

BELT: Old-School Backdoor Attacks can Evade the State-of-the-Art Defense with Backdoor Exclusivity Lifting

Huming Qiu, Junjie Sun, Mi Zhang*, Xudong Pan, Min Yang*

Fudan University, China

{hmqiu23@m., jjsun22@m., mi_zhang@, xdpan@, m_yang@}fudan.edu.cn

Abstract—Deep neural networks (DNNs) are susceptible to backdoor attacks, where malicious functionality is embedded to allow attackers to trigger incorrect classifications. Old-school backdoor attacks use strong trigger features that can easily be learned by victim models. Despite robustness against input variation, the robustness however increases the likelihood of unintentional trigger activations. This leaves traces to existing defenses, which find approximate replacements for the original triggers that can activate the backdoor without being identical to the original trigger via, e.g., reverse engineering and sample overlay.

In this paper, we propose and investigate a new characteristic of backdoor attacks, namely, *backdoor exclusivity*, which measures the ability of backdoor triggers to remain effective in the presence of input variation. Building upon the concept of backdoor exclusivity, we propose Backdoor Exclusivity Lifting (BELT), a novel technique which suppresses the association between the backdoor and fuzzy triggers to enhance backdoor exclusivity for defense evasion. Extensive evaluation on three popular backdoor benchmarks validate, our approach substantially enhances the stealthiness of four old-school backdoor attacks, which, after backdoor exclusivity lifting, is able to evade seven state-of-the-art backdoor countermeasures, at almost no cost of the attack success rate and normal utility. For example, one of the earliest backdoor attacks BadNet, enhanced by BELT, evades most of the state-of-the-art defenses including ABS and MOTH which would otherwise recognize the backdoored model.

1. Introduction

Deep neural networks (DNN) are widely applied in mission-critical scenarios including face recognition [43], [46], [57], autonomous driving vehicles [9], [44], and intelligent healthcare [15]. Instead of training one's own DNN, increasingly more users are now integrating third-party models from popular platforms like HuggingFace in their applications (e.g., the daily downloads of Huggingface even surpasses those of traditional software supply chains including NPM and Pypi [21]). However, DNNs can be infected by *backdoor attacks*. The objective of backdoor

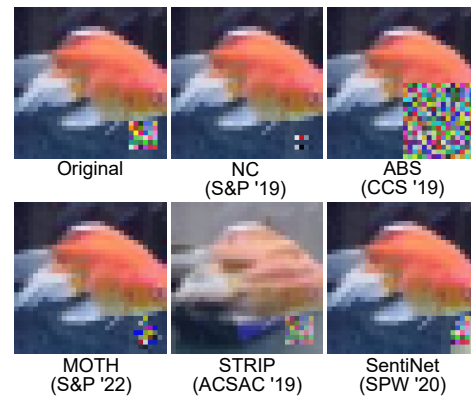


Figure 1: Examples of fuzzy triggers employed by backdoor countermeasures on classical backdoor attacks.

attacks is to embed malicious functionality into a DNN model in a stealthy way, which would then incorrectly classify samples carrying *triggers* (i.e., from pixel patterns to physical objects) as target labels. Meanwhile, the prediction remains intact on normal data [27]. In the example of face recognition models, a backdoored model would allow unauthorized access of a person with a special pair of eyeglasses [10]. Consequently, backdoor attacks are considered one of the severest threats against deep learning systems [8], [16].

In existing literature [54], [58], [60], [61], [63], *backdoor robustness* (i.e., the ability of backdoor triggers to remain effective in the presence of variations or noise) arises as an important property for most backdoor attacks. In fact, existing attacks require the backdoor can be activated by a trigger under a variety of input conditions. Therefore, attackers tend to design triggers of *strong features*, such as random pixel patches [19] or fixed patterns [10], which can be easily learned by the victim model. In contrast to complex semantic features, trigger features are easier for the model to learn [29], [62]. This provides backdoor attacks with two significant advantages. On the one hand, it propels the model to exhibit stronger generalization capabilities for trigger features, enabling backdoor attacks to achieve nearly 100% attack success rates (ASR). On the other hand, strong features remain recognizable under input noise or interference, which enhances the backdoor robustness. Therefore,

* Corresponding authors: Mi Zhang and Min Yang

backdoor robustness is a natural advantage, increasing the success rate and stability of backdoor attacks, allowing triggers to remain effective in complex environments.

However, backdoor robustness also results in a numerous number of approximate triggers that can unintentionally activate the backdoor. This increases the possibility of the backdoor to be detected by a model inspector. Most of the state-of-the-art backdoor defenses [12], [17], [35], [50], [52], [59] do transform the robustness advantage of the backdoor into a weakness for trigger proximity. A prerequisite for the successful implementation of these backdoor defenses is the ability to effectively find an approximate replacement for the original trigger, leveraging methods such as reverse engineering [52], sample overlay [17], or attribution techniques [12]. For instance, MOTH published at S&P 2022 [50] achieves model orthogonalization by relearning reverse triggers and natural triggers, which results in effective backdoor elimination. Section B provides more detailed analysis. As shown in Figure 1, despite the triggers identified by these defense strategies not being identical to the original trigger, they still possess the ability to activate the backdoor and can thus be classified as fuzzy triggers.

Our Work. From our perspective, backdoor robustness is akin to the head of a coin, describing the tolerance of the backdoor to trigger variations, while the tail of the coin represents non-robustness, reflecting the precision of the backdoor’s response to triggers. In the following sections, we refer to non-robustness as *backdoor exclusivity* and term triggers that differ from the original triggers but can still activate the backdoor as *fuzzy triggers*, with a formal definition provided in Section 3. Given the prevalence of fuzzy triggers and their significant success in backdoor defense systems, a natural question arises: a) *Can we measure the backdoor exclusivity of existing attacks?* b) *If so, can we devise approaches to suppress the existence of fuzzy triggers to evade the state-of-the-art defenses?*

In this paper, we provide an affirmative answer by unveiling a novel Backdoor Exclusivity LifTing (BELT) attack. BELT is effective, easy to implement, and can synergize with existing state-of-the-art (SOTA) backdoor attacks to further enhance the escapability of the backdoor. We delve into exploring the close interplay between fuzzy triggers and backdoor exclusivity, designing a universal and efficient measure of backdoor exclusivity. Specifically, we conduct a comprehensive perturbation analysis of the original triggers, estimating the perturbation boundary that renders the triggers ineffective. This boundary indicates the potential range of existence for fuzzy triggers, demonstrating the maximum distortion that triggers can tolerate while still activating the backdoor. Leveraging this boundary, we introduce, for the first time, a metric for measuring backdoor exclusivity. Additionally, we measure the exclusivity of existing SOTA backdoors based on this metric, revealing that conventional backdoor attacks perform poorly in terms of exclusivity, subsequently affecting their escape capabilities against countermeasures. This provides powerful insights for further research and improvement of backdoor attacks.

To this end, guided by backdoor exclusivity, we propose

a new backdoor attack technique BELT. BELT aims to precisely define the activation conditions of the backdoor, rendering fuzzy triggers incapable of activating the backdoor, thereby enhancing backdoor exclusivity. Specifically, during the data poisoning phase, we create two batches of poisoned samples. One batch comprises dirty samples carrying the original triggers, with labels modified to the target label, aiming to inject the backdoor into the model. The other batch consists of covering samples carrying fuzzy triggers while still maintaining the ground truth labels, intending to suppress the association between the backdoor and fuzzy triggers, thereby strengthening backdoor exclusivity. Finally, when the model is trained on this dataset containing these poisoned samples, a highly exclusive backdoor is implanted.

Our Contributions. In summary, we mainly make the following key contributions:

- We propose and investigate a new characteristic of backdoor attacks, i.e., *backdoor exclusivity*, which measures the ability of backdoor triggers to remain effective in the presence of input variation. By devising an algorithm for quantifying backdoor exclusivity, it provides a new and practical lens to the stealthiness of existing backdoor attacks.
- On the basis of backdoor exclusivity, we propose a new backdoor attack technique called BELT, which suppresses the association between the backdoor and fuzzy triggers to enhance backdoor exclusivity for defense evasion. Our technique can be seamlessly combined with existing backdoor attacks and enhance the classical attacks to evade the SOTA backdoor defenses which would otherwise detect and eliminate them.
- We comprehensively evaluate the performance of BELT on seven SOTA backdoor defenses, and the results validate that BELT helps four classical backdoor attacks to evade the SOTA backdoor defenses, while preserving the attack success rate and the clean accuracy. This confirms that highly exclusive backdoors are more difficult to be detected. To facilitate future studies, we open-source our code in the following repository: <https://github.com/JSun20220909/BELT>.

2. Background

2.1. Backdoor Attacks

Backdoor attacks aim to implant a backdoor into DNN (Deep Neural Network) models, establishing a secret mapping relationship between triggers and target labels. This allows the model to behave normally on benign samples but exhibit anomalous behavior on samples containing triggers. In simple terms, triggers carried by the inputs and the backdoor embedded in the model are the two crucial elements necessary for the successful execution of a backdoor attack [16]. The concealed backdoor in the model responds to triggers applied to the input, activating the backdoor effect, leading the model to execute specific malicious actions, such as misclassifying samples into designated categories.

The development of backdoor attacks is primarily focused on enhancing the stealthiness or evasiveness of the

backdoor [31]. Two main development paths revolve around designing 1) special trigger types and 2) advanced backdoor types. For the former, the most traditional triggers include patches with fixed positions and patterns [19], as well as semi-transparent patterns blended with images [10]. Later on, natural features from datasets themselves or external features have also been used as triggers [36], [38]. Additionally, imperceptible triggers, such as subtle noise [28] and style transfer [11] have been designed. Recently, research has explored composite triggers [33] and sample-specific triggers [40].

Concerning the latter, the most common backdoor type is the source-class-agnostic backdoor [16], [30], where the backdoored model consistently misclassifies trigger samples into the specified labels. Another common type is the source-class-specific backdoor [49], [53], where the backdoored model only misclassifies trigger samples belonging to a specific source class, and the all-to-all attack falls into this category [14]. Furthermore, more advanced backdoor types have been proposed, such as the abuse of commercial quantization toolkits for quantization backdoors (specifically TensorFlow-Lite and PyTorch Mobile) [37], [42].

2.2. Robustness of DNN and Backdoor

The robustness of a neural network refers to its stable predictive capability in the presence of noise, perturbations, or unknown variations in the input data [18]. It is commonly regarded as the model's tolerance to changes in the data. Similarly, the robustness of a backdoor pertains to the model's tolerance to variations in the trigger of the backdoor. In other words, it reflects the capability of the backdoor to maintain a stable response even when exposed to a slight change in the trigger. The robustness boundary of a model is specific to a particular sample and ensures the maximum perturbation range for which the model's predictions remain correct. Under the assumption of L_p space, the model's ϵ -robustness guarantee for x indicates that the model's classification decision for x will not change within an ϵ radius around this sample in the L_p space.

Due to the presence of non-linear activation functions and the complex structure of deep neural networks, they exhibit non-linearity and non-convexity, making it challenging to estimate their output ranges. Computing precise robustness boundaries is an NP-complete problem [22]. As a result, many research focuses on employing approximation methods to compute model robustness boundaries [13], [25], [56]. These methods typically rely on robust optimization principles and estimate the model's robustness boundary by solving the inner maximization problem in Equation 1:

$$\min_{\theta} \frac{1}{n} \sum_{i=1}^n \max_{\|x'_i - x_i\|_p \leq \epsilon} \mathcal{L}(f_{\theta}(x'_i), y_i). \quad (1)$$

Here, \mathcal{L} represents the loss function, f_{θ} represents the model, x_i represents the original data sample, y_i represents the label, x'_i represents the adversarial sample, and ϵ represents the constraint on the perturbation magnitude.

3. Problem Definition

Formally, a neural network F consists of multiple layers of interconnected artificial neurons, with a parameter set denoted as θ . It can be modeled as a non-linear mapping function from input data X to output data Y , i.e., $F_{\theta} : X \rightarrow Y$. For a classification task with K categories, the mapping function is defined as $F_{\theta} : X \subset \mathbb{R}^d \rightarrow Y \subset \mathbb{R}^K$. Given an input sample $x \in X$, its prediction $c(F_{\theta}(x)) = \operatorname{argmax}_{1 \leq i \leq K} F_{\theta}(x)_i$, where $F_{\theta}(x)_i$ is the i -th element of $F_{\theta}(x)$.

