Cairn: Identifying Network Locations for Large Scale Censorship by Resource-Constrained Adversaries

Anshika Agarwal, Devashish Gosain, H. B. Acharya and Sambuddho Chakravarty

Indraprastha Institute of Information Technology Delhi (IIITD), New Delhi, India
{devashishg,anshika1448,acharya,sambuddho}@iiitd.ac.in

Abstract

Censorship of the Internet by government is a hotly contested topic. Some nations lean more toward free speech; others are much more conservative. How feasible is it for a government to censor the Internet? What mechanisms can it use? Where all should it install the censorship infrastructure? What collateral damage can be seen in other countries? In this paper, we attempt to look at these questions in general, and present a case study of India - a country which currently performs limited censorship, but which will likely change its access policies in the near future.

I. Introduction

Censoring the Internet is a hard problem: it is decentralized, routes around disruptions, and is designed to be resilient to interruptions. While a sufficiently resourceful adversary can filter (or monitor) almost all traffic [16], this is not true for resource constrained nations, who cannot afford to place dedicated infrastructure in every network. But exactly how hard is it for a given government to become censorious? Can it, for example, make do with network monitors in those few key Autonomous Systems (ASes) and network elements that forward most of the nation's traffic? How can we measure the potential censoring power of a regime? (The US censors much less than, for example, Iran. But if it did decide to censor content, the effect would be much greater.) How much collateral damage will a nation cause, if it becomes censorious? In this paper, we make a start toward answering such questions.

The case we study is India, a democratic nation that favors free speech, but undecided on questions of censorship [3].(For example, in August 2015, Indian ISPs blocked 857 pornographic and torrent sites under State orders [6]; public outcry forced them to backtrack.) There are several known engineering challenges in implementing a censorship scheme; for example, how to identify the content to block, *etc.* We take a new approach, and focus on the network itself - which ASes and network elements would be most effective for installing censorship infrastructure, how effective it would be, and what collateral damage would result. Formally, we aim to answer the following questions.

- *Is it feasible to filter or monitor Internet traffic? If so, how, and where?* While India is among top Internet consumers, with over 300 million users, the Internet in India consists of only about 900 active Autonomous Systems (ASes), of which less than 100 are ISP networks (the others are stubs, relying on the ISPs for Internet connectivity). Is the Internet in India sufficiently localized that it can be effectively policed, or are there too many "throats to choke"? What mechanisms might be effective?
  - Is there a small number of key ASes (networks) and routers, such that the government can deploy network monitoring or filtering infrastructure at only these ASes and intercept most of the traffic to censored destinations?
  - Which censorious ISPs deploy DNS injectors [9] so that they can filter most DNS requests?
  - What fraction of Indian ASes would be affected if censorious ISPs choose to hijack IP prefixes [5]?
- *Will traffic filtering cause collateral damage?:* Some nations get Internet connectivity through others; as a consequence, censorship by an "upstream" nation can lead to collateral damage, where requests for content originating from the "downstream" nation are forcibly filtered. If India becomes a censorious regime, to what extent will this affect traffic of non-Indian origin?

We begin with a review of the background and related work, in the next section.

II. Background and Related Work

The interaction of the Internet with government policy (especially censorship and privacy issues) is an extensively studied subject. Government interference with the Internet comes under two main headings, as follows.

1) Network censorship, where specific traffic is filtered and blocked.
2) Network surveillance - silently monitoring traffic. (This is harder to detect.)

In this paper, we study the structure of the network in India (i.e., the connectivity of autonomous systems, and how they forward traffic). The aim is to identify key points through which almost all of the traffic, DNS requests, *etc.* must pass. *These key points would be the most cost-effective locations to perform censorship or surveillance.*

A. Background

Our paper relies heavily on mapping the structure of the Internet, an area of research called *network tomography* [13]. The Internet consists of routers and hosts, but also has some further structure: the routers and hosts belong to Autonomous Systems, which are independent networks (independent in the sense, they themselves choose who to exchange traffic with). There are over $40,000$ ASes in the Internet, including ISPs (e.g. AT&T) and customer networks. Consequently, Internet mapping proceeds at two levels:

1) *AS-level mapping.* Gao *et al.* [17] show how to infer the paths from a given IP address prefix to every AS on the Internet. The algorithm uses publicly-available BGP routes, obtained from various Internet Exchange Points across the globe [7]), to estimate the relationships and connections between ASes, and builds a directed graph of the Internet where each node is an AS.
2) *Router-level mapping.* An AS is not a black box, but contains hosts and routers. Mahajan *et al.* [18] show how the internal structure of an AS can be mapped, by a combination of `traceroute` probes, IP alias resolution [1], and reverse DNS lookups.

