Citadels in Cyberspace

Student Name: Madhur Rawat

IIIT-D-MTech-CS-17-MT15030
June, 2017

Indraprastha Institute of Information Technology
New Delhi

Thesis Committee
Dr. Sambuddho Chakravarty (Advisor)
Dr. Rahul Purandare (Internal Examiner)
Dr. Anupam Joshi(External Examiner)

Submitted in partial fulfillment of the requirements
for the Degree of M.Tech. in Computer Science

Certificate

This is to certify that the thesis titled **"Citadels in Cyberspace"** submitted by **Madhur Rawat** for the partial fulfillment of the requirements for the degree of *Master of Technology* in *Computer Science & Engineering* is a record of the bonafide work carried out by her / him under my / our guidance and supervision in the Security and Privacy group at Indraprastha Institute of Information Technology, Delhi. This work has not been submitted anywhere else for the reward of any other degree.

Dr.Sambuddho Chakravarty
Indraprastha Institute of Information Technology, New Delhi

Abstract

Cyberwarefare remains a sparsely explored domain of cyber security research, most often involving targeted attacks by one nation against another, using botnets. These botnets use malwares to launch various kinds of attacks against their targets – ranging from exploiting vulnerabilities, launching Distributed Denial of Service (DDoS) attacks, to various forms of traffic interception attacks.

A powerful nation could use network cartography based techniques to identify key locations within its own nation, where it could install *defenders* that involve interception of illegitimate traffic. More specifically, the government may use network tomography to identify a relatively small number of Autonomous Systems(ASes) such that they can intercept large fraction of network paths (and potentially a large fraction of network traffic).

In our research, we use network tomography to construct such large scale network maps which could be used to identify *Cyber Defense Line* (*viz.,* collection of strategically important ASes that intercept all the network paths of the country) for installing defenders to prevent various kinds of targeted attacks (like DDoS). These defenders would intercept traffic of large fraction of users based on their location, intercepting large fraction of network traffic. We study how well these defenders can prevent the attacker from crippling the critical networked services, such as financial institutions, defense sites *etc.* based on their networked locations.

For our analysis we selected 9 different countries (including China and India) and found "Cyber defense line" for aforementioned network services, DNS infrastructure and for *full* country network map. We found that, countries are significantly similar in network structures *viz.,* all have hierarchical structure. For all sample countries, we found that handful ASes, intercept more than $\approx 90\%$ of all intra country AS paths. For example, in India only 4 ASes capture more than 95% of the network paths. Interestingly, this holds true, if we select ASes based on different AS properties (like customer degree, cone size, and peer degree *etc.*.) Finding *cuts* in country's AS topology is only meaningful, when one aims for intercepting 100% paths by the cut. Our results reveal that,for majority of our sample countries, all boundary ASes (that have peering relationship with foreign ASes of the country) capture more than 99% paths, whereas for 100% paths interception we require considerably very large number of ASes (for example, in China 9 ASes intercepts over 90% of the paths, 90 ASes for 99% of paths and 213 ASes for 100% paths).

Acknowledgments

I am extremely grateful and remain indebted to my guide Dr.Sambuddho Chakravarty for being a source of inspiration and for his constant support in the Design,Implementation and Evaluation of the thesis. The quality of the work would not have been as high without his well- appreciated advice. It is an honor and privilege to have him as my mentor. I sincerely thank him for all his support.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

Considering the rise in large scale targeted attacks like Mirai and Wanna Cry, it becomes imperative for countries to strengthen their defense line in cyber realm. In order to protect their critical infrastructure, they need to place *defenders* (network filtering infrastructures like) in some strategically important locations. The naive solution is to place defenders in all the boundary ASes of the country such that all the foreign traffic can be intercepted by the defenders before entering the country. This would prevent the attacks from foreign ASes, but fails to prevent homegrown attacks. Thus, in order to prevent from inside attacks, we need to find "key" locations in the country's network map which intercept large fraction of network paths.

