Recent improvements of ASR models in the face of adversarial attacks

Raphael Olivier¹, Bhiksha Raj¹

¹Language Technologies Institute, Carnegie Mellon University, USA
rolivier@cs.cmu.edu, bhiksha@cmu.edu

Abstract

Like many other tasks involving neural networks, Speech Recognition models are vulnerable to adversarial attacks. However recent research has pointed out differences between attacks and defenses on ASR models compared to image models. Improving the robustness of ASR models requires a paradigm shift from evaluating attacks on one or a few models to a systemic approach in evaluation. We lay the ground for such research by evaluating on various architectures a representative set of adversarial attacks: targeted and untargeted, optimization and speech processing-based, white-box, black-box and targeted attacks. Our results show that the relative strengths of different attack algorithms vary considerably when changing the model architecture, and that the results of some attacks are not to be blindly trusted. They also indicate that training choices such as self-supervised pretraining may significantly impact robustness by enabling transferable perturbations. We release our source code as a package that should help future research in evaluating their attacks and defenses.

Index Terms: speech recognition, security, robustness, adversarial attacks

1. Introduction

In recent years Automatic Speech Recognition (ASR) systems have invested an considerable number of practical applications, and security is a critical component of many of them. Yet there is a dangerous lack of certainty regarding the robustness of ASR models to security threats. For instance neural Speech Recognition systems are vulnerable to adversarial attacks, one of the most emblematic shortcomings of modern Deep Learning architectures[1, 2]. These attacks lead models to make wrong predictions by crafting small, hardly perceptible perturbations of their inputs. Applied to domains like banking[3] or home security[4], where ASR systems are used, such attacks could lead to critical failures and potentially enable fraudulent transactions or theft.

Adversarial attacks against ASR models have been around for several years and their results on baselines like DeepSpeech2[5] or Speech Commands[6] are well known[7, 8]. Research on Speech Recognition has since then hit multiple milestones by adopting Transformer models, looking into various architectures and even self-supervision. Yet most works on ASR attacks still often evaluate them on the same baseline models or a very limited number of models[9, 10, 11]. Rare exceptions typically focus on specific types of attacks, like universal perturbations[12]. This leaves a number of fundamental questions largely unanswered: how do LSTMs and Transformers compare in terms of robustness? What about encoder-decoders and encoder-only models? Does self-supervised pretraining, a staple of recent ASR systems, affect adversarial vulnerabilities? Robustness for Computer Vision has seen tremendous progress in recent years, largely thanks to standardized benchmarks and baselines[13, 14, 15, 16]. At the same time Randomized Smoothing is the only strong, principled defense that has been adapted to Speech Recognition[17]. Recent works[18, 19] have shown that ASR adversarial examples are different from image ones in key aspects, and must therefore be the object of specific research. In that regard, setting the foundations for a standardized, systematic evaluation of attacks on speech models is an important first step.

Our contribution throughout this paper consists in laying out some of these foundations. We start by reproducing a representative panel of attacks: targeted and untargeted, with and without labels, white-box and black-box, optimization and signal processing-based. We evaluate them on the LibriSpeech test-clean set against multiple standard models trained on the same data but varying in architecture, loss, training paradigm and size. These results both set a standard to beat in future attack and defense works, and let us draw some (cautious) conclusions on the relative robustness of ASR architectures.

We also investigate the conditions under which adversarial examples may transfer between models. We study multiple architectures - notably variations of Wav2Vec2 that were pre-trained with self-supervised objectives. Surprisingly, we show that the transferability of adversarial examples is significantly boosted for such models, even for targeted attacks - which so far were systematically non-transferable between ASR models[19]. To an extent, these results indicate that ASR models today are more vulnerable than in the past. We draw attention on the dangers of fine-tuning private models from publicly available speech embeddings.

Arguably one of the limitations for a standard evaluation of ASR attacks until this point was the lack of a practical codebase to do so. Our final contribution consists in releasing our source code¹ in the form of an simply extensible package built on the Speechbrain toolkit[20]. We hope this will help performing a thorough evaluation of adversarial attacks in the future.

2. Adversarial attacks on ASR

In this section we describe the attacks that we evaluated. We adopt the taxonomy of [18].

