

Adequacy of the Gradient-Descent Method for Classifier Evasion Attacks

Yi Han, Benjamin I. P. Rubinstein

School of Computing and Information Systems, University of Melbourne
 {yi.han, benjamin.rubinstein}@unimelb.edu.au

Abstract

Despite the wide use of machine learning in adversarial settings including computer security, recent studies have demonstrated vulnerabilities to evasion attacks—carefully crafted adversarial samples that closely resemble legitimate instances, but cause misclassification. In this paper, (1) we analyse the effectiveness of the gradient-descent method—the leading approach for generating adversarial samples—against non-linear support vector machines, and conclude that carefully reduced kernel smoothness can significantly increase robustness to the attack; (2) we propose a quantity similar to margin that can efficiently predict potential susceptibility to gradient-descent attack, before the attack is launched; and (3) we design a new adversarial sample construction algorithm based on optimising the multiplicative ratio of class decision functions. Our results demonstrate that the new method not only increases the attack’s success rate, but also achieves success with less perturbation.

1 Introduction

Recent years have witnessed several demonstrations of machine learning vulnerabilities in adversarial settings [Dalvi *et al.*, 2004; Lowd and Meek, 2005; Barreno *et al.*, 2006; Rubinstein *et al.*, 2009; Brückner and Scheffer, 2011; Biggio *et al.*, 2012; Goodfellow *et al.*, 2014; Alfeld *et al.*, 2016; Li *et al.*, 2016]. Due to its approximation of best-response and its effective simplicity, gradient descent [Biggio *et al.*, 2013] has emerged as a leading approach to evasion attacks.

We refer to the carefully crafted inputs that resemble legitimate instances but cause misclassification, as *adversarial samples*, and the malicious behaviours that generate them as *evasion attacks* [Russu *et al.*, 2016]. Figure 1 illustrates the attack’s effect in the previously-explored vision domain [Szegedy *et al.*, 2013; Goodfellow *et al.*, 2014; Papernot *et al.*, 2016c]: Figures 1a and 1b present original images from [Samaria and Harter, 1994] for “Adam” and “Lucas”, who are correctly identified by a face recogniser. However, after indiscernible changes are applied to Figure 1a the model mistakenly identifies Figure 1c as “Lucas”.

Can these attacks be thwarted, are there effective attack alternatives? This paper addresses these questions, with a case study on the support vector machine with radial basis function (RBF) kernel. Our main contributions include:

- An analysis of kernel precision parameter’s impact on the success rate of evasion attacks, concluding that larger precision (less smooth kernels) achieves robustness to gradient-descent attack;

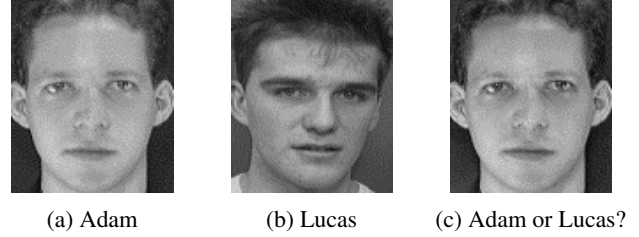


Figure 1: An example evasion attack against a learning model: Image (c) is misclassified as Lucas.

- An novel geometric classifier parameter related to margin that strongly correlates with model vulnerability, providing an avenue to predict (unseen) attack vulnerability; and
- A new approach for generating adversarial samples in multiclass scenarios, with results demonstrating significantly higher effectiveness in manipulating test data and fooling the target model.

The remainder of this paper is organised as follows: Section 2 overviews previous work on evasion attacks; Section 3 presents our research problem; we present a detailed example of how gradient-descent can fail in Section 4; Section 5 presents the gradient-quotient approach for constructing adversarial samples; experimental results are presented in Sections 6 and 7; and Section 8 concludes the paper.

2 Related Work

Barreno *et al.* [2006] categorise how an adversary can tamper with a classifier based on whether they have (partial) control over the training data: in causative attacks, the adversary can modify the training data to manipulate the learned model; in exploratory attacks, the attacker does not poison training, but carefully alters target test instances to flip classifications. See also [Barreno *et al.*, 2010; Huang *et al.*, 2011]. This paper focuses on the targeted exploratory case, also known as evasion attacks [Biggio *et al.*, 2013].

Generalising results on efficient evasion of linear classifiers via reverse engineering [Lowd and Meek, 2005], Nelson *et al.* [2012] consider families of convex-inducing classifiers, and propose query algorithms that require polynomially-many queries and achieve near-optimal modification cost.

Szegedy *et al.* [2013] demonstrate changes imperceptible to humans that cause DNNs to misclassify images. Additionally, they offer a linear explanation of adversarial samples and design a “fast gradient sign method” for generating such samples [Goodfellow *et al.*, 2014]. In a similar vein, Nguyen *et al.* [2015] propose an approach for producing

DNN-adversarial samples unrecognisable as such to humans.