It has been known [18] and our preliminary research [3] also shows that Internet has grown into a structure with a modest number of "key routers" in a small number of "key Autonomous Systems (ASes)" that intercept large number of network paths, and thus potentially captures considerable fraction of users traffic. If an adversary takes control over such key ASes (by installing botnet *zombies*), entire nations traffic maybe be monitored (or in extreme case filtered). There are various techniques an adversary may employ so as to snoop or inject traffic. *e.g.* large scale government-level adversaries could launch attacks on other nations by installing botted zobmies , thereby snooping (or injecting) large fraction of users' traffic.

In order to protect one's country against such large scale attacks, government might install defenders at few specific locations. In our research we explore the feasibility of identifying a minimal set of network points (called as *Cyber Defense Line*) a nation may identify which may be used for monitoring traffic to a chosen network destination. This may be applicable for both network monitoring and cyber warfare scenarios.

Internet has grown with interdependence among ASes for network connectivity, finding cyber defense line gives leverage to countries, for eavesdropping traffic destined for various important websites across the nation. If nation installs defenders in this defense line, it may withstand a large scale attack against the entire nation.

Cyber Defense Line can be found by identifying those ASes, which intercepts large fraction of network paths. To achieve this, we intend to use C-BGP [15] to construct a nation-level Internet map consisting of ASes (nodes) and their *business relationships* [6](edges) (and validate with

other popular approach given by Qiu and Gao [14]).

Once the nation level AS map is created, we annotate it with node weights. The node weights are AS characteristics (or properties) [20] (explained in detail in section 3.1). We selected five properties (*viz.,* customer degree, peer degree, provider degree, cone size and betweenness) for finding the cuts in the topology. Corresponding to each characteristic, we found a cut. These characteristics play an important role in defining the strategic importance of the AS. On the annotated graph, we apply Ford-Fulkerson algorithm to obtain the residual graph of the original graph. From the residual graph we obtain the cut for the entire graph such that any communication path transits the found cut.

To our surprise we found that, countries are significantly similar in their topological structures *viz.,* all have hierarchical structure. For all sample countries, we found that handful ASes, intercept more than $\approx 90\%$ of all intra country AS paths. For example, in India only 4 ASes capture more than 95% of the network paths. Interestingly, this holds true, if we select ASes based on different AS properties (like customer degree, cone size, and provider degree *etc.*. Finding *cuts* in country's AS topology is only meaningful, when one aims for intercepting 100% paths by the cut. Our results reveal that, for majority of our sample countries, all *boundary ASes* (that have peering relationship with foreign ASes of the country) capture more than 99% paths, whereas for 100% paths interception we require considerably very large number of ASes like for China we require over 200 ASes for complete coverage. This contradicted our intuition, that border ASes serve well primarily for foreign traffic, but they are also the "heavy-hitter" ASes for all intra country AS paths as well.

1.1 Problem Description

In this study, we aim to find the "Cyber Defense Line" for different countries so as to withstand large scale network attacks like DDoS. It is the set of ASes (headquartered in the same country) which can collaboratively filter the malicious flows (like DDoS [11]) against the benign traffic. The goal is to find optimal locations (ASes) for defenders such that with minimum defense installations, a country can safeguard its important Internet destinations like Banking, Defense, Ministry websites and DNS infrastructure *etc.*.

1.2 Motivation

There has been a flurry of cyber attacks (*eg.,* Stuxnet, Mirai), that has lead to severe disruptions of Internet across the globe. Very recently, a powerful botnet based attack *WannaCry* has once again proved that countries are still not well equipped to defend against sophisticated cyber attacks. It becomes a meaningful exercise to study the network tomography of the country, so as to find important locations where we can install defenders.

1.3 Background

Our work in this paper involves mapping the Internet and finding the best places to put *defenders* [19] against large scale botnets. The context for this work comes from the area of network cartography i.e. mapping the structure of the Internet. Our work depends on finding the paths to a particular destination taken by Internet traffic. In this sub-section, we give a short introduction to Internet mapping, and explain our method of mapping.

