How Secure are Secure Interdomain Routing Protocols?

Full version from June 21, 2010

Sharon Goldberg
Microsoft Research

Michael Schapira
Yale & UC Berkeley

Peter Hummon
AT&T Labs

Jennifer Rexford
Princeton

ABSTRACT

In response to high-profile Internet outages, BGP security variants have been proposed to prevent the propagation of bogus routing information. To inform discussions of which variant should be deployed in the Internet, we *quantify* the ability of the main protocols (origin authentication, soBGP, S-BGP, and data-plane verification) to blunt traffic-attraction attacks; *i.e.,* an attacker that deliberately attracts traffic to drop, tamper, or eavesdrop on packets.

Intuition suggests that an attacker can maximize the traffic he attracts by *widely* announcing a *short* path that is not flagged as bogus by the secure protocol. Through simulations on an empirically-determined AS-level topology, we show that this strategy is surprisingly effective, even when the network uses an advanced security solution like S-BGP or data-plane verification. Worse yet, we show that these results *underestimate* the severity of attacks. We prove that finding the most damaging strategy is NP-hard, and show how counterintuitive strategies, like announcing longer paths, announcing to fewer neighbors, or triggering BGP loop-detection, can be used to attract even more traffic than the strategy above. These counterintuitive examples are not merely hypothetical; we searched the empirical AS topology to identify specific ASes that can launch them. Finally, we find that a clever export policy can often attract almost as much traffic as a bogus path announcement. Thus, our work implies that mechanisms that police export policies (*e.g.,* defensive filtering) are crucial, even if S-BGP is fully deployed.

Categories and Subject Descriptors. C.2.2 Computer Communication Networks: Network Protocols.
General Terms. Security.

1. INTRODUCTION

The Internet is notoriously vulnerable to *traffic attraction* attacks, where Autonomous Systems (ASes) manipulate BGP to attract traffic to, or through, their networks. Attracting extra traffic enables the AS to increase revenue from customers, or drop, tamper, or snoop on the packets [2–4]. While the proposed extensions to BGP prevent many attacks (see [5] for a survey), even these secure protocols are susceptible to a *strategic* manipulator who deliberately exploits their weaknesses to attract traffic to its network. Given the difficulty of upgrading the Internet to a new secure routing protocol, it is crucial to understand how well these protocols blunt the impact of traffic attraction attacks.

1.1 Quantifying the impact of attacks.

We evaluate the four major extensions to BGP, ordered from weakest to strongest: origin authentication [6,7], soBGP [8], S-BGP [9], and data-plane verification [5,10]. While the stronger protocols prevent a *strictly* larger set of attacks than the weaker ones, these security gains often come with significant implementation and deployment costs. To inform discussions about which of these secure protocols should be deployed, we would like to *quantitatively* compare their ability to limit traffic attraction attacks. Thus, we simulate attacks on each protocol on an empirically-measured AS-level topology [11–13], and determine the percentage of ASes that forward traffic to the manipulator.

Performing a quantitative comparison requires some care. It does *not* suffice to say that one protocol, say S-BGP, is four times as effective as another protocol, say origin authentication, at preventing *a specific type of attack strategy*; there may be *other attack strategies* for which the quantitative gap between the two protocols is significantly smaller. Since these more clever attack strategies can just as easily occur in the wild, our comparison must be in terms of the *worst possible attack* that the manipulator could launch on each protocol. To do this, we put ourselves in the mind of the manipulator, and look for the *optimal* strategy he can use to attract traffic from *as many ASes as possible*.

However, before we can even begin thinking about optimal strategies for traffic attraction, we first need a model for the way traffic flows in the Internet. In practice, this depends on local routing policies used by each AS, which are not publicly known. However, the BGP decision process breaks ties by selecting shorter routes over longer ones, and it is widely believed [14] that policies depend heavily on economic considerations. Thus, conventional wisdom and prior work [14–16] suggests basing routing policies on business relationships and AS-path lengths. While this model (used in many other studies, *e.g.,* [2, 17]) does *not* capture all the intricacies of interdomain routing, it is still very useful for *gaining insight* into traffic attraction attacks. All of our results are attained within this model.

© ACM, 2010. This is the authors' full version of the work whose definitive conference version [1] was published in *SIGCOMM'10*, August 30–September 3, 2010, New Delhi, India. This full version is available as Microsoft Research Technical Report MSR-TR-2010-18. This technical report first appeared on February 23, 2010. This is the latest version from June 21, 2010.

1.2 Thinking like a manipulator.

If routing policies are based on AS path lengths, then intuition suggests that it is optimal for the manipulator to announce the *shortest path* that the protocol does not reject as bogus, to *as many neighbors* as possible. Depending on the security protocol, this means announcing a direct connection to the victim IP prefix, a fake edge to the legitimate destination AS, a short path that exists but was never advertised, a short path that the manipulator learned but is not using, or even a legitimate path that deviates from normal export policy. Indeed, we use simulations on a measured AS-level topology to show that this "smart" attack strategy is quite effective, even against advanced secure routing protocols like S-BGP and data-plane verification.

Worse yet, we show that our simulations *underestimate* the amount of damage manipulator could cause. Through counterexamples, show that the "smart" attack is surprisingly *not optimal*. In fact, the following bizarre strategies can sometimes attract even more traffic than the "smart" attack: announcing a *longer* path, exporting a route to *fewer* neighbors, or triggering BGP's *loop-detection* mechanism. In fact, we show that prefix hijacking (i.e., originating a prefix you do not own) is *not* always the most effective attack against today's BGP! These counterexamples are not merely hypothetical—we identify specific ASes in the measured AS-level topology that could launch them. Moreover, we prove that it is NP-hard to find the manipulator's optimal attack, suggesting that a comprehensive comparison across protocols must remain elusive.

1.3 Our findings and recommendations.

While we necessarily *underestimate* the amount of damage a manipulator could cause, we can make a number of concrete statements. Our main finding is that secure routing protocols only deal with one half of the problem: while they do restrict the *paths* the manipulator can announce, they fail to restrict his *export policies*. Thus, our simulations show that, when compared to BGP and origin authentication, soBGP and S-BGP significantly limit the manipulator's ability to attract traffic by announcing bogus short paths to all its neighbors. However, even in a network with S-BGP or data-plane verification, we found that a manipulator can still attract traffic by cleverly *manipulating his export policies*. Indeed, we found that announcing a *short* path is often less important than exporting that path to the *right set of neighbors*. Thus:

- Advanced security protocols like S-BGP and data-plane verification do *not* significantly outperform soBGP for the "smart" attacks we evaluated.
- Defensive filtering of paths exported by stub ASes (*i.e.,* ASes without customers) provides a level of protection that is *at least* comparable to that provided by soBGP, S-BGP and even data-plane verification.
- Tier 2 ASes are in the position to attract the largest volumes of traffic, even in the presence of data-plane verification and defensive filtering (of stubs).
- *Interception attacks* [2,3]—where the manipulator both attracts traffic and delivers it to the destination—are easy for many ASes, especially large ones.

We could quibble about whether or not manipulating export policies even constitutes an *attack*; after all, each AS has the right to decide where it announces paths. However, our results indicate that a clever export policy can attract almost as much traffic as a bogus path announcement. Indeed, Section 6.1 presents an example where an AS in the measured topology gains almost as much exporting a provider-learned path to another provider, as he would by a prefix hijack (announcing that he owns the IP prefix). Thus, our results suggest that addressing traffic attraction attacks requires both mechanisms that prevent bogus path announcements (*e.g.,* soBGP or S-BGP) as well as mechanisms that police export policies (*e.g.,* defensive filtering).

1.4 Roadmap.

Section 2 presents the routing model, threat model, and our experimental setup. Section 3 describes the vulnerabilities of the secure routing protocols and presents an example of how a manipulator can attract traffic by exploiting them. Section 4 describes and evaluates the "smart" *attraction* attacks, and Section 5 uses both theory and simulation to analyze *interception* attacks. Section 6 presents counterexamples, found in real network data, that prove that the "smart" attacks are not optimal. Section 7 shows that finding the optimal attack strategy is NP hard. Section 8 presents related work, Section 9 discusses some practical challenges relating to the implementation of routing security protocols, and Section 10 discusses the effect of our modeling assumptions on our results and provides further recommendations.

This full version also contains a variety of supplementary information in the appendix. Appendix A has our treatment of sibling relationships, and Appendix B has the details of our simulation methodology. Appendix D presents a counterexample from Section 6 in more detail, and Appendix E presents a supplementary example that shows how an interception attack can fail, and corrects an error in [2]. Proofs of our theorems are in Appendices F-G. Finally, Appendix H presents versions of all the graphs in the body of this paper, computed from a different AS topology dataset [12,13] than the graphs presented in the body of this paper [11].

2. MODEL AND METHODOLOGY

We first present a model of interdomain routing and routing policies, based on the standard models in [18] and the Gao-Rexford conditions [15], followed by our threat model for traffic attraction, and finally our experimental setup.

2.1 Modeling interdomain routing.

The AS graph. The interdomain-routing system is modeled with a labeled graph called an *AS graph*, as in Figure 1. Each AS is modeled as a single node and denoted by its AS number. Edges represent direct physical communication links between ASes. Adjacent ASes are called *neighbors*. Since changes in topology typically occur on a much longer timescale than the execution of the protocol, we follow [18] and assume the AS-graph topology is static. BGP computes paths to each destination IP prefix separately, so we assume that there is a unique *destination IP prefix* to which all other nodes attempt to establish a path. As shown in Figure 1, there is a single AS v that rightfully 'owns' the destination IP prefix under consideration.

Establishing paths. In BGP, an AS first chooses an

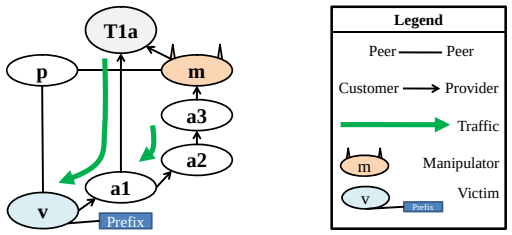


Figure 1: Anonymized subgraph of CAIDA's AS graph.

outgoing edge on which it forwards traffic based on a local ranking on outgoing paths, and then announces this path to some subset of its neighbors. To model this, we assume that each node n has a set of *routing policies*, consisting of (a) a *ranking* on outgoing paths from n to the destination d, and (b) a set of *export policies*, a mapping of each path P to the set of neighbors to which n is willing to announce the path P. We say that node n has an *available path* aPd if n's neighbor a announced the path "aPd" to n. If an available path aPd is ranked higher than the outgoing path that node n is currently using, then an *normal* node n will (a) forward traffic to node a, and (b) announce the path $naPd$ to all his neighbors as specified by his export policies.

Business relationships. We annotate the AS graph with the standard model for business relationships in the Internet [15]; while more complicated business relationships exist in practice, the following is widely believed to capture the majority of the economic relationships in the Internet. As shown in Figure 1, there are two kinds of edges: *customer-provider* (where the customer pays the provider for connectivity, represented with an arrow from customer to provider), and *peer-to-peer* (where two ASes owned by different organizations agree to transit each other's traffic at no cost, represented with an undirected edge). Because some of our results are based on CAIDA's AS graph [11], we also consider *sibling-to-sibling* edges. Details about our treatment of siblings is in Appendix A. Finally, our theoretical results sometimes use [15]'s assumption that an AS cannot be its own indirect customer:

GR1 The AS graph contains no customer-provider cycles.

2.2 Modeling routing policies.

In practice, the local routing policies used by each AS in the Internet are arbitrary and not publicly known. However, because we want to understand how false routing information propagates through the Internet, we need to concretely model routing policies. Since it is widely believed that business relationships play a large role in determining the routing policies of a given AS [14, 15], and we have reasonably accurate empirical maps of the business relationships between ASes [11–13], we base our model on these relationships.

Rankings. BGP is first and foremost designed to prevent loops. Thus, we assume that node a rejects an announcement from its neighbor b if it contains a *loop*, *i.e.,* if node a appears on the path that node b announces. Beyond that, we can think of the process ASes use to select routes as follows; first applying local preferences, then choosing shortest AS paths, and finally applying a tie break. Since the local preferences of each AS are unknown, and are widely believed to be based (mostly) on business relationships, we model the three step process as follows:

LP **Local Preference.** Prefer outgoing paths where the next hop is a customer over outgoing paths where the next hop is a peer over paths where the next hop is a provider.

SP **Shortest Paths.** Among the paths with the highest local preference, chose the shortest ones.

TB **Tie Break.** If there are multiple such paths, choose the one whose next hop has the lowest AS number.[1]

Our model of local preferences is based on on Gao-Rexford condition **GR3**, and captures the idea that an AS has an economic incentive to prefer forwarding traffic via customer (that pays him) over a peer (where no money is exchanged) over a provider (that he must pay). Notice that this implies that an AS can sometimes prefer a *longer* path! (*e.g.,* in Figure 1, AS m prefers the five-hop customer path through $a3$ over the four-hop provider path through Tier 1 $T1$.)

Export Policies. Our model of export policies is based on the Gao-Rexford condition **GR2**:

GR2 AS b will only announce a path via AS c to AS a if at least one of a and c are customers of b.

GR2 captures the idea that an AS should only be willing to load his own network with transit traffic if he gets paid to do so. However, because **GR2** does *not* fully specify the export policies of every AS (for instance, an AS could decide to export paths to only a *subset* of his customers), it does not suffice for our purposes. Thus, we model normal export policies as follows:

NE An AS will announce *all* paths to *all* neighbors *except* when **GR2** forbids him to do so.

2.3 Threat model.

One strategic manipulator. We assume that all ASes in the AS graph behave *normally*, *i.e.,* according to the policies in Section 2.1 - 2.2, except for a *single manipulator* (*e.g.,* AS m in Figure 1). We leave models dealing with colluding ASes for future work.

Normal ASes and normal paths. We assume that every *normal* AS uses the routing policies in Section 2.2; thus, the *normal path* is the path an AS (even the manipulator) would choose if he used the normal rankings of Section 2.2, and *normal export* is defined analogously. (*e.g.,* In Figure 1, the manipulator m's *normal path* is through his customer AS $a3$.) We shall assume that every normal AS knows its business relationship with his neighbors, and also knows the next hop it chooses for forwarding traffic to a given destination. In order to evaluate the effectiveness of each secure routing protocol, we assume that ASes believe everything they hear, *except* when the secure routing protocol tells them otherwise. As such, we do not assume that ASes use auxiliary information to detect attacks, including knowledge of the network topology or business relationships

[1]We need a consistent way to break ties. In practice, this is done using the intradomain distance between routers and router IDs. Since our model does not incorporate geographic distance or individual routers, we use AS number instead.

between distant ASes, *etc.*, unless the secure routing protocol *specifically* provides this information.

Attraction *v.s.* Interception attacks. In an *attraction attack*, the manipulator's goal is to attract traffic, *i.e.,* to convince the maximum number of ASes in the graph to forward traffic that is destined to the *victim IP prefix* via the manipulator's own network. To model the idea that a manipulator may want to eavesdrop or tamper with traffic before forwarding it on to the legitimate destination, we also consider *interception attacks*. In an interception attack, the manipulator has the additional goal of ensuring that he has an *available path to the victim*. This is in contrast to an attraction attack, where the manipulator is allowed, but not required, to *create a blackhole* where he has no working path to the victim IP prefix (*e.g.,* Figure 11).

The fraction of ASes attracted. In this paper, we measure the success of an attack strategy by counting *the fraction of ASes in the internetwork* from which that manipulator attracts traffic; this amounts to assuming that every AS in the internetwork is of equal importance to the manipulator.[2] However, it is well known that the distribution of traffic in the Internet is *not* uniform across the ASes; to address this, we also report the fraction of ASes of *various sizes* from which the manipulator attracts traffic, where we measure size by the number of direct customers the AS has. We leave measuring the *volume of traffic* a manipulator attracts to future work; one (rough) way to do this would be to correlate the volume of traffic that an AS receives to the size of the IP address space owned by that AS.

Attack strategies. To capture the idea that the manipulator is strategic, we allow him to be more clever than the normal ASes; specifically, we allow him to use knowledge of the global AS graph and its business relationships in order to launch his attacks. (However, most of the strategies we considered require only knowledge that is locally available at each AS.) An attack strategy is a set of routing announcements and forwarding choices that deviates from the normal routing policies specified in Section 2.2. An attack strategy may include, but is not limited to:

- Announcing an unavailable or non-existent path.
- Announcing different paths to different neighbors.
- Announcing a legitimate available path that is *different* from the *normal path*.
- Exporting a path (even the legitimate normal path) to a neighbor to which *no path* should be announced to according to the normal export policies.

Indeed, one might argue that some of these strategies do not constitute 'dishonest behavior'. However, it is important to consider these strategies in our study, since we shall find that they can sometimes be used to attract as much traffic as the traditional 'dishonest' strategies (*e.g.,* announcing non-existent paths).

Scope of this paper. This paper focuses on traffic attraction attacks; we do not consider other routing security issues, for instance, mismatches between the control- and data-plane [4, 10], or traffic deflection attacks, where a manipulator wants to divert traffic from himself or some distant, innocent AS [5].

[2]We acknowledge that a manipulator may want to attract traffic from a *specific subset* of ASes. We avoid analyzing this, because we lack empirical data to quantify that subset of ASes that a given manipulator may want to attract.

2.4 Experiments on empirical AS graphs.

All the results and examples we present are based on empirically-obtained snapshots of the Internet's AS graph annotated with business relationships between ASes.