2.1. Untargeted attacks

2.1.1. Projected Gradient Descent

The Projected Gradient Descent (PGD) attack is an direct optimization attack. We use the untargeted PGD, which aims at producing denial of service by generating any wrong output. It optimizes the following objective with projected gradient descent for multiple steps:

\[ \arg\max_{\|\delta\|<\epsilon} L(f(x + \delta), y) \]  

¹https://github.com/RaphaelOlivier/robust_speech
where $f$ is the model, $L$ its loss function, $(x, y)$ the original input and label, and $\epsilon$ a bound on the adversarial perturbation $\delta$. PGD is a general machine learning attack and has been applied to ASR models in the past[18, 17]. We consider both the $L_2$ and $L_\infty$ for the choice of norm in Eq. 1. We control the perturbation size of the latter by fixing the Signal-Noise Ratio (SNR) of the attack as a hyperparameter. The SNR is defined with $\text{SNR}(\delta, x) = \log_{10}(20 \frac{\|\delta\|_2}{\|x\|_2})$ and measured in decibels (dB). For each input we set $\epsilon$ accordingly: $\epsilon = \|x\|_2 / 10^{\frac{\text{SNR}}{20}}$. For $L_\infty$ PGD, we directly set $\epsilon$ as a hyperparameter.

2.1.2. Genetic ASR attack

[8] propose an indirect optimization attack for ASR models. It employs a genetic algorithm where a population is maintained and renewed, using the adversarial objective as a fitness score. Such indirect attacks are useful to attack models that are only available as a black-box oracle, without gradient information; but also to fool models whose gradients are not useful due to the obfuscation effect of an incomplete defense[21].

The authors of [8] use this method as a targeted attack. However they only evaluated it on the Speech Commands dataset with 10 possible labels. To run such an attack on a large ASR model with a full English sentence as the target is considerably more challenging. To keep some amount of attack success we use the same algorithm for a simpler, untargeted objective: the loss on the original label is used as a fitness score. Perturbations are $L_\infty$-bounded by a hyperparameter $\epsilon$.

2.1.3. Kenanville attack

The DFT Kenanville attack[22] is a Signal Processing attack: it does not consider model predictions or loss to modify the audio signal. Instead, this attack removes the spectral components of the input that have the lowest power spectral density (PSD). This leaves human perception mostly unchanged, but typically affects the predictions of ASR models, which tend to exploit high-frequency components more than humans. Like $L_2$-PGD the distortion of that attack is controlled with the SNR.

2.2. Targeted attacks

2.2.1. Carlini&Wagner

The Carlini&Wagner (CW) attack[13] is a targeted, direct optimization attack and a standard for evaluating the robustness of machine learning models. The same authors apply it to the DeepSpeech2 ASR model in [7]. At its core is the optimization of $\delta$ to minimize the objective

$$c \cdot L(f(x + \delta), y_t) + \|\delta\|_2^2$$

such that $\|\delta\|_\infty < \epsilon$. Here $y_t$ is the target of the attack and $c$ a regularization parameter controlling the relative importance of the attack objective and the size of the perturbation. The objective is optimized with Adam[23]. The additional $L_\infty$ constraint $\epsilon$ is first set large, then progressively decreased.

2.2.2. Imperceptible attack

The Imperceptible attack[10] extends the CW attack by adding a second attack stage where the $\|\delta\|_2^2$ regularization is replaced with a regularization term based on a psychoacoustic model. This leads to less perceptible adversarial examples. It is also a rare example of attack proposed against a LAS-type model[24] rather than DeepSpeech. We do not report metrics for this attack (they are nearly identical to CW), but we discuss it and provide adversarial examples along with our source code.

2.3. Self-supervised attack

Recent years have seen the emergence of self-supervised pre-training for ASR models such as Wav2Vec 2.0[25, 26]. These models are pretrained on unlabeled speech data. During pre-training, given input $x$ the network computes both a quantized latent representation $q(x)$ from low-level features and a contextualized representation $c(x)$ with a Transformer. It is trained to match these two vectors with a contrastive loss.

An adversarial example for such a model would intuitively apply a small perturbation $\delta$ that makes the representation of $c(x + \delta)$ very different from $c(x)$. Even in absence of a training label, attacking self-supervised models is possible[27]. To attack Wav2Vec2 we wrote an algorithm inspired by [28], in which our loss term is simply the squared distance of the natural and adversarial representations $\|c(x + \delta) - c(x)\|_2^2$. By plugging this loss term into the $L_\infty$-PGD objective, we obtain the "untargeted" SSL attack on Speech.