The Internet consists of routers and hosts, organized into networks called Autonomous Systems (ASes). These networks operate independently, but collaborate to route traffic among themselves. ASes can be customers, peers, or providers to other ASes; besides a physical connection, there must be an acceptable business relationship between two ASes, before they route traffic through each other.[1]

Mapping the Internet involves two tasks – Finding inter-AS connections (and relationships) and mapping routers and hosts (and their connections, inside ASes).

Projects such as CAIDA Ark [1] and *iPlane* [13] map Internet routes with `traceroute`. Traceroute returns router-level paths from a source to a destination, hop-by-hop; the map is built by running traceroute from distributed volunteer nodes to various /24 prefixes. This data is consolidated into a graph where the nodes represent ASes, and edges represent links between them.

Such approaches are generally limited by the network locations and availability of the volunteer nodes; they may not provide the AS-level path between any two randomly chosen ASes, and even where they do, they may be inaccurate.

In our research we used two approaches (1) Gao and Qiu [14], that uses RIBs collected from the Routeviews project [4] and "stitches together" known links, thus constructing paths to our target sites from every AS in the Internet. (2) C-BGP [15] that simulates the BGP session between ASes and creates the AS-level graphs.

[1] A customer AS routes traffic through its providers; but providers do not route "through" traffic through their customers. The only traffic a provider sends a customer, is meant for that customer, or *its* customers, and so on.

Chapter 2

Literature Survey

A great deal of previous work has focused on different aspects of botnets, their detection and defense [5, 7, 11, 17]. There is abundant literature on Botnet detection detection tools. As botnets represent a multifaceted and distributed threat, these tools detect from different aspects, for example, deployment location (host-based, network-based), depth of analysis (header-based, Deep Packet Inspection (DPI)), scope of analysis (single bot behavior, group behavior), detection methodology (signature-based, anomaly / behavior-based). Snort [16], is an open source IDS that boasts of an extensive library of malware-related signatures. Some of these signatures are specific to botnets and are useful in detection of known threats. BotSniffer [9], detects bots by looking for group behavior in network activities as bots are pre-programmed to respond to commands from the C&C server in a certain way. BotMiner [8], detects bots in a network by clustering similar communication and malicious activity patterns and then performs cross-cluster correlation. BotTracer [12] employs virtual machine techniques to detect botnets based on three invariants in the life of a botnet; automatic startup of bot with no user intervention (startup), C&C establishment (preparation) and attack.*etc.*.

But, where to place the *defenders*, is still an unexplored area. Sweeny *et al.,* [19] developed the concept of "Cyber High ground". An attacker who controls this cyber high ground gains a superior capability to achieve his malign objectives.They assume, the that defenders are randomly placed in the network topology, and an intelligent adversary can bypass them with tactically placing the bots by exploiting the topology knowledge.

In this work we answer the question "how hard its is for an attacker to accomplish its malign intentions when defenders are *intelligently* installed in the physical network topology."

Chapter 3

Proposed Methodology

We used C-BGP, a popular tool for AS topology construction. This tool requires AS relationships as input file and runs BGP session between the ASes. Once The BGP session is completed, we run AS level traceroute command to obtain paths between all-to-all pair of ASes of a given country. We merge the paths to obtain the complete AS-level topology of the country. The aim is to first find the cyber defense line of tyhe country and to validate how effective it is in handling attacks from known malicious ASes of the globe.

3.1 Identifying Cyber Defense Line

Cyber defense line is the collection of strategically important ASes that could intercept all network paths leading to important destinations of the country.

We formulate this problem as finding "minimum cardinality cut", such that all communication paths between all source (s) and target (t) pair transit this minimum cut.