B. Related Research

This paper contributes to the study of country-level network censorship. Much work in this area focuses on China; for example, Winter *et al.*[19] examine how the Chinese authorities use DPI-capable routers to detect Tor Bridges. A major step forward was made by Verkamp *et al.*[8], who deployed clients in 11 countries to identify their network censorship activities – IP and URL filtering, keyword filtering DNS censorship *etc.* Later authors - Nabi [15] in Pakistan, and Halderman *et al.* [10] in Iran - demonstrate different methods of censorship employed by their respective regimes, as well as different forms of content blocked.

However, such a study of censorship in repressive regimes is necessarily limited, as it requires Internet access from inside the country. (Nabi was able to run probes from only five locations, and Halderman from only one.) We take a different direction with this paper, and study censorship as an engineering problem. How feasible is it for the State to carry out censorship by standard means (DNS injection attacks, IP filtering and IP prefix hijacking)? How many, and which, autonomous systems would it need to control? We explain our approach in detail in the next Section.

[1]Different interfaces of the same router, with different IP addresses, are called IP aliases

III. Problem Description and Methodology

A. Problem Description

Given that most governments do not have the resources for an extensive monitoring solution like PRISM [16], the question arises how powerful a resource-constrained governmental adversary is. Specifically, we are interested in the following questions:

- Is it possible for the Government to monitor/censor a large fraction of Internet traffic by controlling only a small number of network locations? And by what means?
- What fraction of traffic could be filtered, and who would be most affected?
- Would such censorship affect users outside the country as well?

In this paper, we explore these questions with a case study of India.

Threat Model: Our adversary is a censorious but resource-budgeted government. The adversary aims to monitor and filter Internet traffic, and for this purpose may perform IP filtering, DNS injection, and IP prefix hijacking attacks.

B. Evaluation Methodology

a) Identifying Potential Network locations for IP filtering:: In order to estimate the locations for installing IP filtering infrastructure, we mapped the complete Internet topology consisting of ASes as nodes, then focused on Indian ASes and their connections. Gao *et. al.*'s algorithm [17] was used to find the AS paths connecting the home AS of some chosen IP prefixes (corresponding to censored sites) to every other AS in the world. (The algorithm builds a graph of ASes and their links from known AS paths in BGP routing

tables, obtained from a number of vantage points [7], and known business relationships between ASes [12].)

Unlike other nations, which have an unambiguous list of blocked sites [15], India has no clear censorship policy. We chose sites reported as blocked in India, from the crowd-sourced censorship-reporting site, Herdict [2]. These included social networking sites, political sites, sites related to unfriendly nations, and p2p file-sharing sites. We also chose several adult sites from Alexa [1], popularly accessed in India. Our set of censored websites corresponded to 211 unique IP prefixes.

We then calculated the paths between all Indian ASes and these prefixes, a total of 186679 paths. The ASes appearing in these paths were sorted by frequency of occurrence; we selected the few most popular.

Intra-AS topology generation and network "choke" routers: The router level topology was computed for two major ASes (ISPs) that appear in a very large fraction of paths. Using `planetlab` nodes, we ran `traceroute` probes to one representative IP in each prefix advertised by the ASes. (Our approach follows Mahajan *et al.* [18].) We then resolved aliases with `Midar` [4], selected the routers common to many `traceroute` paths, and attempted to identify any "key" routers, a small set of which could give the adversary coverage of all paths.

b) Identifying Potential Sites for DNS Injection:: Another common approach to censorship is to prevent the DNS service from resolving requests - the censor intercepts DNS connections and responds back with bogus IPs or NXDOMAIN responses. This is referred to as *DNS Injection*.