Papernot *et al.* published a series of further works in this area: (1) introducing an algorithm that searches for minimal regions of inputs to perturb [Papernot *et al.*, 2016c]; (2) demonstrating effectiveness of attacking target models via surrogates—with over 80% of adversarial samples launched fooling the victim in one instance [Papernot *et al.*, 2016b]; (3) improved approaches for fitting surrogates, with further investigation of intra- and cross-technique transferability between DNNs, logistic regression, SVMs, decision trees and k -nearest neighbours [Papernot *et al.*, 2016a].

Moosavi-Dezfooli *et al.* [2016b] propose algorithm DEEP-FOOL for generating adversarial samples against DNNs, which leads samples along trajectories orthogonal to the decision boundary. A similar approach against linear SVM is proposed in [Papernot *et al.*, 2016a]. Based on DEEPFOOL, Moosavi-Dezfooli *et al.* [2016a] design a method for computing “universal perturbations” that fool multiple DNNs.

Most relevant to this paper is the work by Russu *et al.* [2016], which analyses the robustness of SVMs against evasion attacks, including the selection of the regularisation term, kernel function, classification costs and kernel parameters. Our work delivers a much more detailed analysis of exactly how the kernel parameters impact vulnerability of RBF SVM, and explanations of why.

3 Preliminaries & Problem Statement

This section recalls evasion attacks, the gradient-descent method, the RBF SVM, and summarises the research problem addressed by this paper.

Evasion Attacks. For target classifier $f : \mathbb{R}^d \rightarrow \{-1, 1\}$, the purpose of an *evasion attack* is to apply minimum change δ to a target input \mathbf{x} , so that the perturbed point is misclassified, i.e., $f(\mathbf{x}) \neq f(\mathbf{x} + \delta)$. The magnitude of adversarial perturbation δ is commonly quantified in terms of L_1 distance. Formally, evasion attacks are framed as optimisation:

$$\arg \min_{\delta \in \mathbb{R}^d} \|\delta\|_1 \quad \text{s.t.} \quad f(\mathbf{x}) \neq f(\mathbf{x} + \delta) .$$

Note that we permit attackers that can modify all features of the input, arbitrarily, but that aim to minimise the magnitude of changes. Both binary and multiclass scenarios fall into the evasion problem as described; we consider both learning tasks in this paper. In multiclass settings, attacks intending to cause specific misclassification of the test sample are known as *mimicry attacks*.

Gradient-Descent Method. The *gradient descent method*¹ has been widely used for generating adversarial samples for evasion attacks [Biggio *et al.*, 2013; Goodfellow *et al.*, 2014; Moosavi-Dezfooli *et al.*, 2016b; Papernot *et al.*, 2016c], when f outputs confidence scores in \mathbb{R} and classifications are obtained by thresholding at $\tau = 0$. The approach applies gradient descent to f directly, initialised at the target instance. Formally given target instance $\mathbf{x}_0 \in \mathbb{R}^d$ evaluating $f(\mathbf{x}_0) > \tau$,

$$\mathbf{x}_{t+1} = \mathbf{x}_t - \varepsilon_t \cdot \nabla_{\mathbf{x}} f(\mathbf{x}_t) ,$$

¹Not to be confused with gradient descent for local optimisation.

where ε_t follows an appropriately-selected step size schedule, and the iteration is terminated when $f(\mathbf{x}_t) < \tau$.

The Support Vector Machine. Recall the dual program of the soft-margin SVM classifier learner, with hinge-loss

$$\arg \max_{\alpha \in \mathbb{R}^n} \mathbf{1}'\alpha - \frac{1}{2}\alpha'\mathbf{G}\alpha \quad \text{s.t.} \quad \alpha'y = 0, \quad \mathbf{0} \preceq \alpha \preceq C\mathbf{1} \quad (1)$$

where $\{(\mathbf{x}_i, y_i), i = 1, \dots, n\}$ is the training data with $\mathbf{x}_i \in \mathbb{R}^n$ and $y_i \in \{-1, 1\}^n$, α are Lagrange multipliers, $\mathbf{0}$, $\mathbf{1}$ the all zeros, ones vectors, $C > 0$ the regularisation penalty parameter on misclassified samples, and \mathbf{G} the $n \times n$ Gram matrix with entries $G_{ij} = y_i y_j k(\mathbf{x}_i, \mathbf{x}_j)$. The RBF kernel $k(\mathbf{x}_i, \mathbf{x}_j) = \exp(-\gamma \|\mathbf{x}_i - \mathbf{x}_j\|_2^2)$ has precision parameter $\gamma > 0$ that controls kernel width $\sqrt{2/\gamma}$. By the Representer Theorem, the learned classifier

$$f(\mathbf{x}) = \sum_{i=1}^n \alpha_i y_i k(\mathbf{x}_i, \mathbf{x}) + b . \quad (2)$$

Adequacy & Improvements to Gradient-Descent Method.