There are multiple minimum cardinality cut sets possible for this directed graph. *Which cut to select for placement of defenders?* We selected those ASes which are *strategically important.* These are the five characteristics on which strategic importance of the AS depends:

1. Provider Degree : number of provider an AS has
2. Customer Degree: number of customers an AS has
3. Peer Degree: number of peers an AS has
4. Cone Size: set consisting of the AS itself and its customer descendants.
5. Betweenness: is a measure that quantifies the centrality of a vertex in terms of its involvement in connecting pairs of vertices in a graph

All characteristics have their own importance for finding the appropriate defense line. For example, a sophisticated attacker might select an AS which has high provider degree/peer degree,

if one provider fails (or detects its malign interests), it can use other provider for uninterrupted attack. Similarly, a transit AS with high customer degree/cone size is a good choice for defender placement, as many malicious ASes hide behind the upstream transit AS, so as to achieve high unobservability [10]. Finally, betweenness of a vertex is the number of AS pairs it serves, hence it is good heuristic for traffic flows through the vertex. An AS with high betweenness value is also a good choice for defender placement.

We calculated best five different cuts (for each aforementioned characteristics). Each characteristic holds some strategic importance and are important heuristics for finding defense line.

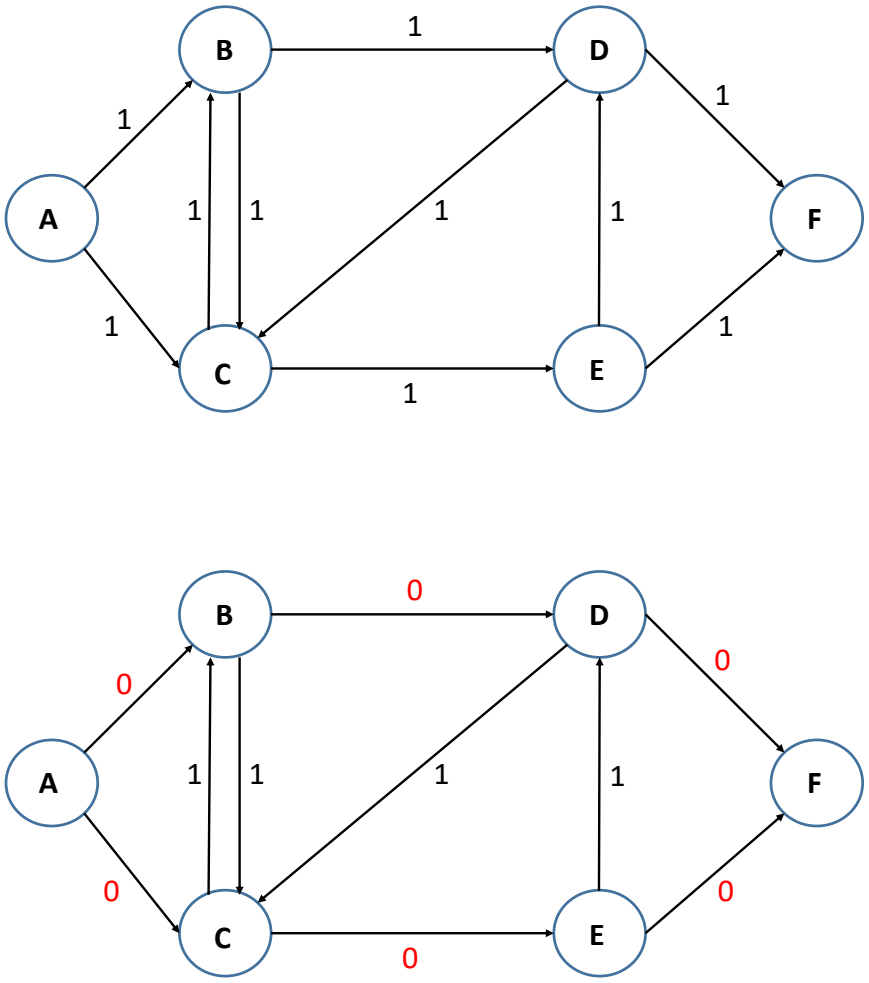

Figure 3.2: Residual AS topology

3.1.1 Naive approach

The aim is to find the set of ASes that intercept all the Internet paths of the country. We adopted the following approach