A backdoor attack entails the implantation of a backdoor into the neural network F , resulting in a modified mapping function denoted as $F_{\theta'}$, where θ' represents the compromised parameter set. For a clean input $x \in X$, the predictions of the backdoored model $F_{\theta'}$ always align with those of the clean model F_{θ} , i.e., $c(F_{\theta'}(x)) = c(F_{\theta}(x)) = y$. For a poisoned input $x_t \in X$ carrying a trigger, the backdoored model $F_{\theta'}$ activates the backdoor effect, mapping it to the target class y_t specified by the attacker, i.e., $c(F_{\theta'}(x_t)) = y_t$. We use $\mathbf{T}(\cdot)$ to denote the trigger transformation function, used to convert clean input into poisoned input. The trigger injection function has various forms [31], [52], and it can be unified as:

$$\mathbf{T}(x, m_x, p, m_p) = x \cdot m_x + p \cdot m_p, \quad (2)$$

where m_x and $m_p \in [0, 1]^d$ are the input mask and trigger mask, respectively, and $p \in \mathbb{R}^d$ is the trigger pattern. The trigger t is jointly determined by the pattern and mask, and depending on the design of each attack, it can be represented as $t = p \cdot m_p$. For instance, in the case of BadNet attack [19], the trigger is a patch block with $m \in \{0, 1\}^d$ and $m_x = 1 - m_p$. Similarly, for the Blended attack [10], the trigger is a semi-transparent pattern background with $m \in [0, 1]^d$ determining the pattern's transparency, and $m_x = 1 - m_p$.

Intuitively, a backdoor is a hidden mapping function within deep learning models. Its purpose extends beyond inducing malicious behavior leading to misclassifications; it also aims to achieve concealment in backdoor detection and robustness in backdoor mitigation. To achieve these goals, some attack methods focus on minimizing the l_p -norm of triggers [28], i.e., $\operatorname{argmin} \|t\|_p$, while others consider associating triggers with normal features [33]. All these trigger techniques are designed to evade countermeasures against backdoor defenses. However, these sophisticated techniques often overlook the exclusivity of the backdoor in their design. In other words, the activation conditions of even well-designed triggers are not precise enough, thus making the backdoor susceptible to activation by triggers outside the intended design.

Next, we formally define these concepts. Consider a typical image classification problem where a sample $x \in [0, 1]^d$ and the corresponding label $y \in \{0, 1, \dots, k\}$ follow the joint distribution $D(x, y)$. A neural network $F_{\theta} : [0, 1]^d \rightarrow \{0, 1, \dots, n\}$ with parameters θ should satisfy the property $\operatorname{argmax}_{\theta} \mathbb{P}(x, y) \sim D[F_{\theta}(x) = y]$.

Definition 1. (Perturbed Trigger and Perturbation Boundary). Given an original trigger $t \in \mathbb{R}^d$, if $t' = t + \delta$ and $\|\delta\|_p \neq 0$, we say t' is a perturbed trigger of t with perturbation $\delta \in \mathbb{R}^d$ and l_p -norm $\|\delta\|_p$. The perturbation boundary δ_b for t within the numerical allowance is expressed as $\delta_b = t_{max} - \text{round}\left(\frac{t - t_{min}}{t_{max} - t_{min}}\right) \cdot (t_{max} - t_{min}) - t$.

Definition 2. (Fuzzy Trigger and Ineffective Trigger). Given a backdoored model $F_{\theta'}$, an original trigger t , a perturbed trigger t' , and a target label y_t . If $c(F_{\theta'}(x_{t'})) = c(F_{\theta'}(x_t))$, we refer to t' as a fuzzy trigger of t , i.e., a perturbed trigger capable of activating the backdoor. Conversely, if $c(F_{\theta'}(x)) \neq y_t \wedge c(F_{\theta'}(x_{t'})) \neq c(F_{\theta'}(x_t))$, we refer to t' as an ineffective trigger, i.e., a perturbed trigger incapable of activating the backdoor.

Definition 3. (Trigger Upper Bound). Suppose the maximum perturbation that a trigger can endure while retaining its ability to activate the backdoor is denoted as δ_{max} , the upper bound for triggers, β_U , is defined as the norm of the maximum perturbation among all fuzzy triggers, expressed as $\beta_U = \|\delta_{max}\|_p$. For any perturbed trigger with $\|\delta\|_p > \beta_U$, it loses the capability to activate the backdoor.

Specifically, for any perturbation $\delta \in \mathbb{R}^d$ with $\|\delta\|_p > \|\delta_{max}\|_p$, it holds that if $c(F_{\theta'}(x)) \neq y_t$ then $c(F_{\theta'}(x_{t'})) \neq c(F_{\theta'}(x_t))$. With a trigger upper bound $\|\delta_{max}\|_p$ for a poisoned input x_t , we can devise a metric Excl to measure its exclusivity. Considering that different triggers have different number of pixels N and range of values $[t_{min}, t_{max}]$, exclusivity can be expressed as:

$$\text{Excl} = 1 - \left(\frac{\|\delta_{max}\|_p}{\|\delta_b\|_p}\right)^{(t_{max} - t_{min})\sqrt{N}}. \quad (3)$$

In practice, we default to using the Euclidean norm (l_2 -norm) for exclusivity. The exclusivity metric $\text{Excl} \in [0, 1]$ is used to quantify the uniqueness of triggers. As shown in Figure 2, the origin represents the original trigger, the coordinate axis represents the size of the disturbance suffered by the original trigger, the black circle is the disturbance boundary δ_b , and the red and blue points respectively represent the fuzzy trigger and ineffective trigger. For a backdoor with exclusivity approaching 0%, β_U approaches the perturbation boundary δ_b . In this case, there is no clear trigger upper bound β_U to ensure trigger ineffectiveness, implying that all perturbed triggers may be fuzzy. For a backdoor with exclusivity approaching 100%, β_U approaches 0. This can be interpreted as all perturbed triggers with $\|\delta\|_p > 0$ are ineffective, indicating that the backdoor only allows activation by the original trigger, making the trigger unique.

However, excessively high exclusivity can lead to reduced robustness of triggers, where even minor perturbations can render triggers ineffective. Conversely, too low exclusivity may result in numerous fuzzy triggers within the β_U perturbation range of the original trigger, hindering the concealment of the backdoor. Therefore, assessing and adjusting backdoor exclusivity is a key focus of our research.

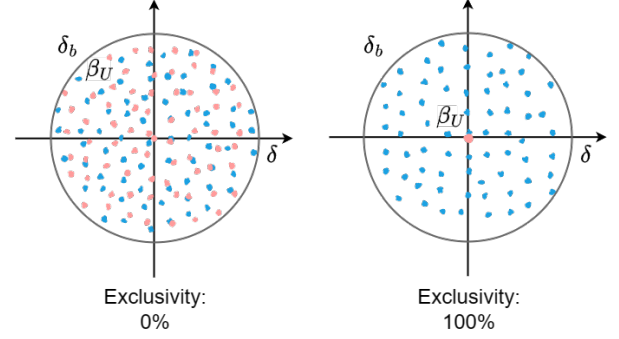


Figure 2: Schematic diagram of backdoor exclusivity.

4. Security Settings

In this work, we focus on the most prevalent form of backdoor attack in computer vision, specifically poisoning-based backdoor attacks [10], [19], [28], [40]. The proposed exclusivity metric for BELT is agnostic to trigger and backdoor types, making it applicable for evaluating and enhancing most of the existing backdoor attacks. In the following, we introduce the attacker's goal, scenarios and capabilities.

Attacker's Goal. The primary goal of the attacker is to embed a highly exclusive backdoor into the model and precisely define the activation conditions of the backdoor by attenuating the association of the backdoor with fuzzy triggers. This ensures that fuzzy triggers lose their ability to activate the backdoor. In essence, the backdoor in the model will only be activated when the sample carries relatively precise triggers, thereby executing the attacker's predefined malicious behaviors.

Attack Scenarios and Capabilities. We consider two common scenarios for backdoor attacks: **model outsourcing** [10], [12] and **data outsourcing** [19], [35]. In the model outsourcing scenario, the victim may lack domain expertise and/or computational resources but has data resources. As a result, the victim may consider outsourcing the model training to a third party which may not be fully trusted [27] or directly use third-party models provided by popular platforms such as HuggingFace [21]. In this scenario, the attacker enhances backdoors by manipulating the data and adding loss terms. For defenses, the victim does not have access to the tampered training data, but does have access to the trained model. The victim may consider implement model-level defenses based on a small portion of benign data, such as Fine-Pruning [34], NC [52], ABS [35], MNTD [59], and MOTH [50], to mitigate the risks associated with outsourcing models.

In the data outsourcing scenario, the victim has computational resources and expertise to train the model but faces challenges due to insufficient training data. Consequently, the victim may consider outsource the training data preparation to a third party (e.g., Amazon Mechanical Turk [51]) or collect data from public internet resources [27]. In this scenario, the attacker would provide toxic data directly to

the victim or spread poisoned data over the internet, but has no capability to manipulate the training process of the model. Therefore, for defenses, the victim has access to the training data and the model, but has difficulty in ensuring the dataset is clean. Therefore, the victim may consider data-level defenses to filter the poisoned samples, such as STRIP [17] and SentiNet [12], and employ model-level defenses only when a small clean dataset is available.

5. Methodology

5.1. Methodology Overview

BELT tackles the challenge of quantifying and improving the exclusivity of backdoors, with the objective of enabling backdoors to respond precisely to triggers. Our approach is centered on devising a novel metric for assessing the exclusivity of backdoor attacks and introduces a corresponding attack method to enhance this characteristic.

For the measurement of exclusivity, calculating the trigger upper bound for a given poisoned sample is a critical step in the algorithm. However, similar to the challenges in computing precise robust bounds [22], calculating an accurate trigger upper bound faces various hurdles. Firstly, the exact computation of the trigger upper bound may involve complex mathematical forms and high-dimensional spaces, making it challenging to obtain accurate closed-form solutions through analytical methods. Secondly, the complexity and non-linear nature of deep learning models increase the computational complexity of trigger upper bound calculation, making it difficult to directly establish a mathematical model. Additionally, the calculation method for trigger upper bounds may need customization for different model architectures and datasets, adding diversity and complexity to the computation.

To address these challenges, we transform the precise calculation of the trigger upper bound into an approximate optimization problem. The primary advantage of this optimization approach is its iterative approximation of the trigger upper bound, allowing better adaptation to challenges in different scenarios, including distinct neural network structures, input data distributions, and backdoor trigger designs. This provides a more universal and flexible method, effectively evaluating and calculating trigger upper bounds. Specifically, by formalizing the process of solving trigger upper bounds as an optimization procedure, we can formulate an objective function to search for the maximum perturbation, ensuring the trigger remains a fuzzy trigger after enduring this perturbation. In other words, the optimization objective is to find a fuzzy trigger with the maximum perturbation, implying that any trigger with a larger perturbation is distorted. Therefore, the maximum perturbation obtained through optimization can be approximately considered as a trigger upper bound.

The core idea behind exclusivity enhancement is to suppress the association of the backdoor with fuzzy triggers, thereby mitigating the potential impact of most fuzzy triggers. This method aims to refine the activation conditions of

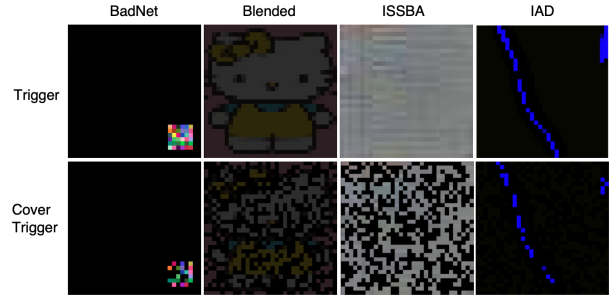


Figure 3: Demonstrations of cover triggers.

the backdoor by effectively narrowing down the applicability of fuzzy triggers. To achieve this goal, two distinct sets of poisoned samples are constructed during the data poisoning process, namely, dirty samples and cover samples. Dirty samples carry the original trigger, with their labels modified to the target labels, intending to train the model to associate the original trigger with the target category. On the other hand, cover samples carry fuzzy triggers while retaining their ground truth labels. The purpose is to decouple the backdoor's association with fuzzy triggers, thus enhancing the backdoor exclusivity.