Algorithmic simulations. At the core of our experiments is our *routing tree algorithm* (presented in Appendix B.1) that determines the paths that each AS uses to reach the destination prefix under the assumption that each AS 'normally' uses the routing policies of Section 2.2. Because we run a large number of experiments over the full (≈30K node) AS graph, we avoid the heavy message-passing approach used by standard BGP simulators; instead, we use lightweight algorithmic approach based on breadth-first search. The routing tree algorithm is also used to simulate the result of a manipulator's attack strategy. In Appendix B.1, we discuss how we simulate a bogus path announcement by 'seeding' the routing tree algorithm with the bogus path, and simulate strategic export policies by removing certain links between the manipulator and his neighbors.

Average case analysis. Since the influence of an attack strategy depends heavily on the locations of the manipulator and the victim in the AS graph, we run simulations across many (manipulator, victim) pairs. Rather than reporting average results, we plot the *distribution* of the fraction of ASes that direct traffic to the manipulator. We by no means believe that a manipulator would select its victim at random; however, reporting distributions allows us to measure the extent to which a secure protocol can blunt the power of the manipulator, determine the fraction of victims that a manipulator could effectively target, and identify positions in the network that are effective launching points for attacks. Ideally, to determine how damaging a given attack strategy can be, we would have liked to run simulations over *every* (manipulator,victim) pair in the AS graph. However, this would require $(30\text{K})^2$ simulations per dataset, which would be prohibitive. Instead, we run experiments on randomly-chosen (manipulator, victim) pairs. We found that 60K experiments of each type were sufficient for our results to stabilize.

Multiple datasets. Because the actual AS-level topology of the Internet remains unknown, and inferring AS relationships is still an active area of research, we run simulations on a number of different datasets: multiple years of CAIDA data [11], and Cyclops data [12] augmented with 21,000 peer-to-peer edges from [13]'s IXP dataset. Even though these datasets use different relationship-inference algorithms, the trends we observed across datasets were remarkably consistent. Thus, all the results we present are from CAIDA's November 20, 2009 dataset (with slight modifications to the sibling relationships, see Appendix A.2); counterparts of these graphs, computed from Cyclops and IXP data [12, 13] are in Appendix H.

Realistic examples. Rather than providing contrived counterexamples, we give evidence that the attack strategies we discuss could succeed in wild by ensuring that *every example we present comes from real data*. To find these examples, we (algorithmically) searched the empirically-measured AS graph for specific subgraphs that could induce specific counterexamples, and then simulated the attack strategy.

All the examples we present here were found in CAIDA's November 20, 2009 dataset [11], and then "anonymized" by replacing AS numbers with symbols (*e.g.,* in Figure 1, m for manipulator, v for victim, $T1$ for a Tier 1 AS, *etc.*). We do this in order to avoid 'implicating' innocent ASes with our example attacks, as well as to avoid reporting potentially erroneous AS-relationship inferences made in the CAIDA dataset (see Section 6.4 for further discussion).

3. FOOLING BGP SECURITY PROTOCOLS

This section overviews the security protocols we consider, and presents *the set of (possibly) bogus paths that a manipulator can announce to each neighbor without getting caught.* We use the anonymized subgraph of CADIA's AS graph in Figure 1 to demonstrate the fraction of traffic a manipulator m could attract by announcing one of these (possibly) bogus paths to all its neighbors.

Our focus is on protocols with well-defined security guarantees. Thus, we consider the five major BGP security variants, ordered from weakest to strongest security, as follows: *(unmodified) BGP, Origin Authentication, soBGP*, *S-BGP*, and *data-plane verification.* Because we focus on security guarantees and not protocol implementation, we use these as an umbrella for many other proposals (see [5] for a survey) that provide similar guarantees using alternate, often lower-cost, implementations. Furthermore, our ordering of protocols is strict: an attack that succeeds against a strong security protocol, will also succeed against the weaker security protocol. We also consider *defensive filtering* as an orthogonal security mechanism.

BGP. BGP does not include mechanisms for validating information in routing announcements. Thus, the manipulator can get away with announcing any path he wants, including (falsely) claiming that he is the owner of the victim's IP prefix. Indeed, when the manipulator m in Figure 1 (an anonymized Canadian Tier 2 ISP) launches this attack on the v's IP prefix (an anonymized Austrian AS), our simulations show that he attracts traffic from 75% of the ASes in the internetwork.[3]

Origin Authentication. Origin authentication [6] uses a trusted database to guarantee that an AS cannot falsely claim to be the rightful owner for an IP prefix. However, the manipulator can still get away with announcing any path that *ends* at the AS that rightfully owns the victim IP prefix. For instance, in Figure 1, the manipulator m can attract traffic from 25% of the ASes in the internetwork by announcing the path (m, v, Prefix), even though no such path physically exists.

soBGP. Secure Origin BGP (soBGP) [8] provides origin authentication as well as a trusted database that guarantees that any announced path *physically exists* in the AS-level topology of the internetwork. However, a manipulator can still get away with announcing a path that *exists* but is not actually *available.* In Figure 1, the manipulator m can attract traffic from 10% of the ASes in the internetwork by announcing the path (m, p, v, Prefix). Notice that this path is unavailable; **GR2** forbids the Swiss Tier 2 ISP p to announce a peer path to another peer.

Of course, finding paths that exist in the AS graph requires the manipulator to have knowledge of the global topology of the network. However, obtaining this information is not especially difficult; an industrious manipulator might even obtain this information from the AS graph datasets [11–13] that we used in this paper, or even (ironically) from the soBGP database itself!

S-BGP. In addition to origin authentication, Secure BGP [9] also uses cryptographically-signed routing announcements to provides a property called *path verification.* Path verification guarantees that every AS a can only announce a path abP to its neighbors if it has a neighbor b that *announced* the path bP to a. Thus, it effectively limits a single manipulator to announcing available paths. For instance, in Figure 1, the manipulator's *normal path* (see Section 2.3) is the five-hop customer path (m, $a3$, $a2$, $a1$, v, Prefix); announcing that path allows him to attract traffic from 0.9% of the ASes in the internetwork. However, with S-BGP the manipulator could instead announce the *shorter* four-hop provider path (m, $T1$, $a1$, v, Prefix), thus doubling attracted traffic to 1.7%. Indeed, S-BGP does *not* prevent the manipulator from *announcing* the shorter, more expensive, provider path, while actually *forwarding traffic* on the cheaper, longer customer path.

Data-plane verification. Data-plane verification [5, 10] prevents an AS from announcing one path, while forwarding on another. Thus, if the manipulator in Figure 1 wants to maximize his attracted traffic, he must also forward traffic on the provider path.

Defensive Filtering. Defensive filtering polices the BGP announcements made by stubs. A *stub* is an AS with no customers, and in our model, **GR2** implies that a stub should *never* announce a path to a prefix it does not own. Thus, our model of defensive filtering has each provider keep a "prefix list" of the IP prefixes owned by its direct customers that are stubs. If a stub announces a path to *any* IP prefix that it does not own, the provider drops/ignores the announcement, thus enforcing **GR2**. In most of our analysis, we assume that *every provider* in the internetwork correctly implements defensive filtering (see also the discussion in Section 9). As such, we assume that *defensive filtering completely eliminates all attacks by stubs.*

Anomaly Detection. Anomaly detection mechanisms are outside our scope. Firstly, many of these provide functionalities that approximate the security guarantees described above, so their effectiveness is upperbounded by the schemes we evaluate. Secondly, the remaining protocols usually do not have well-defined guarantees; *e.g.,* [17,19] flag suspicious routes as potential export policy violations, but do not *guarantee* the detection of *every* export policy violation.

4. SMART ATTRACTION ATTACKS

We simulate attraction attacks on measured graphs of the Internet's AS-level topology [11–13] to determine how much traffic a manipulator can attract in the *average case.* This section first presents the attack strategies we simulated, and then reports our results.

[3]In fact, another strategy, called a *subprefix hijack*, is available to manipulator; by announcing a longer, more specific subprefix of the victim's IP prefix, he can attract traffic from 100% of the ASes in the internetwork. This work does not consider subprefix hijacks, mostly because these attacks are well understood, but also because they can be prevented by the filtering practices discussed in [5].

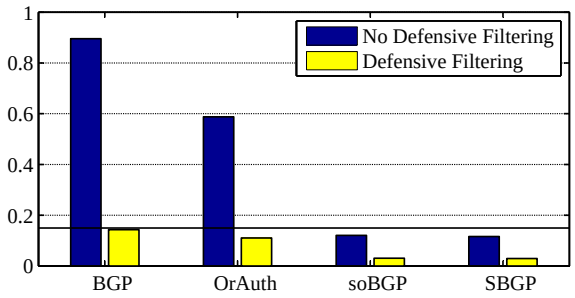


Figure 2: Lower bounds on the probability of attracting at least 10% of ASes in the internetwork.

4.1 A smart-but-suboptimal attack strategy.

We assumed that ASes make routing decisions based on business relationships and path length, and that a manipulator m cannot lie to his neighbor a about their business relationship (*i.e.,* between m and a). Thus, intuition suggests that the manipulator's best strategy is to widely announce the shortest possible path:

"Shortest-Path Export-All" attack strategy. Announce to *every* neighbor, the *shortest* possible path that is *not flagged as bogus by the secure routing protocol.*

Every "Shortest-Path Export-All" attack strategy on S-BGP is also an attack on data-plane verification. The "Shortest-Path Export-All" attack strategy on S-BGP has the manipulator announce his shortest *legitimate available path* to the victim, instead of his *normal path* (see Sections 2.3 and 3). Notice that if the manipulator actually decides to *forward* his traffic over the announced path, he has a successful attack on data-plane verification as well! Thus, the "Shortest-Path Export-All" attack strategy on data-plane verification is *identical* to the attack on S-BGP. (To reduce clutter, the following mostly refers to the attack on S-BGP.)

We underestimate damage. Section 6 shows that the "Shortest-Path Export-All" attack strategy is *not* actually optimal for the manipulator, and Section 7 shows that finding the optimal attack strategy is NP-hard. Thus, we give up on finding the *optimal* attack strategy, and run simulations assuming that the manipulator uses this smart-but-suboptimal attack. This means that the results reported in this section *underestimate* the amount of damage a manipulator could cause, and we usually *cannot* use these results to directly compare different secure routing protocols. In spite of this, our simulations do provide both (a) useful lower bounds on the amount of damage a manipulator could cause, and (b) a number of surprising insights on the strategies a manipulator can use to attract traffic to his network.

4.2 Defensive filtering is crucial.

Our first observation is that defensive filtering is a crucial part of any Internet security solution:

Figure 2: We show the probability that, for a randomly chosen (manipulator,victim) pair, the manipulator can attract traffic destined for the victim from at least 10% of the ASes in the internetwork. The manipulator uses the "Shortest-Path Export-All" attack strategy. The first four bars on the left assume that network does *not* use defensive filtering. We show the success of the manipulator's strategy on each of the four BGP security variants, in a network with and without defensive filtering of stubs. The horizontal line in Figure 2 shows the fraction of attacks that are completely eliminated by defensive filtering; since 85% of ASes in the CAIDA graph are stubs, properly-implemented defensive filtering guarantees that only 15% of manipulators can successfully attack any given victim.

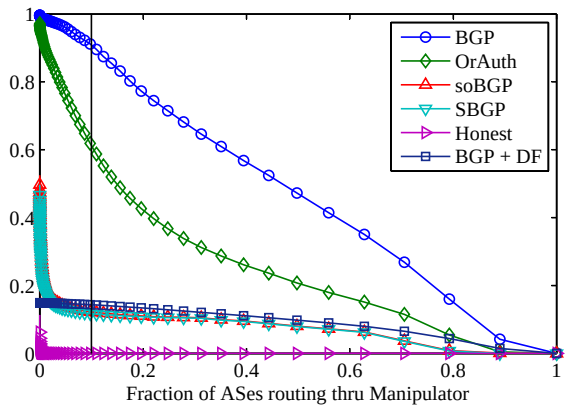


Figure 3: CCDF for the "Shortest-Path Export-All" attack strategy.

Despite the fact that we used *sub-optimal* strategies for the manipulator, we have two concrete observations:

1. Even if we assume the manipulator runs the sub-optimal "Shortest-Path Export-All" attack strategy on a network that has S-BGP but not defensive filtering, he can still attract 10% of the ASes in the internetwork with probability $> 10\%$. Furthermore, more clever strategies for S-BGP (*e.g.,* Figure 14 and 15) might increase the manipulator's probability of success to the point where defensive filtering *alone* performs even better than S-BGP alone.

2. Even if both S-BGP *and* defensive filtering are used, there is still a non-trivial 2% probability that the manipulator can attract 10% of the ASes in the internetwork. Better attack strategies could increase this probability even further. This is particularly striking when we compare with the normal case, where the manipulator manages to attract 10% of the ASes in the internetwork with about 10^{-4} probability (not shown).

4.3 Attack strategy on different protocols.

The reader may wonder why we chose to focus specifically on the probability of attracting 10% of the ASes in the internetwork in Figure 2. In the interest of full disclosure, we now present the full picture:

Figure 3: We show the complimentary cumulative distribution function (CCDF) of the probability that at least a x-fraction of the ASes in the internetwork forward traffic to the manipulator when he uses the "Shortest-Path Export-All" attack strategy. Probability is taken over the uniform random choice of a victim and manipulator, and observe that Figure 2 simply presents a crosssection of these results at the x-axis value of $x = 10\%$. Because this figure carries quite a lot of information, we walk through a few interesting points:

BGP curve. Here, the manipulator *originates*, *i.e.,* announces that he is directly connected to, the victim prefix. This curve looks almost like the CCDF of a uniform distribution, since the manipulator and the victim both announce

one-hop paths to the prefix, and are thus are about equally likely to attract traffic.

Origin Authentication curve. This time the manipulator announces that he has a direct link to the AS that legitimately owns the victim prefix. Because the manipulator's path is now two hops long, the amount of traffic he can attract on average is reduced.

soBGP and S-BGP curves. For the attack on soBGP, the manipulator announces the shortest path that *exists* in the AS graph. For the attack on S-BGP (and data-plane verification), the manipulator announces the shortest *available* path that he learned from his neighbors. Oddly, the soBGP and S-BGP curves are almost identical, despite the fact that S-BGP provides stronger security guarantees than soBGP (see also Section 4.4). For now, however, notice that both curves drop off sharply, with a knee around $x = 2\%$, $y = 15\%$. This means that 85% of manipulations do not manage to attract more than 2% of the ASes in the internetwork; these numbers roughly correspond to the fact that 85% of ASes in the graph are stubs that fail to attract much traffic with the "Shortest-Path Export-All" attack strategy on soBGP and S-BGP. Meanwhile, between $x = 2\%$ to $x = 60\%$, both curves tend to flatten out, suggesting that if a manipulator is able to attract at least 2% of the ASes in the internetwork, he is almost equality likely to be able to attract 60%. We spend more time on this observation in Section 4.5.

Honest curve. Here the manipulator behaves 'normally', *i.e.,* using the ranking and export policies of Section 2.2. This curve looks almost like a delta-function at $x = 0$. That is, a randomly-chosen AS is likely to attract only a negligible fraction of the ASes in the internetwork by behaving normally.

BGP+Defensive Filtering curve. Defensive filtering eliminates all "Shortest-Path Export-All" attack strategies on BGP by stubs, *i.e.,* by 85% of ASes. Thus, this is approximately 'BGP' curve scaled down to 15%.

Different-sized ASes are equally affected. This paper consistently measures the manipulator's success by *counting the number of ASes* that route through him as a result of his attack strategy. We also produced versions of Figure 3 that count the fraction of ASes *of a given size* that route through the manipulator: (a) All ASes, (b) ASes with at least 25 customers, and (c) ASes with 250 customers. We omit these graph as they were almost identical.

4.4 S-BGP forces long path announcements.

Figures 2 and 3 show that S-BGP is *not* much more effective in preventing "Shortest-Path Export-All" attack strategies than the less-secure soBGP. To understand why, let's compare the lengths of the path that the manipulator can announce with soBGP and S-BGP:

Figure 4: We show the probability that the manipulator can announce a path that is shorter than the *normal path*, *i.e.,* the path he would have chosen if had used the rankings in Section 2.2. Probability is taken over a randomly-chosen victim, and a manipulator that is randomly chosen from one of the following four *classes*: (a) Any AS in the graph, (b) *Non-stubs*, or ASes with at least one customer (c) Medium-sized ASes with at least 25 customers, and (d) Large ASes with at least 250 customers. If we focus on the results for S-BGP, it is clear that *larger* ASes are more likely to find

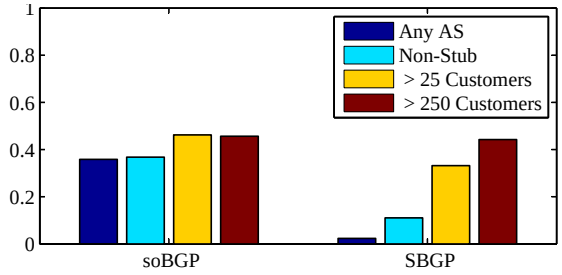


Figure 4: Probability of finding a shorter path.

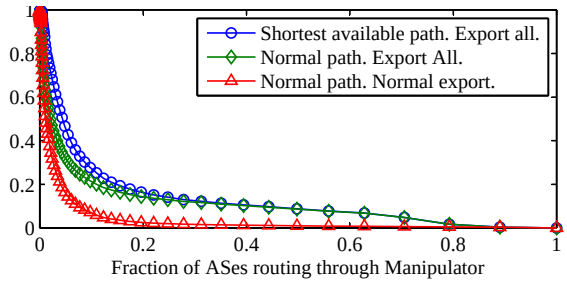


Figure 5: Aggressive export policies.

shorter paths through the network; this follows from the fact that these ASes are both more richly connected (*i.e.,* they have large degree), as well more central (*i.e.,* they are closer to most destinations in the internetwork). Furthermore, we can also see that ASes (especially small ASes) are more likely to find short paths with soBGP than they are with S-BGP.