1. Annotate the Country's AS topology with all the edge weights to be one (shown in figure 3.1).
2. For every *s-t pair*, we obtain the residual graph of the AS topology using Ford-Fulkerson. Figure 3.2 represents the *residual graph* of A-F as *s-t* pair.
3. In residual graph, for paths whose all edges are zero, we selected them for cut computations. The number of such paths in the residual graph is the cardinality of the cut set (for graph in figure 3.1, cut size is two).
4. We selected all possible combinations of cuts (in figure 3.2, (B,C), (B,E), (D,C), (D,E) are four possible cuts for the said *s-t* pair).
5. Based on different AS characteristics, we found different cuts that maximizes the characteristic value.
6. We union the cuts for all *s-t* pair of the graph to get the complete cut of the graph.

3.1.2 Advanced Approach

1. Annotate the AS topology with AS characteristic value as node weights
2. Apply Graph transformation such that weight on nodes shift to edges preserving the same Graph properties.
3. For every *s-t* pair, apply Ford Fulkerson algorithm
4. Obtain Residual Graph
5. Find the cut that has maximum Characteristic value.
6. We union the cuts for all *s-t* pair of the graph.
7. Cut was selected with maximizing the weights, hence it is not minimal.
8. To minimize the cut we adopt the following scheme
    - Sort the cut nodes based on the frequency of occurrence in cuts of different s-t pair (in descending order).
    - Starting with first node in the sorted list check whether all the paths are intercepted by the the node

- if not; then with first and second node check whether all the paths are intercepted by the the nodes
- when all the paths are intercepted by nodes, we have the minimum cardinality cut with maximized weights.

3.2 Effective Attack Space

The Internet has grown into an enormous network offering a variety of services, which are spread over a multitude of domains. Unfortunately, many ASes not only host normal users and content, but also malicious content used by attackers to accomplish their wrong deeds. In ASMATRA [21], authors propose a method for detecting ASs that provide transit service for malware hosters, without being malicious themselves. We obtained the list of transit ASes as well as maligned ASes from [2]. There are total of about 11,100 ASes in our list known to participate in malicious activities. We mapped paths from these ASes to our selected countries (ASes headquartered in them). We later find out the defense line of each country specific to attack from these malicious ASes.

Chapter 4

Evaluation and Results

4.1 Experimental Results

Continuing from the description of our experiment in the previous section, in this section we present our results.

4.1.1 Naive Approach

Naive approach is a non polynomial time problem. We begin with analysis of Israel, a country small in network size (with 214 ASes compared to Russia with over 5000 ASes). For only one *s-t* pair, we obtain 30 residual paths as shown in table 4.1.

No. of Paths	**Path Length**
2	7
5	6
8	5
10	4
5	3

Table 4.1: Number of paths in residual graph of one particular *s-t* pair

The total computations require to find all the cuts is 7^2 x 6^5 x 5^8 x 4^10 x 3^5 = 37,924,385,587,200,000,000. Thus, naive approach cannot be adopted for finding the minimum cut.

4.1.2 Advanced Approach

We selected 9 different countries for our analysis, and for each country, we found the cyber defense line involving various cuts of the nations network topology. For five different AS characteristics (explained earlier in section 3.1), we obtain five different cuts for each country. Table 4.2 - 4.10 represents the cyber defense line for various countries. Table 4.2, represents the scenario, where we assume attack (like DDoS) can happen from any AS of the country and can be targeted to

important Internet destinations (called as victims) of the same country. First column represents, AS characteristics, and rest columns denote different types of victim sets. In "all to all" column, values represents the number of defenders required to safeguard every AS of the country from attack happening from anywhere in the country. But, in general, nation will first aim to defend its critical infrastructure against such attacks, thus in third column, "all to important destinations", we selected three important destination sets *viz.,* Banking websites (B), Government Websites (G) and Transport Websites (T). Each table entry corresponds to number of defenders (*i.e.* cut size) required to protect these destinations from the attack. Finally entries of column four "all to top DNS", represents defenders required to protect DNS infrastructure.