To identify key ASes for DNS injection, we began by identifying the DNS resolvers across all Indian prefixes. We probed IP prefixes of every Indian AS for available DNS servers (UDP port 53) using `nmap` [14]. The probe requests evoke three kinds of responses:*open*, *filtered*, and *closed*. (*Closed* corresponds to ICMP `'destination port unreachable'` message responses from the destination. *Open* means the client received a meaningful response. *Filtered* indicates that the client received no response [2].)

Each IP, for which we obtained a *filtered* or *open* response, was sent a request to resolve the IP address of some popular WWW destinations (*e.g.* `https://www.google.com`). Addresses that allowed resolution were added to our list of publicly available DNS resolvers.

Finally, using Gao's algorithm, we constructed a graph of prefix-to-AS paths connecting the IP prefixes corresponding to DNS resolvers, and all the Indian ASes. To find the ASes which would be most effective at DNS injection, we identified ASes at the intersection of a large number of these paths.

c) Impact of IP Prefix Hijack Based Censorship:: IP Prefix Hijacking attack involves malicious BGP routers advertising fake AS paths, in an attempt to poison routes to an IP prefix (*e.g.* [5]). Such advertisements make the router appear to be an attractive choice for routing traffic to the prefix [11] (see Figure 1).

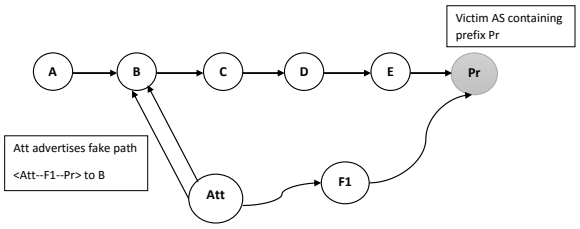

Fig. 1. IP Prefix Hijacking: Valid path: $A-B-C-D-E-Pr$. A is the origin AS and Pr the AS with the destination prefix. Attacker Att advertises a shorter path $Att-F_1-Pr$, to AS B. If B chooses this path and directs its traffic to Att, the attacker can censor the traffic.

The malicious AS either broadcasts a shorter path to the prefix, or claims to own it outright. The attacking AS advertises fake routes for the targeted prefix to all its neighbors. Receiving ASes accept these advertisements based on the following heuristic [11]:

1) If there exists a customer path towards the target IP and iff the advertisement presents a shorter customer path, then choose it, else reject it.
2) If there exist a provider path towards the target IP and iff the advertisement presents a shorter provider path, then accept it. For all other cases, the paths are accepted without considering the length.
3) If there exist a peer path towards the target IP and iff the advertisement bears a shorter peer path, accept it. Customer paths are accepted without length considerations while provider paths are ignored.

Estimating the Impact of Prefix Hijack Attack: To study the potential impact IP prefix hijacking, we used the previously constructed AS-level topology and chose an attacker AS with a high *node degree*[3]. Inspecting the prefix-to-AS paths, we identified ASes with which the attacker AS had a business relationship, and applied the above heuristics to determine the number of ASes potentially affected by fake advertisements.

d) Collateral Damage Due to Traffic Censorship:: Several non-Indian ASes rely on Indian ASes for Internet connectivity. Censorship activities in Indian ASes

[2]This may be due to unavailability or filtering by firewall(s)

[3]Number of ASes that are adjacent to the said AS

may potentially filter the traffic of these non-Indian customers as well. In the past, such inadvertent filtering has been reported by Sparks *et. al.* [9]. As one of our research objectives, we try to identify ASes outside India that may be affected by Indian censorship. To that end we identified paths which do not originate in India, but pass through or terminate in India. The non-Indian customers on such paths may face unwanted access restrictions.

IV. Experimental Results

Continuing from the description of our experiment in the previous section, in this section we present our results. First, we consider IP filtering, and how many ASes and routers must be selected for effective censorship (in terms of coverage of paths to filtered destinations). With a similar argument, we identify the network locations where the adversary could launch a DNS injection attack. Then we present results from simulating IP prefix hijack attacks on Indian ASes. Finally, we report the collateral damage to foreign ASes due to IP filtering in India.

