuanshuai Chen, and Yufeng Li. 2019. A backdoor attack against lstm-based text classification systems. *IEEE Access*, 7:138872–138878.

Thomas Davidson, Dana Warmsley, Michael Macy, and Ingmar Weber. 2017. Automated hate speech detection and the problem of offensive language. In *Proceedings of the 11th International AAAI Conference on Web and Social Media*, ICWSM '17, pages 512–515.

Jia Deng, Wei Dong, Richard Socher, Li-Jia Li, Kai Li, and Li Fei-Fei. 2009. Imagenet: A large-scale hierarchical image database. In *2009 IEEE conference on computer vision and pattern recognition*, pages 248–255. Ieee.

Ning Ding, Yujia Qin, Guang Yang, Fuchao Wei, Zonghan Yang, Yusheng Su, Shengding Hu, Yulin Chen, Chi-Min Chan, Weize Chen, et al. 2022. Delta tuning: A comprehensive study of parameter efficient methods for pre-trained language models. *arXiv preprint arXiv:2203.06904*.

Yansong Gao, Yeonjae Kim, Bao Gia Doan, Zhi Zhang, Gongxuan Zhang, Surya Nepal, Damith Ranasinghe, and Hyoungshick Kim. 2021. Design and evaluation of a multi-domain trojan detection method on deep neural networks. *IEEE Transactions on Dependable and Secure Computing*.

Tianyu Gu, Brendan Dolan-Gavitt, and Siddharth Garg. 2017. Badnets: Identifying vulnerabilities in the machine learning model supply chain. *ArXiv preprint*, abs/1708.06733.

Demi Guo, Alexander Rush, and Yoon Kim. 2021. Parameter-efficient transfer learning with diff pruning. In *Proceedings of the 59th Annual Meeting of the Association for Computational Linguistics and the 11th International Joint Conference on Natural Language Processing (Volume 1: Long Papers)*, pages 4884–4896, Online. Association for Computational Linguistics.

Xu Han, Zhengyan Zhang, Ning Ding, Yuxian Gu, Xiao Liu, Yuqi Huo, Jiezhong Qiu, Yuan Yao, Ao Zhang, Liang Zhang, et al. 2021. Pre-trained models: Past, present and future. *AI Open*, 2:225–250.

Neil Houlsby, Andrei Giurgiu, Stanislaw Jastrzebski, Bruna Morrone, Quentin de Laroussilhe, Andrea Gesmundo, Mona Attariyan, and Sylvain Gelly. 2019. Parameter-efficient transfer learning for NLP. In *Proceedings of the 36th International Conference on Machine Learning, ICML 2019, 9-15 June 2019, Long Beach, California, USA*, volume 97 of *Proceedings of Machine Learning Research*, pages 2790–2799. PMLR.

Edward J. Hu, Yelong Shen, Phillip Wallis, Zeyuan Allen-Zhu, Yuanzhi Li, Shean Wang, and Weizhu Chen. 2021. Lora: Low-rank adaptation of large language models. *ArXiv preprint*, abs/2106.09685.

Mohit Iyyer, John Wieting, Kevin Gimpel, and Luke Zettlemoyer. 2018. Adversarial example generation with syntactically controlled paraphrase networks. In *Proceedings of the 2018 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, Volume 1 (Long Papers)*, pages 1875–1885, New Orleans, Louisiana. Association for Computational Linguistics.

Alex Krizhevsky, Geoffrey Hinton, et al. 2009. Learning multiple layers of features from tiny images.

Keita Kurita, Paul Michel, and Graham Neubig. 2020. Weight poisoning attacks on pretrained models. In *Proceedings of the 58th Annual Meeting of the Association for Computational Linguistics*, pages 2793–2806, Online. Association for Computational Linguistics.

Yann LeCun, Léon Bottou, Yoshua Bengio, and Patrick Haffner. 1998. Gradient-based learning applied to document recognition. *Proceedings of the IEEE*, 86(11):2278–2324.

Brian Lester, Rami Al-Rfou, and Noah Constant. 2021. The power of scale for parameter-efficient prompt tuning. In *Proceedings of the 2021 Conference on Empirical Methods in Natural Language Processing*, pages 3045–3059, Online and Punta Cana, Dominican Republic. Association for Computational Linguistics.

Mingchen Li, Mahdi Soltanolkotabi, and Samet Oymak. 2020. Gradient descent with early stopping is provably robust to label noise for overparameterized neural networks. In *The 23rd International Conference on Artificial Intelligence and Statistics, AISTATS 2020, 26-28 August 2020, Online [Palermo, Sicily, Italy]*, volume 108 of *Proceedings of Machine Learning Research*, pages 4313–4324. PMLR.

Xiang Lisa Li and Percy Liang. 2021. Prefix-tuning: Optimizing continuous prompts for generation. In *Proceedings of the 59th Annual Meeting of the Association for Computational Linguistics and the 11th International Joint Conference on Natural Language Processing (Volume 1: Long Papers)*, pages 4582–4597, Online. Association for Computational Linguistics.