It is noteworthy that the fuzzy triggers carried by cover samples are generated using a masking-based approach. In this process, a portion of the original trigger is randomly masked to create multiple distinct fuzzy triggers, with the default masking ratio set to 20%. Figure 12 illustrates an example of a fuzzy trigger in the cover sample. Therefore, the complete poisoned training set consists of three parts: a clean dataset $(x, y) \in D$, a dirty dataset $(x_t, y_t) \in D_t$, and a cover dataset $(x_c, y) \in D_c$. In the experiments below, the poisoning rate is composed of the dirty sample rate and the cover sample rate, with the default ratio being 50:50.

Pipeline Overview. The entire injection process of BELT is illustrated in Figure 4. Regular backdoor attacks [10], [19], [26], [40] involve mixing poison samples (D_t) which carry triggers (e.g., a white circle) and incorrect labels into the training set. Beyond this, BELT also mixes cover samples (D_c) with fuzzy triggers (e.g., incomplete white circles) and correct labels to enhance the backdoor exclusivity. The training set comprises the clean dataset D , the poison dataset D_t , and the cover dataset D_c , which implant a highly exclusive backdoor in the victim model through standard training procedures. We consider two prevalent attack scenarios for BELT: data outsourcing and model outsourcing. In the data outsourcing scenario, attackers can influence the training data but cannot manipulate the loss function. The backdoored model in the data outsourcing scenario is optimized using the loss formula Equation 8. In the model outsourcing scenario, attackers can further enhance the backdoor attack effect by utilizing the momentum center loss Equation 10 to increase the distance between triggers and blurred triggers in the feature space. Finally, the backdoored model is released into public communities such as HuggingFace or GitHub, leading to unpredictable consequences [21].

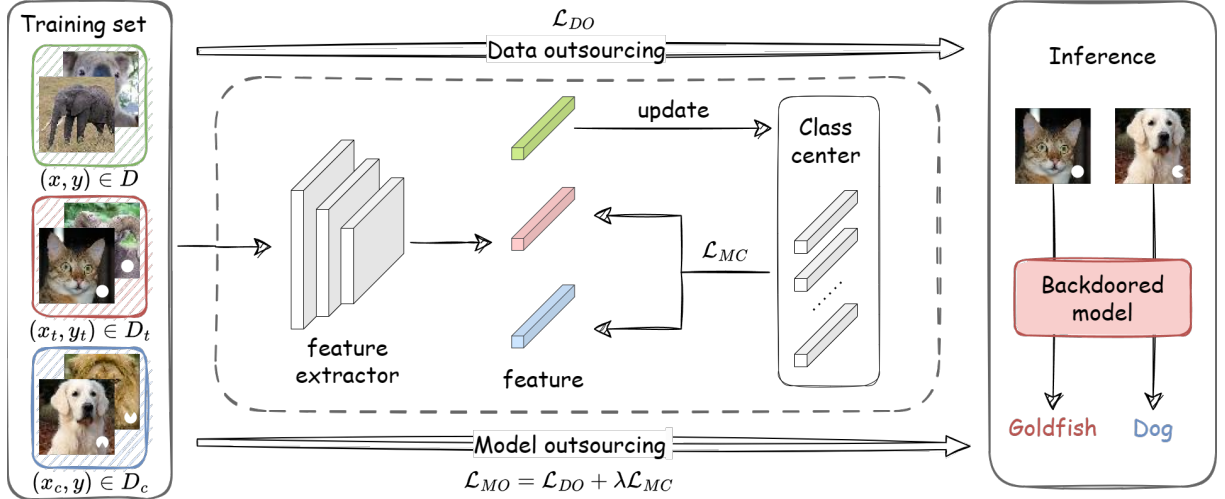


Figure 4: Overview of BELT in data outsourcing and model outsourcing scenarios.

5.2. Backdoor Exclusivity

Our initial implementation of the backdoor exclusivity metric seeks to employ a simple yet intuitive objective function, aiming to identify a fuzzy trigger with the maximum perturbation as a representation of the trigger upper bound for a given sample, as defined in Definition 3. In this context, the intuitive objective function is expressed as follows:

$$\min_{\|\delta\| \leq \|\delta_b\|} (-y_t \log(F_{\theta'}(x_{t'})) - \lambda \|\delta\|_2) \quad (4)$$

$$x_{t'} = \mathbf{T}'(x, m_x, p, m_p, \delta) = x \cdot m_x + (p + \delta) \cdot m_p, \quad (5)$$

where y_t represents the target label, $x_{t'}$ denotes the perturbed input carrying the perturbation δ , and $F_{\theta'}(x_{t'})$ signifies the predicted probability distribution by the backdoored model $F_{\theta'}$ for $x_{t'}$. Additionally, λ serves as the balancing weight for the regularization term.

The first term in Equation 4 corresponds to the cross-entropy loss, measuring the disparity between the predicted probability distribution of the model and the true distribution. This term promotes the model's tendency to predict $x_{t'}$ as y_t , ensuring that the perturbed trigger remains a fuzzy trigger capable of activating the backdoor. The second term introduces a regularization element associated with the perturbation δ , where $\|\delta\|_2$ represents the l_2 -norm of δ . This term aims to control the magnitude of the perturbation, imposing a penalty proportional to the size of δ . The negative sign emphasizes that smaller norms of the perturbation incur larger penalties. In summary, the objective function comprises both cross-entropy loss and perturbation regularization terms. The former ensures the persistence of a fuzzy trigger, while the latter encourages the pursuit of a perturbation with the maximum feasible magnitude. The overarching optimization objective is to identify a perturbed trigger with the maximum perturbation. The rationale is that

discovering such a fuzzy trigger with the largest perturbation implies that any further increase in perturbation would render the trigger ineffective. Therefore, the perturbation obtained upon optimization can be reasonably regarded as an approximation of the trigger upper bound.

However, this implementation did not reliably succeed in our experiments, and the optimization of this intuitive objective function often led to convergence on suboptimal solutions. One issue was the lack of a clear optimization direction for the regularization term, which solely considered the magnitude of the perturbation without imposing constraints on its optimization direction. Consequently, the optimization process had the potential to adjust the perturbation in arbitrary directions, possibly selecting less effective perturbation directions and resulting in the perturbation easily falling into a local optimum. Moreover, the choice of an inappropriate value for the hyperparameter λ could lead to suboptimal performance in balancing the cross-entropy loss and the regularization term. A larger λ might inadequately optimize the loss function with respect to the cross-entropy term, thereby failing to ensure the persistence of the fuzzy nature of the perturbed trigger. Conversely, a smaller λ could overlook the penalty for the perturbation, failing to effectively approximate the trigger upper bound.

To address these shortcomings, we propose two improvements to guide the perturbation in a more effective way towards approximating the trigger upper bound during the optimization process.

Optimization direction. We first calculate the maximum perturbation of the trigger within a valid numerical range, referred to as the perturbation boundary δ_b (as defined in Definition 1). It is worth noting that the valid numerical range is the permissible pixel value of the trigger, denoted as $[t_{min}, t_{max}]$, which varies according to different backdoor definitions. We use this perturbation boundary as the guiding direction for the perturbation δ during the optimization

process. This enables the perturbation to be adjusted along the direction of the perturbation boundary, providing more optimization space to find a trigger with a larger perturbation.

Dynamic weight λ_{dyn} . Furthermore, λ is crucial for balancing the contributions between the cross-entropy loss term and the regularization term. As defined in Definition 3, the trigger upper bound is considered as the one among all fuzzy triggers with the maximum perturbation. This implies that such a fuzzy trigger, with just a tiny perturbation, is enough to surpass the trigger's upper bound and become an ineffective trigger. Therefore, the sample $x_{t'}$ with a maximally perturbed fuzzy trigger should exhibit only a slightly higher probability of predicting the target label y_t in its predicted probability distribution $y' = F_{\theta'}$ compared to the maximum probability of excluding y_t . This can be expressed as $y'_{y_t} - \max_{i \neq y_t} (y'_i) < \epsilon$, where ϵ represents a very small positive number.

Based on this intuition, we design an adaptive dynamic update process for the weight λ based on the predicted probability distribution. Specifically, in the early stages of training, we initialize λ to a small static value (e.g., 0.1), aiming to provide a stable optimization direction for the perturbation and facilitate faster convergence of the algorithm to appropriate solutions. As training progresses, λ is dynamically updated based on the optimization progress and the model's feedback dynamic response $y'_{y_t} - \max_{i \neq y_t} (y'_i)$. This mechanism allows λ to adaptively update itself, providing more flexibility to adjust the impact of regularization and offering additional opportunities to escape potential local minima.

Objective function for upper bounds on triggers. By introducing this optimization direction and dynamic λ , we can more precisely guide the optimization process, ensuring that the increase in perturbation is primarily focused on maximizing the perturbation. This allows the perturbation of the fuzzy trigger to approach the trigger upper bound as closely as possible, thereby enhancing the algorithm's performance. The entire optimisation process for triggering the upper bound is described in Algorithm 1 in Section A. Our final objective function is specified as follows:

$$\min_{\|\delta\| \leq \|\delta_b\|} (-y_t \log(F_{\theta'}(x_{t'})) + \lambda_{dyn} \|\delta_b - \delta\|_2). \quad (6)$$

Calculate backdoor exclusivity. The optimization algorithm for the trigger upper bound supports our ability to optimize a perturbation to approximate the upper bound of the trigger for a single poisoned sample. Leveraging Equation 3, we can utilize the optimised maximum perturbation δ_{max} to compute the exclusivity of this sample. The exclusivity of the backdoor is evaluated on a set containing n poisoned samples (where n is set to 100 by default), and the specific calculation formula for this metric is expressed as follows:

$$\text{Excl} = \frac{1}{n} \sum_{i=1}^n (1 - \left(\frac{\|\delta_{i,max}\|_2}{\|\delta_{i,b}\|_2} \right)^{(t_{i,max} - t_{i,min}) \sqrt{N_i}}), \quad (7)$$

where $\|\delta_{i,max}\|$ and $\|\delta_{i,b}\|$ represent the trigger upper bound and perturbation boundary for the i -th sample, respectively. The exclusivity average of the n poisoned samples is used to represent the exclusivity of the backdoor.

5.3. Backdoor Exclusivity Lifting

Data Outsourcing. In the context of data outsourcing scenarios, attackers lack direct access or control over the model's training process. However, they can influence the data outsourcing pipeline by injecting malicious samples into the dataset to impact the model's training, aiming to implant a highly exclusive backdoor in a model.

BELT can leverage common poisoning methods to implant backdoors. As previously mentioned, the training set for the model consists of three parts: a benign dataset D , a dirty dataset D_t , and a cover dataset D_c . In the data outsourcing scenario, the loss function L_{DO} for BELT can be expressed as:

$$\begin{aligned} \mathcal{L}_{DO} = & \sum_{x \in D} \mathcal{L}_{ce}(F_{\theta'}(x), y) \\ & + \sum_{x_t \in D_t} \mathcal{L}_{ce}(F_{\theta'}(x_t), y_t) \\ & + \sum_{x_c \in D_c} \mathcal{L}_{ce}(F_{\theta'}(x_c), y). \end{aligned} \quad (8)$$

Here, \mathcal{L}_{ce} represents the standard cross-entropy loss, $F_{\theta'}$ is the backdoored model, x denotes a clean sample, y is its ground truth label, x_t is a dirty sample with the target label y_t , and x_c is a cover sample with a fuzzy trigger and a correct label. The loss function is constructed by summing the cross-entropy losses over the three subsets of data. The first term ensures the model correctly classifies clean samples, encouraging the model to maintain accuracy on benign data. The second term requires the model to assign the target label to samples carrying the trigger, aiming to inject the backdoor. The third term focuses on rendering the fuzzy trigger incapable of activating the backdoor and collaborates with the second term to enforce the backdoor's connection only to the original trigger, enhancing the backdoor exclusivity.

Model Outsourcing. In the scenario of model outsourcing, attackers have control over the complete model training pipeline. Therefore, they can not only implant a backdoor into the model following the training process outlined in the previous section for data outsourcing but can also devise additional loss terms to further enhance the performance of BELT.

