

Ramadevu Bhavani Srinivas (BR237643)

bramadevu@albany.edu

REPORT

Project- 2: Internet Path Analysis using PlanetLab.

Abstract:

This project has basically given practical knowledge in networking. In our paper we have up to date measurement results on the internet path analysis using PlanetLab. The points made in this report are based on a small scale experimental observation which would not include all the points about the network path analysis but some. There would 10 different nodes selected in planetlab which were being accessed for conducting this experiment of running traceroute and ping for every consecutive hour and the output information has been fetched and then accessed for analysis. With the fetched data, I have been analyzing the values of RTT, number of hops, packet loss, network congestion and network outages and routing path analysis. What does these data get us into? The answer to this would be show the internet stability and would give us hands on experience to know what causes the internet unstable and what could be done. One important result is the packet loss among all the hops is around 1.9%

1. Motivation: Why is Internet path stability important to measure?

In our daily life we have internet as one of the main dependent resource which we might not have realized. With the growing number of internet users increased the internet traffic too which leads to many known problems such as delayed website responses, unreachable websites, Error 404 and such are familiar to all users. The reason behind these anomalies are caused by servers overload sometimes or browser unresponsiveness sometimes or another major factor is internet routing instability. So this makes a point that internet today is lagging in for one such reason would be grown users and the next one would be as internet is network or networks, consisting of many parties who run their networks independently which makes the internet routing particularly difficult. The worst thing then that was the benefit of these parties are sometimes conflicting. So this routing anomalies has to be studied further and to find a best stable routing algorithm is next to impossible. Hence, this is where the idea of making it better could help but how? By studying the internet stability would help us know what are the main

sources of problem and where exactly the problem arise. With this study we can have a field of research in those fields to help the performance go better. This explains why the internet path stability measurement is important.

2. Introduction:

In order to measure the internet path stability we use the PlanetLab nodes to have a measurement among well spread geographical range. The first step in this project was to selecting 10 nodes based on the checklist which is one pair should be transatlantic, one transpacific, two or more from other continents then North America and rest could be from North America. For this project the nodes which has been taken are denoted as A, B, C and so on and figure 2.1 shows the table of nodes and the location of node. So In rest of the paper node1 “planet-lab1.itba.edu.ar” would be denoted A or node A for better understanding as the node links might look similar. The two functions we have used to measure the path stability are traceroute and other one is ping.

NODE LINK	Continent/Country	Alphabetically Denoted
1. planet-lab1.itba.edu.ar	South America	A
2. planetlab4.mini.pw.edu.pl	Europe (New Zealand)	B
3. planetlab4.goto.info.waseda.ac.jp	Asia(Japan)	C
4. planetlab2.utdallas.edu	North America(US)	D
5. pl1.cs.montana.edu	North America(US)	E
6. plonk.cs.uwaterloo.ca	North America(Canada)	F
7. pl2.sos.info.hiroshima-cu.ac.jp	Asia(Japan)	G
8. planetlab1.cs.otago.ac.nz	Europe(New Zealand)	H
9. planetlab2.aut.ac.nz	Europe(New Zealand)	I
10. saturn.planetlab.carleton.ca	North America(Canada)	J

Figure2.1 Nodes and alphabetically denoted.

Traceroute is computer diagnostic tool for displaying the route (path) and measure transit delays of packets across Internet Protocol. Ping on the other hand is administrative software utility used to test the reachability of a host on internet protocol. Using the planet lab nodes we are going to use these tools to know the transit delays, reachability of a host and many other stuff. The first we have to do is to get inside in any one of the node and run and these tools to reach other node and get the important details as output of these tools. The data output for these tools could be collected while making them work for 2 weeks continuously and in every hour these tools are run and the data has been collected. This happens to the first phase in the project and when it comes to the second phase we have analysis of data we have collected. We are going to use a tool called Gawk or awk which is known to be one among the powerful tools for analysis. Using these tools we collect the important parameters from the data output and make some conclusions based on it. Let's now talk about how to achieve the data.

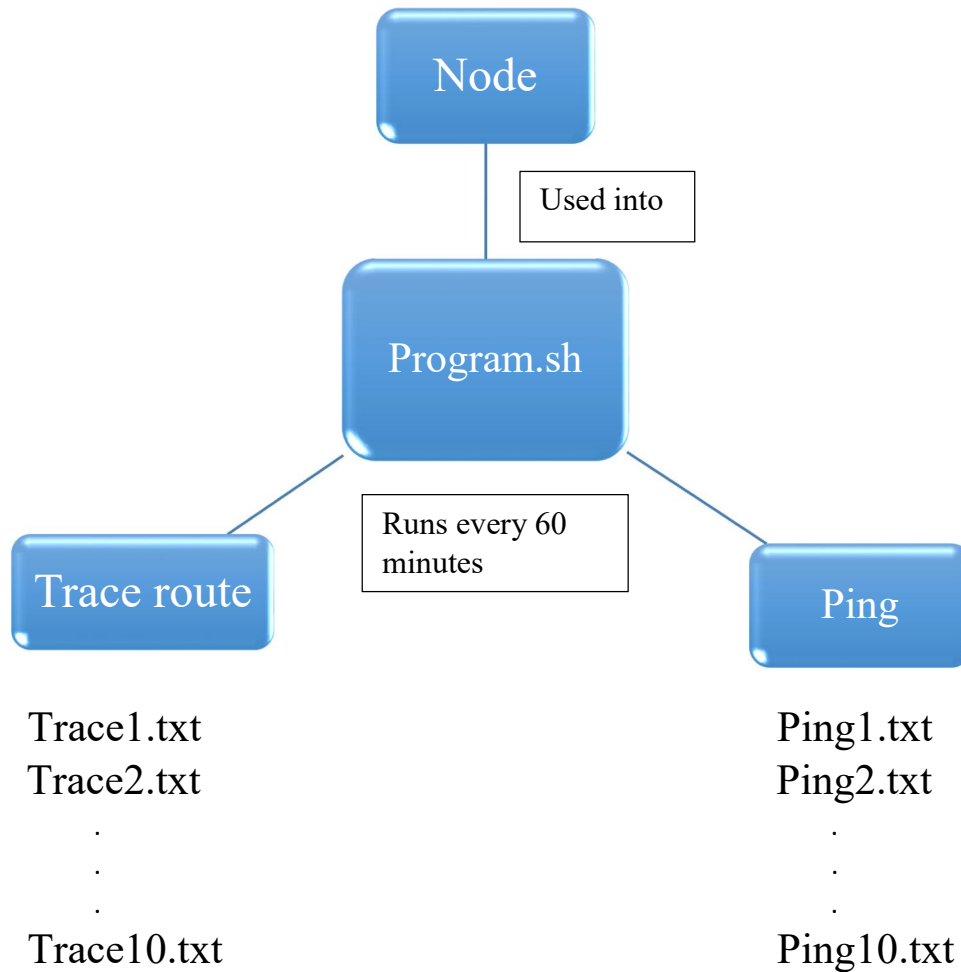
3. Methodology:

Our methodology has two phases one is measurement framework and the other one is analysis frame work. We will go through both of these phases in details and then comes details of each analysis parameter procedure which is being used for extraction of data from the raw data that we have collected over a period of 2 weeks of time. The main apparatus for this experiment was Planet lab nodes, which are being accessed for utilizing tools like traceroute and ping at different geographical locations. For analysis, I have used grep, gawk which are really powerful tool for analyzing and lastly the data presentation in the respective format and data processed in excel. This is the overview of tools of software and hardware that I have used. Here are the pairs of node I have used in my project and their alphabetical representation of tracerouting and ping would be like this throughout this project.

