(a) Success Percentage (b) Average Disturbed ASes (c) CDF of Disturbed ASes (d) Average Path Change

Fig. 2: Success Percentages, Disturbed ASes, and Path Length Change

number to the path and advertises the route. When the hole punched route propagates to one of the blacklisted ASes, their first step will be to scan the path for their own AS number. Since their AS number appears in the path, the blacklisted AS will reject the path because it appears to form a loop. We call this technique for restricting path propagation *Fraudulent Route Reverse Poisoning*, or FRRP. The ASes surrounding the link that we want to avoid appear in the path; however, their presence is irrelevant for actual packet forwarding, because they appear after the destination AS.

FRRP can also be used to force ASes which contain high numbers of bots to ignore the hole punched paths, resulting in attack traffic remaining on the original path. Excessive blacklisting of bot ASes could result in the hole punched routes not propagating to the critical ASes. As shown in Figure 1, the majority of bots on the Internet live within a small number of ASes. Thus the bulk of attack traffic can be left in place by blacklisting only these bot heavy ASes.

Results. To evaluate the effectiveness of our approach, we built upon a BGP simulator used in our prior work [3]. The simulator is essentially a collection of software routers who speak BGP configured in a realistic topology. The topology used in the simulation is from Caida's inferred AS relationships dataset taken from December of 2016 [1]. The BGP policies used by the simulated routes matched the current best practices used by operators. We also have a dataset of of 23 botnet families which were observed launching DDoS attacks between late August 2012 and March 2013 with a total of 2.2 million unique hosts, which we use to measure the affects of bot location on our experiment.

Using our simulator, we can examine both the effectiveness and cost of a reactor using our system to migrate critical traffic off of links suffering under DDoS. Our experiment repeatedly picks two random ASes from the Internet's default free zone, that is ASes that are not stub ASes, fixing one of the ASes as the reactor and the other as an AS generating critical traffic. For each link on the original path between the reactor and critical AS, we simulate the reactor attempting to respond to a DDoS attack impacting that link. In each attack scenario, we determine the following: if we succeed at moving traffic off the attacked links, how many additional ASes see a change in their best path to the reactor AS (termed *disturbance*), the average increase in path length among the disturbed ASes, and if any disturbed ASes switch to using a next-hop that is less preferable economically.

Figure 2a shows the percentage of success in avoiding links along the path between reactor-critical AS pair. As can been seen, success is inversely proportional to the number of bot heavy ASes that need to be blacklisted. When preventing propagation to the 100 largest ASes by bot population we have success rates no less than 78%. Increasing blacklisting to the 1000 largest ASes by bot population results in success rates around 40%. Thankfully, blacklisting only the 100 largest ASes covers 79% of all attack traffic. Figure 2b shows the average number of disturbed ASes as a function of how far away from the reactor the attacked link is. For all distances, on average less than 5000 ASes among a total of over 55,000 ASes in the Internet are disturbed. Large bot AS blacklisting results in fewer disturbed ASes due to poorer propagation of hole punched roues. It should be noted that the current method of avoiding links does not perform any actions to reduce the amount of disturbed ASes outside of bot heavy ASes. No instances of an AS switching to a less economically preferable route, defined by switching from a customer learned route to a peer or provider learned route, were observed as a result of reactor actions. This means our current method incurs no additional monetary costs on ASes outside of the reactor. Figure 2d shows the average path length increase seen by disturbed ASes as a function of distance between the attacked link and reactor. Though the path length change is greater on links closer to the reactor, with about a 2.5 hop increase for links less than 2 hops out from the reactor and decreasing for links further out.

Future Work. Looking ahead, we will be exploring more advanced heuristics to minimize the side-effects of utilizing FRRP to mitigate the effects of DDoS attacks. We will also be developing a realistic link capacity model for our simulation, which will allow us to move traffic off links based on the their actual bandwidth limits.

Acknowledgments. We would like to acknowledge Aziz Mohaisen from SUNY Buffalo for providing the data describing bot locations across the Internet.

References

[1] CAIDA AS relationship dataset. http://www.caida.org/data/active/as-relationships/index.xml.

[2] M. S. Kang, S. B. Lee, and V. D. Gligor. The crossfire attack. In *Security and Privacy (SP), 2013 IEEE Symposium on*, pages 127–141. IEEE, 2013.

[3] M. Schuchard, J. Geddes, C. Thompson, and N. Hopper. Routing around decoys. In *Proceedings of the 2012 ACM Conference on Computer and Communications Security*, CCS '12, pages 85–96, New York, NY, USA, 2012. ACM.

[4] A. Yaar, A. Perrig, and D. Song. Siff: A stateless internet flow filter to mitigate ddos flooding attacks. In *Security and Privacy, 2004. Proceedings. 2004 IEEE Symposium on*, pages 130–143. IEEE, 2004.