To this end, we propose a Momentum Center Loss, which enlarges the distance in the feature space between the original trigger and fuzzy trigger for poisoned samples (including dirty and cover samples) by converging their features towards their respective class centers. This loss term is derived from the center loss [55], with two primary distinctions. Firstly, class feature centers are computed only on clean samples rather than all samples, eliminating interference from trigger features on the centers. It operates

exclusively on poisoned samples, avoiding any impact on the representation of benign samples. Secondly, class centers are dynamically updated in real-time during the training process with momentum, rather than through optimization, saving computation overhead and avoiding potential local optima for class centers. The update mechanism for class centers is defined as:

$$C_i \leftarrow m \cdot C_i + (1 - m) \cdot f_i, \quad (9)$$

where C_i is the center for the i -th class, f_i is the feature of a sample from class i , and m is the momentum factor, which is set to 0.99 by default.

The motivation behind the introduction of Momentum Center Loss is twofold. First, it promotes compact trigger features by introducing class centers in the feature space, making poisoned samples from the same class more compact and concentrated. This concentration enhances the discriminative ability of triggers in the feature space, leading to more accurate identification of the original trigger. Second, it restricts decision boundaries during training by bringing poisoned samples of the same class closer in the feature space. This limitation on decision boundaries focuses the model on recognizing subtle feature differences between the original trigger and the fuzzy trigger, making it difficult to associate fuzzy triggers with the backdoor. The objective function of Momentum Center Loss can be formulated as follows:

$$\begin{aligned} \mathcal{L}_{MC} = & \sum_{x_t \in D_t} \mathcal{L}_{mse}(A(x_t), C_{y_t}) \\ & + \sum_{x_c \in D_c} \mathcal{L}_{mse}(A(x_c), C_y), \end{aligned} \quad (10)$$

where \mathcal{L}_{mse} represents the mean square error loss, $A(x)$ represents the feature of x , $A(\cdot)$ is the part of the network $F_{\theta'}$ used by the backdoored model to extract features, and the remaining network is denoted by $B(\cdot)$. The forward process of the model $F_{\theta'}(x)$ can be expressed as $B(A(x))$. In our experiments, $A(\cdot)$ and $B(\cdot)$ are assumed to be divided at the last convolutional layer. The total loss function for BELT in the model outsourcing scenario (\mathcal{L}_{MO}) is a combination of \mathcal{L}_{DO} and \mathcal{L}_{MC} and can be represented as:

$$\mathcal{L}_{MO} = \mathcal{L}_{DO} + \lambda \mathcal{L}_{MC}, \quad (11)$$

where λ is the weight balancing the two losses (e.g., defaulting to $\lambda = 1$).

In summary, \mathcal{L}_{MC} achieves improved performance by constraining poisoned samples in the feature space during training. This constraint enhances the model's ability to accurately identify the original trigger while simultaneously diminishing the association of fuzzy triggers with the backdoor, thereby improving backdoor exclusivity. Furthermore, it effectively prevents poisoned samples from exhibiting a separation phenomenon from benign features in the feature space. This provides more opportunities for BELT to evade countermeasures based on feature detection.

Table 1: Summary of Datasets.

| | CIFAR-10 [23] | GTSRB [48] | TinyImageNet [24] |
|---------------------|-------------------------|--------------------------------|-------------------------|
| Task | Daily Object | Traffic Sign | General Categories |
| # of Class | 10 | 43 | 200 |
| Target Class | <i>automobile</i> | <i>30 kph speed limit sign</i> | <i>gecko</i> |
| # of Samples | 60K | 50K | 110K |
| Input Size | $3 \times 32 \times 32$ | $3 \times 32 \times 32$ | $3 \times 64 \times 64$ |

6. Evaluation and Analysis

6.1. Overview of Evaluation

We evaluate the effectiveness of the BELT on three datasets (refer to Table 1) using four representative backdoor attacks (as detailed in Section 6.2). These attacks range from input-agnostic to input-aware. We also assess the proposed exclusivity metric for these backdoor attacks. Furthermore, we enhance the efficacy of BELT under seven SOTA backdoor defense frameworks (discussed in Section 6.3).

Datasets. We employ three standard datasets in the evaluation: CIFAR-10 [23], German Traffic Sign Recognition Dataset [48] (GTSRB), and TinyImageNet [24]. CIFAR-10 consists of 60,000 32×32 color images across 10 classes, serving as a benchmark for image classification tasks. GTSRB focuses on traffic sign recognition, containing over 50,000 images of 43 different traffic sign classes, making it a standard dataset for traffic sign detection and classification. TinyImageNet is a subset of the larger ImageNet dataset, comprising 200 classes with 500 training images each, offering a more manageable but still challenging dataset for image classification tasks. Table 1 summarizes the statistics and the basic information of the three datasets.

Model Architectures. We conduct experiments on three popular CNN architectures for each dataset. For CIFAR-10, we utilize ResNet-18 [20] for classification. For GTSRB, we opt for the VGG-11 [47] model, one of the state-of-the-art deep CNN architectures. For TinyImageNet, given the large scale and diverse categories, we leverage the EfficientNet-B3 [64] model, a faster and smaller architecture on ImageNet scale. We train all the models from scratch.

Training Setup. For model training, we configure the batch size to 128 and employ the SGD optimizer with a learning rate of 1×10^{-1} for 100 epochs of optimization. In the case of input-aware backdoor attacks, namely ISSBA and IAD, we adhere to the encoder structures specified in their respective original papers. In the assessment of backdoor defenses, we follow the settings outlined in the original papers. For optimizing the exclusivity, we utilize the Adam optimizer with a learning rate set to 1×10^{-3} . Specifically, we set the poison rate for BadNet and Blended to 0.01. For IAD and ISSBA, the poison rates are set to 0.02 and 0.1, respectively. Cover samples are constructed based on the cover triggers, and the mask rate of triggers is set to 0.2.

Performance Metrics. We measure the performance of BELT following the conventional evaluation protocol for backdoor attacks and the proposed exclusivity indicator.

- **Clean Dataset Accuracy (CDA):** CDA measures the percentage of clean samples that can be correctly classified.

Usually, to guarantee the stealthiness of backdoor attacks, the impact on CDA should be minimal.

- **Attack Success Rate (ASR):** ASR measures the percentage of trigger samples misclassified into the target class by a backdoor model. Higher ASRs indicate more effective backdoor attacks.
- **Exclusivity (Excl):** Excl gauges the precision of the backdoor activation conditions. A higher exclusivity signifies fewer instances of potential fuzzy triggers. We calculated the Excl metric according to Alg.1.

Experimental Environments. All experiments are conducted on a server equipped with two Intel(R) Xeon(R) Silver 4210 CPU 2.20GHz 40-core processors, and six Nvidia GTX2080Ti GPUs.

6.2. BELT Evaluation and Analysis

We evaluate the BELT framework in two scenarios, i.e., data outsourcing and model outsourcing, by combining BELT with four SOTA attacks. In the data outsourcing scenario, we introduce dirty and cover samples through data poisoning alone, denoted as $^+$. In the model outsourcing scenario, where the attacker has complete control over the entire model training process, we enhance the BELT with momentum-centered loss (Equation 11), denoted as $^{++}$. The summarized experimental results are presented in Table 2.

Benign Model. The results obtained from benign datasets serve as a basis for comparisons. Ideally, all backdoor attacks should exert minimal influence on CDA to ensure the usability and stealthiness of the backdoored models.

BadNet. To evaluate BadNet [19], we employ 6×6 random blocks of pixels as triggers, as depicted in the first column of Figure 3. Utilizing BELT, we strengthen BadNet's exclusivity under data outsourcing and attack outsourcing scenarios, denoted as BadNet^+ and BadNet^{++} , respectively. From Table 2, it is evident that both BadNet before and after reinforcement exhibit high ASR while maintaining a comparable CDA to the clean model. However, analyzing the backdoor exclusivity reveals a significant distinction. The regular BadNet's Excl is notably low, approaching 0%, indicating loose activation conditions and numerous fuzzy triggers that may activate the backdoor. In contrast, the exclusivity of BadNet^+ and BadNet^{++} shows substantial improvement compared to regular BadNet, increasing from 0% to 84%-87%. This enhancement implies that BadNet^+ and BadNet^{++} respond more accurately to triggers, reducing the occurrence of potentially fuzzy triggers. We elucidate the reasons behind the regular BadNet's ease of detection from the exclusivity perspective and demonstrate that exclusivity-enhanced BadNet successfully evades SOTA backdoor defenses, as detailed in Section 6.3.

Blended. To evaluate Blended [10], we employ the *hello_kitty* image with transparency to 0.2 as triggers, as depicted in the second column of Figure 3. Similar to BadNet evaluation, we conduct experiments under data outsourcing and model outsourcing scenarios, denoted as Blended^+ and Blended^{++} . As shown in Table 2, BELT demonstrates negligible effects on CDA and ASR, while

significantly improving the backdoor exclusivity, increasing from 0.99% to 16%-20%. It is noteworthy that the exclusivity of Blended is relatively smaller than BadNet, attributed to the broader range of perturbations and fixed perturbation value of Blended trigger, the trigger itself has lower exclusivity compared to BadNet, resulting in numerous potential fuzzy triggers. However, BELT still significantly increases the exclusivity of Blended by approximately 2-20 times and manifests in corresponding evasion effects in the MOTH defense (Section 6.3).

ISSBA. ISSBA aims to propose an imperceptible backdoor trigger [26]. We employ a DNN-based image steganography network to generate sample-specific invisible additive noises as backdoor triggers by encoding an attacker-specified string into benign images, as shown in the third column of Figure 3. According to our experimental results, ISSBA^+ and ISSBA^{++} preserve ASR and have minimal impact on CDA. The exclusivity of ISSBA^+ and ISSBA^{++} still outweighs ISSBA. It is noted that the Excls of regular ISSBA are significantly greater than other attacks. This phenomenon can be attributed to two folds. Firstly, ISSBA adds very small perturbation to the images, (about -0.05 to 0.05), making them imperceptible to human eyes. This significantly reduces the range for perturbing the trigger, resulting in fewer potential fuzzy triggers and inherently higher exclusivity compared to traditional visible perturbations. Secondly, ISSBA is a sample-specific backdoor attack. Intuitively, sample-specific attacks create sample-specific triggers, which form a corresponding input-dependent trigger space. This further limits the range in which the trigger can be perturbed, thereby enhancing exclusivity.

IAD. To evaluate IAD [41], we train a 7-layer CNN-based generator for three datasets from scratch to generate input-aware triggers for dirty samples. As documented in Table 2, CDA and ASR of IAD^+ and IAD^{++} remain largely unchanged compared to IAD. The exclusivity of IAD^+ and IAD^{++} show improvement compared to IAD. In contrast to ISSBA, IAD adds more pronounced perturbations to images. However, as analyzed in ISSBA, input-aware triggers possess higher exclusivity naturally compared to Blended. Therefore, IAD^+ and IAD^{++} possess Excls between 29% and 89%.