Nodes in the	Pair	Alphabetical representation
South America	Europe (New Zealand)	A->B, B->A
Asia(Japan)	North America(US)	C-D,D->C
North America(US)	North America(Canada)	E->F,F->E
Asia(Japan)	Europe (New Zealand)	G->H,H->G
Europe (New Zealand)	North America(Canada)	I->J,J->I

3.1 Measurement Framework:

In this frame work, firstly I had to select 10 nodes which I have already shown in the table 2.1. So that was my nodes which has been tested after selection and then worked on in this project. The selected node details and code for entering into a node has been well studied and now here comes the part where I use the basic tools for this project that are traceroute and ping. I come up with a program which would be automated to run the traceroute from entering into one node to other node of the pair and then reverse traceroute for same nodes. Likewise I'll be handling all the 10 nodes in 5pair of nodes and would be running traceroute and ping for them consecutively every hour for 2 weeks for a decent data output from these tools. The period of two weeks is for making the data consistent to draw the conclusion from it. The output of tools (traceroute and ping) would be stored in accordance that each node's traceroute is stored separately which in the time of analysis would make the work simpler. So this the whole flow of measurement framework. We can visualize this flow in the diagram below Fig 3.1



The output is stored for each nodes traceroute as in the name format given in the diagram. This would help us remember less the name or address of nodes instead would be in alphabetical and its files would be in sequential order. So in this phase this is our only goal to get the data of nodes from using these tools of traceroute and ping to store in a systematic manner and use it for analysis phase.

The programs I have used to put the automated data into files was in bash programming and the sample code would look something like this

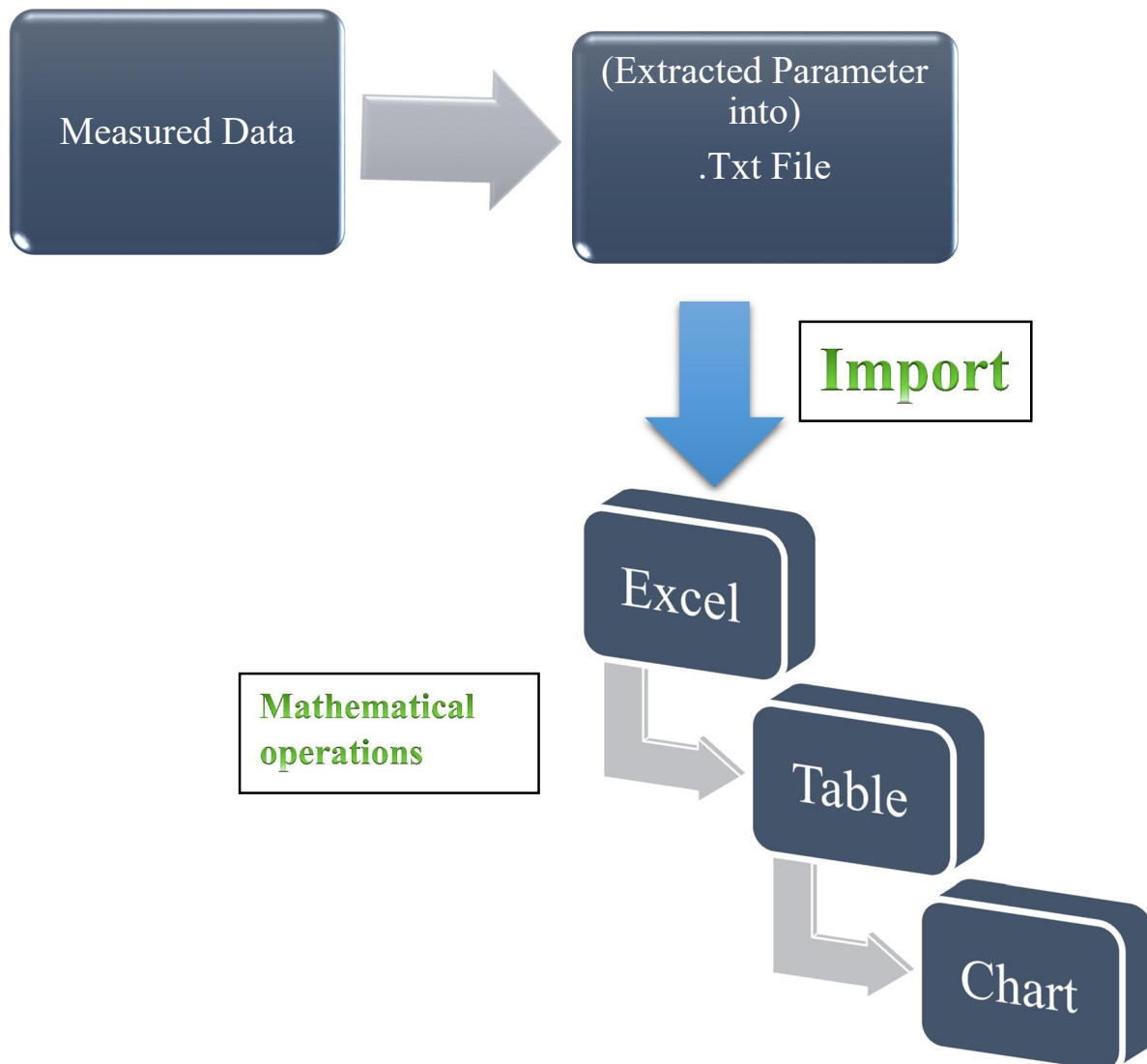
```
Program1.sh
#!/bin/sh

nodeA="planet-lab1.itba.edu.ar"
nodeB="planetlab4.mini.pw.edu.pl"

while true
do
run="ssh albany_ccn6@$nodeA ping -c 20 $nodeB >>
/home1/s/b/br237643/trace1.txt"
eval $run
sleep 3600
done
```

3.2 Analysis Framework:

This is the second phase in the methodology and also the final one. In this phase we analyze the data that has been stored in files of trace1.txt, ping1.txt and so on. First we have finalized the parameters that we need to analyze for studying. While starting this phase I had a little idea about what I want then as I studied the traceroute and ping tools characteristics and the data requirement for studying internet routing stability I had more parameters I wanted to use. The flow chart (fig. below) for analysis framework would give the overview of what we have to do here.