2.4. Transferred attacks

[29] have shown that adversarial examples computed with optimization attacks against a model tend to be effective at fooling other models as well. This transferability effect is a major cause on concern: by attacking a source, proxy model that was trained locally or publicly available, and then transferring the perturbations to the actually targeted model, an adversary can fool even commercial models of unknown architecture.

However, transferability is rarely claimed by attacks on ASR models. In fact[18] have shown that it is not achievable with current targeted optimization attacks on the DeepSpeech2 model, even when the models differ only by their random training seed.[19] analyse this phenomenon on a Speech Command model and identify factors limiting transferability, such as current networks or vocabulary size. We extend this analysis with a wider set of architectures and by studying untargeted attacks as well. We also study the effect of self-supervised pretraining on transferability.

3. Experimental setup

3.1. Dataset

We use the LibriSpeech dataset[30]. All our models are trained on the full 960h training set, with the exception of the wav2vec2-100h model which was pretrained on the full set and fine-tuned on a 100h clean subset.

We evaluate our adversarial attacks on the clean test set. For the most computationally expensive attacks, CW, Imperceptible and Genetic, we restrict our evaluation to 100 utterances only.

3.2. Models

In order to minimize the time and the computational footprint of our experiments, we evaluate pretrained models directly provided by SpeechBrain[20]. Some models output characters (31 output neurons), others output subwords with 5000 Byte Pair Encodings (BPE). All subwords (resp. character) models share their vocabulary and tokenizer. We do not use external language models for decoding. The detailed hyperparameters of all models are available in our source code.

We use two subword Seq2Seq encoder-decoder models following the Listen, Attend and Spell (LAS) architecture[24].
One uses Transformers and the other LSTMs. Each was trained with both the CTC Loss on the encoded states and Attention+Cross-Entropy Loss. When generating attacks we use either the Cross-Entropy Loss or the CTC loss, effectively treating each network as two different models: LAS and CTC. These two models share their latent encoded space.

Finally, we use multiple variations of Wav2Vec 2.0: the base model pretrained on 960h, base models fine-tuned on 960h and 100h respectively, and the large model fine-tuned on 960h. All models were imported using the Speechbrain interface to Huggingface transformers[31].

3.3. Evaluation

3.3.1. Attack methodology

We evaluate all attacks against all models whenever applicable. For the PGD and Kenansville attacks we vary the hyperparameters controlling the amount of noise distortion; however for each attack we keep all other hyperparameters constant. This includes the number of iterations in optimization attacks, which is respectively equal to 100 (PGD), 500 (SSL), 2000 (Genetic) and 5000 (CW). These values are greater or equal to those used by their original authors. Our targeted attacks use a set of three possible target sentences. For each input we select the target the closest length to the true label.

3.3.2. Metrics

To evaluate our attacks we rely on several metrics:

- For untargeted attacks, the Word-Error Rate (WER) of the model on the adversarial example with respect to the true label. The higher, the stronger the attack.
- For targeted attacks, the WER on the adversarial example with respect to the target sentence. The lower, the stronger the attack. We also report the accuracy, or success rate of these attacks, i.e. the fraction of inputs for which a successful adversarial example was found.
- The Signal-Noise Ratio (SNR) of the perturbation: the higher the SNR, the less perceptible the noise. 20dB can be considered a threshold for “acceptable” noise level that does not disturb human comprehension; 30 – 40dB is an estimate of “imperceptible” noise. Both these threshold are approximate, as human perception does not align well with $L_2$ norms.

4. Results and discussion

We plot the results of the PGD and Kenansville attacks in Figure 1, while the CW and Genetic attack results are displayed in Table 1.

4.1. Direct optimization attacks

We start by analysing direct optimization attacks: PGD (Fig 1a, 1b), and CW (Table 1 columns 2-5).

The analysis of the PGD plots show large variations in the WER of different models under attack. The relative ranks of all models are consistent between $L_\infty$ and $L_2$ attacks. The only exception is the Transformer CTC encoder, which compared to other models is more robust to $L_\infty$ attacks than $L_2$ attacks. CW results on the other hand show a clear gap between the Transformer models and the LSTM models: the former always predict the attack target on adversarial examples with low noise ($SNR \geq 30dB$), while the latter require more noise for imperfect target transcriptions. The Imperceptible attack achieves almost identical results (not reported), with SNRs varying by up to 3dB.