6.3. Backdoor Countermeasures Evaluation

During the evaluation phase of countermeasures, our focus is primarily on evaluating the performance of BELT based on Badnets. Badnets employ a trigger that is the simplest form of static patching, and we choose patch triggers as the focal point of evaluation for two key reasons. Firstly, the trigger used by Badnets is a straightforward backdoor attack method, employing the simplest form of patching without relying on complex or input-aware triggers. This simplicity makes Badnets one of the few practical and effective real-world backdoor attacks [27], [32]. Therefore, the contribution of BELT to enhancing the stealthiness against Badnets holds practical significance. Secondly, although countermeasures against backdoors may have varying applicability to

Table 2: Comparison of four existing backdoor attacks before and after BELT (+/++ denotes data/model outsourcing scenarios).

| Backdoor Attack Type | CIFAR-10-ResNet18 | | | GTSRB-VGG11 | | | TinyImageNet-EN-B3 | | |
|-----------------------|-------------------|--------|--------------|-------------|--------|--------------|--------------------|--------|--------------|
| | CDA(%) | ASR(%) | Excl(%) | CDA(%) | ASR(%) | Excl(%) | CDA(%) | ASR(%) | Excl(%) |
| Benign | 94.69 | - | - | 97.81 | - | - | 53.90 | - | - |
| BadNet [19] | 93.17 | 100.00 | 0.00 | 97.12 | 99.15 | 0.00 | 50.95 | 100.00 | 34.01 |
| BadNet ⁺ | 94.85 | 99.98 | 84.55 | 98.12 | 99.99 | 84.14 | 52.79 | 99.99 | 67.19 |
| BadNet ⁺⁺ | 94.62 | 100.00 | 87.09 | 98.35 | 99.98 | 89.34 | 52.31 | 100.00 | 72.30 |
| Blended [10] | 95.28 | 99.79 | 0.99 | 98.37 | 99.27 | 3.92 | 51.77 | 99.58 | 29.27 |
| Blended ⁺ | 94.48 | 98.47 | 16.18 | 96.41 | 99.37 | 20.70 | 51.95 | 98.78 | 49.22 |
| Blended ⁺⁺ | 94.61 | 99.14 | 20.06 | 97.70 | 99.98 | 24.21 | 51.31 | 99.29 | 53.98 |
| ISSBA [28] | 94.80 | 99.03 | 21.98 | 97.64 | 99.89 | 23.34 | 48.70 | 100.00 | 43.00 |
| ISSBA ⁺ | 95.16 | 97.57 | 23.73 | 98.12 | 99.97 | 25.76 | 48.86 | 99.91 | 46.66 |
| ISSBA ⁺⁺ | 94.13 | 99.97 | 27.33 | 98.01 | 100.00 | 29.68 | 48.26 | 99.87 | 53.03 |
| IAD [40] | 93.32 | 99.93 | 6.18 | 97.19 | 99.25 | 14.84 | 50.43 | 99.18 | 38.19 |
| IAD ⁺ | 92.78 | 97.04 | 29.67 | 97.33 | 99.51 | 48.89 | 47.95 | 99.47 | 55.19 |
| IAD ⁺⁺ | 93.34 | 99.56 | 36.71 | 97.74 | 99.85 | 75.07 | 48.93 | 98.95 | 89.26 |

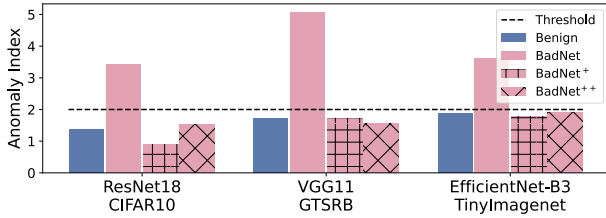


Figure 5: Performance of Neural Cleanse on backdoored models before and after BELT.

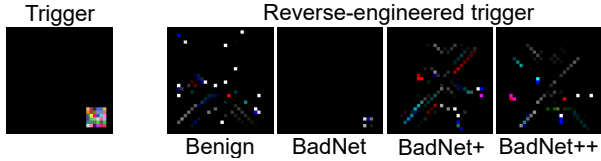


Figure 6: The trigger reverse-engineered by Neural Cleanse on the target label.

different types of backdoor attacks depending on different threat models, many countermeasures are relatively effective against Badnets [12], [17], [35], [50], [50], [52]. By evaluating BELT based on Badnets, we can more clearly elucidate the effectiveness of BELT in enhancing backdoor evasibility. The methodology of the evaluated defense countermeasures is described in Section B.

6.3.1. Neural Cleanse. We evaluate all BadNet models trained in Section 6.2 using Neural Cleanse [2]. We conduct 100 optimization periods through a reverse engineering process to generate reverse triggers for each class of the evaluated models. The neural cleanup process is repeated 10 times for each model to obtain an average anomaly metric, as illustrated in Figure 5. The results reveal that the anomaly index of the BELT model for all settings remains below the threshold of 2. This suggests that Neural Cleanse fails to detect the backdoor in the BELT model, whether it is a BadNet⁺ or a BadNet⁺⁺. The reason for this failure lies

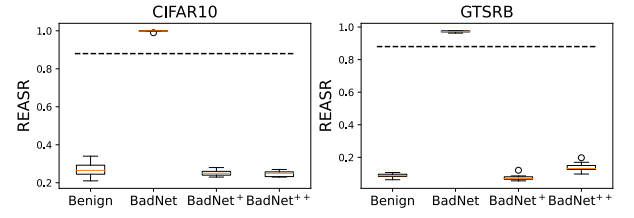


Figure 7: Performance of ABS on backdoored models before and after BELT.

in Neural Cleanse’s inability to accurately reverse engineer the fuzzy trigger through the reverse engineering process. Figure 6 provides an example set of reverse triggers for the target tag on the CIFAR-10 task, where the first column represents the original trigger for the backdoor. The benign model, lacking a backdoor, presents the reverse triggers as natural features of the target class, while the BadNet model, with a exclusivity of 0%, allows fuzzy triggers to be easily reverse-engineered. However, for BadNet⁺ and BadNet⁺⁺, the reverse triggers of the target class closely resemble those of the benign model. This is attributed to BELT significantly reducing the presence of fuzzy triggers by strengthening the backdoor exclusivity, making it challenging for Neural Cleanse to identify fuzzy triggers within the narrowed exclusivity boundary during the reverse engineering process.

6.3.2. ABS. We use ABS [4] to evaluate the Badnet models in Section 6.2 based on training on two tasks, CIFAR-10 and GTSRB. We construct a small clean dataset by randomly sampling 10 samples from each class to support ABS execution. In total, we sample 100 samples for CIFAR-10 and 430 samples for GTSRB. Subsequently, following ABS’s default settings, we detect the 10 most likely compromised neurons and reverse-engineer a corresponding trigger for each of these neurons to calculate the REASR metric. Figure 7 presents the REASR distribution for the 10 most likely compromised neurons in each model.

It is observed that ABS can effortlessly detect the back-

Table 3: Performance of MNTD on backdoored models before and after BELT.

| Test model set | CDA(%) | ASR(%) | Score | AUC(%) |
|--------------------------|--------|--------|-------|--------|
| Benign | 61.36 | - | 3.46 | |
| Backdoored | 61.29 | 99.73 | 12.14 | 95.63 |
| Benign | 61.36 | - | 3.46 | |
| Backdoored ⁺ | 62.18 | 85.27 | 7.34 | 75.81 |
| Benign | 61.36 | - | 3.46 | |
| Backdoored ⁺⁺ | 62.44 | 95.44 | 7.55 | 77.61 |

door in the regular Badnet model, as its REASR exceeds the threshold of 0.88 and approaches 1.0. However, ABS fails to effectively detect Badnet⁺ and Badnet⁺⁺, where their REASR values are close to those of the benign model. This is not surprising; similar to Neural Cleanse, ABS performs reverse engineering on compromised neurons to obtain corresponding reverse triggers. The strong exclusivity of the backdoor hinders this process, preventing it from acquiring a reverse trigger capable of activating the backdoor, resulting in REASR values far below the threshold.

6.3.3. MNTD. For the evaluation of Meta-Neural Trojan Detection (MNTD) [5], we adhere to the training settings of MNTD initially, employing transfer learning to construct a meta-classifier. This meta-classifier is trained on the CIFAR-10 dataset, comprising 2048 benign models and 2048 backdoor models within a shadow model set. During the evaluation phase, we train 256 benign test models (referred to as "Benign") and 256 backdoor test models (referred to as "Backdoored"). Additionally, we train an additional 256 backdoor models in the data outsourcing scenario (referred to as "Backdoored⁺") and another 256 backdoor models in the model outsourcing scenario (referred to as "Backdoored⁺⁺").

It is crucial to highlight that both "Backdoored⁺" and "Backdoored⁺⁺" maintain identical training settings as "Backdoored," encompassing model architecture, backdoor configurations, and training hyperparameters. This ensures that any impact on detection performance stems solely from the actions of the backdoor itself, rather than changes in hyperparameters [45]. In Table 3, the average performance of the three test model sets is presented. MNTD demonstrates commendable performance on the test set containing ordinary backdoored models ("Backdoored"), achieving an AUC of 95.63%. However, the high-exclusivity backdoor models effectively resist MNTD detection, exhibiting AUCs of 75.81% and 77.61% for the test sets based on "Backdoored⁺" and "Backdoored⁺⁺," respectively. The primary cause lies in the fact that backdoors with stronger exclusivity exhibit reduced responsiveness to optimized queries compared to those with weaker exclusivity. Consequently, meta-classifiers are inclined to predict lower scores for strongly exclusive backdoor models, posing challenges in distinguishing them significantly from benign models and leading to diminished detection performance.

Table 4: Performance of MOTH on backdoored models before and after BELT.

| Attack Type | CIFAR-10-ResNet18 | | GTSRB-VGG11 | |
|-----------------------|-------------------|---------------|-------------|--------------|
| | CDA(%) | ASR(%) | CDA(%) | ASR(%) |
| BadNet | 92.32 | 32.47 | 75.31 | 38.29 |
| BadNet ⁺ | 93.41 | 98.62 | 74.88 | 77.56 |
| BadNet ⁺⁺ | 93.03 | 100.00 | 67.76 | 99.71 |
| Blended | 93.64 | 33.74 | 76.39 | 1.30 |
| Blended ⁺ | 92.34 | 96.43 | 62.61 | 98.86 |
| Blended ⁺⁺ | 91.98 | 99.53 | 88.66 | 92.54 |
| ISSBA | 81.29 | 1.20 | 95.36 | 66.91 |
| ISSBA ⁺ | 85.61 | 87.78 | 69.86 | 74.50 |
| ISSBA ⁺⁺ | 84.42 | 99.05 | 92.21 | 93.66 |
| IAD | 92.21 | 9.78 | 69.53 | 57.81 |
| IAD ⁺ | 90.38 | 92.46 | 66.75 | 77.30 |
| IAD ⁺⁺ | 91.79 | 97.89 | 69.30 | 77.21 |

6.3.4. MOTH. According to the original configurations outlined in MOTH [6], we conduct experiments on both backdoored models and augmented backdoored models using three standard datasets. Following the warm-up and two-sided backdoor generation training pipeline, we adopt the pair scheduling method from the same source. Promising pairs are determined based on the largest growth of class distance within a fixed number of optimization cycles. MOTH is evaluated on backdoored models obtained from previous experiments, and the effectiveness of our proposed BELT framework is demonstrated in Table 4. Our focus lies on examining the CDA and ASR of both original backdoored models and BELT-augmented models. The defense effects under identical experimental conditions are documented, showing the remaining CDA and ASR of the model after applying the MOTH defense. In essence, BELT reinforces the backdoor exclusivity, rendering the backdoor samples more stealthy. This reinforcement could potentially weaken defenses that rely on hardening the model's decision boundaries. Results in Table 4 reveal a significant reduction in ASR for non-augmented models following the MOTH defense. Conversely, models augmented with our BELT framework exhibit a substantial increase in ASR compared to models without BELT. These experimental outcomes underscore the efficacy of our proposed BELT framework.

6.3.5. STRIP. Figure 8 displays the entropy distribution results of benign samples and trigger-carrying samples on a regular Badnet and a exclusivity-enhanced Badnet as evaluated by STRIP [3]. The assessed models utilize the ResNet18 architecture and are trained on the CIFAR-10 dataset. The distribution is evaluated on 1000 trigger images and 1000 clean images. For the regular Badnet model, STRIP effectively distinguishes samples carrying triggers from clean samples because there is a noticeable gap in the entropy value distribution between trigger samples and clean samples. However, for Badnet⁺ and Badnet⁺⁺, their entropy

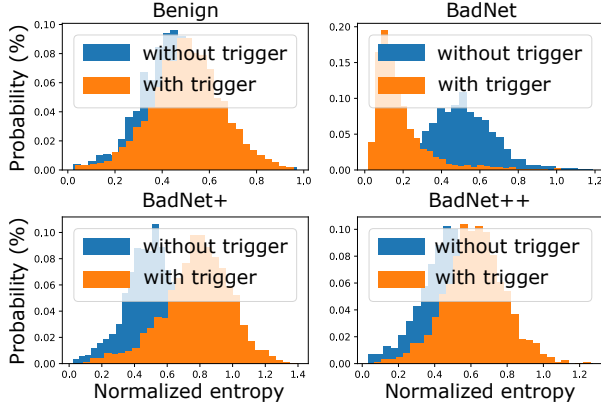


Figure 8: Performance of STRIP on backdoored models before and after BELT.