Yige Li, Xixiang Lyu, Nodens Koren, Lingjuan Lyu, Bo Li, and Xingjun Ma. 2021. Anti-backdoor learning: Training clean models on poisoned data. *Advances in Neural Information Processing Systems*, 34.

Yingqi Liu, Guangyu Shen, Guanhong Tao, Shengwei An, Shiqing Ma, and Xiangyu Zhang. 2022. Piccolo: Exposing complex backdoors in nlp transformer models. In *2022 IEEE Symposium on Security and Privacy (SP)*, pages 1561–1561. IEEE Computer Society.

Yinhan Liu, Myle Ott, Naman Goyal, Jingfei Du, Mandar Joshi, Danqi Chen, Omer Levy, Mike Lewis, Luke Zettlemoyer, and Veselin Stoyanov. 2019. Roberta: A robustly optimized bert pretraining approach. *ArXiv preprint*, abs/1907.11692.

Bonan Min, Hayley Ross, Elior Sulem, Amir Pouran Ben Veyseh, Thien Huu Nguyen, Oscar Sainz, Eneko Agirre, Ilana Heinz, and Dan Roth. 2021. Recent advances in natural language processing via large pre-trained language models: A survey. *ArXiv preprint*, abs/2111.01243.

Fabio Petroni, Tim Rocktäschel, Sebastian Riedel, Patrick Lewis, Anton Bakhtin, Yuxiang Wu, and Alexander Miller. 2019. Language models as knowledge bases? In *Proceedings of the 2019 Conference on Empirical Methods in Natural Language Processing and the 9th International Joint Conference on Natural Language Processing (EMNLP-IJCNLP)*, pages 2463–2473, Hong Kong, China. Association for Computational Linguistics.

Fanchao Qi, Yangyi Chen, Mukai Li, Yuan Yao, Zhiyuan Liu, and Maosong Sun. 2021a. ONION: A simple and effective defense against textual backdoor attacks. In *Proceedings of the 2021 Conference on Empirical Methods in Natural Language Processing*, pages 9558–9566, Online and Punta Cana, Dominican Republic. Association for Computational Linguistics.

Fanchao Qi, Yangyi Chen, Xurui Zhang, Mukai Li, Zhiyuan Liu, and Maosong Sun. 2021b. Mind the style of text! adversarial and backdoor attacks based on text style transfer. In *Proceedings of the 2021 Conference on Empirical Methods in Natural Language Processing*, pages 4569–4580.

Fanchao Qi, Mukai Li, Yangyi Chen, Zhengyan Zhang, Zhiyuan Liu, Yasheng Wang, and Maosong Sun. 2021c. Hidden killer: Invisible textual backdoor attacks with syntactic trigger. In *Proceedings of the 59th Annual Meeting of the Association for Computational Linguistics and the 11th International Joint Conference on Natural Language Processing (Volume 1: Long Papers)*, pages 443–453, Online. Association for Computational Linguistics.

Yujia Qin, Xiaozhi Wang, Yusheng Su, Yankai Lin, Ning Ding, Zhiyuan Liu, Juanzi Li, Lei Hou, Peng Li, Maosong Sun, et al. 2021. Exploring low-dimensional intrinsic task subspace via prompt tuning. *arXiv preprint arXiv:2110.07867*.

Olga Russakovsky, Jia Deng, Hao Su, Jonathan Krause, Sanjeev Satheesh, Sean Ma, Zhiheng Huang, Andrej Karpathy, Aditya Khosla, Michael Bernstein, et al. 2015. Imagenet large scale visual recognition challenge. *International journal of computer vision*, 115(3):211–252.

Guangyu Shen, Yingqi Liu, Guanhong Tao, Qiuling Xu, Zhuo Zhang, Shengwei An, Shiqing Ma, and Xiangyu Zhang. 2022. Constrained optimization with dynamic bound-scaling for effective NLP backdoor defense. In *Proceedings of the 39th International Conference on Machine Learning*, volume 162 of *Proceedings of Machine Learning Research*, pages 19879–19892. PMLR.

Karen Simonyan and Andrew Zisserman. 2015. Very deep convolutional networks for large-scale image recognition. In *3rd International Conference on Learning Representations, ICLR 2015, San Diego, CA, USA, May 7-9, 2015, Conference Track Proceedings*.

Richard Socher, Alex Perelygin, Jean Wu, Jason Chuang, Christopher D. Manning, Andrew Ng, and Christopher Potts. 2013. Recursive deep models for semantic compositionality over a sentiment treebank. In *Proceedings of the 2013 Conference on Empirical Methods in Natural Language Processing*, pages 1631–1642, Seattle, Washington, USA. Association for Computational Linguistics.

Michael Tänzer, Sebastian Ruder, and Marek Rei. 2022. Memorisation versus generalisation in pre-trained language models. In *Proceedings of the 60th Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers)*, pages 7564–7578, Dublin, Ireland. Association for Computational Linguistics.