From Figure 4, we can conclude that S-BGP is doing exactly what it is designed to do: it is limiting the set of paths the attacker can announce, thus forcing him to announce longer paths. However, in light of the results in Figures 2-3, we must ask ourselves why forcing the manipulator to announce longer paths does not seem to significantly limit the amount of traffic he attracts. We could explain by arguing that path lengths in the Internet are fairly short, (averaging about 5 hops in our simulations, see Appendix C); so the paths that the manipulator can get away with announcing in soBGP are only a few hops shorter than the paths he can announce with S-BGP. Indeed, as we show in the next section, the fact that AS paths are normally so short means that the *length* of the manipulator's path often plays less of a role than the *set of neighbors that he exports to*.

4.5 Export policy matters as much as length...

We now show that the attacker's export policy is as important as the length of the path he announces:

Figure 5: We show another CCDF of the probability that at least a x-fraction of the ASes in the internetwork forward traffic to the manipulator; probability is taken over a randomly-chosen victim, and a manipulator chosen randomly from the class of ASes that have at least 25 customers. We consider three different strategies: (a) Announce the shortest available path to all neighbors (equivalent to the "Shortest-Path Export-All" attack strategy on S-BGP), (b) Announce the normal path to all neighbors, and (c) Announce the normal path using the normal (**GR2** and **NE**) export policy.

This figure shows that, on average, announcing a *shorter* path is much less important than announcing a path to more neighbors (*i.e.,* the curves for (a) and (b) are very close,

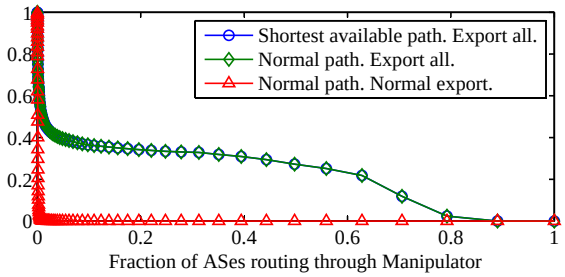


Figure 6: Aggressive export policies when the normal path is through a provider.

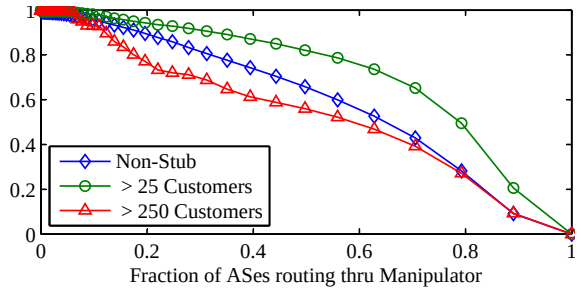


Figure 7: "Shortest-Path Export-All" attack strategy on BGP by different manipulators.

while the curves for (b) and (c) are quite far apart). Indeed, when we considered smaller manipulators (not shown), the curves for (a) and (b) are even closer together. One way to explain the small gap between (a) and (b) is to note that the manipulator's normal path is very often also his shortest path (this holds for 64% of (manipulator, victim) pairs from this class); and even when it is not, his normal path tend to be quite short.

To understand the large gap between (b) and (c), we note that by violating the normal export policy, the manipulator can announce paths to his providers, even when his normal path is not through a customer. His providers are more likely to choose the customer path through the manipulator, over some possibly shorter, non-customer path.

4.6 ... especially when using provider paths!

The effectiveness of the export-all strategy is particularly pronounced when we zoom in on the cases where the normal path is a *provider path* (which happens for about 34% of (manipulator,victim) pairs conditioning on the manipulator having at least 25 customers).

Figure 6: This is Figure 5 conditioned on the fact the manipulator's normal path is through a provider. In this case, the manipulator's normal path is always his shortest available path,[4] so we show only two strategies instead of three (*cf.,* Figure 5): (b) Announce the normal path to all neighbors (c) Announce the normal path using the normal (**GR2** and **NE**) export policy.

The figure shows that exporting to all neighbors dramatically increases the amount of traffic attracted by the manipulator. This follows from the fact that the normal (**GR2** and **NE**) export policy requires the manipulator to export provider paths to *customers only* (curve (c)); when the manipulator violates this export policy by exporting to *providers* (and peers) as well (curve (b)), his providers will prefer the customer path through the manipulator, and significantly increase the amount of traffic the manipulator attracts. This effect is particularly pronounced here because we considered manipulators with at least 25 customers in this figure (roughly modeling 'Tier 2' ASes), that stand to gain by attracting traffic from their providers, the Tier 1s.

Thus, Figure 5-6 teach us that, as well as creating *short* paths, it is crucial for the manipulator to create *customer* paths.

[4]By **LP**, if the normal path is a provider path, then all paths available to the manipulator must be provider paths, and by **SP**, he chooses the shortest one.

4.7 Tier 2s usually cause the most damage.

Next, we would like to determine which ASes in the Internet are likely to be the most successful manipulators. We consider non-stub manipulators from three different classes: (a) Non-stubs (ASes with at least 1 customer), (b) ASes with at least 25 customers, (roughly modeling "Tier 2 ASes"), and (c) Large ASes with at least 250 customers ("Tier 1 ASes"):

Figure 7: We once again show a CCDF of the probability that at least a x-fraction of the ASes in the internetwork forward traffic to the manipulator, when the manipulator launches the "Shortest-Path Export-All" attack strategy on BGP. Despite the fact that the "Tier 1" manipulators are more central than the "Tier 2s", we make the surprising observation that "Tier 2s" manage to attract more traffic than than "Tier 1s". In fact, for certain regimes, even smaller non-stub ASes tend to attract more traffic than the "Tier 1s"!

This bizarre observation is actually easy to explain. In the "Shortest-Path Export-All" attack strategy on BGP, every manipulator (regardless of its size or location in the network) announces a single-hop path to the victim prefix. Thus, announced path length does *not* play a role when we compare across classes of manipulators. On the other hand, despite their centrality, Tier 1 ASes are more expensive to route through than every other AS in the internetwork; a Tier 1 is always a provider or peer of its neighbors, so even if those neighbors learn a short path through the Tier 1, they will prefer to route over a (potentially longer) path through one of their own customers. Furthermore, Tier 2s are more central and richly connected than smaller ASes on the edge of the internetwork, and thus they tend to attract more on average than the smaller ASes ("Non-Stubs").

The reader may be troubled by the fact that the (red triangle) curve for the manipulators with at least 250 customers has a different shape than the other curves in Figure 7. We saw exactly this effect on all our experiments across different datasets, and one main reason it occurs is because the AS graph we used only has 34 ASes (out of a total of 33K ASes) that have at least 250 customers; this is consistent with the idea that are about 12 (or so) Tier 1 ASes in the Internet. Because we had so few manipulators to choose from, the effect of individual manipulators on the results become more pronounced, and the curves become less 'smooth'.

4.8 S-BGP is vulnerable to stubs.

The picture for origin authentication looks about the same as Figure 7. However, the results change slightly when we look at soBGP and S-BGP/data-plane verification:

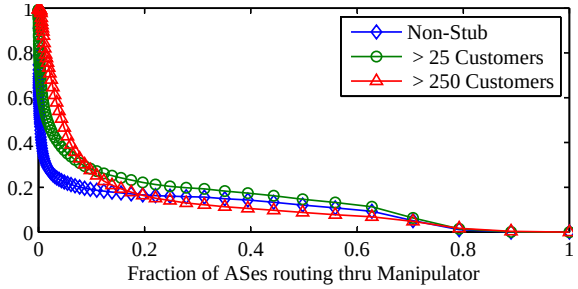


Figure 8: "Shortest-Path Export-All" attack strategy on S-BGP/data-plane verification by different manipulators.

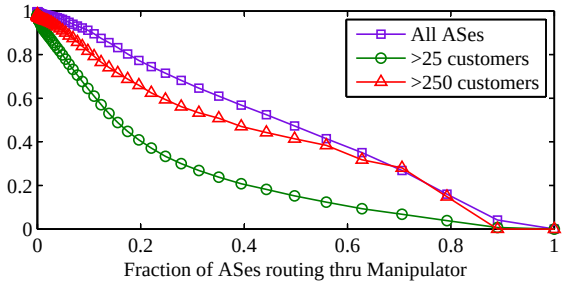


Figure 9: "Shortest-Path Export-All" attack strategy on BGP for different victims.

Figure 8: This is the CCDF for S-BGP/data-plane verification (*cf.,* to Figure 7). "Tier 2" manipulators usually come out on top, except when we consider manipulations that attract 10% of the ASes in the internetwork or less. In this regime, the Tier 1 ASes come out on top, so that the S-BGP curve mimics normal behavior (not shown). Tier 1s tend to attract more traffic than others when everyone is behaving normally, because they are likely to have short customer paths they can announce to all of their (many) neighbors.

4.9 Tier 1s are more vulnerable to attacks?!?

Next, we determine which ASes in the internetwork are most vulnerable to attack. This time, we consider *victims* from three classes: (a) All ASes, (b) ASes with at least 25 customers, and (c) Large ASes with at least 250 customers:

Figure 9: This is another CCDF of the probability that at least a x-fraction of the ASes in the internetwork forward traffic to the manipulator, when the manipulator launches the "Shortest-Path Export-All" attack strategy on BGP. Probability is taken over a randomly chosen manipulator, and victim from one of the three classes above.

We make the surprising observation that the "Tier 2" ASes ("> 25 Customers") tend to be *less vulnerable* than "Tier 1" ASes ("> 250 Customers), despite the fact that the "Tier 1" ASes tend to be more central and richly connected! To explain this, we once again observe that despite their centrality, Tier 1 ASes are always providers or peers of their neighbors, so that their neighbors will prefer (potentially longer) customer paths that lead to a manipulator at the edge of the internetwork, over a shorter path to legitimate victim Tier 1 ASes. On the other hand, Tier 2 ASes are the customers of the Tier 1s; thus, when they are the victims of an attack strategy, their Tier 1 neighbors, and the customers

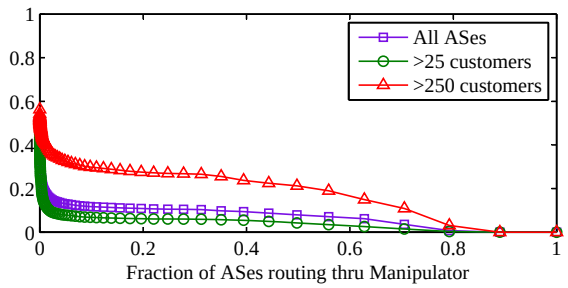


Figure 10: "Shortest-Path Export-All" attack strategy on S-BGP for different victims.

of these Tier 1s, will tend to prefer the short customer path to the victim (a Tier 2), over the longer path to a manipulator (at the edge of the internetwork). We also note that smaller ASes (represented by the curve corresponding to "All ASes") tend to be the most vulnerable to the "Shortest-Path Export-All" attack strategy on BGP, since legitimate paths to these ASes tend to be slightly longer than the paths to the larger, more central ASes.

The results are even more surprising when we look at soBGP and S-BGP/data-plane verification:

Figure 10: This is the CCDF for S-BGP/data-plane verification (*cf.,* to Figure 9). While the "Tier 2" ASes remain the least vulnerable (for the reasons we discussed above), here we see that the "Tier 1" ASes are even more vulnerable than the smaller ASes at the edge of the internetwork! We explain this roughly as follows: For attacks on S-BGP, the manipulator is forced to announce only available paths that may be quite long. Thus, the amount of traffic he attracts tends to decrease (as compared to the "Shortest-Path Export-All" attack strategy on BGP). Thus, manipulators on the edge of the internetwork tend to attract traffic mostly because (by **LP**) other ASes prefer (possibly long) customer paths over any non-customer paths. Next, because Tier 1 ASes *have no providers*, Tier 1 victims *cannot* rely on the fact that other ASes prefer customer routes in order to attract traffic to their network; thus, their legitimate routes tend to be less preferable than the ones announced by manipulators at the edge of the internetwork. By contrast, smaller ASes and Tier 2s do have providers, and these providers will prefer *shorter, legitimate* customer paths to the smaller ASes and Tier 2s, rather than *longer* customer routes to manipulators at the edge of the internetwork.

Even when there is soBGP or S-BGP or data-plane verification (but no defensive filtering), the "Tier 1" ASes remain surprisingly vulnerable to attack by stub ASes. (See also Section 6.1 for a detailed example of this type of attack.)

4.10 Summary.

In some sense, the results of this section suggest that secure routing protocols like S-BGP and soBGP are only dealing with one half of the problem: while they do restrict *the path* the manipulator can choose to announce, they fail to restrict his *export policies*. Indeed, because defensive filtering restricts both the export policies and the paths announced by stubs, we find that it provides a level of protection that is at least comparable to that provided by S-BGP, and even data-plane verification, alone.

Even if we eliminate attacks by stubs via defensive filter-

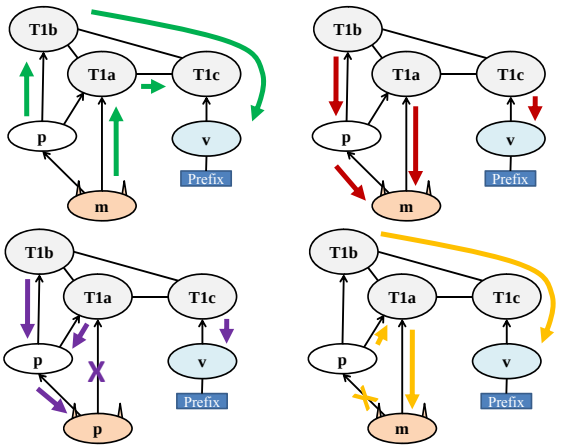


Figure 11: (a) Normal outcome. (b)-(d) Blackhole.

ing, Figures 7 - 8 show that the internetwork is still vulnerable to non-stub ASes that both (a) deviate from normal routing policies by announcing shorter paths, and (b) deviate from normal export policies by announcing non-customer paths to *all* their neighbors. Furthermore, we have seen that it is exactly these non-stub ASes (and in particular, the Tier 2s) that are in the position to launch the most devastating attacks. The success of these attack strategies can be limited with soBGP, S-BGP, or data-plane verification.

5. SMART INTERCEPTION ATTACKS

We now turn our attention to traffic interception attacks [2, 3, 5]. In an interception attack, the manipulator would like to attract as much traffic as possible to his network (in order to eavesdrop or tamper with traffic) before forwarding it on to the victim IP prefix. Thus, we require that an interception attack *preserves an available path from the manipulator to victim.*

5.1 A stub that creates a blackhole.

To provide some intuition, we first show how a manipulator could lose a working path to a victim:

Figure 11: For simplicity, let's consider an attack on BGP where the manipulator falsely originates the victim's prefix. The manipulator m is a web-hosting company in Illinois, and wants to attract traffic destined for the victim v a web-hosting company in France. The manipulator is a multi-homed stub with two providers, a Tier 1 AS $T1a$, and a Chicago-area telecom provider p. The left figure shows the normal outcome, where the manipulator has a path to victim available through each of his providers. The right figure shows what happens when the manipulator announces the victim's prefix to each of his providers; since each of them prefer short customer paths, they will forward their traffic through the manipulator. The manipulator has now created a *blackhole*; he has no available path to the victim v through either of his providers.

Suppose now that the manipulator tried to be a little more clever, and did *not* announce the victim's prefix to his Tier 1 provider $T1a$. Unfortunately for the manipulator, this strategy still creates a blackhole. As show in the bottom left (purple) figure, $T1a$ will prefer his customer path through manipulator ($T1a$, p, m, Prefix) over his peer path to the legitimate prefix ($T1a$, $T1c$, v, Prefix). Thus, both the manipulator's providers will still forward their traffic to the manipulator, and the blackhole remains. It is easy to see that a blackhole also occurs when the manipulator only announces the victim prefix to his Chicago provider p (see the bottom right (orange) figure).

To preserve a path of type...	May announce to neighboring... Customers	Peers	Providers
Customer	✓*	✓*	✓
Peer	✓*	✓*	X
Provider	✓	X	X

Table 1: Guidelines for interception.

5.2 When do interception attacks succeed?

The reader may be surprised to learn that there are many situations in which blackholes are *guaranteed not to occur*. We can prove that, within our model of routing policies, the manipulator can aggressively announce paths to certain neighbors while still preserving a path to the victim:

THEOREM 5.1. *Assume that **GR1** holds, and that all ASes use the routing policies in Section 2.2. Suppose the manipulator has an available path through a neighbor of a type x in the normal outcome. If there is ✓ in entry (x, y) of Table 1, then a path through that neighbor will still be available, even if the manipulator announces* any *path to* any *neighbor of type y.*

Appendix G presents the proofs. We also not that the results marked with ✓* hold even if the internetwork does not obey **GR1**. We also observe that this theorem is 'sharp'; if there is an X in entry (x, y) of Table 1, we show by counterexample that the manipulator *can sometimes* lose an available path of type x if he announces certain paths to a neighbor of type y. Indeed, Figure 11 is a counterexample that proves the X in the lower-right entry of Table 1.

Results of this form were presented in an earlier work [2]. However, [2] claims that a peer-path *cannot* be lost by announcing to a provider (and vice versa). In Appendix E we present an example contradicting this, that proves the remaining X entries in Table 1.