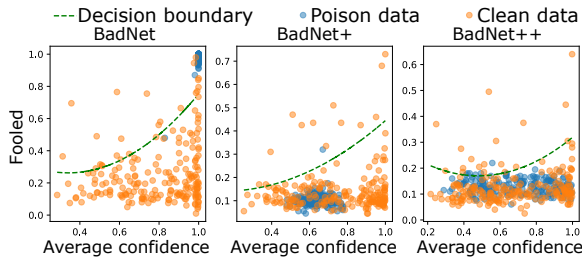


Figure 9: Performance of SentiNet on backdoored models before and after BELT.

distributions are similar to the benign model, with a significant overlap, rendering STRIP ineffective. The primary reason for this phenomenon is that the high exclusivity of the backdoor disrupts the strong hijacking effect of the trigger under different perturbations. As a result, the perturbed trigger, when overlaid with benign samples, is no longer a fuzzy trigger capable of activating the backdoor.

6.3.6. SentiNet. We partition the clean data into intervals based on a fixed average confidence step and select the two data points with the highest Foolde within each interval as decision points for fitting the decision boundary. Figure 9 illustrates the detection performance of SentiNet [7]. For a regular Badnet, the trigger on poisoned data significantly influences the model output, resulting in high average confidence and Foolde within each interval. This leads to an effective decision boundary that distinguishes poisoned data from clean data. However, the detection performance of SentiNet is not satisfactory for Badnet⁺ and Badnet⁺⁺. Poisoned data and clean data are confounded, causing the decision boundary to be ineffective in distinguishing them. One possible reason is that GradCAM cannot ensure the capture of a complete trigger (see the last column of Figure Figure 1). For highly exclusive backdoors, such incomplete triggers do not elicit a response from the backdoor, escaping detection by SentiNet.

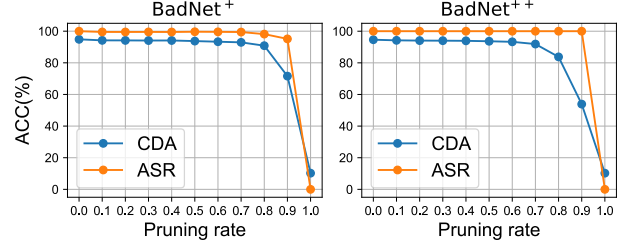


Figure 10: Performance of Fine-Pruning on backdoored models after BELT.

Table 5: Ablation study results for trigger upper bound optimization algorithm.

| Baseline | Trigger upper bound β_U | | |
|--------------------|-------------------------------|---------------------|----------------------|
| | Badnet | Badnet ⁺ | Badnet ⁺⁺ |
| Comparison Group A | 5.13 | 6.19 | 6.09 |
| Comparison Group B | 5.13 | 6.41 | 6.12 |
| Comparison Group C | 7.76 | 6.39 | 6.21 |
| Overall | 7.76 | 6.68 | 6.36 |

6.3.7. Fine-Pruning. Fine-Pruning [34] is one of the earliest defenses based on parameter updating, which is motivated from the following observation: the inputs with triggers usually activate neurons that are dormant in the presence of clean inputs. Therefore, Fine-Pruning attempts to erase the backdoor by pruning neurons which are scarcely activated for the clean inputs. To reduce the impact on CDA, Fine-Pruning further applies fine-tuning after pruning to restore the model performance.

To verify the impact of updating model parameters on BELT, we apply Fine-Pruning (with the default configuration in its official implementation [1]) on BadNet⁺ and BadNet⁺⁺, with the CIFAR10 dataset and the ResNet18 architecture. As shown in Figure 10, Fine-Pruning fails to effectively remove the backdoor enhanced by BELT, since ASR remains higher than CDA at various pruning rates. Only when the pruning rate reaches 90% does ASR begin to decrease, while CDA has already suffered an unacceptable loss.

7. Discussion

(a) Ablation Studies. We conducted the following ablation experiments to validate the effectiveness and contribution of each component in the trigger upper bound optimization process. The experimental subject is the Badnet model, with a ResNet18 architecture, trained on the CIFAR-10 dataset. The specific results are presented in Table 5.

- **Comparison Group A: Intuitive objective function.** First, we investigated the impact of an intuitive objective function on the optimization of the trigger upper bound. In this baseline, the optimization process does not include the optimization direction and dynamic weights. The objective function used is as defined in Equation 4.

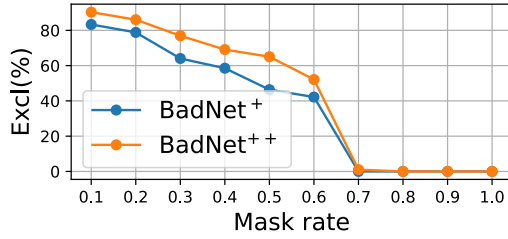


Figure 11: Comparison of backdoor exclusivity of Badnet under different mask rates.

However, such an optimization process is prone to local optima, resulting in a trigger upper bound significantly smaller than its actual precise value, especially for a regular Badnet.

- **Comparison Group B: Without optimization direction.** We reveal the influence of the optimization direction on the trigger upper bound. Here, we use the regularization term from Equation 4 instead of the one from Equation 7, while retaining the dynamic weight mechanism, to eliminate the impact of the optimization direction on the optimization results. The results show a noticeable difference from the overall performance, indicating that the optimization direction guides the process, aiding in escaping local optima and finding a more significant perturbation for a fuzzy trigger.
- **Comparison Group C: Without dynamic weight.** We use this baseline to validate the effectiveness of dynamic weights. Here, we remove the dynamic weight mechanism from Equation 7 and replace it with a small static value (0.1). The table shows a significant performance drop on both BadNet⁺ and BadNet⁺⁺, confirming that dynamic weights help bring the perturbation closer to the trigger upper bound during the optimization process.

These three baselines illustrate that the optimization direction and dynamic weight mechanism can play a positive role in the optimization of the trigger upper bound. By introducing these two components, we can effectively calculate a more accurate trigger upper bound.

(b) Effect of Mask Rate on Exclusivity. Cover samples are instances with a fuzzy trigger and correct labels, designed to suppress the association between the backdoor and the fuzzy trigger, thereby enhancing the exclusivity of the backdoor. In our approach, the trigger carried by cover samples is constructed through a masking-based method. It involves randomly masking a fixed percentage (e.g. 20%) of the original trigger, generating different fuzzy triggers.

The quality of the fuzzy trigger carried by cover samples directly influences the degree of exclusivity enhancement. Therefore, we focus on the impact of mask rates on backdoor exclusivity. We trained multiple Badnet models using different mask rates, employing the ResNet18 architecture and the CIFAR-10 dataset. As depicted in Figure 11, a mask rate of 1.0 indicates that the fuzzy trigger on cover samples is completely masked, treating these samples as clean samples, corresponding to the training setting of a

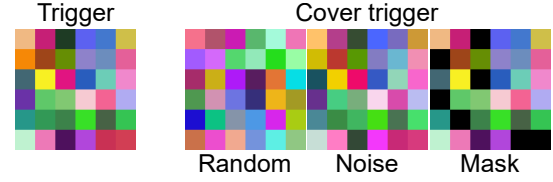


Figure 12: Examples of cover triggers constructed in three different methods.

conventional backdoor. As the mask rate decreases, backdoor exclusivity gradually increases. This is attributed to lower mask rates improving the quality of the fuzzy trigger, making it closer to the original trigger. By suppressing the association between the backdoor and high-quality fuzzy triggers, backdoor exclusivity can be significantly enhanced.

(c) Cover Trigger Construction. In our previous experiments, we focused on constructing cover triggers (fuzzy triggers carried by cover samples) using a masking-based approach. Here, we explore other possible methods for constructing cover samples. Specifically, we additionally consider two ways to construct cover triggers, namely, random sampling and noise injection. The random sampling approach constructs a cover trigger by randomly sampling from the distribution of the original trigger. On the other hand, the noise injection approach involves adding noise (Gaussian noise with a mean of 0 and a standard deviation of 0.1) to the original trigger, creating a cover trigger. Figure 12 illustrates examples of cover triggers constructed using these two methods.

We use these two approaches to build two new cover datasets, and each is used to train a Badnet backdoored model. The models use a ResNet18 architecture and the CIFAR-10 dataset. The final backdoor exclusivity achieved by these models is 58.43% and 80.05%, respectively. In comparison, the cover triggers constructed based on the masking approach show the most significant improvement in exclusivity, reaching 84.55% under the same settings. The improvement in exclusivity with cover triggers constructed through random sampling is limited, mainly because it is challenging to construct cover triggers in a controlled manner using this approach. In contrast, cover triggers constructed by adding noise and the masking approach can be controlled by adjusting the noise intensity and masking ratio. However, constructing cover triggers based on adding noise is challenging to determine the appropriate noise intensity. We opt for the masking-based approach, using a default mask rate of 20%, which achieves good exclusivity enhancement in all settings.

(d) Adaptive Defense. In this part, we analyze the potential adaptive defense against BELT. As the effectiveness of BELT relies on the exclusivity of backdoors, only sufficiently precise triggers have the ability to activate the backdoor. In other words, the backdoor exclusivity prevents the backdoor from responding to fuzzy triggers. Therefore, an adaptive defender may attempt to add noises to the input data to make the potential triggers

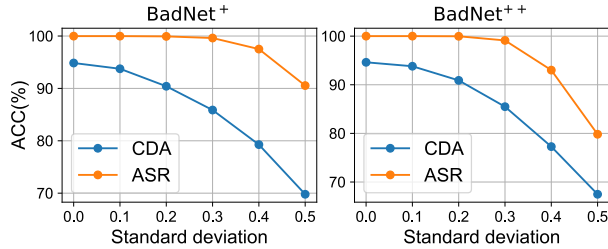


Figure 13: Performance of BELT in Gaussian noise with different standard deviations.

fuzzy, thereby circumventing the backdoor effect. Below, we further verify the resilience of BELT to Gaussian perturbations. As shown in Figure 13, for BadNet⁺ under the CIFAR-10 and ResNet18 settings, CDA/ASR decreases from 94.85%/99.98% to 69.79%/90.54% as the standard deviation of the noise increases from 0 to 0.05. BadNet⁺⁺ exhibits the same trend as BadNet⁺, with ASR consistently outperforming CDA as the noise intensity increases. This indicates that BELT achieves balance between backdoor exclusivity and perturbation resistance.

(e) Limitations and Future Works. In this study, we have taken a step towards evaluating and fortifying backdoor exclusivity in the context of data outsourcing and model outsourcing scenarios. To precisely quantify backdoor exclusivity is computationally challenging. We instead design an optimization-based algorithm to estimate the exclusivity score. Our algorithm incorporates optimization directions and dynamic weights to evade the potential local minima during the estimation. The experimental results show the estimated exclusivity score does reflect well the stealthiness of different backdoor attacks. Considering the importance of the exclusivity score in characterizing the backdoor stealthiness, it would be meaningful for future works to devise more accurate estimation of backdoor exclusivity via, e.g., more advanced numeric techniques.

To evade existing defenses, BELT suppresses the correlation between the backdoor and the fuzzy triggers, a key trait exploited by the state-of-the-art defenses for backdoor detection. However, in the data outsourcing cases, the activation vectors of the poisoned samples may be outliers to the benign ones for existing backdoor attacks, which may leave an extra dimension for the defender to do, e.g., data cleansing [39]. Nevertheless, when the attacker has more control over the victim model (e.g., in the model outsourcing case, a more popular scenario due to the rise of third-party model supply chains such as HuggingFace [21]), BELT makes further efforts in introducing momentum-based center loss to make poisoned sample features to be indistinguishable from benign ones. In our study, we have tried our best to cover the typical backdoor defenses published at top-tier conferences in recent years. Future works may consider further validating our attack technique on more newly proposed backdoor defenses.

8. Conclusion

In this work, we propose and investigate a novel characteristic of backdoor attacks called *backdoor exclusivity*. Based on our proposed approximation algorithm to quantify exclusivity, we conduct a comprehensive analysis of the intricate relation between backdoor exclusivity and the existence of many fuzzy triggers in the classical backdoor attacks, which are intensively exploited by the state-of-the-art defenses to detect and recover the triggers. To enhance the capability of existing backdoor attacks to evade the state-of-the-art defenses, we introduce Backdoor Exclusivity LifTing (BELT) which suppresses the association between the backdoor and the potential fuzzy triggers and can be seamlessly combined with almost any existing backdoor attacks. We thoroughly validate the effectiveness of BELT on four existing backdoor attacks which would otherwise be detected by the state-of-the-art defenses. After applying the BELT technique, the backdoored models exhibit high evasiveness against seven state-of-the-art backdoor defenses. This is primarily attributed to BELT refining the activation conditions of the backdoor, disrupting the necessary assumptions of these defense mechanisms, and causing them to struggle in obtaining an effective fuzzy trigger in the presence of a strongly exclusive backdoor.