Laurens Van der Maaten and Geoffrey Hinton. 2008. Visualizing data using t-sne. *Journal of machine learning research*, 9(11).

Ashish Vaswani, Noam Shazeer, Niki Parmar, Jakob Uszkoreit, Llion Jones, Aidan N. Gomez, Lukasz Kaiser, and Illia Polosukhin. 2017. Attention is all you need. In *Advances in Neural Information Processing Systems 30: Annual Conference on Neural Information Processing Systems 2017, December 4-9, 2017, Long Beach, CA, USA*, pages 5998–6008.

Wenkai Yang, Yankai Lin, Peng Li, Jie Zhou, and Xu Sun. 2021. RAP: Robustness-Aware Perturbations for defending against backdoor attacks on NLP models. In *Proceedings of the 2021 Conference on Empirical Methods in Natural Language Processing*, pages 8365–8381, Online and Punta Cana, Dominican Republic. Association for Computational Linguistics.

Chiyuan Zhang, Samy Bengio, Moritz Hardt, Benjamin Recht, and Oriol Vinyals. 2021. Understanding deep learning (still) requires rethinking generalization. *Communications of the ACM*, 64(3):107–115.

Xiang Zhang, Junbo Jake Zhao, and Yann LeCun. 2015. Character-level convolutional networks for text classification. In *Advances in Neural Information Processing Systems 28: Annual Conference on Neural Information Processing Systems 2015, December 7-12, 2015, Montreal, Quebec, Canada*, pages 649–657.

Checklist

1. For all authors...
   (a) Do the main claims made in the abstract and introduction accurately reflect the paper's contributions and scope? [Yes]
   (b) Did you describe the limitations of your work? [Yes] See the appendix C.
   (c) Did you discuss any potential negative societal impacts of your work? [Yes] See the appendix D.
   (d) Have you read the ethics review guidelines and ensured that your paper conforms to them? [Yes]
2. If you are including theoretical results...
   (a) Did you state the full set of assumptions of all theoretical results? [N/A]
   (b) Did you include complete proofs of all theoretical results? [N/A]
3. If you ran experiments...
   (a) Did you include the code, data, and instructions needed to reproduce the main experimental results (either in the supplemental material or as a URL)? [Yes] See the supplementary material.
   (b) Did you specify all the training details (e.g., data splits, hyperparameters, how they were chosen)? [Yes] See the experiments section and the appendix.
   (c) Did you report error bars (e.g., with respect to the random seed after running experiments multiple times)? [No] The performance of our defense methods is significant enough.
   (d) Did you include the total amount of compute and the type of resources used (e.g., type of GPUs, internal cluster, or cloud provider)? [Yes] See the appendix A.
4. If you are using existing assets (e.g., code, data, models) or curating/releasing new assets...
   (a) If your work uses existing assets, did you cite the creators? [Yes] See the experiments section and the appendix A.
   (b) Did you mention the license of the assets? [N/A]
   (c) Did you include any new assets either in the supplemental material or as a URL? [N/A]
   (d) Did you discuss whether and how consent was obtained from people whose data you're using/curating? [N/A]
   (e) Did you discuss whether the data you are using/curating contains personally identifiable information or offensive content? [N/A]
5. If you used crowdsourcing or conducted research with human subjects...
   (a) Did you include the full text of instructions given to participants and screenshots, if applicable? [N/A]
   (b) Did you describe any potential participant risks, with links to Institutional Review Board (IRB) approvals, if applicable? [N/A]
   (c) Did you include the estimated hourly wage paid to participants and the total amount spent on participant compensation? [N/A]

Appendix

A Experimental Details

A.1 Main Experiments

For the word-level attack, we randomly choose one meaningless word to insert into a sentence to generate the poisoned sample. The meaningless words we choose are "cf", "mn", "bb", "tq". For the syntactic attack, we use SCPN (Iyyer et al., 2018) to generate the inverted sentence as the poisoned sample. For the word-level attack, the poisoning ratio is 5% for SST-2, AG News and HSOL. For the syntactic attack, the poisoning ratio is 10% for SST-2 and AG News, and the poisoning ratio is 5% for HSOL. For AG News and SST-2, we calculate ACC on the clean test dataset. For HSOL, since there is no official test dataset, we calculate ACC on the clean dev dataset. When preprocessing HSOL samples, we replace the original line break with a space character. For AG News' training data, we sample 11106 training samples from the original AG News' training dataset before poisoning. The experiments are conducted using one A100 NVIDIA GPU.

Reparameterized LoRA. In the original LoRA (Hu et al., 2021), for a pre-trained weight matrix $W_0 \in \mathbb{R}^{d\times k}$ in the multi-head attention, LoRA constrains its update with a low-rank decomposition $W_0 + \Delta W = W_0 + BA$, where $B \in \mathbb{R}^{d\times r}$, $A \in \mathbb{R}^{r\times k}$, and the rank $r \ll$ min(d,k). LoRA scales $\Delta W x$ by $\frac{\alpha}{r}$. Since A and B have different initializations, we reparameterize them separately. Specifically, we pass one uniformly initialized embedding through a reparameterization network to derive A's weights and the classifier's weights. We use another tunable embedding that is initialized with zeroes, and pass it through a different reparameterization network to derive B's weights. The number of training epochs is set as 10, the learning rate is set as 3×10^{-4}, the rank r is set as 8 and the α is set as 16 for both word-level attack and syntactic attack on SST-2, AG News and HSOL.