The first job in this phase is to extract the data from the files we have stored in the measurement phase. The tool we use for extracting the data we want is gawk, grep. These are the tools I have used in this project but there are some more options for this. The first parameter I wanted was the path length. Using the gawk commands I have extracted the path length (hop count) from the data files I have collected over a period of two weeks. The sample command is:

```
cat /home1/s/b/br237643/trace.txt |gawk '(/traceroute/) {print a} {a = $1}' > /home1/s/b/br237643/ana.txt
```

The output for this command would be the last hop count it has encountered before starting another traceroute action. Using the commands in similar fashion I have stored the analyzed data into named txt files. These txt files are then imported in excel for mathematical operations like calculating the min, max average and SD etc.

The data in the excel are then sorted and necessary mathematical operations were performed and tabular sorted data is obtained. These data can then be used for the graph or chart representation. The parameters I have analyzed for this project are time-latency, hop count, the outages, packet loss then processing of these data has helped me write this report for the project.

4. Analysis:

Let us now look at the part of data analysis where all the data output produced by the tools has been processed and based on observations we make some points.

4.1 Path Length and Variations in Measurements.

The path length in our project would be the hop count given by the tool traceroute which will be considered as the path length. We are going to analyze the path length for all the pair of nodes paths that is A->B, B->A, C->D and so on. The important thing which is noticeable here is the path length from A->B would be same as B->A.

	A->B	B->A	C->D	D->C	E->F	F->E	G->H	H->G	I->J	J->I
Average	15.10714	15.21429	11	17	12	11	18.1875	18	20	19
Min	15	15	11	17	12	11	18	18	20	19
Max	16	18	11	17	12	11	19	18	20	19
SD										
STDEV	0.310685	0.591662	0	0	0	0	0.392067	0	0	0
SD							0.390312			
STDEV.P	0.309295	0.589015	0	0	0	0		0	0	0
SD										
STDEV.s	0.310685	0.591662	0	0	0	0	0.392067	0	0	0

Figure 4.1 Table for Path length

As we can observe that all the pair have same or nearly same path length. The pair here means A->B and B->A (reverse and flow) of the packets in the networks have same path which has been taken from the traceroute output. However, we have an exception here with C->D and D->C the path length varies by a big margin. The average path length from C->D is 11 whereas from D->C is 17.

What would be the cause of such huge difference in the number of hops between two nodes?

So for the path C->D (Japan to US) and D->C (US to Japan) is the exception case here, which would tell us a fact about networking now. For a same path on different direction we could have different number of hops. There would be several causes for this difference in Hop Count (Path Length). *First would be Assumptions of symmetry, the server algorithm for packet transmission to further servers would be different which has caused the change in the number of hops. Second one could be Load-balancing and contemporaneous path changes and there might be different causes which we couldn't figure out with this experiment.*

For the cases where standard deviation is not zero, the main cause would be network congestion due to which the packet has to take alternate path or longer path than usual and resulted in the path difference. Also a point to observe that minimum value for the hop count is near to the average value. The reason behind this would be most of the time internet routing is stable.

Let us now consider the traceroute output to see how it differs the count by 17 and 11.

The image shows two Notepad windows side-by-side, displaying traceroute results. The left window, titled 'Sample2.txt - Notepad', shows the output for a path from C to D. The right window, titled 'Sample1.txt - Notepad', shows the output for a path from D to C. Both outputs list hop numbers, IP addresses in brackets, and three round-trip time measurements in milliseconds.

```

Sample2.txt - Notepad
File Edit Format View Help
1 133.9.81.190 (133.9.81.190) 0.732 ms 1.179 ms 1.610 ms
2 cl2948gl3.goto.info.waseda.ac.jp (133.9.81.254) 0.661 ms 0.869 ms 1.101 ms
3 133.9.77.62 (133.9.77.62) 0.415 ms 0.426 ms 0.416 ms
4 tokyo1-RM-XE-9-0-11-20.s5.sinet.ad.jp (150.99.187.69) 0.748 ms 0.738 ms 0.736 ms
5 tokyo1-GM-AE0-100.s5.sinet.ad.jp (150.99.64.29) 0.704 ms 0.690 ms 0.686 ms
6 lax-GM-ET-2-1-0-100.s5.sinet.ad.jp (150.99.89.243) 99.321 ms 99.317 ms 99.309 ms
7 abilene.lax.gw.sinet.ad.jp (150.99.199.94) 107.900 ms 108.014 ms 108.001 ms
8 et-1-0-0.111.rtr.hous.net.internet2.edu (198.71.45.20) 140.479 ms 140.465 ms 140.452 ms
9 74.200.187.33 (74.200.187.33) 146.056 ms 146.047 ms 146.035 ms
10 vl-430-utd-ntg-gw1.dfw.tx-learn.net (208.76.227.222) 138.242 ms 138.252 ms 138.241 ms
11 (129.110.125.52) 140.885 ms 140.873 ms 140.975 ms

Sample1.txt - Notepad
File Edit Format View Help
1 (129.110.125.1) 0.170 ms 0.147 ms 0.170 ms
2 vl434-utd-ge-0-1-7-gw2.dfw.tx-learn.net (208.76.224.234) 1.047 ms 1.043 ms 1.027 ms
3 ntg-gw1-dllstx-MX480-lo0.dfw.tx-learn.net (208.76.224.248) 1.060 ms 1.024 ms 0.893 ms
4 dls-bb1-link.telvia.net (213.248.104.81) 0.887 ms 0.870 ms 0.862 ms
5 dls-b21-link.telvia.net (62.115.140.9) 1.364 ms 1.354 ms 1.338 ms
6 ae-18.r07.dllstx09.us.bb.gin.ntt.net (213.248.81.250) 1.842 ms 1.932 ms 1.912 ms
7 ae-5.r22.dllstx09.us.bb.gin.ntt.net (129.250.3.40) 1.585 ms 1.628 ms 1.596 ms
8 ae-5.r22.isanca07.us.bb.gin.ntt.net (129.250.7.69) 33.411 ms 35.793 ms 40.151 ms
9 ae-0.r21.osakjp02.jp.bb.gin.ntt.net (129.250.2.177) 159.301 ms * 148.623 ms
10 ae-5.r22.osakjp02.jp.bb.gin.ntt.net (129.250.6.192) 147.531 ms 152.193 ms 168.797 ms
11 ae-2.r01.osakjp02.jp.bb.gin.ntt.net (129.250.3.199) 151.080 ms 150.984 ms ae-1.r01.osakjp02.jp.bb.gin.ntt.net (129.250.2.255) 179.759 ms
12 ae-0.sinet5.osakjp02.jp.bb.gin.ntt.net (61.200.91.154) 150.674 ms 138.182 ms 146.353 ms
13 tokyo1-RM-ET-4-1-0-152.s5.sinet.ad.jp (150.99.71.104) 150.935 ms 144.209 ms tokyo1-RM-ET-5-1-0-1152.s5.sinet.ad.jp (150.99.90.28) 140.407 ms
14 waseda.gw.sinet.ad.jp (150.99.187.70) 143.922 ms 138.282 ms 143.886 ms
15 cl2948gl3a.goto.info.waseda.ac.jp (133.9.77.61) 144.078 ms 145.363 ms 138.663 ms
16 mbone-goto.goto.info.waseda.ac.jp (133.9.81.194) 138.753 ms 144.804 ms 144.445 ms
17 planetlab4.goto.info.waseda.ac.jp (133.9.81.164) 138.333 ms 140.866 ms 138.297 ms
  
```

In C->D, the path followed is from Colorado but whereas in D->C the path is followed from Michigan. Hence, so this difference in routing is causing the change in the Hop count.

