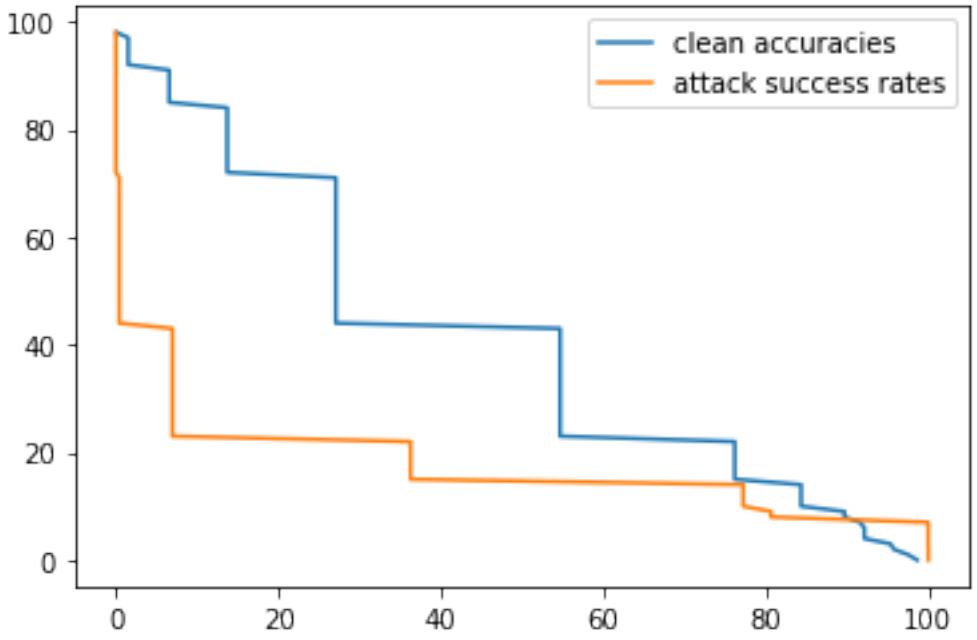
Aman Gupta
aag9131
December 9, 2022

ML for CyberSecurity Lab2

Report

Github : https://github.com/amangupta42/ML_CyberSec_Lab2

In the lab we implement and are able to observe the effects of pruning and the effect it has on the attacking accuracies. We can see that with increase in the fraction of channels pruned (X) the attacking success rate decreases but at the cost of also decreasing the clean test accuracies.



The graph above shows the variation of the attack success rate and test accuracy on clean data with different values of X = fraction of channels pruned.

The table below shows some of the numerical values obtained.

X	Attack Success Rate	Test accuracy on clean data
2	100%	97.50%
4	99.97%	95.34%
10	80.64%	89.68%
20	36.26%	76.16%
40	6.96%	54.67%