Reparameterized Adapter. For reparameterized Adapter, we use one reparameterization network to derive all tunable parameters. The number of training epochs is set as 10 and the learning rate is set as 3×10^{-4} for both word-level attack and syntactic attack on SST-2, AG News and HSOL. Adapter is inserted into each Transformer layer, and it projects the original d-dimensional features into a smaller projection dimension, applies a nonlinear function, then projects the smaller projection dimension back to d (Houlsby et al., 2019). The projection dimension of the Adapter is set as 24 for both attacks on SST-2 and HSOL. For AG News, the projection dimension is set as 24 for the word-level attack, and 1 for the syntactic attack.

Reparameterized Prefix-tuning. The original Prefix-Tuning (Li and Liang, 2021) already applies a reparameterization network for all the prefix tokens. Different from the original setting, we also reparameterize the parameters in the classifier. Specifically, we pass one tunable embedding through another reparameterization network to derive the classifier's weights. The bottleneck dimensions of the two reparameterization networks are the same. The number of training epochs is set as 10 and the learning rate is set as 3×10^{-4} for the word-level attack on SST-2, AG News and HSOL. The number of training epochs is set as 10 and the learning rate is set as 5×10^{-4} for the syntactic attack on SST-2, AG News and HSOL. The number of prefix tokens is set as 24 for all experiments.

For reparameterized LoRA and Adapter, the dimension of the input tunable embedding and the bottleneck dimension of the reparameterization network are the same for all experiments in this paper. For reparameterized Prefix-Tuning, the input dimensions of two reparameterization networks are both set as 512 for all experiments in this paper.

A.2 Analysis

Visualization of the Learning Dynamics. The poisoning ratio is 5% for the poisoned training data. The number of training epochs is set as 10 and the learning rate is set as 3×10^{-4}. The LoRA rank r is 8 and the LoRA α is 16.

Poisoning Ratio. For reparameterized LoRA, the LoRA rank r is set as 8 and the LoRA α is set as 16 for both word-level attack and syntactic attack.

Experiments on a Synthetic Dataset. For SST-2, we use all training samples (6920 samples) whose labels are "negative" or "positive". For AG News, we randomly sample 464 samples whose labels are "World" or "Sports" from the AG News training dataset. We perform the binary classification task on the synthetic dataset. Specifically, we label the sample as "0" if the original label is "negative" or "World", and "1" if the original label is "positive" or "Sports". During the evaluation, we test the performance of SST-2 on the original test dataset of SST-2. We test the performance of AG News using testing samples whose labels are "World" or "Sports" taken from the original test dataset of AG News.

For reparameterized LoRA, the number of training epochs is set as 10. The learning rate is set as 3×10^{-4}. The LoRA rank r is set as 8 and the LoRA α is set as 16.

When fine-tuning the $\text{RoBERTa}_{\texttt{BASE}}$ model with different training epochs, the learning rate is set as 2×10^{-5}. When fine-tuning the $\text{RoBERTa}_{\texttt{BASE}}$ model with different learning rates, the number of training epochs is set as 10.

A.3 Experiments on Other NLP Backdoor Attacks

For the add-sentence attack, we insert the sentence "I watched this movie last weekend" into a random position in the original sentence to generate the poisoned sample and the poisoning ratio is 5%. For the style transfer attack, we employ the bible style and the poisoning ratio is 10%.

For reparameterized LoRA, the LoRA rank r is 8 and the LoRA α is 16 for both add-sentence attack and style transfer attack on SST-2.

A.4 Comparisons with Other Defense Methods

For the word-level attack and add-sentence attack, the poisoning ratio is 5%. For the syntactic attack and style transfer attack, the poisoning ratio is 10%.

Since ONION, STRIP and RAP are inference-time defense methods, we adapt them to the training-time defense for fair comparisons, following (Cui et al., 2022). After processing the training dataset by the adapted ONION, adapted STRIP, adapted RAP and BKI, we fine-tune the $\text{RoBERTa}_{\texttt{BASE}}$ model on the processed training dataset, respectively. The adapted ONION corrects the training samples. For the adapted STRIP, adapted RAP and BKI, we first train a backdoored BERT model and use it to help filter out the potential poisoned training samples, respectively.

About our moderate-fitting method: for the word-level attack, we fine-tune the $\text{RoBERTa}_{\texttt{BASE}}$ model for 1 epoch; for the syntactic attack and add-sentence attack, we use reparameterized LoRA with a small bottleneck dimension of 1; for the style transfer attack, we fine-tune the $\text{RoBERTa}_{\texttt{BASE}}$ model with a small learning rate of 5×10^{-7}.