A. Network Locations for IP Filtering

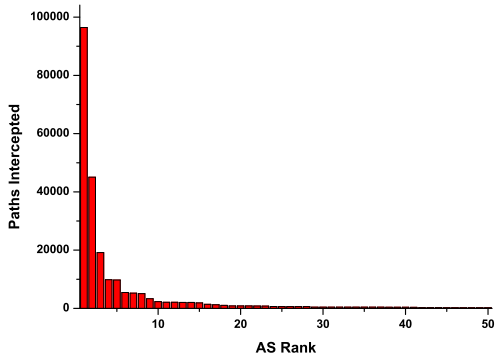

Fig. 2. Paths intercepted by individual ASes vs AS rank (acc. to paths freq.)

We obtained 186679 paths connecting Indian ASes to the potentially filtered sites. Figure 2 represents the number of paths an individual AS intercepts. The horizontal axis of the graph represents ASes ranked according to the number of paths each one intercepts. The ASNs and their owner organizations are presented in the table I. Apparently, some Indian ASes - a very small number - appear in the majority of these paths. The cumulative results of *paths intercepted* vs *total number of ASes* is presented in figure 3.

From figure 3, *approximately* 4 *ASes can censor over* 90% *of the paths to the censored destinations*.

Rank	ASN	Owner
1	9498	Bharti Airtel
2	4755	Tata Comm.
3	55410	Vodafone
4	9583	Sify Ltd.
5	9730	Bharti Telesonic
6	9885	NKN Internet
7	55824	NKN Core
8	45820	Tata Teleservices
9	18101	Reliance Comm.
10	10201	Dishnet Wireless

TABLE I
AS RANKS, THEIR ASNS AND THEIR OWNERS.

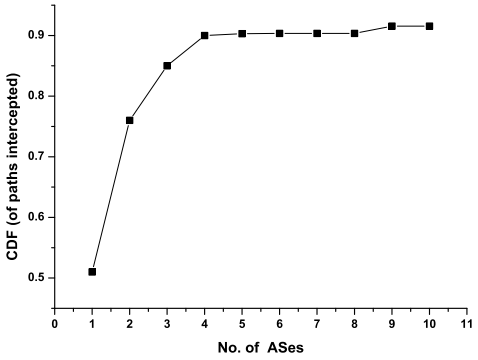

Fig. 3. CDF of Indian paths intercepted by ASes.

a) Intra-AS Topology:: We used Mahajan *et al.*'s approach [18], as described in the previous section, to create router-level maps of the most significant two ASes, *AS*9498 and *AS*4755. We sorted the routers by the number of `traceroute` paths they uniquely intercept, and selected those routers that appear on a large number of paths. Figure 4 shows the fraction of paths these routers cumulatively intercept. (For privacy concerns, we refrain from revealing the IP addresses of these routers.)

Apparently, about 15 routers cumulatively appear in about only 33% and 52% of the paths corresponding to *AS*4755 and *AS*9498 respectively. At most 5% of the paths transit any router (corresponding to router ranked 1). It implies that for these ASes, no small number of routers can collectively censor a large volume of traffic.

B. Censorship Through IP Prefix Hijack

As described in the previous section, we chose to simulate attacks from the ASes with high node degree. Based on our censored prefix-to-AS topology graph, we identified the top 10 ASes, sorted by their node degrees, and determined the number of ASes potentially vulnerable to attacks from each of these ASes. The results of these simulations are presented in table II.

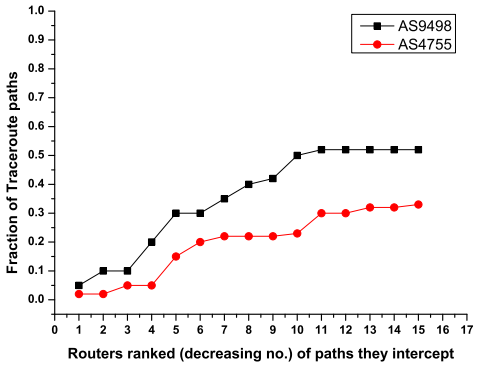

Fig. 4. CDF of `traceroute` paths intercepted by individual routers, sorted by increasing number of paths through each router(for *AS*9498 and *AS*4755.)