It can be easily depicted from the tables that, countries significantly differ in their network topological structures and thus have different cut sizes. For instance, in India, we require 291 ASes (from total of 1176 nodes) for defender placement whereas, for Argentina defender count is 255 (out of 492 ASes) suggesting that Argentina has more distributed and flattened network structure compared to India.

For some countries like Egypt, there is a same set of ASes (total of seven), in cut calculation for all AS characteristics. It shows that for entire network, a very strong defense line is feasible consisting of these ASes only.

But, there is a caveat, among all the cuts for all the countries boundary ASes alone capture more than 99% of the intra country paths. This exercise of cut calculations is only meaningful, if government aims to safeguard all its ASes, with every path being intercepted by the defender cut.

AS Property	**All to All**	**All to Imp.**				**All to top DNS**			
	$\|CutSet\|$	**B**	**G**	**T**	$B \cup G \cup T$	**25%**	**50%**	**75%**	**100%**
Customer Degree	218	40	5	25	43	57	89	116	145
Provider Degree	217	31	5	25	35	57	89	116	145
Peer Degree	208	32	5	20	35	57	89	116	145
Cone Size	201	40	5	21	42	57	89	115	141

Table 4.2: China Defense Line (Total AS count: 345)

AS Property	**All to All**	**All to Imp.**				**All to top DNS**			
	$\|CutSet\|$	**B**	**G**	**T**	$B \cup G \cup T$	**25%**	**50%**	**75%**	**100%**
Customer Degree	392	86	54	65	98	128	149		348
Provider Degree	405	86	59	82	102	128	149		347
Peer Degree	412	82	67	78	95	128	149		347
Cone Size	588	55	40	65	80	93	114		274
Betweenness	291	82	53	65	93	117	135		347

Table 4.3: India Defense Line (Total AS count: 1176)

AS Property	All to All	All to Imp.				All to top DNS			
	$\|CutSet\|$	**B**	**G**	**T**	$B \cup G \cup T$	**25%**	**50%**	**75%**	**100%**
Customer Degree	155	56	33	9	53	81	101	117	136
Provider Degree	158	29	46	14	49	77	102	117	136
Peer Degree	103	22	40	13	40	72	78	85	92
Cone Size	164	44	31	9	47	76	92	107	126
Betweenness	147	49	32	9	52	78	96	104	119

Table 4.4: Iran Defense Line (Total AS count: 407)

AS Property	All to All	All to Imp.				All to top DNS			
	$\|CutSet\|$	**B**	**G**	**T**	$B \cup G \cup T$	**25%**	**50%**	**75%**	**100%**
Customer Degree	44	3	3	4	5	10	19	20	25
Provider Degree	44	4	4	4	5	10	19	21	25
Peer Degree	43	4	4	4	5	10	19	20	25
Cone Size	110	4	4	4	6	10	18	19	30
Betweenness	43	9	9	4	9	10	19	20	25

Table 4.5: Israel Defense Line (Total AS count: 214)

AS Property	All to All	All to Imp.				All to top DNS			
	$\|CutSet\|$	**B**	**G**	**T**	$B \cup G \cup T$	**25%**	**50%**	**75%**	**100%**
Customer Degree	45	12	8	4	13	18	29	31	36
Provider Degree	45	10	7	3	11	18	21	31	36
Peer Degree	36	12	8	4	13	18	21	27	37
Cone Size	53	10	7	3	11	17	20	29	34
Betweenness	38	10	7	3	11	15	18	23	24

Table 4.6: Pakistan Defense Line (Total AS count: 87)

AS Property	All to All	All to Imp.				All to top DNS			
	$\|CutSet\|$	**B**	**G**	**T**	$B \cup G \cup T$	**25%**	**50%**	**75%**	**100%**
Customer Degree	7	5	5	5	5	5	7	8	9
Provider Degree	7	5	5	5	5	5	7	8	9
Peer Degree	7	5	5	5 5		5	7	8	9
Cone Size	7	5	5	5	5	5	7	8	8
Betweenness	7	5	5	5	5	5	7	8	9

