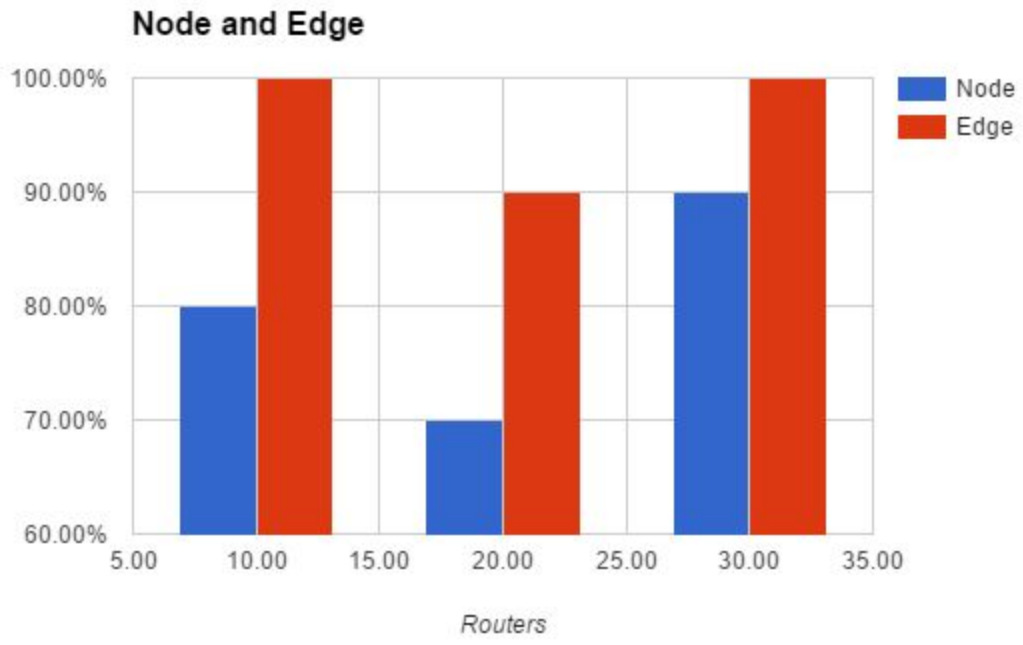
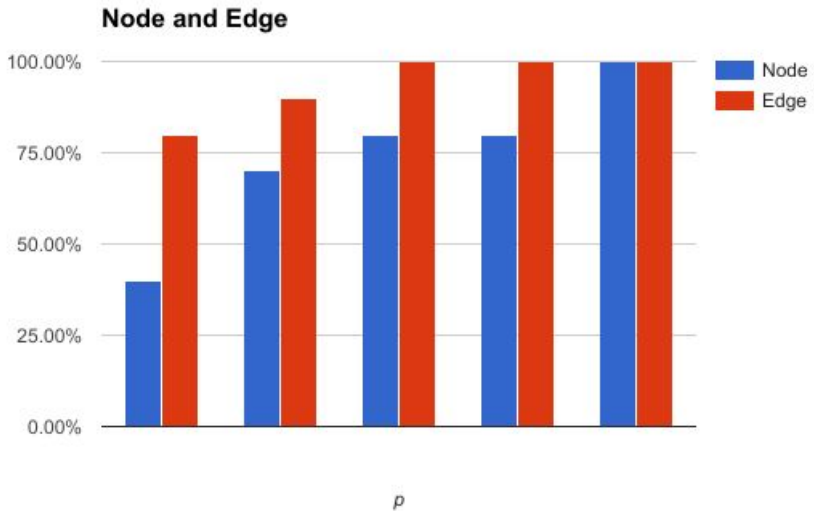
Jake Wheeler
CS445
02/21/2017
HW1