Tier 1s and Stubs. Theorem 5.1 leads to a number of observations, also noted by [2]. First, interception is easy for Tier 1s. Since Tier 1s have no providers, they need only concern themselves with the four upper-left entries in Table 1, which indicate that they can announce paths to all their neighbors. Secondly, interception is hard for stubs. A stub's neighbor is always a provider, putting it in the bottom-right entry of Table 1, indicating that aggressive announcements could cause a blackhole (*e.g.,* Figure 11).

5.3 When do "Shortest-Path Export-All" attack strategies cause a blackhole?

The observations of Section 5.2 are borne out by our experiments. Recall that in the "Shortest-Path Export-All" attack strategy, the manipulator announces his shortest (non-rejected) to *all* of his neighbors. We now show that this simple attack strategy often allows the manipulator to intercept traffic without creating a blackhole:

Figure 12: We show the probability that the manipulator has some available path to the victim if he uses the "Shortest-Path Export-All" attack strategy for each of the four BGP

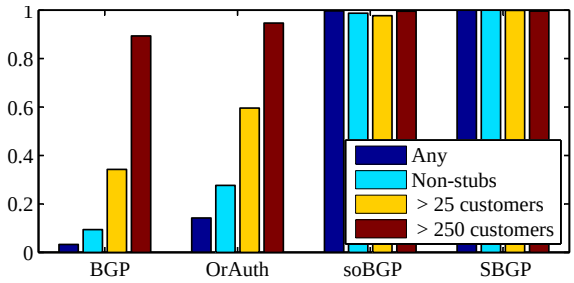


Figure 12: Probability that the "Shortest-Path Export-All" attack strategy does *not* create a blackhole.

security variants. We present results for a randomly-chosen victim, and a manipulator chosen from the usual four classes (see Figure 4). We assume that manipulator runs the "Shortest-Path Export-All" attack strategy on each BGP security variant. We can make a number of observations:

1. Manipulators with the *most* customers are *least* likely to create a blackhole. As discussed in Section 5.2, these manipulators are most likely to have an available customer path to the victim, and as shown in the first row of Table 1, can get away with announcing to *all* their neighbors without creating a blackhole.

2. The attack on BGP is most likely to cause a blackhole (*cf.,* the attack on origin authentication, or soBGP). Because the manipulator announces a more attractive (*i.e.,* short) path, he is more likely to convince *all* of his neighbors to forward traffic to him, and thus create a blackhole.

We note that our empirical results generally agree with Theorem 5.1; whenever there was a gap between the two, we found a customer-provider loop (*i.e.,* a violation of **GR1**) in the AS graph that we used for running our simulations. We are not particularly troubled by this gap, since the algorithms used to produce AS relationship graphs from empirical data [11,12] sometimes introduce artifacts like customer-provider loops.

5.4 Interception by announcing available paths.

Figure 12 and other simulation results (not shown), also indicate that the "Shortest-Path Export-All" attack strategy on S-BGP, *never* creates a blackhole (as long as the manipulator had a path to the victim in the normal outcome). This observation matches intuition; since S-BGP forces the manipulator to announce an available path, the manipulator must of course have an available path to the victim! Indeed, we conjecture that it is possible to prove a more general statement that implies *every* successful attraction attack strategy on S-BGP is also an interception attack. That is, suppose ASes use the routing policies in Section 2.2 and **GR1** holds, and consider *any* path P that is available to the manipulator in the normal outcome. Then path P remains available if the manipulator announces P to *any* subset of his neighbors. We leave the proof of such a statement to future work.

5.5 Two interception strategies.

Figure 12 immediately suggests a simple interception strategy that seems to work every time:

"Shortest-Available-Path Export-All" attack strategy: The manipulator should announces his shortest *available* path from the normal outcome to all his neighbors. Recall that this is exactly the "Shortest-Path Export-All" attack strategy on S-BGP.

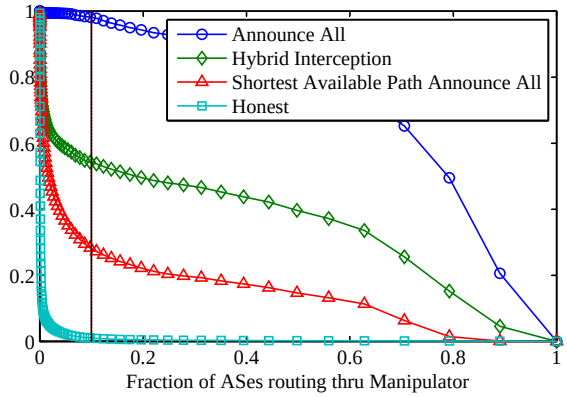


Figure 13: Interception attacks on BGP.

Figure 3, shown that this strategy attracts more traffic than the normal strategy, but also suggests that when the network does *not* use S-BGP, there may be better interception attack strategies. Indeed, Figure 12 shows that there is a non-trivial probability that the manipulator has an available path to the victim, even if he launches the "Shortest-Path Export-All" attack strategy on the BGP. This suggests the following two-phase strategy:

"Hybrid Interception" attack strategy: First, run the "Shortest-Path Export-All" attack strategy on the secure routing protocol, and check if there is an available path to the victim. If no such path is available, announce the shortest path that was available in the normal outcome to all neighbors.[5]

By no means do we believe that these two strategies are optimal; indeed, while we evaluated more clever attack strategies, we omitted them here in the interest of brevity and simplicity. What is surprising is that even these trivial strategies can be quite effective for certain manipulators.

5.6 Evaluating interception strategies.

From the discussion above (Figures 11 and 12, Section 5.2), it is clear that ASes with very few customers are unlikely to attract large volumes of traffic without blackholing themselves. For this reason, we focus our evaluation on manipulators with at least 25 customers, and for brevity only present attacks on BGP:

Figure 13: This is a CCDF of the probability that at least a x-fraction of the ASes in the internetwork forward traffic to the manipulator, under the assumption that the network uses BGP. We compare the (a) "Shortest-Path Export-All" attack strategy where the manipulator *is allowed to create a blackhole* (and thus tends to attract more traffic than the interception strategies above), with (b) the two interception strategies above, as well as (c) the normal strategy. Our key observation is that the "Hybrid Interception" attack strategy

[5]We note that while this strategy will attract at least as much traffic as the "Shortest-Available-Path Export-All" attack strategy, the manipulator stands a higher chance of getting caught if he creates a blackhole in the first phase of the strategy.

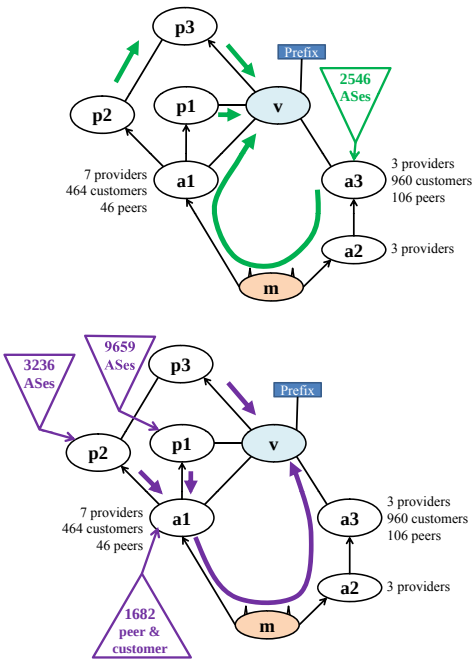


Figure 14: Announcing a longer path.

intercepts a large fraction of traffic; *e.g.,* at least 10% of the ASes in the internetwork with probability over 50%!

5.7 Summary.

On average, traffic interception is difficult for stubs, but a manipulator with many customers can quite easily launch an interception attack. Indeed, manipulators with many customers can intercept a large volume of traffic with even the highly non-optimal "Hybrid Interception" attack strategy. Furthermore, as we shall discuss in Section 6, there may be more clever traffic interception attacks that allow the manipulator to attract even larger portions of the internetwork, and some of these strategies may even work for stubs (*e.g.,* Figure 14)!

6. SMART ATTACKS ARE NOT OPTIMAL

We now prove that the "Shortest-Path Export-All" attack strategy is *not* optimal for the manipulator. We present three surprising counterexamples[6], found in CAIDA's AS graph and then anonymized, that show that (a) announcing *longer* paths can be better than announcing shorter ones, (b) announcing to *fewer* neighbors can be better than to announcing to more, and (c) the *identity* of the ASes on the announced path matters, since it can be used to *strategically trigger BGP loop detection.* In fact, (c) also proves that announcing a longer path can be better than a prefix hijack (where the manipulator originates a prefix he does not own)!

6.1 Attract more by announcing longer paths!

Our first example is for a network with soBGP, S-BGP or data-plane verification. We show a manipulator that *triples* his attracted traffic by announcing a *legitimate path to the victim, that is* not *his shortest path.* (This contradicts the optimality of the "Shortest-Path Export-All" attack strategy, which requires announcing shortest paths.) In fact, this strategy is so effective, that it attracts almost as much traffic as an aggressive prefix hijack on unmodified BGP!

Figure 14: The manipulator m is a small stub AS in Basel, Switzerland, that has one large provider $a1$ that has almost 500 customers and 50 peers, and one small provider AS $a2$ in Basel that has degree only four. The victim is European broadband provider v with over 100 customers and 26 peers.

Prefix hijack. In a network with (unmodified) BGP, the manipulator could run a simple prefix hijack, announcing "m, Prefix" to both his providers, and attract traffic from 62% of the ASes in the internetwork (20550 ASes), including 73% of ASes with at least 25 customers, and 88% of ASes with at least 250 customers. However, this strategy both creates a blackhole at the manipulator, and fails against soBGP or S-BGP.

Naive strategy. The upper (green) figure shows the "Shortest-Path Export-All" attack strategy, where the manipulator naively announces a *three-hop* available path, (m, $a1$, v, Prefix) to his provider $a2$. Since ASes $a2$ and $a3$ prefer the customer path that leads to the manipulator, over their existing peer paths, both will forward traffic to the manipulator. He intercepts traffic from 16% of the ASes in the internetwork (5569 ASes), including 25% of ASes with at least 25 customers, and 41% of ASes with at least 250 customers.

Clever strategy. The lower (purple) figure shows the manipulator cleverly announcing a *four-hop* available path (m, $a2$, $a3$, v, Prefix) to his provider $a1$. The large ISP $a1$ will prefer the longer customer path through the manipulator over his shorter peer connection to victim v, but this time, the manipulator *triples* the amount of traffic he attracts, intercepting traffic from a total of 56% of the ASes in the internetwork (18664 ASes), including 69% of ASes with at least 25 customers, and 85% of ASes with at least 250 customers. In fact, *by announcing a longer path, the manipulator earns almost as much traffic as the aggressive prefix hijack.*

Why it works. Notice that the manipulator's large provider $a1$ has hundreds more neighbors then his small provider, $a2$, and that the clever strategy attracts large ISP $a1$'s traffic while the naive strategy attracts small AS $a2$. Attracting traffic from the larger AS is crucial to the manipulator's success; in fact, it is more important than announcing short paths.

Details. Figure 14 shows that in the naive (green) strategy, large ISP $a1$'s two providers $p1$ and $p2$ route along *peer* paths that do not go through the manipulator, and can thus announce paths to their customers only. On the other hand, in the clever strategy, large ISP $a1$'s two providers $p1$ and $p2$ use *customer* paths through the manipulator; as such, they can announce paths to their customers, peers and providers, and each carry a large volume of traffic (from almost 13K ASes). Thus, in clever (purple) strategy, the manipulator attracts traffic from almost 1.7K ASes that route through large ISP $a1$ along customer or peer paths, as well as 13K ASes that route through ISP $a1$'s providers, ASes $p1$ and $p2$. On the other hand, in the naive (green) strategy, the manipulator attracts traffic from about 2.5K ASes that are AS $a3$'s customers, peers and providers; these 2.5K ASes do not route through the manipulator when he uses the clever (purple) strategy. Thus, in the naive (green) strategy, the

[6]Each example was chosen to contradict the optimality of one aspect of the "Shortest-Path Export-All" attack strategy.

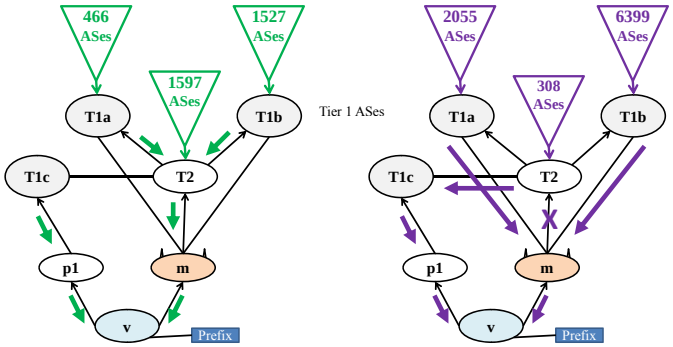


Figure 15: Exporting less.

attacker gains traffic from 2.5K ASes, while in the clever (purple) strategy on the right, the manipulator gains traffic from about 3.2K + 9.6K + 1.7K ASes, for a difference of 3.2K + 9.6K + 1.7K - 2.5K = 12K ASes. The basically accounts for the fact that the naive strategy on the right attracts traffic from only 5K nodes, while the clever strategy attracts traffic from 18K nodes.

When it works. This strategy only involves deviating from normal export policy, rather than *lying* about paths. Thus, it succeeds against *any* secure routing protocol (except when it is launched by stubs in a network with defensive filtering).

6.2 Attract more by exporting less!

This example is for a network with origin authentication, soBGP, S-BGP, data-plane verification, and/or defensive filtering. We show a manipulator that intercepts traffic from 25% *more* of the ASes in the internetwork by exporting to *fewer* neighbors. (This contradicts the optimality of the "Shortest-Path Export-All" attack strategy, which requires exporting to as many neighbors as possible.)

Figure 15: The victim v is a stub serving a liberal arts college in Illinois. The manipulator is a large ISP m, and is competing with the victim's other provider $p1$, a local ISP in Illinois, to attract traffic destined for v.

Naive strategy. The "Shortest-Path Export-All" attack strategy requires the manipulator to announce his path to all his neighbors. On the left, when the manipulator announces a path to his Tier 2 provider $T2$, both $T2$ and its two Tier 1 providers $T1a$ and $T1b$ will route through the manipulator. As a result, $T1a$ and $T1b$ use *four-hop* paths to the victim, and the manipulator attracts traffic from 40% of the ASes in the internetwork, (13463 ASes), including 44% of the ASes with at least 25 customers, and 32% of ASes with at least 250 customers.

Clever strategy. On the right, the manipulator increases his traffic volume by almost 25%, by *not* exporting to his Tier 2 provider $T2$. Because $T2$ no longer has a customer path to the victim, he is forced to use a peer path through $T1c$. Because $T2$ now uses a peer path, he will not export a path to to the two Tier 1 $T1a$ and $T1b$. The Tier 1s $T1a$ and $T1b$ are now forced to choose shorter *three-hop* peer paths to the victim through the manipulator. Because the $T1a$ and $T1b$ now announce shorter paths to their customers, they become more attractive to the rest of the internetwork, the volume of traffic they send to the manipulator quadruples. Thus, the manipulator attracts 50% of the ASes in the internetwork (16658 ASes), including 59% of the ASes with at least 25 customers, and 29% of ASes with at least 250 customers.

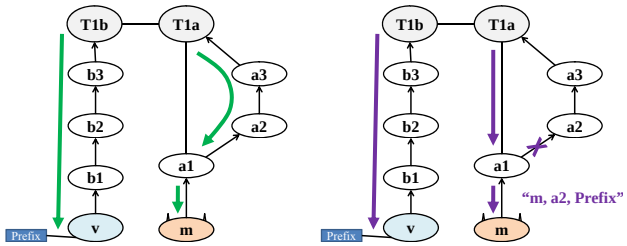


Figure 16: False loop prefix hijack.

Why it works. The manipulator's strategy forces influential ASes (*i.e.,* Tier 1s) to choose *shorter* peer paths over *longer* customer paths. He does this by *suppressing* announcements to certain providers, thus eliminating certain customer paths from the internetwork.

Details. To account for change in traffic through the manipulator, notice that in the naive (green) strategy, the manipulator m attracts traffic from about 0.5K ASes that route through Tier 1 $T1a$ and 1.5K ASes that route through $T1b$, and 1.6K other ASes that route through $T2$. In the clever (purple) strategy on the right, the two Tier 1's $T1a$ and $T1b$ announce shorter paths and attract traffic from a total 8.4K ASes. Meanwhile, $T2$, who no longer forwards traffic through the manipulator, only attracts traffic from about 300 ASes; this sharp decrease in traffic flowing through $T2$ follows from the fact that in the clever strategy, $T2$ uses a *peer* path to the victim, and thus will no longer accept traffic from its peers and providers. Thus, in the clever strategy, the attacker gains traffic from 8.4K - .3K ASes, and in the naive strategy the attacker gains traffic from .5K + 1.5K + 1.6K ASes, for a difference of 4.5K ASes; this roughly accounts for the 25% increase in the number of ASes that the manipulator attracts by using the clever strategy.

When it works. This strategy only involves using a clever export policy, rather than lying about paths, and therefore succeeds against *any* protocol, including data-plane verification.

6.3 Attract more by gaming loop detection!

To show that the identity of the ASes on the announced path can affect the amount of attracted traffic, our last example involves gaming BGP loop detection. (This contradicts the optimality of the "Shortest-Path Export-All" attack strategy, which suggests announcing *any shortest path*, regardless of the identity of the ASes on that short path.) While gaming loop detection was explored in other works, *e.g.,* [3–5], what is remarkable about this example is that it proves that this attack strategy *can attract more traffic than an aggressive prefix hijack.*

Figure 16: The manipulator m is a stub in Clifton, NJ with two providers. This figure only depicts his NJ-area provider, $a1$. The manipulator wants to blackhole traffic destined for a prefix owned by the victim v, a stub in Alabama.

