流水线

数据集：cifar10、GTSRB、Imagenet（1k张、5k张）、SVHN（感觉可要可不要，纯属增加工作量）

攻击方法：adversarial patch、ROA

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Method | Attack | CIFAR10 | | | SVHN | | | GTSRB | | |
| Clean | Robust | | Clean | Robust | | Clean | Robust | |
| 0.4% | 2.4% | 1% | 3% | 1% | 3% |
| DS | Advpatch | 83.9 | 68.9 | 56.2 |  |  |  |  |  |  |
| ROA |  |  |  |  |  |  |  |  |  |
| PatchGuard | Advpatch | 84.6 | 69.2 | 57.7 |  |  |  |  |  |  |
| ROA |  |  |  |  |  |  |  |  |  |
| LGS | Advpatch |  |  |  |  |  |  |  |  |  |
| ROA |  |  |  |  |  |  |  |  |  |
| Ours | Advpatch |  |  |  |  |  |  |  |  |  |
| ROA |  |  |  |  |  |  |  |  |  |

需要对比的防御方案：（其实选两个就可以了）

PatchGuard

<https://github.com/inspire-group/PatchGuard>

DS

<https://github.com/alevine0/patchSmoothing>

LGS

<https://github.com/fabiobrau/local_gradients_smoothing>

Patch攻击的可解释性