While the gradient-descent method has been effective against a number of machine learning models, e.g., DNNs, linear SVMs, logistic regression [Biggio *et al.*, 2013; Goodfellow *et al.*, 2014; Moosavi-Dezfooli *et al.*, 2016b; Nguyen *et al.*, 2015; Papernot *et al.*, 2016b], there is no general guarantee that gradient descent converges to a global minimum of $f(\cdot)$ or even converges to local optima quickly—relevant to computational complexity (a measure of hardness) of evasion. Under linear models—a major focus of past work—gradient descent quickly finds global optima. While DNNs have been argued to exhibit local linearity. The existing body of evidence is insufficient to properly assess the effectiveness of the attack approach. As we argue in the next section, the approach is in fact *unlikely to be successful against certain SVMs with RBF kernels, when kernel parameter γ is chosen appropriately*.

Problem 1 *What limitations of the gradient-descent method are to be expected when applied to evasion attacks?*

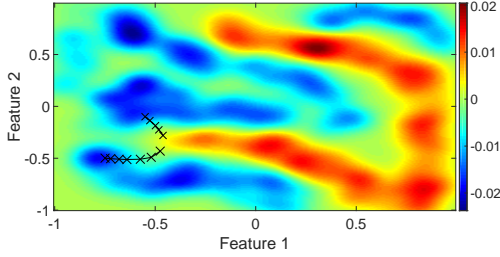
Problem 2 *Are there simple defences to the gradient-descent method for popular learners?*

Problem 3 *Are there more effective alternative approaches to generating adversarial samples?*

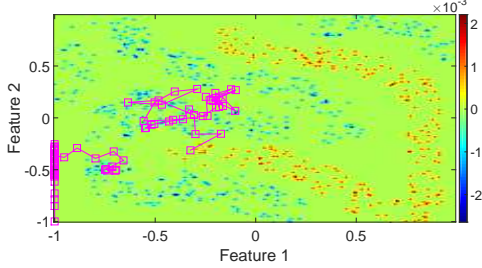
We address each of these problems in this paper, with special focus on the RBF SVM as a case study and important example of where the most popular approach to evasion attack generation can predictably fail, and be improved upon.

4 Gradient-Descent Method Failure Modes

In this section, we explore how the gradient-descent method can fail against RBF SVMs with small kernel widths.



(a) $\gamma = 10^2$ model: two black curves display attack paths under gradient descent, of two target points reaching the decision boundary.



(b) $\gamma = 10^4$ model: two magenta curves display attack paths under gradient descent, of the two target points now move away from the boundary or take significantly more steps.

Figure 2: Heatmaps visualising decision boundaries of RBF SVM’s trained on a sample dataset.

Illustrative Example. To demonstrate our key observation, we trained two RBF SVMs on a toy two-class dataset comprising two features [Chang and Lin, 2011; Chang and Lin, 2016], using two distinct values for γ : 10^2 and 10^4 . Figure 2 displays the heatmaps of the two models’ decision functions. As can be seen, for the larger γ case, additional regions result with flat, approximately-zero, decision values. Since the gradients in these regions are vanishingly small, it is significantly more likely that an iterate in the gradient-descent method’s attack trajectory will become trapped, or even move towards a direction *away from the decision boundary altogether*. Notably, both models achieve test accuracies of 100%.

In Figure 2(a), the two black curves marked with crosses demonstrate how two initial target points $(-0.55, -0.1)$ and $(-0.75, -0.5)$, move towards the decision boundary following the gradient-descent method. However, the two magenta curves marked with squares in Figure 2(b) demonstrate how the same two points either move away from the boundary or take significantly more steps to reach it, following the same algorithm but under a different model with a much larger γ .

This example illustrates that although the gradient-descent method makes the test sample less similar to the original class, it does not necessarily become similar to the other class.

Discussion. We employ Figure 3 to further explain possible failure modes of the gradient-descent method: points may get stuck or even move in the wrong direction. In this given 2D case, x_1 belongs to Class 1, x_2 to Class 2. At instance x , the k^{th} component of the gradient is $\nabla^k f(x) = \sum_{i=1}^2 2\gamma\alpha_i y_i (x_i^k - x^k) \cdot \exp(-\gamma \|x - x_i\|_2^2)$. Clearly, the

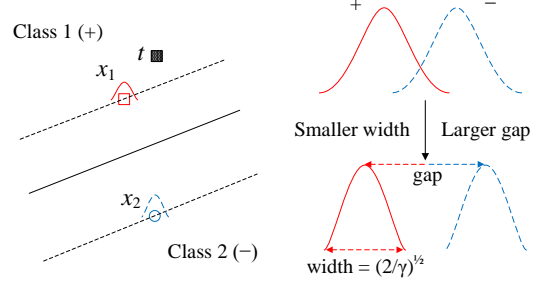


Figure 3: Gradient-descent method failure modes.

sign of ∇^k can be flipped by various choices of γ . Suppose $x_1^1, x_2^1 > x^1$, then solving for $\nabla^1 = 0$, we obtain the *point at which this phase transition occurs* as:

$$\gamma = \frac{\log \alpha_1(x_1^1 - x^1) - \log \alpha_2(x_2^1 - x^1)}{\|x - x_1\|_2^2 - \|x - x_2\|_2^2}.$$

The failure modes hold true in multiclass scenarios. For test sample x the classifier evaluates an $f_i(x)$ per class i and selects the maximiser (a one-vs-all reduction). Suppose that $f_1(x)$ and $f_2(x)$ are the highest class scores. If γ is chosen appropriately as above, then gradient descent reduces both $f_1(x)$ and $f_2(x)$ without ever reranking the two classes.