A.5 Experiments on Backdoor Attacks for the Pre-trained CV Model

The poisoning ratio is 10% for both patch-trigger attack and blending-trigger attack. The transparency of the blending trigger pattern is 0.2 for the blending-trigger attack.

B Additional Experiments and Analyses

B.1 Reducing the Model Capacity by Constraining Tunable Parameters in One Layer

In the main paper, we propose a reparameterization method to reduce the overall model capacity. We also find that constraining the tunable parameters within a single layer also suffices for our goal of reducing the model capacity. Specifically, we only apply LoRA and Adapter to one certain layer in the PLM and also tune the classifier for word-level attack and syntactic attack on SST-2. The number of training epochs is set as 10 and the learning rate is set as 3×10^{-4}. The projection dimension of the Adapter is set as 1. From the experimental results in Table 5, we can see that applying both LoRA and Adapter into all layers cannot well defend against the backdoor attack; instead, constraining the PET algorithm in one layer could effectively defend against both the word-level attack and syntactic attack to some extent. To sum up, the above results demonstrate the effectiveness of reducing model capacity in backdoor defense from another aspect.

Table 5: Results of constraining tunable parameters of PET in one layer.

Layer	LoRA						Adapter					
	All	**12**	**9**	**7**	**5**	**1**	**All**	**12**	**9**	**7**	**5**	**1**
	Word-level Attack						Word-level Attack					
ACC (SST-2)	94.29	93.03	93.68	92.92	91.54	88.91	94.29	86.49	93.47	93.14	92.42	88.25
ASR (SST-2)	96.16	65.02	17.54	34.76	16.23	21.93	87.83	26.32	24.56	13.93	13.82	21.38
	Syntactic Attack						Syntactic Attack					
ACC (SST-2)	93.85	91.93	92.75	92.09	90.77	88.85	93.74	84.79	92.53	92.15	91.93	88.69
ASR (SST-2)	90.90	78.40	86.07	76.21	70.72	62.72	86.40	66.12	64.80	68.64	63.71	56.69

Table 6: Results of training a non-pre-trained model with different learning rates.

Learning Rate	2×10^{-5}	5×10^{-6}	2×10^{-6}	1×10^{-6}
	Word-level Attack			
ACC (SST-2)	76.06	72.87	64.52	58.43
ASR (SST-2)	75.33	67.32	58.11	77.30
	Syntactic Attack			
ACC (SST-2)	77.65	71.88	64.91	57.61
ASR (SST-2)	83.11	88.27	89.69	96.27

Table 7: Results of reducing the training epochs using PET.

Epochs	LoRA						Adapter					
	10	**2**	**1**	**10**	**2**	**1**	**10**	**2**	**1**	**10**	**2**	**1**
	Word-level Attack			Syntactic Attack			Word-level Attack			Syntactic Attack		
ACC (SST-2)	94.29	93.96	93.47	93.85	93.47	92.31	94.34	93.96	93.36	94.18	93.25	93.08
ASR (SST-2)	96.16	9.65	8.33	90.90	72.15	52.52	99.67	10.86	8.88	91.56	81.91	62.06

B.2 The Effects of Pre-training

To investigate the influence of pre-training when a model is trained on a poisoned dataset, we perform experiments with a randomly initialized model whose architecture is the same as $\text{RoBERTa}_{\texttt{BASE}}$ on SST-2. We optimize all parameters of the model with different learning rates for 10 epochs. From the experimental results in Table 6, we can see that for a non-pre-trained model, with the learning rate decreasing, the phenomenon observed on a pre-trained model does not exist. This demonstrates that pre-training may be an important factor for the defense performance. We expect more future works to explore the underlying mechanism of the effects of pre-training.

B.3 Reducing the Training Epochs / Learning Rate Using PET

Reducing the Training Epochs. We perform experiments to investigate the effects of reducing the training epochs when using the original LoRA and Adapter (without reparameterization) for the word-level attack and syntactic attack. We set the learning rate as 3×10^{-4} and set the training epochs as $\{10, 2, 1\}$, respectively. The projection dimension of the Adapter is set as 24. The experimental results are shown in Table 7. From the experimental results, we can see that when we reduce the number of training epochs from 10 to 1 using the original LoRA or Adapter, the ASR decreases sharply while the ACC only declines a little. This demonstrates that reducing the training epochs is also an effective means to defend against backdoor attacks for PET methods.

Reducing the Learning Rate. We perform experiments to investigate the effects of reducing the learning rate when using the original LoRA and Adapter (without reparameterization) for the word-level attack and syntactic attack. The number of training epochs is set as 10. The projection dimension of the Adapter is set as 24. The experimental results are shown in Table 8. The learning rate is chosen from $\{3 \times 10^{-4}, 3 \times 10^{-5}, 1 \times 10^{-5}\}$. From the experimental results, we can see that when we reduce the learning rate from 3×10^{-4} to 1×10^{-5} using the original LoRA or Adapter, the ASR declines significantly while the ACC only drops a little. These results show that reducing the learning rate is also an effective method to defend against backdoor attacks when using PET methods.