Overall two trends emerge from these results:

- Encoders-decoder are harder to attack than encoder-only models. LAS models get lower WER than CTC models on PGD and lower SNR on CW attacks. The Transformer LAS model has a lower PGD WER than the Transformer encoder.
- Transformers are harder to attack than LSTMs with PGD, but easier with CW.

The higher robustness of encoder-decoders may simply be a result of their higher depth, which is a known cause of gradient obfuscation[21]. The fact that CW is effective against Transformer Seq2Seq models points towards that explanation: this attack’s objective is especially powerful at circumventing optimization issues. The inconsistent results of PGD and CW against LSTMs and Transformers are harder to explain, and certainly deserve more attention in future works. At the very least it shows that the performance boost of transformers does not clearly carry over in terms of robustness. It also emphasizes the need to evaluate multiple models when crafting new attacks, and multiple attacks when building new models.

4.2. Other attacks

The Kenansville DFT attack (Figure 1c) has little effect in our evaluation setting: SNRs greater than 20dB fail to increase the WER significantly, and adversarial examples with lower SNRs are easily detected by the human ear. Comparing these results to [22] is not easy for two reasons: the authors report different metrics to measure distortion, and evaluate on a different dataset. The adversarial examples they publicly released show that the original speech inputs are of lower quality than the LibriSpeech clean test set. It is therefore possible that Kenansville is most effective on inputs that are already challenging to the ASR models.

The Genetic attack[8] (Table 1 column 6) also only achieves to degrade the WER of each model by 8 to 20 points, even with an SNR of 20dB. This is not particularly surprising: this attack was originally evaluated on the much less challenging Speech Commands dataset.

<table>
<thead>
<tr>
<th>Model</th>
<th>Clean WER</th>
<th>Carlini&amp;Wagner WER↓</th>
<th>SNR</th>
<th>Acc.</th>
<th>Genetic WER↑</th>
</tr>
</thead>
<tbody>
<tr>
<td>LSTM LAS</td>
<td>5.02</td>
<td>16.98</td>
<td>14</td>
<td>66%</td>
<td>25.49</td>
</tr>
<tr>
<td>LSTM CTC</td>
<td>6.15</td>
<td>4.63</td>
<td>23</td>
<td>91%</td>
<td>24.27</td>
</tr>
<tr>
<td>Trf LAS</td>
<td>4.11</td>
<td>0</td>
<td>37</td>
<td>100%</td>
<td>21.6</td>
</tr>
<tr>
<td>Trf CTC</td>
<td>5.88</td>
<td>0</td>
<td>40</td>
<td>100%</td>
<td>20.63</td>
</tr>
<tr>
<td>W2V-100h</td>
<td>6.27</td>
<td>0</td>
<td>35</td>
<td>100%</td>
<td>13.19</td>
</tr>
<tr>
<td>W2V-960h</td>
<td>3.53</td>
<td>0</td>
<td>35</td>
<td>100%</td>
<td>16.63</td>
</tr>
<tr>
<td>W2V-large</td>
<td>2.85</td>
<td>0</td>
<td>32</td>
<td>100%</td>
<td>11.08</td>
</tr>
</tbody>
</table>

Table 1: results of all models on clean data and under the (targeted) Carlini&Wagner attack and the (untargeted) Genetic attack. For CW we report the WER, SNR and attack accuracy (i.e. success rate). The bound for the Genetic attack corresponds to an average SNR of 20dB. The up and down arrows indicate whether large or small WER values mean successful attacks.
Figure 1: Attacks results for the untargeted (a) $L_2$-PGD attack, (b) $L_\infty$-PGD attack and (c) DFT Kenansville attack, for different SNR values. The legend on the right is shared by all plots.

<table>
<thead>
<tr>
<th>Source Model</th>
<th>Target model</th>
<th>PGD WER↑</th>
<th>CW WER↓</th>
</tr>
</thead>
<tbody>
<tr>
<td>LSTM CTC</td>
<td>LSTM LAS</td>
<td>721</td>
<td>85.8</td>
</tr>
<tr>
<td>Trf CTC</td>
<td>LSTM LAS</td>
<td>14.13</td>
<td>95.83</td>
</tr>
<tr>
<td>LSTM CTC</td>
<td>Trf LAS</td>
<td>34.28</td>
<td>108</td>
</tr>
<tr>
<td>W2V-960h</td>
<td>W2V-100h</td>
<td>80.01</td>
<td>48.15</td>
</tr>
<tr>
<td>W2V-100h</td>
<td>W2V-960h</td>
<td>84.38</td>
<td>61.11</td>
</tr>
<tr>
<td>W2V-960h</td>
<td>W2V-large</td>
<td>45.89</td>
<td>91.4</td>
</tr>
<tr>
<td>W2V-large</td>
<td>W2V-960h</td>
<td>37.46</td>
<td>62.65</td>
</tr>
</tbody>
</table>

Table 2: Transferred attack results on selected source/target model pairs. The $L_2$-PGD SNR bound is 25dB. Results in italic indicate full or partial attack transferability.