Figure 3 presents a geometric explanation, where distance between support vectors of opposite classes exceeding kernel width results in gradient-descent method iterates becoming trapped in the “gap” between. This section partially addresses Problem 1 through the discussed limitations, while setting γ can provide a level of defence per Problem 2.

5 The Gradient-Quotient Method

The previous section motivates Problem 3’s search for effective alternatives to decreasing current class i $f_i(x)$ while increasing desired class j $f_j(x)$. Rather than moving in the direction $-\nabla f_i(x)$ as the gradient-descent method does (noting this is in the subgradient for the one-vs-all reduction), we propose following the gradient of the quotient $-f_i(x)/f_j(x)$:

$$x_{t+1} = x_t - \varepsilon_t \cdot \nabla(f_i(x)/f_j(x)).$$

Remark 1 Employing $f_i(x) - f_j(x)$ in place of $f_i(x)/f_j(x)$ does not achieve the desired result by the same flaws suffered by the gradient-descent method: $f_i(x)$, $f_j(x)$ and $f_i(x) - f_j(x)$ are decreased simultaneously, while $f_i(x)$ can remain larger than $f_j(x)$, with no misclassification occurring.

Note that while in the above, i is taken as the current (maximising) class index, taking j as the next highest-scoring class corresponds to evasion attacks while taking j as any fixed target class corresponds to a mimicry attack. The results of Section 7 establish that this method can be more effective for manipulating test data in multiclass settings. However, it is not appropriate to binary-class cases as $-f_1(x)/f_2(x) = 1$.

Step Size. The step size ε_t is important to select carefully: too small and convergence slows; too large and the attack incurs excessive L_1 change, potentially exposing the attack.

Algorithm 1: Gradient-quotient step size.

Input : Iterate x_t ; Current quotient gradient $\nabla \in \mathbb{R}^d$;
Parameter $\eta > 0$

Output: Step size ε_t

- 1 Select $i \in \arg \max_{j \in [d]} |\nabla^j|$.
 - 2 Select $\varepsilon_t > 0$ such that $\varepsilon_t \cdot |\nabla^i| \in \sqrt{t}[5\eta, 10\eta]$.
-

In our experiments, we limit the largest change made to a single feature per iteration, and determine the step size accordingly as described in Algorithm 1. Here η is a domain-specific value corresponding to a unit change in a feature, *e.g.*, for a grayscale image $\eta = 1$ corresponds to a unit change intensity level. The select rule’s $[5\eta, 10\eta]$ is motivated by round-off practicalities in steps: if the largest gradient component were smaller than 5η , it is likely that most other components would be 0, making convergence extremely slow. Since $[5\eta, 10\eta]$ is a relatively conservative start, we increase it gradually; as explained next, the maximum step number in our experiments is 30. This increasing step size corresponds to a variant of guess-then-double.

6 Experiments: Gradient-Descent Method

Section 4 demonstrates that RBF SVM is less vulnerable to evasion attacks when γ is set appropriately. In this section, we present a more detailed analysis of the impact of γ on the attack’s success rate, further addressing Problems 1 and 2.

6.1 Dataset

MNIST is a dataset of handwritten digits [LeCun *et al.*, 1998a; LeCun *et al.*, 1998b]. We choose this dataset as it facilitates comparison of our results with past work. MNIST contains a training set of 6×10^4 samples (only the first 5×10^4 are used in our experiments), and a test set of 10^4 samples. Following the approach of [Papernot *et al.*, 2016a], we divide the training set into 5 subsets of 10^4 samples, $D_1 \sim D_5$. Each subset is used to train models separately. Specifically, in the experiments that study binary-class settings, only the data in D_1 (or the test dataset) that belong to the two classes are used for training (or testing respectively).

6.2 Impact of γ on Vulnerability (Binary Class)

We begin with the binary scenario and investigate how γ impacts the success rate of causing SVMs to misclassify three pairs of digits—1 & 2, 3 & 4, 5 & 7. Note that all models discussed in this subsection are trained on D_1 . An attack is considered successful if the perturbed test sample is misclassified within 30 steps. The reason why we choose 30 is that although larger values will increase the attack’s success rate, the changes made to the original samples are so obvious they would be easily detected by manual audit. Tables 1a–1c illustrate a phase transition in each of the three cases: a small decrease of γ causes a significant jump in success rate.²

²Testing for effect of C revealed much less impact on success rate, especially when $\gamma = 0.5$ —in these cases, a smaller $C = 10$ is chosen.