4.2 Detection of outages throughout the project.

As we have already mentioned the methodology for the examining the outages in the path of the traceroute. By the help of analysis tool gawk we can figure the place where the probe is lost or couldn't be processed further. The outages in each path is represented in the graph below figure 4.2.1

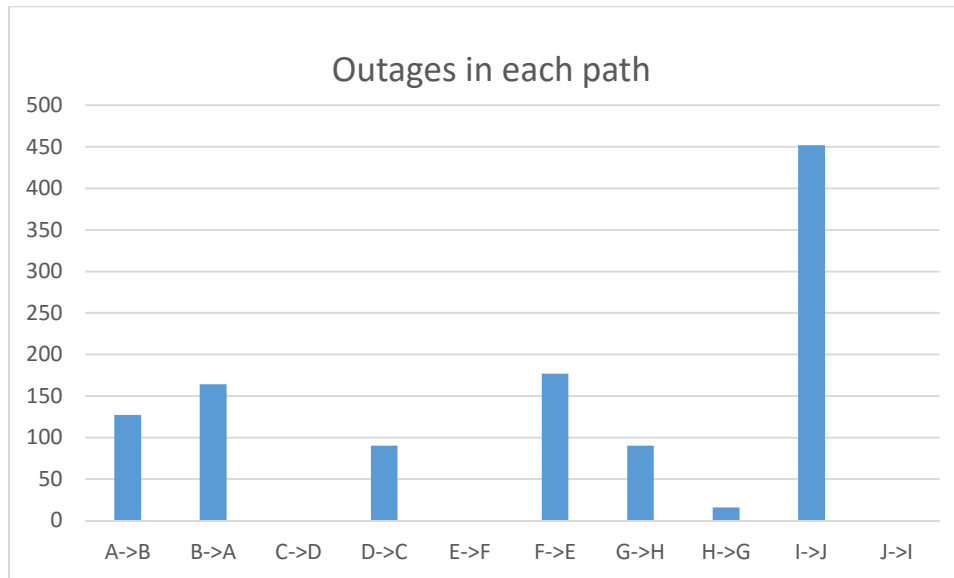
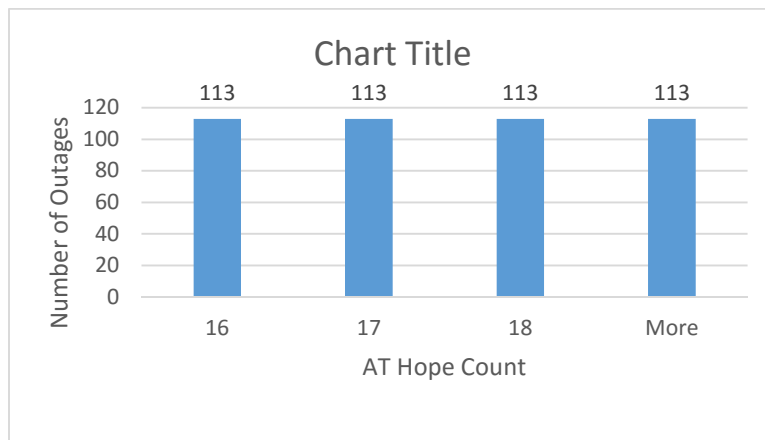


Figure 4.2.1 Number of times outages that has been experienced in each path

There is a specific pattern in these outages when we look at the place or server or number of hop when have failed to get the probe back in traceroute points us to a specific pattern. Let's us examine one pattern of number of hops at which the outages has occurred in I->J in figure 4.2.2



So this tells us that in that path at a specific hop the server is either in load or the congestion is always there that it causes consistent outages in the network. To observe rest of the outages in path you can view the excel file in DATA ANALYSIS/ OUTAGES/outages.xls file. Let's now

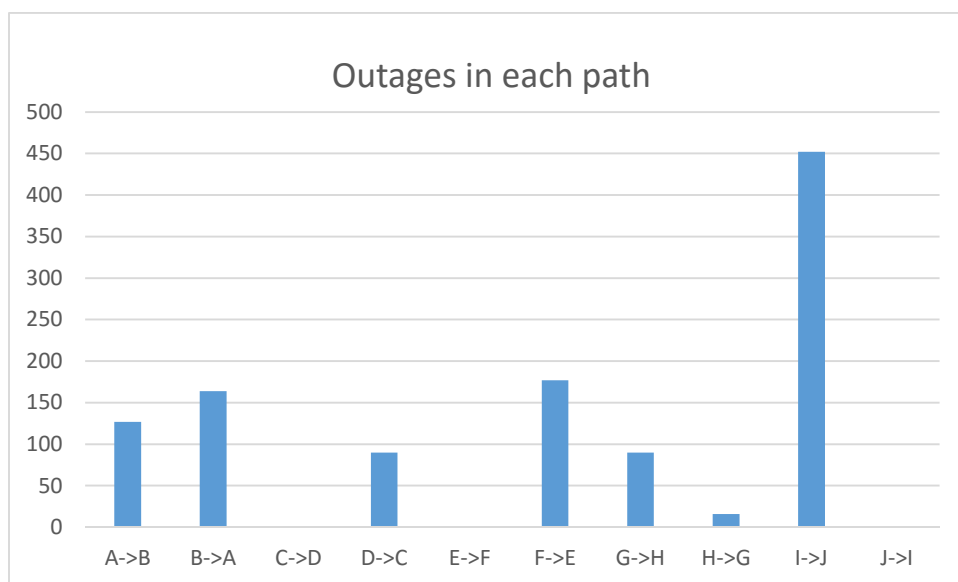
consider the paths which has no outages seems like the best network has been among those paths. But the fact is E->F (US-CANADA) has zero outages among the intra continents link. So that infers that the error rate or outages in intra continent link is less than inter continent links.

Another important result while considering the pairs, the pair which has highest outages includes I->J and J->I with count of 452 number of outages. The nodes are from Europe and Canada. But the pair with minimum number of outages is USA to Japan. Isn't this irony?. So this where, it is shocking to see that the outages doesn't really depend on geological location of the nodes but the servers and internet routing stability. USA Japan are geographical longest distance when compared to Canada-Europe.

We have two types of outages, one is temporary outages and the second is the permanent outages. There could be different causes for each of these outages. Let's consider these two outages for our experimental data.

4.2.1. Temporary outages

The next topic we discuss here is temporary network outages. When a sequence of consecutive traceroute probes are lost, the most likely cause is either a temporary loss of network connectivity, or very heavy congestion lasting 10's of seconds. In our experiment we have experienced some of the temporary outages. In our experiment we have taken account of only temporary outages since it was just two weeks of data measurement. The figure above figure 4.2.1 shows the temporary outages.



To understand the cause of the temporary outages we need more details such as if the probe was lost in the traceroute it should maintain a log of error message saying it is either because of network congestion or protocol unreachable and etc. Here are some of the error message which helps us to determine the cause of the outages.