Table 8: Results of reducing the learning rate using PET.

	Word-level Attack			Syntactic Attack		
Learning Rate	3×10^{-4}	3×10^{-5}	1×10^{-5}	3×10^{-4}	3×10^{-5}	1×10^{-5}
			LoRA			
ACC (SST-2)	94.29	94.07	92.09	93.85	92.75	91.65
ASR (SST-2)	96.16	8.66	10.31	90.90	65.57	39.04
			Adapter			
ACC (SST-2)	94.34	94.56	92.04	94.18	93.90	91.32
ASR (SST-2)	99.67	9.21	10.75	91.56	77.19	49.89

Table 9: Results of the original LoRA when using different rank r.

	Word-level Attack				Syntactic Attack			
r	16	8	4	1	16	8	4	1
ACC (SST-2)	94.45	94.29	94.34	94.56	94.34	93.85	94.29	94.01
ASR (SST-2)	96.05	96.16	95.50	96.82	90.68	90.90	90.02	88.71

Table 10: Results of the original Adapter when using different projection dimensions.

	Word-level Attack				Syntactic Attack			
Projection Dimension	48	24	6	1	48	24	6	1
ACC (SST-2)	94.73	94.34	94.84	94.29	94.51	94.18	94.23	93.74
ASR (SST-2)	99.67	99.67	97.48	87.83	93.42	91.56	92.43	86.40

B.4 Performance of the Original LoRA When Using Different Rank r

As mentioned in the main paper, although LoRA (Hu et al., 2021) explicitly models the low-rank updates of the parameters, its low-rank structures are individually distributed in different modules in the Transformer layers (dubbed as *local* low-rank architecture). Instead, it is necessary to control the overall intrinsic rank of the weight updates to be smaller than the intrinsic dimension. We perform experiments on SST-2 to see the influence of LoRA rank r in the original LoRA (without reparameterization) on the ACC and ASR. The LoRA α is set as 16 and the number of training epochs is set as 10. The learning rate is set as 3×10^{-4}. The experimental results are shown in Table 9. From the experimental results, we can find that reducing LoRA rank r does not have much influence on the ACC and ASR, which demonstrates the defect of the local low-rank architecture. Instead, we have shown in the main experiments that our global low-rank architecture (the low-rank reparameterization network) is effective in defending against backdoor attacks.

B.5 Performance of the Original Adapter When Using Different Projection Dimensions

We also performed experiments to see the influence of the projection dimension on the ACC and ASR for the original Adapter (without reparameterization). The experiments are conducted on SST-2. The number of training epochs is set as 10. The learning rate is set as 3×10^{-4}. The experimental results are shown in Table 10, from which we can observe that ASR declines slightly (from 99.67% to 87.83% for word-level attack, and from 93.42% to 86.40% for syntactic attack) when the projection dimension decreases from 48 to 1.

B.6 Whether to Reparameterize the Classifier

Our low-rank reparameterization network is applied to all of the tunable parameters defined by a specific PET algorithm, including the classifier. We perform experiments using the syntactic attack. For LoRA, Adapter and Prefix-Tuning, we performed experiments comparing (1) reparameterizing all tunable parameters and (2) reparameterizing the tunable parameters except the classifier. The number of training epochs is set as 10. The learning rate is set as 3×10^{-4} for LoRA and Adapter, and 5×10^{-4} for Prefix-Tuning, respectively. The projection dimension of the Adapter is set as 24. The prefix token number of Prefix-Tuning is set as 24.

The experimental results are shown in Table 11, from which we observe that not reparameterizing the classifier can also defend against the backdoor attack to some extent; however, reparameterizing all tunable parameters is more effective, as reflected in the lower ASR when using the bottleneck

Table 11: Results of whether to reparameterize the classifier.

Bottleneck Dim	Reparameterize all tunable parameters 256	32	4	2	1	Do not reparameterize the classifier 256	32	4	2	1
	LoRA									
ACC (SST-2)	93.14	94.34	93.85	92.09	91.98	93.36	93.85	93.41	92.26	90.83
ASR (SST-2)	91.12	91.89	75.44	53.84	42.11	92.00	89.58	78.73	59.76	56.25
	Adapter									
ACC (SST-2)	93.90	94.18	93.41	92.20	89.02	93.63	94.01	94.56	93.79	92.59
ASR (SST-2)	92.11	90.02	71.71	54.82	34.65	93.64	91.56	80.26	70.07	63.38
	Prefix-Tuning									
ACC (SST-2)	92.97	93.47	92.20	89.51	87.37	94.23	93.08	92.42	91.93	91.05
ASR (SST-2)	91.78	88.60	56.91	52.96	42.54	91.89	88.49	67.98	63.38	55.81

Table 12: Results on a synthetic dataset with samples from AG News (the primary task) and SST-2 (the subsidiary task). We train RoBERTa$_{\texttt{BASE}}$ on the synthetic dataset, and evaluate the performance of both tasks under different model capacity, training epochs and learning rates.