<table>
<thead>
<tr>
<th>Target model</th>
<th>WER↑ (30dB)</th>
<th>WER↑ (20dB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>LSTM LAS</td>
<td>6.89</td>
<td>23.48</td>
</tr>
<tr>
<td>LSTM CTC</td>
<td>7.91</td>
<td>23.23</td>
</tr>
<tr>
<td>Trf LAS</td>
<td>4.13</td>
<td>8.43</td>
</tr>
<tr>
<td>Trf CTC</td>
<td>6.31</td>
<td>12.85</td>
</tr>
<tr>
<td>W2V-100h</td>
<td>28.64</td>
<td>82.28</td>
</tr>
<tr>
<td>W2V-960h</td>
<td>48.79</td>
<td>96.36</td>
</tr>
<tr>
<td>W2V-large</td>
<td>3.4</td>
<td>9.95</td>
</tr>
</tbody>
</table>

Table 3: SSL attack results on all models, with SNR bounds of 30dB and 20dB. Attacks are transferred from the Wav2Vec2-base pretrained model, without fine-tuning. Results in italic indicate full or partial attack transferability.

4.3. Transferred attacks

In Table 2 we report the results of transferred PGD and CW attacks between selected source-target model pairs. The first three rows report our results on supervised LAS and CTC models. They confirm the results that [18] achieved on DeepSpeech2: the CW attack displays almost no transferability between ASR models (WER $\geq 90\%$), for example between Transformer encoder and LSTM Seq2Seq. Untargeted PGD attacks achieve only a partial degradation of target model’s performance, even at 25dB SNR. The only exception is the PGD transfer between LSTM CTC and LAS models, i.e. models that share the same encoder. And even such parameter sharing is not sufficient to transfer CW perturbations (WER $\geq 85\%$).

However, results are different between Wav2Vec2 models. When transferring perturbations between Wav2Vec2 base models fine-tuned from the same pretrained encoder, we achieve a PGD degradation to 80% WER, and even partial transferability for CW (48% and 61.11%). These results are confirmed by the SSL attack (Table 3): perturbations crafted against the Wav2Vec2 base pretrained encoder substantially degrade the performance of both Wav2Vec2 fine-tuned models, but have very limited effect on any other model. With CW we even observe partial transferability from Wav2Vec2-Large to Wav2Vec2-base (WER $= 62.65\%$), while these models have different architectures and were not using the same initial weights. This shows that part of this transferability is indeed due to the Wav2Vec2 architecture and pretraining, and not just to weight initialization.

To our knowledge, this is the first case of targeted and transferable adversarial attack on ASR models. These findings should be confirmed by experiments on a much larger scale, as they could prove particularly worrisome. The recent trend in Natural Language Processing consists in training a few large self-supervised models that are applied to many contexts with small amounts of fine-tuning or even zero-shot prompting. Should Speech Recognition take a similar path, ASR adversarial attacks may become a much greater concern.

5. Conclusion

In this work we have explored the relative strengths and weaknesses of Transformers/LSTMs and LAS/CTC models, with respect to adversarial attacks. We have updated the state of multiple standard attacks against recent ASR models. Finally, we have illustrated the surprising vulnerability of Wav2Vec2 to transferred targeted attacks compared to all other ASR architectures studied in the past. Our results hint towards self-supervised pretraining as a condition for the transferability of ASR adversarial examples.

Direct extensions of this work involve evaluating more attacks, like stronger Black box attacks[9]; and applying attacks to Transducer ASR models, which are popular in streaming Speech Recognition applications[32]. In addition we plan to investigate the effect on robustness of factors that we have left aside in this work, such as vocabulary size or language models. Finally the transferability of perturbations between self-supervised models is worth exploring at a larger scale. More generally, we hope that our methodology, findings and code will help accelerate research efforts on ASR robustness.

\footnote{Since no pretrained Transducer is currently provided with Speech-brain, these extensions require important computational efforts.}
6. References