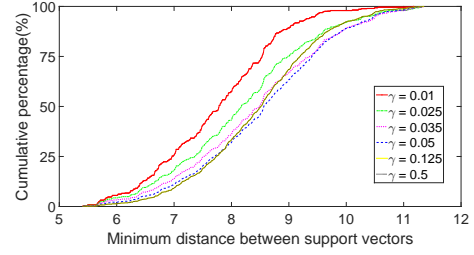


Figure 4: Minimum distance between each support vector of class “3” and all support vectors of class “4”.

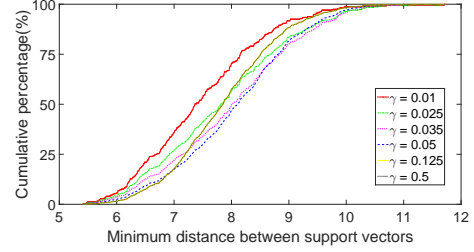


Figure 5: Minimum distance between each support vector of class “4” and all support vectors of class “3”.

Inter-Class-SV Distance. Since γ controls how quickly the RBF kernel vanishes, we are motivated to compare minimum (Euclidean) distance between each support vector of one class (sv_{1i}) and all support vectors of the opposite class (sv_{2j}), *i.e.*, $\text{MinDist}(sv_{1i}) = \arg \min_j \text{Distance}(sv_{1i}, sv_{2j})$. Our intuition is that a larger γ suggests (1) a quicker drop of values for both the kernel function and the gradient; (2) a wider gap between the two classes. Both observations contribute to the lower success rate of the evasion attack.

Figures 4 and 5 present the minimum distance between support vectors of classes “3” and “4” (due to space limitations, we omit the similar two sets of results). Observe that when γ first decreases from 0.5, the support vectors of the opposite class move further away—here the corresponding model is still less vulnerable to evasion attack. As γ continues to decrease the trend reverses, *i.e.*, the support vectors of opposite class move closer to each other. A smaller γ already means the RBF kernel vanishes more slowly, and the closer distance between the two classes makes it even easier for a test sample to cross the decision boundary. Consequently, the corresponding model becomes much more vulnerable.

This prompts the question: Given a model with a γ , is there a way to determine whether the model is robust? The results in Tables 1a–1c witness a strong correlation between success rate and the percentage of “ $2/\sqrt{\gamma} \geq \text{minimum distance}$ ”—the lower the percentage the less vulnerable the model.

Margin Explanation. We have observed a positive correlation between margin per support vector and this minimum distance. These findings suggest that separated inter-class support vectors leads to more secure models, lending experimental support to the geometric argument (Section 4).

Table 1: Success rate and average L_1 change for gradient-descent method evasion attack (binary class).

(a) RBF SVM: digits 1 and 2.

γ	0.01	0.02	0.025	0.05	0.1	0.11	0.125	0.5
C	5×10^4	5×10^4	5×10^4	5×10^4	5×10^4	5×10^4	5×10^4	10
Accuracy(%)	99.4	99.5	99.6	99.5	99.8	99.7	99.5	98.6
$1 \rightarrow 2$	Succ rate (%)	100	100	100	100	90.1	68.9	36.3
	$P(2/\sqrt{\gamma} \geq MinDist) (%)$	100	100	100	100	68.4	55.0	35.0
$2 \rightarrow 1$	Succ rate (%)	94.1	68.9	54.8	17.0	11.3	13.3	15.2
	$P(2/\sqrt{\gamma} \geq MinDist) (%)$	100	100	100	59.3	7.5	4.8	2.8

(b) RBF SVM: digits 3 and 4.

γ	0.01	0.025	0.035	0.05	0.125	0.5
C	10^4	10^4	10^4	10^4	10^4	10
Accuracy(%)	99.5	99.7	99.6	99.5	99.5	99.8
$3 \rightarrow 4$	Succ rate (%)	100	94.5	76.0	53.4	14.8
	$P(2/\sqrt{\gamma} \geq MinDist) (%)$	100	100	96.7	61.7	0.29
$4 \rightarrow 3$	Succ rate (%)	100	100	98.1	82.5	11.8
	$P(2/\sqrt{\gamma} \geq MinDist) (%)$	100	100	99.2	79.7	0.4

(c) RBF SVM: digits 5 and 7.

γ	0.01	0.025	0.035	0.05	0.1	0.5
C	10^4	10^4	10^4	10^4	10^4	10
Accuracy(%)	99.3	99.5	99.6	99.6	99.1	99.7
$5 \rightarrow 7$	Succ rate (%)	100	97.0	87.4	71.1	41.8
	$P(2/\sqrt{\gamma} \geq MinDist) (%)$	100	100	98.7	75.6	0.2
$7 \rightarrow 5$	Succ rate (%)	100	100	99.8	91.1	15.5
	$P(2/\sqrt{\gamma} \geq MinDist) (%)$	100	100	100	87.2	0.2

(d) Linear SVM.