Table 4.7: Egypt Defense Line (Total AS count: 55)

AS Property	All to All	All to Imp.				All to top DNS			
	$\|CutSet\|$	**B**	**G**	**T**	$B \cup G \cup T$	**25%**	**50%**	**75%**	**100%**
Customer Degree	283	34	29	36	41	63	117	161	195
Provider Degree	252	39	39	40	45	61	119	160	198
Peer Degree	263	43	43	45	49	61	120	164	198
Cone Size	300	36	32	34	40	76	115	159	192
Betweenness	255	34	30	35	41	64	106	139	167

Table 4.8: Argentina Defense Line (Total AS count: 492)

AS Property	**All to All**	**All to Imp.**				**All to top DNS**			
	$\|CutSet\|$	**B**	**G**	**T**	$B \cup G \cup T$	**25%**	**50%**	**75%**	**100%**
Customer Degree	67	11	32	23	33	34	36	48	56
Provider Degree	74	14	32	19	34	33	35	48	56
Peer Degree	57	11	32	23	35	33	35	48	52
Cone Size	65	13	32	22	33	34	36	47	54
Betweenness	60	13	30	22	32	33	34	42	47

Table 4.9: Vietnam Defense Line (Total AS count: 206)

AS Property	**All to All**	**All to Imp.**				**All to top DNS**			
	$\|CutSet\|$	**B**	**G**	**T**	$B \cup G \cup T$	**25%**	**50%**	**75%**	**100%**
Customer Degree	245	5	7	20	20	51	73	102	127
Provider Degree	246	8	8	16	18	51	76	103	128
Peer Degree	100	8	9	20	21	51	54	103	128
Cone Size	350	5	6	17	19	53	94	134	174
Betweenness	82	6	6	17	19	44	64	73	82

Table 4.10: South Korea Defense Line (Total AS count: 711)

Chapter 5

Future Work and Limitations

5.1 Future Work

We aim to extend this research for major nations states like the US, Russia, Australia and Germany *etc.* We plan to validate our present results with another popular network mapping approach given by Qiu and Gao [14] in future. We also aim to analyze a scenario, where an attack may happen from a sophisticated adversary which intelligently place *bots*, with an intent to avoid our defender sets. We also aim to explore the feasibility of identifying a minimal set of network points (called as *cyber high ground*) an adversary may identify which may be used for monitoring traffic to a chosen network destination. This may be applicable for both network monitoring and cyber warfare scenarios.

AS is not a mere node, rather a collection of thousand of routers, at which router (or routers), defense infrastructure should be installed is also left as a future exercise.

5.2 Limitations

We rely on C-BGP simulator for network mapping, this tool takes caida relationship file as input and generates AS level map but it does not incorporate real BGP paths. The accuracy of our map is the artifact of the underlying simulator.

The list of important Internet destinations categorized into (banking, government and transport) is not exhaustive. We collected all the possible destinations publicly available.

Chapter 6

Conclusion

6.1 Concluding Remarks

Considering the rise in large scale targeted attacks like Mirai and Wanna Cry, it becomes imperative for countries to strengthen their defense line in cyber realm. To best of our knowledge, this is the first study for measuring the potential defense capabilities of various nation states against large scale attacks (like DDoS). The initial results reveal that, countries are significantly similar in network structures, all being hierarchical (with few ASes being central an important). Our initial intuition was, that border ASes of the country primarily transports foreign traffic, internal ASes contribute heavily, towards the intra country traffic. Thus, we mapped the country's network topology and found such cuts which capture 100% intra country paths. To our surprise we found that:

- All the boundary ASes are part of the cut
- Boundary ASes (less than 50% of the cut size) collectively captures more than 99% of the intra country AS paths and remaining 1% paths are intercepted by significantly large number of internal ASes (more than 50% of the internal paths).
- In boundary ASes also, less than 10 ASes capture more than 90% of the paths.