1. With a single attacker, an accurate path can be found given a certain number of packets. The less packets that are received, for both node and edge sampling the less packets are marked from the attacker's end of the network making determining the route more of a guessing game than an obvious choice. Given that these algorithms are probability based, there is always the slim chance that the algorithm could fall short, and for instance only find packets marked with your own gateway router, although edge sampling seems to handle this better. Having two users would not change the effectiveness of the algorithms, so long as each user is reconstructing the paths themselves.
    a. Changing the amount of routers only seemed to add the possibility of packets occasionally being marked with other routers. This does not change the result for node sampling, because the lesser nodes are disregarded anyways. Edge sampling seemed to not be affected as well, with the fluctuations in tests only coming from the probabilistic nature of the algorithms.



    b. Increasing the number of branches affects node sampling little, because all packets are collected and assessed anyways, the highest number of packets will still be tagged with the gateway and less so from the routers behind it leading to the attacker. When applied to edge sampling, the higher number of branches means each edge is more likely to show up in the result, whether they are significant or not.

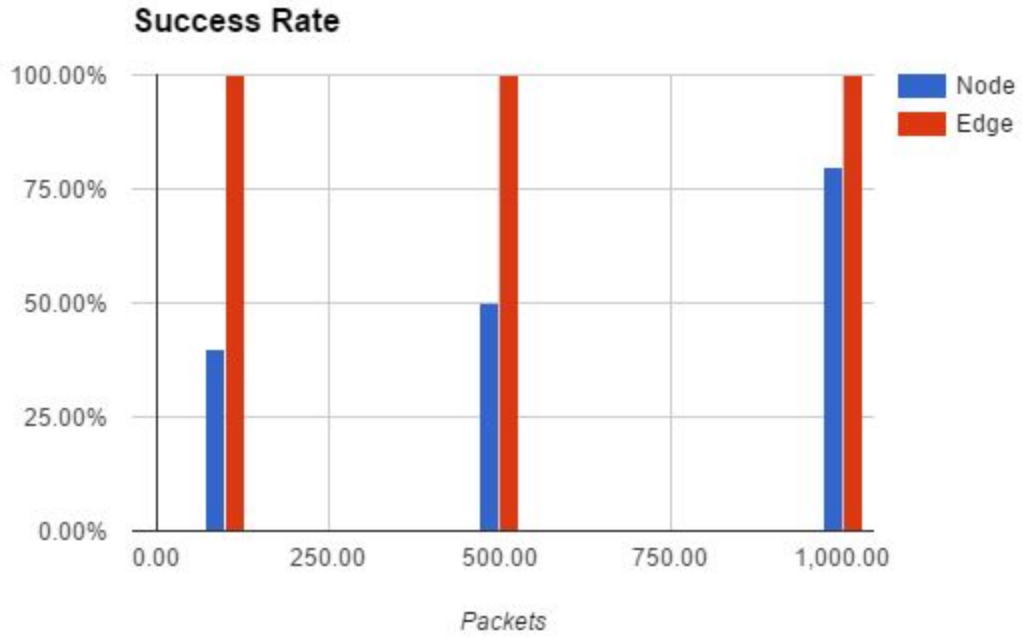
c. As seen in the graph below, increasing the probability, p increases the success rate of both algorithms in situations with a high amount of packets being analyzed.