The traceroute doesn't provide these details when it encounters outage to figure the cause of it.

The !H is a "host unreachable" error message (it indicates that an ICMP error message was received). The trace will stop at this point. Possible ICMP error messages of this nature include:

!H: Host unreachable. The router has no route to the target system.

!N: Network unreachable.

!P: Protocol unreachable.


!S: Source route failed. You tried to use source routing, but the router is configured to block source-routed packets.

!F: Fragmentation needed. This indicates that the router is misconfigured.

!X: Communication administratively prohibited. The network administrator has blocked traceroute at this router.

An Example of temporary outage of I->J Path.

```
traceroute to saturn.planetlab.carleton.ca (134.117.226.180), 30 hops max,
60 byte packets
 1  156.62.231.241 (156.62.231.241)  0.908 ms  0.975 ms  0.964 ms
 2  210.7.38.49 (210.7.38.49)  1.091 ms  1.091 ms  1.081 ms
 3  et-1-2-0-202.pe1.wnpa.akl.aarnet.net.au (182.255.119.204)  1.759 ms
1.754 ms  1.741 ms
 4  et-2-0-0.pe1.msct.nsw.aarnet.net.au (113.197.15.76)  24.552 ms  24.633
ms  24.624 ms
 5  et-1-3-0-199.pe2.brwy.nsw.aarnet.net.au (113.197.15.78)  24.913 ms
24.899 ms  24.867 ms
 6  et-0-0-0.pe1.a.hnl.aarnet.net.au (113.197.15.99)  117.942 ms  117.916
ms  117.912 ms
 7  et-1-0-0.bb1.a.sea.aarnet.net.au (202.158.194.110)  169.480 ms
169.557 ms  169.543 ms
 8  207.231.240.21 (207.231.240.21)  162.990 ms  163.081 ms  163.066 ms
 9  clgr2rtr1.canarie.ca (205.189.32.175)  173.808 ms  173.820 ms  173.811
ms
10  wnpgr1rtr1.canarie.ca (205.189.32.177)  188.160 ms  188.158 ms  188.147
ms
11  toro1rtr1.canarie.ca (205.189.32.181)  221.332 ms  209.432 ms  209.397
ms
12  border3.orion.on.ca (205.189.32.42)  209.880 ms  209.836 ms  209.885
ms
13  be201.p01-toro.orion.on.ca (66.97.16.21)  210.163 ms  210.206 ms
210.252 ms
14  be107.pe01-otwa.orion.on.ca (66.97.16.54)  214.858 ms  215.416 ms
215.495 ms
15  CARLETON-ORION-RNE.DIST1-OTWA.IP.orion.on.ca (66.97.23.142)  214.611
ms  214.673 ms  214.754 ms
16  * * *
17  * * *
18  * * *
19  * * *
20  saturn.planetlab.carleton.ca (134.117.226.180)  214.724 ms  214.726 ms
214.745 ms
```



4.2.2: Long-term outages

We held our experiment using planet lab nodes which are often prone to cause some outages. One of these outage I came across was permission denied due to change in the credentials. The planetLab node keeps maintenance which changes some network information due to which I was unable to access a node. Sometime the planetlab nodes are under repair and cannot be accessed at those time, these types of outages are the long term outages. One of the long-term outages we experienced is shown in figure below.

```
unix1% ssh alban_ ccn6@pl2.eng.monash.edu.au
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@@
@  WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!  @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that the RSA host key has just been changed.
The fingerprint for the RSA key sent by the remote host is
4f:c9:b0:94:17:0d:1d:6e:7a:a2:be:5f:24:e1:cf:05.
Please contact your system administrator.
Add correct host key in /home1/s/b/br237643/.ssh/known_hosts to get rid of this message.
Offending key in /home1/s/b/br237643/.ssh/known_hosts:3

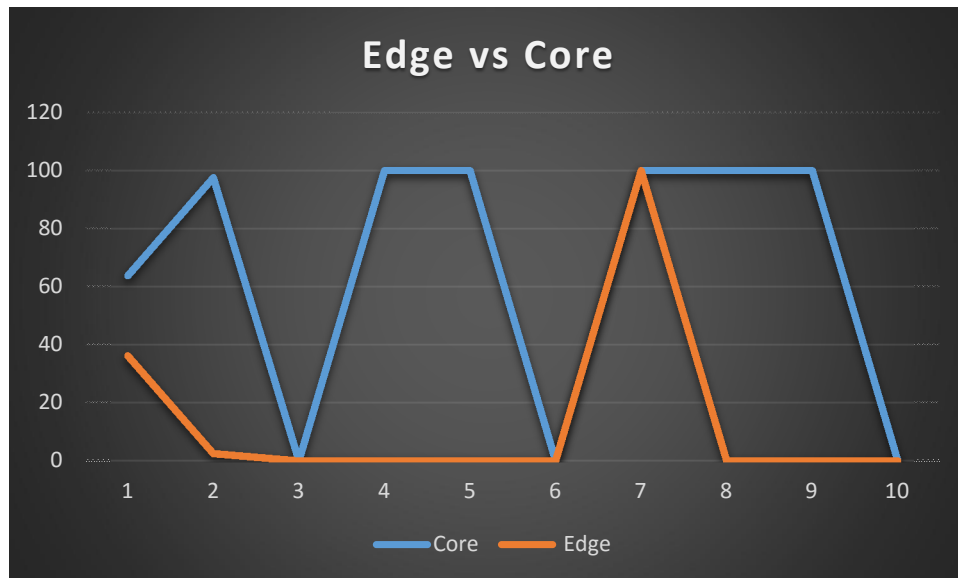
RSA host key for pl2.eng.monash.edu.au has changed and you have requested strict checking.
Host key verification failed.
```

4.3 Determining the outages into Edge and Core outages.

The outages that have been experience inside the Local ISP falls under edge outages and here in the traceroute the local ISP of whose node we are using to determine the route falls under edge. Any outages that falls in other then the local ISP are categorized under Core outages. As now we know what are the Edge and Core outages let us consider the data of outages and here we have the analyzed data for the Edge outages vs Core outages.

