CSCI 667 - Homework 5 (EXTRA CREDIT)[*]

Assigned Dec 3rd; Due 11:59pm on Dec 10th

Prof. Adwait Nadkarni

Note: This homework assignment **will not be graded as a part of the 100 points for the course, but will be graded for 2 extra credit points.** This is an all or nothing hw, i.e., there will be no partial credit, and you will be given 2 bonus points only if you get everything correct.

1 Intrusion Detection

(a) {10 points} This problem considers the base rate fallacy discussed in class. Let $Pr(M)$ be the probability that a given packet is malware (i.e., ground truth). Let Pr(A) be the probability that there is an alarm raised by the IDS. Your IDS is 99.9% accurate at detecting intrusions [i.e., $Pr(A|M) = 0.999$] and it is 99.9% accurate at detecting when an event is not an intrusion [i.e., $Pr(!A|!M) = 0.999$]. An intrusion occurs once every one million events (i.e., the base rate of incidence is 1 / 1,000,000). What is the "true alarm" rate [i.e., determine $Pr(M|A)$]? Show your work.

(b) {10 points} This problem considers the creating of ROC curves discussed in class. Assume the same trivial detection algorithm as the slides. $D(k, T) \rightarrow [0, 1]$, takes a package of length k and a threshold T. If the packet length $k \leq T$, then an alarm is raised. Produce a table similar to that in the lecture slides showing the TP% and FP%. From this table, draw an ROC curve. Use the following traffic classifications:

- Attack packet lengths: 1, 2, 2, 3, 3, 6, 6, 10
- Non-attack packet lengths: 3, 3, 5, 6, 7, 7, 8, 8, 8, 9

[*] Last revised on December 3, 2024.