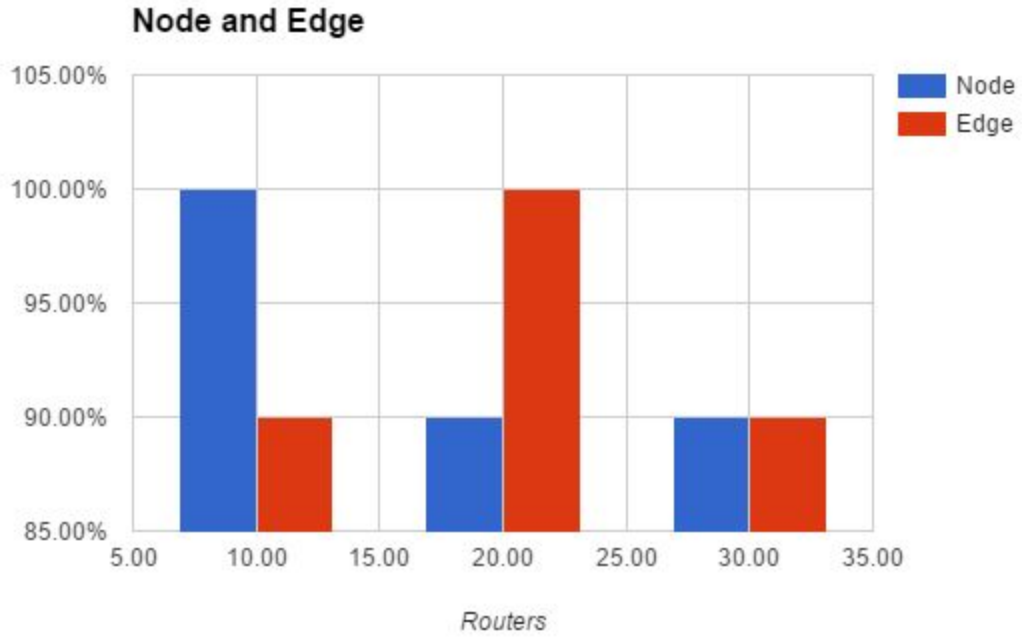
d. Increasing the packet rate only helps find the attacker quicker. No matter the algorithm, this makes the attacker stand out and makes them much easier to spot given that they fill out our routes much quicker.

2. Edge sampling seems to find the correct path in much less packets than node sampling, succeeding in as little as 100 packets as shown in the graph below while node sampling does not succeed consistently until 1000+ packets. Given the probabilistic nature of

these algorithms however, results may vary.

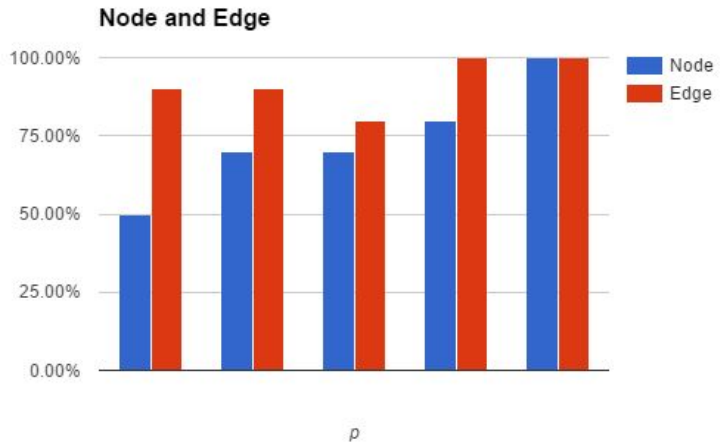


3. Adding another attacker complicates the analysis of the data a bit, but it is still certainly possible to interpret. The algorithms will attempt to show the route as if it goes through one of the attackers, but with a good eye it is easy to spot. The algorithms will show routers up until the victim no longer has a common route to the attackers. It will then print the rest of the routes out “intertwined”. Without a knowledge of the network topology, this will be difficult to decipher. For the following tests, I’ve considered the interweaved routes as a success.
    a. The router test provided similar results, aside from the expected variability of the probability succeeding or failing.



b. Increasing the number of branches interestingly showed me no different results with two attackers. I believe this is due to the hierarchical structure of the network, no matter how many branches the network ends on, they are all still funnelled through a single gateway to get to the victim.

c. This test was the one that I saw most change between one and two attackers, but it still doesn't seem very significant. The second attacker just seems to add a slightly higher chance of failure across all tests.



d. Assuming both attackers are each sending packets at the same rate and are not interfering with each other, having a higher rate would still set them aside from non attackers and make them easier to spot.