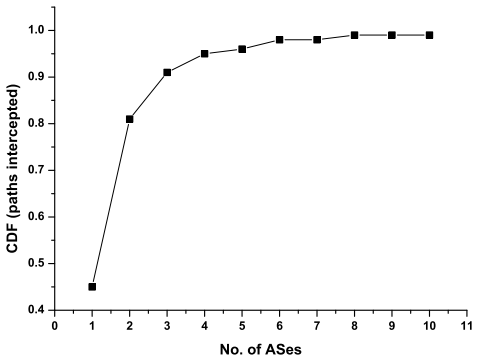

Fig. 5. CDF of `DNS` paths intercepted by top 10 Ases.

		Number of Affected AS'es	
Owner Name	**Attacking ASN**	**Indian**	**Non-Indian**
Bharti Airtel Ltd.	9498	896	59
Tata Comm.	4755	896	41
Reliance Comm. Ltd.	18101	896	41
Vodafone Spacetel Ltd.	55410	896	42
Sify Ltd.	9583	896	58
Bharti Telesonic Ltd.	9730	749	23
Tata Teleservices	45820	560	1
Host Palace	13329	896	45
Dishnet Wireless Ltd.	10201	896	24
Idea Cellular Ltd.	55644	896	37

TABLE II
IP PREFIX HIJACK

From the table, we see that a small number of ASes in India can potentially affect traffic from ALL Indian ASes, as well as a considerable number of foreign ones. For example, an attack by *AS*9498 can affect a total of 955 ASes (896 Indian and 59 others).

C. Censorship Through DNS Injection

Using our approach for identifying open DNS resolvers, we identified a total of 55234 publicly accessible DNS servers from probing all 9.4 million IP addresses of India.

After identifying the prefixes corresponding to these each resolver IP, we selected one corresponding to each AS[4] Ultimately 355 prefixes, representative of unique 355 Indian ASes, were selected. Using Gao's algorithm, we estimated paths from Indian ASes to prefixes of DNS resolvers in India. *Cumulatively, 8 ASes (according to path frequency) can intercept* 99.14% *of these paths, and potentially launch DNS Injection attacks (see figure 5).* These ASes also appear among our top 10 AS choices for IP filtering and IP prefix hijacking.

a) Collateral Damage:: Our graph of paths from censored prefixes to ASes has 186679 paths of Indian origin (1.76% of paths). About 121931 paths of foreign origin (1.15% of paths, *comparable to the fraction originating in India*) transit through or terminate in an Indian AS. *Censorship by Indian ASes may inadvertently impact a very large number of unintended customers, across Finland, Hong Kong, Singapore, Malaysia, the US etc.*

V. Discussion and Future Work

Internet censorship in developing nations is both easier and harder than in the developed world. The Internet infrastructure is smaller, but the government is also resource constrained. In this paper, we study how this trade-off affects the feasibility of censorship in India, a country which shows signs of becoming censorious [3].

Previous work on censorship in poorer countries [8], [10], [15] focuses on the content (*what* is being censored), and the mechanism (*how* censorship is implemented). As large-scale censorship is not yet in effect in India, we have taken a list of likely future targets, and focused on the mechanisms of IP filtering, DNS injection, and IP prefix hijacking. We find that there are indeed a few key ASes (less than 10) where an adversary with limited budget might deploy its infrastructure to devastating effect. Another surprising result is the extent of collateral damage - many foreign ASes can be affected by Indian censorship, including a substantial portion of Africa, and several "free" countries such as Norway and the US.

It is important to note that we make use of no features peculiar to India. Our analysis may, therefore, be applied for other countries as well. In our immediate future

[4]For multiple prefixes belonging to same AS, we selected the one with the most resolvers.

work, we intend to do this; our long-term goal is to develop metrics for how hard it is to censor traffic in a country, as well as how "central" a country is, i.e. how much collateral damage it can cause.