Paths	Edge	% Edge	CORE	%core
A->B	46	36.22	81	63.8
B-A	4	2.439024	160	97.57
C->D	0	0	0	0
D->C	0	0	90	100
E->F	0	0	1	100
F->E	0	0	0	0
G->H	177	100	0	100
H->G	0	0	16	100
I->J	0	0	452	100
J->I	0	0	0	0

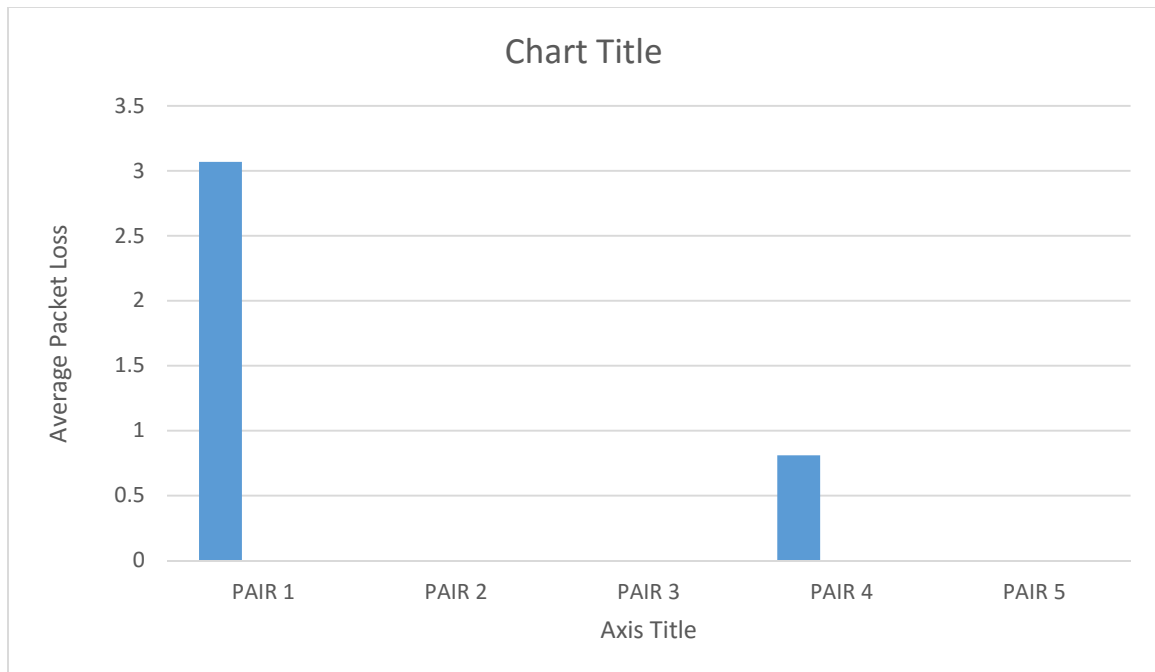
Chart to show Edge vs Core Outages



4.3 Reliability based on continent links:

In this section we are going to check if there is any significance difference in the reliability of continent links. In order to achieve this we use the packet loss parameter that we have encountered in the network among the links using ping tool. So we have to analyze the packet loss among different and I have come up with table values which shows the average packet loss percentage among a pair of nodes.

Node pairs	Average percentage error.
Pair 1 (South America – Europe)	3.07
Pair 2 (Japan-USA)	0.00
Pair 3 (USA-Canada)	0.00
Pair 4 (Japan-Europe)	0.81
Pair 5 (Europe-Canada)	0.00



Based on this table we can figure the reliability among the inter continent and intra continent links. Pair 3 is the intra continent and rest pairs are the inter continent links. So on the given data we can say intra continent links are more reliable than inter continent link. Since this is a tiny data examination to conclude anything on the strong note.

4.4 Fluttering

We use the term “fluttering” to refer to rapidly-oscillating routing.

In our experiment we have come across fluttering and there would many other occurrences which has been detected. The main idea of detecting fluttering is when it occurs and why? And the other question is what the post effects of fluttering?

In this section we are going to see an example of fluttering and at the end of this section we can figure the answers to the questions posted above.

In the traceroute from I->J we have fluttering occurring at a specific number of hop. “de-hmb.nordu.net (109.105.97.14)” Sweden is being routed sometimes and sometimes not. There is no specific pattern but a specific hop number is there where this server details are there with time.

1	165.242.90.1 (165.242.90.1)	0.818 ms	0.977 ms	1.095 ms		1	165.242.90.1 (165.242.90.1)	1.723 ms	1.806 ms	1.821 ms		
2	165.242.35.66 (165.242.35.66)	1.407 ms	1.487 ms	1.631 ms		2	165.242.35.66 (165.242.35.66)	1.947 ms	2.003 ms	2.201 ms		
3	165.242.3.35 (165.242.3.35)	2.933 ms	2.986 ms	3.041 ms		3	165.242.3.35 (165.242.3.35)	2.252 ms	2.380 ms	5.196 ms		
4	202.15.114.1 (202.15.114.1)	3.284 ms	3.300 ms	3.347 ms		4	202.15.114.1 (202.15.114.1)	6.483 ms	6.562 ms	6.622 ms		
5	hiroshima-RM-XE-4-0-1-0.s5.sinet.ad.jp (150.99.188.1)	3.416 ms		4.193 ms		5	hiroshima-RM-XE-4-0-1-0.s5.sinet.ad.jp (150.99.188.1)	7.091 ms	7.226 ms	7.135 ms		
4.247 ms						6	tokyo1-GM-ET-8-1-0-1136.s5.sinet.ad.jp (150.99.89.201)	14.726 ms	15.056 ms	tokyo1-GM-ET-7-1-0-136.s5.sinet.ad.jp (150.99.82.103)	13.337 ms	
6	tokyo1-GM-ET-8-1-0-1136.s5.sinet.ad.jp (150.99.89.201)	15.563 ms		13.293 ms		7	lax-GM-ET-2-1-0-100.s5.sinet.ad.jp (150.99.89.243)	112.088 ms	112.151 ms	112.211 ms		
ms	tokyo1-GM-ET-7-1-0-136.s5.sinet.ad.jp (150.99.82.103)	13.444 ms				8	207.231.246.7 (207.231.246.7)	119.981 ms	120.212 ms	120.460 ms		
7	lax-GM-ET-2-1-0-100.s5.sinet.ad.jp (150.99.89.243)	112.194 ms	112.196 ms			9	us-chi.nordu.net (109.105.97.81)	166.237 ms	164.149 ms	165.145 ms		
112.190 ms						10	us-ash.nordu.net (109.105.97.134)	181.198 ms	180.869 ms	181.001 ms		
8	207.231.246.7 (207.231.246.7)	120.085 ms	120.184 ms	120.328 ms		11	nl-sar.nordu.net (109.105.97.138)	278.516 ms	278.484 ms	272.295 ms		
9	us-chi.nordu.net (109.105.97.81)	163.912 ms	164.866 ms	166.269 ms		12	de-hmb.nordu.net (109.105.97.18)	283.160 ms	dk-uni.nordu.net (109.105.97.126)	274.954 ms	de-hmb.nordu.net (109.105.97.18)	282.775 ms
10	us-ash.nordu.net (109.105.97.134)	180.554 ms	180.816 ms	182.262 ms		13	de-hmb.nordu.net (109.105.97.18)	283.560 ms	ndn-gw.pionier.gov.pl (109.105.98.125)	262.912 ms	260.601 ms	
11	nl-sar.nordu.net (109.105.97.138)	278.042 ms	272.554 ms	uk-hex.nordu.net (109.105.97.140)	255.175 ms	14	ndn-gw.pionier.gov.pl (109.105.98.125)	260.660 ms	z-poznan-gw3.nask.10Gb.rtr.pionier.gov.pl (212.191.224.74)	267.172 ms	267.249 ms	
12	dk-uni.nordu.net (109.105.97.126)	281.635 ms	276.935 ms	277.051 ms		15	welcome-at.pw.edu.pl (148.81.253.70)	267.230 ms	z-poznan-gw3.nask.10Gb.rtr.pionier.gov.pl (212.191.224.74)	266.961 ms	265.371 ms	
13	ndn-gw.pionier.gov.pl (109.105.98.125)	262.991 ms	305.706 ms	289.899 ms		16	194.29.132.162 (194.29.132.162)	256.610 ms	263.948 ms	263.128 ms		
14	ndn-gw.pionier.gov.pl (109.105.98.125)	279.298 ms	z-poznan-gw3.nask.10Gb.rtr.pionier.gov.pl (212.191.224.74)	268.193 ms	268.095 ms	17	194.29.132.162 (194.29.132.162)	262.014 ms	256.180 ms	258.693 ms		
15	z-poznan-gw3.nask.10Gb.rtr.pionier.gov.pl (212.191.224.74)	267.769 ms	welcome-at.pw.edu.pl (148.81.253.70)	267.843 ms	267.877 ms	18	coi-mini.rtr.pw.edu.pl (194.29.132.2)	258.824 ms	256.302 ms	258.513 ms		
16	194.29.132.162 (194.29.132.162)	265.168 ms	welcome-at.pw.edu.pl (148.81.253.70)	267.902 ms	194.29.132.162 (194.29.132.162)	19	planetlab4.mini.pw.edu.pl (194.29.178.14)	257.292 ms	255.022 ms	257.151 ms		
17	194.29.132.162 (194.29.132.162)	255.604 ms	coi-mini.rtr.pw.edu.pl (194.29.132.2)	261.510 ms	194.29.132.162 (194.29.132.162)							
18	194.29.132.162 (194.29.132.162)	256.231 ms										