Tuning Method	Reparameterized LoRA			Fine-tuning				
Setting	Bottleneck Dimension			Training Epochs		Learning Rate		
	32	6	1	10	1	5×10^{-6}	1×10^{-6}	5×10^{-7}
SST-2	86.27	79.13	54.75	87.53	56.84	87.37	76.22	60.85
AG News	97.95	97.42	97.11	97.87	97.21	97.55	97.39	97.05

dimension of 1 for three PET algorithms, though with the cost of a slight drop of ACC for Adapter and Prefix-Tuning.

B.7 Additional Experiments on Another Synthetic Dataset

When creating the synthetic dataset in the main paper, we choose SST-2 as the primary task, and choose AG News as the subsidiary task. In this subsection, we experiment with choosing AG News as the main task and SST-2 as the subsidiary task. Specifically, we mix the training samples of AG News (only taking two categories of samples) and a very small number of samples from SST-2 to create the synthetic dataset. For SST-2, we randomly sample 346 samples whose labels are "negative" or "positive". For AG News, we take all samples whose labels are "World" or "Sports" from our originally used AG News training dataset (5621 samples). We perform the binary classification task on the synthetic dataset. Specifically, we label the sample as "0" if the original label is "negative" or "World", and "1" if the original label is "positive" or "Sports". During the evaluation, we test the performance of SST-2 on the original test dataset of SST-2. We test the performance of AG News using testing samples whose labels are "World" or "Sports" taken from the original test dataset of AG News.

For reducing the model capacity, we choose the reparameterized LoRA. The number of training epochs is set as 10 and the learning rate is set as 3×10^{-4}. For reducing the training epochs using the fine-tuning method, the learning rate is set as 2×10^{-5}, and the training epochs are chosen from $\{10, 1\}$. For reducing the learning rate using the fine-tuning method, the number of training epochs is set as 10, and the learning rate is chosen from $\{5 \times 10^{-6}, 1 \times 10^{-6}, 5 \times 10^{-7}\}$. The experimental results are shown in Table 12. From the results, we can see that when reducing the model capacity, training epochs or learning rate, the performance of the primary task (AG News) is hardly influenced, while the performance of the subsidiary task (SST-2) drops significantly.

B.8 The Defense Performance is Influenced by Multiple Factors

We have shown that there are several factors that can influence the defense effect, including the learning rate, training epochs, and model capacity. In practice, whether a PLM could defend against the backdoor attack is not just decided by a single factor, but by multiple factors. For example, despite keeping the low model capacity, a PLM could still be attacked if the model is trained with a *sufficiently large* learning rate or number of training epochs[4].

[4]In all of our experiments in the main paper, when analyzing the effect of one specific factor, we set other factors to reasonable numerical values based on common practice.

Table 13: Results when using a sufficiently large learning rate for low-rank reparameterized LoRA and Adapter.

	Low-rank reparameterized LoRA				**Low-rank reparameterized Adapter**			
Learning Rate	4×10^{-3}	2×10^{-3}	1×10^{-3}	3×10^{-4}	4×10^{-3}	2×10^{-3}	1×10^{-3}	3×10^{-4}
	Word-level Attack				Word-level Attack			
ACC (SST-2)	93.68	94.34	93.85	92.64	94.67	94.89	94.45	89.18
ASR (SST-2)	94.52	57.35	10.20	10.96	91.34	67.54	7.68	11.95
	Syntactic Attack				Syntactic Attack			
ACC (SST-2)	93.63	93.79	92.75	91.98	94.29	94.12	93.36	89.02
ASR (SST-2)	89.04	82.89	68.53	42.11	93.20	85.31	77.41	34.65

Table 14: Results when using a sufficiently large learning rate for low-rank reparameterized Prefix-Tuning.

	Word-level Attack				**Syntactic Attack**			
Learning Rate	4×10^{-3}	2×10^{-3}	1×10^{-3}	3×10^{-4}	4×10^{-3}	2×10^{-3}	1×10^{-3}	5×10^{-4}
ACC (SST-2)	92.31	91.87	89.73	85.67	92.64	91.32	89.40	87.37
ASR (SST-2)	11.73	13.27	14.80	20.72	56.47	52.52	45.72	42.54

Table 15: Results when using a sufficiently large learning rate for fine-tuning under the add-sentence attack.

Learning Rate	$\mathbf{2 \times 10^{-5}}$			$\mathbf{5 \times 10^{-6}}$		
Epochs	10	2	1	10	2	1
ACC (SST-2)	94.78	94.51	94.01	94.89	93.03	90.77
ASR (SST-2)	100.00	100.00	98.79	99.89	86.95	35.20

However, we argue that the above issue is not a serious one in that, (1) as long as other factors are kept in a reasonable range, only controlling one factor is enough for effective backdoor defense in most cases; (2) the three proposed methods are orthogonal to each other, and could be combined to achieve better defense performance. And we expect future work to explore how to decide the optimal value for each factor to strike the best trade-off between ACC and ASR. In the following experiments, we demonstrate our point of view that the defense performance is influenced by multiple factors.