	$C = 1000$			$C = 5000$		
	Succ rate (%)	Ave L_1 change	Accuracy (%)	Succ rate (%)	Ave L_1 change	Accuracy (%)
$1 \rightarrow 2$	100	5812	99.3	100	4685	99.2
$2 \rightarrow 1$	100	9575		100	8883	
$3 \rightarrow 4$	100	10085	99.7	100	9520	99.6
$4 \rightarrow 3$	100	8372		100	6593	
$5 \rightarrow 7$	100	7748	99.0	100	7169	99.0
$7 \rightarrow 5$	100	7408		100	6024	

Linear SVM. The experiments were performed for linear SVMs, with results serving as baseline. Table 1d demonstrates that success rates under linear models are 100%, as expected. However a larger C requires smaller changes to the target sample, as larger C leads to smaller margin.

6.3 Impact of γ on Vulnerability (Multiclass)

This section further investigates the impact of γ on success rate of evasion attacks, in multiclass scenarios. Two RBF SVMs with γ as 0.05 and 0.5, are trained on both D_1 and D_2 , respectively. For comparison, four linear SVMs are also trained on the two datasets with different values of C . An attack is considered successful if the perturbed test sample is misclassified within 30 steps. As can be seen from Table 2: (1) for RBF SVMs, the success rates under the models with larger γ are much lower; (2) for linear SVMs the success rates are always 100%, but the average L_1 change is smaller as C increases—observations consistent with previous results.

Table 2: Success rate and average L_1 change of gradient-descent method evasion attack, in multiclass scenarios.^a

		Accuracy (%)	Succ rate (%)	Ave L_1 change
RBF ($\gamma = 0.05, C = 10^3$)	Model 1	87.2	91.8	10037 ^b
	Model 2	87.7	92.8	10323 ^b
RBF ($\gamma = 0.5, C = 10$)	Model 1	94.8	24.4	4509 ^b
	Model 2	94.8	23.7	4637 ^b
Linear ($C = 10^3$)	Model 1	89.0	100	7259
	Model 2	89.2	100	6837
Linear ($C = 2 \times 10^4$)	Model 1	91.4	100	4766
	Model 2	91.7	100	4604

^a Since it takes more than an order of magnitude longer to run experiments using RBF SVM than linear kernel, each result regarding RBF SVM is based on 1000 test samples, while each linear SVM result is based on 5000 test samples.

^b Only the successful cases are counted.

7 Experiments: Gradient-Quotient Method

In this section we present experimental results establishing the effectiveness of our proposed method for generating adversarial samples.

7.1 Attacking the Model Directly

Recall that based on our new approach, a test sample \mathbf{x} is updated as $\mathbf{x}_{t+1} = \mathbf{x}_t - \varepsilon_t \cdot \nabla(f_1(\mathbf{x})/f_2(\mathbf{x}))$, where $f_1(\mathbf{x})$ and $f_2(\mathbf{x})$ are the scores for the top two scoring classes for \mathbf{x} . In order to test whether this method is more effective than the popular gradient-descent method, we run similar experiments to Section 6.3, where one RBF SVM ($\gamma = 0.5, C = 10$) and one linear SVM ($C = 1000$) are trained on D_1, \dots, D_5 , respectively. Comparing the results in Table 2 and Table 3, we observe that: (1) for the RBF SVMs with $\gamma = 0.5$, the success rates increase from around 24% to a resounding 100%. Moreover we have tested a wide range of values for γ from 0.01 through 10, with *resulting success rates always 100% under our new approach*; (2) the required L_1 perturbation also decreases. These two observations establish that the new approach is more effective in crafting adversarial samples.

Table 3: Success rate and average L_1 change of the evasion attack (the gradient quotient method, multiclass scenarios).^a

		Accuracy (%)	Succ rate (%)	Ave L_1 change
RBF ($\gamma = 0.5$, $C = 10$)	Model 1	94.8	100	4532
	Model 2	94.8	100	4571
	Model 3	95.0	100	4429
	Model 4	95.2	100	4475
	Model 5	95.0	100	4610
Linear ($C = 10^3$)	Model 1	89.0	100	4927
	Model 2	89.2	100	5251
	Model 3	89.1	100	5317
	Model 4	89.2	100	5311
	Model 5	88.9	100	5066

^a Each result regarding RBF SVM is based on 800 test samples, while each result on linear SVM is based on 5000 test samples.

7.2 Attacking via Surrogate

Up until now, we have implicitly assumed that the attacker possesses complete knowledge of the target classifier, which may be unrealistic in practice. Hence, we next examine attacks carried out via a surrogate. For example, in order to mislead a RBF SVM, the attacker first trains their own RBF SVM on a similar dataset, builds the attack path of how a test sample should be modified, then applies it to the target SVM.