Standard prefix hijack. The manipulator announces the path (m, Prefix) and attracts traffic from most of the ASes in the internetwork, exactly 32010 ASes. Notice also that because Tier 1 $T1a$ prefers customer paths, he will

choose to forward his traffic along the *five-hop* customer path through the manipulator.

False loop prefix hijack. The manipulator claims that *innocent* AS $a2$ originates the prefix, announcing (m, $a2$, Prefix) to his provider $a1$. However, when this *false loop* is announced to AS $a2$, BGP loop detection will cause $a2$ to reject the path through the manipulator's provider $a1$. As a result, the Tier 1 $T1a$ has no customer path to the prefix, and instead chooses the shorter peer path. Now, $T1a$ announces a shorter, *four-hop* path to his neighbors ($T1a$, $a1$, m, $a2$, Prefix), making him more attractive to the rest of the internetwork, and attracting more traffic to the manipulator. For this, and other reasons that are discussed in Appendix D, the manipulator attracts 360 more ASes than standard prefix hijack, *i.e.,* 32370 ASes.

Why it works. The manipulator games BGP loop detection, effectively 'removing edges' from the network (*i.e.,* the edge between $a1$ and $a2$), to force large ISPs to choose shorter peer paths over longer customer paths.

When it works. This strategy involves lying about the path announced by an innocent AS (*i.e.,* AS $a2$). Because S-BGP and data-plane verification prevent lying about paths, this strategy only works with BGP, origin authentication, or soBGP.

6.4 How realistic are these examples?

While all the counterexamples we presented were found in CAIDA's AS graph, we encourage the reader to view these examples as sample attack strategies that *could* succeed in the wild, rather than predictions of what would occur if a *specific* AS was to launch a given attack strategy. Indeed, any missing edge or wrongly inferred business relationship in CAIDA's dataset introduces a gap between what happens between the *actual ASes* depicted in each counterexample, and what would really happen if these attack strategies were launch by *these specific ASes* in practice on the Internet.

How common are these examples? Each of our counterexamples is induced by a very particular AS graph topology. Our objective in this section is not to argue that these examples are common; indeed, we had to work hard to find them. Instead, our goal is to contradict the optimality of the "Shortest-Path Export-All" attack strategy, and to argue that the attack strategies to contradict its optimality could realistically occur in the wild. That said, we speculate that the strategy of Section 6.1 succeeds most often in practice (*i.e.,* strategically attracting traffic from influential ASes instead announcing short paths).

Peering with indirect customers. Both Figures 15-16 rely on the existence a pair of ASes (p, c), such that c is both a *peer* of p, and also an *indirect customer* of p (*i.e.,* ASes $(T1a, m)$ and $(T1b, m)$ in Figure 15 and ASes $(T1a, a1)$ in Figure 16). While this topology may initially seem strange, since it requires an AS p near the top of the customer-provider hierarchy to peer with a smaller AS c lower down in the hierarchy, there are a number reasons why this it could occur in practice:

1. The Internet evolves over time. Thus, AS c could have started out as a small, insignificant, indirect customer of the large ISP p. Over time, c could have increased its connectivity to the point where the large ISP p is willing to establish a peer connection with c. Meanwhile, c's direct provider may be unwilling to change their relationship.

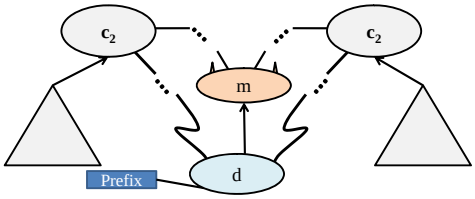


Figure 17: DILEMMA for proving hardness.

2. Many ASes today increase their connectivity by adopting an "open" peering policy, where they seek to establish peering relationships with *all* possible ASes, regardless of their position in the Internet hierarchy, or the amount of traffic flowing across the link. (This peering strategy is facilitated via connections through Internet Exchange Points (IXPs) [13, 20].)

Finally, we mention that we found multiple instances of these topologies in our datasets. Both 'triangular' topology formed ASes $(T1a, T2, m)$ in Figure 15, and the 'trapezoid' topology formed by ASes $(T1a, a3, a2, a1)$ in Figure 16 were found in each of our datasets [11] and [12, 13] approximately 2000 times.

7. FINDING OPTIMAL ATTACKS IS HARD

After all the bizarre attack strategies in Section 6, the reader might not be surprised by the following:

THEOREM 7.1. *If ASes use the routing policies of Section 2.2, then finding a manipulator's optimal traffic attraction attack strategy on a general AS graph is NP-hard.*

This theorem holds for (a) any of the secure protocols variants and (b) also covers interception attacks; our proof uses a reduction to the standard NP-hard problem of finding the maximum independent set of nodes in a graph. We also show that it is hard to *approximate* the optimal attack within a constant factor *i.e.,* we cannot even design an algorithm that gets "close" to the optimal attack on a general AS graph. This suggests that a full characterization the manipulator's optimal attack strategy will remain elusive.

We present a version of this theorem that shows that in the case of BGP, origin authentication, or soBGP, it is hard for the manipulator to decide *which path* to announce to each neighbor. (The result holds even if the manipulator has a small constant number of neighbors.) On the other hand, the reader might suspect that the finding the optimal attack strategy becomes *easier* if the manipulator is only allowed to announce an *available* path, as with S-BGP. Surprisingly, this is not the case; we present another version of this theorem that shows that even if the manipulator is forced to announce his *normal path*, it is still hard for him to choose *the optimal set of neighbors to announce paths to.* (This last result is meaningful only when the manipulator has a large number of neighbors.)

Proof sketch (Fig. 17). Our proof, in Appendix F, proceeds in two stages. First, we present a special internetwork topology 'gadget' called DILEMMA, and then we use the DILEMMA gadget to reduce from our problem (*i.e.,* finding the most damaging traffic attraction strategy) to the standard NP-hard problem of finding the maximum independent set of nodes in a graph. Then, we show how a DILEMMA can exist for the different secure routing protocols considered

in this paper. In a DILEMMA internetwork (Figure 17), the manipulator m wants to attract the traffic for the victim d from two influential ASes c_1 and c_2, whose carry traffic from the majority of the network. A DILEMMA construction must guarantee that m can attract each of the ASes individually, but cannot attract both ASes simultaneously.

8. RELATED WORK

Previous papers have proposed security extensions to BGP (see [5] for a survey). These papers typically use a particular attack model to analyze the proposed protocol, and compare it to BGP, but understandably do not address attacks outside of their model, like traffic-attraction attacks.

Recent theoretical work [4, 21] considers strategic attacks launched by economically-motivated ASes. These papers construct example topologies—sometimes quite contrived—where an AS can manipulate a particular variant of BGP. However, these papers do not define a specific attack strategy, investigate the optimality of attacks, or demonstrate whether the example topologies exist in practice. In contrast, we evaluate attacks on an empirically-measured AS-level topology, and show that our counterexamples are realistic by finding them in the AS level topology.

There have been many works that empirically investigate attacks on BGP (see [5] for a survey). Our work is most closely related to an earlier study of prefix-hijack and interception attacks [2]. While [2] focuses on (unmodified) BGP and two specific attacks (i.e., prefix-hijack and invalid-next-hop attacks), we consider attacks against a variety of secure routing protocols. We show that the attacks considered in [2] are suboptimal (Section 6.3), and prove that finding the the optimal attack is NP-hard. The work in [2] suggests guidelines for interception similar to the ones we present in Table 1. However, our guidelines correct an error in [2]'s earlier paper (see Section 5.2).

Our work is also related to earlier work [22], that compares several BGP security protocols under *partial* deployment. In contrast, we focus on a *full* deployment, using a model that captures realistic routing policies. However, [22] considers a simplified model that ignores business relationships, and instead assumed that normal ASes prefer shortest paths and export paths to all neighbors. This simplification means that soBGP and S-BGP are the same within their model, making it difficult to compare across protocols.

9. IMPLEMENTATION ISSUES

Many of our results compare the efficacy of defensive filtering to that of soBGP and S-BGP. However, these mechanisms differ greatly in (a) the number of ASes that use them on the Internet today, as well as (b) the trust model for which they were designed.

Origin authentication with RPKI/ROA. The operations community is currently working towards deploying origin authentication, by developing a Resource Public Key Infrastructure (RPKI) to issue cryptographic public keys to ASes and routers, and Route Origin Authorizations (ROAs) to map the IP address space to owner ASes [7]. This infrastructure is a first step towards deploying soBGP or S-BGP.

Defensive filtering in practice. While defensive filtering is considered a best common practice on the Internet today, and is anecdotally known to be used by several large ISPs, its implementation is far from perfect. First, the incentives to implement defensive filtering are lopsided; in some sense, the provider derives little local benefit for *itself or its customers*, and is instead altruistically protecting the *rest of the Internet* from attacks. Secondly, the provider has to manually maintain up-to-date "prefix lists" of the IP addresses owned by each of its stub customers. To address the second issue, we suggest that RPKI and ROAs are used by each provider to *automatically* derive prefix lists for their stub customers.

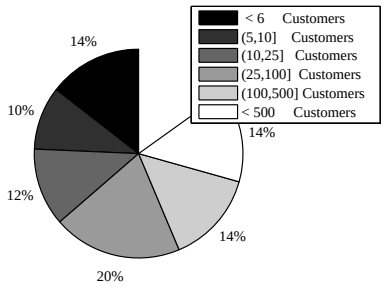


Figure 18: Distribution of stubs, according to the size of their smallest provider.

What if only large ASes filter? Thus far, we considered a perfect world in which *every* provider implements defensive filtering, including tiny ASes with only a few customers. In the following, we consider what happens when only the *large* ASes filter announcements from their stub customers:

Figure 18: Attacks by a given stub are thwarted only if *all* its providers implement defensive filtering. Thus, we presents a pie chart of the stubs (*i.e.,* ASes with no customers), breaking them up by the *size* of their *smallest* provider. First, note that we present only 85% of the pie; the other 15% of ASes in the internetwork are non-stubs. Thus, the figure shows that if only providers with more the 500 customers were to implement defensive filtering, then attacks by 14% of the ASes in the internetwork would be eliminated (the white slice of the pie only). Similarly, if only providers with more than 25 customers filter, then attacks by $14\% + 14\% + 20\% = 48\%$ of ASes in the internetwork would be eliminated. Thus, reasonable improvements can be obtained even if only the "Tier 2s" (ISPs with more than 25 customers) implement defensive filtering.

Trust models. Moreover, we caution that defensive filtering operates in a problematic trust model. Because it is a purely *local mechanism* at each provider, there is no known way for an AS to validate that another AS has implemented defensive filtering properly. This trust model essentially amounts to assuming that *every provider is honest.* This is in contrast to the trust model used in S-BGP and soBGP; S-BGP, for instance, ensures than even a malicious AS may only announce available paths (as long as it does not collude with, or comprise the keys of, some other AS), and also allows any AS to validate the paths announced by any other AS.

10. CONCLUSIONS

Because we work within a *model* of routing policies, we caution against interpreting our results as *hard numbers* that measure the impact of an attack launched by a *specific* manipulator in the wild. However, the *trends* uncovered by our quantitative analysis do allow us to arrive at a number of

useful insights; indeed, many of these insights are obtained by *averaging* over multiple possible (manipulator, victim) pairs, and we suspect that they hold up even if some ASes deviate from the policies in our model. Furthermore, the trends we identified were remarkably consistent across multiple AS topology datasets [11–13]. That said, future work might look into how our results hold up under different routing policy models; *e.g.,* assuming that some fraction of ASes in the network use simple shortest path policies, while the rest use those of Section 2.2, or assuming that some ASes equally rank peer- and provider-paths.

While secure routing protocols can blunt traffic attraction attacks, we found that *export policies* are a very effective attack vector that these protocols do not address. Thus, we suggest that secure routing protocols (*e.g.,* soBGP and S-BGP) should be deployed *in combination* with mechanisms that police export policies (*e.g.,* defensive filtering). We believe both are needed; defensive filtering to eliminate attacks by stub ASes, and secure routing protocols to blunt attacks launched by larger ASes, (especially since we found that large ASes can launch the most damaging attacks). We note, however, that policing export policies is a significant challenge in practice. Defensive filtering of stubs requires voluntarily compliance from each provider, and it is difficult to check for proper implementation (as evidenced by recent events [23]). Moreover, given the complexity of routing policies used in practice on the Internet, we lack even a *definition* of what it means to deviate from normal export policies. Thus, while anomaly-detection techniques that flag suspicious routes [17, 19] could help, understanding these issues remains an important avenue for future research.

Acknowledgments

The authors thank Jeff Lupien and Paul Oka for outstanding research assistance, and Boaz Barak, Randy Bush, Kevin Butler, Nick Feamster, Avinatan Hassidim, Elliott Karpilovky, Arvind Krishnamurthy, Dave Ward, Dan Wendlandt, the members of the MSR-New England Lab, and the anonymous SIGCOMM reviewers for comments and discussions.

11. REFERENCES

[1] S. Goldberg, M. Schapira, P. Hummon, and J. Rexford, "How secure are secure interdomain routing protocols?," in *ACM SIGCOMM*, 2010.

[2] H. Ballani, P. Francis, and X. Zhang, "A study of prefix hijacking and interception in the Internet," in *ACM SIGCOMM*, 2007.

[3] A. Pilosov and T. Kapela, "Stealing the Internet: An Internet-scale man in the middle attack," Aug. 2008. Presentation at DefCon 16, `http://eng.5ninesdata.com/~tkapela/iphd-2.ppt`.

[4] S. Goldberg, S. Halevi, A. D. Jaggard, V. Ramachandran, and R. N. Wright, "Rationality and traffic attraction: Incentives for honest path announcements in BGP," in *ACM SIGCOMM*, 2008.

[5] K. Butler, T. Farley, P. McDaniel, and J. Rexford, "A survey of BGP security issues and solutions," *Proceedings of the IEEE*, January 2010.

[6] P. McDaniel, W. Aiello, K. Butler, and J. Ioannidis, "Origin authentication in interdomain routing," *Computer Networks*, Nov. 2006.

[7] IETF, "Secure interdomain routing (SIDR) working group." http://datatracker.ietf.org/wg/sidr/charter/.

[8] R. White, "Deployment considerations for secure origin BGP (soBGP)." draft-white-sobgp-bgp-deployment-01.txt, June 2003, expired.

[9] S. Kent, C. Lynn, and K. Seo, "Secure border gateway protocol (S-BGP)," *J. Selected Areas in Communications*, vol. 18, pp. 582–592, April 2000.

[10] E. L. Wong, P. Balasubramanian, L. Alvisi, M. G. Gouda, and V. Shmatikov, "Truth in advertising: Lightweight verification of route integrity," in *PODC*, 2007.

[11] X. Dimitropoulos, D. Krioukov, M. Fomenkov, B. Huffaker, Y. Hyun, and kc claffy, "AS relationships: Inference and validation," *ACM SIGCOMM Computer Communication Review*, Jan. 2007.

[12] Y.-J. Chi, R. Oliveira, and L. Zhang, "Cyclops: The Internet AS-level observatory," *ACM SIGCOMM Computer Communication Review*, Oct. 2008.

[13] B. Augustin, B. Krishnamurthy, and W. Willinger, "IXPs: Mapped?," in *Proc. Internet Measurement Conference*, Nov. 2009.

[14] G. Huston, "Interconnection, peering, and settlements," in *Internet Global Summit (INET)*, June 1999.

[15] L. Gao and J. Rexford, "Stable Internet routing without global coordination," *IEEE/ACM Transactions on Networking*, 2001.

[16] L. Gao, "On inferring automonous system relationships in the Internet," *IEEE/ACM Transactions on Networking*, vol. 9, pp. 733–745, Dec. 2001.

[17] J. Karlin, S. Forrest, and J. Rexford, "Autonomous security for autonomous systems," *Computer Networks*, Oct. 2008.

[18] T. Griffin, F. B. Shepherd, and G. Wilfong, "The stable paths problem and interdomain routing," *IEEE/ACM Transactions on Networking*, Apr. 2002.

[19] M. Lad, D. Massey, D. Pei, Y. Wu, B. Zhang, and L. Zhang, "PHAS: A prefix hijack alert system," in *Proc. USENIX Security Symposium*, 2006.

[20] P. Gill, M. Arlitt, Z. Li, and A. Mahanti, "The flattening internet topology: Natural evolution, unsightly barnacles or contrived collapse?," *Proc. of Passive and Active Measurement (PAM) Conference 2008*, April 2008.

[21] H. Levin, M. Schapira, and A. Zohar, "Interdomain routing and games," in *ACM STOC*, May 2008.

[22] H. Chang, D. Dash, A. Perrig, and H. Zhang, "Modeling adoptability of secure BGP protocol," in *ACM SIGCOMM*, Sept. 2006.

[23] Rensys Blog, "Pakistan hijacks YouTube." `http://www.renesys.com/blog/2008/02/pakistan_hijacks_youtube_1.shtml`.

[24] Y. Liao, L. Gao, R. Guerin, and Z.-L. Zhang, "Inter-domain routing under diverse commercial agreements," *IEEE/ACM Transactions on Networking*, 2010.

[25] J. Hastad, "Clique is hard to approximate to within $n^{1-\epsilon}$," *Acta Mathematica*, vol. 182, 1999.

[26] L. Gao, T. Griffin, and J. Rexford, "Inherently safe backup routing with BGP," *IEEE INFOCOM*, 2001.