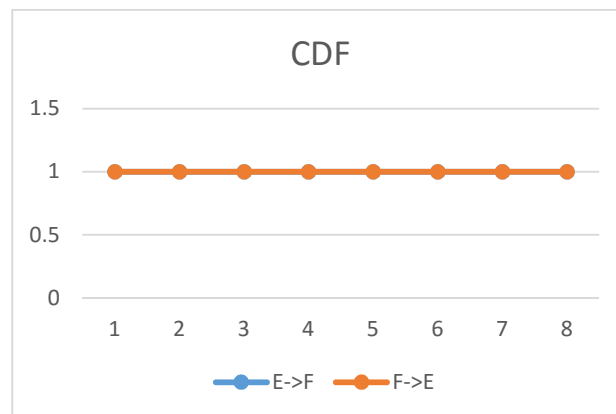
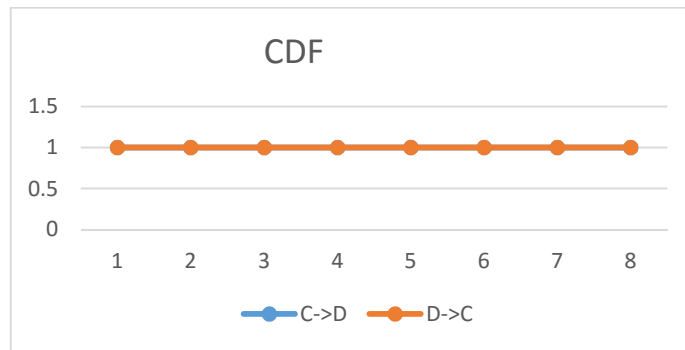
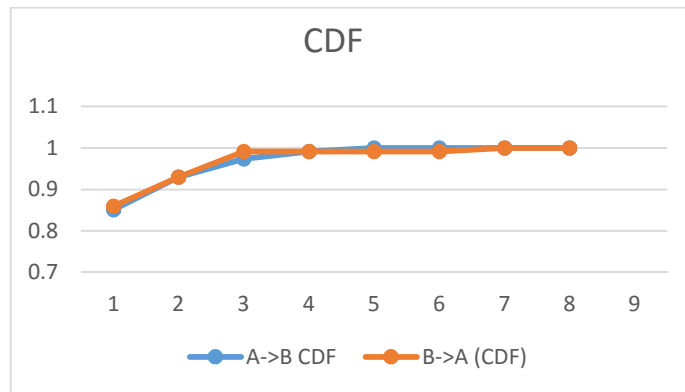
While fluttering helps in network to reduce the load on the other also causes problem to some application. First, a fluttering network path presents the difficulties that arise from unstable network paths (x 7.1). Second, if the fluttering only occurs in one direction, then the path suffers from the problems of asymmetry (x 8.1). Third, constructing reliable estimates of the path characteristics, such as round-trip time and available bandwidth, becomes potentially very difficult, since in fact there may be two different sets of values to estimate. Finally, when the two routes have different propagation times, then TCP packets arriving at the destination can lead to spurious “fast retransmissions” [St94] by generating duplicate acknowledgements, wasting bandwidth. These problems all argue for eliminating large-scale fluttering whenever possible. On the other hand, when the effects of the flutter are confined, invisible at the network layer (such as split-routing used at the link layer, which would not show up at all in our study), then these problems are all ameliorated. Furthermore, if fluttering is done on a coarser granularity than per packet (say, per TCP connection), then the effects are also lessened.

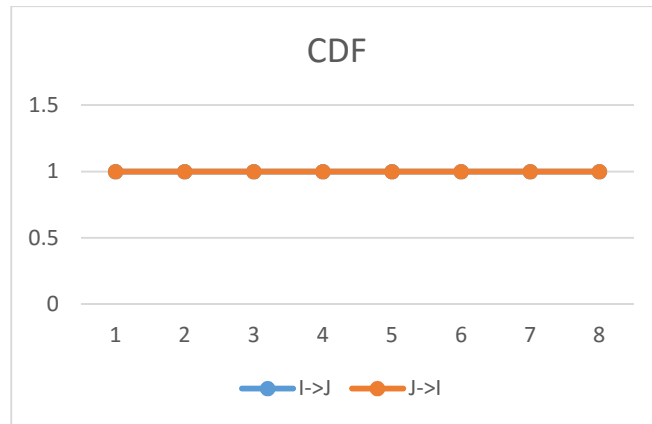
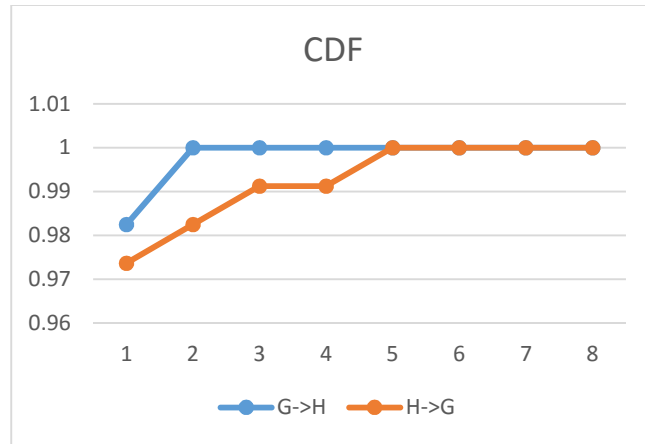
4.5 Detecting a hop out of unexpected general direction :

In section we will discuss the unusual routing in the network which cause unexpected hop. For an instance A node traverses from US to Germany through Asia is kind off unusual. This would cause the packet to travel more in the network which is a wastage of resource first of all. Then the second point is TCP cannot predict the path as such unusual and the RTT predicted would go wrong, which would case data retransmission for a packet which is taking unexpected hop path. These hops could also cause traffic for an unnecessary traverse.

