CS 445/645: Internet Security

Instructor: Shamik Sengupta, Office: SEM 204

Assignment 1 (Total 20 points)
Assigned on: Thu Feb 1, 2018, Due back on: Thu, Feb 8, 2018

Email your homework to ssunr.papers@gmail.com
Subject: CS 445: lastname_hw1 Or CS 645: lastname_hw1
Name your report: lastname_hw1.pdf
Send your code: lastname_hw1.zip

1. Simulate the behavior of probabilistic packet marking (as explained in Class) using a programming language (e.g., C, C++, Java or Python). You will compare the performance of node sampling algorithm and the edge sampling algorithm. The algorithms are given in the class slides. Present the accuracy of the model in identifying the source of the attack. Show your results using graphs.

Inputs: Topology of the network. Number of routers and their connecting edges eventually connecting them to the victim, V. (Hint: You can use topology files as inputs and read from the file to generate topology in the program. Make sure the routers are somewhat closely connected).

Input Guideline:
DO NOT use more than d=15 hops.
Use the number of routers, as 20 spread around for your runs.
Each router has unique IP addresses. (Hint: to keep it simple, you can assume a smaller unique number for routers; it is not necessary to assume 32 bit IP address).
Use the number of branches as 3, 4, or 5 for your runs.
Assume attacker or attackers are at the end of the routers. In case of multiple attackers, assume at most one attacker per branch. (Hint: there can be branches at the end of which there is no attacker).
If there is no attacker at the end of the branch, assume normal user.

Guideline for different simulation runs and comparisons:
Assume different packet marking probability, p = 0.2, 0.4, 0.5, 0.6, 0.8 for your runs.

Assume normal users send packets at a much slower rate than the attackers. Attackers use syn flood or ping flood attacks. You can use attacker's rate of pumping packets is x times higher than normal users. Choose different x values for your different runs.

Outputs: For a DoS attack, use node sampling and edge sampling algorithms to trace back the source of the attack. Answer the following.

1) For a single attacker, compare the accuracy of the traceback for both node sampling and edge sampling. Are you able to accurately find the path back to the attacker if there is one single attacker and one normal user? What is the case if there are one single attacker and two normal users?
   Compare the above results for the following cases:
   a) p = 0.2, 0.4, 0.5, 0.6, 0.8
   b) x = 10, 100, 1000
   and show your comparison results through plots. Explain the physical significance of your plots.

2) How many packets are you receiving before producing an accurate result of the traceback. Compare both the algorithms.

3) Repeat the above experiment with two attackers creating DoS attacks. Show your results, plots and explanations.

Marks distribution:
Correct programming that is designed and executed properly [5].
Q1 [8]
Q2 [2]
Q3 [5]