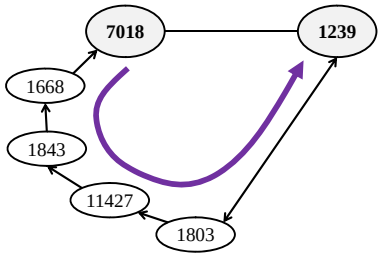


Figure 19: The trouble with siblings.

APPENDIX

A. SIBLINGS

Because some of our results are based on CAIDA's AS graph [11], our model also includes *sibling* relationships, where two different ASes are owned by the same organization.

A.1 Modeling sibling relationships.

A recent paper [24] provides an excellent treatment of sibling-to-sibling relationships that we adapt for our purposes. First, our model of export policies must account for sibling relationships:

GR2s AS b only exports a path via AS c to AS a if at least one of a and c are customers or *siblings* of b.

Our **NE** export rule now uses the modified **GR2s** (see Section 2.2). Next, in addition to considering customer, peer, and provider paths, the work of [24] introduces two new path types:

Sibling down. The first edge(s) on the path are sibling edges, and the first non-sibling edge is a customer-provider edge. A path that contains exclusively sibling edges is also considered sibling down.

Sibling up. The first edge(s) on the path are sibling edges, and the first non-sibling edge a peer-to-peer or provider-customer edge.

Our modified model of local preferences is also based on [24]:

LP s Prefer customer paths, over sibling down paths, over peer paths, over provider paths, over sibling-up paths.

As discussed in [24], captures a type of "hot potato routing", where the AS prefers to send traffic outside its organization rather than carrying it through its own network.

A.2 Sibling rivalry in CAIDA's AS graph.

Sibling-to-sibling relationships seem to be the grand 'fudge-factor' in works that involve AS-level business relationships . CAIDA is the first to acknowledge the challenges of dealing with sibling-to-sibling relationships [11]; their approach is based on manually assigning these relationships to two ASes if they are owned by the same organization. This means that a large AS (*e.g.,* AS1239, with almost 1400 customers) can be a sibling of a tiny AS (*e.g.,* AS1803, with only four customers) if the two are owned by the same organization (*e.g.,* Sprint). The problem this causes is best illustrated by an example.

Figure 19: We show CAIDA's snapshot of the local topology around AS 1239 and AS 1803. Because CAIDA classes AS1803 and AS1239 as siblings, our model suggest that tiny AS 1803 will carry traffic from his provider AS 11427 to the large network of AS 1239; in fact, our model suggests that AT&T Worldnet's Teir 1 AS 7018, that has over 2.2K customers, would route all traffic for AS 1239 over the long customer path through the sibling AS 1803. This is, of course, completely ridiculous. In practice, AS1803 is unlikely to advertise transit paths through AS1239 to any of it's providers; AS 1239 essentially acts like a provider for AS1803, despite the fact that the two ASes are owned by the same organization.

To deal with these unbalanced sibling relationships, we preprocess CAIDA's data as follows:

Sibling preprocessing: We convert sibling-to-sibling relationships to customer-provider relationships when at least one sibling has more then seven customers, and one sibling is at least twice the size of the other sibling.

This approach does remove some of the the artificially long paths we describe above. However, because CAIDA's AS-relationship inference algorithms *starts* by using heuristics to assign sibling relationships, and then proceeds to infer the other relationships, we suspect that these sibling relationships can introduce inaccuracies in the results. On the other hand, these inaccuracies do not seem to matter very much, given that the results we obtained on the preprocessed CAIDA dataset matches well with the results we obtained from the Cyclops dataset that has no sibling edges (see Appendix H).

B. SIMULATION METHODOLOGY

We sketch the algorithms we developed for our simulations.

B.1 Routing tree algorithm.

At the core of our experiments is a *routing tree algorithm* that simulates the paths that each AS will choose to reach a prefix owned by a legitimate destination AS d. The routing tree algorithm assumes that ASes use the routing policies of Section 2.2, and is implemented using a specialized three-stage breadth-first search (BFS) on the AS graph:.

1^{st} *stage.* Our model of routing policies assumes that ASes prefer short path through their customers over all other paths; as such, we first construct a partial routing tree by performing a BFS 'upwards' from the 'root' node d, using only customer-to-provider or sibling-to-sibling edges. If an AS is offered equal length paths through both a customer and a sibling, the BFS forces the node to choose the customer path. (In Figure 20, this amounts to adding edge $(d, 1)$ then $(d, 2)$ then $(1, 3)$).

2^{nd} *stage.* Next, we capture the fact that (1) **GR2** allows only a single peer-to-peer edge to exist on any path through the network, and that (2) nodes prefer short paths through peers over paths through providers. To do this, in the second stage of the algorithm, we use only peer-to-peer edges to connect *new* nodes to the nodes *already added* to the partial routing tree in the 1^{st} stage of the algorithm. (In Figure 20, this amounts to adding edges $(1, 4)$ and $(2, 5)$ but not $(1, 2)$ or $(7, 4)$).

3^{rd} *stage.* Finally, we add provider/sibling up paths. We do this by traversing the existing partial routing tree with a BFS, and adding *new* nodes to the tree using provider-to-customer or sibling-to-sibling edges. (In Figure 20, this

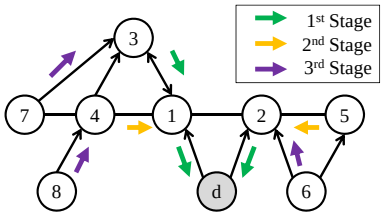


Figure 20: Routing tree algorithm.

amounts to adding edges $(2, 6)$, $(3, 7)$ and finally $(4, 8)$ but not $(3, 4)$). Again, when an AS is offered equal length paths through both a provider and a sibling, the BFS forces the node to choose the provider path.

We capture **TB**, the fact that ASes break ties on AS numbers, by ensuring the that BFS traverses lexicographically by AS number. We capture **NE**, the fact that a node announces a path to *all* of his neighbors (except when forbidden by **GR2**), by running the algorithm above on all the edges in the AS graph.

B.2 Simulating the "Shortest-Path Export-All" attack strategy.

Given a (manipulator, victim) pair (m, d), we use the routing tree algorithm to determine the outcome of each "Shortest-Path Export-All" attack strategy on each secure routing protocol as follows:

BGP. In this attack, both the manipulator m, and the legitimate destination d originate the IP prefix (See Section 3 and 4.1). To simulate this, we run the routing tree algorithm with *two* roots, m and d.

Origin Authentication/soBGP/S-BGP. Observe that this strategy requires the manipulator to announce, *to all his neighbors*, an attack path that is no longer than his shortest available path (see Section 3 and 4.1). We simulate the "Shortest-Path Export-All" attack strategy using the following trick: First, we augment the AS graph with *fake nodes* corresponding to all the ASes on the manipulator's attack path, excluding the manipulator and victim themselves. These fake nodes are given negative AS numbers. Then, we connect the victim to the manipulator via customer-provider edges through these fake nodes. Thus, the *fake path* is always the manipulator's shortest customer path to victim, that is through an AS with lowest possible AS number (a negative number). Thus, our routing policies in Section 2.2 require the manipulator to choose this path. Thus, to simulate the "Shortest-Path Export-All" attack strategy, it suffices to run the routing tree algorithm on the AS graph augmented with the fake path.[7]

C. PATH DISTRIBUTION

As a sanity check of our routing model, we show the distribution of path lengths and path types.

Figure 21: We show the distribution of path length and path type when all ASes behave normally. The distribution is over a randomly-chosen destination, and a source chosen from the same four classes as in Figure 4. We can

[7]To account for BGP loop detection, we also include a simple check in the routing tree algorithm that cause a real node to reject a path that contains it fake counterpart.

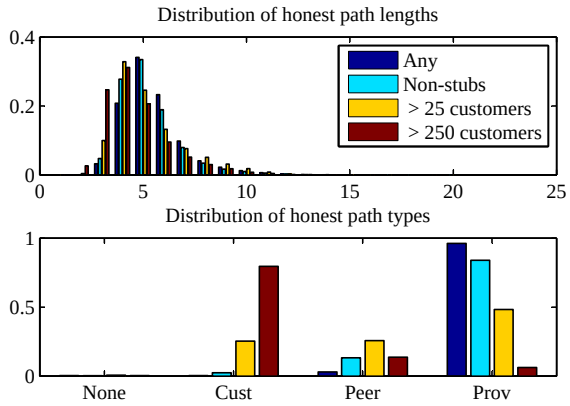


Figure 21: Path length and type distributions

see majority of paths in the internetwork are short (about 5 hops on average), and further that larger ASes tend to have slightly shorter paths. Furthermore, as expected, we find that smaller ASes tend to use provider paths most frequently, while larger ASes tend to use customer paths most often, and that medium sized "Tier 2" ASes with at least 25 customers uses the largest (relative) fraction of peer paths.

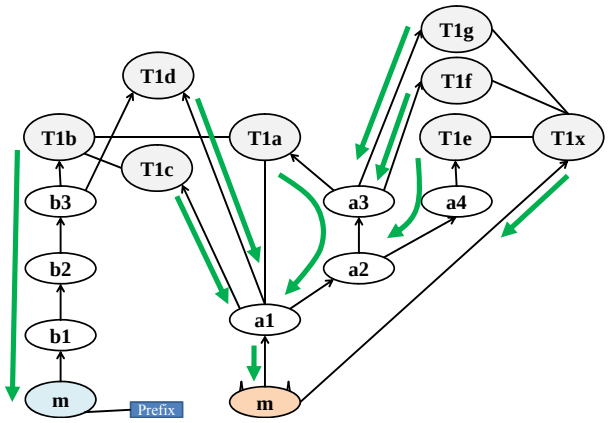
D. CLEVER FALSE LOOPS

We explain the example in Section 6.3 in more detail.

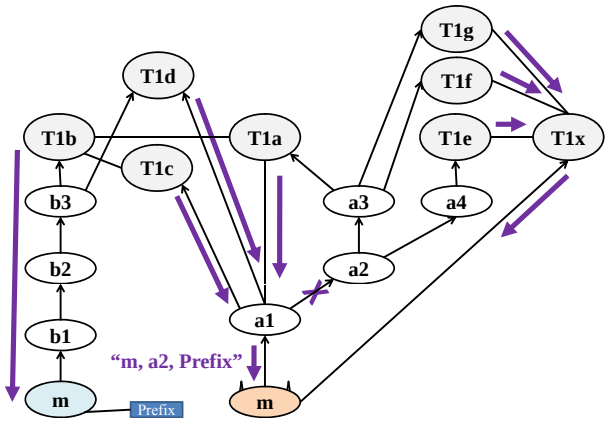
Figure 22(a). Simple Prefix Hijack. In the simple prefix hijack, the manipulator m, a stub in Clifton, NJ, announces the path (m, Prefix) to both of his providers, $a1$ a NJ-area ISP, and $T1x$ a large American backbone provider that is often considered to a be a Tier 1 network. The manipulator manages to attract traffic from most of the Tier 1 ASes in the internetwork. However, many of these Tier 1's, namely $T1a$, $T1e$, $T1f$, and $T1g$, use long, five-hop customer paths to the manipulator. The results of the attack is that the manipulator manages to blackhole traffic from a total of 32010 ASes.

Figure 22(b). False Loop Prefix Hijack. We now show how the manipulator can attract traffic from an additional 360 ASes by using a clever 'false-loop prefix hijack' attack. Now, the manipulator's clever strategy is to announce the path (m, Prefix) to his large provider AS $T1x$, while announcing the false loop (m, $a2$, Prefix) to his other provider AS $a1$. As such, AS $a2$ will no longer forward traffic to his customer $a1$, choosing to forward traffic over an alternate peer path (not shown). Thus, the manipulator has eliminated a customer path from the network, and many of the Tier 1 ASes, including $T1a$, $T1e$, $T1f$, and $T1g$, will be forced to forward traffic over shorter peer paths. (Thus, $T1e$, $T1f$, and $T1g$, now use a three-hop peer path, instead of five-hop customer paths used in the simple prefix hijack.) These ASes now become more attractive to the rest of the internetwork, increasing the volume of traffic flowing through the manipulator to 32370 ASes. Notice that the manipulator's strategy ensures that his provider $a1$ still forwards its traffic to the manipulator. Since quite a few Tier 1 ASes, namely $T1a$, $T1c$, and $T1d$, route through the manipulator's provider $a1$, the false loop prefix hijack strategy ensures that the manipulator does not lose a large amount of traffic by eliminating customer paths from the network.

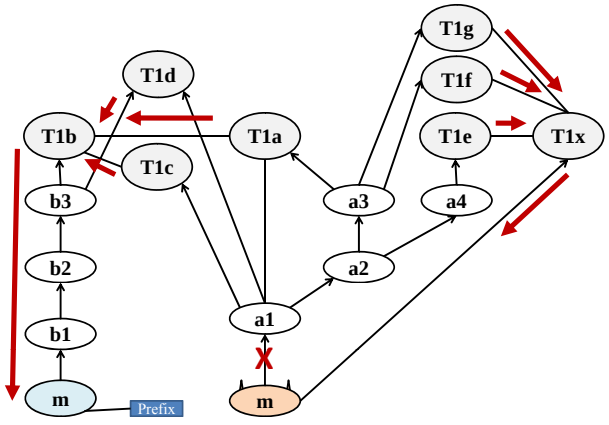
Figure 22(c). Prefix Hijack and Filtering. Now



(a) Simple Prefix Hijack



(b) False Loop Prefix Hijack



(c) Prefix Hijack, Filtering Announcements to $a1$

Figure 22: Using false loops.

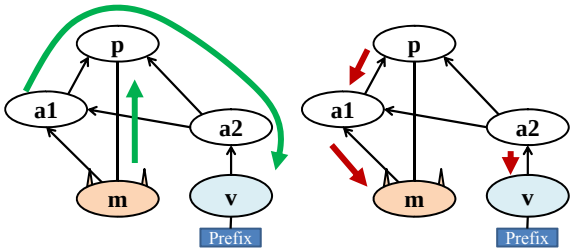


Figure 23: Disrupting a path through a peer.

suppose the manipulator decides to eliminate a customer path from the network by suppressing the announcement to his provider $a1$. By doing this, the manipulator eliminates the customer path used by $T1c$ and $T1d$, as well as the peer path used by $T1a$, and these Tier I ASes will now forward their traffic to the legitimate destination v instead. Thus, the manipulator loses traffic from about 2K ASes, attracting traffic from a total of 30028 ASes, and we find that the manipulator would have been better off if he had used the simple prefix hijack instead.

E. FAILED INTERCEPTION ATTACKS

We provide an example that proves the bottom-middle and middle-right X entries in Table 1, and shows that there is an error in claims made in Section 2.2. of [2].

E.1 Export to provider, disrupt peer path.

We prove that the manipulator can lose a peer path to the victim by announcing an attractive path to his provider:

Figure 23: We consider an attack on BGP, where the manipulator falsely originates the victim prefix. The manipulator m a not-for-profit corporation that fosters science and education in New York State, while the victim v is an ISP providing services to multiple universities in Austria. The manipulator has a a single provider $a1$, a single peer p, and 44 customers (not shown). The left (green) figure shows the normal outcome, where the manipulator has a paths to victim available through both his peer and his provider. The middle (red) figure shows what happens when the manipulator announces the victim's prefix to his provider AS $a1$; now, his peer AS p has *two* available customer paths of equal length. Since AS $a1$ has a lower AS number than AS $a2$, our **TB** rule requires p to choose the path through $a1$ that leads to the manipulator. The manipulator has now "blackholed" himself; both his peer and his provider forward traffic to the manipulator, and none of the manipulator's customers have any path to the victim AS 1853.

E.2 Export to peer, disrupt provider path.

We can also use the example of Figure 23, with a slight modification, to prove that the manipulator can lose a provider path to the victim by announcing an attractive path to his peer. Assume that AS $a1$ has no customer or peer paths, nor any provider paths shorter than two hops, available to the victim v. In that case, if the manipulator *does* announce a path to his peer p, but *not* to his provider AS $a1$, the provider will prefer his two-hop provider path ($a1$, m, Prefix) over any path to the legitimate victim, and again the manipulator creates a blackhole.

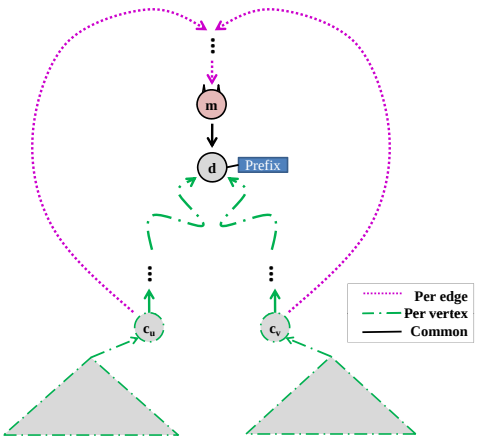


Figure 24: DILEMMA for proving hardness.

F. FINDING OPTIMAL ATTACKS IS HARD

We now show that, from the perspective of the manipulator, finding the optimal traffic attraction attack on BGP is computationally hard. We shall then show that, in fact, not only is finding the optimal attack hard, but even finding a "reasonable" attack, that is "not far" from the optimum, *i.e.,* approximates the optimum, is computationally hard. Our hardness results are obtained via a general proof technique that can be applied to show similar impossibility results for optimal (and approximate) traffic attraction attacks on other security enhancements to BGP (*e.g.,* SBGP, soBGP, and more).