Acknowledgements

We would like to thank the anonymous reviewers for their insightful comments that helped improve the quality of the paper. This work was supported in part by the National Key Research and Development Program (2021YFB3101200), National Natural Science Foundation of China (62172104, 62172105, 61972099, 62102093, 62102091). Min Yang is a faculty of Shanghai Institute of Intelligent Electronics & Systems and Engineering Research Center of Cyber Security Auditing and Monitoring, Ministry of Education, China. Mi Zhang and Min Yang are the corresponding authors.

References

- [1] kangliucn/fine-pruning-defense (github repository), 2018. <https://github.com/kangliucn/Fine-pruning-defense>.
- [2] bolunwang/backdoor (github repository), 2019. <https://github.com/bolunwang/backdoor>.
- [3] garrisonsys/strip (github repository), 2019. <https://github.com/garrisonsys/STRIP>.
- [4] naiyeleo/abs (github repository), 2019. <https://github.com/naiyeleo/ABS>.
- [5] Ai-secure/meta-neural-trojan-detection (github repository), 2021. <https://github.com/Ai-secure/Meta-Neural-Trojan-Detection>.
- [6] Gwinhen/moth (github repository), 2022. <https://github.com/Gwinhen/MOTH>.
- [7] vtu81/backdoor-toolbox (github repository), 2023. https://github.com/vtu81/backdoor-toolbox/blob/main/cleaners_tool_box/sentinet.py.
- [8] BARACALDO, N., AND OPREA, A. Machine learning security and privacy. *IEEE Security & Privacy* 20, 5 (2022), 11–13.

- [9] CAO, Y., WANG, N., XIAO, C., YANG, D., FANG, J., YANG, R., CHEN, Q. A., LIU, M., AND LI, B. Invisible for both camera and lidar: Security of multi-sensor fusion based perception in autonomous driving under physical-world attacks. In *2021 IEEE Symposium on Security and Privacy (SP)* (2021), IEEE, pp. 176–194.
- [10] CHEN, X., LIU, C., LI, B., LU, K., AND SONG, D. Targeted backdoor attacks on deep learning systems using data poisoning. *arXiv preprint arXiv:1712.05526* (2017).
- [11] CHENG, S., LIU, Y., MA, S., AND ZHANG, X. Deep feature space trojan attack of neural networks by controlled detoxification. In *Proceedings of the AAAI Conference on Artificial Intelligence* (2021), vol. 35, pp. 1148–1156.
- [12] CHOU, E., TRAMER, F., AND PELLEGRINO, G. Sentinet: Detecting localized universal attacks against deep learning systems. In *2020 IEEE Security and Privacy Workshops (SPW)* (2020), IEEE, pp. 48–54.
- [13] COHEN, J., ROSENFELD, E., AND KOLTER, Z. Certified adversarial robustness via randomized smoothing. In *international conference on machine learning* (2019), PMLR, pp. 1310–1320.
- [14] DOAN, K., LAO, Y., ZHAO, W., AND LI, P. Lira: Learnable, imperceptible and robust backdoor attacks. In *Proceedings of the IEEE/CVF international conference on computer vision* (2021), pp. 11966–11976.
- [15] FENG, Y., MA, B., ZHANG, J., ZHAO, S., XIA, Y., AND TAO, D. FIBA: Frequency-injection based backdoor attack in medical image analysis. In *Proc. CVPR* (2022), pp. 20876–20885.
- [16] GAO, Y., DOAN, B. G., ZHANG, Z., MA, S., ZHANG, J., FU, A., NEPAL, S., AND KIM, H. Backdoor attacks and countermeasures on deep learning: A comprehensive review. *arXiv preprint arXiv:2007.10760* (2020).
- [17] GAO, Y., XU, C., WANG, D., CHEN, S., RANASINGHE, D. C., AND NEPAL, S. STRIP: A defence against Trojan attacks on deep neural networks. In *Proc. ACSAC* (2019), pp. 113–125.
- [18] GAWLIKOWSKI, J., TASSI, C. R. N., ALI, M., LEE, J., HUMT, M., FENG, J., KRUSPE, A., TRIEBEL, R., JUNG, P., ROSCHER, R., ET AL. A survey of uncertainty in deep neural networks. *Artificial Intelligence Review* 56, Suppl 1 (2023), 1513–1589.
- [19] GU, T., DOLAN-GAVITT, B., AND GARG, S. BadNets: Identifying vulnerabilities in the machine learning model supply chain. *arXiv preprint arXiv:1708.06733* (2017).
- [20] HE, K., ZHANG, X., REN, S., AND SUN, J. Deep residual learning for image recognition. In *Proc. CVPR* (2016), pp. 770–778.
- [21] JIANG, W., SYNOVIC, N., SETHI, R., INDARAPU, A., HYATT, M., SCHORLEMMER, T. R., THIRUVATHUKAL, G. K., AND DAVIS, J. C. An empirical study of artifacts and security risks in the pre-trained model supply chain. In *Proceedings of the 2022 ACM Workshop on Software Supply Chain Offensive Research and Ecosystem Defenses* (2022), pp. 105–114.
- [22] KATZ, G., BARRETT, C., DILL, D. L., JULIAN, K., AND KOCHENDERFER, M. J. Reluplex: An efficient smt solver for verifying deep neural networks. In *Computer Aided Verification: 29th International Conference, CAV 2017, Heidelberg, Germany, July 24-28, 2017, Proceedings, Part I* 30 (2017), Springer, pp. 97–117.
- [23] KRIZHEVSKY, A., HINTON, G., ET AL. Learning multiple layers of features from tiny images. *Computer Science Department, University of Toronto, Tech. Rep 1* (2009).
- [24] LE, Y., AND YANG, X. Tiny imagenet visual recognition challenge. *CS 231N* 7, 7 (2015), 3.
- [25] LI, L., XIE, T., AND LI, B. Sok: Certified robustness for deep neural networks. In *2023 IEEE symposium on security and privacy (SP)* (2023), IEEE, pp. 1289–1310.
- [26] LI, S., XUE, M., ZHAO, B. Z. H., ZHU, H., AND ZHANG, X. Invisible backdoor attacks on deep neural networks via steganography and regularization. *IEEE Transactions on Dependable and Secure Computing* 18, 5 (2020), 2088–2105.
- [27] LI, Y., JIANG, Y., LI, Z., AND XIA, S.-T. Backdoor learning: A survey. *IEEE Transactions on Neural Networks and Learning Systems* (2022).
- [28] LI, Y., LI, Y., WU, B., LI, L., HE, R., AND LYU, S. Invisible backdoor attack with sample-specific triggers. In *Proc. ICCV* (2021), pp. 16463–16472.
- [29] LI, Y., LYU, X., KOREN, N., LYU, L., LI, B., AND MA, X. Anti-backdoor learning: Training clean models on poisoned data. *Advances in Neural Information Processing Systems* 34 (2021), 14900–14912.
- [30] LI, Y., MA, H., ZHANG, Z., GAO, Y., ABUADDBA, A., XUE, M., FU, A., ZHENG, Y., AL-SARAWI, S. F., AND ABBOTT, D. Ntd: Non-transferability enabled deep learning backdoor detection. *IEEE Transactions on Information Forensics and Security* (2023).
- [31] LI, Y., WU, B., JIANG, Y., LI, Z., AND XIA, S.-T. Backdoor learning: A survey. *arXiv preprint arXiv:2007.08745* (2020).
- [32] LI, Y., ZHAI, T., JIANG, Y., LI, Z., AND XIA, S.-T. Backdoor attack in the physical world. *arXiv preprint arXiv:2104.02361* (2021).
- [33] LIN, J., XU, L., LIU, Y., AND ZHANG, X. Composite backdoor attack for deep neural network by mixing existing benign features. In *Proc. CCS* (2020), pp. 113–131.
- [34] LIU, K., DOLAN-GAVITT, B., AND GARG, S. Fine-pruning: Defending against backdooring attacks on deep neural networks. In *Proceedings of RAID* (2018).
- [35] LIU, Y., LEE, W.-C., TAO, G., MA, S., AAFER, Y., AND ZHANG, X. ABS: Scanning neural networks for back-doors by artificial brain stimulation. In *Proc. CCS* (2019), pp. 1265–1282.
- [36] LIU, Y., MA, X., BAILEY, J., AND LU, F. Reflection backdoor: A natural backdoor attack on deep neural networks. In *ECCV* (2020), Springer, pp. 182–199.
- [37] MA, H., QIU, H., GAO, Y., ZHANG, Z., ABUADDBA, A., XUE, M., FU, A., ZHANG, J., AL-SARAWI, S. F., AND ABBOTT, D. Quantization backdoors to deep learning commercial frameworks. *IEEE Transactions on Dependable and Secure Computing* (2023).
- [38] MA, H., WANG, S., AND GAO, Y. Horizontal class backdoor to deep learning. *arXiv preprint arXiv:2310.00542* (2023).
- [39] MA, W., WANG, D., SUN, R., XUE, M., WEN, S., AND XIANG, Y. The“ beatrix”resurrections: Robust backdoor detection via gram matrices. In *NDSS* (2023).
- [40] NGUYEN, T. A., AND TRAN, A. Input-aware dynamic backdoor attack. *NIPS* 33 (2020), 3454–3464.
- [41] NGUYEN, T. D., MARCHAL, S., MIETTINEN, M., FEREIDOUNI, H., ASOKAN, N., AND SADEGHI, A.-R. Diot: A federated self-learning anomaly detection system for iot. In *2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS)* (2019), IEEE, pp. 756–767.
- [42] PAN, X., ZHANG, M., YAN, Y., AND YANG, M. Understanding the threats of trojaned quantized neural network in model supply chains. In *Annual Computer Security Applications Conference* (2021), pp. 634–645.
- [43] PARKHI, O. M., VEDALDI, A., AND ZISSERMAN, A. Deep face recognition.
- [44] PENG, Z., YANG, J., CHEN, T.-H., AND MA, L. A first look at the integration of machine learning models in complex autonomous driving systems: a case study on apollo. In *Proceedings of the 28th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering* (2020), pp. 1240–1250.
- [45] QIU, H., MA, H., ZHANG, Z., ABUADDBA, A., KANG, W., FU, A., AND GAO, Y. Towards a critical evaluation of robustness for deep learning backdoor countermeasures. *IEEE Transactions on Information Forensics and Security* (2023).
- [46] SARKAR, E., BENKRAOUDA, H., AND MANIATAKOS, M. Facehack: Triggering backdoored facial recognition systems using facial characteristics. *arXiv preprint arXiv:2006.11623* (2020).