Our results were surprising as boundary ASes of all our sample countries are not only transporting foreign traffic rather they are also the heavy hitter ASes for the country's inbound traffic. Boundary ASes cumulatively capture more than 99% of the intra-country AS paths). This makes the government task easy as for strong safeguarding they need to place defenders in only handful ASes of their country.

Bibliography

[1] Archipelago (ark) measurement infrastructure. http://www.caida.org/projects/ark/.

[2] Malicious ases list.

[3] Qi points : placing decoy routers in the internet (Technical Report. https://repository.iiitd.edu.in/jspui/handle/123456789/442.

[4] Route views project. http://archive.routeviews.org/.

[5] Bhuyan, M. H., Kashyap, H. J., Bhattacharyya, D. K., and Kalita, J. K. Detecting distributed denial of service attacks: methods, tools and future directions. *The Computer Journal 57*, 4 (2013), 537–556.

[6] Gao, L. On inferring autonomous system relationships in the internet. *IEEE/ACM Transactions on Networking (ToN) 9*, 6 (2001), 733–745.

[7] García, S., Zunino, A., and Campo, M. Survey on network-based botnet detection methods. *Security and Communication Networks 7*, 5 (2014), 878–903.

[8] Gu, G., Perdisci, R., Zhang, J., Lee, W., et al. Botminer: Clustering analysis of network traffic for protocol-and structure-independent botnet detection. In *USENIX security symposium* (2008), vol. 5, pp. 139–154.

[9] Gu, G., Zhang, J., and Lee, W. Botsniffer: Detecting botnet command and control channels in network traffic. In *NDSS* (2008), vol. 8, pp. 1–18.

[10] Howard, R. *Cyber fraud: tactics, techniques and procedures*. CRC press, 2009.

[11] Khattak, S., Ramay, N. R., Khan, K. R., Syed, A. A., and Khayam, S. A. A taxonomy of botnet behavior, detection, and defense. *IEEE communications surveys & tutorials 16*, 2 (2014), 898–924.

[12] Liu, L., Chen, S., Yan, G., and Zhang, Z. Bottracer: Execution-based bot-like malware detection. *Information Security* (2008), 97–113.

[13] Madhyastha, H. V., Isdal, T., Piatek, M., Dixon, C., Anderson, T., Krishnamurthy, A., and Venkataramani, A. iplane: An information plane for distributed

services. In *Proceedings of the 7th symposium on Operating systems design and implementation* (2006), USENIX Association, pp. 367–380.

[14] Qiu, J., and Gao, L. As path inference by exploiting known as paths. In *Global Telecommunications Conference, 2006. GLOBECOM'06. IEEE* (2006), IEEE, pp. 1–5.

[15] Quoitin, B., and Uhlig, S. Modeling the routing of an autonomous system with c-bgp. *Netwrk. Mag. of Global Internetwkg. 19*, 6 (Nov. 2005), 12–19.

[16] Roesch, M., et al. Snort: Lightweight intrusion detection for networks. In *Lisa* (1999), vol. 99, pp. 229–238.

[17] Silva, S. S., Silva, R. M., Pinto, R. C., and Salles, R. M. Botnets: A survey. *Computer Networks 57*, 2 (2013), 378–403.

[18] Subramanian, L., Agarwal, S., Rexford, J., and Katz, R. H. Characterizing the internet hierarchy from multiple vantage points. In *INFOCOM 2002. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE* (2002), vol. 2, IEEE, pp. 618–627.

[19] Sweeney, P., and Cybenko, G. Identifying and exploiting the cyber high ground for botnets. In *Cyber Warfare*. Springer, 2015, pp. 37–56.

[20] Tozal, M. E. Autonomous system ranking by topological characteristics: A comparative study. In *Systems Conference (SysCon), 2017 Annual IEEE International* (2017), IEEE, pp. 1–8.

[21] Wagner, C., François, J., State, R., Dulaunoy, A., Engel, T., and Massen, G. Asmatra: Ranking ass providing transit service to malware hosters. In *Integrated Network Management (IM 2013), 2013 IFIP/IEEE International Symposium on* (2013), IEEE, pp. 260–268.