Our analysis may be extended in several ways. For example, what happens if a country blocks different content - search engines and social networking sites (as seen in China), instead of pornography (or other objectionable content)? Also, in practice, targeted content is often hosted on social media sites, or other sites with apparently benign URLs; a real censor does not just block IP addresses, it performs real-time pattern recognition w.r.t. content. (Semantics-based filtering is very hard: attempts to block jihadi sites also block sites that monitor militancy, such as `jihadwatch.org`.) How might a sophisticated but resource-poor adversary perform such censorship? We intend to study these questions in our future work.

VI. Concluding Remarks.

In this paper, we have applied a novel method of analysis to study censorship (by a resource-restricted adversary) as an engineering problem. Our results show that it is indeed feasible for the Indian Government to become a censorious regime. *However, while it is sufficient for a censor to assume control over a small fraction of Indian ASes, it is not enough to control a small proportion of the routers in the ASes.*

1) *Potential locations for monitoring and filtering network traffic:* The adversary, given control over the routers of only 4 ASes, can observe 90.52% of the paths to our sample censored sites.
2) *Potential ASes to filter DNS requests:* With control of 8 ASes, the adversary can deny access to alternative DNS servers for 99% of the users.
3) *IP Prefix Hijacking:* There exist several ASes which can single-handedly launch IP Prefix hijacking attacks that affect all Indian users.

Further, there are ASes outside India whose traffic may be inadvertently censored if the Indian government employs these means of censorship.

References

[1] Alexa - Actionable Analytics for the Web. http://www.alexa.com/.

[2] Herdict:Help Spot Web Blockages. http://herdict.org/.

[3] Internet Censorship in India. https://en.wikipedia.org/wiki/Internet_censorship_in_India.

[4] Midar. http://www.caida.org/tools/measurement/midar/.

[5] Pakistan hijacks youtube. http://research.dyn.com/2008/02/pakistan-hijacks-youtube-1/.

[6] Porn websites blocked in india: Government plans ombudsman for online content. http://gadgets.ndtv.com/internet/news/porn-websites-blocked-in-india-government-plans-\ombudsman-for-online-content-723485.

[7] University of Oregon Route Views Project. http://www.routeviews.org/, 2000.

[8] Inferring mechanics of web censorship around the world. In *Presented as part of the 2nd USENIX Workshop on Free and Open Communications on the Internet* (Berkeley, CA, 2012), USENIX.

[9] ANONYMOUS. The collateral damage of internet censorship by dns injection. *SIGCOMM Comput. Commun. Rev. 42*, 3 (June 2012), 21–27.

[10] ARYAN, S., ARYAN, H., AND HALDERMAN, J. A. Internet censorship in iran: A first look. In *Presented as part of the 3rd USENIX Workshop on Free and Open Communications on the Internet* (Berkeley, CA, 2013), USENIX.

[11] BALLANI, H., FRANCIS, P., AND ZHANG, X. A study of prefix hijacking and interception in the internet. *SIGCOMM Comput. Commun. Rev. 37*, 4 (Aug. 2007), 265–276.

[12] GAO, L. On inferring autonomous system relationships in the internet. *IEEE/ACM Trans. Netw. 9*, 6 (Dec. 2001), 733–745.

[13] HADDADI, H., RIO, M., IANNACCONE, G., MOORE, A., AND MORTIER, R. Network topologies: inference, modeling, and generation. *IEEE Communications Surveys Tutorials 10*, 2 (Second 2008), 48–69.

[14] LYON, G. Nmap: the network mapper - free security scanner. http://insecure.org/fyodor/.

[15] NABI, Z. The anatomy of web censorship in pakistan. In *Presented as part of the 3rd USENIX Workshop on Free and Open Communications on the Internet* (Berkeley, CA, 2013), USENIX.

[16] (NSA), U. S. N. S. A. Prism (surveillance program). https://en.wikipedia.org/wiki/PRISM_(surveillance_program).

[17] QIU, J., AND GAO, L. As path inference by exploiting known as paths. Tech. rep., In Proceedings of IEEE GLOBECOM, 2005.

[18] Rocketfuel: An ISP Topology Mapping Engine. http://www.cs.washington.edu/research/networking/rocketfuel/.

[19] WINTER, P., AND LINDSKOG, S. How the Great Firewall of China is blocking Tor. In *Proceedings of the USENIX Workshop on Free and Open Communications on the Internet (FOCI 2012)* (August 2012).