- [47] SIMONYAN, K., AND ZISSERMAN, A. Very deep convolutional networks for large-scale image recognition. *arXiv preprint arXiv:1409.1556* (2014).
- [48] STALLKAMP, J., SCHLIPSING, M., SALMEN, J., AND IGEL, C. Man vs. computer: Benchmarking machine learning algorithms for traffic sign recognition. *Neural Networks* 32 (2012), 323–332.
- [49] TANG, D., WANG, X., TANG, H., AND ZHANG, K. Demon in the variant: Statistical analysis of DNNs for robust backdoor contamination detection. In *USENIX Security Symp.* (2021), pp. 1541–1558.
- [50] TAO, G., LIU, Y., SHEN, G., XU, Q., AN, S., ZHANG, Z., AND ZHANG, X. Model orthogonalization: Class distance hardening in neural networks for better security. In *S&P* (2022), vol. 3.
- [51] TURK, A. M. Amazon mechanical turk. *Retrieved August 17* (2012), 2012.
- [52] WANG, B., YAO, Y., SHAN, S., LI, H., VISWANATH, B., ZHENG, H., AND ZHAO, B. Y. Neural Cleanse: Identifying and mitigating backdoor attacks in neural networks. In *S&P* (2019), IEEE, pp. 707–723.
- [53] WANG, S., GAO, Y., FU, A., ZHANG, Z., ZHANG, Y., SUSILO, W., AND LIU, D. Cassock: Viable backdoor attacks against dnn in the wall of source-specific backdoor defenses. In *Proceedings of the 2023 ACM Asia Conference on Computer and Communications Security* (2023), pp. 938–950.
- [54] WEBER, M., XU, X., KARLAŠ, B., ZHANG, C., AND LI, B. Rab: Provable robustness against backdoor attacks. In *2023 IEEE Symposium on Security and Privacy (SP)* (2023), IEEE, pp. 1311–1328.
- [55] WEN, Y., ZHANG, K., LI, Z., AND QIAO, Y. A discriminative feature learning approach for deep face recognition. In *Computer Vision—ECCV 2016: 14th European Conference, Amsterdam, The Netherlands, October 11–14, 2016, Proceedings, Part VII 14* (2016), Springer, pp. 499–515.
- [56] WENG, T.-W., ZHANG, H., CHEN, P.-Y., YI, J., SU, D., GAO, Y., HSIEH, C.-J., AND DANIEL, L. Evaluating the robustness of neural networks: An extreme value theory approach. *arXiv preprint arXiv:1801.10578* (2018).
- [57] WENGER, E., PASSANANTI, J., BHAGOJI, A. N., YAO, Y., ZHENG, H., AND ZHAO, B. Y. Backdoor attacks against deep learning systems in the physical world. In *Proc. CVPR* (2021), pp. 6206–6215.
- [58] WU, T., WANG, T., SEHWAG, V., MAHLOUJIFAR, S., AND MITTAL, P. Just rotate it: Deploying backdoor attacks via rotation transformation. In *Proc. AISec* (2022).
- [59] XU, X., WANG, Q., LI, H., BORISOV, N., GUNTER, C. A., AND LI, B. Detecting AI trojans using meta neural analysis. In *S&P* (2021), IEEE, pp. 103–120.
- [60] XUE, M., HE, C., SUN, S., WANG, J., AND LIU, W. Robust backdoor attacks against deep neural networks in real physical world. In *2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)* (2021), IEEE, pp. 620–626.
- [61] XUE, M., WANG, X., SUN, S., ZHANG, Y., WANG, J., AND LIU, W. Compression-resistant backdoor attack against deep neural networks. *Applied Intelligence* (2023), 1–16.
- [62] YANG, Y., LIU, T. Y., AND MIRZASOLEIMAN, B. Not all poisons are created equal: Robust training against data poisoning. In *International Conference on Machine Learning* (2022), PMLR, pp. 25154–25165.
- [63] ZHANG, J., DONGDONG, C., HUANG, Q., LIAO, J., ZHANG, W., FENG, H., HUA, G., AND YU, N. Poison ink: Robust and invisible backdoor attack. *IEEE Transactions on Image Processing* 31 (2022), 5691–5705.
- [64] ZHOU, L., FU, A., YANG, G., WANG, H., AND ZHANG, Y. Efficient certificateless multi-copy integrity auditing scheme supporting data dynamics. *IEEE Transactions on Dependable and Secure Computing* (2020).

Appendix A.

Trigger Upper Bound Optimization Algorithm

The detailed optimization process for trigger upper bounds is shown in Algorithm 1.

Algorithm 1 Optimize Trigger Upper Bound

Require: Backdoored model $F_{\theta'}$, target label t , clean image x and mask m_x , trigger pattern p and mask m_p , perturbation boundary δ_b

- 1: Initialize optimizable perturbation δ and regular term weight λ
- 2: Set learning rate α and number of epochs E
- 3: **for** epoch $\leftarrow 1$ to E **do**
- 4: $x' = \text{clip}(x \cdot m_x + (p + \delta) \cdot m_p, 0, 1)$ ▷ Add perturbed trigger for x
- 5: $y' = F_{\theta'}(x')$
- 6: **if** $\text{epoch} > \frac{E}{2}$ **then**
- 7: $\tilde{y}' = \text{normalize}(y')$
- 8: $\lambda \leftarrow \lambda + \tilde{y}'_{y_t} - \max_{i \neq y_t}(\tilde{y}'_i)$ ▷ Dynamic update λ
- 9: **end if**
- 10: $\mathcal{L} = -y_t \log(y') + \lambda \|\delta_b - \delta\|_2$
- 11: $\delta \leftarrow \delta - \alpha \frac{\partial \mathcal{L}}{\partial \delta}$
- 12: **end for**
- 13: **return** Trigger upper bound $\|\delta\|_2$ for x

Appendix B.

Methodology Description

B.1. Neural Cleanse

In addressing the susceptibility of neural networks to backdoor attacks, the Neural Cleanse [52] framework focuses on the reverse engineering of triggers, aiming to detect and mitigate the creation of “shortcuts” in the latent space that lead to misclassification. The core concept involves estimating the minimum perturbation necessary to generate the smallest “shortcut” for each targeted category, effectively reverse engineering the trigger. The methodology consists of three key steps: firstly, reverse engineering the smallest trigger for a given label using an optimization algorithm; secondly, iteratively applying this process to generate a one-to-one corresponding reverse-engineered trigger per label; and thirdly, evaluating whether a reverse-engineered trigger for a category is significantly smaller than others, identifying it as a genuine trigger. If no significant outlier is detected, the model is deemed benign. To assess the anomaly index of the model, Neural Cleanse utilizes the Median Absolute Deviation (MAD) for robustness against outliers. The L_1 norm of all reverse-engineered triggers is calculated, and MAD is determined by computing the median of absolute deviations. The anomaly index is expressed as the absolute difference between the minimum norm and the median, divided by the product of the median absolute deviation and a constant estimator (1.4826). A model with an anomaly

index greater than 2 is considered more than 95% likely to be backdoored.

B.2. ABS

Artificial Brain Stimulation (ABS) [35] serves as a backdoor detection methodology, drawing inspiration from Electrical Brain Stimulation (EBS). ABS employs a controlled approach, manipulating the activation of individual artificial neurons while keeping others fixed to assess their impact on classification behavior, thereby scrutinizing neural models for the presence of backdoors. Rooted in the recognition that concealed damaged neurons exert influence over backdoor behavior, ABS leverages Neuron Stimulation Functions (NSF) to gauge the repercussions of neuron activation on label output. ABS initiates the identification of damaged neurons by computing the NSF of the selected layer, designating neurons with significantly heightened output activation as candidate damaged neurons. In an iterative process, ABS scans neurons, marks those with notable output activation increases as damaged candidates, and utilizes an optimized method for reverse engineering to generate triggers for the ten most probable damaged neurons. The determination of a model's susceptibility to backdoors is contingent on a threshold derived from the Reverse-Engineered Trojan Trigger Attack Success Rate (REASR); if the REASR of the reverse trigger surpasses the 88% threshold, the model is classified as harboring a backdoor, otherwise, it is deemed benign.

B.3. MNTD

Meta Neural Trojan Detection (MNTD) [59] focuses on training a meta-classifier capable of distinguishing between backdoored and clean models within a specific dataset. The process involves three main steps: shadow model generation, meta-classifier training, and target model detection. Initially, a multitude of shadow models, comprising both clean and backdoored models, are trained on a small dataset accessible to the defender. These backdoored models undergo various poison attacks, including modification and blending attacks. The resulting shadow models, intentionally trained with limited convergence to minimize training overhead, form the basis for subsequent steps. In the meta-classifier training phase, a modest number of queries are fed into the shadow models, generating concatenated outputs (logits) for each query. These logits, alongside ground-truth labels (benign or backdoored), serve as inputs for training the meta-classifier. Importantly, the queries are iteratively updated to optimize efficiency during meta-classifier training. The final step involves utilizing optimized queries as input for the target model, obtaining logits that are then inputted into the meta-classifier, producing a score. This score serves as an indicator of the target model's malicious degree, with a higher score indicating potential backdoor injection. MNTD uses the area under the curve (AUC) as the primary metric to evaluate meta-classifier performance. In this case, the meta-classifier first calculates the scores of all models in the test

model set and then calculates the AUC based on the model's label (0 for benign models and 1 for backdoored models).

B.4. MOTH

Model Orthogonalization (MOTH) [50] represents an innovative technique for fortifying models, particularly those with potential backdoors, by introducing additional training steps to eliminate any latent vulnerabilities in the model. To elaborate, MOTH employs a unique approach to compel the model to eradicate low-level backdoor features. This is achieved through an iterative process that generates minimal backdoors between classes a and b , as well as between b and a . The proposed framework leverages adversarial training to enhance the reinforcement process. MOTH identifies minimal backdoors originating from the victim class towards the target class, utilizing these samples with unaltered labels as training data. This strategic utilization encourages the model to disregard potential target shortcuts and instead prioritize the inherent characteristics of the training samples. In practical applications, particularly when dealing with models susceptible to hidden backdoors, an initial step involves symmetric hardening to create symmetric backdoors. Subsequently, promising scheduling pairs are carefully chosen based on the maximal increase in the distance between classes. Finally, the model undergoes training in model orthogonalization using these selected pairs.

B.5. STRIP

STRIP [17] is an online detection method functioning at the data level, is crafted to discern contaminated data harboring triggers within the input. The procedure strategically capitalizes on the input-agnostic strength of triggers, allowing STRIP to identify contaminated inputs through an evaluation of the consistency of perturbed replicas. This method involves the superimposition of the input with clean samples, leading to the creation of multiple copies. These copies, when fed into the model, generate predicted labels, and their consistency is measured through an assessment of entropy. The presence of low entropy in a perturbation signifies a triggering input, whereas high entropy suggests a clean input. STRIP adeptly exploits the dominant hijacking effect of triggers, effectively transforming it into a vulnerability for online detection. In practical terms, as an input is introduced into a backdoored model, the generation of multiple copies is facilitated by overlaying it with clean samples, and the ensuing perturbations undergo scrutiny for their consistency. Predictions characterized by low entropy serve as an indicative marker for a trigger-carrying sample, allowing for a clear differentiation from clean inputs.

B.6. SentiNet

SentiNet [12] is a data-level detection technology encompassing adversarial object localization, the proposal of classes through segmentation, and the generation of masks

using GradCAM. Its primary objective of identifying trigger inputs capable of compromising neural network predictions, all without relying on a priori knowledge of the attack vector. The methodology strategically leverages model interpretability and object detection techniques to unveil contiguous regions within input images that wield significant influence over classification outcomes. These identified regions are postulated to possess a heightened probability of harboring triggers that exert an impact on the classification process. Once pinpointed, these influential regions are systematically excised and transposed onto alternative images endowed with ground-truth labels. The efficacy of this process is contingent upon the attainment of sufficiently elevated misclassification rates and confidence levels for the transposed images, thereby designating the excised patch as an adversarial entity housing a concealed backdoor trigger. Specifically, SentiNet overlays the continuously influential regions of the test image onto a set of clean test images. These covered images are then fed into the network, and the success rate of deceiving the model, denoted as Foolde, is calculated. Simultaneously, low saliency inert patterns replace the content of the overlapped regions (e.g., Gaussian noise) to compute the average confidence value of inert patterns, denoted as Average confidence. The combination of these two metrics is used to determine whether a sample carries a trigger.

Appendix C. Meta-Review

The following meta-review was prepared by the program committee for the 2024 IEEE Symposium on Security and Privacy (S&P) as part of the review process as detailed in the call for papers.

C.1. Summary

This paper studies the feasibility of inserting a backdoor that is robust to natural variations, yet remains stealthy against existing fuzzy-triggers-based detection mechanism. Two attack scenarios, data outsourcing and model outsourcing, are investigated. The key approach towards this attack is to leverage heuristic design to tailor the objective function in the optimization process. This attack is then empirically evaluated over three datasets and the corresponding models to demonstrate the effectiveness of the attack.

C.2. Scientific Contributions

- Provides a Valuable Step Forward in an Established Field.

C.3. Reasons for Acceptance

- 1) The core scientific contribution of this work is observing how modern defenses exploit fuzzy triggers for backdoor detection. With this observation, adversaries can employ an adversarial-training-like recipe to reduce the correlation between fuzzy and true triggers.
- 2) The authors propose a simple yet effective way, i.e., backdoor exclusivity lifting, to improve the existing attack's robustness on SOTA defenses. The method aims to reduce the backdoored behavior with fuzzy triggers while maintaining the backdoor effectiveness with the original triggers. This provides a more stealthy backdoored model. Evaluations show that the proposed method indeed provides more robust backdoored models.