We start by presenting our proof technique. We then show how it can be used to obtain hardness results for traffic attraction attacks on BGP; these results amount to showing that its hard for the manipulator to decide which *paths* to export to which neighbors. We then move on to showing the even if the manipulator is restricted to announcing he normal paths (*e.g.,* because the network uses data-plane verification), that it is still hard for the manipulator to decide which *neighbors to export to.*

F.1 Key Ideas and Outline of Our Proofs.

The DILEMMA network. Our computational hardness results rely on showing the potential existence of the following scenario (see Fig. 17): The manipulator m is directly connected to the destination d. m wishes to attract as much traffic as possible, while all other nodes behave normally. The network contains two nodes, c_u and c_v, each with many direct and indirect customers whose routes to d go only through it. The number of nodes in the trees beneath c_u and c_v, that are of equal size, is significantly bigger than the number of nodes in rest of the network. Hence, m's main goal is to attract c_u and c_v's traffic. However, in our constructions below, m shall always be able to attract *either* c_u's *or* c_v's traffic, but will be *unable* to attract *both* nodes' traffic *simultaneously.* Thus, m will have to choose which one of the two nodes to attract, inevitably losing the traffic of the other node and of all nodes in the subtree beneath it. m's inability to attract both c_u and c_v (alongside its ability to attract each of them alone) shall play a crucial role in our proofs.

Once we prove the existence of a small network as described above, that we term "DILEMMA", we use it as a building block in a reduction from the MAX-INDEP-SET problem, that is a notoriously computationally hard problem.

The MAX-INDEP-SET problem. The MAX-INDEP-SET problem is defined as follows:

DEFINITION F.1 (INDEPENDENT SETS). *Let $G = (V, E)$ be a graph. A subset of the vertices $I \subseteq V$ is an* independent set *if there is no edge in E between two vertices in I.*

DEFINITION F.2 (MAX-INDEP-SET). *In the* MAX-INDEP-SET *problem the input is a graph $G = (V, E)$ and the objective is to find an independent set I of maximum size.*

The following is well known:

THEOREM F.3. *MAX-INDEP-SET is NP-hard.*

Reducing from MAX-INDEP-SET. We now outline our reductions from MAX-INDEP-SET to the problem finding an optimal attack on BGP (or security enhancements to BGP), that establish the computational intractability of the latter.

Given an instance of MAX-INDEP-SET $G = (V, E)$ we construct a network such that computing the traffic-attraction-maximizing attack in the network is equivalent to computing a maximum independent set in G. The node-set in our network contains the destination node d, the manipulator m, and a node c_v for each vertex $v \in V$ (and some additional nodes, as explained below). m is directly connected to d.

We ensure that, for each edge $e = (u, v) \in E$, m shall only be able to attract either c_u's or c_v's traffic, but not both nodes simultaneously, by constructing DILEMMA for c_u and c_v (adding nodes and links appropriately). Importantly, our constructions of DILEMMA gadgets are consistent, in the sense that if the manipulator cannot attract node c_v in one such gadget (because it chose to attract the other node in that gadget), then it also cannot attract c_v in all other DILEMMA gadgets that c_v participates in. Fig. 24 illustrates the vertex-specific, edge-specific, and general components of each DILEMMA constructions (for each pair of neighboring nodes, c_u and c_v, that are connected by an edge (u, v) in E).

Now, consider an attack by m. Observe that because the trees beneath the c_v's constitute the vast majority of the nodes in the network, and because the nodes in the tree beneath each of the c_v's can only connect to d via that node, the success of m's attack is measured by how many of the c_v's it was able to attract. By construction, if two vertices in V, u and v, are connected by an edge in G then m cannot attract both c_u and c_v and thus the vertices corresponding to nodes that m is able to attract form an independent set in G. The converse is also true: Let $I \subseteq V$ be an independent set in G, then m can attract all the c_v's corresponding to vertices in I (because no two such nodes participate in a DILEMMA construction).

Therefore, a maximum independent set in G corresponds to a traffic-attraction-maximizing attack in our network, and vice versa. The NP-hardness of MAX-INDEP-SET (and the fact that our reduction is computationally-efficient) now implies the NP-hardness of finding an optimal attack.

On the hardness of approximating the optimal attack. In fact, the close connections, presented above, between independent sets in G and traffic attraction, when

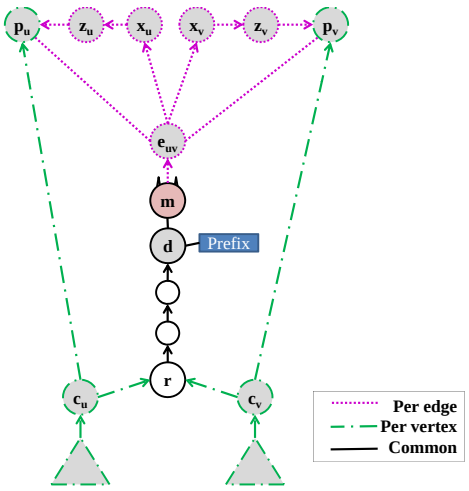


Figure 25: BAT-FROM-HELL-I.

combined with the following theorem, due to Hastad, imply a stronger result.

THEOREM F.4. *[25] Given a graph $G = (V, E)$, finding an independent set of size at least $\frac{OPT}{|V|^{\frac{1}{2}-\epsilon}}$, where OPT is the size of the maximum independent set in G, is NP-hard.*

Using the above theorem, and the exact same construction as before, we can now show that not only is finding the optimal attack computationally-hard, but so is finding an attack that approximates (in terms of number of attracted nodes) the optimal attack within any constant factor!

F.2 Finding Optimal Attacks on BGP is Hard!

We present the following theorems:

THEOREM F.5. *Finding an attack on BGP , that maximizes the traffic volume that goes through that node, is NP-hard.*

THEOREM F.6. *Finding an attack on BGP that approximates the optimal (traffic-volume-maximizing) attack within a constant factor C, is NP-hard for any constant C.*

PROOF SKETCH. The proofs of both theorems follows the outline presented in Sec. F.1. Hence, the main ingredient of the proof is showing the existence of a DILEMMA construction. We shall now present the DILEMMA construction; here, the manipulator's dilemma will be to decide *which path* should be announced to *which neighbors*. His strategy will be similar to the "false loop prefix hijack" of Section 6.3.

The DILEMMA construction. Consider the network in Fig. 25, called "BAT-FROM-HELL-I". m is the node that wishes to attract as much traffic as possible for the victim prefix, while all other nodes behave normally. The network is such that

1. each of the nodes c_u and c_v has a large number of (direct and indirect) customers k in the subtree below it that can only reach d through it. Let k be big enough so that m be much more concerned with attracting c_u and/or c_v than with attracting all other nodes in the drawing;
2. p_u and p_v have lower AS numbers than r. Hence, if faced with a choice between the 4-hop route to d through r and a (false) 4-hop path to the prefix that has either p_u or p_v as next-hops, both c_u and c_v would prefer the latter route.

We now show that while m can attract c_u's traffic, or c_v's traffic, it cannot attract both nodes' traffic simultaneously. To see why this is true, consider node m's options. Observe that for m to attract c_u's (and its customers) traffic, it is necessary that c_u be offered a route of length 4 or less by p_u (because c_u already has an available route of length 4 through r). Recall that nodes prefer customer routes over peer routes (by **LP**) and so p_u prefers routes in which z_u is its next-hop node over routes in which the next-hop node is e_{uv}. Recall that when faced with two customer routes, they prioritize shorter routes (by **SP**). Unfortunately, observe that, no matter what m does, any route from p_u to m that has z_u as a next hop cannot be of length less than 4 (in fact, this is the case even if m hijacks d's prefix and announces it to e_{uv}). Hence, if p_u routes through z_u then c_u's available route through p_u shall consist of at least 5 hops and therefore will not be chosen by c_u.

How can m prevent p_u from routing through z_u? The easiest way is, of course, simply not to announce a route to e_{uv}. However, this will also mean that p_u will not learn of any route that goes through m. To avoid this, m must use a "false loop prefix hijack" strategy as in Section 6.3). He will announce a route to e_{uv} that contains one of the nodes x_u or z_u. By doing so m can ensure that one of these nodes shall not propagate this route further because of BGP's loop detection mechanism, and that p_u still have a loop-free route through m that is announced to it directly by e_{uv}. For example, if m announces mz_ud to e_{uv} then p_u learns the route $e_{uv}mz_u$ from e_{uv} and no route from z_u. Therefore, p_u shall make the route $p_ue_{uv}mz_u$ available to c_u, which, in turn, will choose this 4-hop route. Thus, m can attract c_u's traffic. Similarly, m can attract c_v's traffic by announcing the route mz_v to e_{uv}.

Can m attract both c_u and c_v at the same time? The answer is NO. Recall that to attract c_u m must include one of the nodes in the set $\{x_u, z_u\}$ in its announces route. Similarly, to attract c_v m must include one of the nodes in the set $\{x_u, z_u\}$. However, if m's announced route contains at least one node from each of these sets, and d, then p_u's route must be of length at least 4 and so both c_u and c_v shall not have a 4-hop route through p_u. This will result in both c_u and c_v choosing to forward traffic to r.

The reduction. We prove the correctness of the above two theorems via the arguments in Sec. F.1. We reduce from MAX-INDEP-SET. For every vertex $v \in V$ we create a node c_v. For every edge $e = (u, v) \in E$, we construct a BAT-FROM-HELL-I gadget to ensure that m not be able to attract both c_u and c_v simultaneously. Fig. 25 describes the construction of BAT-FROM-HELL-I for the edge (u, v) (illustrating the per-vertex, per-edge, and common to all gadgets, parts of the construction). Observe that our constructions of BAT-FROM-HELL-I gadgets are consistent, in the sense that if the manipulator cannot attract node c_v in one such gadget (because it chose to attract the other node in that gadget), then it also cannot attract c_v in all other BAT-FROM-HELL-I gadgets that c_v participates in. The arguments in Sec. F.1 now imply the theorems. □

Extending to origin authentication and soBGP. The proof strategy above can easily be extended to attacks on

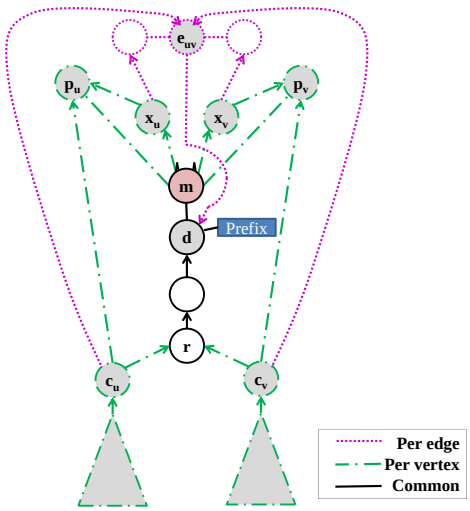


Figure 26: BAT-FROM-HELL-II.

origin authentication by adding more nodes and edges to the BAT-FROM-HELL-I. The modified BAT-FROM-HELL-I construction adds an extra node between r and d in Figure 25, and extra node y_i between nodes x_i and z_i with edges from y_i to nodes m and d. Then we use a similar argument as above to obtain the theorem.

F.3 It's still hard, even if the manipulator must announce normal paths.

The reader might suspect that the computational task shall become much easier if the manipulator is severely constrained by security mechanisms (and hence the space of feasible attacks it must consider is significantly smaller). Surprisingly, this is not the case. We show that the above results hold even if the security mechanism (*e.g.,* data-plane verification) forces the manipulator to announce his *normal path*! We show that finding the optimal attack is computationally hard even if the only decision the manipulator makes is *whether or not to export its normal path* (and thus, the path it actually uses).

THEOREM F.7. *Even if the manipulator may only announce the normal path, finding an attack that maximizes the traffic volume through the manipulator is NP-hard.*

THEOREM F.8. *Even if the manipulator may only announce the normal path, finding an attack that approximates the optimal (traffic-volume-maximizing) attack within a constant factor C, is NP-hard for any constant C.*

PROOF SKETCH. The proofs of both theorems follows the outline presented in Sec. F.1. Hence, the main ingredient of the proof is showing the existence of a DILEMMA construction. We shall now present such a construction.

The DILEMMA construction. Consider the network in Fig. 25, called "BAT-FROM-HELL-II". m is the node that wishes to attract as much traffic as possible, while all other nodes are behaving normally. The network is such that

1. each of the nodes c_u and c_v has a large number of (direct and indirect) customers k in the subtree below it that can only reach d through it. Let k be big enough so that m be much more concerned with attracting c_u and/or c_v than with attracting all other nodes in the drawing;
2. p_u and p_v have lower AS numbers than r. Hence, if faced with a choice between the 3-hop route to d through r and a 3-hop route to d that has either p_u or p_v as next-hops, both c_u and c_v would prefer the latter route.

We now show that while m can attract c_u's traffic, or c_v's traffic, it cannot attract both nodes' traffic simultaneously. To see why this is true, consider node m's options. m is forced to announce its normal path to d, md. Hence, m's only decision is to which neighboring nodes to announce the route md. Observe that if m announces md to x_u, then p_u will choose the customer route $p_u x_u md$ over the peer route $p_u md$ (by LP). This will result in c_u choosing the 3-hop route through r over the 4-hop route through p_u. Similarly, if m announces md to p_v this will result in the loss of c_v's traffic. Therefore, to attract c_u's traffic it is necessary that m not announce a route to x_u and, similarly, to attract c_u's traffic it is necessary that m not announce a route to x_u. Observe that if m does not announce md to both x_u and x_v then the edge e_{uv} shall be forced to choose its only available (provider-learned) route to d, $e_{uv}d$. In this case, both c_u and c_v will have a v-hop route to d through e_{uv} (and will choose it by SP). This will result in m's loss of both c_u's and c_v's traffic.

The above shows that while m can easily attract c_u's traffic alone (by not announcing md to x_u and announcing md to all other neighbors), or c_v's traffic alone (by not announcing md to x_v and announcing md to all other neighbors), it cannot attract both c_u and c_v's traffic simultaneously.

The reduction. We prove the correctness of the above two theorems via the arguments in Sec. F.1. We reduce from MAX-INDEP-SET. For every vertex $v \in V$ we create a node c_v. For every edge $e = (u, v) \in E$, we construct a BAT-FROM-HELL-II gadget to ensure that m not be able to attract both c_u and c_v simultaneously. Fig. 26 describes the construction of BAT-FROM-HELL-II for the edge (u, v) (illustrating the per-vertex, per-edge, and common to all gadgets, parts of the construction). Observe that our constructions of BAT-FROM-HELL-II gadgets are consistent, in the sense that if the manipulator cannot attract node c_v in one such gadget (because it chose to attract the other node in that gadget), then it also cannot attract c_v in all other BAT-FROM-HELL-II gadgets that c_v participates in. The arguments in Sec. F.1 now imply the theorems. □

F.4 Two Remarks

Attraction *v.s.* Interception. While our results are stated for attraction attacks (as they only discuss the amount of traffic that the manipulator can attract), the fact that in all of our DILEMMA constructions the manipulator is directly connected to d, and so always has a route available, implies that all of our hardness results extend to interception attacks.

The degree of the manipulator. Our hardness results are in the number of edges that the manipulator has (that is roughly the size of V in the MAX-INDEP-SET instance). However, the result in Sec. F.2 can easily be made to hold even if the manipulator only has a constant (even 2) number of neighbors. This can be achieved via the addition of intermediate nodes. In contrast, our result in Sec. F.3, where the manipulator only chooses whether to announce its actual path to each neighbor, is computationally easy if the

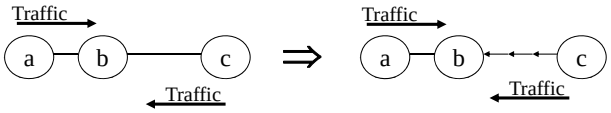


Figure 27: Lemma G.1.

manipulator has a constant number of neighbors (as it can simply go over all the possibilities).

G. GUIDELINES FOR INTERCEPTION

We prove the results marked with a ✓ in Table 1. That is, we provide guidelines that guarantee that a manipulator's attack strategy preserves an available path to the victim IP prefix.

To do this, we consider the *normal outcome* , where the all nodes behave normally, and the *manipulated outcome* , where a single AS m, the manipulator uses some attack strategy that *deviates* from the normal routing policies of Section 2.2. The victim IP prefix is legitimately owned by a destination AS d. Let the nodes on m's available path to d in the normal outcome be $a_1, ..., a_{t-1}$, so that m routes to d on the path $ma_1....a_t$ (where for convenience we will set $d = a_t$). We would like to guarantee that the manipulator's attack strategy leaves him with an available path to d through a_1 (in the manipulated outcome). That is, we want to guarantee that a_1 will not route through m in the manipulated outcome.

G.1 A useful lemma.

Before we start, we need the following useful concept:

Transitive customers. A node b is a *strict transitive customer* of node c if b is connected to c via a path consisting of only customer-provider links as in the right half of Figure 27. We also restate here a simple, useful lemma of the Gao-Rexford conditions proved by Gao, Griffin and Rexford in [26].

LEMMA G.1 ([26, THEOREM VII.4]). *If either the path $P = abRc$ or the path $P' = cR'ba$ is available, and if node a is not a customer of node b, then node c is a strict transitive customer of node b over the available path.*

We remark that Lemma G.1 still holds as long as all the nodes on the available path (except perhaps the last one, closest to the destination) behave normally, according the routing policies in Section 2.2.

G.2 Available path through peers/customers. May export to peers & customers.

We prove the four results ✓* results in the top left corner of Table 1. The following claim that does *not* require **GR1**:

CLAIM G.2. *Suppose that nodes use the routing policies of Section 2.2. Suppose m's path to d in the normal outcome is a peer or customer path (*i.e., *a_1 is a peer or customer of m). Then m has an available path through a_1 in manipulated outcome, even if m announces* any *(possibly false) path to* any *of his neighboring* peers or customers.