Previously, modification is terminated upon misclassification or once 30 steps are taken. However, since there is no guarantee that the surrogate and target classifiers misclassify the test sample simultaneously, all test samples are modified 30 times by the surrogate in this experiment; an attack is considered as successful if the target classifier also misclassifies the adversarial sample within 30 steps. We modify the method as

$$\mathbf{x}_{t+1} = \begin{cases} \mathbf{x}_t - \varepsilon_t \cdot \nabla(f_1(\mathbf{x}_t)/f_2(\mathbf{x}_t)) & \text{prior to surrogate misclassification} \\ \mathbf{x}_t + \varepsilon_t \cdot \nabla(f_1(\mathbf{x}_t)/f_2(\mathbf{x}_t)) & \text{otherwise} \end{cases}$$

In other words, before the test sample is misclassified by the surrogate, it travels “downhill”, but after crossing the decision boundary it travels “uphill”. Otherwise the test case continues oscillating back and forth around the boundary.

We reuse the RBF SVMs trained in the last section, each of which serving as both surrogate (S_i) and target (T_i) classifiers. As can be seen from Table 4, the success rates are all over 65%. Specifically, those values inside the bracket are the success rates when the target classifier misclassifies before the surrogate, while the values outside are the overall success rates. For comparison, the same experiments have been performed for linear SVMs, producing similar success rates (at around 60%), notably higher than previous findings (around 40%) reported by Papernot *et al.* [2016a].

Table 4: Success rate of evasion attacks via surrogate (RBF SVM).^a

	T_1	T_2	T_3	T_4	T_5
S_1	100	66.1 (9.2)	69.8 (9.5)	68.3 (9.8)	66.4 (7.1)
S_2	68.0 (8.2)	100	67.2 (8.4)	72.4 (10.4)	67.9 (7.4)
S_3	65.0 (8.4)	66.1 (9.4)	100	67.3 (11.1)	65.9 (8.5)
S_4	65.3 (10.0)	67.2 (10.8)	67.0 (10.6)	100	65.3 (8.8)
S_5	67.0 (9.2)	67.8 (8.9)	69.4 (9.0)	69.4 (9.1)	100

^a Each result is based on 800 test samples.

7.3 Mimicry Attacks

We tested the gradient-quotient method for mimicry attacks. Our results show that in most cases this approach can successfully make the original digit misclassified as any of the other nine digits. Due to space limitations, those results are omitted.

8 Conclusions and Future Work

Recent studies have shown that it is relatively easy to fool machine learning models via adversarial samples. In this paper, we demonstrate that the gradient-descent method—the leading approach to generate adversarial samples—has limitations against RBF SVMs, when the precision parameter γ controlling kernel smoothness is chosen properly. We find predictable phase transitions of attack success occur at thresholds that are functions of geometric margin-like quantities measuring inter-class support vector distances. Our characterisation can be used to make RBF SVM more robust against common evasion and mimicry attacks.

We propose a new method for manipulating target samples into adversarial instances, with experimental results showing that this new method not only increases attack success rate, but decreases the required changes made to input points.

For future work, (1) regarding the gradient-descent method, we intend to replicate and expand findings for γ and smoothness in general, in other settings and for other classifiers. (2) We will explore suitability of our new generation approach when the target is not an SVM, with direct attacks or SVM surrogates. (3) Further investigation into light-weight yet efficient countermeasures also serves as an important direction for future work.