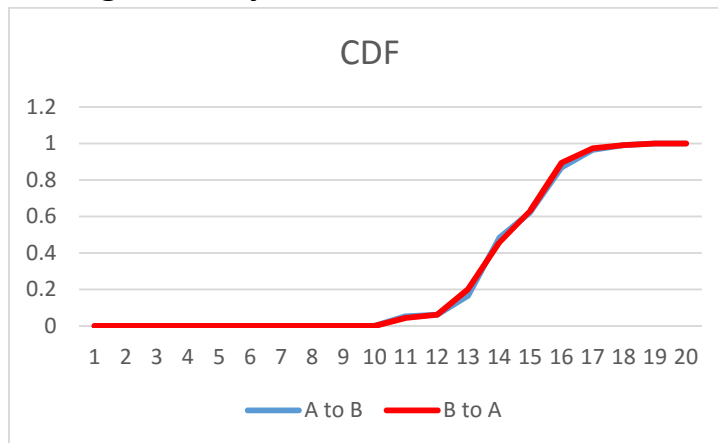
Regarding our project I have tried to detect any of these paths but I have noticed any. The reason could be this project data is tiny to have this unusual hop. Now let's consider the point of causing this hop. The algorithm sometimes work bad which is one instance of the case we are talking right now.

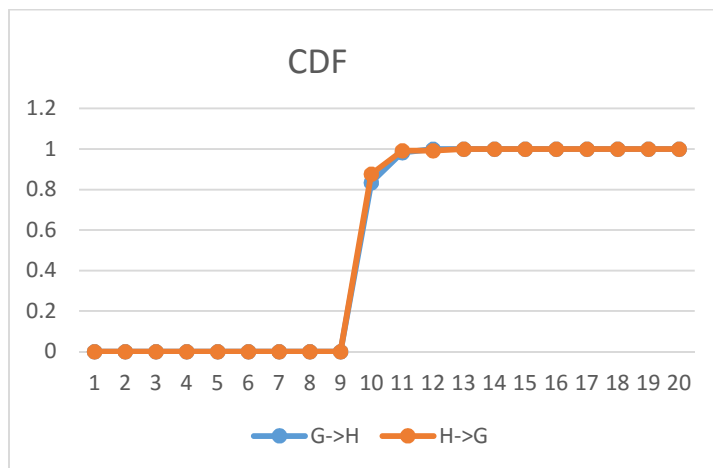
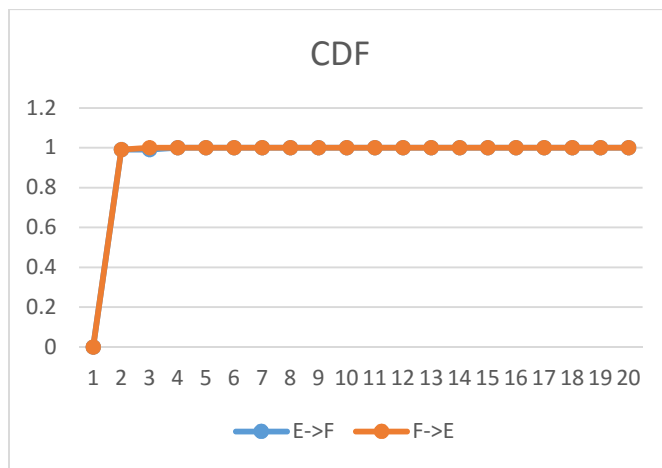
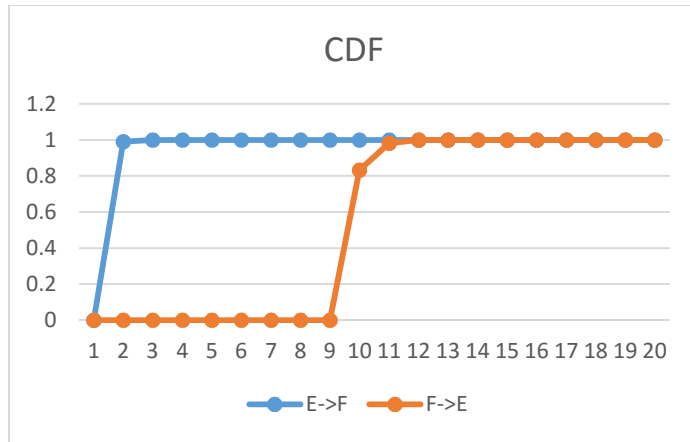
4.6 Average Packet loss in Pair wise:

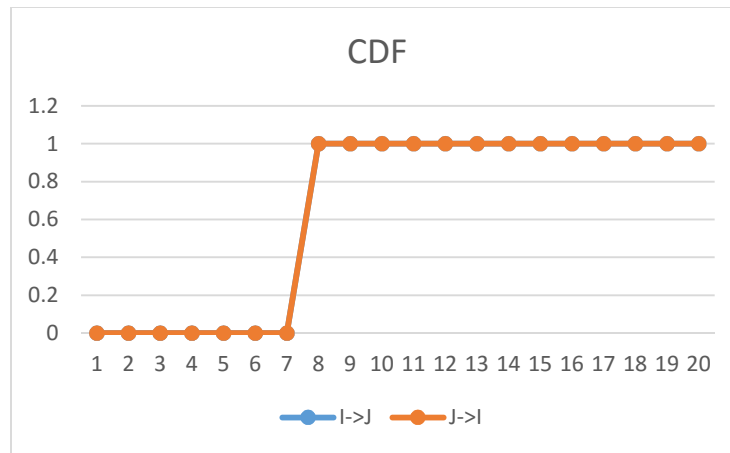




4.6 Average Latency in Pair wise Path:







5. Conclusion:

We have conducted our analysis on 10 nodes that have been geographically spread, over the period of two weeks. The study characterizes the path length and variations over these measurements. The next point we have emphasis our study on is the outages. The two types of outages, our study mainly focuses on the temporary outages. There are the data which shows that these temporary outages and the average error rate cause of temporary outage is around 5% which is wastage of our resource in trying to transmit. The concept we came across was fluttering, we have discussed the fluttering advantages and disadvantages so depending on the need we could use it.

Our statistical methodology helps us to know the probability of the latency at a given path among the node. Also we have extended our study not just to the latency but also the packet loss. We can see that the whole packet loss over this project was around 1.2% which is arguable and there should be some methodology to understand its causes.

Based on our data we can say it strongly that the internet stability has increased or decreased. For a pointed answer I think our project need be scaled big and the analysis data should be large enough to drag some conclusion based on it. But still basing on this observation a packet loss of 1.9% and temporary outage of 5% on whole hops seems to be stabilized internet routing. But as I mentioned earlier for a strong sentence we have make our project on a large scale.