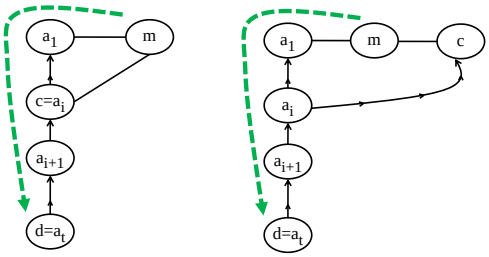


Figure 28: Case 1 (left) and Case 2 (right) in Claim G.2.

PROOF. First, notice that if m's available path in the normal outcome is a peer or customer path, then **GR2** tells us that a_1's available path in the normal outcome must be a customer path, and Lemma G.1 immediately tells that for every $i \in [t-1]$, a_{i+1} is a customer of a_i. By **NE**, it follows that every a_i hears an announcement from his customer a_{i+1}.

Let c be any neighbor node of m that heard a path announcement from m. Recall that c must be either a peer or customer of m. We now have two cases:

- Suppose that c is one of the nodes on m's available path in the normal outcome, *i.e.,* $c = a_i$ for any $i \in [t-1]$. We argued above that a_i learns a path from it's customer a_{i+1}. Now, recall that by definition m is a provider or peer of n. It follows from **LP** that for $c = a_i$, the customer path through a_{i+1} is more attractive than the peer or provider path through m, and so $c = a_i$ will prefer to route through a_{i+1}.
- Suppose that n is not one of the nodes on m's available path in the normal outcome. Repeatedly applying **GR2** tells us that the only nodes that can hear about c's path through m must be strict transitive customer of c. Suppose that some a_i for $i \in [t-1]$ hears about the path through m. It follows that a_i learns about the path through m from his provider. Again, by **NE** a_i hears an announcement from his customer a_{i+1}, and by **LP** this customer path through a_{i+1} is preferred over the provider path through m.

It follows that in each case, every a_i for $i \in [t-1]$ will prefer to route through a_{i+1} instead of routing through m. In particular a_1 has a path to d that does not go through m. By **NE**, a_1 will announce this path to m and the claim follows. □

G.3 Available path through customers. May export to providers.

In Section E.1, we presented an example that proves that if a_1 is *peer* of m, then m may lose an available path through a_1 by lying to one of his neighboring providers. However, we now prove the ✓ in the top right of Table 1, showing that if a_1 is a *customer* of m, then m can even get away with lying to his neighboring providers. This claim requires **GR1**:

CLAIM G.3. *Suppose that **GR1** holds, and that nodes use the routing policies of Section 2.2. Suppose m's path to d in the normal outcome is a customer path (*i.e., *a_1 is a customer of m). Then m has a available path through a_1 in the*

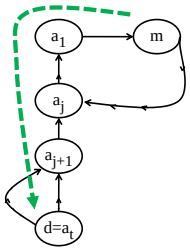


Figure 29: Proof of the induction step in Claim G.3.

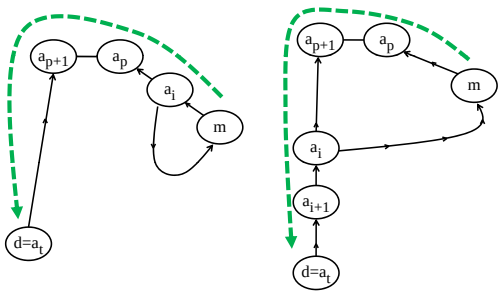


Figure 30: Case 1 (left) and Case 2 (right) in Claim G.4.

manipulated outcome, even if m announces any *(possibly false) path to* any *of its neighbors.*

PROOF. Now, observe that if a_1's available path to d in the manipulated outcome is unchanged, then by **NE** a_1 announces this path to m and we are done. Thus, we suppose that the path $a_1...a_td$ is not used in the manipulated outcome. It follows that there must be some node a_i for $i \in t$ that is closest to the destination d that forwards traffic over a different path in the manipulated outcome (*i.e.,* different from the $a_i...a_t$ path he used in the normal outcome). The proof now follows from the following (backward) induction from $j = 1...i$.

Base case. Let $a_{j+1} = a_{i+1}$. From the way we defined a_i, it follows that a_{i+1} uses the same customer path to d in the normal outcome and the manipulated outcome, so it follows that a_{i+1}'s available path does not go through m.

Induction step. Suppose that in the manipulated outcome a_{j+1} uses a customer path to d that does not go through m. Then in the manipulated outcome a_j also forwards along a customer path to d that does not go through m.

We now prove the induction step. First, observe that the Lemma G.1 and the fact that a_1 uses a customer path in the normal outcome immediately tells us that a_{j+1} is a customer of a_j. By **NE**, a_{j+1} must export a path to a_j in the manipulated outcome; thus, a_j has a customer path available in the manipulated outcome. By **LP**, it follows that whatever path a_j chooses in the manipulated outcome must also be a customer path. To finish the proof of the induction step, we shall show, by contradiction, that this path does not go through m: Suppose that the available path that a_j chooses in the manipulated outcome goes through m. Then, since this path is a customer path, Lemma G.1 tells us that the manipulator m as a strict transitive customer of a_j along this path. Now recall that that m uses a customer path in normal outcome, and apply Lemma G.1 again to obtain that that a_j must be a strict transitive customer of m. It follows that there is a customer-provider loop in the AS-graph (between a_j and m), which violates **GR1**, and we have arrived at our contradiction.

From the induction, we learn that a_1 must use a customer path in the manipulated outcome that does not go through m. By **NE**, a_1 announces this path to m and the claim follows. □

G.4 Available path through providers. May export to customers.

We showed how a manipulator might disrupt an available path through a *provider* by announcing to a *provider* (Section 5.1), or a *peer* (Appendix E.2). We now show that a manipulator that wants to preserve an available path through a provider *may* export any path to his *customers*, proving the ✓ on the bottom left of Table 1. We again rely on **GR1**:

CLAIM G.4. *Suppose that **GR1** holds, and that nodes use the routing policies of Section 2.2. Suppose m's path to d in the normal outcome is a provider path (*i.e., *a_1 is a provider of m). Then m has a path available through a_1 in the manipulated outcome, even if m announces* any *(possibly false) path to* any *of its neighboring* customers.

PROOF. Since m only announces paths to his customers, repeated applications of **GR2** immediately tell us that the only nodes that can hear about paths through m are strict transitive customer of m. Now consider m's available path $a_1...a_t$, and let a_p be the node closest to m such that m is a strict transitive customer of a_p. (We know that a_p exists since in particular a_1, a provider of m, is one such node.) We now show that no a_i will choose to route through m:

- Suppose some node a_i for $i \in [p]$ learns about the path through m. We argued above that a_i must be a strict transitive customer of m. However, by the definition of a_p, m is also a strict transitive customer of a_i! It follows that there is a customer-provider loop in the AS graph, which violates **GR1**. It follows that no a_i for $i \in [p]$ will learn about the path through m.
- Suppose some node a_i for $i = p...t-1$ learns about the path through m. Above we argued that a_i must be a strict transitive customer of m, so it follows that a_i learns about the path through m from his provider.

  Now, by the definition of a_p and **GR2** we know that a_{p+1} is either a peer or customer of a_p. Applying **GR2** again tells us that a_{i+1} is a customer of a_i for each $i = p+1...t-1$. By **NE**, we know that a_{i+1} announces a path to a_i for every $i = p...t-1$. It follows that for every a_i for $i = p...t-1$, the path it learns through its peer or customer a_{i+1} is more attractive than the provider-path through m.

It follows that in each case, every a_i for $i \in [t-1]$ will route through a_{i+1} instead of routing through m. In particular a_1 will have a path to d that does not go through m. By **NE**, a_1 will announce this path to m and the claim follows. □

H. CYCLOPS+IXP DATASET

This appendix presents versions of all the graphs in this paper, computed from the 'Cyclop+IXP' AS Graph datasets [12,13]. We constructed this dataset from the November 20, 2009 Cyclops dataset, by removing 276 edges connected to 4-byte ASNs, and removing 444 edges with unclassified business relationships. Then, we augmented the dataset with 21890 peer-to-peer edges from the recent IXP dataset [13], using only edges with good confidence, and ignoring edges that referred to ASes that were not in the Cyclops dataset. We note that the Cyclops dataset does *not* include any sibling-to-sibling edges, and is also derived using a different relationship inference algorithm than the CAIDA dataset.

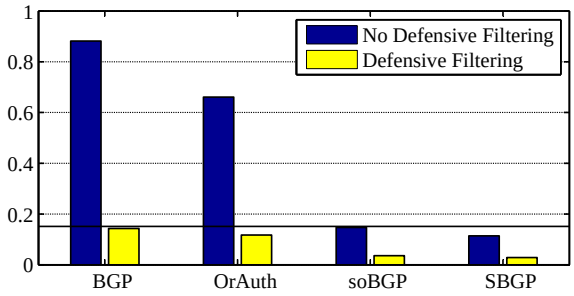


Figure 31: Lower bounds on the probability of attracting at least 10% of ASes in the internetwork. Cyclops+IXP dataset.

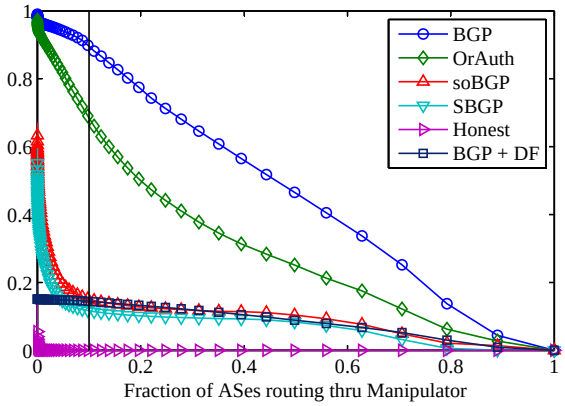


Figure 32: CCDF for the "Shortest-Path Export-All" attack strategy. Cyclops+IXP dataset.

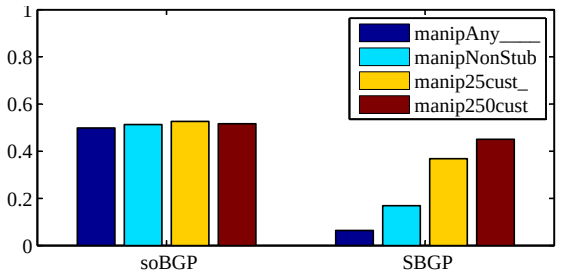


Figure 33: Probability of finding a shorter path. Cyclops+IXP dataset.

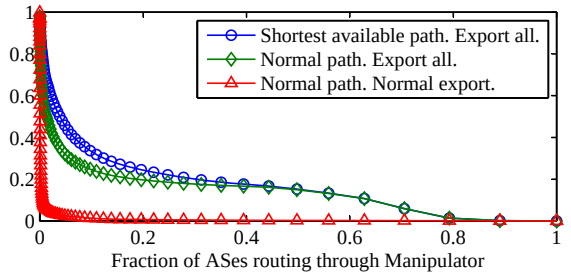


Figure 34: Aggressive export policies. Cyclops+IXP dataset.

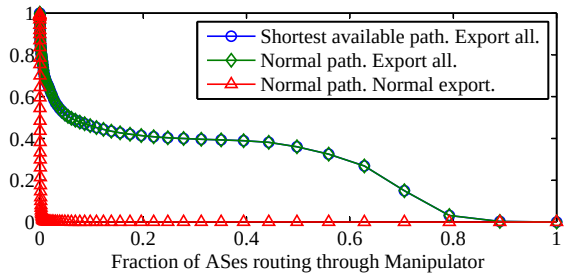


Figure 35: Aggressive export policies when the normal path is through a provider. Cyclops+IXP dataset.

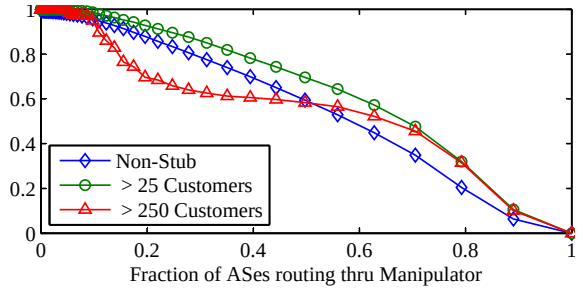


Figure 36: "Shortest-Path Export-All" attack strategy on BGP by different manipulators. Cyclops+IXP dataset.

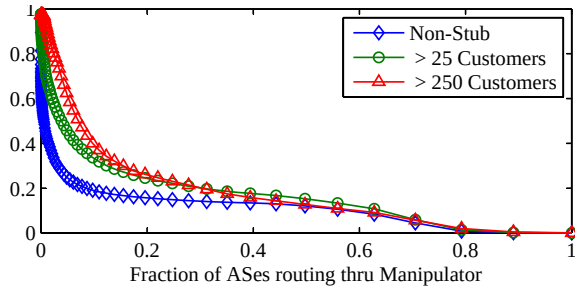


Figure 37: "Shortest-Path Export-All" attack strategy on S-BGP/data-plane verification by different manipulators. Cyclops+IXP dataset.

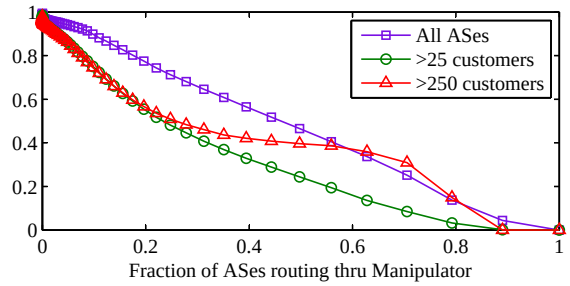


Figure 38: "Shortest-Path Export-All" attack strategy on BGP for different victims.

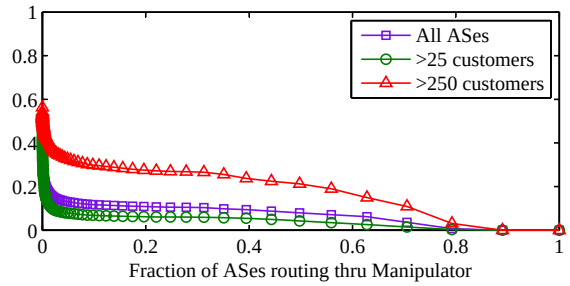


Figure 39: "Shortest-Path Export-All" attack strategy on S-BGP for different victims.

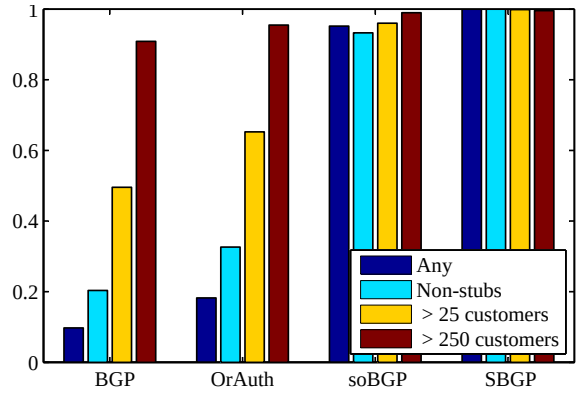


Figure 40: Probability that the "Shortest-Path Export-All" attack strategy does *not* create a blackhole. Cyclops+IXP dataset.

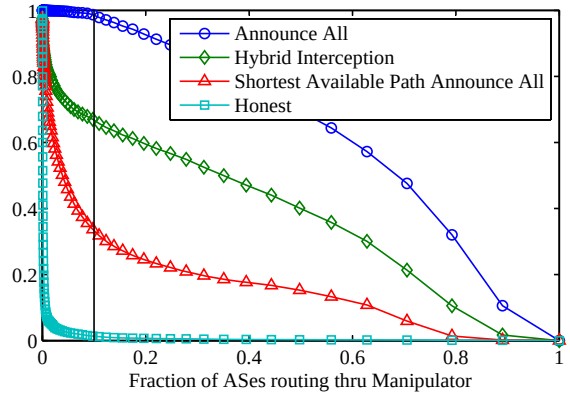


Figure 41: Interception attacks on BGP. Cyclops+IXP dataset.

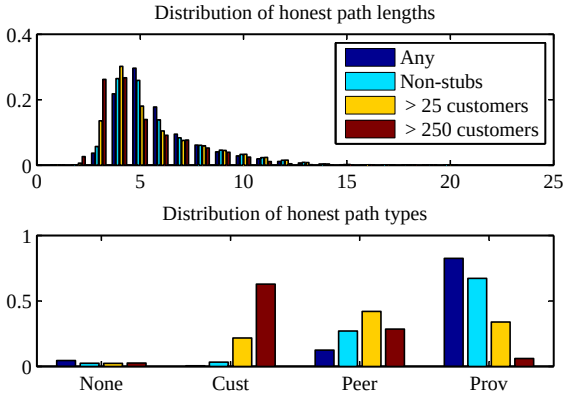


Figure 42: Path length and type distributions. Cyclops+IXP dataset.

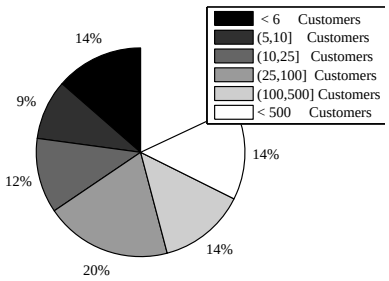


Figure 43: Distribution of stubs, according to the size of their smallest provider.