References

- [Alfeld *et al.*, 2016] Scott Alfeld, Xiaojin Zhu, and Paul Barford. Data poisoning attacks against autoregressive models. In *AAAI*, pages 1452–1458, 2016.
- [Barreno *et al.*, 2006] Marco Barreno, Blaine Nelson, Russell Sears, Anthony D. Joseph, and J. D. Tygar. Can machine learning be secure? In *AsiaCCS*, pages 16–25, 2006.
- [Barreno *et al.*, 2010] Marco Barreno, Blaine Nelson, Anthony D. Joseph, and J. D. Tygar. The security of machine learning. *Machine Learning*, 81(2):121–148, 2010.
- [Biggio *et al.*, 2012] Battista Biggio, Blaine Nelson, and Pavel Laskov. Poisoning attacks against support vector machines. In *ICML*, pages 1807–1814, 2012.
- [Biggio *et al.*, 2013] Battista Biggio, Igino Corona, Davide Maiorca, Blaine Nelson, Nedim Šrđić, Pavel Laskov, Giorgio Giacinto, and Fabio Roli. Evasion attacks against machine learning at test time. In *ECML PKDD*, pages 387–402, 2013.
- [Brückner and Scheffer, 2011] Michael Brückner and Tobias Scheffer. Stackelberg games for adversarial prediction problems. In *KDD*, pages 547–555, 2011.
- [Chang and Lin, 2011] Chih-Chung Chang and Chih-Jen Lin. LIBSVM: A library for support vector machines. *ACM Transactions on Intelligent Systems and Technology*, 2(3):1–27, 2011.
- [Chang and Lin, 2016] Chih-Chung Chang and Chih-Jen Lin. LIBSVM data: Classification (binary class). <https://www.csie.ntu.edu.tw/~cjlin/libsvmtools/datasets/binary.html#fourclass>, 2016.
- [Dalvi *et al.*, 2004] Nilesh Dalvi, Pedro Domingos, Mausam, Sumitanghai, and Deepak Verma. Adversarial classification. In *KDD*, pages 99–108, 2004.
- [Goodfellow *et al.*, 2014] Ian J. Goodfellow, Jonathon Shlens, and Christian Szegedy. Explaining and harnessing adversarial examples. *eprint arXiv:1412.6572*, 2014.
- [Huang *et al.*, 2011] Ling Huang, Anthony D. Joseph, Blaine Nelson, Benjamin I. P. Rubinstein, and J. D. Tygar. Adversarial machine learning. In *ACM AISec Workshop*, pages 43–57, 2011.
- [LeCun *et al.*, 1998a] Yann LeCun, Leon Bottou, Yoshua Bengio, and Patrick Haffner. Gradient-based learning applied to document recognition. *Proc. IEEE*, 86(11):2278–2324, 1998.
- [LeCun *et al.*, 1998b] Yann LeCun, Corinna Cortes, and Christopher J.C. Burges. The MNIST database of handwritten digits. <http://yann.lecun.com/exdb/mnist/>, 1998.
- [Li *et al.*, 2016] Bo Li, Yining Wang, Aarti Singh, and Yevgeniy Vorobeychik. Data poisoning attacks on factorization-based collaborative filtering. In *NIPS*, pages 1885–1893, 2016.
- [Lowd and Meek, 2005] Daniel Lowd and Christopher Meek. Adversarial learning. In *KDD*, pages 641–647, 2005.
- [Moosavi-Dezfooli *et al.*, 2016a] Seyed-Mohsen Moosavi-Dezfooli, Alhussein Fawzi, Omar Fawzi, and Pascal Frossard. Universal adversarial perturbations. *eprint arXiv:1610.08401*, 2016.
- [Moosavi-Dezfooli *et al.*, 2016b] Seyed-Mohsen Moosavi-Dezfooli, Alhussein Fawzi, and Pascal Frossard. DeepFool: A simple and accurate method to fool deep neural networks. In *CVPR*, pages 2574–2582, 2016.
- [Nelson *et al.*, 2012] Blaine Nelson, Benjamin I. P. Rubinstein, Ling Huang, Anthony D. Joseph, Steven J. Lee, Satish Rao, and J. D. Tygar. Query strategies for evading convex-inducing classifiers. *J. Machine Learning Research*, 13(1):1293–1332, 2012.
- [Nguyen *et al.*, 2015] Anh Nguyen, Jason Yosinski, and Jeff Clune. Deep neural networks are easily fooled: High confidence predictions for unrecognizable images. In *CVPR*, pages 427–436, 2015.
- [Papernot *et al.*, 2016a] Nicolas Papernot, Patrick McDaniel, and Ian Goodfellow. Transferability in machine learning: from phenomena to black-box attacks using adversarial samples. *eprint arXiv:1605.07277*, 2016.
- [Papernot *et al.*, 2016b] Nicolas Papernot, Patrick McDaniel, Ian Goodfellow, Somesh Jha, Z. Berkay Celik, and Ananthram Swami. Practical black-box attacks against deep learning systems using adversarial examples. *eprint arXiv:1602.02697*, 2016.
- [Papernot *et al.*, 2016c] Nicolas Papernot, Patrick McDaniel, Somesh Jha, Matt Fredrikson, Z. Berkay Celik, and Ananthram Swami. The limitations of deep learning in adversarial settings. In *EuroS&P*, pages 372–387, 2016.
- [Rubinstein *et al.*, 2009] Benjamin I. P. Rubinstein, Blaine Nelson, Ling Huang, Anthony D. Joseph, Shing-hon Lau, Satish Rao, Nina Taft, and J. D. Tygar. ANTIDOTE: understanding and defending against poisoning of anomaly detectors. In *IMC*, pages 1–14, 2009.
- [Russu *et al.*, 2016] Paolo Russu, Ambra Demontis, Battista Biggio, Giorgio Fumera, and Fabio Roli. Secure kernel machines against evasion attacks. In *ACM AISec Workshop*, pages 59–69, 2016.
- [Samaria and Harter, 1994] Ferdinando Samaria and Andy Harter. Parameterisation of a stochastic model for human face identification. In *IEEE Workshop on Applications of Computer Vision*, pages 138–142, 1994.
- [Szegedy *et al.*, 2013] Christian Szegedy, Wojciech Zaremba, Ilya Sutskever, Joan Bruna, Dumitru Erhan, Ian Goodfellow, and Rob Fergus. Intriguing properties of neural networks. *eprint arXiv:1312.6199*, 2013.