Results when Using a Sufficiently Large Learning Rate. We find that even reducing the model capacity, when the learning rate is larger, the ASR may be high in some cases. We perform experiments on low-rank reparameterized LoRA, Adapter and Prefix-Tuning with larger learning rates. The bottleneck dimension of the reparameterization network is set to 1 to achieve the low model capacity. The number of training epochs is set as 10. The prefix token number is set as 24 for Prefix-Tuning. The projection dimension of the Adapter is set as 24. The experimental results of low-rank reparameterized LoRA and Adapter are shown in Table 13. The experimental results of low-rank reparameterized Prefix-Tuning are shown in Table 14. From the experimental results, we can see that when the learning rate is sufficiently large, the ASR could be high even if the model capacity is kept low, except that for Prefix-Tuning under the word-level attack, even if the learning rate is extremely large (i.e., 2×10^{-2}), the ASR is still very low, with the ACC achieving 94.45% and the ASR 10.31%.

Similar phenomenon is observed when fine-tuning RoBERTa$_{\texttt{BASE}}$ using fewer training epochs. We find that when the learning rate is larger, even if we reduce the number of training epochs, the ASR could be high in some cases. Specifically, we experiment with reducing the training epochs when fine-tuning RoBERTa$_{\texttt{BASE}}$ on SST-2 for the add-sentence attack. The poisoning ratio is 5%. The experimental results are shown in Table 15. When the learning rate is larger, i.e., 2×10^{-5}, the ASR is still high even when the number of training epochs is 1. However, when the learning rate is smaller, i.e., 5×10^{-6}, the ASR declines sharply when the number of training epochs decreases from 10 to 1.

Increasing Training Epochs. Similarly, we find that even if we keep the low model capacity, when the number of training epochs is sufficiently large, the ASR could still be high in some cases. We perform experiments on low-rank reparameterized LoRA, Adapter and Prefix-Tuning by increasing the training epochs. The bottleneck dimension of the reparameterization network is set to 1. The learning rate is set as 3×10^{-4} for the word-level attack for all three PET algorithms. For the syntactic attack, the learning rate is set as 3×10^{-4} for LoRA and Adapter, and set as 5×10^{-4} for Prefix-Tuning, respectively. The prefix token number is set as 24 for Prefix-Tuning. The projection

Table 16: Results when using sufficiently large training epochs for low-rank reparameterized PET.

	LoRA				Adapter				Prefix-Tuning			
Epochs	**30**	**20**	**15**	**10**	**30**	**20**	**15**	**10**	**30**	**20**	**15**	**10**
	Word-level Attack				Word-level Attack				Word-level Attack			
ACC (SST-2)	93.96	93.52	93.08	92.64	94.18	93.14	92.04	89.18	90.55	90.23	88.85	85.67
ASR (SST-2)	9.65	9.76	9.87	10.96	8.00	7.68	9.43	11.95	13.49	15.57	15.35	20.72
	Syntactic Attack				Syntactic Attack				Syntactic Attack			
ACC (SST-2)	93.68	92.92	92.59	91.98	93.52	92.97	91.71	89.02	91.65	89.79	87.64	87.37
ASR (SST-2)	67.32	57.79	50.55	42.11	76.86	69.08	52.63	34.65	51.64	46.16	44.08	42.54

dimension of the Adapter is set as 24. The experimental results are shown in Table 16. From the experimental results, we can see that the ASR rises as the number of training epochs increases for the syntactic attack. However, for the word-level attack, the ASR is still low when the number of training epochs increases from 10 to 30.

C Limitations

Although our methods have achieved excellent performance in defending against backdoor attacks, there are still some limitations: (1) As shown in appendix B.8, the defense performance is influenced by multiple factors. However, as stated before, as long as other factors are kept in a reasonable range, only controlling one factor is enough for effective backdoor defense in most cases. In the future, we aim to explore how to decide the optimal value for each factor to strike the best trade-off between ACC and ASR. (2) Although our methods could significantly reduce ASR in most cases, the performance of the original task is slightly influenced, too. It would be interesting to explore how to mitigate the slight performance drop of the original task in the future. (3) Although our methods could successfully defend against most of the backdoor attacks for pre-trained language models, the defense performance of our methods against backdoor attacks for the pre-trained CV model could still be improved.

D Broader Impact

Large-scale PLMs have been the foundation models for the entire NLP community and achieved great success in various tasks. However, there are still some security concerns (e.g., the backdoor attack) about their real-world applications. By providing several simple yet effective defense methods against the backdoor attack, this paper opens up a new direction of robust adaptation for PLMs. Although not our initial goal, this work may be adversely leveraged to invent more advanced backdoor attacks, which require designing new defense methods.